Occasional Studies

Banknote design for retailers and public

DNB Occasional Studies

Vol.8/No.4 (2010)

Hans de Heij

De Nederlandsche Bank
Eurosysteem

Central bank and prudential supervisor of financial institutions

Author: Hans de Heij
e-mail: h.a.m.de.heij@dnb.nl

Aim of the Occasional Studies is to disseminate thinking on policy and analytical issues in areas relevant to the Bank.
Views expressed are those of the individual authors and do not necessarily reflect official positions of De Nederlandsche Bank.

Subscription orders for DNB Occasional Studies and requests for specimen copies should be sent to:

De Nederlandsche Bank NV
Communications
P.O. Box 98
1000 AB Amsterdam
The Netherlands
Internet: www.dnb.nl

Occasional Studies

Vol.8/No.4 (2010)

Hans de Heij

Banknote design for retailers and public

Abstract

Two stakeholders of banknote design are discussed, retailers and the general public. A retailer on average receives around 120 banknotes a day. A security check should be effected in less than two seconds and avoid discussion with the client. A private person on average receives one or two banknotes a day. For the public the probability of receiving a counterfeit is low and confidence in receiving genuine banknotes high. On the whole, people in the Netherlands are familiar with two security features, the watermark and the holographic stripe. In daily practice the public is not willing to verify a banknote, but if they do, it should be done within 6 seconds. A 'negative' stakeholder is the counterfeiter. They target the retailer and create counterfeits with UV features that look similar to – or even better – than a genuine euro banknote.

For a new banknote design a central bank may choose from over 20 retail and 50 public security features. This selection process is usually done in an organised way, although cost analyses are often not used (or published). However, this process by the central bank can be made more transparent and better manageable in an *all-in-one model*. A structured approach is suggested for the selection of both retail and public security features in the design of a new banknote. It starts with listing all features of the existing banknote and its users (security matrix).

The second step is a marketing analysis of the banknote to be replaced; the creation of a feature-action matrix. In case of the retailer it is a tool-feature analysis (e.g. ultra violet light, infra red light and magnifier) and in case of the public it is a human action-feature analysis (e.g feel, look, tilt). If desired these feature-action matrices are reset for the new banknote.
The third step is the most difficult one. The central bank has to decide which security features may be abandoned based on aspects such as public knowledge, user requirements, counterfeit analysis and costs. The study defines more than 25 of such criteria which a central bank may consider. Other criteria may be added; it is an open method.
The retail and public features that are retained should be enhanced, not only technologically, but also in terms of design in order to improve their usability.
The last step is the selection of new features. These features should fit into both the (reset) action-feature matrices and meet user requirements. A wider choice of

automatic devices is needed that are more reliable. To come to reliable detector features the central bank may include such features while leaving the development of the devices to the market. There is also a need for new human assisted retail features, since UV light and magnification features should be replaced.
In case of public features there is a need for a wider choice of feel and look-at features.

Selecting public features is only the first part in the design process of new banknotes. After this, a central bank must decide on the conceptual design of the public security features. Experimental psychology may support the development of innovative banknote design concepts, which is illustrated by several examples.

This study also covers the counterfeit models developed and used by DNB since 1814. The recent models have been updated and now form part of the method proposed, such as *intrinsic and extrinsic features* (1976), *internal and add-on features* (1985), *system approach* (1991) and *the simple method* (2006). Other models introduced are *resilience grades* (European Central Bank, 2007), *secure calc* (US Treasury, 2009) and *security effectiveness* (Bank of Canada, 2010).

Keywords: applied design, currency, payment system, cash money, banknote design, retail security features, public security features, counterfeiting.

Table of contents

Abstract 5

1. Introduction 9

2. Generic security matrix 17

3. Retailer 27
3.1 Analysis of retail security features 27
3.2 Method for selecting retail security features 41
3.3 Designing retail security features 49

4. Public 53
4.1 Analysis of public security features 54
4.2 Method for selecting public security features 74
4.3 Designing public security features 84

5. Central bank 123

6. Counterfeiter 127
6.1 Counterfeit analysis 127
6.2 Methods to analyse counterfeited banknotes 130
6.3 Design principles against counterfeiting 149

7. Conclusions 153

Acknowledgement 153

Appendix 1 - Public knowledge of security features 155
Appendix 2 - Intrinsic and extrinsic security features (1976) 159
Appendix 3 - Internal and add-on features (1985) 161
Appendix 4 - System approach (1991) 167
Appendix 5 - Simple method (2006) 191
Appendix 6 - Time required checking a banknote 195
Appendix 7 - Nested features 203

Appendix 8 - Response policies of central banks on counterfeited banknotes 204
Appendix 9 - Which features should be developed? 209
Appendix 10 - Conjoint research: what does the public want? 217
Appendix 11 - All-in-one method applied to retail features in euro banknotes 221
Appendix 12 - All-in-one method applied to public features in euro banknotes 231

References (Chronological) 241

Publications in this series as from January 2003 253

1 Introduction

A stakeholder approach as a basis for banknote design was proposed by De Nederlandsche Bank (DNB) in 2007 in the Occasional Study 'Public feedback for better banknote design 2' written by Hans de Heij [94]. To implement such a stakeholder approach in the design process of a new banknote, a methodology was proposed in 2008 using a 'Programme of Requirements' [108]. Listing the requirements from a user's point of view should be the start of banknote design. In 2009 the user requirements of three stakeholders, the colour-blind, the partially sighted and the blind, were published by DNB [148]. This study continues with the user requirements of two more stakeholders, the retailer and the general public. The counterfeiter is introduced as a third, 'negative stakeholder'. The cost of new produced banknotes is paid by the central bank and therefore the bank is a stakeholder, too.

The security industry has launched many new security features, especially for the public. This current preoccupation with providing banknote security features for the public is questioned. Central banks can choose between more than 50 public security features. One of the questions is, do central banks target the right user group? Should the focus not be on the retailer instead of the general public? [166]. The retailer is a key person in preventing acceptance of counterfeit banknotes; on average they receive around 120 banknotes a day, against just one or two by the public. The focus of the Bank of Canada is also primarily on retailers rather than the public. However, this is not yet common practice among central banks.

One of the main tasks of a central bank's currency department is to design banknotes that can be authenticated. We have to keep in mind that the individual features are a means to this end and not an aim in themselves. 'Security features are only as good as the authentication checks made on these notes' is a valid statement made by the Bank of England in 2010 [167].

Accountable and transparent central banks

Little is known about banknote design for reasons of confidentiality. Modern governments are stepping back, leaving more responsibilities to citizens, who are better educated and have their own opinions. Following this trend, modern central banks should become transparent and accountable for their policies, including banknote design. For example, since 1985 the United States Department of the

Table 1

Year	Public input asked by central bank on
1965	Introduction of low denomination, NLG 5 (Netherlands)
1978	Introduction of mid-denomination, NLG 50 (Netherlands)
1981	Introduction of high denomination, NLG 200, 250 or 500 (Netherlands)
1983	Start of 2-year periodic 'knowledge and appraisal' (Netherlands)
1996	Euro design contest (European Monetary Institute)
1999	Themes (Canada)
2004	National side of euro coins (Estonia)
2005	Design contest (Denmark)
2006	Names suggested for new designs: input possible via website (UK)
2007	Design contest (Switzerland)
	Dimensions, subjects for new euro design (Netherlands)
2008	2-euro coin design by internet (EU)
2009	Conjoint analysis of public security features (Netherlands)

Overview of the history of invited public input in banknote design (non-exhaustive).
NLG = Netherlands guilders

Treasury has published several public reports on the 'next generation currency design', the most recent one in 2007 [15, 25, 36 and 102]. 'Any change to the design of the currency would not be made without a public debate; it is hoped that this report will add value to the debate,' according to the 1993 edition. A similar statement is made in the 2007 edition.

Central banks are also more open on the planned introduction date of the new banknote series. Examples of this trend are Canada, Denmark, the euro zone, Switzerland and the USA.

More public input
Modern central banks involve the public more and more in the banknote design process. Table 1 provides a non-exhaustive overview as first described in 'Banknote opinion polls: a method for collecting customer feedback on banknote design' [112].

To gain public input and opening the dialog central banks could start to use the *Social Media* on the internet like online forums, blogs and social networking sites ('crowd surfing').

How should a central bank organise the selection process for new retail and public features so that new banknote designs will be counterfeit-proof?

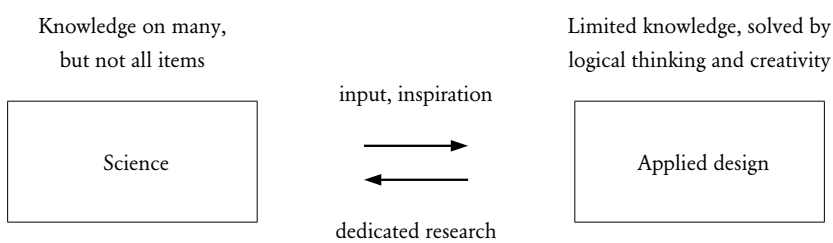
The study introduces the 'all-in-one method' to select security features for new banknote designs. This approach lists all relevant issues for a smooth decision making process. This is necessary as central banks seem to follow each other in suboptimal features promoted by the security industry.

Balance between science and confidentiality

This study is a balance between opening up the methodology on banknote design on the one hand and the confidentiality of design security principles on the other, especially machine-readable features. Being more open about the methodology is a further step towards a scientific approach, necessary for the author's thesis study 'Key elements in banknote design'. A scientific approach means bringing the findings to the public domain and linking them to other references. However, many references in the banknote design world are confidential and may not be quoted. Internet has led to fast and widespread information dissemination, making it more difficult for central banks to keep information confidential. Instead of rearguard action, central banks could proactively feed the internet with (controlled) information. The future trend will therefore be to bring more and more information to the public domain as is already the case in the United States, Canada, the United Kingdom and the Netherlands (e.g. by DNB).

Being more open could also close the information gap between central banks and the industry, as will be explained further on in this study. Of course, a central bank does not have to say how ultimate security features are constructed in order to prevent counterfeiting. However, patent applications by central banks or suppliers may also unveil the basic security principles, since all patent applications are made public. Key in the banknote's security are not the individual security features, but the integration of these features in the banknote design.

Figure 1



Schematic presentation of the relation between science and applied design. The aim of science is to increase knowledge; the aim of applied design is to solve a design problem. Scheme prepared by author.

Table 2

Argument	Example
Counterfeits	Existing banknotes are counterfeited too much (e.g. above a certain threshold).
	Enhance quality of security features (e.g. new feature on the market).
New denomination	Introduction of a high denomination (because of inflation).
	Dropping zeros (because of inflation).
	One denomination is very popular, releasing pressure by introducing new denominations (e.g. filling the gap between 25 and 100 by introducing a new 50).
Public criticism	Note is not appreciated by public.
	Note looks outdated.
Durability	More durable, e.g. polymer notes.
	Banknote dimensions suboptimal for wallets; trend towards smaller banknotes.
Improvement	Mistake(s) in old note, e.g. in text or year.
	Improvements for visually impaired.
Additional income or propaganda	Commemorative notes.
Logistics	Need to restock (choice between reprint or a new design).
Management	Maintaining a central bank's know-how (constant flow of new banknotes, e.g. a new note every two years).
	New Governor/President, new Secretary (e.g. new signature).

Overview of a central bank's arguments to introduce a new banknote or a new series of banknotes.

Applied design
Every day central banks realise new banknote designs. Keep in mind that this study focuses on tomorrow's contracted graphic designer. What should the central bank tell the new banknote designer?
Finding an answer follows from the development phases of 'applied design': information, analysis, problem definition, planning and drafting; each a necessary step towards the ultimate design phase. Not all knowledge is available in applied design; the design team has to work with what they know as illustrated in Figure 1.

Why a new banknote?
People often ask, 'Why do we need a new banknote?' The answer is 'To keep up with technological developments in the reproduction industry.' This is, of course, a very general answer. In fact, there are several reasons for introducing new banknote series (Table 2). An example is the development of the second series of euro banknotes (ES2), in which one or more innovative security features would be introduced for public use, the so-called 'quantum leaps'. Instead of a new design it was decided to upgrade the current banknotes, re-using the main design elements from the first series [e.g. 57, 58, and 99].

Strengths and weaknesses of banknotes as a means of payment
A second question people often ask is, 'Will we still be paying with banknotes in the future?' The reply is: 'Yes. Cash money will be used in the future, too, because it has sustainable competitive advantages over other means of payment, such as debit and credit cards, but also over newcomers like e- and m-payments.' E-payments are electronic payments via the internet, and m-payments require a universal mobile phone as a payment device and terminal. The strong points of banknotes and coins are that they:
- Permit direct person-to-person payment (without any intermediate),
- Guarantee anonymity,
- Allow fast settlement, within less than 20 seconds,
- Provide a sense of reliability, as payment does not depend on technology functioning properly,
- Guarantee insight into the amount of money available and, consequently, budget control,
- Allow for hoarding (e.g. in case of limited trust in saving accounts at commercial banks or in case of a financial turmoil),
- Are relatively cheap (compared to other means of payment).

The weak points of banknotes are that they can easily be lost, stolen or taken in a hold-up, can be counterfeited and are relatively costly to society.

Of course, some of the strong and weak points of cash money are also true for other means of payment. A recent study in this field was published in June 2009 by Anneke Kosse (DNB) [162].

Cash payments will probably decrease
What will change most probably the coming decade is the number of cash transactions in the Netherlands. Since 1814, banknote circulation has roughly increased yearly, both in volume and value. However, since the 1990s growth of the value of banknotes in circulation has not kept up with economic growth. We are on the eve of a decline in banknote circulation in the Netherlands, since the use of debit card payments was further encouraged in 2009 in a public campaign. In 2009 DNB for the first time in its history registered a decline in public demand for banknotes. In that year, the amount of banknotes withdrawn from ATMs dropped by about 10% [163]. Dutch supermarkets would like to reduce cash payments to a minimum. In the near future they will further encourage the use of debit cards, for example by introducing more 'PIN only' checkouts (PIN = Personal Identification Number, the four digit code of e.g. a debit card).

Euro banknotes, for daily payments and hoarding
Euro banknotes are both used for daily payments and hoarding (banknotes used as a store of value). Analysis by the European Central Bank (ECB) in 2010 reported that around 2/3 of the total *value* of all euro banknotes in circulation is used for hoarding, especially outside the euro area. Euro banknote circulation is still growing, but gradually at a lower pace. Future growth is mainly expected as an increase in higher denominations [171].
One might conclude that the use of euro banknotes is shifting from a daily payment instrument to a hoarding tool. However, this could be the case because of today's specific situation; the interest rate is at a historically low level of around 1% and public trust in financial institutions is also low because of the financial turmoils in the period 2007-2010.
In June 2010, the Bank of England reported that 'there is more cash in circulation than ever before'. They also noticed an increase in demand for higher value notes during the credit crunch [167].

When do people pay cash?
On different occasions people pay differently as research in the Netherlands [73] and Germany [153, 168] shows. The German investigation explicitly sums up the situations where cash is the favoured means of payment:
- Fast-food restaurants, cafés, pubs and snack bars,
- Chemists,
- Retail businesses for daily needs,
- Retail businesses for longer-term needs,
- Petrol stations,
- Hotels and guesthouses.

The value and perception of money

Value perception is another argument why cash money will continue to be used in the future. The form money takes, influences its perceived value. According to Prelec and Simester, people are willing to pay twice as much for a basketball game ticket if they use a credit card than if they paid cash. Cash money is perceived as more valuable than credit card money, because the credit card is financed with future income. Cash money comes straight from their pockets, while credit card settlement is further away in the future [47].

For charity, people would rather put a few out-of-pocket coins into a money box than use a debit card. It feels as if coins are already lost anyway. Parents and grandparents will recognise this feeling when giving their (grand) children pocket money.

A similar feeling was reported in Italy in 2002, when the euro was introduced. Italians were used to tipping at restaurants using banknotes, since coins were not worth much. The 1,000 lira banknote equalled 0.516 euro. From this point of view, it is understandable why, in 2003, the Italians pleaded for the introduction of a one-euro banknote. However, by now, the Italians have learned to live with coin tipping.

Finally, the elderly will tend to stick to the use of cash, as they are used to it and trust this means of payment over others. Research by the Bundesbank showed that two groups use cash more than others, i.e. youngsters (18 to 24-year olds) and the elderly (over 54 years) [153, 168].

2 Generic security matrix

The first banknotes issued by DNB in 1814 were called 'robins' and had four security features. One of the security features was the handwriting (see also section 6.2.1.1 on unique original). These first notes of April 1814 were temporary. The notes were made rather hastily; delivery by Enschedé occurred within three days. For the second delivery, in October 1814, two new security features were added. The paper had a watermark and in the middle of the notes 'DNB' was printed in blue using gravure print. So in 1814 six security features were used in NLG banknotes. See also Section 6.2.1.1 on unique original

More and more security features
The first forged NLG banknotes appeared in 1836. DNB responded immediately and ordered a new series, replaced the watermark and did not change the print. Twenty years later the Board of DNB took the decision to issue a whole new type of banknotes. The main reason was that the robins were forged and counterfeited. The invention of photography made it possible to copy a banknote directly onto the stone of a lithographic printing machine without the intervention of an engraver. The extent of the circulation was increased to about 90 million guilders, making it impossible to sign all banknotes by hand. The signatures of the Board and the date of the new model (1860) from now on were printed by Enschedé, as the value indications had been since 1825. For safety reasons, banknotes were numbered by the central bank. Those numbers were no longer handwritten by a clerk; instead, numbering presses were ordered and this meant the birth of DNB's printing house [16, 34, 43, 55 and 105].

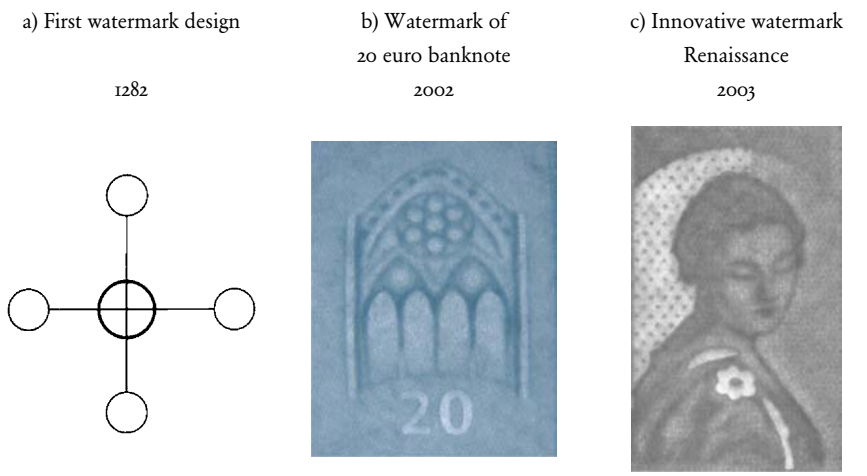
Modern banknotes contain far more features than the four to six found on the first banknotes in the 19th century. New features were added to these existing ones, such as a security thread. Foil and silk screen printing were introduced in the 1980s to combat colour copying of banknotes.
Today, central banks can no longer just add features to a new banknote design. Banknote sizes are much smaller than in the old days and there is also a much wider choice. Besides, each time new features are added, the costs of the notes will increase. The question for central banks is how to make a balanced choice of the features on offer.

Old features are kept

If new features are added, old features have to be shed. This may sound logical, but it is often not the case. Existing features, for instance the watermark, are usually kept. The first watermarks were made in Bologna, Italy, in 1282, long before the first Western banknotes appeared. This means it has a lifespan of well over 700 years! The first multi-tone watermarks were issued by the French central bank in 1829, followed in 1855 by the first shaded watermark in the banknotes of the Bank of England. Watermark technology is improved over the decades, while the basic principles are kept. In the 1990s watermarks appeared combining both line and shaded watermarks (Figure 2).

Letterpress and gravure printing are also still in use at all banknote printing works. These production techniques have a long history, too. The very first Western banknote was issued in 1657 by Stockholms Banco and was printed by letterpress,

Figure 2



a) Sketch of the first line watermark, Bologna (1282). The first NLG notes in 1814 included such a line watermark.
b) Multi-tone, mould made watermark of 20 euro banknote. The numerals 20 are a line watermark (also called 'electrotye watermark' or 'high light').
c) First watermark combining three different techniques: a shadow watermark (portrait), three line watermarks (high lights in coat) and a 'pixel watermark' (background of the portrait). Pixel watermarks were developed by ArjoWiggins Security Products in 2002/2003. Pixel watermarks are created by attachment of a piece of metal onto a mould to give a low density of fibres in the corresponding part of the watermark. The first pixel watermarks were used to create a lighter area in a banknote paper, e.g. for the area of the see-through register.
The idea to create a shadow watermark with an integrated line and pixel watermark was made by DNB (De Heij) in 2003. The proposal of DNB was to use the watermark 'Renaissance' as designed by Inge Madlé for an emergency euro 50 banknote in 2000 ordered by ECB/DNB.
The watermark shown was prepared for DNB in November 2003 by security paper mill VHP, part of ArjoWiggins Security Products [112].
The first banknote using an additional pixel watermark is the Mexican 200 pesos, a commemorative banknote issued in September 2009.

which is still used today for banknote numbering. The first copper plate engraving was used for British pound banknotes in 1694 and is also still considered to be an essential part of a banknote [26, 38, 46]. A tradition spanning over 300 years. The origin of micro-printing is not exactly known, but Dutch guilder notes issued in 1860 are the first available example of micro-printing in offset used in banknotes. Still in use as a security feature in many banknotes including the euro, the application of micro-printing is a tradition spanning 150 years.

Features for detectors
The same pattern is observed for machine-readable features, as presented by De Heij (DNB) at Banknote 2005. The use of UV features, which can only be discerned using UV light, has spanned over 40 years. IR features have been in use for around 35 years. The lifespan of the magnetic and spectral properties exceeds 25 years.

A conclusion of this paper is that features migrate from higher to lower user levels. For example, the UV feature was introduced in the 1970s as a machine-readable feature for central banks and around 1985 became a retail feature. Another example is the ISARD, which was also introduced in the 1970s as a machine-readable feature and today is used as a nail scratch feature in the euro series (see Appendix 3) [69, 81].

Long life cycles for DEM and USD notes
Nowadays central banks claim that banknotes should be upgraded with new public security features. This trend started in the 1980s. Let us briefly look at the time when banknotes circulated for decades and were not replaced often.
The German Mark banknotes (DEM) first issued in 1948 circulated until the mid-1990s, a life cycle of some 40 years. With 68 years, the life cycle of the US dollar series was even longer. In 1996, US dollar banknotes received their first major change since 1928. The intervening years had seen the introduction of minor changes (e.g. the addition of 'In God We Trust' in the mid-50s; the replacement of Latin by English on the treasury seal in the 60s, and the application of micro-printing and security threads in the early 90s).

Life span of NLG features
When DNB still issued its own Netherlands guilder banknotes, no new public features were introduced for 70 years. Instead, DNB enhanced understanding of its public banknote features by optimising the design of the banknotes and through publications. Machine-readable features came in 1968 and foil and silk screen were introduced in the 1980s as *anti-copy features*. If these failed (no gloss) or were absent, the public would be triggered to check the watermark and other public security features.

Life cycle of NLG banknotes: 12-15 years
DNB's policy in the 1980s was to issue a new banknote design every two years. This

means that, with six denominations, an NLG banknote series' life cycle would be around 12 years. This policy ensured a constant work load for the central bank, designers and printing works. However, new versions of the most counterfeited denominations, e.g. the NLG 100 note, were issued more frequently than others. The result was that the public usually carried banknotes from different series in their wallets.

Shorter life cycles
Today's trend towards shorter life spans for banknote design is a constant. The question is, 'Are we heading for life cycles of 5, 10, 15 or 20 years?' Short life cycles of 7 to 10 years are foreseen by the United States Department of the Treasury. On the website of the Department of the Treasury's Bureau of Engraving and Printing (BEP) you can read, 'In keeping with the strategy of maintaining the security of our currency by enhancing the designs every 7-10 years, a new series of U.S. currency is being issued.' An example is the replacement of the 1996 USD 20 model in 2004.

In 2003, the ECB also assumed that a new banknote's life cycle would be around seven years and that a further decline in lifespan was likely [57, 58]. However, the lead time to realise the second series of euro banknotes (ES2) already exceeds these seven years. The ES2 project started in 2003 and is expected to 'be issued in a few years' time' (2008 ECB Annual Report). Indeed, the first factor determining the life cycle of a banknote is the time required to develop a new design.

Legal lifespan of security features is 20 years
The lifespan of many security features is clearly much longer than that of a banknote design. Still, central banks argue that new banknote designs are required to stay ahead of the counterfeiter. That is in fact the case, some new features are added, but most features rely on existing banknote techniques.

The life span of a series of banknotes can be set at 20 years, being the period a patent – if applicable – provides the central bank the exclusive rights to use this feature. Therefore, recently patented or soon to be patented security features should be selected. The central bank as patent owner has the exclusive rights to the feature's use. This is a reason for central banks to come up with a new banknote, since after this period of 20 years the feature may be produced free of any claims. Recently, the patent on optically variable ink (OVI) expired, giving anyone access to the production of such inks or the right to order such inks, such as the 'metameric optically variable pairs' presented in September 2009. Some features may have an additional 'nest level,' which is still protected by a patent even if the patent on the original feature has expired (nest levels are explained in section 4.1.7.6).

New security features are usually a dedicated barrier against counterfeits coming in (photography in the 1850s, colour copiers in the 1980s, home scanners in 1990s).

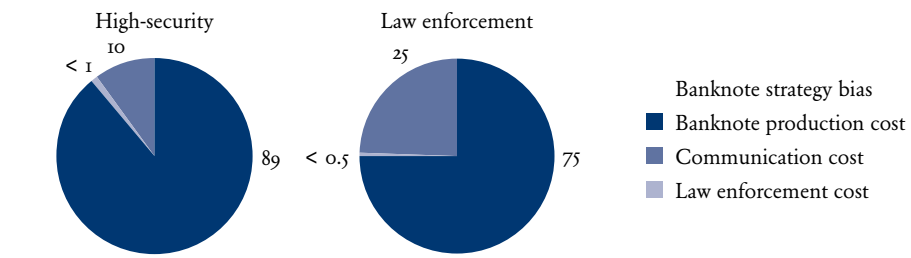
After 30 years of groundbreaking innovations in the reproduction and information technology industry, it appears that no new (technical) threats are in the offing. This makes it more difficult for central banks to target a specific phenomenon. Recent features like micro-optics or inks with a magnetic kernel are examples which are not focussed on a specific threat. Inspiration is also found in the combination of two worlds: the polymer banknotes with their characteristic transparent areas and the traditional, cotton based banknotes, which have no transparent areas. Such new features known as 'transparent windows' are also not focussed on a specific threat; they are meant to build additional barriers to the counterfeiter. The patent on a transparent window in banknotes (*Wertpapier mit Fenster*) will expire in 2015 [39].

Banknotes too small for all features

Since banknote dimensions have been reduced over time, in some cases over 50% [148], central banks have to discontinue obsolete features; otherwise there is not enough space for new ones to enter the banknote design. Awareness of the need to limit the number of security features is increasing. 'As we continue to develop security features, we need to ensure we do not overcomplicate banknotes for the public,' stated the well known security printer De La Rue Currency at the 2008 Currency Conference [118]. Usually, it is a tough decision for a central bank to take, since once a feature is 'in,' it is hard to get it out. The public has grown accustomed to it and retailers have invested in authentication devices and training. And last but not least, central banks also want to retain certain features, for instance, the ones used in their sorting machines.

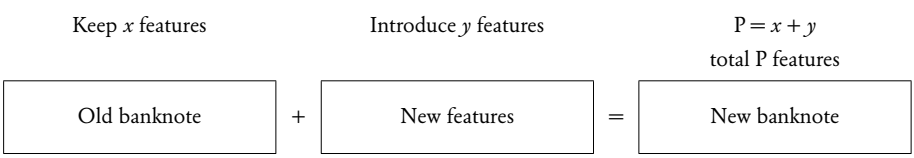
Figure 3

Percent



Two basic strategies to protect banknotes against counterfeiting. Central banks following the strategy of high-security banknotes will spend relatively more money on the security of banknotes. Central banks opting for the strategy of law enforcement will spend relatively more money on law enforcement. The figures are estimates; fictional figures.

Figure 4



Example of the gradual approach applied to the selection of P security features for the new banknote. P may refer to a typical user group, such as retail or public security features.

Self defending banknotes

A central bank may have a bias towards either more secure banknotes or to law enforcement (Figure 3). This bias is driven by national culture. In Europe, central banks rely more on *self defending banknotes*, while for example the US Treasury has a stronger bias towards *law enforcement with respect to criminals reproducing banknotes*. This bias towards law enforcement dates back to President Lincoln, who explicitly assigned the Secret Service the task of combating counterfeiting and this still holds today. The European bias towards self defending banknotes explains why the production of euro banknotes involves two more steps than that of the US dollar, namely foil and silk screen printing (or rotogravure). This makes euro notes more costly than dollar notes (see also Chapter 5 on banknote costs) [156, 175].

Features have to leave

Most central banks have been issuing banknotes since the 19th century and replace existing banknotes with new ones for reasons discussed in the Introduction. In case of the launch of new security features, the basic change policy would be to introduce a number of *y* new features. In the event of a total of P features, *x* features are kept $x = P - y$). This principle is illustrated in Figure 4 [108].

The first central bank to limit the number of security features beforehand was probably DNB in 1989. During the design process of the NLG 100/Little Owl, which introduced several new security features against colour copying, the limit was used for the first time. If new features are introduced, others have to go, DNB argued. The limit was set at 20, divided over several user groups, including 4 security features for the public and 3 for retailers. Since the previous banknote (NLG 25/Robin) incorporated 20 security features, the limit was set at 20. In 2000, DNB for the first time published the *security matrix* listing all stakeholders, as applied for the NLG 10/Kingfisher. In this case the total number of security features was also set at 20 [44, 81, and 94].

Table 3

Level	Letter(s)	Type of stakeholder/feature	Number
0	T	Trigger *(retail and general public)*	3
1		*Retailer (R)*	
	RA	a) automatic device in shop	2
	RH	b) human assisted, visible	1
2	P	*General public*	3 - 6
3		*Banknote Equipment manufacturers (BEM)*	
	BA	a) banknote acceptors	- *
	TS	b) detector(s) third-party sorting	1 - 3
4	B	*Central banks*	3
5		*Counterfeit Deterrence Systems (CDS)*	
	CC	a) colour copy machines	1
	CS	b) scanners, all-in-one devices	1
6	F	*Forensic*	3
Total	**N**	**Total security features**	**18 - 23**

Generic security matrix listing the different stakeholders (in italics) and their type of features.
N = T + RA + RH + P + BA + TS + B + CC + CS + F.
*) often used: thickness of notes and spectral properties like opacity and colour measurements. Suppliers of banknote acceptors need tight tolerances of the banknotes produced.

Generic security matrix

Many central banks would not be able to produce a clear list of all stakeholders and their features for their notes. This also depends on the definition of a security feature. Hence, the first step in the *all-in-one method* proposed in this study is to define a security matrix of the banknote to be replaced by listing all security features and adding its users or stakeholders. A generic *security matrix* is provided in Table 3. It is, of course, up to a central bank to set a limit to the total number of security features N.

Three 'independent' features for each stakeholder

In general three features for each stakeholder are enough. When three security features are statistically independent from each other and the expected probability on reproducing one feature is 1 in 1,000, the probability that all three features are well reproduced is $(10^{-3}) \times (10^{-3}) \times (10^{-3}) = 10^{-9}$, or 1 in 1,000,000,000, which DNB at the time of the NLG notes considered a low probability and thus considered a safe banknote!

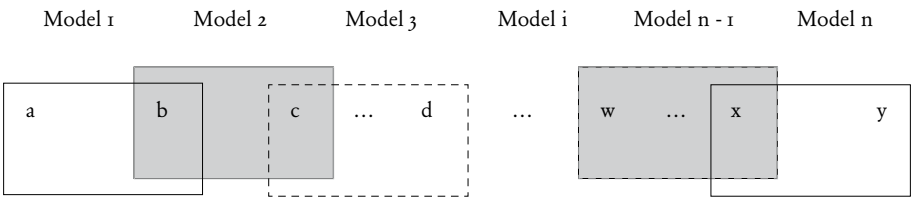
With seven user levels as defined in Table 3, the total number of security features would be N = 21 (= 7 x 3).

Definition of a security feature
In 1994 the Swiss banknotes set a new record; over 30 security features were incorporated. At the 2009 Banknote Conference, the ECB revealed that the number of security features classified in their Counterfeit Monitoring System (CMS) is 33 [149]. In the CMS, fluorescent fibres count for 6 features (red, blue and green on both front and reverse), while other central banks, like DNB, consider this just one feature, a clear example of a different definition of the same security feature (or features). This is one of the reasons why different figures are provided, varying from 26 by Klaus Bender [90], to 33 by the ECB, and 37 according to DNB [81]. This high amount of security features in the euro was the result of the policy of the greatest common divisor, which provided that in 1996 all 11 central banks adopting the euro banknotes could keep their security features (Twelve countries introduced the euro coins and banknotes in 2002; Greece joined the euro area in 2001).

Most important stakeholder?
Cashiers, cash handlers, banknote tellers, shop keepers, super market check-out staff, merchants or retailers are terms for those who are using cash professionally and especially for the person taking care of the cash transactions with the client, the person at the cash desk. In this study the term retailers is preferred and as the most important users of banknotes, they are set at level 1, based on the analysis done in Sections 3 and 4. A stereotype of a shop can not be recognised; there are one-man businesses on the street and large chains of shops. Large shops often have a back office where banknotes may be verified by trained security employee.

New banknote designs should first of all focus on retailers instead of the general public, since they are the most crucial party in preventing the spread of counterfeit banknotes. As said in the Introduction, this is not yet common practice at central banks.

Figure 5



Generic principle of continuity of automatically detectable retail features (RA) in subsequent banknote series. One of the two features should be compatible with the old series and should therefore overlap with the next banknote series (backward compatibility).

Define R
Three retail features (R) are anticipated in the example of the generic security matrix provided in Table 2, two for automatic detection (RA) and one for human assisted detection (RH). Since retailers would most probably like to use automatic devices instead of human assisted ones (like UV lamps), automatic devices have priority over human assisted ones.
In case retailers do not have authentication devices, they may use the public security features.

Backward compatibility of retail features in automatic devices
When a new series of banknotes is issued, a retailer still needs the existing detection technology to authenticate old banknotes. A retailer is not inclined to buy a new device when a new banknote is issued. That is why central banks should have a generic policy to introduce new machine-readable features, as illustrated in Figure 5. This generic principle of being 'backwards compatible' not only applies to banknote authentication devices used by retailers, but also to other banknote processors such as banknote acceptors and banknote sorting machines.

Define P
Once the central bank has decided on the number of retail features, the focus will be on public features. In the case of the euro banknotes, six features are dedicated to the general public, while only three are needed for reliable authentication. On average, about 2.5 features are recalled by the Dutch and only very few people are able to recall four or more features. It seems that 4 features suffice [44, 81]. However, central banks may want to opt for a mix of *active* and *sleeping* public security features. For example, three features will be actively communicated, while two public features will be kept dormant. Dormant features will be activated – some or all – if one or more of the other features are found to be heavily counterfeited.

Table 4

User group		Number	Remarks
Level 1	Public	6	
Level 2	a) Retailers – human	2	
	b) Retailers – automatic device	At least 4	
	c) Third-party sorting machines		
Level 3	Central bank sorting machine	4 to 6	2 or 3 in substrate and 2 or 3 applied in printing works

Overview of the proposed number of security features in the Euro Series 2 (ECB).

People can make their own choice in case of more than three public features. Older people can stick to the features they learned at a younger age. This implies that the minimum set of public features is three and the maximum is six, or $3 \leq P \leq 6$.

Trigger features
Specific banknote features prompting the *subconscious authentication*, of the banknote are called *trigger features*. Trigger features were first introduced by De Heij in 2006 [81]. Examples of such trigger features are different paper tints, scan and screen traps, bright colours outside the euroscale, grey colours and the banknote paper properties. Trigger features are further explained in Section 4.1.1.

Security matrix Euro Series 2
At the 2007 Currency Conference, the ECB presented the desired number of security features for the next series of euro banknotes (Table 4), based on work done in 2004 -2005 and broken down into three user groups (levels 1, 2 and 3) [92, 114, 136].

The main target of the second series of euro banknotes (ES2) is to introduce one or two innovative public security features [e.g. 99]. So if the aim is to keep the total of six public security features, as is the case in the first series, one or two new public features have to be introduced (y) and four or five features have to be improved (x). The security matrix as published by the ECB (Table 4) recognises three stakeholders: the public, retailers and central banks. Compared to the generic security matrix presented in Table 3, three stakeholders are missing: Banknote Equipment Manufacturers (BEMs), the users of Counterfeit Deterrence Systems (CDS) and forensic analysers.

3 Retailer

In recent decades the importance of the retailer as a separate stakeholder of new banknote design has increased. Retailers were for the first time recognised in 1982 as a separate user group by Dr. Peter Koeze (DNB) named 'cashiers' in those days [10]. Around 1985 retailers in the Netherlands started to use special tools like UV lamps, to verify banknotes received from their customers [69]. Their importance increased and, as said, it seems that the retailers should be the #1 user group or stakeholder in the generic security matrix (Table 3). Retailers receive 120 banknotes a day on average, while a member of the public just one or two. New banknote designs should first and foremost be designed to serve the retailer.

This chapter is divided in three sections:

3.1 Analysis of retail security features,
3.2 Method for selecting retail security features,
3.3 Designing retail features.

3.1 **Analysis of retail security features**

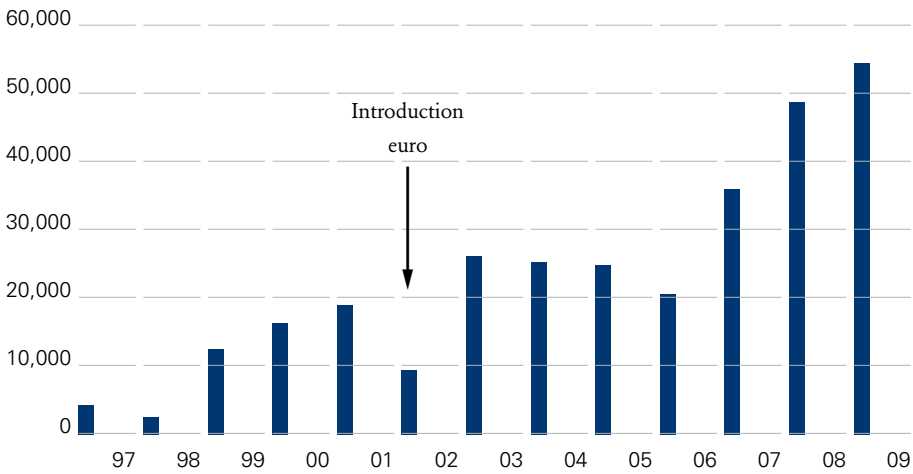
Any action to select new security features for a new banknote design should – following the phases of applied design – start with analysing the existing situation. These analyses are split in the following subsections:

3.1.1 Rise of counterfeits,
3.1.2 Counterfeiter focus is on mid denominations,
3.1.3 High denominations no longer used for daily payments,
3.1.4 What does the retailer check?
3.1.5 User requirements retailer.

3.1.1 **Rise of counterfeits**

The number of counterfeits registered in the Netherlands (NL) has grown, as is shown in Figure 6, over the last 12 years. Since the introduction of the euro banknotes in 2002, Dutch retailers have been confronted with about 4 times more counterfeits:

Figure 6



Development of the number of registered counterfeits in the Netherlands over the years 1997 - 2009. In 2002 the euro was introduced. In that year DNB received 5,301 NLG and 4,038 EUR counterfeits.

16,299 counterfeit guilder notes in 2000 [45] against 54,949 euro counterfeits in 2009 [163]. About 80% of the counterfeits are offset prints and about 20% are made with ink jet printers (2009). In the US it is roughly the other way around: the majority of the counterfeited dollar banknotes are made with ink jet printers.

A comparison of the number of counterfeited guilder notes with that of euro counterfeits in NL should take the following into account. The figures on the euro counterfeits in NL also include – of course – euro counterfeits coming in from

Table 5

Key figures euro banknote circulation (in %)	Euro denominations						
	5	10	20	50	100	200	500
Share in number (total)	11	15	19	39	11	1	4
Share in value (total)	1	2.5	6.5	32	18.5	4.5	35
Counterfeits (total)	0.5	1.5	41.5	42.5	12	1.5	0.5
Counterfeits in NL	0	2	5	74	18	1	0

Overview of key figures of the euro banknote circulation. May 2010, except for counterfeits (total), which are the figures representing the first half year 2010 [174].

Figure 7

The incidence of euro counterfeits in the Netherlands, 12-month rolling average number of detected fake banknotes in circulation. Figures concern 'counterfeits passed' as registered by the National Analyse Centre of DNB, 2002 - June 2010.

other euro and non-euro countries. The figures for the old guilder notes (NLG) did *not* include NLG counterfeits detected in other countries.

Damage in shoplifting is higher

The total loss suffered on counterfeited banknotes in the Netherlands is about 2 million euro (about 50,000 counterfeits per year with an average value of about 40 euro). The lose out on counterfeits is mainly put at the retailers. However, the total loss incurred by Dutch retailers because of shoplifting is around 325 million euro, much higher than the total value of the counterfeits. Debit card fraud (skimming) is believed to be around 36 million euro; credit card fraud is not included in this figure and is proportionally expected to be about 10 times higher. Table 6 provides

Table 6

Lose out retailers	Euro 2009
Counterfeited banknotes	2 mln
Debit card fraud (skimming)	36 mln
Shoplifting	325 mln

Overview of the (estimated) lose out of retailers in the Netherlands in 2009 [164, 169].

Table 7

Counterfeit level	Average number of counterfeits detected per million notes in circulation within one year [c/mln]	Country/currency
1	0 – 10	Australia, Japan, Latvia, Norway, Romania, Sweden, United States (including 1 USD-notes), Netherlands before euro
2	10 – 50	Hungary, Canada (in 2010),
3	50 – 100	Euro (average in euro area), USD (excluding 1 USD-notes), Netherlands NLG (1973, 1978)
4	100 – 200	Brazil, Euro in NL (2009)
5	200 – 500	Canada (in 2004), Great Britain (in 2008)
6	500 – 1,000	Canada (in 1973)
7	> 1,000	-

Seven levels of counterfeits and some of the countries where these levels have been established [14, 95, 101]. Average number of counterfeits detected per million notes in circulation within one year [c/mln]. The counterfeit level in the euro area in 2009 was 67 c/mln. For euro counterfeits in NL see Section 4.1.3. No case is known in which more than 1,000 c/mln were found to have circulated.

an overview. From this view it is understandable that counterfeited banknotes do not have the first interest of the retailer.

What quantities do counterfeiters produce?
Usually the counterfeit level is defined by the number of counterfeits per million notes passed in circulation [c/mln] (or parts per million, ppm) within one year (see Table 7). Counterfeits seized by police before the criminals could use them for payments are not part of these figures and generally significant higher in quantity. Still counterfeit statistics are based on incomplete information. More study is needed here to answer questions like:
- How is the denominator, the number of genuine notes outstanding, calculated?
- Are all counterfeits detected reported to the authorities?

Of course, world currencies like the US dollar and the euro are more attractive for counterfeiters than the currencies of small economies. This explains why, in

comparison to NLG banknotes, today 4x more counterfeits are detected in the Netherlands.
The Bank of Canada (BoC) is a central bank being transparent with counterfeit figures, just as the Bank of England. Counterfeit figures may be highly volatile, as was recently demonstrated in Canada (up to 470 c/mln in 2004) and the United Kingdom (up to 298 c/mln in 2008). At the peak in Canada in 2004 counterfeiting reached 1,292 c/mln (spread over the two models of the CAD 10) [101].
The counterfeit rate of USD banknotes is believed to be around 60 c/mln [159]. Including the one-dollar bills this rate is reported to be around 5 on 1 million [102]. Australia claims a very low counterfeit rate of just 6 c/mln. This low figure is attributed to the counterfeit deterrence capability of the polymer notes.

Counterfeiting may be triggered by new design
Central banks should be cautious with the issuance of new banknote designs. There is a remarkable phenomenon that shortly after the issuance of a new model, the number of counterfeits rapidly rises to figures exceeding those of the old notes. This phenomenon occurred in Canada after the issuance of the new CAD 10 in 1999, and in the United Kingdom, shortly after the introduction of the new GBP 20 in 2007, after which counterfeit figures surged to an all-time high. In the Netherlands, too, counterfeit figures increased shortly after the issuance of the NLG 25/Robin in 1989. In case of the CAD 10 the counterfeiting problem was not due entirely to the phenomenon of a series changeover, but also to the fact that, in retrospect, insufficient security features were included. This resulted in high counterfeit rates. The CAD 5 and 10 were subsequently re-issued with more security features, like e.g. the holographic foil stripe.

3.1.2 Counterfeiter focus is on mid denominations

In the past counterfeiters in the Netherlands focussed on the highest banknote denominations. In the 1970s this was the NLG 1,000 (value EUR 454). The 1,000 guilder was one of the most targeted denominations in the 1970s, although this denomination was hardly used in daily cash payments [14]. Retailers and public became alert and the counterfeiter moved to lower denominations like the NLG 100. This denomination became by far the most counterfeited Dutch guilder banknote. Lower denominations like the 5 and 10 guilder notes were not attacked. The profit for the counterfeiter on such low denominations of bogus notes is too low. This pattern seems to be also true for the euro banknotes. The counterfeiter targets mainly the euro 20 and 50, and leaves aside the low (5 and 10 euro) and the high denominations (200, 500).

The ATM-note is targeted by counterfeiter
Counterfeiters focus on the most popular ATM-denomination. Countries seem to have their own dominant 'ATM-banknote', the most popular denomination. In the

United Kingdom this is the GBP 20 making up around 70% of the total stock of banknotes in circulation (and around 65% in value) [167]. In the Netherlands this is the euro 50 with a 40% share in numbers.
'Nine out of ten shops in the Netherlands do not accept euro 100 notes. As a consequence people cannot and do not want to pay with 100 euro bills and ATMs do not provide euro 100 notes.' is the opinion of Philip Hans Franses [97]. As a consequence, if high denominations are not accepted in the shops, than counterfeiters will not produce them. The counterfeiters are more-or-less forced to use the ATM-note for their bogus notes.
The Bank of Canada experienced in 2004 the opposite. In Canada the ATM-note is the CAD 20 and the two low denominations CAD 5 and 10 were the most frequent counterfeited denominations.

Why does retailer not want to receive high denominations?
The retailer does not want to receive high denominations for three reasons:
1) Accepting high denominations means that the retailer should have large amounts of banknotes at their cash desk to return in exchange to their customer.
2) A high number of banknotes in the cash box will increase the risk of being attacked.
3) Accepting a counterfeited banknote of a high denomination leads to high losses.

3.1.3 High denominations no longer used for daily payments

Around 1985 the first stickers appeared at gasoline stations in the Netherlands warning their customers that no change will be returned from high banknote denominations like the NLG 1,000 (Figure 8). Later also other shops copied this policy and with the introduction of the euro in 2002 this did not change.

Figure 8

Warning to clients of gasoline stations in the Netherlands at the time of the guilder notes, around 1985: 'We give no change to this note!'

Euro sticker history

At first only the 200 and 500 euro were not accepted in the Netherlands (Figure 9a) and the euro 100 joined later (Figure 9b). The most popular denomination in the Netherlands, the euro 50, appeared for the first time on such a sticker in 2009 (Figure 9c). In other countries of the eurozone such stickers are found too, like e.g. in France (Figure 9d).

Recently, however, the Dutch public's demand for euro 100 notes has started to rise, though, and several ATMs in the Netherlands now contain euro 100 banknotes (Figure 9e).

Figure 9

a)

b)

c)

d)

e)

Communication examples on the use of high euro banknote denominations in the Netherlands.
a) Sorry, no change (gasoline station, 2004).
b) These banknotes are not accepted (liquor store, 2008).
c) No euro 50 banknotes accepted by public transport automate in Amsterdam (2009).
d) No banknotes accepted in ticket machines of the French railroads SNCF (2010).
e) This ATM issues also euro 100 notes (ABN AMRO branch, 2009).
Pictures by De Heij.

In other countries high denominations are accepted by the retailers, despite the public's perception that high denominations are hard to spend, like e.g. in Canada. The CAD 100 (about 75 euro) is welcomed by 97% of the retailers [154].

3.1.4 What does the retailer check?

Although the retailer does not like to receive high denominations, the average retailer in Europe receives, as said before, on average about 120 banknotes a day. And 20% of the retailers even gets over 200 banknotes a day, as was found in ECB research in 2004 [60].
Let us now have a look at the question which features the retailer is suppose to check? The euro banknotes include dedicated human assisted features to be operated by a retailer, like UV features and IR features. Table 8 is a *tool-feature matrix*, listing the tools the retailer may use to verify a just received euro banknote from a customer.

Table 8

Euro Series 2002 – Retailer

Tools used by retailer	Retail features	
	Front	Reverse
Human interpretation		
1. UV lamp	6	5
2. Magnifier	4	3
3. IR viewer	1	1
Automatic device		
4. Left to market (n)	m	m

Tool-feature matrix of the Euro Series 2002. The listed tools, devices are used by a retailer to verify retail security features. On the front the retailer may check 6 properties by using an UV lamp: 1) UV dull paper, 2) red fibres, 3) blue fibres, 4) green fibres, 5) blue print becomes yellow/green, 6) yellow ink becomes orange.
On the reverse the retailer may check 5 properties by using an UV lamp: 1) UV dull paper, 2) red fibres, 3) blue fibres, 4) green fibres, 5) map of Europe lights up yellowish.
On the front the retailer may check 4 micro-texts using a magnifier: 1) security thread, 2) foil, 3) offset and 4) intaglio.
On the reverse the retailer may check 3 micro-texts: 1) security thread, 2) offset (positive micro lettering) and 3) offset (negative micro lettering).
Both on the front and the reverse there is one feature visible with an IR camera (front: right part of the window/gate, reverse: the banknote number on the right side of the note).
n = number of devices successfully tested by ECB; today over 40 devices.
m = no specific feature implemented; several automatic devices can authenticate euro banknotes.

Development of automatic devices was left to the market
The euro banknotes do not have dedicated features incorporated to be used for a specific automatic device. It was left to the market to develop automatic devices to be used by the retailer; the market selects their 'own specification' from the existing banknotes. Therefore the production of the euro banknotes should be stable and kept within tolerances over the years.
To assist the retailer in making a choice out of all devices offered, the ECB provides on their website a list of 'Successfully tested types of banknote handling machines' (www.ecb.int). Over 40 devices are on this list (2010). The test is done with genuine and counterfeited banknotes coming from circulation. Since new counterfeited euro banknotes may appear at any time, the list does not inform on reliability or accuracy.

Analysis of human assisted retail features
Retail features in the euro banknotes may be checked with an automatic device or tools needed human operation and interpretation. Figure 10 provides an example of both. The human assisted features are supposed to be checked with an UV lamp, IR viewer or a magnifying glass. In some cases, a mirror is used to check the colour-changing feature (or Optical Variable Ink or OVI). However, this feature is particularly meant for the general public. This mirror device (Euro OK) is an

Figure 10

Infra red viewer

Automatic device

Authentication tools for retailers.
Left: Example of an IR viewer showing the IR properties of a euro 10 banknote (Secure Project C.M.S, 2004).
Right: Example of an automatic device (Euro Laser Scan, Grupo Sallen, 2004).

example of an initiative of the market to provide a human assisted tool to verify euro banknotes.

Strong bias to UV and micro-text features
Table 8 tells us that euro banknotes have a strong bias to features to be checked under UV light: in total 11 UV features! Of course several of these UV features may be checked within one look.
Micro-texts are also frequently printed in a banknote and intended to be used by the retailers. On the euro banknotes one may count over 7 variants of micro-texts, used on the front and the reverse of the euro banknote. Micro-texts come on the front in different heights and on the reverse in both positive and negative lettering. Furthermore such texts may be found on the security thread and on the holographic foil.
Since UV and micro-text features are over represented in the euro banknotes, these features qualify to be reduced or eliminated in a new designed euro note.

Which devices does the retailer use?
Now we know which features are in the euro banknotes dedicated to the retailers, we arrive at the questions which of these features are actually used by them?
Many Dutch retailers (40%) do not check a banknote for genuineness; at least not with the help of a device as may be concluded from Table 9 (row 6, none). Fortunately, the category that uses a device is growing as may be concluded from Table 9 (row 2, auto detection).
No research is done to which denominations are checked. Authentication tendency is probably denomination specific; low denominations like euro 5 and 10 are less frequent checked than higher denominations.

Table 9

Retail device	Used in the Netherlands by		
	2007	2008	2009
1. UV lamp	35%	36%	33%
2. Auto detection	16%	18%	22%
3. IR viewer	4%	5%	3%
4. Different	3%	3%	4%
5. Magnifier or mirror	0%	0%	0%
6. None	45%	41%	40%

Overview of Dutch retailers using a retail device to authenticate euro banknotes (2007, 2008 and 2009) [94, 124, 152].

Although Table 9 shows that more authentication devices are used in 2009, there is also a strong increase of counterfeits in the Netherlands in 2009. The place to spend counterfeits is at the shops, which is relatively easy since many Dutch retailers don't use any form of checking device.

The use of a magnifier, which was never used by retailers anyway, has become obsolete. Today only the banknote printers seem to use magnifying glasses! Magnifying glasses are probably used in the past by bankers, as might be observed in the movie 'The Counterfeiters' playing in the 1940s (see also Chapter 6). From a marketing point of view, there is a need for a follow-up. Features based on a filter, e.g. a polarisation filter, seem to fulfil the user requirements and are therefore attractive.

If 40% of the retailers are not using any device in 2009 it indicates that around 60% does have a device and might be using it. A similar, although lower figure (43%) was reported by the Banco de España in 2008 for the presence of banknote authenticity devices at Spanish shops. They reported also that 47% of their customers are not annoyed by verification with authenticity devices of the banknotes they offer to pay for a purchase; but on the other hand 41% are annoyed by it [117].
Despite awareness of counterfeits only 21% check all denominations reported the ECB for the euro zone in 2007; 10% never check any banknote [100]. According to the ECB research done in 2009, 18% of the Dutch cashiers say that they always check a banknote and 17% of the retailers' response is that they never check [151].

The results reported in Table 9 qualitatively match the data for the Netherlands in Table 10, as reported in the 2009 'Cashier Survey' of the ECB, except for the pen tests for starch content; the pen test is not reported in the Dutch research presented in Table 9. Euro banknote paper does not contain starch and therefore will not leave a dark brownish mark as most commercially available paper does. The pen is not recommended for authentication of euro banknotes because it is not always accurate and results can be manipulated using various chemicals [e.g. 141].

UV checks on banknotes not properly done
Table 10 clarifies that authentication using a UV lamp is very popular in the Netherlands (44%) but not that much in the euro area (19%). Since the mid 1980s DNB has encouraged the use of UV lamps, but today Dutch retailers are discouraged to rely on UV features, because many retailers tend to misjudge the UV properties of real and counterfeited euro banknotes. Real notes are mistaken for counterfeits and vice versa. Research conducted by DNB in 2006, using respondents working in the retail sector, showed that UV light checks on banknotes are often not properly conducted. Counterfeits have well-imitated UV features, often even brighter than the ones in the real notes. The cause of this increase is today's wide availability of UV inks for ink jet printers. This explains why so many counterfeits with an UV

Table 10

Retail device	NL 2009	Euro area 2009
UV lamp	44%	19%
Euro 'pens' indicating whether the banknote paper is genuine	14%	14%
IR viewer	3%	8%
Authentication device/equipment	16%	8%
You don't use any tools (spontaneous)	33%	54%
Other tool (spontaneous - specify)	1%	1%
Don't know	0%	1%

Results on the question: 'Do you use any tools to help you check the authenticity of euro banknotes? If so, which ones? (multiple answers possible).Cashier Survey 2009, ECB [151].

imitation are not rejected [80]. Therefore, retailers can no longer rely on a UV lamp check, as advised since 2006 by DNB.

UV features on counterfeits

The increase of UV imitations has also been recognised by the ECB. In 2006 about 80% of counterfeits showed attempts to imitate the UV fluorescent part of the printing image. The counterfeiter targets the retailer and creates counterfeits with UV features that look similar – or even better – than in a genuine euro banknote. The UV fluorescence of the counterfeited notes is often stronger than that of the original, making the counterfeit look *more real* and misleading to the retailer, as shown in Figure 11 (see also ref. 88). These brighter reflections of the inks and fibres under an UV lamp are an example of the importance of the implicit quality

Figure 11

Euro 50 - Genuine (2002)

Euro 50 - Counterfeits (2005)

Example of heuristic quality of banknotes under UV light. Because of the brighter reflection of the UV features in the counterfeited note, many people accept this note as real (quality heuristics).

of a banknote (or heuristic quality, see Chapter 4). In this case the counterfeiter exaggerates the original features. The girl behind the counter might think: This note looks very bright; it must be a real one! Or, in case she has received some training, she might think that it is a washed genuine banknote. Because of the bleaching agents in some detergents (real) washed banknotes might light up under UV light. It may also go the other way; a washed banknote may be misjudged as a counterfeit.

Short and long UV
The response of the security industry on imitated UV features has been to use more complex UV, for example using UV light of two different wavelengths: short (254 nm or C) and long UV light (365 nm or A). Examples are *Gemini* (by De La Rue), *MultiFlo* (by KBA Giori), *Trichromatic Fluorescence* or *HCS* (by Banque de France), polarized UV light (by Landquart) and *CLUE* (by the central bank of Belgium). Responses using *double UV features* applies the (undesired) *nested feature* approach and creates features that take too long to check. Nested features are explained in Appendix 7. Furthermore, the price of a tool checking two wavelengths will most probably increase.

Automatic devices are preferred
When a retailer would like to verify a just received banknote, there is an option between two types of devices:

1) The type of device letting the retailer decide whether the note is genuine or not, e.g. UV lamps, IR viewers, magnetic marks viewing detectors, magnifiers and mirrors.
2) The type of device that indicates whether a note is genuine or not, often by a green/red light, a text display or sound (a beep).

Human assisted retail features like UV features made visible with an UV lamp and IR features becoming visible on an IR viewer leave room for interpretation by the retailer and are time-consuming. Detectors telling whether or not the note can be accepted are for that reason preferred over detectors requiring retailers' interpretation. An advantage of auto detection devices is these devices provide the retailer with an easy argument to their customer in case of a suspected banknote: 'The *detector* does not accept this note, would you have another one for me?' Ideally, a detector should therefore be operated within 2 seconds and should be equipped with a retail feature providing a high reliability. This seems to be the trend, since the use of automatic devices is increasing, although slow (Table 9).

Risk of genuine/fake automatic devices
The use of equipment for retailers to authenticate banknotes is a relevant policy issue for central banks and gives some food for thoughts. The retailer might not use any of the public or other features anymore and might rely only on an automatic device telling 'yes, the banknote is real' or 'no, the banknote is a fake'. There is

Figure 12

In transmission a retailer might check in one glance: watermark, security thread and see-through register. Also the overall heuristic quality of the note offered will be noticed.

also a moral hazard problem for a central bank providing or endorsing a banknote reader; what happens if it is defeated by counterfeits?

Retailer puts banknote on transparent counter
Some retailers have a special transparent counter (showcase). While preparing the change the retailer parks a just received banknote on such a transparent counter and several features could be checked within one glance: watermark, thread and see-through register (Figure 12).

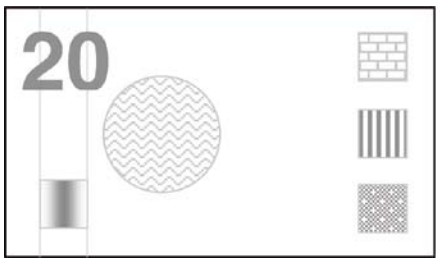
3.1.5 **User requirements retailer**

Since the retailer is a key person to stop the circulation of counterfeits it is important to know what their requirements are. What does the retailer want? From the analysis done it seems that the following requirements apply to the retailers:

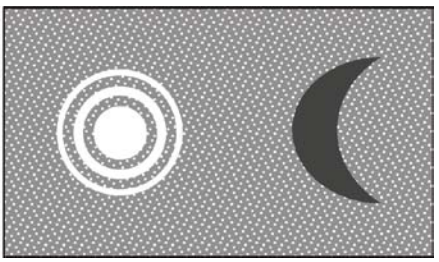
1) Retailers would not like to be forced to buy new authenticity devices when a new banknote arrives. Authenticity devices should be usable for both the old and the new banknotes (backward compatibility of authenticity devices).
2) Retailers would rather not check banknotes, considering it time-consuming and likely to offend the customer.
3) Retailers do not want to engage the public in a discussion or debate - so require a feature and device that provide independent and unequivocal validation.
4) The retailer does not like high denominations (100, 200 and 500 euro and in some cases euro 50).
5) Ideally, retailers do not want to spend anymore than 2 s checking each note.

Figure 13

Public features on front



Retail features on reverse



Retail features for human assisted checking should be positioned on one face of the banknote, preferably the reverse (in order that the front can be reserved for public security features).

6) Retailers would prefer to return suspicious banknotes to the client and ask for another one or for having the payment settled through other means, e.g. a debit card.
7) Retailers would like future banknotes to be ready for more secure automatic devices instead of human assisted retail features.
8) Retailers do not use a magnifying glass (large shops with a back office might use a strong magnifier).
9) Retailers would like to have all human assisted features on one side of the note (e.g. the reverse, see Figure 13).
10) The human assisted feature is independent of any source of energy (no electricity, no batteries).

Listing these retail user requirements and communicate them to the industry is a central bank's task. The industry should use these requirements as input for their developments. Clearly more analysing research is required to investigate the needs of this most important stakeholder, the retailer.

3.2 Method for selecting retail features

How to arrive at the selection of new retail features? In this chapter the all-in-one method proposed is explained by the following steps:

3.2.1 Defining a tool-feature matrix for a new banknote,
3.2.2 What goes out? - retailer,
3.2.3 What will be improved? - retailer,
3.2.4 What goes in? - retailer,
3.2.5 Completion of retail features.

3.2.1 Defining a tool-feature matrix for a new banknote

Creation of a tool-feature matrix of the existing banknote is a first step, like is done in Table 8. It came out that micro-texts and UV features should not be continued. The IR viewer is only used by a very limited amount of 3% of the retailers (Table 9) and is therefore also a candidate to be removed. Based on this analysis the central bank could opt for the policy to abandone all existing human assisted retail features and to introduce one full new human assisted tool-feature. Following the concept provided in Figure 13 this new dedicated retail feature should be positioned on the reverse. Other combinations of tool-feature could be left to the market. Such a policy is reflected by Table 11.

Table 12 describes a tool-feature matrix similar to Table 11, in this case also one feature is offered to be operated by an automatic device. The development of a tool to read such a feature is left to the market. Such an automatic device should have a high reliability (close to 100%) and should be operable within 2 seconds. The device provides a signal (a red or green light or a beep). Since the detection speed can be slow a botanical DNA taggant could be the feature the central bank includes in the new banknote. Other features may serve this purpose too, like improved IR and UV features (double wavelength), magnetic pigments or thin steel fibres into the paper. In case of an IR or UV feature the central bank would also have a backward compatible human assist feature, since the more complex IR and/or UV feature may also still be seen with the use of an IR viewer or UV lamp.

Table 11

New banknote series – Retailer

Tools used by retailer	Retail features	
	Front	Reverse
Human interpretation		
1. Feature by central bank	-	1
2. Left to market	m	m
Automatic device		
3. Left to market	m	m

Alternative tool-feature matrix using one dedicated human operated retail feature. The central bank offers the feature; the market is invited to offer human assisted tools and automatic devices.
m = no specific feature implemented, left to market.

Table 12

New banknote series – Retailer

Tools used by retailer	Retail features	
	Front	Reverse
Human interpretation		
1. Feature by central bank	-	1
2. Left to market	m	m
Automatic device		
3. Feature by central bank	-	1
4. Left to market	m	m

Central bank offers one human assisted feature and one detector feature (but not the device).
m = no specific feature implemented, left to market.

To have these tools available at the time of the issue of the new banknote, the specifications of the new feature(s) should be given about one year in advance to the producers of both human assisted tools and to the producers of automatic devices.

Table 13

New banknote series – Retailer

Tools used by retailer	Retail features	
	Front	Reverse
Human interpretation		
1. Feature by central bank	-	1
2. Left to market	m	m
Automatic device		
3. Feature by central bank	-	2
4. Left to market	m	m

Alternative tool-feature matrix using 3 retail features. All retail features on the reverse matching with the concept provided in Figure 13.
m = no specific feature implemented, left to market.

In case the central bank's policy is an even stronger invitation to the industry to develop automatic devices, matrix of Table 13 could be followed. The two dedicated features for automatic devices should – of course – be selected on the basis of input of the market. This policy would stress the importance of retailers preventing the spread of counterfeited banknotes and is the one used in the coming Sections.

3.2.2 What goes out? - retailer

Third step of the all-in-one method is to determine which features should not return in the new banknote; make an analysis of the existing features. To come to such an analysis a methodological tool is needed to assist the selection process of security features. Many criteria are relevant like:
- Cash handler's knowledge,
- User requirements like time and backward compatibility of authenticity devices with existing banknotes,
- Counterfeit analysis,
- Cost.

All together over 25 criteria are determined and are explained further on.

Dash board graphics: indicator colours
The next question to be answered is: How to deal with these 25 criteria? Adding up all kinds of criteria to a single score may be done by using an *additive value function* [17]. Although very tempting, adding up the scores of different criteria by mathematical calculations may not be helpful to the selection process. Both National Research Council (NRC) and ECB experienced that finally the artificial scoring of security features ended up in a limited value range, driving scores to the mid values (see section 6.2.2).

Instead of any figures, *dash board graphics* are proposed to indicate the score on a certain item. Examples of dash board graphics are pie charts, gauges, thermometers and traffic or indicator lights. Indicator lights like colours are defined on a nominal scale and cannot be added up (everything will become brown!). There is a choice between a 3 or 5 colour system. Five colours are for example used for the estimated risk of a terrorist attack by Homeland Security Advisory System in the USA (severe = red, high = orange, yellow = elevated, blue = guarded and green = low). For the sake of simplification, just three indicator colours are proposed: green, yellow and red (*traffic light model*). This way the observer of a matrix conform Table 14 will keep an overview. When a criterion is not applicable or may not be scored for other reasons the score is presented in grey.
The next step will be to set a threshold for each criterion employed in deciding what goes out. Proposals are made, but it is stressed here that central banks may bring in their own criteria and thresholds. Also test results from other central banks

or other parties like Europol can be inserted in the method. This is one of the reasons why the method is named all-in-one method.

The disadvantage of traffic model is that criteria are not weighted; the traffic light representation does not tell that a feature appears to be twice as effective as an other one. Criteria might be subjective; the user of the all-in-one methodology might come up with very different results by laying down other thresholds than the ones proposed. How the criteria proposed relate to each other is unknown and is an other disadvantage. On the other hand the proposed dash board graphics enables a quick scan by the human eye. The competitive strengths and weaknesses of the different features are made visible, which enables the decision making process.

To provide an example, the threshold values on knowledge of the retailers could be set as follows:

= score of retail knowledge ≤ 10%

= score of retail knowledge > 10% and < 50%

= score of retail knowledge ≥ 50%

Elimination process
Now the process of elimination may start: which feature or features go out? This phase is often overlooked by central banks but is important as it partly defines the requirements for the feature(s) coming in! This elimination is done by using *m* criteria on *n* features, according to the principle provided in Table 14. The all-in-one method is flexible and feature *i* or criterion *j* may be added or removed.

Table 14

Banknotes series What goes out? Criterion	Security feature					
	Feature 1	Feature 2	…	Feature i	…	Feature n
1 …						
2 …						
…						
j …						
…						
m …						

Example of a completed security feature criteria matrix What goes out? using the traffic light model.

Appendix II provides additional information
This section is a summary of the all-in-one method applied to the retail features; in Appendix II you may find additional information.

Conclusion on what goes out comes first of all of the analysis of the tool-feature matrix: magnifier and UV tools are out. As a consequence the micro-text and UV features are abandoned.

3.2.3 What will be improved? - retailer

Qualifying for improvement are the features operated by an IR viewer: the IR absorbing intaglio ink on the front and the black numeral on the reverse (see Appendix II). A decision should be made which of the features should be maintained and can be improved or enhanced in terms of design (perception, communication) and technology. To create one backward compatible feature to the previous euro series the IR viewer is maintained.

The first question to be answered at this stage is: Are *technical* improvements possible? Usually the answer is a yes, since existing technologies are constantly improved. The second question to be answered is if the *design* of the remaining features can be improved? Again the answer to this question is a yes, as will be illustrated in the following.

Table 13 indicates that the central bank is looking for one feature using a human assisted tool and 2 new features for automatic devices. It is also known that the IR

Table 15

New banknote series Retailer	Retail security feature	Improvable?	
		Technology	Design
1. Automatic device 1	1. Existing		
	2. New	IR	
2. Automatic device 2	3. Existing		
	4. New		
3. Human assisted	5. Existing	IR*	
	6. New		

Tool-feature matrix for a new banknote including 3 retail features. One automatic device will be based on an improved IR feature. A new human assisted feature will be introduced. The new IR feature will also be visible with an IR viewer (IR*), which should no longer be promoted (with an eye on abondoning this tool in future designs).

feature will remain. To come to a further analysis this information is inserted in Table 15.

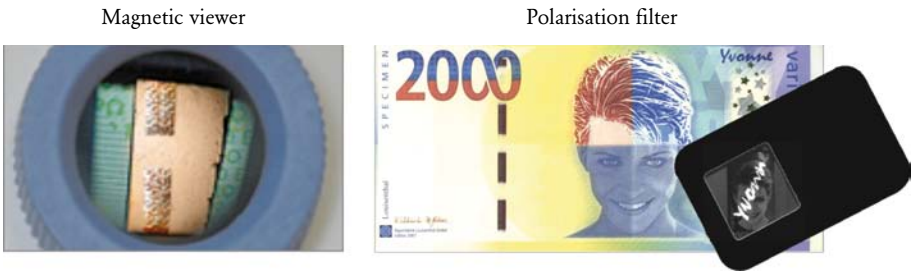
Improvements in IR feature
The IR may be improved by optimising the feature for automatic devices – device 1 in Table 15 – e.g. by adding additional spectral properties. The IR feature is proposed for the reverse side of the banknote, leading in case of the euro banknotes to the existing IR absorbing banknote number. This feature can be improved for a detector by printing a second IR absorbing ink in this area, e.g. by adding an additional pattern or frame around the number.
The IR feature for automatic device 1 will still be visible with an IR viewer and fulfils therefore the principle of backward compatibility (see Chapter 2, Figure 5).

3.2.4 What goes in? - retailer

The all-in-one method is continued with step 5, in which we focus on what goes in. Based on what will remain, the tool-feature matrix for the retailer is updated as done in Table 15. Automatic device 1 is reserved for the improved IR feature, so we are searching for 2 new features:
- One feature for automatic device 2,
- One new human-assist feature.

Make an inventory of available new security features
Next step in the method is to make a list of all the new features for the retailer, addressing the tool-feature requirement of Table 15. New retail features should also match the user requirements. For security reasons the retail features should be based on different physical and chemical phenomena (so limit the spectral features!).

Figure 14



Two examples of new human operated tools to verify retail feature:
Left: Magnetic marks viewing detector showing the magnetic properties of the security thread on the euro banknotes (Dors, 2007),
Right: Polarisation filter showing the text Yvonne in the foil (Papierfabrik Louisenthal, 2007) [94].

Figure 15

Barcode reader and banknote

Metameric barcode

Cashier feature with three functions: security check, denomination recognition and cash management developed by DNB in 2001.
Left: a barcode on the banknote is readable with the laser light scanners used at supermarkets (660 nm). Right: metameric barcode 'NoCopyCode', developed by Joh. Enschedé. A barcode with 'camouflage' based on metameric inks. Any code could be used, like e.g. EAN-13, EAN- 8. Metameric inks are explained in Appendix 4.

At least two features qualify (see Appendix 11):
- A device reading botanic DNA,
- A device reading the pattern of very thin steel fibres (e.g. added to the paper).

Since many retailers use a barcode scanner, the central bank might include a feature to be checked by this scanner:
- A barcode scanner which may also check a banknote for genuineness (Figure 15).

The following features seem to match the user requirements for a human assisted retail feature:
- Polarisation filter using a feature in the foil shown in Figure 14, right hand side,
- Liquid crystal-based polarisation.

Magnetic pigments to be viewed with a magnetic pigments viewer as shown in Figure 14, left hand side does not seem to match the user requirements.

3.2.5 Completition of retail features

The all-in-one method applied to the retail features in the euro banknotes is concluded with a proposal for a tool-feature matrix for the new banknote, as done in Table 16. As an example, the human assisted IR feature (HA-type) will remain and will serve in the future notes as RA-type. So, instead of a dedicated IR feature made visible to the human eye by an IR viewer, the IR feature will be first of all a feature dedicated to an automatic device (which might still also be visible by an IR viewer).

Table 16

New banknote series – Retailer

Tool		Banknote		
		Feture	Front	Reverse
1. Automatic device 1	1. Detector 1	Improved IR feature, including banknote number	-	1
2. Automatic device 2	2. Detector 2	Taggent (e.g. DNA modified fibres into the paper)	(1)	1
3. Human assisted	3. Polarisation filter	Hidden image in print or foil	-	1
Leave to market	…	…	m	m

Tool-feature matrix for a new banknote including 3 retail features. In this example all of the existing features are replaced by new; none of the existing features will be improved. The DNB modified fibres into the paper will work on both the reverse and the front of the banknote.
m = no specific feature implemented, left to market.

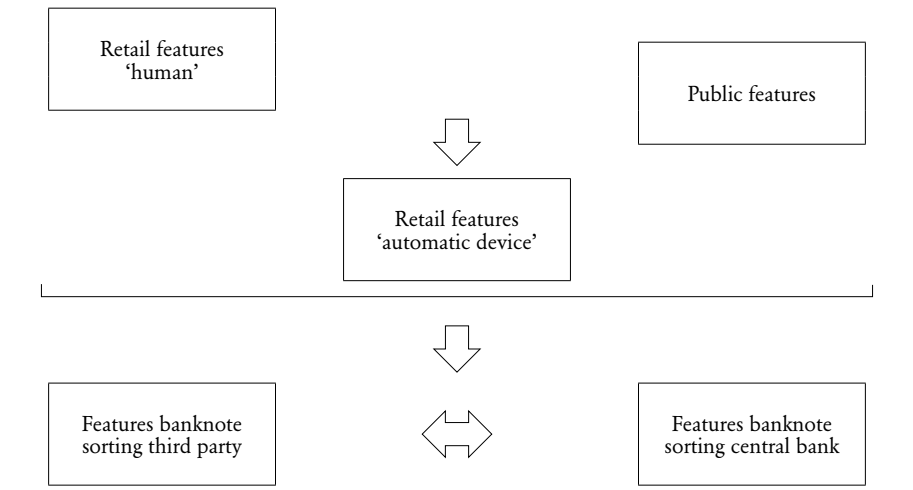
The second automatic device will be dedicated to the detection of a taggant, like e.g. DNA modified fibres into the paper substrate. Again, the central bank will include the feature in the new banknote and the industry is invited to develop the automatic device. These fibres will work on both the front and the reverse side of the banknote.
The tool for the human assisted feature is a polarisation filter, showing a hidden image in print or foil.

3.3 Designing retail features

It is logical to start with the selection of retail and public features, since they will dominate the banknote design. Figure 16 provides such a strategy. Within the 'detector user levels' there is more choice for central banks since detector features usually have more *design freedom*.

Three banknote concepts
In Table 17, three different security feature matrices are presented for three different concepts: models A, B and C. In the case of model A, the production costs of the new note should be similar to the note it is to replace. Model B allows a rise of the cost price by 5% and model C by up to 10%. Dutch guilder banknotes were developed according to model A; the production costs of the new banknote should not increase. Ideally, of each package of features, a complete prototype should be created and tested on retailer and public preference.

Figure 16



Strategy for selection order of security features. First the retail and public features should be selected, since they dominate the design. For machine-readable features more design freedom is allowed and central banks have more to choose from.

Especially larger central banks might opt for the development of different concepts and make a choice further on in the development process.

Nano-symbols instead of micro-text
Micro-texts could be deleted from the Programme of Requirements for the new banknote. Instead of micro-texts (letter height about 200 µm), nano-lettering could be introduced as a forensic feature (letter height about 2 µm). The micro-text features migrate in the generic security matrix from level 1 (retailer human assisted) to level 6 (forensic). Instead of texts also symbols could be used (see Appendix 4, Figure A4.11c and d).

UV extrusion fibres
One of the UV features could also be kept for forensic users. Instead of coloured fibres to be checked by the retailer using an UV lamp, the fibres could receive a micro-extrusion profile [69]. This profile could be made visible in a forensic laboratory.

Table 17

Three sets of security features and their cost increase (model A, B and C)

	Model A + 0%	Model B + 5%	Model C + 10%
Trigger	1. Grey colours (saturated)	1. Bright colours, e.g. colour outside euroscale	1. Bright colours, e.g. colour outside euroscale
3	2. High definition, e.g. screen and scan traps	2. High definition, e.g. screen and scan traps	2. High definition, e.g. screen and scan traps
	3. Different paper tints	3. Different paper tints	3. Different paper tints
Retailer device	4. IR feature	4. IR feature	4. IR feature
2	-. Leave to market	-. Leave to market	5. Botanical DNA
Retailer human	5. Polarisation in foil	5. Laser pen and opaque white boll	6. Liquid crystal-based polarisation
1			
General public	6. Feel: CtIP, nail scratch	6. Feel: CtIP, nail scratch	7. Feel: CtIP, nail scratch
6	7. Feel: CtIP, tactile patterns	7. Feel: embedded tactility	8. Feel: thermo chromic
	8. Look at: gravure in four segments [148]	8. Look-at: 3D image on foil patch	9. Look-at: 3D image on 12 mm foil stripe
	9. Look-through: full embedded security thread, e.g. Wings	9. Look-through: windowed thread (with colour switch)	10. Look-through: windowed thread (with micro-optics)
	10. Tilt: strong iridescent ink in note colour	10. Tilt: colour switch (on thread)	11. Tilt: iridescent band with two colours
	11. Tilt: plain continuous stripe in note colour with transparent parts	11. Tilt: strong iridescent ink in colour of the note	12. Tilt: micro-optics (on thread)
Banknote acceptors	-. Leave to market	-. Leave to market	-. Leave to market
Third party sorting	12.	12.	13.
1			
Central bank	13.	13.	14.
3	14.	14.	15.
	15.	15.	16.
CDS	16.	16.	17.
2	17.	17.	18.
Forensic	18. Nano-symbols	18. Nano-symbols	19. Nano-symbols
1 or 2	-	19. UV fibres extrusion	20. UV fibres extrusion
Total	**18**	**19**	**20**

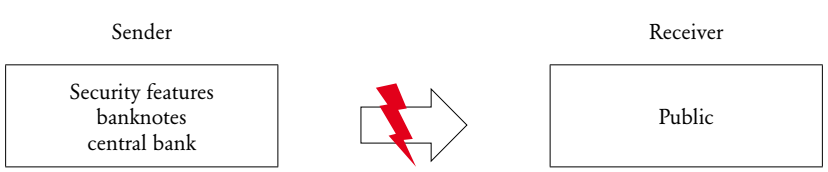
Three conceptual banknotes A, B and C with different cost prices and different sets of security features. CtIP = Computer to Intaglio Plate. Features mentioned are examples to illustrate the principle. Three user groups are not specified for security reasons (third party sorting, central bank and CDS).

4 Public

This Chapter is the most extensive one. The reason is that public features are harder to design as retail features are. The knowledge to *design* public security features is limited; the second part of this Chapter makes a start to fill this gap (section 4.3). Improved design should lead to more interest of the public in the banknote and its security features, as the central bank's message does not come across [81, 94]. Ian Lancaster, an authority in the field, agrees: 'I believe that it has become clear that the public do not either care enough or have adequate knowledge to undertake even first line inspection.'[79].
Figure 17 represents the basic *sender-receiver* communication model as employed for banknote design.

User-friendly public security features
On conferences about banknotes and their design one may often hear that public security features should be user-friendly. The ECB, for example, formulated this criterion of user-friendly public security features as follows in October 2007: 'With respect to communications on the current series of banknotes, such qualitative research has helped to make communication tools, such as brochures, leaflets and electronic communication media, more easily comprehensible by avoiding technical terms for the security features and by providing simple instructions on how to authenticate a banknote.' [99]. This policy should be the starting point for a new series of banknotes, rather than being developed once the note is ready for issue. To arrive at the desired user-friendly public features the central bank needs to develop first a design philosophy and a strategic communication policy. Both should be prepared before the actual design process starts [94].

Figure 17



Basic sender-receiver communication model. The banknote security features communicated by the central bank (sender) do not get across to the public (receiver).

Self explaining security features
The statement above implies that security features require explanation. While that is true for some, other features don't need explanation but can be authenticated intuitively, as was proven by research of the Bank of Canada (BoC) and reported in section 4.1.6 on the effect of training. Security features were evaluated with trained and untrained participants. For security features like the holographic stripe, untrained participants were able to identify nearly all of the counterfeits even when good quality counterfeits were included. The conclusion of the BoC is that some security features are inherently usable by the public and do not require training or education.

This chapter on security features for public use follows a similar methodology as introduced for the retailer:

4.1 Analysis of public security features,
4.2 Method for selecting public security features,
4.3 Designing public security features.

4.1 Analysis of public security features

The analysis on public security features done is reported in the following sections:

4.1.1 Heuristic quality and rule based quality of banknotes,
4.1.2 Public overestimates the number of counterfeits,
4.1.3 Probability of receiving a counterfeit in NL,
4.1.4 Confidence in banknotes,
4.1.5 Vicious circle: public – counterfeiter – central bank,
4.1.6 Effect of training,
4.1.7 User requirements for public security features.

4.1.1 Heuristic quality and rule based quality of banknotes

Familiarization or habituation obviously plays a role in banknote recognition. This means that people will soon stop responding to details of a banknote, but will see the note as a whole. This brings us the question: How do we know at first glance if the just received banknote is any good?
This judgement is based on two different perceptual rules:
1) Heuristic evaluation,
2) Rule-based decision making (using the public features).

Checking the public security features is referred to as the *rule based quality* of the banknote. When the central bank leaflet tells us that the watermark has both lighter and darker shades than its surroundings, we may verify if the watermark is genuine.

By following the instruction a person may authenticate a public security feature is an example of rule based quality. Knowledge on the public security features of a banknote is typically knowledge that we have learned, e.g. by reading a brochure on banknotes or by doing an interactive training on a website of a central bank.
Opposite to this rule based quality is the *heuristic quality*, the implicit quality standards of the banknote. An alarm is set off in our brains if a banknote feels limp. Or if the banknote looks blurred or pale, or is heavily damaged and repaired with cello tape. Such properties might trigger a refusal of the note or a thorough – rule based – authenticity check on the basis of the security features.

Heuristic = instantly perceived high product quality
Heuristics refers to 'discover' and is the application of experience-derived knowledge to a problem. The term 'heuristic quality' was first introduced by developers of software for public use. Via label branding the term found its way to the banknote world.
The heuristic quality of a banknote is the instantly perceived high product quality of the real banknote. Also the quality of the design contributes to the heuristic evaluation (e.g. well-readable numerals, clear security features, attractive design).
The heuristic quality of a banknote is typically located in the *implicit long-term memory* of our brains; it is knowledge that we gained by incidence, by using banknotes subconsciously. The security features learned are stored in our *explicit long-term memory*. In Subsection 4.3.1.3 you may find a further explanation of these two parts of the long-term memory.

Examples of heuristic quality of banknotes
DNB recognised the phenomenon of heuristic banknote quality for the first time in 1990. The colours of the counterfeits of the new-issued NLG 25/Robin were more saturated (i.e. less pale) than the original, making the counterfeits look more real than the genuine banknote. Figure 18 is an example of the heuristic quality of the euro 50 banknote.

Figure 18

Euro 50 - Genuine (2002)

Euro 50 - Counterfeits (2007)

Example of heuristic quality of banknotes. The counterfeited banknote is accepted for real in 2007.

Table 18


	Overall banknote: trigger features	Public security features
Terms	Banknote characteristics	Security features
Perceived quality	Heuristic (including trigger features)	Rule based
Authentication	Subconscious	Conscious
Long-term memory	Implicit	Explicit

Overview of introduced terminology concerning the overall banknote and its security features.

Trigger features
Trigger features are introduced in Chapter 2 and provide the banknote an overall quality and contribute to the heuristic quality of the banknote. Trigger features are not meant to be checked by the public. Subconsciously, both retailers and public use the trigger features.
Next to these trigger features banknotes are also recognised by their banknote characteristics. This term refers to banknote properties that do not have the status of a security feature. Examples of banknote characteristics are special patterns (e.g. guilloches), special print (e.g. rainbow printing) and special paper characteristics (e.g. 100% cotton).

It seems that central banks should focus more on the trigger features and other overall quality aspects (heuristic quality), next to their attention for the security features (rule based quality).
Table 18 provides an overview of the introduced terminology.

Paradox: foil should be perceived as difficult to counterfeit
A well known discussion item in the banknote security industry is 'simplicity versus complexity'. Security features should be difficult to counterfeit, yet simple to verify by the public. Related to this discussion is the perceived quality of the public security features. This phenomenon surfaced for the first time in the project 'Foil with public appeal', a DNB research project done in 2004 for the ECB, when the following paradox was found. The public considers itself unable to check the foil on complex parts and is unwilling to check the foil's details. The very presence of the foil in itself is deemed a sufficient guarantee of authenticity. The public argues that the foil serves to deter counterfeiters, as they assume that reproducing

it is difficult if not impossible (provided that it is e.g. well-integrated in the banknote, and is visually complex). Transparent parts associated with tape or looking like stickers are perceived as easy for the counterfeiter. However, one of the conclusions of this research was that the public is willing to check if the foil and denomination match. Is it the right foil from a denomination point of view? And, does the image match the printed image? From among the 13 prototypes submitted, a clear winner was chosen (see Figure 19 and Table A4.6) [63]. A recent example coming close to this advice is the commemorative banknote of the Central Bank of Morocco, issued in 2009 (Figure 20).

Contra productive CDS

A special group of security features should prevent scanners and copiers to reproduce a banknote, named the CDS-features (Table 3). Such CDS-features are counterproductive to the heuristic quality of the banknote since they require too much space [108] and make the note appear blurred and pale. As a result, people tend to confuse counterfeits, which are sharper and have more saturated colouring, for genuine euro notes. Furthermore, pale banknotes are disliked, as was found in 2002 research by DNB [49].

Instead of being added once the design is ready, CDS-features should become part of the design process. Therefore, it is necessary to set requirements that may be used during the design of the banknote. The optimal CDS-feature would be an

Figure 19

Printed and foil portrait are similar, foil includes also the numeral

Portrait flips to grand piano

Design concept of music note. In the foil there are just two switching from portrait (tilt + 60°) to (surprising) a grand piano (tilt - 30°).
The public's favourite concept from a series of 13 prototypes with foils, delivered by DeLaRue Holographics in 2003. The public was found willing to verify the portrait in the foil with the printed portrait and the numeral 50 in the foil with the printed numeral. Images should switch in North-South direction without overlapping, and no banknote should feature more than two images.

Figure 20

Good example of foil design in this commemorative MAD 50, issued in 2009 in Morocco. The public can check if the images on the foil are the same as the printed images. And secondly, the public can verify the value at the top of the foil.
The portraits are from left to right respectivily the Kings Mohammed VI, Hassan II and Mohammed V. Original design: Roger Pfund.

intrinsic and invisible one using the complete banknote surface. An *intrinsic* feature, such as a taggant might be an option for such counterfeit deterrence systems, since high-speed detection is not required. Taggants are not visible and therefore inconspicuous. Furthermore they take no space. See Appendix 4 for some more analysis of CDS-features.

We leave this subject here, concluding that more analysing research is needed to optimise future banknotes on the phenomena of heuristic and rule based quality.

4.1.2 Public overestimates the number of counterfeits

At the height of the first media attention for euro counterfeits in the Netherlands, in February 2004, people estimated the number of counterfeits to be much higher than the actual number of counterfeits circulating. Within a 5-year period entrepreneurs estimated that 0.5 to 10% of the euro notes in the Netherlands would be counterfeits. Consumers were expecting even much higher levels: 30-100% [81]. Such high figures were also reported in 2004 in research done by the ECB; 49% of the retailers believed that they have come across a fake euro banknote [60].
In a recent survey by DNB on the safety of payment instruments, 11% of the Dutch respondents reported having received a counterfeit banknote or coin at one time or another [162]. This public perception is remarkable, since it is far above the reality of around 50 c/mln passed or 0.005% in 2008 (see Figure 23). Although the different researches did provide rather different figures, they point in one direction: the public overestimates the number of counterfeits; it may be concluded that the public's perception of the number of counterfeits in circulation exceeds the real number by as much as between 20% and 200% (NL, 2008).

Press releases of central banks on counterfeit figures
How may the public's overestimation on the counterfeit situation be explained? The short messages in the news paper or on the radio might trigger this phenomenon. Central banks usually report regularly with a press release about the number of counterfeits received. The public perception of these figures is: 'Good heavens, that is a lot!' Central banks report in a statistical and juridical way on their counterfeited banknotes, leaving the public with a passive attitude and negative feeling. Instead of a reactive communication policy on counterfeited banknotes central banks might opt for a more informative and proactive policy, like reporting on:
- The difference between genuine and most counterfeited notes,
- The probability of receiving a counterfeit,
- Public confidence.

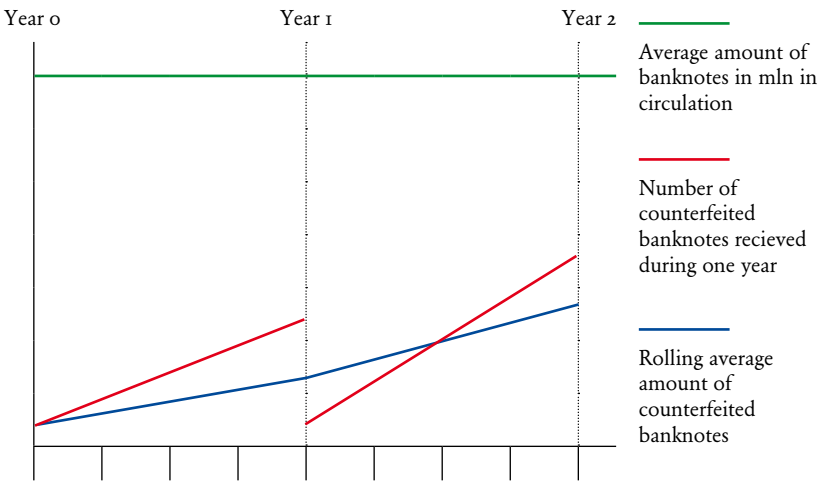
A study to the effect on the public perception of press releases on counterfeits would be useful.

4.1.3 **Probability of receiving a counterfeit in NL**

The probability to receive a counterfeit is quite different for a retailer or a public person. Retailers receive more banknotes than the public and they also receive the ATM-notes. Next to the indicator of 'counterfeits per million notes in circulation' (Table 7), the probability indicator will put the number of counterfeits into perspective. To calculate the probability of the receipt of a false banknote during a cash transaction, it is necessary to know how many cash transactions take place and in how many of these transactions counterfeited banknote are involved. Such figures are not available. The probability of receiving a counterfeit becomes therefore a doubtful measure; it depends on both the number of counterfeits circulating – which is unknown – and their rate of circulation.
Still it is possible to make an estimate using the (average of the) rolling average. Figure 21 explains the difference between statistics based on the number of counterfeits received during a time interval (month, quarter or year) and a rolling average. For reasons of explanation straight lines are used; the real probability may vary and may be higher or lower, since counterfeits are not equally put in circulation.
An average rolling average of the number of counterfeited banknotes will bring us closer to the truth of the number of counterfeits circulating at a certain moment in time. That is why the average rolling average may be divided by the average amount of banknotes in circulation.

Probability to receive a counterfeit in NL is 1:10,000
Let us do some calculations on the Dutch figures! At the end of 2009 the total circulation of euro banknotes was 13.6 billon banknotes (13.10^9). The Dutch share of this total is 5.6% (capital key) being about 730 millions of euro notes. As the

Figure 21



Schematic representation of the total number of banknotes in circulation (green) and the counterfeits received in year 1 and year 2. The red line is the number of counterfeited banknotes received during the year. In the start of year 2 the counting starts again. The blue line is the rolling average amount of counterfeited banknotes.

Netherlands is like a euro area 'province', the number of euro banknotes in circulation is not exactly known but is estimated to be approximately 500 million. It follows that with a rolling average of about 50,000 counterfeits (see Figure 7), the counterfeit level in the Netherlands may be calculated at around 100 c/mln, which is above the average of 67 c/mln for the whole euro area (in 2009). So the probability for a Dutchman to receive a counterfeited banknote is 1 to 10,000. The odds of winning a lottery are usually higher than receiving a counterfeit in circulation. Ruud Van Renesse agrees: 'The probability of a member of the public receiving a counterfeit is virtually negligible. So why would the public inspect banknotes at all? It is hardly worth their while.' [88, 96]. Still the advice of the Bank of England on their website is valid: 'Although counterfeit banknotes are rare (only a small fraction of 1% of banknotes in circulation is counterfeit) it always pays to be careful.'

Recalculation probability for only euro 20 and 50

The calculated probability of 1 on 10,000 is valid for the total circulation, including all denominations. In daily practice most counterfeits concern the euro 20 and 50 which is close to 80% of all counterfeits (79% according to Table 5). The share of these two denominations is about 60% of the total number of banknotes in circulation (Table 5). Suppose that this figure is also similar for the 'euro province Netherlands', than the calculation is made as follows:

$$\frac{0.8 \text{ x } 50{,}000}{0.6 \text{ x } 500 \text{ mln}} = \text{about } 130 \text{ c/mln}$$

Making this calculation once more for only the euro 50 (74% of counterfeits and 40% off the circulation) this value would go up even further to 190 c/mln (for 2009). Only the last person accepting a counterfeit will bear the damage of a lost value, in this case often the retailer, since it is expected that only one payment is done with the counterfeited euro 50 banknote. So the probability for a Dutch *retailer* to receive a counterfeited euro 50 banknote would be about 1:4,500 (in 2009). For the *public* this probability is not reached and will be lower. Still central banks keep a moral obligation to social weaker people; useally they be left holding the baby, in this case a valueless banknote

4.1.4 **Confidence in banknotes**

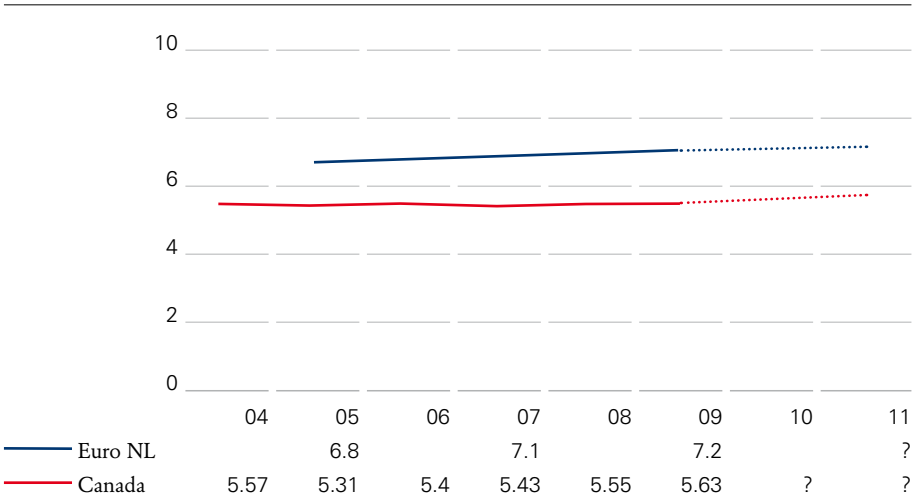
In addition to the cognitive average knowledge of public security features, DNB followed the 2004 example of the Bank of Canada and considered the Dutch citizens' confidence in euro banknotes a relevant psychological indicator. In 2005 the first measurement of the public's trust in banknotes was reported by DNB. The results of both central banks are compared with each other in Figure 22. The Bank of England has measured aspects of public confidence since 2004 too, but did not publish the results.

It is remarkable that the graphs for both Canada and the euro zone are similar. To be clear, it may not be a conclusion that the confidence in the euro in the Netherlands is higher than the confidence in the Canadian dollar in Canada. The definition of confidence is not similar. In Canada it is a confidence index that is measured, based on 4 variables [132]. In the Netherlands the confidence is simply the answer to one question asked to the public [94].
The public's confidence that euro banknotes in circulation are authentic is around 7 on a scale from 1 to 10 [81, 94, 133]. Although the Dutch public may overestimate the number of counterfeits in circulation, it does not seem to affect their confidence in the euro banknotes!

The 'Cash Handlers Surveys' of the ECB also show a rather stable outcome when people are asked about their opinion on the protection of the euro against counterfeiting. Over the years 2004, 2007 and 2009 about 50% of the European cash handlers is of the opinion that the euro banknotes are sufficiently secure against counterfeiting. For the Netherlands the opinion is also evenly split [60, 100, 151].

Counterfeit numbers have no influence on public confidence
The confidence graphs may be rather flat; the counterfeit situation in both Canada and the euro zone is volatile. The counterfeit trends in Canada and the euro area

Figure 22
Scale 0 - 10

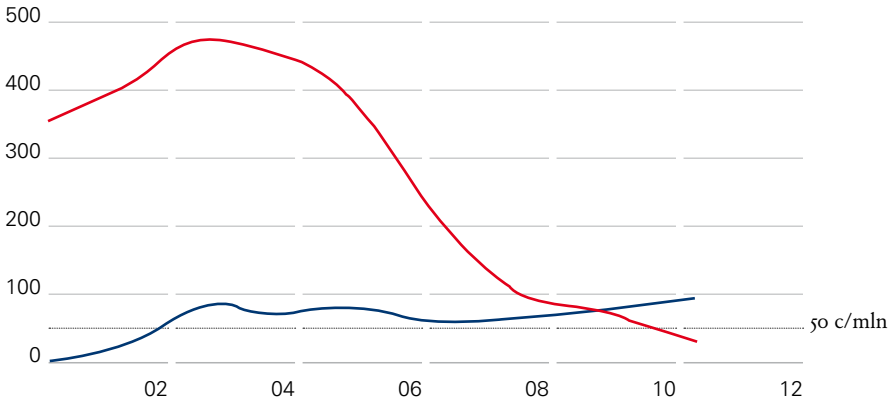


Public confidence score for the euro (in NL) and for the Canadian dollar over the years 2004 - 2011.

are contrary to each other. While in Canada the number of counterfeits dropped from 470 c/mln in 2004, the number of counterfeits in the euro area is clearly on the rise, as is shown in Figure 23. This is of particular interest since in both situations the confidence is rather stable. Bank of Canada started with their confidence index at the counterfeit peak in 2004 when the public just started to regain confidence in the CAD notes, even though the actual rate of counterfeiting was still high.

Both graphs underpin the hypothesis that the public trusts their banknotes blind and is not bothered by the counterfeits in circulation, neither when the counterfeit trend is going up nor when it is going down. The result of this high confidence is that the Dutch people find euro banknotes withdrawn from an ATM real and reliable. They are also not bothered by the counterfeits in circulation and ready to accept banknote change from retailer without looking at it; indeed, the Dutch accepts the euro banknotes blind.
However some other research results indicate the opposite. When a counterfeit trend is going up, like in the Netherlands, people do know more security features: on average 2.5 in 2009 versus 1.9 in 2007. Also the group of people that can not recall a single security feature decreased from 20% in 2007 to 7% in 2009 (See Appendix 1, Table A1.1). An explanation for the raised public awareness are the additional information actions of DNB in 2007 and 2008. Also younger generations move in the research while older generations, who were not trained in banknote security features, disappear.

Figure 23
In c/mln

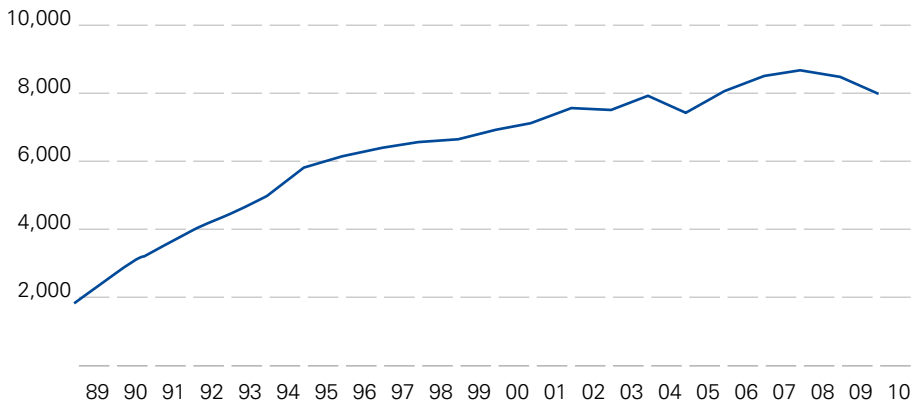


Counterfeits in Euro (blue curve) and Canada (red curve). Counterfeit threshold is set at 50 c/mln. Curves are constructed using the following figures:
EUR: 2004 = 62, 2007 = 49, 2008 = 55, 2009 = 67.
CAD: 2004 = 470, 2007 = 105, 2008 = 65, 2009 = 100, 2010 = 35 [101].

4.1.5 Vicious circle: public – counterfeiter – central bank

The first Automatic Teller Machine (ATM) was put in use in 1967 by Barclays Bank in London. The number of ATMs reached their saturation level around 2005 in the Netherlands as is depicted by Figure 24. A similar graph is published by the Bank of England [167]. It took about 30 years, but since the first years of the new millennium most Europeans get their banknotes out of an ATM (see e.g. references 65, 167). These notes are genuine and can be trusted for real, since cash recycling machines in Europe are only filled with fit banknotes checked on their authentication; a standardised recycling procedure was agreed for the Eurosystem in 2005, known as the 'Banknote Recycling Framework' (BRF) [66]. Credit institutions and professional cash handlers have to verify the euro notes used for filling the ATM. This contributes to the trust the public have in the notes they receive from the ATM. The future will bring more automatic use of banknotes, e.g. by the growth of cash-in/cash-out machines (cash recycle machines).
The public spends the notes coming out of the ATM at the shops. The retailer returns the change: one or two 5, 10 or 20 euro banknotes in case of a payment with a euro 50 note. These way members of the Dutch public receive on average one or two low banknote denominations a day [64]. These figures match with research done in Germany by the Bundesbank in 2008 [153, 168]. The average number of payments a day by a German person is 1.6 of which 80% is done in cash.

Figure 24



Development of ATMs in the Netherlands over the years 1989 - 2010.
Source: Nederlandse Vereniging van Banken (NVB).

Since the public trusts both the notes coming out of the ATM as the change they receive from the retailer, they are not triggered to authenticate their banknotes. As a consequence the counterfeiters are, as we will see, decreasing the quality of the public security features and focus on the retail features.

Central banks get weary of public's apathy

'The fast majority of counterfeits is of poor and mediocre quality' is a statement regularly heard, e.g. at the 'First International Banknote Designers Conference' in 2010. While central banks correctly communicate that the difference between a real and a counterfeit note is easy to tell, this message does not come across to the public. The central banks seem to over-claim this statement, leading to disappointment by public users (e.g. when they try to find the security features, see also user requirement 4.1.7.2 on easy to find). Since the probability of receiving a counterfeit note is low, the public has no drive to become interested in public security features. Central banks sometimes get weary of the public's apathy, as is witnessed by the following three statements made by central bank managers:

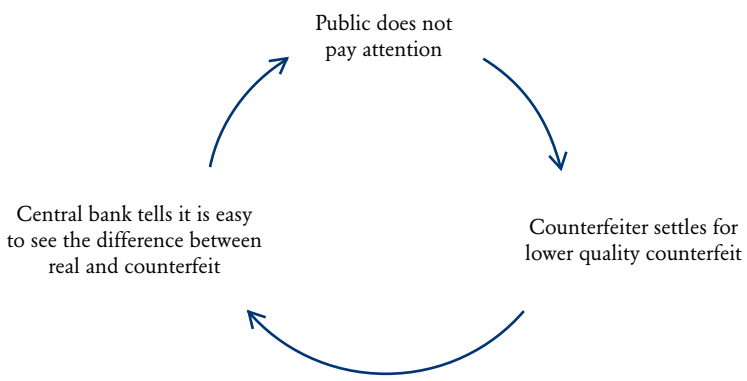
- I believe that in most cases the public is not concerned and does not really look at their banknotes (Thomas Ferguson, former Director of the Bureau of Engraving and Printing of the United States) [119],
- The public in general appears to have no clue what features to look for, and if they do, often they do not know exactly what the feature should display (ECB Monthly Report 2007) [99],
- The general public is urged to continue to play its part in the fight against counterfeiting by taking an interest in their money and being alert to the

possibility of fraud (José Manuel Páramo, member of the Executive Board of the ECB, on the occasion of the first Europol congress on counterfeiting) [93].

Summarizing: 'It is your civic duty to know your banknotes', the slogan of the central bank of Sierra Leone introduced in 2010.
How can this weariness be explained? Research by DNB sheds some light on this matter. The quality of counterfeits seems to be declining according to the 'simple method' as used by DNB. This method is explained in Appendix 5. It is an assumption of many that the quality of the counterfeited banknotes is always on the rise; instead counterfeiters seem to reason that counterfeited banknotes do not have to be very close to the original to be accepted by the public. The outcome of the simple method is that the quality of the public features reproduced in counterfeit euro banknotes is relatively low, i.e. 6.4 on a scale of 0 - 12. Probably, this quality will decline further; today's counterfeits are, with some exceptions, characterized by a higher quality of retail features and a lower quality of public features.

Vicious circle
The probability that the public receives a counterfeit is low and – as we have learned – the confidence in euro banknotes is relative high. This is why the public is not checking euro banknotes. As a consequence the counterfeiter starts producing a lower quality. This lower quality triggers the central banks to tell the public that it is easy to distinguish between a real and a counterfeit note! Here the vicious circle becomes clear (Figure 25). The vicious circle may be broken when the number of counterfeits is increasing and when people may become more alert.

Figure 25



How to break the vicious circle? Make designs that get attention of the public!

4.1.6 **Effect of training**

Central banks tend to promote their new banknotes with (increasing) media attention. Even movie stars were hired by the central bank of the United States to promote their latest redesigns! The effect on public knowledge of the security features of such media events is – as far as known – not researched. The assumption is that this will be limited as is found by the following three research studies done to the effect of training.

Effect of training (OLAF, 2005)
A first report on the effect of training came in 2005 from the European Anti-Fraud Office (OLAF). Research subject was the knowledge of security features and the ability to recognise counterfeits. The respondents were split into two groups: the general public and cashiers. Despite a poor public knowledge it was reported that the public was very well capable to recognise counterfeits. On the other hand, the public also classified several real banknotes as counterfeits. The cashiers recognised almost all counterfeits.
Training did increase to an almost 100% score in recognising both real and counterfeited banknotes. There was no significant difference found between training based on only real banknotes versus training sessions including counterfeited notes [67].

Effect of training (DNB, 2006)
The effect of training as reported by OLAF in 2005 was also found in a research project of DNB. In 2005 DNB investigated how accurately retailers (cash handlers) and the public (consumers) can distinguish counterfeit euro notes from genuine ones. Also examined was the question whether the use of DNB's educational CD-ROM entitled 'Genuine or Counterfeit?' led to improved performance and whether such aids as UV lamps or IR viewers helped to identify notes correctly. The results show that the public is quite capable of recognising a counterfeit note: without practice, members of the general public correctly identified 88% of counterfeit notes they were given to examine, while after training they scored as high as 96%. Remarkable scores were recorded by cash handlers operating without aids: even without training they showed themselves expert at sifting the wheat from the chaff (98% correctly identified counterfeit notes).
Recognising genuine euro notes proved slightly more challenging; just as in the OLAF-research the public classified several real banknotes as counterfeits.
Using the CD-ROM was helping untrained consumers in particular. Just by practising respondents soon managed to bring their performance up to the level of experienced cash handlers [80]. The findings were also reported at the Banknote 2006 conference.

Effect of training (BoC, 2010)
The Bank of Canada has quantified the effect of training. People seem to feel by intuition what is real banknote and which one is fake; just by looking and comparing is one of the findings. Training does little to improve authentication in case of a good security feature or in case of a poor counterfeited banknote. Untrained individuals are able to authenticate security features with an accuracy that can reach 97%. For the most sophisticated counterfeits training caused the greatest improvements in performance [155].

Increase of awareness of security features (DNB, 2002)
Next to training activities, central banks may raise public awareness of security features by improved banknote design and information campaigns as was done in the Netherlands. Public knowledge of security features increased significantly, as reported in 'A method for measuring the public's appreciation and knowledge of banknotes' [49]. Over the years, the public's awareness of security features in the Netherlands increased from an average of 1.03 feature in 1983 to 2.5 in 2009 [112, 133].

4.1.7 **User requirements public**

Good banknote design will reduce the need of training on real-fake banknotes and will also reduce the need of communication campaigns. For good design it is essential to know what the public wants. Here we arrive at the user requirements for public security features.
While the time needed to check a feature seems to be the most important user criterion for both the retailer and the public, there are more. In 2002, the Bank of Canada asked respondents to define the ideal security features. De Heij listed these requirements in 2006 and extended them with three more [81] and used these requirements in 2007 to evaluate several public security features [94]. Today the following user requirements for the public are determined:

4.1.7.1 Time,
4.1.7.2 Easy to find,
4.1.7.3 Understandable,
4.1.7.4 Univocal,
4.1.7.5 Single user,
4.1.7.6 Nest levels,
4.1.7.7 Delicate,
4.1.7.8 Striking,
4.1.7.9 Durable.

Similar user requirements will apply to the retailer.

Table 19

Public security feature	Central bank of Russia (2002)	Bank of Canada (2010)
	As accurate as possible, no worry about the time	As fast as possible, while optimizing accuracy
1. Watermark	8	4
2. Security thread	10.1	3.5
3. Holographic stripe	-	3
4. See-through register	-	5.5
5. Optically Variable Ink (OVI)	3.1	-
6. Latent image	18.4	-

Reported time in seconds to check a public security feature based on two different instructions. In case of the Russian Rouble banknotes people were asked to be as accurate as possible, not worrying about the time. In case of the CAD notes respondents were asked to be as fast as possible while optimizing accuracy.

4.1.7.1 *Time*

'It only takes a few seconds to check a banknote' we may read on the ECB's website. A similar phrase is found on the website of the Bank of Canada. The question is if this can be verified.
Research concerning time to verify a security features is rather minimal; the only available studies known are by the Central Bank of Russia [52] and BoC [155]. However, these two studies may not be compared to each other, since the instruction to the respondents was different. In case of the Russian Rouble banknotes people were asked to be as accurate as possible, not worrying about the time. In case of the CAD notes respondents were asked to be as fast as possible while optimizing accuracy. A second difference is that features were masked out from the rest of the banknote in the Canadian experiment as will be explained in Chapter 6. The two studies resulted in quite different values as is provided in Table 19. Based on this data of the BoC it would take 21 s to check a euro 50 banknote on all six public features (see Table A12.2).

Two seconds
How long does it take to master a public security feature? Two studies indicate that a time threshold of a security check on one single security feature is 2 seconds. In its 2006 study 'Counterfeit or genuine: can you tell the difference?', DNB used a fixed pitch of 2 s [80]. The second study concerned a haptic experiment with banknotes and reported that subjects were asked to feel each pattern for one or two seconds [126].

As we have seen, central banks advise the public for reliability reasons to check 3 security features (reliability > 99.99%), which altogether would take about 6 seconds (3 x 2 s = 6 s).
Some features may be checked within one look, especially when such features are grouped together in the banknote design. When for example the watermark and the see-through register are located close to each other in a banknote, checking both features will take less time (see also Subsection 4.3.2.5, Figure 65).

Criterion
Green: The feature is operated in less than 2 s.
Red : To operate the feature takes > 4 s.

4.1.7.2 *Easy to find*

Security features should be easy to authenticate and difficult to counterfeit (simplicity versus complexity), is what central banks often tell, like e.g the ECB in one of its Monthly Bulletins of 2007: 'The main challenge in developing a new series of banknotes is ensuring that, on the one hand, the new banknotes are innovative and difficult to counterfeit, and that, on the other, they are easy to check and have security features that can be easily communicated.' [99]. A similar policy is followed for the US dollar: 'Future US dollar features should be complex yet easy to explain to the users of currency' [121]. Many will agree with such statements. But will the central bank succeed in realising all of this? This is easier said than done! Indeed: 'If you can make it, they can fake it!', runs the motto of Mr. Martin Mund of the European Central Bank.

Central banks refer in such statements to the criterion of *usability*. Standard questions to define a feature's usability are:
1) Is the feature easy to find?
2) Is the feature understandable, accessible?

The second criterion on usability is discussed in Section 4.1.7.3.
In general pubic security features are not easy to find in a banknote. A person willing to check a just received banknote on its authenticity is often disappointed. Looking at the banknote they might think: where should I look, where is it? Analyses and design solutions are presented by De Heij in the two DNB-studies on 'Public feedback for better banknote design' [81, 94]. A relevant design parameter of a feature is its size.

Space
The larger a security feature, the easier to find. A (sub) criterion for easy to find is therefore the space the feature occupies (or surface S). To leave also space to other features, there is an upper limit to the size of a security feature.

Keeping the banknote at a reading distance of about 0.3 m to 0.4 m our eyes would typically focus on object sizes of about 30 mm x 15 mm (or 450 mm²). These dimensions might serve as guidelines for the dimensions of public security features [110]. This size comes quite close to the prescribed size of 400 mm² of the see-through register, one of the common elements in the 3 different banknotes issued in Hong Kong. Watermark areas in banknotes are often advised to be at least about 30 mm x 30 mm (= 900 mm²) [108].

Searching for an under and upper limit, it seems that a feature should have a surface of about 500 mm². If a feature uses space on both sides, like the watermark and the thread, the surface is multiplied by 2.
Clearly, more research on this subject is required.

Criterion
Green: 400 mm² < S < 600 mm².
Red : S < 200 mm² or S > 1.200 mm².

4.1.7.3 *Understandable*

Once the feature is found, the feature can be authenticated. An answer should be given to the following questions:
- Is it clear if the features should be: felt, tilted, looked-through or should be looked-at?
- Is it clear how this effect should be for a real banknote and for a counterfeited banknote?

All together the answers to such questions should tell us if the feature is understandable, if the feature is accessible. Once more this is a criterion needing more research, e.g. by experimental psychologists.

Criterion
Green: The feature is understandable.
Red : The feature is complex.

4.1.7.4 *Univocal*

The feature should not only be understandable, but the outcome should be a clear yes-or-no decision on the authenticity of the feature. In other words, security features should permit unequivocal discrimination between a real and a counterfeit banknote. The security thread is one example of a univocal security feature. If the note is held up to the light, a dark stripe should be seen, darker than any other part of the note.

Criterion
Green: Univocal, clear feature.
Red : The feature is multi interpretable.

4.1.7.5 *Single user group features*

A security thread for the public which is also used as a detector feature for third party sorting (Table 3) is an example of a *multi user feature*. Such a feature may be interpreted as two features, since it serves two user groups: public and 'third party sorting'. Or even more when for example the thread carries also micro-texts and would also have fluorescent properties (adding two retail human assisted features, leading to three user group levels). Ideally, however, a feature should serve just one user group to prevent sub-optimization for one or more of the relevant user groups. Multi user features also impede the replacement of such a feature. For example, if the security thread is no longer used as a public feature, it may still be required as a detector feature. For these reasons, *single user group features* are to be preferred; features for different users should not be paired.

Criterion
Green: Single user group feature.
Red : Features are paired, serving more than one user group (multi user feature).

4.1.7.6 *Nested features*

Related to single user features are nested features. A nested feature is a 'feature in a feature', meant for the same user group (so from that view a single user feature). An example is a foil (nest level 1) with a hologram (nest level 2). Both features are meant for the public.
Nested features are explained in Appendix 7.
The banknote itself is considered as one security product (nest level 0). Individual public features already start at nest level 1 and therefore should not include a second feature (level 2). To force the counterfeiter to layer their work higher nest levels may be considered to be included, but not for public use (see section 4.1, the paradox on holographic foil).

Criterion
Green: The number of nest levels of the feature is ≤ 1.
Red : ≥ 3.

4.1.7.7 *Delicate*

People do not want to offend others when they examine a just received banknote. The preferred authenticity check is therefore one that can be performed in secret.

Figure 26

Promotion material 'Know your banknotes', Bank of England (2006)

Holding a banknote up to the light can hardly be done discretely. To overcome this attitude some central banks, e.g. the Bank of England, promote holding a banknote up to the light as normal behaviour and advocate that such action should not be seen as offending or mistrust (Figure 26).
A retailer using a device to verify a banknote is clearly an obvious action, which seems to be more-and-more accepted by their customers.

Criterion
Green: Delicate checking of the feature.
Red : Obvious checking.

4.1.7.8 *Striking*

The desired security feature should be striking and provide pleasure during checking (the playing man: *homo ludens*). A case in point is *the nail scratch* feature in the euro, the former ISARD feature (see Appendix 5). Also the new micro-optical features (*or floating images*) provide some fun when operated (see Figure A9.3 for some examples).

Criterion
Green: Feature is striking.
Red : Feature is boring, dull.

4.1.7.9 *Durable*

Will the feature work well and resist failure in all required situations? The feature should work under different light conditions and temperatures, by the young and the elderly. For example, people should be able to operate a feature at minimum illuminance of 10 lux (twilight).
A security feature which loses its characteristics by wear and tear will complicate an authenticity check. Features should therefore be hard-wearing.
Features should have:

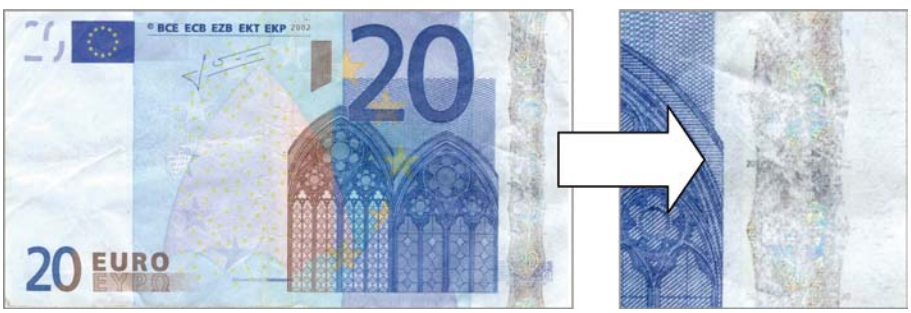
- A chemical durability like resistance to water, acetone and alcohol,
- A mechanical durability like tear resistance, folding endurance, abrasion, scratching,
- Anti soiling properties like e.g. the coffee test,
- Resist 'household attacks' like being washed in the washing machine, being ironed, heated in a microwave oven or left at the dashboard of a car in the hot sun.

The foil may serve as an example here. During circulation, the foil loses its gloss and the hologram becomes creased, making a check difficult for the general public (Figure 27).

Criterion
Green: Feature resists failure.
Red : Feature is vulnerable.

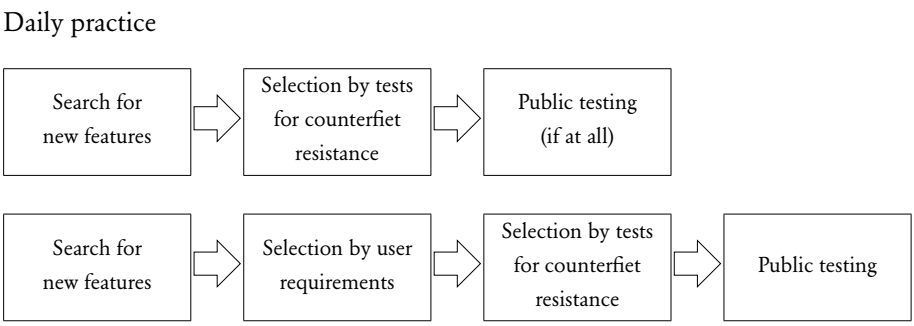
We leave the subject of user requirements here, again with the remark that more research on this topic is needed.

Figure 27



Foil abrasion on EUR 20 note from circulation (Summer 2003). The hologram is no longer visible.

Figure 28



Today a central bank focuses first of all on a public security feature's counterfeit resistance.
The proposed method is first to select public features by their compatibility with user requirements and, subsequently, to test their counterfeit resistance.

Select public security features by user requirements
Now we have completed the user requirements for a public feature, we arrive at the next step: the selection process. New features should first be selected on the basis of their compatibility with user requirements, for then it may be expected that the public will actually use the feature. In a second phase, the user-friendly features should be tested for their counterfeit resistance. The third phase, unfortunately, is often skipped, namely testing how the public responds to a feature combining design elements and technology (see Figure 28).

4.2 Method for selecting public security features

In Chapter 3 the all-in-one method has been applied to the retail features. The all-in-one method is also applicable on the features for the public; it follows similar steps:

4.2.1 Defining a human action feature matrix for a new banknote,
4.2.2 What goes out? - public features,
4.2.3 What will be improved? - public features,
4.2.4 What goes in? - public features,
4.2.5 Completion of public features.

4.2.1 Defining a human action-feature matrix for a new banknote

The all-in-one method starts with analysing the public security features in a banknote according to the human actions needed to check the feature. These human actions

Table 20

Euro Series 2002 – Public

Human action	Public features	
	Front	Reverse
Feel	1	-
Look - at	-	-
Look - through	3	-
Tilt	1	1

Human action-feature matrix of the Euro Series 2002. The 6 public features are divided over feel, look-at, look-through and tilt. The features are also divided over the front (5) and reverse (1).

are phrased in the 'Feel, look, tilt' motto of the euro banknotes. This slogan is used as a stepping stone to recall the public security features. In a *human action-feature matrix* these human actions are identified and distributed over the front or on the reverse side of the banknote. 'Look' is subdivided into 'look-at' and 'look-through' as done in Table 20.

Analysing the human-action feature matrix

Looking at Table 20 it is immediately clear that the euro banknotes do not have a 'look-at' public feature. And the three 'look-through' features provide a strong bias to hold the banknote up to the light. Such a bias in the new banknote is undesired because it doesn't match with the user requirement 'delicate' (Subsection 4.1.7.7).

Table 21

New banknote series – Public

Human action	Public features	
	Front	Reverse
Feel	2	-
Look - at	1	-
Look - through	1	-
Tilt	2	-

Alternative human action-feature matrix using 6 public features. All public features on the front. Features equally divided over feel, look and tilt.

Table 22

New banknote series – Public

Human action	Public features	
	Front	Reverse
Feel	+	o
Look - at	+	
Look - through		o
Tilt	+	o

Action-feature matrix of 6 public security features divided over 3 actively promoted features and 3 sleeping features.
+ = communicated active public security feature
o = non-communicated, dormant public security feature

We also would not like to have, e.g., 4 'tilt' features within a total of 6 public features, especially since people do not favour any tilt actions [81, 94].

Similar to the tool-feature matrix for the retail features, the action-feature matrix for the public could be optimised for the new series, as is done in Table 21. The public features are equally divided over feel, look and tilt; for each category two public features are positioned. The category of look-through features is reduced to one and one look-at feature is introduced. Comparing with Table 20, the central bank is in this example looking for an additional feel feature and for a new look-at feature.

Active and sleeping security features
Other concepts are also possible, like the example of Table 22, where a total of 6 public features, 3 active and 3 dormant, is divided over the front and the reverse sides. Three active features on the front would fit in a communication plan using banknote fronts only.

Disruptive human actions
There are more human actions to operate a public security feature than feel, look and tilt. People might use pressure, their body temperature or both. A disruptive human action to authenticate a banknote makes use of a new emerging technology that unexpectedly displaces an established one. An example is the mentioned nail scratch feature on the euro banknotes. Instead of the promoted feel of the relief of the letters 'BCE ECB EZB EKT EKP' people started to use their nails to verify the relief [81].

Table 23

New banknote series – Public

Human action	Public features	
	Front	Reverse
Feel	2	-
Look - at	1	-
Look - through	1	-
Tilt	1	-
Mobile phone with camera	1	-

Example of an action-feature matrix with a disruptive human action. Mobile phones are so widely spread, that the camera could be seen as an extension of the human senses.

Today there are more mobile phones in the Netherlands than there are residents. The camera in the mobile phones could be seen as a human sense [94] and might be added to the action matrix is done in Table 23, serving once more as an example and may be replaced by any settings a central bank might opt for.

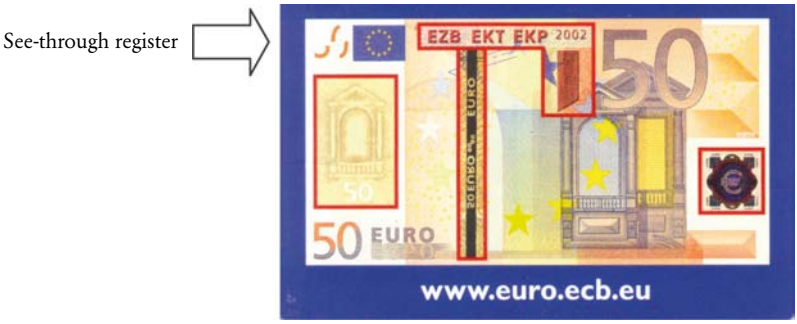
4.2.2 What goes out? – public features

Second step of the all-in-one method is to determine which features should not return in the new banknote by making an analysis of the existing features. To come to such an analysis a methodological tool is needed to assist the selection process of security features. Relevant criteria are:
- Public's knowledge,
- User requirements,
- Cost,
- Counterfeit analysis.

The user requirements are already explained in section 4.1.7. Cost and counterfeit analysis are explained in respectively Chapter 5 and 6. Public knowledge is explained below.

Public knowledge
Cherish familiarity with security features in old series like gold, the adage goes. That is why existing features enjoying high public awareness should be retained. From all features offered over the years these are the most successful ones as they are recalled the best. A fine example of such a traditional feature is the watermark. Used for the

Figure 29



Instruction on public security features on credit card size (ECB, 2009). The see-through register is not marked.

first time in a western banknote in Sweden in 1661, to date, almost 350 years later, it is still the most popular security feature for banknotes.
High public knowledge of security features is one of the most important criteria for deciding which features should be abandoned. However, we have to keep in mind that although many people may know the watermark, this does not mean that they may authenticate the watermark correctly.

DNB was in 1983 the first central bank to investigate the public's knowledge of banknote security features [49]. This method becomes extra useful here. A detailed overview of the public knowledge of the security features in the Netherlands is provided in Appendix 1.

Features left out in information tools (during circulation)
In 2009 the ECB left the information on the see-through register out in most of their new printed information tools, like e.g. a lenticular information card as shown in Figure 29. Also the special colours on the reverse (gold glossy stripe and colour changing numeral are left out). Other brochures issued since 2009 by the ECB reflect this policy too.
Discontinued features while the banknotes are still circulating are first candidates to leave behind.

Criterion:
Green: Features are communicated in recent information tools.
Red : Features are no longer part of information products.

Appendix 12 provides additional information
Additional information to the following summary of the all-in-one method applied to the public features you may find in Appendix 12. Concluding:

Out: 1) See-through register,
2) Colour-changing ink,
3) Holographic foil,
Dubious: 4) Watermark,
In: 5) Tactility (nail scratch),
6) Security thread,
7) Glossy gold stripe.

Introducing a full set of completely new public security features may be considered risky. Such a policy might demand too much public interest, especially since we have learned that the public trust the euro banknotes blind and is not interested in public security features. A central bank might want a more gradual approach and retain dubious features. Discontinuing a dubious feature like the watermark, which is the best known public feature, might be reconsidered.

4.2.3 What can be improved? – public features

Now it is known which features will go out, the features that – as a consequence – will be retained are also known (= existing features minus the 'out' features). Once the security-feature matrix What goes out? is completed (Appendix 12, Table A12.7) and it has been decided which features are abandoned, the remaining features should be filled in Table 24.
In this example we follow the concept of the human action-feature matrix presented in Table 23, which includes one disruptive action: the use of the camera in a mobile

Table 24

New banknote series – Public

Public use	Improve or new	Front or reverse	Public security feature
Feel	Improve	Front	1. Nail scratch
	New	Front	2. …
Look - through	Improve	Front/reverse	3. Security thread
Look - at	New	Front	4. …
Tilt	Improve	Front	5. Glossy gold stripe
Mobile phone	New	Front	6. …

Three features are selected from the existing euro banknotes, using the human-action feature matrix of Table 23. These features should be improved in the next design. Three new features are searched (feel, look-at and mobile phone).

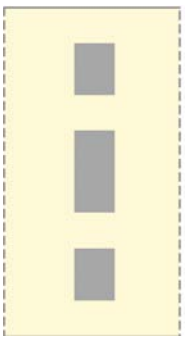
phone! In this concept there is only room for one look-through feature. The security thread is evaluated best; the watermark is for this reason deleted in the category look-through. The features that are retained should be improved in terms of design (public perception, communication) and/or technology.

Design improvements
The study 'Public feedback for better banknote design 2' provides several suggestions for improving existing features, like e.g. helping the human eye to focus on a specific element of a security thread. This study also includes a proposal for the design of a nail scratch feature [94].

Technology improvements
A windowed security thread would be new for the euro banknotes and is a technological improvement of the existing fully embedded thread with a width of just 1.2 mm (Figure 30a). The security industry has developed several security features for the 'windows' of such windowed threads (the small areas were the thread is on the surface of the note). Adding additional public security features to the thread, like holographic foil, colour shifting effects or micro-optics, will increase the number of nest levels and should therefore be considered with care.
Nail scratch features are printed with the gravure printing technique (intaglio), which is recently improved by the *computer to intaglio plate* technology (Figure 30b).

Figure 30

a) Windowed security thread



b) Computer to intaglio plate

c) Bi-coloured brilliant band

Examples of possibilities to improve existing public features by technology and/or design.
a) Security thread. Instead of a fully embedded 1.2 mm thread a 4 to 6 mm wide windowed security thread can be selected.
b) Computer to Intaglio Plate (CtIP). With a high relief and single colour (ink), many gradations can be made! The print was created by Giesecke & Devrient in 2004 within the scope of the 'Proper 3 project', part of the ECB research into New Intaglio Engraving Systems (NIES).
c) Bi-coloured brilliant band called Irisafe. An iridescent striped coating integrated into security papers and characterized by brilliant and changing colours, when the angle of view is changed. A product of Landqart; first introduced in 1997 in Austrian Schilling banknotes.

An example of an improved tilt feature, a dual coloured iridescent band, is shown in Figure 30c. There are also stronger iridescent colours on the market, with a more clear effect (higher saturation, a larger difference between transparency). View angle is around 80° and the view angle of the reflection colour is around 30°. Such inks are known as Colorcrypt, available at the company Merck.

Feature matrix 'What can be improved?'
Similar to the feature matrix *What goes out*? a public feature matrix *What can be improved*? is made as done in Appendix 12, Table A12.9. So, the following existing features will be improved by:
- Nail scratch feature: use CtIP and an inviting design for both right and left handed people,
- Wide windowed security thread,
- Strong iridescent ink, in one colour (of the banknote).

4.2.4 **What goes in? – public features**

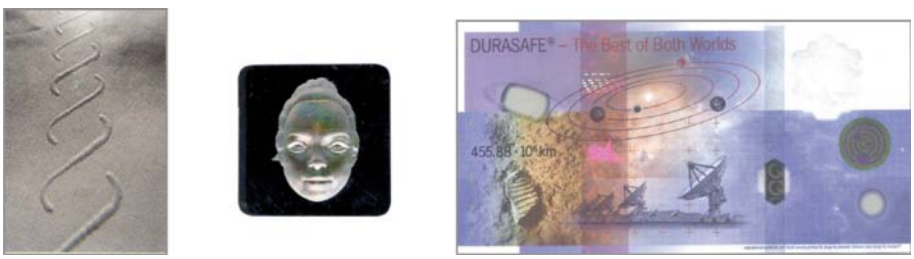
The all-in-one method is continued with step 4 focussing on *what goes in*? Next to 3 features that have to be improved we are also looking for 3 new features:
- One feel feature,

Figure 31

a) Tactile elements inside paper

b) 3D image, foil using E-beam imaging

c) Hybrid banknote using polymer and cotton layers



Examples of innovative public security features.
a) A novel feel feature called Tactocel. A cellulose strip is fed in between the two layers of the paper machine. A pattern is printed on this strip, e.g. the one shown. The pigments used for the printed pattern include a chemical agent which expands when it comes in contact of the water in the paper machine. The expansion causes a volume increase in the printed pattern and hence in the characteristic relief. Product of Fabrica Nacional de Moneda y Timbre (FNMT); sample presented in 2009.
b) A novel foil feature based on the principle of 'visual tactility' (or 3D image). Produced by Optaglio, using a nanotechnology-based imaging method (e-beam). Optimised for poor lighting conditions. The sample was presented in 2009.
c) A novel substrate for banknotes called Durasafe. A composite (or hybrid) substrate using a polymer centre layer with a cotton layer on both sides. The substrate is extruded and is not a laminate. Transparent areas are possible. A product of Landqart; sample presented in 2009.

- One look-at feature,
- One tilt feature.

Make an inventory of available new security features
First action is again to make a list of all the new features for the public use, addressing the marketing description of Table 24. New public features should also match the user requirements.
Figure 31 provide some examples.

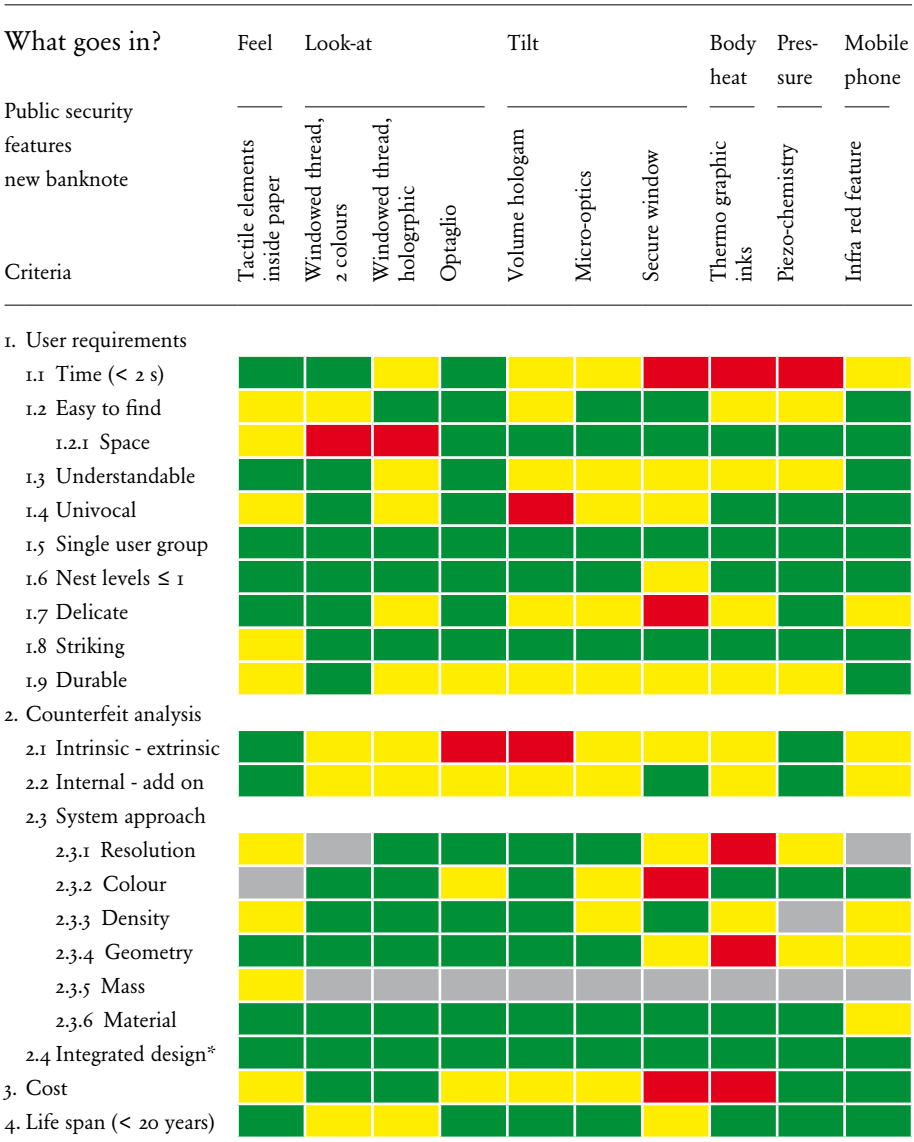
Feel and look-at features are needed
As said, today a central bank may choose from a wide range of public features. However, in certain segments this choice can be quite limited. Most features offered require tilting of the banknote and are based on colour shifting effects, micro-optics or holographic principles. Apart from Tactocel, no explicit feel features are for sale. Spending hardly any focussed looks at the banknote explains that the touch of the banknote is an important trigger on counterfeits (see also section 4.3.1.4 on recollection of banknotes, heading information driven process).
Also the category of look-at features is limited. It seems that suppliers focus too much on tilt and look-through features [134, 156, 170, 175]. Appendix 9 provides more information on 'which features should be developed?'.

New features: take care!
Just as in any other business there are opinion leaders in banknote design. Once such opinion leader has selected a new feature, others will follow. This behaviour is quite typical within the banknote world. As these features often come from the security industry, it may be wondered whether they match the user requirements. In some cases, the features found are tested to verify if people are able to deal with them, but all too often central banks seem to rely on the selection of other central banks.

Matrix 'What goes in?'
Table 25 is the completed matrix 'What goes in?' concerning the public features, representing in the top row the categories feel, look and tilt. Next to the (camera of the) mobile phone two more disruptive technologies are listed in this Table for illustrative reasons: body heath and pressure, which are also seen as human actions. A special group of public features are those that can be verified with the help of a filter. This filter is build in a transparent area of the note, e.g. in polymer notes. By double folding the banknote and moving one half of the note – the one with the filter – over a security feature on the other half, a special effect can be veryfied based on interference colour or something else.

The second row in Table 25 lists the innovative features in the categories mentioned. Some of the innovative features were already specified in Figure 31 like swell inks in paper, 3D foil image and hybrid paper with secure windows. Other examples are

Table 25



What goes in? Overview of all criteria used in making a selection from 10 innovative public security features. Theoretical exercise; scored by De Heij.
*) possibility to come to an integrated design.

volume holograms, micro-optics (or floating images), thermo-graphic inks and an infra red feature to be operated by the camera of a mobile phone.

Table 26

New banknote series – Public

Public use	Improve or new	Front or reverse	Public security feature
Feel	Improve	Front	1. Nail scratch tactility (CtIP)
	New	Front	2. Feel feature in paper
Look-through	Improve	Front/reverse	3. Windowed security thread showing two colours
Look-at	New	Front	4. 3D foil image
Tilt	Improve	Front	5. Strong iridescent ink
Mobile phone + camera	New	Front	6. To be developed

Theoretical exercise: example of a completed human action-public feature matrix for a new banknote with 3 improved features and 3 new public features. One disruptive human action! All public features on the front.

The first group of criteria to be met are the user requirements (see Section 4.7.1), the most important of which would be the time needed to check a feature (i.e. less than 2 seconds). Many of the new features are complex, however, and take over 3 seconds to be checked. As a consequence, they do not receive the green light.

Every three months new features arrive!
And there are much more! Recently announced features are e.g. 'Spherically Pigment Orientation Technology' (SPOT) and 'transparent magnetic material' (MagForm). Selective laser ablation is part of the technology behind SPOT, one of the features promoted by Giesecke & Devrient. It is the policy of this company to invent a new security feature every year!
In transmission the magnetic material used in MagForm, a new feature by De La Rue, will be transparent, which is unusual for magnetic pigments.
To take new features on board is a strong desire, but take care. From guilloches to holograms; every new generation of banknote developers uses a new security technology phase and seems to forget about the old one.

4.2.5 **Completion of public features**

Table 26 provides further insight on the final outcome of the method proposed. Shown is the final human action-public feature matrix as it may be constructed when also the other phases of the all-in-one method are completed. In this example the watermark is no longer part of the new banknote.

4.3 Designing public security features

Once the central bank has finished the feature selection process, the preparatory work is not yet completed. In order to be effective, the selected features should be designed within a communication policy. To arrive at a communication policy more fundamentals on banknote design – and especially perception issues – should be analysed.

Banknote design could be brought further if the central banks and their banknote designers would make more use of cognitive sciences. The relevant area is known as *experimental psychology* (or *cognitive psychology*). Evaluations of banknote designs by psychologists will lead to a list of recommendations from a user's point of view. To come to such design advice questions have to be answered like:
- How do we process stimuli coming from a banknote?
- How to retrieve security feature information from a banknote by just looking at it?
- How do we perceive banknote design elements like colour, shape, movement and depth?

Once the central bank has a clue to such psychological knowledge, a banknote series concept may be prepared. In this phase, questions must be answered like:
- Should all public features go on the front?
- Should all denominations have the same design?
- Should all the look-through features be grouped?
- What should the public security features communicate?

This final Chapter of the method proposed is divided in two sections:
4.3.1 Evidence based design: using experimental psychology,
4.3.2 Banknote series concept.

4.3.1 Evidence based design: using experimental psychology

Any attempt to explain mental processes inevitably oversimplifies. Still the exercise done below will unveil several design principles to come to better banknote designs. Some first suggestions to *evidence based banknote design* were made in both 'Public feedback' papers [81, 94], like *wayfinding features*, the *retrieval path* and the *preset lay-out* ('all features in a row'). Using the banknote as an example, the following subjects are presented in these subsections:

4.3.1.1 Visual information travelling from the eye through the brains,
4.3.1.2 Prototypical design elements,
4.3.1.3 Short and long-term memory,
4.3.1.4 Recollection of banknotes,

4.3.1.5 Change blindness,
4.3.1.6 Eye movement planning.

4.3.1.1 *Visual information travelling from the eye through the brains*

The image of a banknote can only be seen when there is light: day light, artificial light or both. The light that is reflected by the banknote reaches our eyes. The lens in our eye focuses the image of the banknote in the back of our eye, the retina. The centre of the retina is the fovea, the area of the eye used to look at details, it has the highest resolution. The light rays falling on the retina create chemical changes in the photosensitive cells of the retina (only cones, no rods), which then lead to nerve impulses.
On the retina, the banknote is projected upside down, inverted by 180 degrees. From here the banknote information makes a rather long journey; it travels all the way from our eye to the back of our head.

Humans have two eyes and the banknote is usually seen by both. The projection of the image of a banknote is, because of a different location in space, slightly different for each eye, a phenomenon called *binocular disparity*. The brain uses this difference to create depth.
Each eye splits the banknote on their part into two pieces: one image on the side of the nose (*nasal side*) and one image on the *temporal side*. So the image of the banknote in our brains is in the end built up from four segments as a result of our two eyes.
The nerves on the nasal side cross each other in the brains. The temporal sides of both eyes do not cross. The nasal side of the right eye projects on the left part of the brain, the *left cerebral hemisphere* and the nasal side of the left eye on the *right cerebral hemisphere*.

Figure 32

Low-pass filtered (V1) Band-pass filtered (V1)

Simulation of image processing in V1 of a euro 10 banknote: one low-pass filtered image (left) and one band-pass filtered image (right). Images made by De Heij using imaging software.

Figure 33

The silhouette is a prototypical design element of a banknote A banknote silhouette is defined by the length L and the height H. Drawings are scaled proportionally.
Left: any USD denomination, ratio L/H = 2.3 (156 mm/66.3 mm).
Right: euro 50, ratio L/H = 1.8 (140 mm/77 mm).

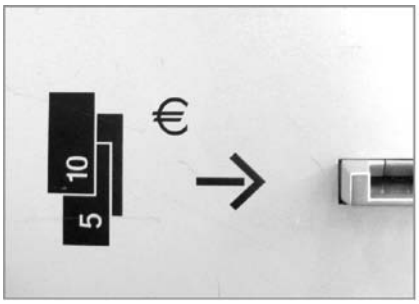
When the banknote information leaves the eye via the optic nerve it is no image yet. The first station passed on the optic nerve is the *Lateral Geniculate Nuclens* (LGN). From the LGN the nerves form a sort of fan called *radioato optica*, which projects the banknote information to the second station, the *primary visual cortex* or *V1 (visual area 1)*, part of the *occipital lobe*, one of the four lobes of our brains. One lob, the *frontal lob*, takes no part in the visual processing; the other three each contribute in a different way.

In V1, the banknote that the eyes have seen is for the first time represented as an image (built up from 4 segments). The V1 processes a neural image consisting of two images, a low-pass filtered one and a band-pass filtered one (Figure 32). V1 also processes colour, shape, texture and motion [89, 157].

Banknotes are rectangles
Characteristic for the low-pass filtered banknote is its silhouette, the contour. In the case of banknotes this silhouette is always a rectangle. However there are a few exceptions like square, pentagon or round banknotes as was the cases for some historic banknotes and for some special issues like commemorative banknotes.
US dollar banknotes have a typical silhouette which is similar for all denominations (Figure 33, left). Rectangles are defined by the length L and the height H and by their orientation (horizontal or vertical also known as landscape or portrait style). The ratio L/H is one of the *prototypical design elements* of a banknote, like is the case for the US dollar banknotes. Prototypical design elements are explained further on in Section 4.3.1.2.
In case of the euro banknotes all 7 denominations have different ratios L/H and therefore the silhouette of a euro banknote is not a prototypical design element (Figure 33, right).

Figure 34

Payment instruction on ticket machine



Instruction to collect banknotes from ATM

Banknote handling instructions on banknote automates. The currency symbol € is used to indicate the euro banknotes.
Left: Feeding instruction of euro banknotes on a ticket automate of the German railroads Deutsche Bahn (Hamburg Hbf, 2010).
Right: Handling instruction on ATM of ABN AMRO (Amsterdam, 2010).
Pictures by De Heij.

Some more proof for this statement is the instruction on the ticket automates of the German railroads as shown in Figure 34 on the left. The banknotes depicted are not using the silhouette or any other prototypical design element of the euro banknotes. The banknote images are:

- Similar in size (while the euro banknotes sizes are all different in both length and width),
- Ratio L/H = 2 and does not fit any of the euro denominations,
- Vertical orientation (while the euro banknotes are horizontal).

To make clear that the banknotes depicted are euro banknotes the euro currency symbol was added to the instruction.
Figure 34 provides one more example, showing the handling instruction to the public to get the euro banknotes out off an ATM. In this case the euro banknotes are only characterised by their currency logo.

Feedback and feed-forward connections
The silhouette or shape is one of the characteristics of a banknote and there are more typical parameters like colour, depth, movement and spatial tasks, each of them processed in different parts of the brain. We seem to be only at the beginning of exploring the human brain. Let us go back to the brain route the visual information on the banknote will take and describe what is known to date about this brain process.

Before the banknote information arrives at V1 a decision is already made about the route after V1. The banknote information can either go via visual centres V2 and V3 to V4 (*ventral* or *what route*) or via V3 to V5 (*dorsal* or *where route*)
And there is much more. Banknote information processing in the human brain is no one-way communication process. It is definitely not a serial process; the brain is a large network with many feedback and feed-forward connections. In other words, the higher visual centres (like V3, V4 and V5) communicate their findings also to the lower centres (like V1 and V2).
As far as known, in V4 the banknote is perceived in terms of colour and shape, while in V5 the banknote is perceived in terms of movement and spatial tasks. Area V3 is part of both pathways, but its processing role is still uncertain.
Just to give a flavour of what is happening, we keep tracing the image of the banknote in our brain. The *Lateral Occipital Cortex* (LOC) receives input from V2 and V3. The LOC has neurons that respond to shapes irrespectively of how the bounding contours are defined, allowing us to discern an object or pattern. Another important part of the human brain is the *Cerebral Cortex*, i.e. a sheet of neural tissue in the outermost of the brain. It plays a key role in memory, attention, perceptual awareness, thought, language, and consciousness. It is constituted of up to six horizontal layers, each of which has a different composition in terms of neurons and connectivity [87, 110, 127].

4.3.1.2 *Prototypical design elements*

Already in childhood people learn to accept a banknote for payment. After a few times the stimulus and the response become linked; people take the note (stimulus),

Figure 35

a) Silhouette cameraman

b) Heart silhouette with little figures

c) Letter U with flora and fauna

d) Tree silhouette with different products

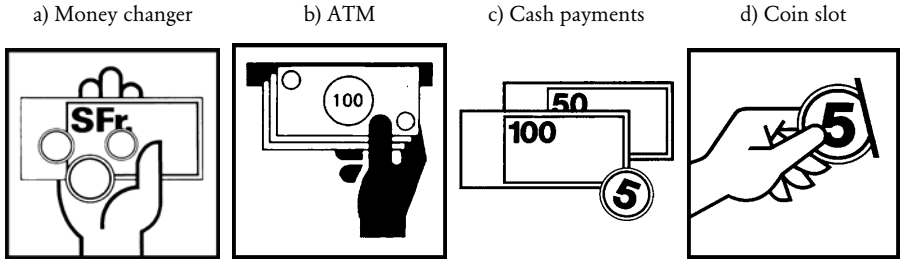
Public security features should have a clear silhouette or skeleton and should therefore be designed in 2D rather than 3D. In graphic design, such silhouette designs are quite popular these days:
a) Silhouette of cameraman (publisher unknown),
b) Heart made by Keith Haring (1980s),
c) Logo if Unilever (2007),
d) Logo of V&D (2008).

have an instant value check and store the note – without further thinking – in their wallet (response). Burrhus Frederic Skinner (1904 – 1990) became famous for his 'stimulus-response' research. Skinner was an exponent of *behaviourism*. Behaviourists consider behaviour simply as a learned response to an external stimulus. Skinner was not interested in how the mind affects behaviour [87].

Gestalt theory
Psychological movements like *introspection, functionalism, associatism* and *behaviourism* did not bring new insights into the perception of products like a banknote, but the *gestalt theory* did.
According to gestalt psychologists the individual elements are not important; it is the whole that matters. It is useless to study single line patterns on a banknote if we want to have an idea of the overall banknote [87].

'Recognition by components' as proposed by Irving Biederman in 1987 is relevant for banknote design [24]. In a split second – from a single visual fixation – humans are able to identify a banknote, often under highly degraded and novel viewing conditions. To account for this extraordinary capacity, Biederman proposed that objects are represented as an arrangement of simple, convex, viewpoint-invariant shape primitives, termed *geons*, such as bricks, cylinders, wedges and cones. Shapes and objects like a banknote or penguin can all be represented by using 36 geons following laws or principles of our brains, the *gestalt laws*. Objects can be identified far more rapidly if they are presented in views that clearly reveal the connections between the component parts, which correspond with the structural skeleton of objects in Biederman's theory.
A person has no choice but to recognize a chair or a banknote by its geons [160].

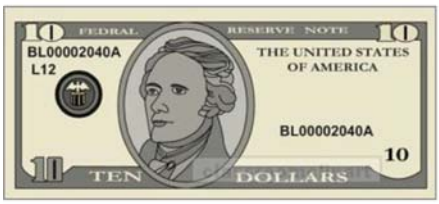
Figure 36



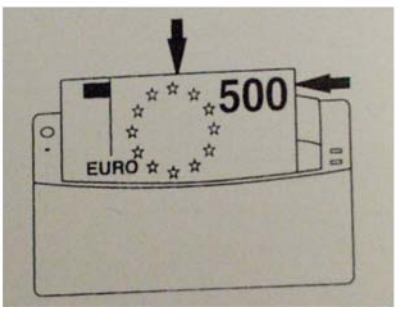
The images, the logos that are often made for money exchange offices or ATMs are a bridge between the geons and the prototypical design elements of a banknote.
a) Money changer (designer unknown, 1980s),
b) Pictogram designed and tested for world wide use by the ATM Industry Association (designer unknown, 1990s),
c) Cash payments (designer unknown, 1980s),
d) Coin slot (designer unknown, 1980s).

Figure 37

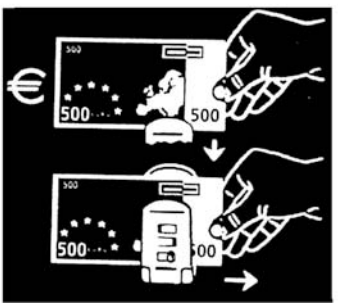
a) Simplified US dollar banknote



b) Cash payment instruction - euro



c) Euro banknote feeding instruction on authenticity device



d) Euro banknote feeding instruction on authenticity device

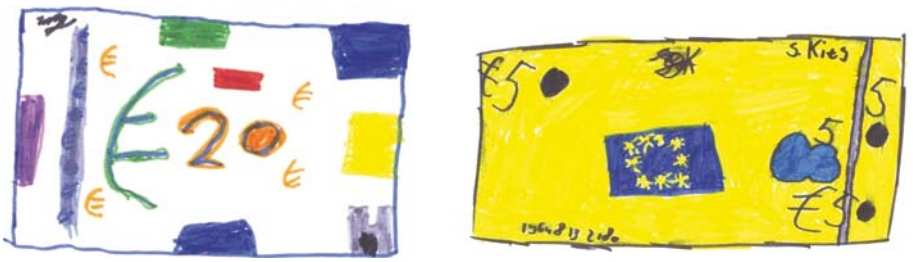
Examples of prototypical design elements for US dollar and euro banknotes.
a) Simplified USD 10 banknote, showing the prototypical design elements of a USD 10 banknote (issued in 2000).
b) Part of an instruction at a gasoline station in France, showing prototypical design elements of euro coins and banknotes (2010).
c) Instruction on a banknote authenticity device CT 2004 by Cash Test (2004).
d) Instruction on a banknote authenticity device Catcoin MD50 (2003).

From the foregoing it follows that public security features should have a clear silhouette or skeleton and should be in 2D rather than 3D and. In graphic design, such silhouette designs are quite popular these days (see Figure 35 for examples). The images, the logos that are often made for money exchange offices or ATMs are a bridge between the geons and the prototypical design elements of a banknote (Figure 36).

Prototypical design elements of euro banknotes

Some more detailed images of banknotes are provided in the designs shown in Figure 37. Such designs are often used for stickers to inform people on cash payments or to inform them on the right use of a banknote detection device. The design of these 'sticker images' tell us that the characteristic design of a euro banknote are the large numerals, the ring of stars, the word EURO and the map of Europe (and not the gate/window or bridge as will be argued further on).

Figure 38



Two banknote designs for a new euro banknote made by 12-year-old children in 2008. Designs were made within 15 minutes.

Draw a banknote!

Other sources on typical design elements of banknotes are drawings. Ask 10 people to draw a banknote within 1 minute and they will probably all be quite similar. At two occasions De Heij asked children to make a drawing for a *new* euro banknote. This is what came out. Most designs did not make use of a window, gate or bridge. From these two exercises (in 2008 and 2009), it emerged that for children around the age of 12 the prototypical design characteristics of a euro banknote are: a large numeral, rectangular areas, euro currency symbol (€), the EU flag and a silver coloured stripe. The research was qualitative; two typical examples are shown in Figure 38.

From the instruction images and the drawings we learn that it is not the image of a window or gate that typifies a euro banknote. This gave De Heij in 2008 the idea to do some 'photo shopping' on the euro banknotes and to offer these images to the Dutch public in the bi-annual public survey of 2009. The outcome of this research is as expected. The images on the euro banknotes may be switched without noticing,

Figure 39

Which is the correct euro banknote?

People do not recall which is the correct euro 10 banknote. The one on the left or the one on the right? Test your self!

Figure 40

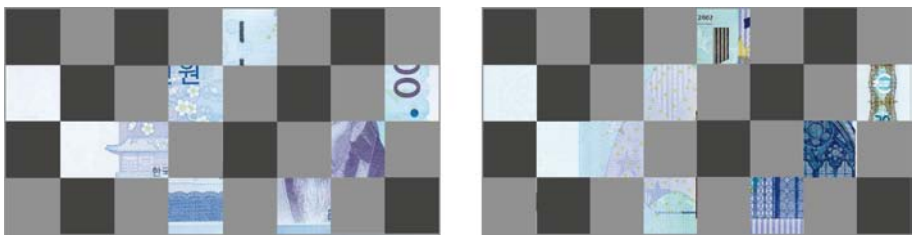
It is me, Alexander Hamilton! I am the portrait on the USD 10; I was the first Secretary of the Treasury (and was never President of the USA) [169, 174].

as long as the colours of the note are used, as reported in the study 'Banknote design for the visually impaired' [148] (see Figure 39). Other currencies, like the USD have similar problems as is illustrated by Figure 40. The portrait depicted in the dollars banknote showed would like to know if you would be able to tell on which denomination he is printed?! This phenomenon is further explained when the memory paths are discussed in Subsection 4.3.1.4.

The decision of the ECB to keep the main design elements of the euro banknotes for the Euro Series 2 was already done in 2003, shortly after the issuance of the first series in 2002. The main argument was 'to signal continuity' (Annual Report

Figure 41

Which banknotes are hidden behind the grid?



Prototypical design elements of these two banknotes are covered. See Figure 42 for the answers! Images prepared by De Heij.

Figure 42

Get the picture!

KRW 1,000 (2007) EUR 20 (2002)

Left: South Korean won 1,000, issued in 2007. The portrait is a Toegye, a Confucian scholar.
Right: euro 20.

ECB, 2003) and no further analysis was done. Such 'too early' decisions are limiting flexibility for more optimal design decisions further on in the project [181].

Get the picture!
Prototypical design elements may be tested by an experiment similar to *Get the picture!*, a popular entertainment programme on television. An image is completely covered with grid elements or 'tiles'. How many and which tiles should be removed before the image becomes clear?

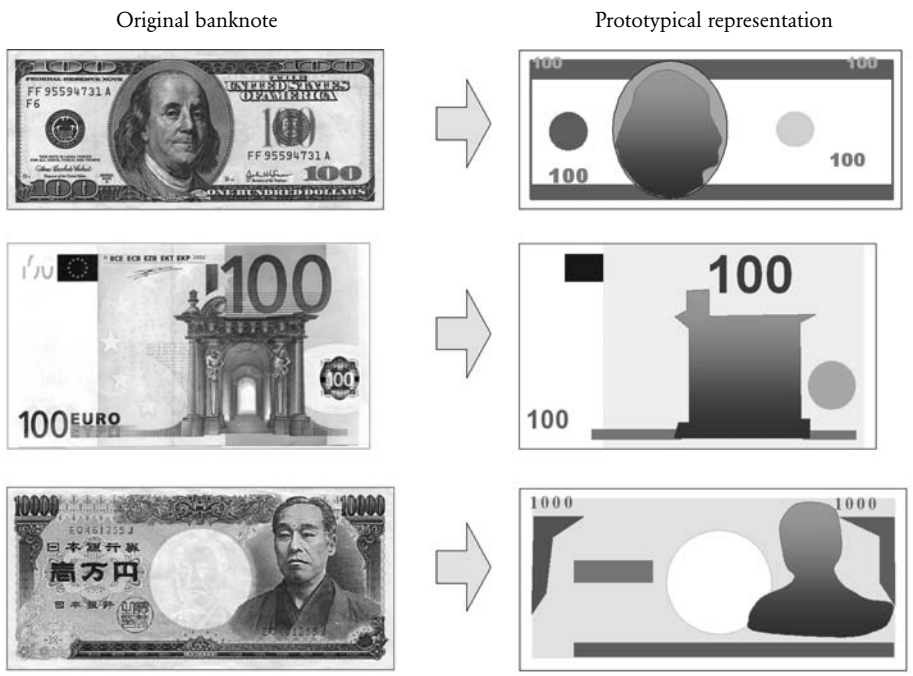
The prototypical design elements of a banknote may be discovered by taking away tiles of the covered image of a banknote. Just as in case of the drawings by children this will give us a clue on the information carrying banknote components. Some tiles facilitate recognition more than others. If, for example, the tile covering the European flag is removed, it will be easier to guess which banknote is hidden.

Figure 41 shows two banknotes covered with a grid. In this stage it is not clear which two banknotes are shown; their prototypical design elements are not yet unveiled. In the game 'Get the picture!' it is usually one image that persons are asked to identify.

Derivation of prototypical design elements
Additional to tests to discover prototypical design elements like discussed above, the most characteristic design elements of a banknote may also be traced back by low-pass filtering techniques. Figure 43 provides some examples using banknotes of three major world currencies: the US dollar, the euro and the Japanese Yen.

Euro banknotes are characterised by vertical orientated design elements like the white area on the left, while the designs of the dollar and the yen banknotes are

Figure 43



Example of a prototypical representation of three different banknotes. From top to bottom: the USD 100 (1996), the EUR 100 (2002) and the JPY 10,000 (1984). Colour is one of the major design parameters and has been left out. Prototypical representations are made by De Heij.

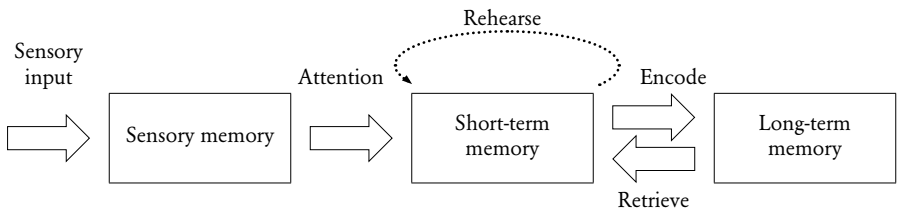
using more horizontal oriented design elements as may be deduced from Figure 43. To enforce the identity of the euro banknotes, the vertical design elements should be kept and could even be made more prominant. Analysing the prototypical representations of these three banknotes is part of a separate future study focussing on *banknote identity* [176].

4.3.1.3 *Short and long-term memory*

The human memory is complex and has many aspects. The characteristics of the short-term memory were first described by G.A. Miller in 1956. Figure 44 is a simplified model of the human memory as published by Frans Verstraten [87].

In the case of a banknote, visual and tactile information enter our body via the human senses. Often there will also be some auditory input, like the rustling of a new banknote and even some odour input might be there in case of freshly printed banknotes. Such *sensory input* is stored in the *sensory memory*, which has a vast

Figure 44



A model of the human memory. The short-term memory together with the retrieve arrow is the working memory.

capacity and works like a photographic plate; it freezes the information for a short term. In the case of visual information, this moment lasts only half a second and for auditory information, a few seconds. The *visual* information in the sensory memory is also called *iconic memory*.

Selection of the sensory memory to the short-term memory is done by *attention*. Attention is a kind of filter that passes information. If we are looking for a euro 20 banknote in our wallet, we know that it is blue and start searching for blue, ignoring other colours.
One of the keys to get attention is emotion. Adding emotive images to a banknote can turn a disinterested audience into an attentive audience. With emotions (arousal), we have more chance to save something on a banknote. It seems logical to use emotive images for the public security features instead of the common practice to add emotion to the main banknote image, which is often a portrait. Without some emotional valence the public security features will not be effective simply because the audience will not care. Numerals (like e.g. 10) or currency symbols (e.g. $ or €) should for this reason not serve as images for the public security features. Proposals for emotive images for the public security features are done in Section 4.3.2.

Short-term memory
The *short-term memory* is like many neural network models, not a separate system. The capacity of the short-term memory is very limited and is different for the different senses. The short-term memory can memorise about 7 letters or words plus or minus 2, as first reported by Miller in 1956 [3]. With *chunking* (combining) this capacity can be increased. To remember EUECSBECBDNB is easier if you read it like EU ESCB ECB DNB. Visual images may also be chunked. The short-term memory may hold information between a few and 30 seconds.
The limitations of the short-term memory are the reason why we must often rely on external visual aids in the process of visual thinking. *Visual queries* for banknotes

Figure 45

Conceptual banknote design for a 100 Florin banknote for the Central Bank of Aruba. Five public security features may be found by following the letters A-R-U-B-A. The study focussed on banknote identity, recording the history of banknote design elements in banknotes issued in the European Union, Netherlands, Caribbean area, South America and USA. Design by De Heij (2007) [165, 170].

should be designed in such a way that they will pass the filter of the visual working memory to the long-term memory. A visual query consists of a series of acts of attention, driving eye movements and tuning our pattern-finding circuits. In case of a banknote design this means that an 'eye travelling path' should be created. An example is provided in Figure 45, when attention is given to the individual letters of the word A-R-U-B-A. Eye movement planning is further discussed in Section 4.3.1.6.

Working memory
The capacity of the short-term memory is enhanced with information input from the long-term memory (the *retrieve* arrow in Figure 44). The short-term memory including the retrieve activity is called the *working memory*. The operative term in working memory is work, not memory. Information is only retained in the working memory from between one-tenth of a second and, at most, a few seconds, and only to support some ongoing cognitive process.
The working memory has two servers: a *verbal working memory* and a *visual working memory*.
The number of items the *visual working memory* may hold is limited. With each cycle the visual working memory may be erased, new items are stored and some may be kept [87, 110, 127].

Add verbal information to banknote design
The working memory uses both visual and verbal (or linguistic) stimuli. Public security features are therefore enforced if the design of these features uses both verbal and visual information. Public security features are better memorised if they have a name and this name is printed along the feature. This principle was introduced by DNB with the *Abstract Series* designed by Jaap Drupsteen. The

Figure 46

Watermark
Kieviet (Lap wing)

See-through register
Stekelbaars (Stickel back)

In the *Abstract series*, the name of the public security feature is printed above the feature. This was first done in 1989, in the NLG 25/Robin.
Left: text KIEVIT above the watermark in the NLG 1000/Lap Wing.
Right: text STEKELBAARS in the see-through register (NLG 10/King Fisher).

name of the watermark was printed besides the watermark and the name of the see-through register besides this public security feature (see Figure 46). The first note of this series was introduced in 1989.
This principle, which DNB based on research conducted by Peek in 1972 [5], is explained in more detail in 'A method for measuring the public's appreciation and knowledge of banknotes', published in 2002 [49]. Verbal stimuli are also one of the reasons for providing a banknote design with a name. The name of the banknote has been printed on the Dutch banknotes consequently since 1953 [43].

Long-term memory
The long-term memory is divided into two parts, the *explicit* and the *implicit long-term memory*. In the case of banknotes, the security features learned are stored in the explicit long-term memory. Knowledge of banknotes gained by accident is stored in the implicit long-term memory. The explicit and the implicit long-term memories correspond with respectively rule-based perception (learning the public security features) and heuristic perception (implicit quality standards), as discussed before in Section 4.1.1.

Imagery
When we look at something, much of what we consciously perceive is not what is 'out there', but what is already in our heads in our long-term memory. We see a banknote from the outside world, but also from the inside. The visual representation of an image from the outside world in our memory is called *imagery*. There are thousands of banknotes, from many countries, old and new, and we collectively

store them by way of a draft, as a general description. The imagery consists of a concept of banknote or *gist*. A gist of a banknote is the rapid characterisation of a banknote, the banknote seen as *a pattern of a pattern*. This is the banknote people will draw when they are asked to draw a banknote in one minute [87, 127].

There is a difference between *removing* an element (a birthmark or a moustache) and *adding* one (start wearing glasses). It is often noticed by people when something has been added, for example to their room. 'What is that ashtray doing there?' But when something is removed from that same room, something that was always there, it is often not noticed.

Many people will also recognise the following situation: 'Look at me, what do you see?', asks the wife of the husband. 'A new dress?', the husband answers hesitantly. 'No, look at my hair! I have been to the hairdresser!' This is a fine illustration of imagery: the majority of what we see is recollection of old images.

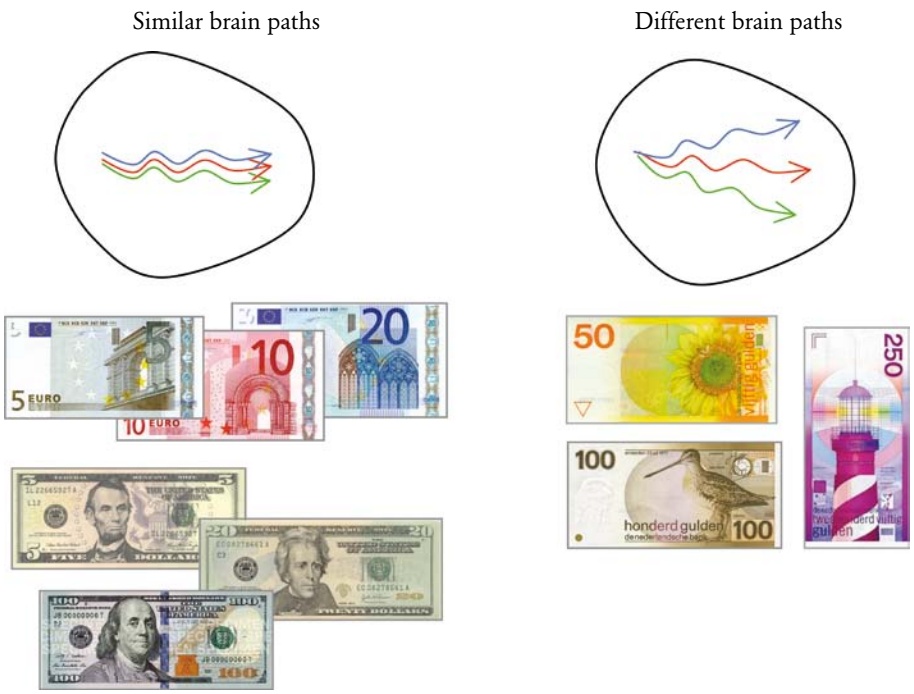
Imagery may also apply to the perception of banknotes. We do not see the original, but we see recollection of an original note! This explains why counterfeiters can permit themselves to leave out some security features, while something added like a stamp or writing on a banknote will often not be overlooked.
There are some other famous recollection examples that might be useful for banknote design, like e.g. the interior of a room. When people are offered an image of that room, they are very well able to reproduce an inventory list of all the furniture and other objects in the room. However, when the same furniture and objects are offered as single images, one by one in a random order, people are less able to recall all objects shown. This speaks in favour of a little story on the note, a stepping stone to recall the public security features on a banknote (see Section 4.3.2.2).

4.3.1.4 *Recollection of banknotes*

Around 1960, computers became a source of inspiration for *cognitive psychology* in two ways. The human brain was regarded as an *information processing system*. The binary representation of information in a computer (zeros and ones) was seen as similar to the storage in the human brain. The second inspiration was the computer program, the software. Programs can already simulate the activities of the human brain as it carries out cognitive tasks. In the 1980s, the first brain-scanning techniques became available for locating the human brain areas that are activated during the performance of certain tasks, the field of *cognitive neurosciences*. Relevant for banknote design is the recognition of human faces.

Recognition of human faces
Recognition of human faces is located in a sub-region of *inferotemporal cortex* (IT),

Figure 47



Schematic representation of memory paths of banknotes. Quite similar to each other like the euro and US dollar series (left) and of the more divergent memory paths of a banknotes series far more variable in theme and main image (right).

which contains neurons specialised in complex visual patterns corresponding to recognizable objects and scenes. There is an IT sub-region called the *fusiform gyrus* that contains cells responding specifically to faces. Hence, given that there is a strong case for using portraits, another subject, e.g. a bird, might fulfil the same function; there are many areas localised in our brains having specific functions in recognising and processing parts of our environment [87, 127].
Portraits on banknotes were world wide introduced since the early 1920s. The recent trend is to leave portraits. Several central banks followed the example of DNB in 1981, like South Africa (1993), Euro (2002), Denmark (2009) and Bermuda (2009). Also the new Swiss banknote series will no longer bear a portrait. However, the debate is not yet finished. At the recent First Banknote Designers Conference the pro and cons of portrait gravures were discussed by banknote designers and engravers (see also Section 6.2.1.2 on portrait feature).

Measuring brain activity
After locating specialised brain areas, it also became possible to measure brain

activity. Such measurements are called *Event Related Potentials* (ERPs). They were first performed with EEG (Electro Encephalogram), later with MEG (Magneto Encephalogram), and nowadays with fMRI (functional Magnetic Resonance Imaging) [127]. However, as nerves are outside the scope of this study, let us return to the banknote.

Memory paths

Long-term memories are not static and should therefore not be compared with fixed repositories like books or CD ROMs. The pathways that are activated when a cognitive task is carried out become stronger if that task is successfully completed. Such paths are called *memory paths* or *brain tracks*. Memory paths are quite passive and become active by priming. Priming activates knowledge in the explicit long-term memory by a cue [87, 127], like for example the letters A-R-U-B-A on the banknote as shown in Figure 45.

If memory paths are too close to each other the paths may – after some time – be combined, which is called *interference*. The main image within in the euro series are quite close to each other and are represented by parallel memory paths, just as the portraits of the US dollar banknotes (Figure 47, left hand side). More divergent memory paths of a banknote series designed with wider variations. Snipe, lighthouse and sunflower used on the NLG banknotes had their own discriminating silhouette and were selected from different categories: a bird, a tower and a flower. Different

Table 27

Name mentioned	Percentage
1. Snipe	25%
2. Lighthouse	15%
3. Sunflower	9%
4. Bird	5%
5. A head of a person	5%
6. Colour	4%
7. Michiel de Ruyter	2%
8. Frans Hals	2%
7. Others	~ 10%
8. Do not know	22%

Spontaneous awareness of pictures on NLG banknotes in 2009. Seven years after circulation of guilder notes ended, the best recalled image by the Dutch is that of the snipe, followed by the lighthouse and sunflower.
The question was phrased as: 'Before the euro, we had guilder notes in our country. Which guilder banknote do you recall best? In other words, which one pops up in your mind?'.

brain paths become active, which seems not the case with the euro banknotes (Figure 47, right hand side).

Images on euro banknotes are mutually replaceable
Some proof for this theory of different memory paths for banknotes is the result of DNB research. The images on the euro banknotes can be switched from one denomination to the other without noticing, as was first reported in 2006 [81] and confirmed in 2009 [94]. One of the reasons the similarity of the internal silhouettes of the euro denominations; all building parts are cut out in a similar square figure. Considering that they can be replaced without this being noticed by the average user if the main colour of the denomination is retained, the conclusion is that the images of windows and gates on the euro banknotes do not contribute to instant value recognition. The same is probably true for the portraits on the US dollar banknotes (see also Section 4.3.1.2 on prototypical design elements and Appendix 6 on the *flash second*).

Recollection of Dutch banknotes
Additional information supporting the preferred design policy of different memory paths for banknotes is provided by the outcome of the survey of the Dutch public's recollection of the last guilder banknote series. In 2009, seven years after the introduction of the euro, DNB asked the Dutch public which images of the former guilder banknotes they could remember [133]. The 'Snipe', as the NLG 100 note then circulating was popularly referred to, was mentioned by far the most, followed by the 'Lighthouse' and 'Sunflower' (Table 27).

Portraits are not recalled
First conclusion of this research is a counter-argument to people in favour of a portrait on a banknote. Only a few people recalled historical persons like Michiel de Ruyter (2%) and Frans Hals (2%). In an earlier research DNB reported that after 27 years of circulation only 14% of the public was able to tell the name of Frans Hals on the NLG 10 [49, 112].

Men proved better able to recall pictures on guilder banknotes than did women, mentioning the lighthouse and Michiel de Ruyter the most. Respondents between 35 and 54 years old could mention more pictures of guilder banknotes than those in the other age groups: the snipe, lighthouse and sunflower. The denominations of 25 and 10 guilders were best recalled (33% and 26%).

Main image serves emotional feelings
The latest guilder banknote series issued by DNB, the 'abstract series' designed by Jaap Drupsteen are not recalled. Kingfisher is only mentioned by 1% (Figure 48c). All denominations of the abstract series carried a bird in the watermark. That is why 5% of the respondents mentioned 'a bird', although they were not able to tell which bird.

Figure 48

Design: Robert Oxenaar

a) NLG 50/Sunflower (1982)

b) NLG 100/Snipe (1981)

Design: Jaap Drupsteen

c) NLG 10/Kingfisher (1997)

d) NLG 100/Little Owl (1992)

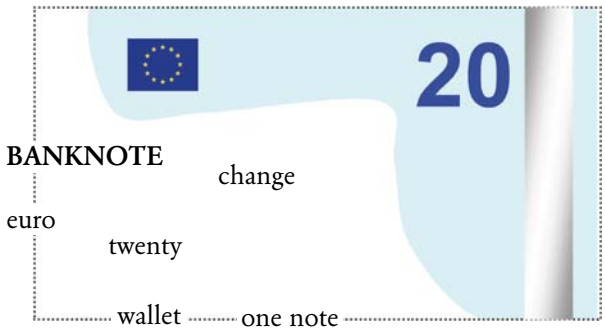
The banknote designs by Oxenaar are better recalled than the – of later date – designs made by Jaap Drupsteen.

From these findings one may ask: Does recalling content make authentication better? The answer is yes for two reasons. First of all people will be able to record the value of the note easiers with a characteristic main subject as in the case with the Oxenaar notes (Figure 48a and b) [148]. Secondly people will experience a stronger emotional experience with the designs made by Oxenaar. A stronger emotional attachment will lead to a higher appreciation of the notes and this will lead on its turn to a higher knowledge of the security features, since there is a correlation between appreciation and knowledge [49]. Banknote designer Roger Pfund advocates for similar reasons of emotional content the introduction of 'art' in banknote designs [94].

No emotions measured on euro images

The previous findings raise the following question: what is the purpose of a main image? The two main functions of a banknote are its value and its security features, which in themselves are sufficient to result in a characteristic design. If the main image is no longer a security feature, such an image on a banknote only adds value if it contributes to an immediate recognition of the banknote or if the image contributes to a positive emotion or appreciation. In case of the euro banknotes the two major stakeholders, the public at large and the retailers, are indifferent to both

Figure 49



Mental map of a euro 20 banknote. Only a few features of the banknote are linked to the knowledge we have about banknotes (e.g. colour, hologram, numeral and flag).
Based on the example of a dog in Visual Thinking for Design [110].

of these purposes of the main images. The euro images do not evoke any emotions as is reported by DNB in 2006 [81], neither do they contribute to instant value recognition [148]. As a consequence these images should be changed or removed.

Mental map
Having touched upon memory paths, imagery and prototypical design elements, we arrive at the subject of a *mental map*. Such a mental map consists of both visual and verbal information like words. If we *think* of a euro 20 banknote, nothing resembling a picture of a banknote appears in our visual working memory, in our imagination. Figure 49 is an example of a mental map made of a euro 20 banknote. The notion of a banknote stored in our head is a combination of features bound together by the knowledge we have about banknotes in general and notions about this particular banknote, like change, cash, euro, twenty, blue, one note.

Analysing a typical cash transaction
Let us take the situation where we receive a banknote in return for a cash payment at the supermarket checkout counter. How do we perceive the change? Assume the change is several coins and one euro 20 banknote. Suppose the retailer hands over first the coins and next the banknote. To focus our attention on the pay out of the coins we use our rapid eye movements (or saccadic eye movements). Once focussed, we follow with smooth eye movements first the coins one by one and then the banknote.
Next step is to stow away the change received in our purse. So there are two moments in time that we might be triggered to check the authenticity of the euro 20 banknote: the pay out by the retailer and the storing of the note in our wallet. What happens during these two moments?

Information driven process

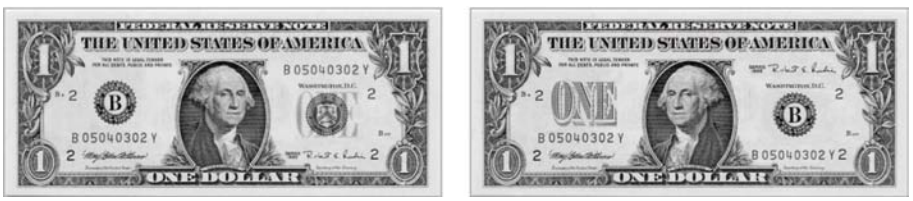
During the pay out by the retailer our first goal is to verify if the correct amount of change is given and especially if the value of the banknote is correct. So the relevant information our brains will enforce while processing the banknote image will be to look for the banknote's value. In this case the colour of the banknote and the denomination numeral will give louder signals. Telling the banknote's value is accomplished by an iterative process of linking and re-linking visual and non-visual information about the banknote.

Our vision, including our brain processing, is fully occupied with the cash transaction itself. First we have traced out the coins in our visual working memory. In parallel our tactile senses become active and the touch of the banknotes may be the most important trigger on counterfeits. This explanation is supported by research done in 2002 by the US Treasury [53]. They reported that 25% of the cash handlers only check the just received banknote if it feels suspicious (against 6% of the general public, the consumers). Similar findings are reported by the ECB in 2007: the most common security feature checked is tactility for 70% of the cashiers [100]. In 1996 the Central Bank of Ireland reported that 70% of the super market check out staff said that it was the feel of the note that 'first alerted them to the fact that something was wrong.' In 1986 research by the Bank of England showed that experienced cashiers were not able to distinguish real and counterfeited notes just by the feel of the paper [49].

Since we have lost the information on the pay out, the next moment when we store the banknote in our wallet, might be the one triggering us to do a security check. Again, only if our brains are instructed to do such a security check; the watermark and the hologram will enhance their signals only if we look for public security features. This bias towards what we seek occurs at every processing stage. For that matter it is useful for central banks to inform the retailers and the public when the number of counterfeits of a certain denomination exceeds a trash hold value (inform on denominations and two or three valid security features; do not report on any figures!).

Figure 50

Which is the correct USD banknote?



People do not recall which is the correct one dollar banknote. The one on the left or the one on the right? Test your self!

Figure 51

Dark background behind portrait

Light background behind portrait

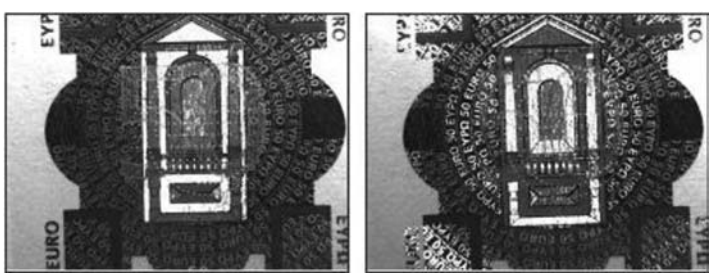
Change blindness illustrated by US dollar 20 banknote. When the above images are shown on a screen most people will not notice the switch in the background to Jackson from dark to light (author and date unknown, around 2007).

4.3.1.5 *Change blindness*

The banknotes shown in Figure 50 are dissimilar, just as in the example of the two euro 10 banknotes in Figure 39. The fact that the portrait on the right-hand side mirrors the one on the left hand side escapes most people's notice. Most people are not confident about the real note (Washington looking to the right is correct) [125]. Such manipulated banknotes designs remind to the phenomenon of *change blindness*.

A real example of the phenomenon of change blindness cannot be provided in a static report like this study. The two images of Figure 51 are used in an animation movie which every 0.5 second shows a switch from one image to the other. In between is a very short dark grey interval (< 0.1 s). Most people fail to notice that the background behind the portrait changes from dark to light.

Figure 52



A switch from dark to light within the renaissance window is seen when the hologram on the euro 50 banknote is tilted [63, 70].

Figure 53

a) Instruction leaflet South Africa (2005)

b) Information tool ECB (2007)

c) Instruction leaflet Hong Kong (1995)

Explaining security features by marking them in the information leaflet. Why not do so on the banknote proper?
a) Image of ZAR 20 as represented in leaflet of the South African Reserve Bank (around 2005).
b) Information tool on credit card size by ECB using numbers to indicate the public security features (2007).
c) Image of HKD 1,000 as represented in leaflet of the Hong Kong Monetary Authority (around 1995).

Holograms

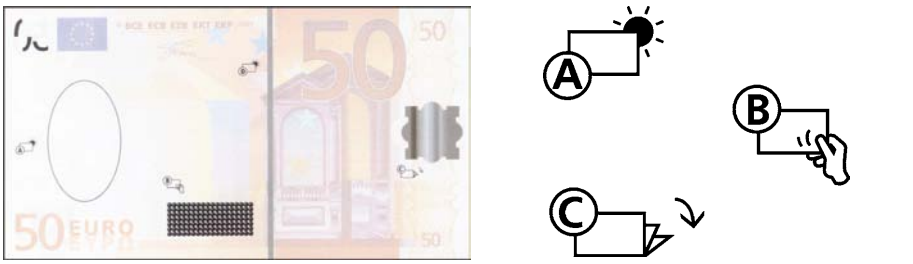
Tilting the euro 50 hologram will also be hindered by a variant of change blindness (Figure 52). The perception of the changing areas is obsructed by the complexity of the design: several areas are active having similar shapes. So-called *achromatic holograms* switch from light to dark and will experience similar perception problems. Introducing movement in security features is also introducing different brain activities. Movement is processed by the ventral route, while static features are processed by the dorsal route. The message: think twice before introducing a movement in banknote security features. See also the example of the 'rolling bar' in Appendix 9.

4.3.1.6 *Eye movement planning*

Banknote design could be explored further using the information leaflets accompanying the issue of a new banknote. Often, numbers or letters are used to identify the security features on such instruction manuals (see Figure 53).

Studying such public instruction leaflets brought De Heij in 2001 to the idea of printing wayfinding icons to mark public security features. Since banknotes are

Figure 54



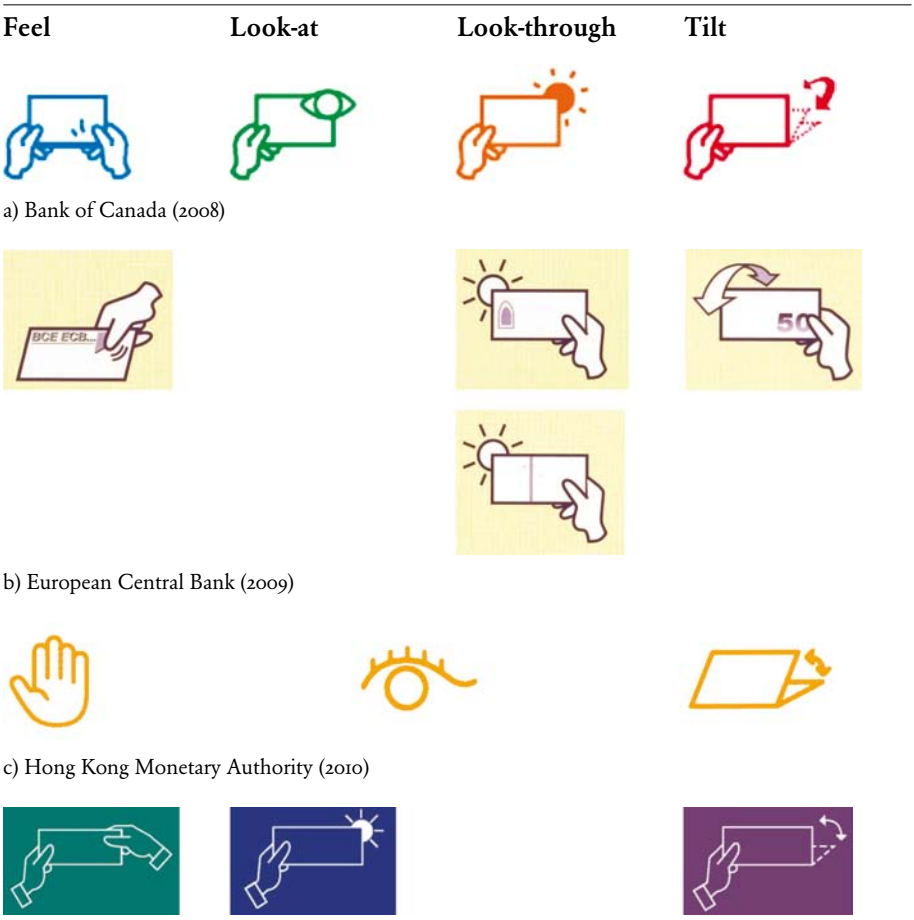
Dummy note with wayfinding features used for testing comprehension (self-explaining and searching). DNB, 2003. On the right three of the original symbols with letters as designed by Paul Mijksenaar and tested by Delft University of Technology. The project was an ECB R&D-project, proposed and managed by DNB [81, 84].

printed matter, just as information leaflets, why not print the symbols directly on the banknote? Apart from alphanumeric information, instructional icons indicate whether a feature should be checked by feeling, looking or tilting. Figure 54 presents an example, a dummy note prepared in 2003.

The wayfinding icons became quite popular as a communication tool. After DNB had used them on its CD-ROM "Genuine or counterfeit" in 2002, others adopted them, like the European Central Bank (2003) and the central banks of South Korea (2006), Chili (2006) and Mexico (2007). It is likely that standardization helps comprehension, just as the symbols used by Microsoft for the Word-programme are world wide similar. Other examples are road signs, most of them being similar in all countries of the world. However, the symbols used look like each other, but are all modified as first reported in 2007 [94]. Bank of Canada developed in 2008 their variant as shown in Figure 55a.
Modifying the original symbols is despite the copyright aspects a remarkable policy, since, unlike the proposed symbols, the altered symbols are (probably) not tested for their comprehensibility [84]. Even more remarkable are the icons introduced in 2009 by the ECB. The original 2003 symbols were redesigned and introduced also hands in the symbol (Figure 55b). In 2010 the Hong Kong Monetary Authority also introduced its own variant of communication symbols, based on the motto 'Viewing, tilting and touching' (Figure 55c). The Bank of Russia stayed quite close to the original design, but also introduced an additional hand (Figure 55d).

Pubic security features indicated by a letter
Whereas wayfinding icons are used in communication tools around the world, the idea of printing them on banknotes has met with resistance, despite proof that this would increase the average number of public security features recognized from

Figure 55



Overview of communication symbols used by central banks, introduced over the years 2008-2010.
a) Communication symbols introduced by the Bank of Canada in early 2008. The design is based on the wayfinding icons developed by DNB in 2003. An additional colour is introduced for each function. Also, each symbol shows a hand. The motto is TiLL: Touch, Tilt, Look through and Look at.
b) Redesigned communication symbols by ECB, 2009. From left to right: feel, look-through (security thread), look-through (watermark) and tilt (notice the thumb on the numeral to be checked!).
c) Communication symbols by Hong Kong Authority. The motto is: Viewing, tilting, touching. For viewing one symbol is used instead of separate symbols for look-at and look-through.
d) Communication symbols by Central Bank of Russia.

around 2 to 4.7 [94]. However, in 2007 alternative design solutions were developed. In the design shown in Figure 45, all five public security features are easy to find by following the letters A-R-U-B-A. Adding icons by way of letters is one of the design parameters of a public security feature and were first used on the Swiss banknote

Figure 56

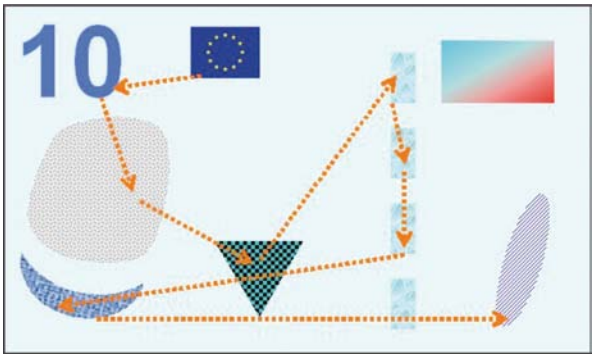
Example of eye-tracking registration on a euro 50 banknote (computer screen-averages). The image was made by reflection and offered on a screen and did not figure a watermark and the foil was a fixed image. Study by ECB [172].

series, introduced in 1994. These letters A, B, C, D, E, F and G are very small though and their function was more the one of a co-ordinate [49, 94].

Eye-tracking registration of existing banknotes

Central banks may verify the prototypical design elements of one of their banknotes by eye-tracking registration. Such a registration will indicate the elements registered by the human eye. Figure 56 is an example of a euro 50 banknote prepared by the ECB. Reading this image it is clear that the words EURO and ΕΥΡΩ and the silver foil patch are attracting the eye. Also the flag and the signature receive attention. For a moment the human eye rests at the centre of the first arch.

Figure 57



Example of eye movement planning (follow me) for 6 public security features on a banknote. The feature in the top right corner is ignored, meaning that the designer needs to improve the eye tracking path.

Figure 58

a) NLG 10/Minerva (1930)

b) NLG 10/Syndic (1943)

Two banknote designs guiding the eye to the watermark area.
a) NLG 50/Minerva, a banknote design of Jacob Jongert. Supported by concentric line patterns, the banknote recipient's eyes are drawn to the white watermark area!
b) NLG 10/Syndic, a banknote design of W. de Jonge. The watermark area is in the zero of the 10, a unique combination of value and security design!

Follow me!

Instead of determining the eye-tracking path once the banknote is issued, *eye movement planning* could be part of the design process for a new banknote! This would indeed be an example of evidence-based design which in fact would be priming, just as the letters A-R-U-B-A. Instead of sketching a banknote out of the blue, a banknote designer might start by distributing the public security features across the note. In other words, the designer starts by designing an *eye tracking path*. An eye tracking path should work as a *follow me* instruction (see Figure 57). Eye tracking paths are dependent on the instruction given, e.g. *check three public security features* or *follow the fish* (Figure 61).

Once the eye tracking path is designed, the features may be worked out in further detail. During the design phase, the eye tracking path must regularly be subjected to verification for compliance with the original plan. Eye tracking instruments are nowadays made widely available by universities, institutes or commercial parties.

Although there were no such instruments in the 1930s, one's eyes are guided to the white watermark area in the design NLG 50/Minerva by Jacob Jongert (Figure 58a). A unique concept is also the design NLG 10/Syndic (Figure 58b), combining value and security design!

4.3.2 **Banknote series concept**

The design phase requires one more action by the central bank before it can kick off. The selected features are in need of a *strategic communication policy*. The bank should find an answer to the following question: how to garner public interest

in selected public security features? The first part of the answer is that the public features should match the user requirements. These user requirements should be complemented with a strategic communication policy. In 2007, DNB reported on such a strategic communication policy for public security features commissioned by Bureau 180 [94]. Different policies were offered:

4.3.2.1 Retrieval path,
4.3.2.2 Tell a little story,
4.3.2.3 Give people a task,
4.3.2.4 Name and motto.

These policies may also be (partly) combined with each other and may come together in:

4.3.2.5 Design policy on a new banknote series.

4.3.2.1 *Retrieval path*

The retrieval path strategy is explained in the DNB Occasional Study 'Public feedback for better banknote design 2' [94]. People will remember e.g. a walking route by 'turn left at the red mail box'. This principle is used in the A-R-U-B-A banknote (Figure 45). If people are invited to find all features by completing a word, this effort, if completed, will work as a memory aid. Using this principle other

Figure 59

Conceptual banknote EUROPA with 6 public features E, U, R, O, P and A.
Concept design by De Heij.
In the case of the euro, two more variants have been generated:
1) the currency code: E-U-R (three (active) features on the front),
2) the currency name: E-U-R-O (four features on the front).

designs can be made as well, like a conceptual design for a new euro banknote as done in Figure 59 using the word E-U-R-O-P-A. The philosophy behind these concepts is that of the homo ludens (the playing man), which is reflected by the search for a meaningful word (e.g. a motto) and, subsequently, for the public security features near each letter of that word. The homo ludens aspect provides the emotional aspect necessary to pass what is stored in the visual working memory on to the long-term memory.

E - U - R - O - P - A

In the case of euro banknotes, the word Europa provides 6 letters, matching perfectly with the requisite 6 public features. The Latin letters will also be understood by other cultures, just as the gate letters at airports. At international tournaments, Greek football players have their names spelled in Latin characters. In Russia, the plate numbers on cars are in Latin, not in Cyrillic

The letters E-U-R-O-P-A feature distinctly on the banknote, providing an easy reference to the six public security features.

Primacy and recency effect

When we see a banknote design for the very first time this information will be most probably stored in our memory. This is known as the *primacy effect*. We recall, for example, the first time we held a euro banknote in our hands (on 1 January 2002), just as we probable also recall our latest withdrawal of 200 euro with a view to the Easter holidays. This is known as the *recency effect*. Given a list of items to remember, we will tend to remember the last few things more than those things in the middle. Hermann Ebbinghaus was the first psychologist who described these effects as part of the 'forgetting curve'. He was also the first to describe the 'learning curve'[1].

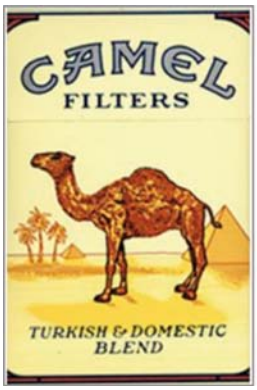
So if we see the E-U-R-O-P-A banknote for the first time, we might store this stepping stone, using the letters to find the security features, in our long term memory. Primacy and recency effects are no guarantee for storing banknote information in our long term memory, but statistically they are more often recalled. We also tend to assume that items at the end of the list are of greater significance [87].

'Pars Pro Toto' effect

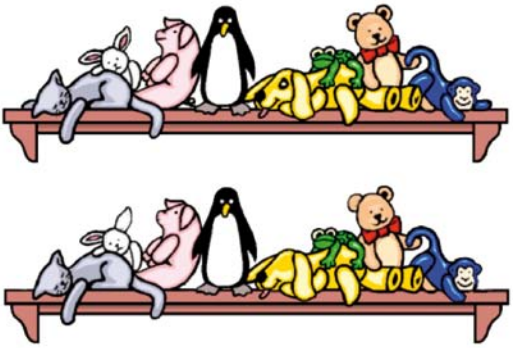
Besides providing an optimal retrieval path function, tracing letters, like E-U-R-O-P-A, also reminds of hunters reading the traces of animals. A few prints of a trail suffice to evoke an image of the animal, including its size, the time when it passed and the chance of catching it. The visual information evokes a situation or a special optical, haptical or acoustical effect. Processing such complex information structures in the cortex without having full detail information is known as the Pars-Pro-Toto function (PPT). The PPT function fuses brain information which is already stored on the basis of previous experiences [78, 157].

Figure 60

a) Hidden image in package



b) Find the difference between the two images



a) Statue of Manneken-Pis might be perceived in the package of Camel cigarettes (in the front leg of the camel).
b) Example of searching the difference between two images.

Search for hidden images

In general people like to search for hidden images and this quality might be exploited in future banknote design. Figure 60 shows two examples. Within the camel shown on a Camel cigarette package one may discover the Brussels statue of Manneken-Pis (little man urinating). Famous are the *Where's Wally?* series created by Martin Handford. The books consist of a series of detailed double-page spread illustrations depicting dozens or more people doing a variety of amusing things at a given location. Readers are challenged to find a character named Wally hidden in the group. Wally's distinctive red-and-white striped shirt, bobble hat, and glasses make him slightly easier to recognize, but many illustrations contain 'red herrings' involving deceptive use of red-and-white striped objects. Within a new banknote series a Wally like character could be hidden – in each denomination on a different spot – serving as a first step to gain interest in the public security features!
Also find-the-hidden-subject puzzles provide fun to both children and adults, just as searching for the differences between two images (Figure 60b).

4.3.2.2 *Tell a story*

The second strategic communication policy is a short story. In several of his publications, De Heij argued in favour of a short story as found on the Dutch guilder notes. Another example is the former 50 franc banknote from France, which tells the story of the Little Prince [44, 81, 94].

Table 28

Florin	Watermark	See through (offset)	Relief print (intaglio)	Colour crypt (silk screen)	Colour shifting wide thread
	A	R	U	B	A
10	Portrait of indian	Turtle	Dolphin	Shell	6 continuous silhouttes: fish, flower, bird, tree, persons head, carnival element
20		Donkey	Rattle Snake	Iguana	
50		Pelican	Owl	Butterfly	
100		Palm tree	Divi Divi (tree)	Cactus, Aloe	
200		William III tower	Bird painting from cave	Old coin	
500		Carnival feather	Group of people in carnival-like clothing	Masque	

Example of a design and communication proposal for 5 public security features. Each public feature is identified with a small letter symbol, reading from left to right: ARUBA. Because of the low volume, the watermark and the colour shifting thread are the same for all denominations.

The five features on the conceptual Aruban banknote also tell a story about the island, a different one per denomination (Table 28). The 10 Florin tells about the animals in the sea, while the theme of the 20 Florin note is 'animals on land'. Animals in the air are found on the 50 Florin note, and the 100 Florin note provides information about the flora typical of the island. Old and new architectural elements are used on the 200 Florin note, and carnival (people!) is reserved as theme for the highest denomination.

4.3.2.3 *Give people a task*

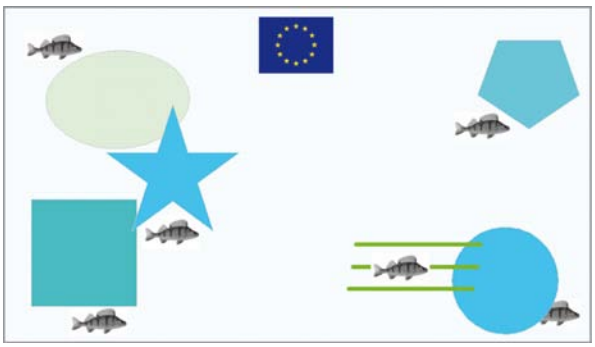
A third communication strategy is to give people a task. This is also applied in the Aruban and Europa concept, by which people are asked to look for respectively all letters from the word Aruba and Europa. Other examples are 'Look for the colour', 'All features in a row' as proposed by DNB in 2007, or 'Look for Yvonne', i.e. the motto of a promotional banknote issued in 2007 by Papierfabrik Louisenthal. Either a portrait or the text Yvonne appears in all public security features. One of the suggestions for the euro in this context is: 'Look under the bridge' [94]. A recent example based on an instruction – follow the fish – is provided in Figure 61.

4.3.2.4 *Name and motto*

When a banknote receives a name, e.g. Snipe or Mona Lisa, people will grow attached to it. This phenomenon has been explained for banknotes in several earlier

Figure 61

Motto 'follow the fish'



A small fish icon can be found close to each public security feature. The features could be designed from using themes like water, water plants, boat or fisher man. Another denomination could have 'follow the bee' or 'follow the helicopter' for a theme. Design by De Heij, made in 2010 [173, 177].

DNB publications [44, 49, 94]. The need to combine visual and verbal information will train the working memory and increase the chance of storage of the public security features in the long-term memory. Added value is created if the banknote name is part of a motto or theme, e.g. Freedom, Big Five (South Africa) or Europa. The search for a communication strategy and, consequently, a suitable motto and theme, can be outsourced by the central bank, as was done by DNB in 2006 [94].

Non-technical terms for public features
The communication strategy would be further enhanced if all public security features also had a name, as already experienced by the central bank of Switzerland and the ECB. In 1994, the Swiss introduced non-technical terms for their features, e.g. *chameleon number*, instead of optically variable ink. The euro has no such names yet, but the ECB intends to change this (see Chapter 4) [99].

4.3.2.5 *Design policy on a new banknote series*

Several communication aspects of a new banknote design are discussed and the next step is to apply it to a new banknote series design. Before commissioning any individual denomination designs, the central bank should commission a series or generic design.

Town planning and architecture
The creation of generic design for a new banknote series may be compared with town planning (the banknote series) and architecture (the individual notes). Analogously with urban development, it is not necessary to design all denominations (or house

Figure 62

Banknote series as proposed by Jan van Toorn for 6 new NLG denominations (10, 25, 50,100, 250 and 1,000). DNB asked the designers in the 1986 contest to design banknotes for just 3 denominations: a low (25), middle (100) and high denomination (1,000).

numbers) of the new banknote series [30]. In the case of the euro series design contest in 1996, the designers were asked to deliver 7 denominations, including front and reverse, watermark design and some other details, in seven months' time [59]. Such a quantitative design exercise is not necessary. People will also understand the generic principles if they see no more than 3 designs: a low, middle and high denomination. This approach, which allows designers more time and energy for the quality of the series design, was adopted by DNB for its 1986 design contest for a new series of guilder banknotes [43] (see Figure 62, for the entry by Jan van Toorn).

No split in banknote series

One of the first policy issues to be solved by the central bank is to decide on public recognition of the security features. For example, should there be a so-called *split* in the banknote series?

The euro banknotes have a split between low (euro 5, 10 and 20) and high denominations (euro 50, 100, 200 and 500), each subset having partly different security features. The use of different public features for low and high denominations renders communication about the banknotes more complicated. In 2004, ECB research reported that close to 70% of the cash handlers were unaware there were two groups of euro banknotes: the low and the high denominations, bearing different security features [60]. Research by DNB in 2007 arrived at a similar conclusion: 'The distinction between low and high euro denominations is not effective as it leaves both public and retailers confused about the security features, besides making the public information tools too complex.' [81].

A split is not appreciated and it would therefore seem advisable to apply the same security features throughout the series.

Table 29

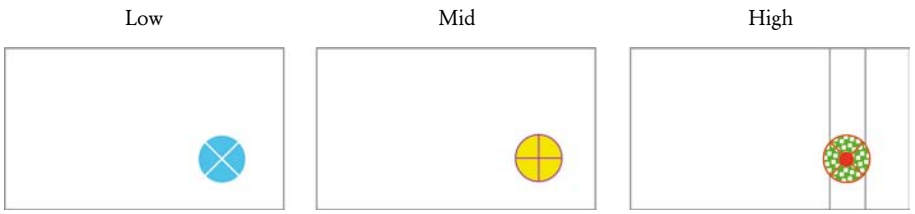
Model	Generic design principe	Description	Example
A.	All features exactly the same	Same main image, often a portrait, same watermarks, etcetera.	UK, Turkey, Brazil, Pakistan, Surinam, Ghana
B.	Small differences between features	Different main image within a fixed lay-out, like similar dimensions. Or similar watermarks but other elements slightly different, e.g. using the numerals.	US dollar, euro, Japanese Yen, Danish bridge series
C.	Maximum difference between features	Different banknote themes (e.g. human, fauna, flora, architecture). Public features within theme of the note.	Cabo Verde, Latvia, former guilder notes

Three different models for public security features.

All public features on the front?
Keeping all public security features on one side, the front, will save operating time, since the note need not be turned and more time can be spent on checking the features (instead of finding them). See also Appendix 6.
Location of the security features was found by the Dutch public to have the highest relative importance. This was the outcome of a so called *conjoint analysis* done by TNS NIPO in order of DNB in 2009 [133]. The number of security features was ranked second and the appearance of the security features was considered less important. The conjoint analysis and their results are reported in Appendix 10.
For communication purposes, all public features should be on the front of the banknote, making a communication concept even stronger.

All features the same?
People are guided more by design than by technology. This conclusion is corroborated by the fact that the letters A-R-U-B-A are followed more easily by the public than the security feature to which each letter refers. Each denomination within a series could be of a different design, having a distinguishing watermark, paper tint and foil element. Different scenarios are conceivable, as shown in Table 29. It is not known whether research efforts are underway to identify an optimum model. However, people tend to believe that use of the same foil on different denominations facilitates fraud [63].

Figure 63



Design of three public security features in respectively a low, mid and high denomination. The design of the features is similar, while the techniques used may differ.

Similar designs, different techniques

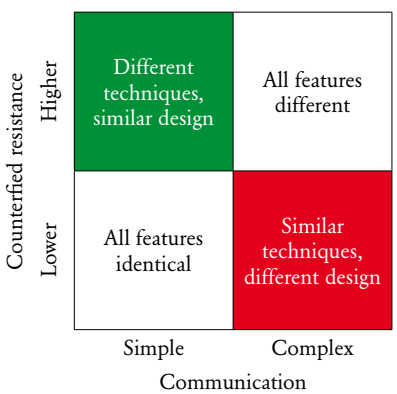
Once the generic principle for the design of the public security features is established, the technique will follow. Figure 63 provides an example. People will accept that public features are based on different technical security principles as long as throughout the series they:

- Are located on the same spot,
- Are similar in shape,
- Require the same human checking action (feel, look-at, look-through, tilt).

Communication versus counterfeits

The above arguments make a strong case for favouring the upper left quadrant in Figure 64 [112, 170]. So, features in banknotes could be based on different techniques,

Figure 64

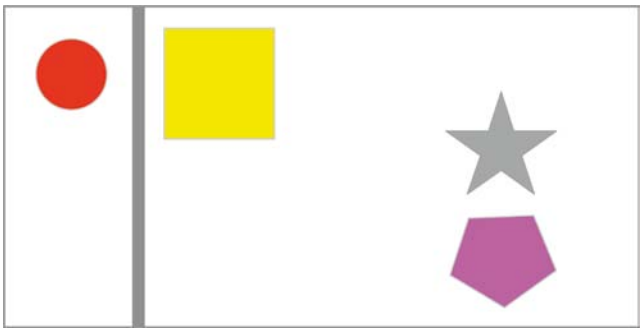


There is a trade-off between the communicativeness of the pubic security features and counterfeit resistance. The best option is to use similar designs, although the techniques used might differ.

Figure 65

Look-through area 3 features:
see-through, thread, watermark

Tilt area 2 features:
hologram, colour change



Look-at and tilt features clustered. The position of the features is chosen so as not to interfere with hands holding the banknote (the look-through area along the long edge and the tilt area towards the centre of the note). Concept by De Heij (2010).

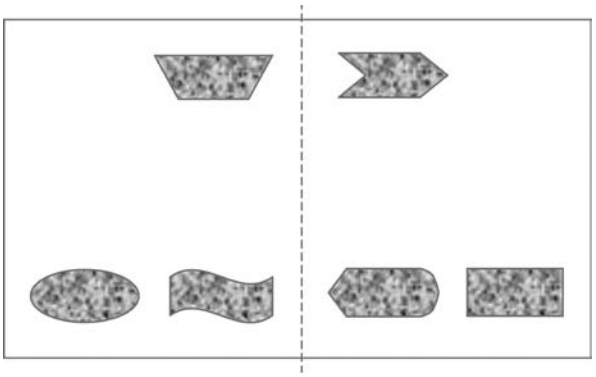
while the designs remain similar! Security features on each denomination should be different, but clearly be part of one family. This public preference emerged from a 2004 survey of the public's appreciation of foils. The main reasons mentioned by the respondents were 'learning' and 'recognition' [63].

Similar designs use similar generic principles, but do not imply restricted designs. The graphic designer will retain the freedom to propose – and is even advised to do so – images from different categories (see Table 29 and Figure 64). Research is needed to make this more certain.

Cluster all features by the human action required (feel, look, tilt)
Public features requiring similar human checking action could be clustered in the new banknote design. This will reduce operating time. All look-through features may be checked at a glance, if grouped together (see Figure 65). The same holds for all tilt features. By the same argument, a transparent window in a banknote could be combined with a see-through feature, as suggested in 2007 [94].
A drawback of this approach may be that one public feature dominates the other features. Grouping the features together might in such a case be suboptimal, as the public may only have eyes for the dominant feature.

Security features in colour of the note
There is some evidence that the public appreciates security features matching the colour of the note. A colour concept like 'Look for the colour' was first proposed in 2007 [94].

Figure 66



Conceptual banknote using:
1) Similar size (30 mm x 15 mm) for all public features.
2) Planned distribution of the public security features over the banknote (preset lay-out).
Concept by De Heij (2010).

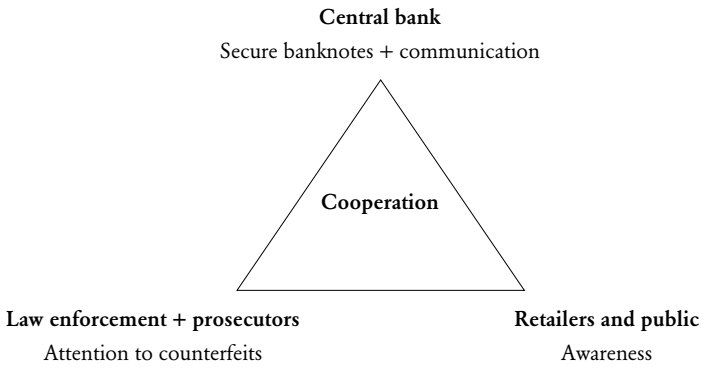
From a counterfeiter's point of view, new features that are limited in colour range are weaker than features offering more colour options. Once the paper tint or the colour-flop imitation is identified by the counterfeiter, banknotes using these features become easier to reproduce, both within the series as internationally.

Security features same size
The size of a public security feature is discussed in Section 4.1.7.2 on easy to find. The proposed dimension is 30 mm x 15 mm. This is input for another conceptual banknote, where all public security features receive similar dimensions (Figure 66).

Individual notes
Just as an architect has freedom within a town planning concept, the graphic designer may fill in the details of the denominations differently. The individual banknote designs should follow the master plan, i.e. the series concept. Denomination design would be more interesting if each note had its own characteristics – including some surprising elements – rather than a design based on the generic principles. It is even thinkable to ask 7 different graphic designers – if 7 denominations are involved, as in the case of the euro series – to work out the master plan. A proper generic design will be so powerful that all denominations will be both part of a series and stand out as an individual note!

Other communication aspects
So far we have discussed the communication by the banknote proper and their design applications. Besides the banknote, the communication on banknotes

Figure 67



For counterfeit deterrence to be effective, maximum cooperation is required. Close collaboration is the best guarantee that the central bank provides secure banknotes and adequate communication, making retailers and consumers aware of the security features and of law enforcement against counterfeiters.

should include information tools like instruction leaflet, banners and internet information including, e.g. animations, which are outside the scope of this study.

Communication regarding counterfeit deterrence should also be seen from a wider perspective (see Figure 67). It is DNB's policy to consider its tasks regarding counterfeit deterrence within the context of cooperation between the three following parties [e.g. 147]:

1) Central bank (producing banknotes with adequate security features),
2) Retailers and public consumer organisations (keeping the retail sector and public at large properly informed),
3) Law enforcement and prosecutors (supporting repressive measures on the part of legal, judiciary and police authorities against counterfeiters).

5 Central bank

When it comes to the selection of security features the central bank is a stakeholder, too. Not only because of the machine-readable security features used in the sorting machines of the central bank (level 4 in Table 3), but also for the purchase price to be paid for new banknotes.
The monetary income on banknotes is high and easily earned. Although constraints on costs for a new banknote design may not form an impediment, security features still have different price levels. Some features are more expensive than others and may take up to 15% of the banknote's price. Other features, such as the majority of the paper-based features (watermark, thread), are less expensive.

Clearly, the price of the notes is dictated by the number and cost of the security features. Central banks have to purchase the newly designed banknotes from a security printer and are reluctant to mention the cost of banknotes. Some central banks are open about the purchase price of their banknotes, like the Swiss National Bank [178], and since the 1990s some more price levels have been unveiled. In 2007 the Central Bank of Columbia published a paper on banknote production costs, including a review of the price per banknote in different countries [104]. The price of a banknote is clear when it is offered by a commercial banknote printer, but central banks may have their own 'in-house' printing works, as is the case in the United States. The Federal Reserve Banks obtain the notes from the BEP for the cost of producing the notes, which is believed to be about four dollarcent a note [180]. Within the euro area there are several in-house printing works like Banca d'Italia and Banque de France and also several central banks ordering their notes on the free market like the Bundesbank and JET. JET stands for 'Joint European Tender,' a group of several European central banks that joined forces in 2009 and purchase their euro banknotes as a group. In 2011 the JET-group represents the following countries: Estonia, Cyprus, Finland, Luxemburg, Malta, the Netherlands, Slovakia and Slovenia. The JET is an initiative of DNB.
The average price of a euro banknote is hard to tell because of this mixed situation of in-house printers and commercial banknote prices (the proportion is about 60/40; 40% of the volume is produced by commercial printers and 60% by state-owned printers). Prices vary for the different denominations. However, the average production cost of euro banknotes is believed to be about 0.07 euro [e.g. 122, 123].

Table 30

Currency	Country/area	Average price	Year	In EURO (2010)	Reference
CHF	Switzerland	CHF 0.30	1995	EUR 0.23	178
YEN	Japan	USD 0.166	2005	EUR 0.22	103
EUR	Euro area	EUR 0.07	2005	EUR 0.07	121, 122
GBP	United Kingdom	GBP 0.03275	2005	EUR 0.05	179
USD	United States	USD 0.04	2010	EUR 0.03	180
THB	Thailand	USD 0.023	2005	EUR 0.03	103

Overview of the average production cost of a single banknote in different countries/areas.
Exchange rate: EUR 1 = USD 1.30.

Price information on banknotes is shown in Table 30. Prices vary from about 3 eurocent (Thailand) to about 23 eurocent (Switzerland). We have to be cautious in drawing conclusions based on this information, of course; the exercise is meant as a first step at gaining insight into the cost of new security features.

Relative costs
If we want to know the cost of a security feature, the average price of a banknote does not tell us much. To find out the cost of a single feature we need to establish the costs of the separate production steps and the number of features contributed. These relative costs of the different production steps of a banknote are unveiled by at least two security printers – Giesecke and DeVrient in 2002 and Crane Currency in 2009 – and are listed in the first column of Table 31. The third column in this Table provides an overview of the number of security features in a 50 euro banknote produced using different production techniques. The generic security matrix as proposed in Table 3 has been included in Table 31 by introducing a third column with 20 features. As the 50 euro denomination is the middle of the euro banknote series, we assume that the cost of this banknote is about 7 eurocent.

It seems that in the case of euro banknotes, offset contributes most security features (13). The average price of such an offset feature would be about 1% of the total price of a euro banknote (or about 0.07 eurocent). However, a new future banknote would only have 5 security features produced by an offset press, bringing the average cost of an offset feature in that case to 2.5% of the total price of a future banknote. A Simultan press is discussed in Appendix 5, an offset press with separate units may print better and cheaper than the traditional offset press used for banknotes.

Table 31

Production step Banknote	Relative cost per production step	Cost in eurocent per production step 50 euro	Total number of features in euro (according to DNB)	Cost in eurocent per feature 50 euro	Total number of features future	Cost in eurocent per feature future
1. Paper	15 - 20%	1.1	10	0.11	4	0.27
2. Foil stripe (10 mm)	15 - 20%	1.1	2	0.55	3	0.37
3. Print - offset	10 - 15%	0.9	13	0.07	5	0.18
4. Print - intaglio	10 - 15%	0.9	7	0.13	4	0.23
5. Numbering	5 - 10%	0.6	3	0.2	2	0.30
6. Silk screen (OVI)	15%	1.0	1	1.0	1	1.0
7. Finishing	15%	1.0	1	1.0	1	1.0
8. Quality control	5 - 10%	0.5	-	-	-	-
Total	90 - 120%	7	37	av. 0.19	20	av. 0.35
6. Iridescent band	3 - 5%	0.3	1	0.3	-	0.3

Overview of the relative cost of the different production steps of a banknote and the number of security features used in the euro note and in an alternative, future banknote. Based on information from Giesecke and DeVrient (2002) [50] and Crane Currency (2009) [135]. Quality control costs are based on a recent estimation made by the participants of the DNB Cash Seminar 2010.

Cost of security feature: maximum 5% of banknote price

If the suggested 20 security features are used in the note (see Chapter 2), the average costs of a single feature is 5% (or 0.35 eurocent). This would give a lead to threshold settings for the costs of a security feature. If the cost of a feature is less than 5% of the total cost of the note it is acceptable and it gets the go-ahead. If the cost of a feature exceeds 10% (or 0.7 eurocent) of the total cost of the banknote, the feature is considered too expensive (red). In this theoretical exercise the production phase of silk screen is regarded as too high (1.0 eurocent) and will receive a red flag.

We close the issue of cost price calculations now we have found a cost criterion for the selection of new security features. It is beyond the scope of this study to report on the cost structure of banknotes.

Criterion

Green: Cost of a security feature < 5% of total cost of the banknote.
Red : Cost of a security feature > 10% of total cost of the banknote.

6 Counterfeiter

New banknote designs are often triggered by the quality of the counterfeits received by the central bank. Fake banknotes are made by counterfeiters and as such they are competitors of central banks. Unlike retailers and the general public, counterfeiters are therefore seen as 'negative stakeholders' of a new banknote design. This chapter addresses the counterfeiter and is subdivided in three sections:

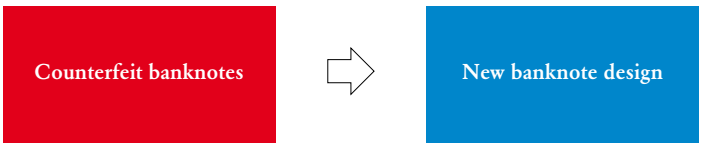
6.1 Counterfeit analyses,
6.2 Methods to analyse counterfeited banknotes,
6.3 Design principles to prevent counterfeiting.

Public interest for counterfeiters
There is and always has been (a romantic) public interest in the persons behind counterfeits. A popular book is the 'The Man who Stole Portugal', written by Murray Teigh Bloom and published in 1966 [4]. Two more publications by Bloom also deal with banknotes and counterfeiting [11, 12]. Two recent examples are the film 'The Counterfeiters' (*Die Fälscher*) released in 2007 and the book 'The Art of Making Money', published in 2009 [141]. 'The Counterfeiters' is about Operation Bernard and this Austrian movie directed by Stefan Ruzowitzky won an Oscar. 'The Art of Making Money' is written by Jason Kersten and describes the life of a US counterfeiter. It gives an emotionally compelling look at the relationships between crime and family, and the destructiveness of greed.

6.1 **Counterfeit analyses**

Analyses of security features should start with the counterfeits that are daily intercepted at the central bank. Counterfeits taken out of circulation should be studied and form input for the design of future banknotes. Such analyses yield information on the banknote to be replaced in terms of both the imitated security features and the reproduction technologies used by the counterfeiter. Being the only party in the banknote chain receiving all counterfeits accepted in circulation, central banks (or in some countries the police or judicial authorities) should analyse these notes closely. Such input is necessary to decide on new security features (Figure 68).

Figure 68

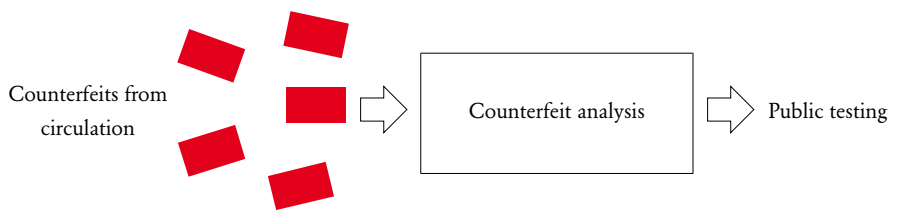


New banknote designs should also be based on an analysis of counterfeit banknotes.

National Analysis Centres (NAC) and Counterfeit Analysis Centre (CAC)
Each member state of the European Union has a centre for the initial analysis of counterfeit euro banknotes at national level, the National Analysis Centre (NAC). The NAC for the Netherlands is housed inside DNB. All NACs report to the Counterfeit Analysis Centre (CAC) at the ECB, which was established in 2002. The ECB Annual Report 2003 states '… the CAC co-ordinates the incorporation of statistical and technical information on euro banknote counterfeits from the National Analysis Centres across the entire EU into a comprehensive database at the ECB.' The focus of the CAC is on classification of counterfeits and its statistics. Input for new euro banknote designs as provided in Figure 69 seems to be of lesser importance. The focus of counterfeit reports is often on statistical data and counterfeits seized, illustrated with anecdotic information, usually about the organisation of the criminals [156]. Studies on counterfeits should be more analytical from the perspective of:

- The reproduction equipment's characteristics, like resolution, colour, density, geometry, mass and material,
- Counterfeiters, such as production time, skills and investment costs involved.

Figure 69



The security features in counterfeits detected in banknote circulation are analysed on frequency and (counterfeit) quality.

Counterfeiters
Banknote counterfeiters reproduce banknotes with the intention to use them for real. The first Dutch counterfeiter was active in 1836 and reproduced the note by hand [e.g. 55]. To date they come in several categories, since the reproduction technology available to counterfeiters is becoming increasingly advanced and cheaper over time, creating new types of counterfeiters. To this end, the NRC [102] and the Bank of Canada [107] work with the following categories of banknote counterfeiters:

1) The primitive or unprofessional kind (fantasy notes and euro notes made with off-the-shelf equipment at home or push-the-button devices like a colour copier),
2) The casual kind, hobbyist, opportunist or petty criminal (using digital publishing tools like PC, scanner, printer, editing software and other desk top publishing equipment),
3) The professional kind (using special equipment, special materials, organised crime),
4) The state-sponsored or sophisticated kind (with access to banknote production techniques).

The ECB uses a similar classification system (unprofessional, semi-professional, professional and sophisticated). An overview is provided in Table 32.

State-sponsored counterfeiters
The US and Canada recognise the category of state-sponsored counterfeiters. State-sponsored counterfeiting happens only occasionally, usually to destabilize hostile

Table 32

Institute	National Research Council USA	Bank of Canada	European Central Bank
Currency symbol	USD	CAD	EUR
Year	2007	2008	2007
Category of counterfeits	1. Primitive 2. Opportunist 3. Petty criminal 4. Professional criminal 5. State-sponsored	1. Primitive 2. Hobbyist 3. Professional 4. State-sponsored	1. Unprofessional 2. Semi-professional 3. Professional 4. Sophisticated

Overview of categories of counterfeiters.

economies. During the Revolutionary War (1775 - 1783), the British Government tried to destabilise the Continental Government by counterfeiting US currency. In 1942, the Germans tried to do the same to the British. Inmates were required to counterfeit the 5, 10, 20 and 50 British pound banknotes, called *Operation Bernhard* (see the movie 'The Counterfeiter' mentioned in the introduction of this Chapter). A recent example is the *Super Dollar*. These dollar notes are believed to be printed by a real banknote printing works outside the USA and have been found to circulate since 1989. The US Government suspects the involvement of the North Korean government [e.g. 102].

Emulation and simulation
A distinction is made between a feature reproduction made by *emulation* and one made by *simulation*, as proposed by the ECB. If an original security feature can be reproduced close to the original by commercially available techniques, this is called emulation, a variant of reverse engineering. If a reproduction is made using materials that are basically unsuitable for recreating the original, this is called simulation.

6.2 Methods to analyse counterfeited banknotes

To facilitate the selection process of security features for new banknotes, a method is required. Different selection methods lead to different preferred features; if selection models were accurate, they should converge. Most methods proposed use input from banknote experts to come to a judgement on 'poor-neutral-good', which is subjective. That is why these methods are not mature (yet), meaning more work to do to come up with a better way of evaluation. Tests on counterfeit resistance should be reproducible by third parties and report on the skills, investment and time involved. This section is an overview of the methods available, starting with an overview of the models developed by DNB:

6.2.1 Models developed or used by DNB,
6.2.2 Other models.

6.2.1 Models developed or used by DNB

Since the first banknotes issued in 1814, DNB has based its banknote security on a model. Since the mid-1970s four models have been developed to analyse counterfeited banknotes and/or select security features:

6.2.1.1 Unique original (DNB, 1814),
6.2.1.2 Portrait feature (DNB, 1921),
6.2.1.3 Intrinsic and extrinsic security features (DNB, 1976),
6.2.1.4 Internal and add-on security features (DNB, 1985),
6.2.1.5 System approach (DNB, 1991),

6.2.1.6 Simple model (DNB, 2006).

Public testing of counterfeits was first done by DNB in 2006:

6.2.1.7 Public testing (DNB, 2006).

This section concludes with a description of the latest model and the subject of this study:

6.2.1.8 All-in-one model (DNB, 2010).

6.2.1.1 *Unique original (DNB, 1814)*

In 1814 DNB issued it's first banknotes called 'robins' which carried four security features. The main security feature was an edge of constructed elements using the *musical notation* invented by J.M. Fleishman. The musical notation was designed to print music pages of individual characters. The musical notation was *unique* and only available at the Dutch printing house of Johannes Enschedé in Haarlem. Therefore, this edge could only be imitated by an engraver with the same qualifications as Fleischman. That die cutter would have had a lot of work to reproduce this letterpress printing. Photography and thus reproduction by photography had not yet been invented.

The red colour of the edge was a second barrier to counterfeiters. The large variation in typography was the third security feature; the texts on the robins were composed of ten different, again unique, fonts and were added in black by separate letterpress printing. The fourth and last security feature was the unique handwriting. All notes were filled by hand with a date, the denomination and a banknote number (in double digits and letters once) in the period 1814 - 1825. Each note was also signed by the president, two directors and the secretary; in total, eight different styles to be mimicked by a counterfeiter!

6.2.1.2 *Portrait feature (DNB, 1921)*

Human figures on banknotes were introduced in the 1920s and are still used on the majority of banknotes issued [161]. For a long time, a portrait on a banknote was seen as an anti-forgery device. It was assumed that people would notice immediately that the expression of a portrait on a real banknote differed from that on a counterfeit note. People are expert in recognizing other people, especially by the eyes, the philosophy went.

A variant of this design philosophy was introduced by DNB in the 1920s. Banknotes should feature a historical portrait, because 'forgeries are less likely to be successful

if the public is well acquainted with its banknotes, i.e. if people study them more closely.' [43]. A portrait of William of Orange appeared on the new NLG 25 issued in 1921 (Figure 70a). Mythical figures, e.g. the Dutch virgin, had already been used in guilder notes since 1860, but they were the same for all denominations. In 1921, a series of guilder notes for the first time featured well-known historical persons, one in each of the three denominations. The portraits were rather small though.

Larger and tactile portraits

Over time, the small portrait introduced in 1921 was to become larger, like the one of Hugo de Groot in the NLG 10 issued in 1953 (Figure 70b). With the portraits designed by Ootje Oxenaar in the 1970s, a completely new style of portrait engraving was introduced (Figure 70c). Instead of a natural, classical engraving, Oxenaar used the intaglio presses of the banknote printer to their maximum. The portraits were made of bold, wide engraving lines with a high tactility and the thinnest printable lines! The portraits also looked slightly like a caricature. The next step for DNB was to abandon using portraits altogether.

Figure 70

a) First, small portrait (NLG 25, 1921)

b) Classic portrait gravure (NLG 10, 1954)

c) Slightly caricatural portrait (NLG 100, 1972)

d) Portrait abandoned (NLG 100, 1981)

Portrait development in banknotes of the Netherlands between 1921 and 1972.

a) NLG 25/Mercury with small portrait of William of Orange (centre, top of the note), issued in 1921. The portraits on the two other notes are Prince Maurits (NLG 40) and Frederik Hendrik (NLG 60). Designer: J. Visser.
b) NLG 10/Hugo de Groot, issued in 1954. Classical portrait gravure. Designer: J.F. Doeve.
c) NLG 100/Michiel de Ruyter, issued in 1972. Innovative portrait gravure with bold engraving lines; slightly caricatural. Designer: R.D.E. Oxenaar.
d) DNB was the first in the Western world to abandon the portrait policy in 1977 (issued in 1981). Designer: R.D.E. Oxenaar.

Abandonment of the portrait feature
In 1981, DNB was the first to do so with the issuance of the NLG 100/Snipe (Figure 70d). Since the majority of banknotes issued worldwide still carried portrait banknotes, at international meetings on banknotes DNB was asked sarcastic questions like 'Tell me, what is the facial expression of a snipe?' [55]. Since the 1990s a portrait as the main image is no longer a security feature; it mainly represents an emotional value.

6.2.1.3 *Intrinsic and extrinsic security features (DNB, 1976)*

The development of the second generation of banknote sorting machines in the 1970s caused DNB to switch from a reactive to a proactive strategy, initiated by Dr. Peter Koeze (DNB). He introduced the concepts of *intrinsic* and *extrinsic features*, borrowed from thermodynamics. If the result of a measurement depends on the size of the sample, the dimension is extrinsic. An example is the volume of gas. If the result of a measurement does not depend on sample size, e.g. the pressure of the gas, the dimension is intrinsic. Reasoning by analogy, fluorescence in banknote paper is seen as intrinsic, since whatever the size of a piece of banknote paper, the fluorescence is the same.
Other examples of intrinsic features are the substrate's properties (e.g. cotton or other paper types, or synthetic or hybrid combinations), the surface properties and the spectral properties. Extrinsic features, like security thread, foil stripe and intaglio print, are only found on smaller areas of the note.
Intrinsic features are typically more difficult to counterfeit than extrinsic features, is one conclusion drawn in those days.
Intrinsic and extrinsic features are explained in more detail in Appendix 2.

Criterion
Green: Intrinsic security feature.
Red : Extrinsic security feature.

6.2.1.4 *Internal and add-on security features (DNB, 1985)*

In the 1980s the security printing industry started developing a wide variety of semi-finished security features. Examples are fluorescent fibres, security threads, foils and special luminescent features. Due to this development the discrimination between intrinsic and extrinsic features was replaced by internal and add-on features. For DNB, an internal security feature became one that can only be produced inside a security paper mill or printing works in the course of the actual production process, such as a watermark or intaglio gravure. Next to watermark and intaglio printing a new unmistakable example of an internal feature was born in the early 1990s: the micro-perforation of a banknote, first used in Swiss banknotes (CHF 50, 1995).

Considering the pros and cons of internal versus add-on features is advisable for other reasons as well. Add-on features like a security thread or a chip may be removed from a banknote. The residue of add-on features might be recovered from the banknote after destruction, while this seems less possible for internal features. Finally, the physical and chemical resistances of add-on features such as foil usually perform less than internal features (see Figure 27).

Add-on features are usually introduced from another industry. An example is holographic materials, which are widely used in fancy postcards and the packaging industry and since the 1990s have also been widely used in banknotes. The security of the banknote's hologram has suffered because of this worldwide proliferation of holographic technologies. Another disadvantage of such features is that they add a link to the production chain. Any additional link will add transportation movements, security requirements and confidentiality clauses and therefore costs. Semi-finished products are, in principle, less suitable as bearers of security features, since they will be supplied to the security paper mill or printer from outside. Since paper mills producing banknote paper are unique and secure manufacturing sites, banknote paper manufacturers are also recognised as producers of internal features (and not as a semi-finished product). Internal features are further explained in Appendix 3.

Criterion
Green: Security feature is produced within security paper mill or printing works.
Red : Feature is delivered as a semi-finished product.

6.2.1.5 *System approach (DNB, 1991)*

In 1991, DNB presented a third counterfeit model, based on the principle that a reproduction of an original banknote will never be identical to the original. The counterfeiters have no access to the banknote security industry and have to use reproduction tools of the reproduction industry. The quality of the reproduction will look poor next to the original, although sometimes enriched as we have seen with UV features (Figure 11). The system approach considers the reproduction system as a black box. The input is a genuine banknote and the output a reproduction. The black box is described by six physical and chemical phenomena. These six dimensions are briefly discussed below; a more detailed description of four phenomena is provided in Appendix 4.

With the system approach, counterfeit resilience can be predicted by a central bank employee from behind his desk. Instead of the métier approach of making all kinds of reproductions (e.g. in the RRC, see Appendix 4) analysis could be done on the basis of technical specifications of (new) reproduction systems. Such analysis may

be verified and illustrated with counterfeit samples made at a reproduction research centre.

Resolution
At a distance of 300 mm the human eye resolution is about 330 dpi. So counterfeits produced above this resolution will look sharp, while counterfeit banknotes reproduced with less than 330 dpi will be perceived as hazy or blurred. Features with a resolution below 330 dpi should therefore be avoided. The resolution of high-definition features is above 800 dpi.

Criterion
Green: The resolution of the feature is > 800 dpi (or 12 lp/mm).
Red : The resolution of the feature is < 330 dpi (or 5 lp/mm).

Colour
Colour is one of a banknote's spectral properties. It meets several defence principles. The seven different paper tints used in the euro series ensure that each watermark in the series has its own unique colour, both in reflection and transmission. The colour reproduction gamut is another colour principle. Special and unique colours are favoured, while colours within the colour gamut delivered by most presses or printers receive a red flag. Grey tints, for example, are more difficult to reproduce than other colour tints.

Criterion
Green: The colours of the feature are unique colours.
Red : The colours of the feature are available within standard reproduction processes.

Density
Like colour, density (D) is a spectral property. Density deals with lightness or the intensity of the reflected light. Watermark and thread are typical density features (also called *opacity* features). A watermark with a highlight (or 'electrotype' or 'line watermark') would receive a higher score than a watermark without such a highlight (Figure 71).

Criterion
Green: D < 0.1 or D > 2.5.
Red : 1 < D < 2.

Geometry
Geometry deals with a banknote's 2D and 3D aspects. By tradition (background) patterns in banknotes are constructed using geometry, e.g. guilloches or line patterns with alternating colours. The intaglio is clearly a 3D parameter, giving relief

Figure 71

Stand-alone highlight (10) Integrated highlight (eyes)

Left: Watermark Arch in EUR 10/Roman including a 'stand-alone highlight', the numeral 10.
Right: Watermark Little Owl in the NLG 100/Little Owl, issued in 1993. The eyes of the owl are 'integrated highlights'. The watermark is also partly overprinted so as not to be an island feature.

height to the flat paper and offset print. Geometry also deals with the tolerances (or registration R) between the different production techniques. The see-through register is first of all a geometry feature – does the front match the reverse? – and secondly a density feature (look-through).

Criterion
Green: - 0.01 mm < R < + 0.01 mm.
Red : R < - 0.1 mm or R > + 0.1 mm.

Mass
The watermark is created by small mass variations and is often the only banknote security feature using this phenomenon. The mass dimension is g/m^2.
Features removing a part of the substrate, e.g. perforations or a cut-out, also influence the banknote's mass. Laser abrasion techniques may also influence mass, since such techniques are capable of removing part of a printed surface.

Criterion
Green: Mass variation used in the feature.
Red : No mass variation used.

Material
Today banknote security is largely based on the different materials used. Most material properties are not unique and may be found in the public industry. The acquired safety of the security feature lies in the combination of the materials and

technology used in manufacturing and assembling. In addition, special materials may be selected, such as a specific substrate or printing ink not used in the printing techniques of the reproduction industry. See also Section 6.3 on Design principles against counterfeiting, island features.

Criterion
Green: Unique materials used.
Red : Widespread, public domain materials used.

6.2.1.6 *Simple method (DNB, 2006)*

To keep track of the quality of the incoming counterfeits, as indicated in Figure 69, DNB developed such a counterfeit analysis model in 2005, the *simple model*. The method was introduced in DNB's monthly report on banknote circulation of January 2006. The idea underlying the method is to take the most recent counterfeits and monitor their quality. Instead of monitoring all counterfeits, this simple method considers only the 10 types most frequently accepted by retailers and the public. For each of the six public security features in a euro banknote, counterfeit quality is simply scored as:

0 point = no imitation
1 point = poor imitation
2 points= good imitation

The simple model indicates which features from existing banknotes are counterfeited most and which least. Euro banknotes have six public features, so the maximum counterfeit quality score is 12. Two interesting conclusions were drawn immediately:
- Not one euro counterfeit received 12 points (6 x 2 = 12); the maximum score to date is 10 points,
- The average quality score is about 6.5 points, which grade is declining as counterfeiters are producing lower qualities over the years.

This simple counterfeit analysis model is further explained in Appendix 5.

Criterion
Green: The imitated feature scores less than 0.5 point.
Red : > 1.5 point.

6.2.1.7 *Public testing (DNB, 2006)*

Next to counterfeit analysis from a reproduction point of view, public testing is another way to analyse counterfeited banknotes. Such a large-scale test was organised by DNB in 2006 and is quoted in this study in Section 4.1.6 on training

[80]. Analysing the data of this study Tom Buitelaar (DNB) in 2007 reported that the majority of respondents were not fooled by imitations. The maximum acceptance rate of bogus notes found is 37.5% for counterfeits with three imitated public features. Furthermore, a correlation was found between public acceptance of the counterfeits presented and the quality of the imitated security features. The highest correlations were found for intaglio relief, security thread and watermark, implying that these features are the most easy to use by the public when checking euro banknotes for genuineness. Some correlation was found for the hologram, indicating that some people also rely on the foil. The lowest correlation was found for the see-through register and the OVI, meaning these features are hardly ever checked [98].
In case of retail features the following was found. Retailers judging real and counterfeited euro banknotes who were not trained in using a UV lamp clearly did worse than respondents that did not use a UV lamp. In case of an IR camera, untrained cashiers did *slightly* better than those without.

Counterfeit test by the public and the Board
When the proof of a new banknote design is printed, central banks could make their own counterfeits of this newly born banknote. Tests using these counterfeits could be carried out among retailers and members of the public. Such tests will provide valuable feedback on banknote design and features.
On a small scale, such a test would be to offer the Governor and the Board two self-made counterfeits together with the proof prints of the new banknote, a push-the-button copy and a professional counterfeit. This would give them an idea of the type of counterfeits that will be made once the note has been issued.

6.2.1.7 *All-in-one method (DNB, 2010)*

The latest method developed for making a selection of security features is the *all-in-one method*, the subject of this paper. This study is a follow-up to the author's paper 'Innovative approaches to the selection of public security features' as presented at the conference of Optical Document Security (ODS) in 2010 [156]. This study, in turn, was an iterative cycle of the 'Innovative approaches to banknote design' paper as presented at the Watermark Conference in 2009 [134].
In its conclusions, the ODS paper referred to a table providing an overview of the public's appreciation of the public security features in the 50 euro banknote, showing nine different feature selection models. Making maximum use of the input from other research, this method provided the basis for the all-in-one method.

Input from others
The all-in-one method is flexible, using input from as many criteria as required. Additional criteria (j) may be added as additional rows in the security feature matrices (e.g. Table 14). The method already proposes over 25 criteria and other

methods, models, approaches and views may be added by, for example, other central banks, Europol or security printers.

Step 1: generic security matrix
The all-in-one method starts with the generic security matrix. The security features of the existing banknote are divided over the different user groups or stakeholders. Six different user groups and their types of features are identified: retailers, the general public, banknote processors, central banks, counterfeit deterrence systems and forensics. Trigger features are also part of the generic security matrix and are used by both retailers and the general public. Trigger features like paper tint, scan and screen traps and bright colours, contribute to the heuristic quality of the banknote. Rule-based banknote quality is provided by public security features such as watermark, security thread and holographic foil. Ideally, each user group receives three security features; two or three features could be added in case of the 'dormant feature strategy'. All together, this leads to a total number of about 20 security features for the new banknote.

Step 2: analysis of feature matrices
Second step in the all-in-one method is to analyse the feature matrices of the existing banknote. The introduction of a new design is an opportunity to optimise these matrices:
- Tool-feature matrix (for the retailer),
- Human action-feature matrix (for the public).

Step 3: what goes out?
Next step is to decide on the feature that will be abandoned before any decision on a new feature is made. This is usually a tough choice for a central bank; once a feature is in, it is hard to get it out. Which features go out is decided on the basis of several criteria, such as:
- Public knowledge, including features left out in information tools (during circulation),
- User requirements, including space and single user group,
- Counterfeit analysis,
- Cost,
- Life span,
- Input from others.

One may add or delete as many criteria as desired. In addition, the proposed threshold values may be adjusted as required.

Step 4: what can be improved?
Once the features to be left out have been determined, it must be decided if the features to be maintained can be improved or enhanced in terms of design (perception,

communication) and technology. Usually, it is not the security technology that has become obsolete, but the design of the security feature that has failed (from the day of introduction). An inventory is made of possible improvements – design and technology – of the features maintained. This inventory is scored in a similar way as step 3, 'what goes out?'.

Step 5: What goes in?
The last step in the method is the search for new features that may enter the new banknote. The candidate *public* features should be classified and listed according to the required human operations such as feel, look at, look through, tilt and possible disruptive human operations such as nail scratching or using the camera on a mobile phone. The candidate *retail* features should be classified and listed according to the tools operated by the retailer.
Similar criteria are used as the ones in step 3, 'what goes out?'

Preferences
While the market is offering more and more *add-on* security features, the number of *internal* security features is limited. Yet, if a choice can be made, internal features (made in-house) are to be preferred over add-on ones (like semi-finished products). Features with a high 'design freedom' are also preferred (i.e. size, shape, and colours) just as:
- Features with 'design variety' (i.e. available in different colours),
- Features that may be combined ('integrated') with other banknote design elements (i.e. partly overlap, avoid island features),
- Nested features should be avoided, since a feature-in-a-feature takes too much time to verify and is too complicated to recall. Such nested features are also more difficult to explain in communication tools,
- Multi-user group features should be avoided as it is difficult to optimise such features for all user groups.

Step 6: Design policy
Once a decision has been made on the security features for the new note, the central bank should develop a design policy covering:
- Design philosophy,
- Strategic communication,
- Banknote series design,
- Individual banknote design.

Before designing a new banknote series concept, the following questions should be answered:
- Should all denominations have the same public security features or should the low denominations have other public security features than the high denominations?

- Should all public features be on the front of the note?
- Should the public security features be similar in design, but differ in the techniques used?
- Should features that are operated by the same human action be grouped together?

6.2.2 **Other methods**

Would it not be wonderful if we could say: 'The counterfeit resistance of a foil is 134% that of a watermark.' Unfortunately, it is not that simple to compare security features. Trying to find an answer, central banks are building artificial models to come to a structured approach, needed for proper security feature selection. The overview starts with four older models:

6.2.2.1 Gresham's law (1558),
6.2.2.2 Legislation (England, 1679),
6.2.2.3 Counterfeit frequency model (traditional),
6.2.2.4 Overt and covert features (around 1980).

Trend towards complex models to analyse security features
Two of the recent models to be used for feature selection were presented in 2005 to an international forum by respectively the central banks of Brazil and Mexico. Both methods were based on a score-based work process. Today the use of artificial models to underpin the selection of banknote security features has become a trend. Most models use algorithms to aggregate criteria to a single value level or a set of values. However, as they are complex and so far have not yielded a proper selection of new features, none of these models has been validated. Except for the Canadian security effectiveness none of the models includes the use of real counterfeits as input for their analysis.
The models developed since 2007 by the NRC, ECB, Bank of Canada and US Treasury will be discussed below.

6.2.2.5 Flow model (NRC, 2007),
6.2.2.6 Resilience grades (ECB, 2007),
6.2.2.7 Threat assessment (BoC, 2008),
6.2.2.8 SecureCalc (US Treasury, 2009)
6.2.2.9 Feature effectiveness (BoC, 2010).

6.2.2.1 *Gresham's law (1558)*

One of the first analyses of money is known as 'Gresham's law', commonly referred to as: 'Bad money drives out good.' The expression 'Gresham's law' dates back to 1858, when British economist Henry Dunning Macleod decided to name the tendency for bad money to drive good money out of circulation after Thomas

Gresham (1519-1579). The principles of Gresham's law can be applied to different fields of study, like coins, banknotes and high inflation rates.

Coins

Until the 1970s coins had an intrinsic value, based on alloys of copper, silver or gold. Coins having less than the officially specified amount of such a precious metal are 'debased' coins or 'bad money'. Good money on the other hand is money that shows little difference between its *intrinsic value* and the *face value* of the coin. Good and bad coins cannot circulate together; bad money will quickly dominate. People spending money will hand over bad coins, keeping the good ones for themselves. This observation was made by Gresham and before him by several others, including Copernicus in 1522. In fact, since the use of silver and gold coins the phenomenon has been noted, e.g. in a Greek play at the end of the 5th century BC.

A more recent example of Gresham's law is related to coins in the Netherlands. Citizens retained the silver guilders in the 1960s when they were replaced by nickel. People wanted to capture the higher current or perceived future intrinsic value of the metal content over their face value, using the newer coins in daily transactions. The same process occurs today with the copper content of coins of low denominations. Central banks notice this, too, when the purchase price of small coins exceeds their face value.

Counterfeited coins are also subject to Gresham's law. In the case of clipped, scraped, or counterfeit coins, the commodity value was reduced by fraud, as the face value remained at the previously higher level.

Banknotes

According to Gresham's law, people will try to get rid of a counterfeited banknote once they know it is a fake. Unfit banknotes are also subject to this principle; people will first spend the soiled, worn and repaired banknotes in their wallets. In case of newly issued banknote design people tend first to spend the old design and keep the new one in their wallets.

Different versions of banknotes can also be subject to Gresham's law, as may occur when paper-based banknotes are replaced by polymer bills.

Inflation

During the Great Inflation in the Weimar Republic in 1923, official money became so worthless that virtually nobody would take it. Instead of cash money, any good, such as food, became a circulating medium of exchange. In 2009, hyperinflation in Zimbabwe showed similar characteristics (Figure 72). These are also examples of Gresham's law at work. In such dark times there is one small light for central banks; the counterfeiter will be inactive since it is useless to forge worthless banknotes.

6.2.2.2 *Legislation (England, 1697)*

One of the options for central banks to limit counterfeiting of banknotes is to use legislation. The first *law* on counterfeiting banknotes was passed in 1697, when British Parliament passed a bill declaring banknote forgery a felony punishable by death. Later, in 1800, the introduction of banknote paper with a wave-line was supported by an Act of Parliament prohibiting the manufacture of paper with wave-line watermarks [26, 38, and 46]. The first banknotes with a penalty text printed on the banknote telling that the counterfeiter could be sentenced to death were issued in France in 1791 [55]. In the United States, President Lincoln assigned the Secret Service the task of combating counterfeiting as reported in Chapter 2.
The first penalty text on Dutch banknotes appeared in 1859 [43, 55].

Within the Eurosystem, legislation on counterfeiting is not yet harmonised. In the Netherlands, the Criminal Code distinguishes the following four situations:
1) Production of counterfeited banknotes with the intention of bringing them into circulation (penalty: 15 to 20 years imprisonment),
2) Purchasing counterfeited banknotes with the intention of bringing them into circulation (penalty: 1 to 5 years imprisonment),
3) Bringing a received counterfeited banknote back into circulation, knowing that it is a false banknote (penalty: 1 month to 1 year imprisonment or a fine of 50 to 10.000 euro),
4) Unauthorised issue of fantasy banknotes with the intention of using them for regular payments (penalty 1 month to 1 year imprisonment or a fine of 50 to 10.000 euro).

Figure 72

Weimar Republic (1923) Zimbabwe (2009)

Two examples of banknotes issued at times of hyperinflation.
Left: Banknote of one million mark, issued in the Weimar Republic during the hyperinflation in 1923. Designer: Herbert Bayer.
Right: Banknote with the highest denomination ever released, the ZWD 100 trillion, issued on 16 January 2009 in Zimbabwe.

6.2.2.3 *Counterfeit frequency model (traditional)*

One of the oldest methods used by central banks is the *counterfeit frequency model*. The basic idea is to keep statistics of the counterfeited features. The more frequent a feature is counterfeited the more reason to replace it by a new one. Of course, this is a quantitative approach; perhaps the reproduction quality of the feature is not really that good. Still, features that are counterfeited most frequently are those that should be replaced first in a new banknote design. The ultimate consequence is to leave a typical banknote production technique like gravure printing or mould made paper with a watermark. A case in point is the Simultan press, a typical banknote production press, which is questioned in Appendix 4.

Table 33 provides the frequency of imitated public security features in counterfeited euro banknotes. Exact figures (frequency) are kept confidential; central banks do not want to be the quality control managers for the counterfeiter. Categories are used instead like 'almost all', 'frequent' and 'some.'

Knowing that the watermark is the best-known public feature, would counterfeiters always incorporate fake watermarks? Or, in more general terms, do counterfeiters use the public's knowledge as reflected by Table A1.1 for optimizing their bogus notes? It seems that counterfeiters have their own opinion and do not follow the presented statistics, although there is some correspondence. A counterfeiter will invest a minimum effort – a minimum number of security features – to create a fake note that they can get away with. So, why do counterfeiters focus on certain features and widely ignore others? The explanation may be found in the 'heuristic quality' of a banknote. The foil stripe is a fine example. The counterfeiter always includes a foil stripe in a counterfeited 20 euro note, although in many counterfeits just a commercially available foil stripe is used, which does not at all match the original one. An authenticity check of the foil stripe is a 'rule-based quality' of the banknote, just as the use of the other public security features. The conclusion is that a counterfeiter pays more attention to the heuristic quality (overall impression) than to the rule-based quality (security features) of the counterfeited banknote.

Criterion
Green: The feature is imitated in < 10% of the counterfeited banknotes.
Red : The feature is imitated in > 80% of the counterfeited banknotes.

6.2.2.4 *Overt versus covert features (around 1980)*

Until 1980, security features were kept secret or covered, because in banking circles the notion reigned that to tell the public was to tell the counterfeiters [44, 49]. Today central banks recognise that counterfeiters will analyse a banknote anyway.

Table 33

Public feature in euro notes	Imitated in some form in euro counterfeit
1. Watermark	Frequent
2. Hologram/silver foil	Almost all
3. Tactility - rubbing finger	Some
- nail scratch	Some
4. Security thread	Frequent
5. Colour changing ink (OVI)	Frequent
6. Glossy gold stripe	Frequent
7. See-through register	Frequent

Counterfeit frequency of public security features in counterfeited euro banknotes (common class).

The Swiss National Bank was the first with a public leaflet in 1976. DNB followed the Swiss example in 1983 with a first experimental leaflet for the NLG 50/Sunflower. Today every central bank makes an effort to familiarise the public with the (public) security features. Communication costs are relatively low (Figure 3).

Overt and *covert* features should not be confused with intrinsic and extrinsic features nor with internal/add-on features. Covert features are banknote security features that are covered, not visible to the human eye. Such features are usually dedicated to detectors and are not published. Opposite to covert features are the overt features, features to be used by the public and retailer.
The terms overt and covert features were never favoured by DNB. Instead, DNB opted for the introduction of *user groups*, including the general public, retailers, central bank sorting machines and forensic experts. DNB was the first to apply user group classification in 1982 [10]. Of course, public features should be evident, even striking, while features for sorting machines should be undetectable to the human eye.

6.2.2.5 *Flow model (NRC, 2007)*

The report 'A Path to the Next Generation of US Banknotes' is quoted several times in this study. This report, commissioned by the BEP from the NRC, provides an extensive analysis of who is counterfeiting and also included a selection method for ranking security features [102]. All features assigned received more or less identical scores, which fell short of the NRC's expectation that the method would discriminate between public security features. Instead, they opted for a *flow model*. A feature that prevents *passing* is more effective than a feature that prevents

reproduction, their conclusion reads. The future they see is a world using many more sophisticated authentication detectors, so that counterfeits can be removed from circulation on an ongoing basis [106]. This observation is quite similar to the one made in this study: the retailer is key in preventing the spread of counterfeited banknotes.

6.2.2.6 *Resilience grades (ECB, 2007)*

At the Euro Conference in 2007, the ECB presented a counterfeit resilience assessment of security features, leading to a *Resilience Grade* of a single feature. The method presupposes trained and attentive public persons. The time needed to counterfeit the features is also part of this method. The method allows for a classification of public security features reflecting their counterfeit resilience (or robustness). The ranking of counterfeit resilience by the ECB is based on the following eight criteria:

1. Complexity (number of properties to be checked),
2. Clarity (univocal properties),
3. Wear & tear resistance (impact of wear & tear on clarity),
4. Equipment needed,
5. Material needed,
6. Material becoming available in the near future,
7. People (knowledge, skills).
8. Counterfeit attacks.

Each criterion is subdivided into several *descriptors* (or sub-criteria). These descriptors are discussed by banknote experts of the ESCB (European System of Central Banks) and points are attributed. The design of the security features tested is part of the clarity criterion. The simulated counterfeit attacks are ranked *good*, *mediocre* or *poor* and are also input. The method provides for several mathematical steps to arrive at Resilience Grades (RG) ranging from RG 1 to RG 6; RG1 for the highest resilience and RG6 for the lowest. The difference between the public features scored, turned out to be quite small; from the six RG -levels just three were used, which corresponded with the NRC's finding reported above.

6.2.2.7 *Threat assessment (BoC, 2008)*

Over the years, the Bank of Canada set up several projects to predict the effectiveness of banknote security features. In 2008, the BoC followed with its publication on *threat assessment*. For the creation of a new public security feature, the BoC recognises 5 development phases called *stages/gates*: from design to production scale-up. Projects should be running on a continuous basis in various stages of maturity [107]. The criteria for passing on to the next stage/gate process are reviewed by a panel of experts on the basis of a *technology scan* and *threat analysis*. The different banknote

user categories, e.g. *human*, *automatic* and *forensic*, are part of the analyses. Human is subdivided into *unassisted* (e.g. general public) and *assisted* (e.g. retailer). Automatic is subdivided into *cash distribution* (e.g. counting, sorting) and *retail* (e.g. vending machines) [129].

6.2.2.8 *SecureCalc (US Treasury, 2009)*

At the Banknote 2009 Conference, the BEP part of the United States Department of the Treasury, also presented a method for evaluating public security features, called *SecureCalc*. This mathematical method is again based on the input from experts [150].

6.2.2.9 *Feature effectiveness (BoC, 2010)*

A model for measuring *feature effectiveness* was published by the Bank of Canada at the Optical Document Security conference in 2010. This approach was validated against the existing series of banknotes. Both the counterfeit statistics and the counterfeits themselves were analysed to give the new security feature tests a comparator. Only then the BoC started to apply the developed methodology to potential new security features and designs.
Instead of internal central bank experts, respondents are recruited from the public. These respondents participate in experimentally testing the security feature. The respondents are not asked their opinion on the security features but instead are asked to identify all the counterfeits in a deck of 300 samples. Of the 300 samples 60 are counterfeits.
A second plus of the Canadian method is the inclusion of real counterfeits. Both the counterfeits and the real notes are masked, except for the public feature to be operated in the test. The public is asked to decide: real or fake? The response is recorded on accuracy as indicated in Table 34. Also the time needed to come to a decision is recorded [155].

Table 34

	Samples	
Response	Fake note	Genuine Note
Identified as fake	Found	False alarm
Identification as genuine	Missed	O.K.

Response accuracy recorded on both fake and genuine banknotes in the security effectiveness test of the Bank of Canada.

The DNB study conducted in 2006 [80] shows similarities with the feature effectiveness study of the BoC, since both include real counterfeits in their public testing. But there are also some differences. The BoC targeted the general public and students, while DNB invited only professional cash handlers to participate. The BoC uses speed as a performance indicator, while DNB used a fixed pitch of 2 seconds. While DNB offered complete banknotes, BoC studies were conducted on whole notes as well as on focus feature tests.

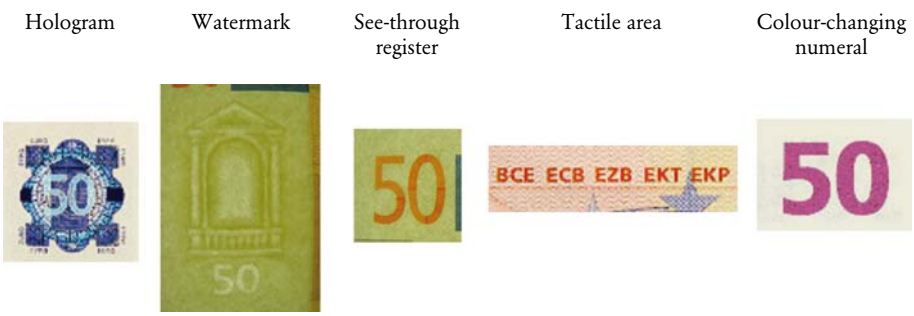
Evaluation
Comparing the models of the ECB, the US Treasury and the BoC, the following observations can be made. All three institutes:
- Feel the need for an 'objective' tool to evaluate public security features for their resistance to counterfeiting.
- Focus on the evaluation of single features, not taking into consideration that a counterfeiter must produce a complete banknote and not just one single feature. Tests on counterfeit resistance should cover the entire new banknote.
- Fail to include the way counterfeiters operate. In other words: the time and investment needed to counterfeit a banknote are not fully covered by the models.
- Base their judgement exclusively on experts' views instead of including the public's comments (except the BoC).
- Fail to conduct physical and chemical measurements on the genuine feature versus counterfeited variants.

6.3 **Design principles against counterfeiting**

Analyses of counterfeited banknotes learn that it is often not the technology that fails, but the design that is inadequate (perception and communication). The needs of the retailer and the public are described in Chapters 3 and 4, respectively. The main message is that security features should fulfil user requirements. Apart from retail and public security features there are also some banknote design requirements typically dedicated to prevent counterfeiting. One of them is 'integrated design' and this is one of the most quoted phrases at conferences on banknotes. It means that banknote designers should avoid island features.

Island features
Related to the geometry phenomenon of the system approach are so-called *island features* or *stand-alone features* (Figure 73). Such security features are not linked to other printing techniques, e.g. by partial overlaps or overprints, and should be avoided since they make life easier for the counterfeiter. As often said, the security of the complete banknote should be found in the integration of these features, e.g. as achieved through overlaps between these features. This principle is explained in Figure 74 and the DNB patent 'Authenticity Mark' [76].

Figure 73



Most public features in the euro banknotes are island features, i.e. they are not linked to other printing techniques, e.g. by way of partial overlaps.

For counterfeiters, reproducing the banknote – both scanning and production – is more difficult if security features are integrated in the design. If a watermark has an integrated highlight, like the eyes of the little owl in Figure 71, the watermark will have a higher counterfeit resistance.

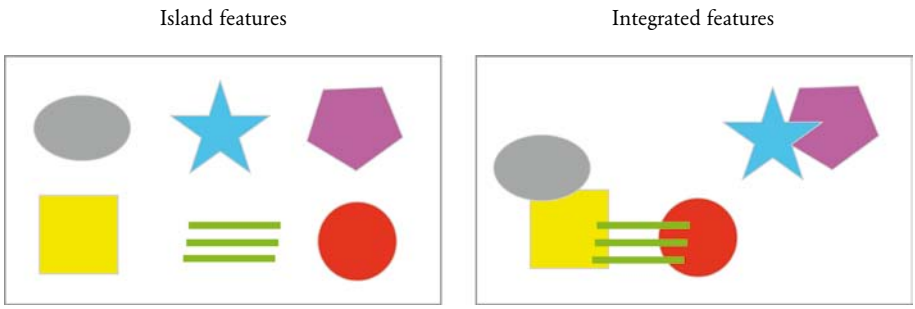
Criterion
Green: Security feature overlaps with other banknote production techniques.
Red : Isolated feature.

Thread, foil stripe or iridescent band are usually simply overprinted in the banknote design and are not really integrated. Such features could be more effective by making them leading in the design process. Also features that are 'not linked', not physically connected to others could be improved, such as the colour changing element (OVI) and the watermark.

Not put all one's eggs in one basket
A second design principle to prevent counterfeiting is to come with a variety of technologies behind the security features. The selection of security features for a new banknote may especially profit from the system approach (see Section 6.2.1.5 and Appendix 4). The central bank could select the features on the principle of 'not put all one's eggs in one basket' and could opt for a strategic spread of the features over the six phenomena (Figure 75).

Life span
A third basic principle to prevent counterfeiters from making fake notes is a patent protection on a security principle of the feature. The life span of a series of banknotes can be set at 20 years, being the period a patent – if applicable – provides the central

Figure 74



Left: banknote with six individual public security features; stand-alone features without integration or overlap ('island features').
Right: banknote with six 'integrated' public security features; partly overlapping each other. Integration is further enhanced by overlap of non-secure areas, such as overprinting with offset.

bank the exclusive right to use this feature. Therefore, recently patented or soon to be patented security features should be selected. The central bank as patent owner has the exclusive rights to the feature's use. Production of the feature can be organised in a controlled and secure plant. A patent protection is an argument for central banks to come with a new banknote, since after this period of 20 years the feature may be produced free of any claims.

Criterion
Green: Patent on the feature is less than 5 years old; patent age < 5 years.
Red : The patent on the feature has expired; patent age > 20 years.

Figure 75

Selection of security features for a new banknote could be based on the policy 'do not put all your eggs in one basket'.

7 Conclusions

7.1 The retailer, not the general public, is the most important stakeholder of security features to be used in new banknote design.

7.2 More research is needed on user requirements of security features, both for the retailer and the general public.

7.3 The most important user requirement is time. Features may take up two seconds for a check, but not more. The accuracy of the check should be at least 90%. In the case of three public security features, the public will take a maximum of six seconds to check a banknote (although usually they will perform no check at all). In case of five or six public features, three features could be actively promoted, while two or three features could be dormant.

7.4 Worldwide, banknotes are provided with similar public security features, because central banks tend to adopt features introduced earlier by other central banks. These early adopters are often influenced by the security industry; the features often do not match user requirements.

7.5 The security industry offers many tilt and look-through features. There is a very limited choice in new feel and new look-at features.

7.6 The proposed all-in-one method offers a structured approach to the development of new banknotes. The method includes a marketing approach and an analysis of the banknote to be replaced. The all-in-one method indicates which features should be maintained and where to look for new security features (e.g. feel features and look-at features, limited tilt features). The method applies to features for both the retailer and the general public.

7.7 Security features that are maintained should be improved on design (communication and perception) and/or the technology behind the feature. New selected security features should be optimised for both: design and technology. Experimental psychology and eye movement planning should be used in designing new banknotes. Once a printing proof is made, tests

should be performed to gain input from retailers and the general public. Such tests should include counterfeited banknotes (made by the central bank).

7.8 The phenomena of heuristic and rule-based quality of banknotes need more analytic research to optimise future banknotes.

7.9 The number of public security features also depends on the motto and theme of the notes (e.g. six public features in case of the motto E-U-R-O-P-A).

7.10 Numerals (e.g. 10) or currency symbols (e.g. $ or €) should not serve as images for the public security features. Instead, emotive images should be created for public security features. The public features should be designed rather in 2D than 3D and should have a clear silhouette.

7.11 Public security features should use both verbal and visual information. Public security features are better memorised if they have a name and this name is printed along the feature.

7.12 Central banks do not have to evaluate all new features offered by the security industry. Using the marketing approach within the all-in-one method will save effort here.

Acknowledgement

This paper is part of the fieldwork of my PhD study 'Key elements in banknote design' at Delft University of Technology, Faculty of Industrial Design Engineering. I want to thank my tutors and supervisor for their interest and inspiring remarks:

- Prof. Jan Jacobs (Delft University of Technology, Faculty of Industrial Design Engineering),
- Prof. Dr. Frans Verstraten (University Utrecht, Faculty of Social and Behavioural Sciences),
- Dr. Theo Boersema (Delft University of Technology, Faculty of Industrial Design Engineering).

Several other people have contributed to the content of this paper. Since the paper is extensive, not all have commented on all subjects. Thanks are due to the following persons and or organisations for their remarks or support:

- Mr. Marco Wind (DNB),
- Dr. Carlo Winder (DNB),
- Dr. Peter Koeze (DNB, retired),
- Dr. Andrea Firth (Bank of Canada),
- Mr. Charles Spencer (Bank of Canada),
- European Central Bank.

Further thanks go to Mr. Jan Binnekamp, head of the Currency Policy Department (DNB), for supporting the study. I also thank all my colleagues at the Currency Policy Department of DNB for their interest and remarks. Finally I am grateful to Mr. Fred Collens (DNB), Mr. René Kurpershoek (DNB) and Mr. Hugo Swelsen (DNB) for editing most of my English.

Appendix 1
Public knowledge of security features

Since 1983, DNB has measured biennial the public's knowledge of security features [49, 112,133]. This knowledge increased from an average of 1.03 in 1983 to 2.5 in 2009 (Table A1.1).
There seems to be room for further improvement. People in the highest social class are able to mention on average twice as much features as those in the lowest social class. People in the 18-35 age bracket can memorize on average more than those aged 55-plus. Knowledge of security features also correlates with gender and wealth. Men can name more security features than women (Table A1.2).

Target is: three public security features
If banknote design and public information were further optimized, the awareness target could be set at an average public knowledge of 3 security features, matching with the requirement of the central bank to check at least 3 security features (see e.g. Chapter 2) [112, 133].
In 2005, research by the European Commission's Anti-Fraud Office (OLAF) reported an average knowledge of 1.3 security features, concluding that there was a 'lack of knowledge about banknote security features aimed at the general public'. No link was found between knowledge of a security feature and the ability to identify genuine banknotes [67].

No more than 4 text elements, picture elements and security features
One of the most important survey findings is the fact that the general public cannot memorise more than 4 text elements, 4 picture elements or 4 security features. Four seems to be the maximum. Most people are able to recall about 2 text elements and about 2 picture elements. On the basis of this finding, DNB decided in 1985 to limit the number of the public security features in a banknote to 4. For Euro Series 2, the target has been set at 6 [92, 136].

Given that surveys show that the public is able to recall about one to three security features, it does not make much sense to have more than 4 public security features in one banknote.
Bearing in mind that it takes a long time for the public to learn new security features, central banks should be careful about altering or leaving out features to which the public has grown accustomed.

Table A1.1

	Public knowledge of security features in NL (%)				
Time	Feb 2002	Feb 2003	Feb 2005	Feb 2007	Feb 2009
Number of respondents	2,002	2,015	1,501	1,506	1,058
Watermark	70	65	68	65	76
Hologram/silver foil	61	52	49	43	55
Security thread	31	13	12	14	15
Special ink: glossy stripe (iridescent gold)	5	3	3	4	2
Special ink: colour changing ink (OVI)	5	3	4	4	3
See-through register	7	5	5	5*	9
Raised ink, relief	7	5	9	5	8
Micro text	3	4	4	4	6
Type of paper	7	8	10	7	14
Ultra violet (UV) total	11	16	23	18	27
- dull paper	*1*	*2*	*5*	*4*	*3*
- fluorescent fibres (red, blue, green)	*5*	*9*	*12*	*7*	*16*
- ink brightens up (front, e.g. flag, sign.)	*3*	*3*	*3*	*3*	*5*
- ink brightens up (rev. e.g. bridge, map)	*2*	*2*	*3*	*2*	*3*
- no specification, hold under UV light	*-*	*1**	*3**	*2*	*0*
Infrared (IR)	2	3	5	3	5
Don't know any security feature	11	18	15	19	7
Average knowledge of security features	2.3	2.0	2.2	1.9	2.5

* = corrected compared to 2007
Public knowledge of the security features of euro banknotes in the Netherlands in 2002, 2003, 2005, 2007 and 2009 (in %) [94, 133]. OVI = Optically Variable Ink.
All measurements are done by TNS NIPO. The answers are given 'repeated by heart'. The type of research is periodic.

Declining incidence of wrong and partly wrong answers
Over the years, the gap between the categories *correct* and *including wrong answers* has clearly narrowed, owing to the decrease in partially wrong answers regarding *blind marks, banknote numbers* and *type of paper* over the years 1983-2009 [112].

Large group that does not know any feature
The average number of security features spontaneously produced by the Dutch public appears to be 2.5 in 2009. To increase this average, communication should focus first of all on the 15-20% of citizens unable to tell one single security feature (Table A1.2). In general, these people are found among elderly citizens, citizens in the lower social classes, the less-educated, women, and people who do not deal with money ('non-retailers') on a daily basis [133].

Also in other countries there is a large group of people not able to tell any security feature. The National Bank of Romania reported in 2006 that 24% have no idea of any security feature. Within the euro area around 30% of the people can not recall one single security feature; in some euro zone countries even more than 50% of the population. A similar figure was found in 2003 by the Bank of Canada: 37% of the general public was not aware of any security feature on the new CAD 5 or 10 note (unaided); for the old notes (20 and 50 dollar) it was even higher: 43%. Spanish researched showed that almost 1 in 5 Spanish cannot name one security feature either [117].

In 2002 the figures clearly show the effect of the introduction of the euro (average 11%). After an increase, this average number of people not able to recall a single feature dropped from 19% in 2007 to 7% in 2009. Perhaps the relative high number of counterfeits in 2009 is a part of the explanation. DNB also pushed promotion activities on security features in 2008 and 2009. And perhaps are people more eager to learn some security features when there is an increase of counterfeited banknotes? Anticipating on the 2011 measurement is interesting; will the figures go back to a level between 15-20% or will the Dutch public be more knowledgeable?

Knowledge of elderly people
Older people are significantly less able to recall one single security feature than the younger ones as shown in Table A1.2.

Cash handler surveys ECB
The ECB also found that the public at large has limited knowledge of euro banknotes' security features. Their qualitative surveys suggest that cash users usually do not pay much attention to the security features of the euro banknotes and are familiar with only a limited number of these features (see Table A1.3). Furthermore, just a

Table A1.2

	2002	2003	2005	2007	2009
Average	11	20	15	19	7
Men	10	15	14	17	6
Women	13	25	15	20	8
< 34 year	5	8	4	6	1
35 - 54 year	9	16	13	16	7
> 55 year	21	37	27	36	12

Distribution by age of people who are not able to recall one single security feature over the years 2002-2009 (euro banknotes, NL).

Table A1.3

ECB Cash handler survey figures in %	2004		2007		2009	
	EUR	NL	EUR	NL	EUR	NL
Public features						
1. Feel of the paper, raised print	79	*47*	70		74	*64*
2. Security thread	34	*31*	41		46	*34*
3. Watermark	36	*44*	47		44	*55*
4. Hologram	37	*23*	41		37	*26*
5. Colour-changing numeral	14	*14*	23		21	*14*
6. Glossy (gold-coloured) stripe	12	*10*	20		20	*17*
7. See-through number	12	*12*	8		8	*11*
Retail features						
9. Ultra-violet properties	17	*36*	14		9	*24*
10. Infra-red properties	4	*4*	4		4	*6*
11. Automatic device	-	-	4		6	*15*
12. Mini/micro-printing	2	*2*	5		8	*2*
13. Wit a euro 'pen'	7	*3*	-		-	-
Other answers						
14. Other features	11	*14*	3		4	*11*
15. Compare with genuine note	3	*0*	8		9	*10*
16. Don't know	-	-	0		1	*0*
17. I don't check	15	*26*	-		-	-

Overview of the spontaneous answers of the cash handlers in the ECB Cash Handlers Surveys over the year 2004, 2007 and 2009 [60, 100, 151]. No data available for NL in 2007.

tiny fraction of the respondents was able to name or describe their functionalities. Knowledge is, in most cases, limited to the traditional security features, i.e. the tactile properties, the watermark and the security thread. The hologram is best known from the relative new features, the recollection of the glossy gold stripe and the colour-changing are around 20%.

Appendix 2
Intrinsic and extrinsic security features (1976)

Isaac Newton (1643 – 1727), the famous English physicist, was possibly the first to make a difference between the *intrinsic value* of a coin, the market price of its metal, and its *extrinsic value*, the face value. Both should be brought into agreement, he observed in 1696. When Newton later became warden of the Royal Mint he invented a new extrinsic security feature for coins, the rim of the coin were marked with stripes (milling or reeding) to prevent coin clipping.

Nearly 300 years later a Dutch physicist working for DNB, Dr. Peter Koeze, introduced *intrinsic* and *extrinsic features* for banknotes. In 1979 DNB started with the development of DNB's second generation of banknote sorting machines. The policy to select machine readable features for these new sorting machines was based on the model of intrinsic and extrinsic features, as proposed by Koeze [6, 156, 175].

The principle of intrinsic and extrinsic features was borrowed from thermodynamics. If the result of a measurement depends on the size of the sample, the dimension is extrinsic. An example is the volume of gas. If the result of a measurement does not depend on sample size, e.g. the pressure of the gas, the dimension is intrinsic. Reasoning by analogy, fluorescence in banknote paper is seen as intrinsic, since whatever the size of a piece of banknote paper, the fluorescence is the same. Intrinsic banknote features mentioned by Koeze were, among others: X-ray fluorescence, absorption of

Figure A2.1

Two exemples of synthetic banknotes.
Left: HTG 50, first synthetic banknote is issued by the central bank of Haiti in 1980 (synthetic type, Tyvek).
Right: CLP 5,000, recent synthetic banknote issued by the central bank of Chile in 2009 (polymer type, Guardian).

electro magnetic micro waves and Electron Spin Resonance (ESR). Another feature mentioned also was based on laser Raman spectroscopy (in the infra red spectrum).
Based on this concept of intrinsic-extrinsic features, the following concept was created for the detectors of the second generation of DNB's sorting machines, introduced in 1981. One intrinsic and one extrinsic feature were proposed for both the paper and the print: UV luminescence (intrinsic, paper), magnetic ink (intrinsic, print), barcode watermark (extrinsic, paper) and intaglio lines (extrinsic, print). In addition, it was proposed to keep number reading (extrinsic, print) [7].

Intrinsic preferred over extrinsic
In this model the intrinsic banknote features are characterised by the choice of materials, while the extrinsic banknote features are set by the choice of the applied production technique. Intrinsic features are typically more difficult to counterfeit than extrinsic features, is one conclusion drawn in those days.
The paper surface of banknote paper shows the mesh wire of the mould of the paper machine and is an intrinsic feature, just as the typical structure of the cotton, which makes every banknote unique. Luminescent features added to the paper are also considered intrinsic. A disadvantage of these pigments is that they can not be burned and remain in the ash content of destroyed unfit banknotes.
Adding plastic fibres to the banknote paper changes the intrinsic properties of the paper. In 1974 DNB issued banknotes printed on a semi-synthetic paper called Paressyn [34, 43]. A substantial percentage of plastic fibres were added to the cotton to increase both the tensile strength and the tearing resistance. This paper was produced by VHP. Today such composite papers are provided by most paper mills (e.g. Diamone by ArjoWiggins).
The unique polymer substrate film for the BOPP (Bi-axially Oriented Poly Propylene) is also considered as an intrinsic feature (two laminated layers of 37.5 µm each). BOPP is a non-fibrous and non-porous polymer.
Central banks opt for polymer because compared to paper banknotes the polymer substrate is more durable, harder to tear, more resistant to folding, more resistant to soil, have a higher resistence to micro-organisms and is waterproof. Producer is Innovia Films. Early 2010 over 30 countries have adopted this substrate. The next Canadian banknote series will also be printed on polymer.

Recently multi-layer substrates are introduced, alternating paper and synthetics.
Such hybrid banknotes have strong intrinsic properties. There are two variants:
1) Film-paper-Film (named Hybrid, produced by Papierfabrik Louisenthal and ArjoWiggins),
2) Paper-film-paper (named Durasafe, produced by Landqart).

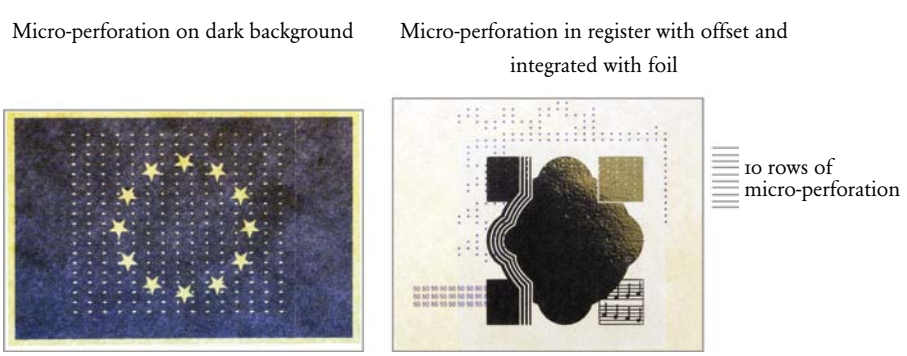
The first Hybrid banknote was issued in 2008 by the central bank of Swaziland.

Appendix 3
Internal and add-on features (1985)

In the 1980s the security printing industry started developing a wide variety of semi-finished security features. Examples are fluorescent fibres, security threads, foils and special luminescent features. Such features are *add on features*; semi-finished products delivered by an external factory, like features on a role, in a box, can or bottle. An *internal security feature* is one that can only be produced *inside* a security paper mill or printing works in the course of the actual production process, such as a watermark or intaglio gravure. The micro-perforation of a banknote, first used in Swiss banknotes (CHF 50, 1995) is a quite recent internal feature (Figure A3.1).
Due to this development internal and add-on features were recognised by DNB next to the discrimination between intrinsic and extrinsic features (see Appendix 2). Internal and add-on features terminology was first used by Hans de Heij and Dr. Peter Koeze (both DNB) around 1985. A description followed in 2005 [69, 156, 175].

Internal features preferred over add on
Add-on features like a security thread or a chip may be removed from a banknote. The residue of add-on features like pigments might be recovered from the banknote after destruction, while this seems less possible for internal features. Finally, the

Figure A3.1



Left: The micro-perforation is good visible on the dark background of the EU-flag.
Right: The micro-perforation is in register with similar 'dots' printed in offset. Furthermore, the micro-perforation is overlapping with the foil (integration).
Studies initiated by DNB (De Heij) in 2003 in co-operation with Orell Füssli [74, 76].

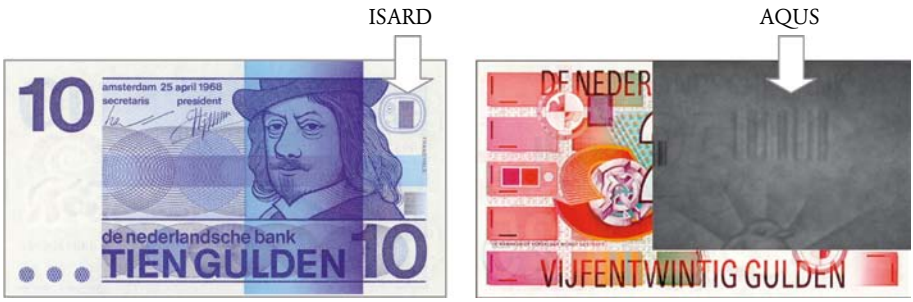
physical and chemical resistance of add-on features such as foil usually perform less than the internal features.

Add-on features like foil are usually introduced from another industry. An example is holographic materials, which are widely used in fancy postcards and the packaging industry, lending appeal to gift paper and cosmetics alike. The security of the hologram has suffered because of this worldwide proliferation of holographic technologies. Another disadvantage of such features is that they add a link to the production chain. Any additional link will add transportation movements, security requirements and confidentiality clauses and therefore costs.
Semi-finished products are, in principle, less suitable as bearers of security features, since they will be delivered from outside to the security paper mill or printer.

ISARD and AQUS
Under this definition, the AQUS and the ISARD are internal features (instead of extrinsic). Finally the sorting machines, introduced in 1981, were to have three security feature detectors: AQUS (barcode watermark), ISARD (intaglio line pattern) and an OCR-B number reader (see Figure A3.2). The ink of the banknote number could be either magnetic or non-magnetic.

Intaglio pattern for a detector: ISARD
Which came first, the chicken or the egg? This is a recognisable statement for any new banknote feature to be detected by a detector. In both cases of ISARD [77] and AQUS there was first the banknote feature, although there were already ideas about the principles of detection.
An intaglio pattern of straight lines was for the first time printed on the NLG 10 banknote issued in 1971. A detector was developed by DNB in cooperation with the

Figure A3.2



Left: first banknote with ISARD, the NLG 10/Frans Hals issued in 1971.
Right: NLG 25/Robin banknote with barcode watermark AQUS, issued in 1990.

TNO/TPD Institute of Applied Physics. The prototype of the Intaglio Scanning and Recognition Device (ISARD) was built in 1971. The ISARD uses reflected light to check for the presence of intaglio printing on the banknote. Later the element of straight lines on the banknotes was also called 'the ISARD' (and by designer Oxenaar 'the television screen'!).

Barcode watermark: AQUS

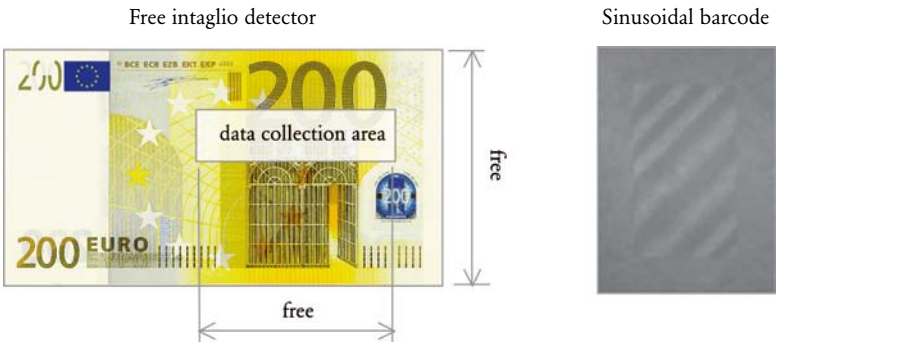
The barcode watermark followed a similar development sequence. Based on a proposal of Karel Schell (Joh. Enschedé), the first bar watermark was introduced in the NLG 250 banknote issued in 1986 [23]. The watermark, created during the paper production process, may be heavily overprinted and hence be made more or less invisible to the public.

Just as for the ISARD, DNB asked TNO/TPD to develop a detector. The prototype dates from 1983 and was called the AQUa watermark reading System (AQUS). Transmitted light is used to check for the presence of the bar watermark in the banknote paper. Here also the element in the banknote was later called 'the AQUS'.

ISARD and barcode watermark in euro banknotes

Both internal features, ISARD and barcode watermark, became part of the euro in 2002. After just a few years, these features were no longer actively used, bringing the life cycle of the ISARD to around 35 years! In fact, it began a second life as a

Figure A3.3



Left: conceptual proposal for a so called 'free intaglio detector'. Instead of the fixed intaglio line element shown in Figure A3.2 any intaglio print area may be used for detection. All relief in this area will be 'added up' and the sum total has to be above a given threshold value. The sum total of all relief on a counterfeit will stay below this threshold. The 'data collection area' area should also be freely adjustable. The first concept was proposed in 1998 by Koeze (DNB) and elaborated further by De Heij in 2003 for a discussion with De La Rue Currency [56].
Right: The initial idea is to transform the sharp-edged bars into sinusoidal waves. Wavelength variation of the bars exploits the characteristics of the mould-made paper machine to the maximum! Optical transmission detection in IR range. Sample produced by Arjo Wiggens (2004). Based on DNB EU patent on BCWM (2003) [54].

nail scratch feature on the euro series [81]. The bar watermark in the euro is quite different from the Dutch AQUS. It takes much more space and doesn't use the density gradation of the AQUS. For the public this euro bar watermark is more obvious and counterfeiters are often imitating it.
Since these features are created with the basic banknote production tools – that is, the paper machine and the intaglio press – these features still have potential and could be further developed as proposed in Figure A3.3.

Taggants
A relatively new development are the so called taggants, specific compounds added to the banknote paper or ink and therefore classified as add-on features. Taggants are a subdivision of banknote markers like numbering or magnetic codes. When engineered at a molecular level, these taggants can provide a unique signature when probed with a suitable reader. There are taggents that are unique to each individual banknote, which virtually eliminates the possibility of mass-producing counterfeits. Up to date taggents are typically manufactured using complex rare earth-phosphor compounds that are hard to source. Their production may also be based on different technologies, e.g. optical, nano or DNA. Since 2004 customized genetic codes can be produced by extracting DNA from an infinite selection of plants (botanic DNA). Taggants are known security features, but their application in security products has remained limited. They could be introduced in banknotes as a retail feature, since today they can only be read by specialised devices operating at slow speed or at standstill. For the same reason, such features could be used as a Counterfeit Deterrent System feature (CDS) or as a forensic feature. Those readable by high-speed detectors could suit the sorting machines of central banks. Each denomination could have a code of its own or even every banknote could receive a unique code.
Although classified as add-on features, taggants have also internal characteristics since they have to be dissolved in paper or ink.

It would seem that the security industry focuses too much on disruptive add-on technologies especially for detectors as is suggested by Table A3.1.
Considering the trend that counterfeiters mainly try to fool the retailer and therefore mainly imitated retail features, a constant development of improved and new retail security features should receive priority.

The NRC also reported on 'technology fields' for innovative features for future banknotes. Colour change in response to pressure is a case in point. The greater the pressure, the greater the shift in the colours [102].

Table A3.1

Banknote production process	Security features	
	Internal	Add-on (delivered as semi finished product)
1. Paper	Mass variations within the paper (watermark, barcode watermark)	Security thread, micro chips (RFID tags), synthetic fibres (e.g. UV), other types of fibres like thin steel, luminescent pigments, other pigments, markers/taggants like e.g. botanical DNA
2. Foil (hot stamping)	Glue, special unique colours, additional layers, nanotechnology, e-beam made holograms (high resolution)	Plain foil with or without hologram
3. Thin-foil (cold transfer technique)	Patch changing colour (1989)	-
4. Silk screen/ rotogravure	Extremely small two dimensional signatures	Magnetic pigments, pigments for Optically Variable Inks (OVI), iridescent inks, liquid crystal inks, metameric optically variable inks
5. Offset	Spectral values (layers of ink), small silicon printed on wafer *	UV fluorescence, IR
6. Intaglio	Ink mass variations	Magnetic pigments, OVI pigments, taggant protected ink (i.e. botanical DNA)
7. Numbering	Number + database	Magnetic pigments, OVI pigments
8. Perforations	(Micro)perforation patterns through finished banknote	-
9. Cutting	Shape of edges, notches	-

Overview of several internal and add-on features that are or could be used in banknotes (the list is far from exhaustive).

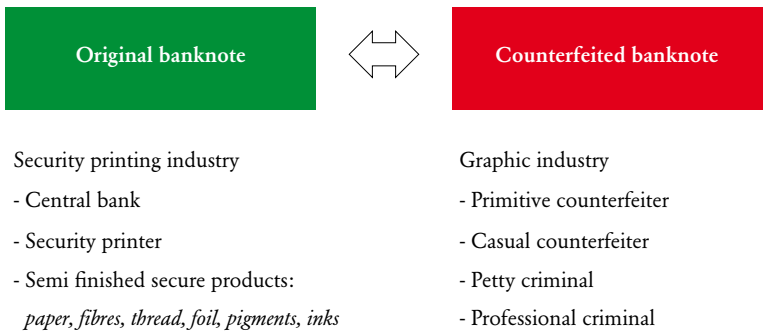
* Recently first prototypes were printed of flexible displays. Individual pixels are printed by using inorganic and organic Light Emitting Diodes (LED). The organic LED's (OLED) are printed using wafer techniques.

Appendix 4
System approach (1991)

In 1991 DNB presented a counterfeit model, based on the principle that a reproduction of an original banknote will never be identical to the original. The counterfeiters have no access to the banknote security industry and have to use reproduction tools of the reproduction industry, as indicated in Figure A4.1. The quality of the reproduction will be different from the original.

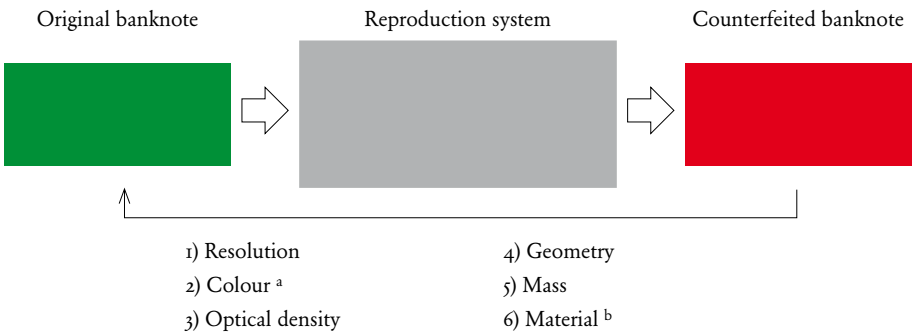
Black box model
The reproduction system of the counterfeiter is seen as a black box. The basic idea behind this model is a system approach. Any reproduction system takes an original banknote as input and outputs a reproduction. The black box is defined in terms of physical and chemical dimensions such as resolution, colour, opacity, geometry, mass and materials. The model was first applied by Dr. Peter Koeze and Hans de Heij in 1984 for the development of new security features like the 'resolution indicator', to be explained in section A4.1. In 1989 the model was successfully applied in an internal report to the DNB Board to protect future NLG banknotes against colour copy machines. This analysis was basis for the innovative NLG 100/Little Owl, the first Dutch note also protected against colour copying, issued in 1993 [28].

Figure A4.1



Schematic presentation of the producers of original and counterfeit banknotes.

Figure A4.2



a = including UV, IR and other spectral features
b = including magnetism, conductivity

The reproduction system is regarded as a black box that reproduces six physical and chemical dimensions found both in genuine banknotes and in counterfeit notes.

Outside DNB the model was first introduced at the 1991 meeting of the Paper Committee of the Banknote Printers' Conference. One of the conclusions of this paper is that 'System analysis by physical and chemical dimensions of reproduction systems leads to a clear development strategy for new security features.' [33]. Over the years the system was developed further [37, 72, 134, 156, 175] and today the model may be described as shown in Figure A4.2. The six key dimensions are specified in more detail in Table A4.1.

Reporting on counterfeits based on black box approach
The black box approach also permits real measurements between original and counterfeits. An example of this is provided in Table A4.2

Table A4.1

Dimension	Units
1. Resolution	dots/inch, line pairs/mm
2. Colour	CIE-diagram (Lab-values), colour travel graphs
3. Opacity	density (log 1/R), gloss measurements
4. Geometry	mm, µm, nm (e.g. register)
5. Mass	paper weight (g/m²)
6. Material	magnetism, taggants, steel fibres, polyester thread, aluminium foil

Overview of the six dimensions used in the system approach and the corresponding units (overview of units is not exhaustive).

Table A4.2

Gloss original hologram	Reproduction	Gloss reproduced hologram
512	Sample A	283
	Sample B	162
	Sample C	709

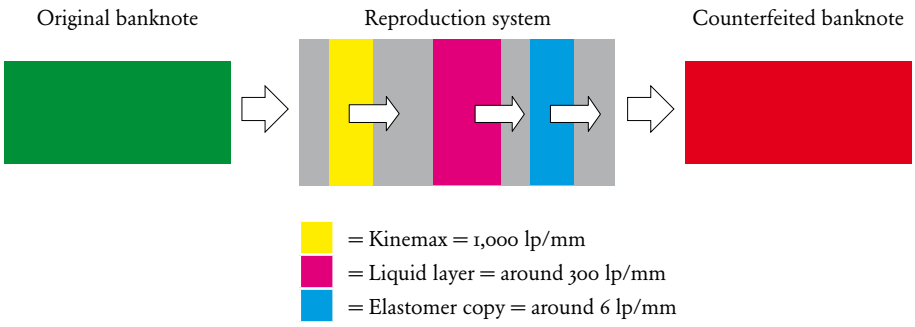
The gloss of the original hologram is compared to three different hot-stamping imitations A, B and C using different foils and fixed on mat adhesive tape. The gloss of the reproduced hologram is measured in 'gloss units' [70, 72].

Sustainable competitive advantage of real notes over counterfeits

The motto of central banks, Interpol, Europol, Secret Services and many others within the security business is to stay one step ahead of the counterfeiters. In this atmosphere one may encounter warrior language such as 'the weapons of choice in the fight against counterfeiting', although milder terms like 'robust security' are also used. Modern managers would probably phrase it as: 'We are looking for sustainable competitive properties of the real note over the counterfeit notes'.

How to find such properties? Here the favoured system approach proved to be helpful. A new security feature to be considered for use in a new banknote must have physical and chemical limits higher – or lower – than the boundaries of commercially available reproduction systems. Consider, for example, that a micro printed element on a banknote should have a *resolution* higher than the resolution of a standard copy machine. Or take the iridescent planchettes made of a *material*

Figure A4.4



Security system (or security chain) in which the weakest link determines the overall security of the document. System approach depending on the weakest link. Lp/mm = line pairs per mm. This is explained in section A4.1 Resolution.

(polyester or acrylic) that is not available in (almost) any commercially available reproduction system.

Weakest link
Studying the key parameters of a reproduction system one should identify the weakest link, as is shown in Figure A4.4.
Although current off-the-shelf dot matrix systems have a high resolution, this does not mean that an imitated hologram will be that sharp. The elastomer copy process will reduce the resolution to just 6 lp/mm.

Keep track of changing key specifications
Now what a central bank has to do is to keep track of improved and/or new technologies. This is an ongoing process. The last three decades have delivered overwhelming innovations, as phrased by security product designer Joost van Roon: 'Scanning, imaging and printing have rapidly evolved. Techniques that were beyond anyone's imagination thirty years ago are commonplace today.' [137]. Personal computers became both cheaper and more powerful in the 1990s. Very affordable image-editing software, desktop scanners and printers became available and delivered good quality. Today you may buy a 4,800 dpi ink jet printer for just 60 euro!

Since the introduction of 'home scanners' and 'all in one devices' no new reproduction technologies appears to have emerged. However, these new technologies are used for about 20% of the euro counterfeits. Since the majority of the fake euro banknotes are printed in offset, it seems that the central bank could be inspired by the older, dedicated security features against offset printing, introduced during the era 1920-1980 of the offset printed counterfeits (Table A4.3).

Table A4.3

Historical counterfeit threats and the reactions of central banks

Threat	Year	Central bank's reaction	Dimension
-	1282	Watermark (line watermark)	Density
	1661	First banknote with watermark (Stockholms Banco)	Density
	1694	Marbled paper (GBP)	Material
	1694	Gravure printing using copper plates, maximum 10,000 passes (GBP)	Geometry
Changing value of real notes	1797	Anti erasure feature: an elaborate £-sign in front of the amount (GBP)	Geometry
Carving	1809	First forgeries. Number by letter press (GBP)	Geometry
Original banknotes not uniform	1819/1836	Plate Transfer Method (hardened steel mother plate) invented by Jacob Perkins	Geometry
	1829	First multi-tone watermark (Banque de France)	Density
	1839	Electrotype invented by Boris Jakobi	Geometry

Table A4.3 *continued*

Historical counterfeit threats and the reactions of central banks

Threat	Year	Central bank's reaction	Dimension
Photography	ca. 1850	Introduction of colour	Colour
	1855	Shaded watermark (GBP)	Density
	1867	Security thread (silk), Crane	Material, density
	1876	First photographic forgery discovered (GB)	-
Offset printing	ca. 1920	Line printing in alternating colours (up to 3 lines)	Geometry
	ca. 1925	First see-through register (RZ press)	Geometry
	1928	First banknote introducing colour, red for 10 shilling, green for 1 pound (GBP)	Colour
	ca. 1960	Simultan press (see-through register)	Geometry
	ca. 1970	Introduction UV features	Colour
	ca. 1980	Magnetic particle printing (e.g. in number)	Material
	ca. 1980	Introduction IR features	Colour
Digital presses	ca 1990	Computer to plate	Resolution
Colour copy machines	1988	Polymer banknote with transparent window and foil with 'pixelgram', ASD 10	Material, density
	1989	Foil with hologram, ATS 1,000	Material, density
	1989	First OVI in intaglio, THB 60, commemorative note, issued 1989	Colour change
	1989	Thin-film patch (OSD) by cold transfer technique, turning from gold to green (CAD 50, issued 1989)	Density, colour
	1990	Windowed thread (Stardust), GBP 5, 20	Geometry, density
	1991	Spectral features (M-feature), DEM 10	Material
	ca. 1994	Common Mark/Security Circles	Geometry, density
Home scanners	ca.1990	Counterfeit Deterrence Systems	Geometry
		Simultan presses with 4/4, usually 3 plates dry offset and one wet.	Resolution
	1992	Silk screen, pearl lustre, NLG 100, 1992	Density
		Iridescent planchettes, NLG 100, 1992	Density
	1995	Micro perforations, CHF 50, 1995	Geometry
All in one devices	ca. 2000	Transparent window in cotton banknotes, BGL 100, commemorative note, issued 2005	Material, geometry, density
	2007	18 mm wide security thread with eliptical clear window in paper, FJD 100	Material, geometry, density
	2008	Hybrid banknote paper: film-paper-film SLZ 100 and 200, commemorative note, 2008	Material
	2009	Watermark with large highlight area (pixel area), MXN 200 commemorative note, issued 2009	Geometry, density
	2012	Hybrid paper: paper-film-paper (new Swiss banknotes?)	Material

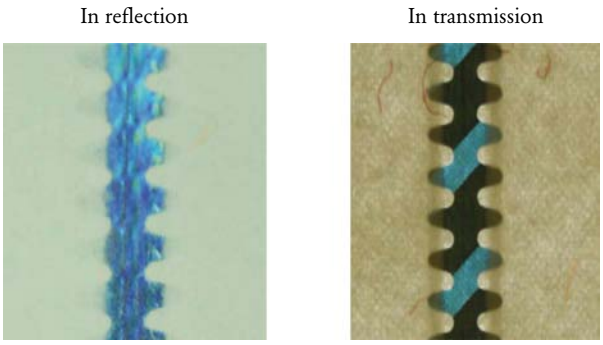
Overview of several historical threats and the reaction of the central banks.

With no obvious new print technology platform in the offing, innovation lies in the improvement of features. A case in point is the introduction of digital engraving around 2000, which ushered in a new phase in a long gravure tradition.
Table A4.3 provides a short and incomplete historic overview of counterfeit threats and the reaction of central banks. The aim of the new protection, like resolution, geometry or colour, is also indicated. It seems that for the first time, the development of new features, such as a transparent window in a cotton banknote, is not specifically aimed at outperforming newly arriving reproduction methods.

Predicting quality of counterfeits
Whenever a new ink jet printer, new imaging software or a new digital press is introduced, the key specifications of the black box will change. An example is the particle size of the pigments in colour copy machines. The pigments of the first generation of colour copy machines (1980, Canon CLC 1) were limiting the resolution, but did deliver some relief to the copies, quite similar to real banknotes. The third generation of copy machines used much smaller pigments (1994, Canon CLC 800) leading to higher print resolutions. The relief disappeared, to the relief of the central banks!

With this system approach it is now even possible to predict the quality of counterfeits. When the colour gamut of any reproduction system is increased, security features based on colour will lose strength. The new banknote under development should receive better key specifications on 'colour' than the latest graphical tools can deliver. An example is the chip industry; they go for higher and higher resolutions. In 2010 Intel introduced the 32 nm-chip and for 2016 a 11 nm-chip is announced (11.10^{-9} !).

Figure A4.5



The Wings security thread shows up quite differently in reflection and in transmission (Goznak, 2007).

Provides insight in dimensions of new features
Another advantage of the system approach is the quick insight it offers into the basic level of defence of a new feature. The Wings security thread for example can be defined in terms of geometry and density (Figure A4.5)

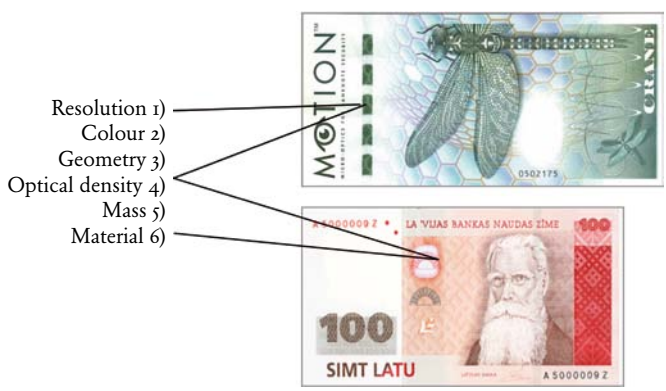
Wide windowed threads, registered foil stripes, bleeding intaglio:all geometry
Windowed security threads were first introduced in 1990 by the Bank of England. The width of these 'Stardust threads' was 1 mm. Around the year 2000 paper suppliers were able to incorporate threads with a width of about 4 mm. These days' windowed threads may be as wide as 8 mm! Clearly an example of improving the geometry parameter of this security feature.

The foil stripes on the low denominations of the euro series are so called 'continuous stripes', since the holographic images are not fixed to a certain position. Since around 2005 it is possible to produce 'registered foil stripes', again an example of improvements on the geometry parameter.

With the 'Computer to Intaglio Plate' technology it is possible to print the gravure up to the edge of the banknotes. With the chemical etching technology this was not possible, except when the notes would be cut out of a sheet with a double cut instead of a single cut. So *off-running* or *bleeding intaglio* print is also an example of a geometry improvement.

Security micro-optics: resolution!
Also, the real security of the micro-optic features is not only the lenticular lenses (geometry), but especially the high resolution of the electro-photographic printing underneath these lenses (around 5 µm or 100 lp/mm, see Table A4.4).

Figure A4.6

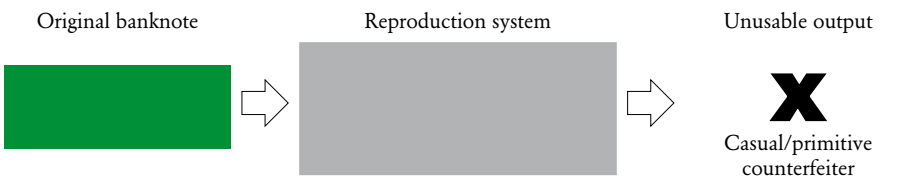


Micro-optics 'Motion' in promotional banknote, 2005. Diameter magnifying lenses: 30 µm, focal point 20 µm. Resolution micro printed symbols: 5 µm (or 100 lp/mm).

Latvia LVL 100 banknote, issued in 2007. First cotton banknote with a transparent window (after the Bulgarian BGL 20 in 2005, which was an occasional issue).

Characterising the micro-optics feature and transparent window feature with the system approach.

Figure A4.7



Basic principle of prevention of banknote reproduction: no output.

A transparent window in a paper banknote is mainly a matter of material and optical density (Figure A4.6). But the model also serves to expose the weak elements in an existing banknote, e.g. the see-through and (intaglio) *portraits*, losing territory in, respectively, the geometry and resolution dimension.

System approach applied on Counterfeit Deterrence Systems
Counterfeit Deterrent Systems (CDS) are generally aimed at preventing counterfeiting by the use of standardized of the shelf reproduction techniques. In 1990 the Bank for International Settlements (BIS) took the initiative to develop such systems. The principle of CDS may also be explained by the system approach, as is done in Figure A4.7.

Two generations of CDS
Today there are two generations of deterrence features. The first was aimed at colour copy machines, introduced to combat the threat posed by colour copy machines. The second CDS generation is directed against the casual counterfeiter trying to manufacture counterfeits at home and introduced in the euro banknotes in 2002.
Both generations have their own feature and both are being used. Both features centre on the use of existing banknote production machines and should be applicable in existing banknotes without much change. The idea behind CDS is also to protect people of becoming a criminal by copying or printing banknotes at home.

Quote from ECB report
The ECB reports regularly on CDS systems. For instance, in October 2007 [99], it wrote, 'The effectiveness of a counterfeit deterrence system that prevents personal computers and digital imaging tools from capturing and reproducing the image of a protected banknote has had a significant impact on the counterfeiting techniques applied over time. The Central Bank Counterfeit Deterrence Group (CBCDG), in which the ECB participates, along with many other central banks around the world, aims to promote the voluntary adoption by hardware and software producers of a

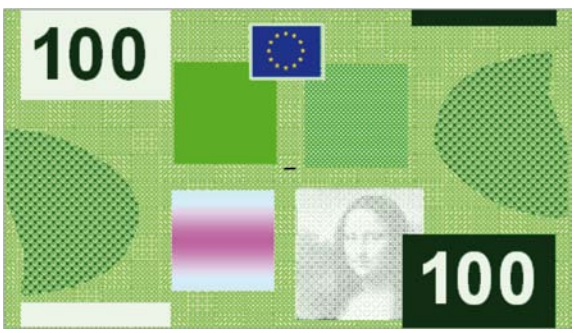
counterfeit deterrence system to prevent the use of PCs, digital imaging equipment and software in the counterfeiting of banknotes. In the early days of the euro banknotes, a significant proportion of the counterfeits was produced with the aid of inkjet and laser printers, as well as colour copiers. However, the effectiveness of CBCDG developments has caused the volume of counterfeits produced by PC-related techniques to decline considerably, while that of counterfeits produced on the basis of traditional printing techniques has increased. Nowadays, approximately half the counterfeits detected and withdrawn from circulation were those produced with fewer than ten distinctly identifiable sources of traditional printing technology.'

Too much space and pale banknotes

CDS features are in need of space, which has a clear negative effect on the overall perception of the banknote. The space attributed to CDS in the euro 50 banknote is close to 55% of the surface. In contrast, the public security features occupy only around 15% [108]. Its large space requirements give the banknote a rather blurred and pale impression. Now the public is known to disapprove of pale banknotes [81, 94]. It seems that existing CDS-features have a strong negative influence on the heuristic quality of the banknote and is from this point of view contra productive to a secure banknote! Indeed, they may accept a more colourful counterfeit note for the real thing!

If the banknote designer would be able to reserve space for the CDS-features in advance, the pale colours and blurring can be made a natural part of the design, e.g. as is done in pre-set lay-outs like the one shown in Figure A4.8. Another policy is to improve the CDS-features on their shortcomings.

Figure A4.8



Conceptual banknote, using the background for CDS-features. This design is optimised for the partially sighted: clear large numerals, alternating between positive and negative against different geometric patterns. Secure tactile patterns are included at the short edges providing a codification for the blind. Maximum attention for the 4 security features in the centre (but not on the folding line). One security feature has a secure purple colour. Design by author (2009) [148, 181].

A4.1 **Resolution**

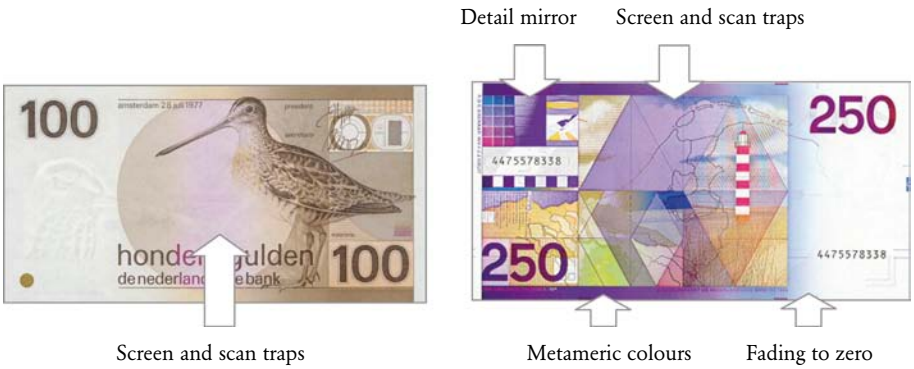
For a better understanding of the system approach, resolution is explained here in more detail. By tradition, banknotes are printed with continuous lines instead of dots. Replication by scanners or copiers may be recognised because it consists of dots specified in dots per inch (dpi), in screen values or in pixels or in any other way. If we want to compare the resolutions applied in banknote production and in the reproduction industry, both must be expressed in the same units. For banknotes, line pairs per millimetre [lp/mm] are preferred.
The finest elements a banknote printer may print are lines of 30 µm wide. If the area between two printed lines is also 30 µm, the line frequency of these lines may be calculated as 16.7 lp/mm ($(10^{-9}$ lp/$(30 + 30).10^{-9}$ m) = 1/60 lp/m = 16.7 lp/mm). A resolution often used is 300 dpi, which is equivalent to 5.5 lp/mm.

Screen and scan traps
Over the decades several security features were developed based on printed lines, such as lines in alternating colours, as will be explained in Section A4.2 on dry offset printing. A review of all kind of security features that can be printed by lines and also dots is provided by Ruud van Renesse in 2002 [51]. One of the classes defined is 'local screen modulation', subdivided in screen- and scan traps. Screen traps are dedicated line patterns that interfere with the screens used to reproduce a banknote with moiré fringes as a result. Scan traps are defined as printed patterns that form aliasing effects when the feature is scanned with similar frequencies as for example the frequency used in the scan trap (eigenfrequency).

Screen traps using line patterns were first applied in the NLG 10/Frans Hals, issued in 1971. Later Dr. Peter Koeze (DNB) found that for being effective, the line width of the printed and the unprinted line should be exactly the same [8]. The frequencies selected for the screen traps were similar to the frequencies used in the reproduction systems used by the counterfeiter, e.g. screen 45 or screen 60 and are therefore also scan traps. Both, screen and scan traps, are security features meant to trigger the public's attention. When screen- and scan traps are printed too small, people will not notice them. That is why a large circle was printed on the NLG 100/Snipe (Figure A4.9). Disturbance by interference (moiré patterns) or by aliasing effects (i.e. eigenfrequency) would disturb the homogenous circle so was the design idea. Today such features are not considered to be public features, but *trigger features* or level 0 (see Chapter 2). Such trigger features make the counterfeited note look blurred, which triggers people to check for example the watermark and other public security features [81, 94].

The NLG 100/Snipe was the first banknote with screen traps based on line pairs with exactly equal line widths (a) and (b), leading to 50% coverage (Figure A4.10).

Figure A4.9

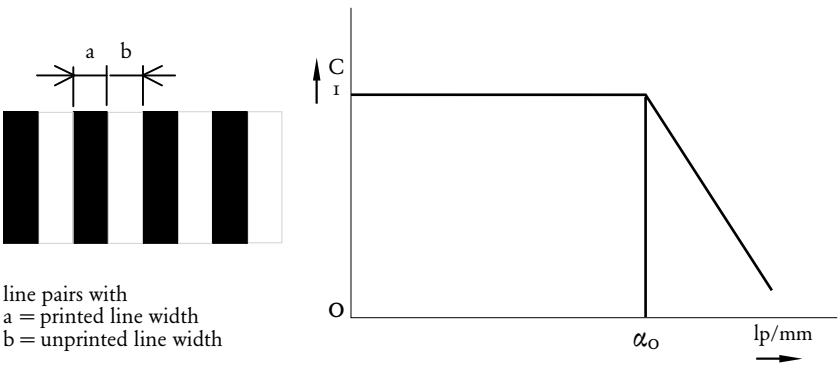


Left: NLG 100/Snipe with screen and scan traps, issued in 1981.
Right: NLG 250/Lighthouse (reverse) with 'resolution indicator' or 'detail mirror' and screen and scan traps, issued in 1986.

Unfortunately, the best line pair specification the printer was able to print was between 40% and 60% coverage, which made the screen traps less effective.

Cut-off frequency
A second defence line is based on the principle that a reproduction system will not be able to reproduce line frequencies above its eigenfrequency (Figure A4.10). In fact, the Nyquist theorem explains that the sample frequency of the system must be at least twice the resolution of the printed matter (Harry Nyquist, 1929).

Figure A4.10



Left: line pairs with line width (a) and an un-printed line width (b). When a = b, the coverage K of the lines is exactly 50% (K = a/(a + b)).
Right: Modulation Transfer Function, where cut-off frequency is α_o and C is contrast.

Table A4.4

Reproduction system	Cut-off frequency [lp/mm]		Cut-off frequency [lp/mm]
Newspaper photo (screen 25)	1.25	Colour copy machines (720 dpi)	13.2
Printed photo, grey scale (screen 48)	2.4	Intaglio press (laser engraving)	14
Printed photo, colour (screen 60)	3	Direct colour printing (800 dpi)	15.7
Human eye at reading distance	**5**	High quality laser printers	50
Flatbed ink-jet printer (300 dpi)	5.5	Daguerre photo print	100
Stamp in photogravure (screen 125)	6.25	Digital-image capture systems	50 -100
360 dpi	6.6	High quality scanner	100
Stochastic screen (400 dpi)	7.9	Electro-photographic systems	100
Ordinary digital photo print	8.3	Graphical film	200
All-in-one device (copier)	10	Imaging software (10,000 dpi)	200
Digital press (600 dpi)	11.1	Perfect lens	700
Intaglio press (chemical etching)	12		

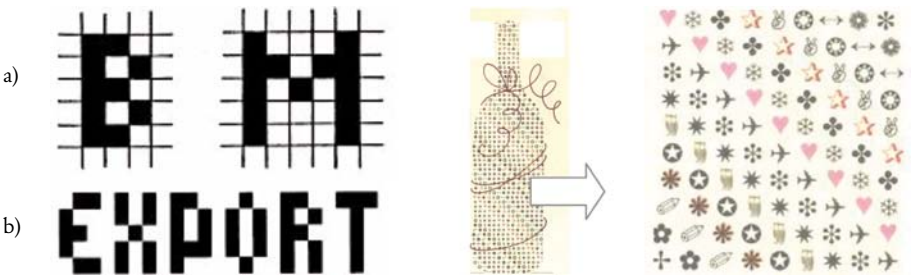
Characterisation of reproduction systems by resolution in terms of line pairs per millimetre.

Table A4.4 provides an overview of several typical cut-off frequencies of printing units and imaging software, provided in lp/mm. Not every new technique achieves better performance than previous ones. A photograph taken about 200 years ago, a Daguerreotype, typically has a pixel size of about 0.5 µm (or 100 lp/mm), the size of a particle of silver amalgam, while a standard digital photograph today would have a pixel size of 6 µm (or 8.3 lp/mm).

Resolution indicator and micro-text (1986)
DNB first applied the black box model for the development of new security features in 1984, when it designed a so called 'detail mirror' [13]. Such an element would indicate the resolution of the counterfeiter's equipment, which is of course expected to be lower than that of the security printer. The detail mirror was introduced in the NLG 250/Lighthouse, issued in 1986 (see Figure A4.9).

The system approach may also contribute to banknote security design. An example is the introduction of intaglio micro-printing for that same note. According to the printer, the 0.2 mm letter height proposed by DNB for the NLG 250 could not be achieved, but DNB proved that it could, with the letter font shown in Figure A4.11a) and b) [20].
During the development of the euro banknotes a similar discussion was done. To be able to print islands within the map of Europe their size should be at least

Figure A4.11



a) Micro-letters proposed by DNB for the NLG 250/Lighthouse based on the cut-off frequency of the intaglio press.
b) The word 'EXPORT' based on the letter type proposed in a).
c) Instead of micro-text, designs may use micro-symbols, combined here into the shape of a bottle.
d) Detail of c).

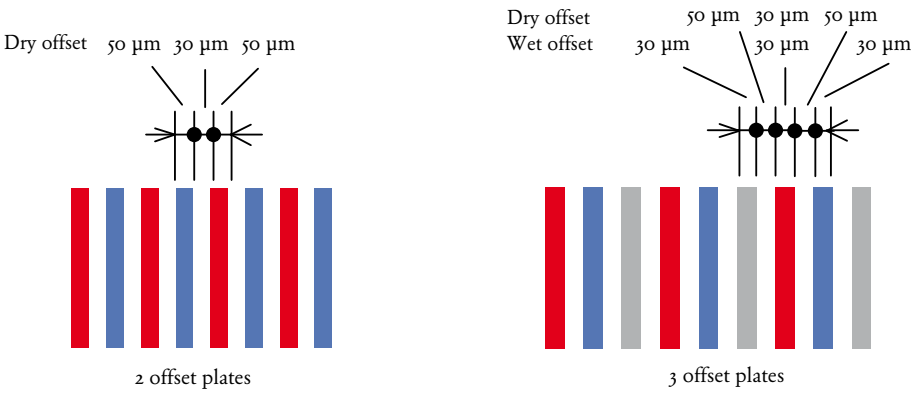
400 km². In reality islands of much smaller size could and are also printed on the euro banknotes like e.g. Texel an the Netherlands (170 km²).
Where several languages have to be used on a banknote, central bank and designers tend to limit themselves to numerals (e.g. '50') or letter designs (such as 'EURO'). Micro-symbols as presented in Figure A4.11c) and d) may be used to create new images, which are more difficult to counterfeit than letter fonts (which are widely available).

A4.2 **Dry offset printing**

This section is specifically dedicated to dry offset Simultan printing, a banknote printing technology which is outdated, in the author's opinion, but also by others, as will be explained in this section.

RZ-offset printing
Around 1920 offset print became widely available, gaining market share from letterpress printing. Offset colour printing uses 3 or 4 screens or plates (blue, cyan, yellow and/or black). This technique was – and still is – based on dots and the reaction of the central banks was to base their banknotes on line work instead. The answer for DNB was the introduction of two-colour offset presses delivered by Roland, the Roland *Zwei Farben Presse* (RZ press), ready for use in 1926. Basic idea of these presses was line print (instead of dots). The technique allowed two lines to be printed in two different colours with white lines in between, as illustrated by Figure A4.12. Lines in each colour were printed from two separate plates. The register between the two plates completed the security of the line work. A typical example from NLG banknotes of this press is shown on the left side of Figure A4.13.

Figure A4.12

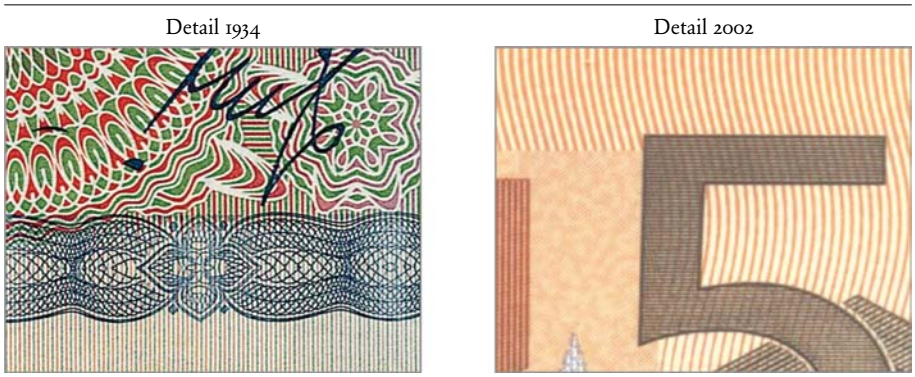


Security principle of alternating line colours, based on two colours (left, since around 1925) and based on three colours (right, since around 1960). Smallest linewidth in dry offset 50 µm (print) and 30 µm (white line) and in wet offset 30 µm (print) and 30 µm (white line).

Simultan printing

The successor of the RZ-press at security printer Enschedé is the Simultan press. These innovative presses were first introduced in the 1960s. A Simultan press is a brand name for a printing press manufactured by Koebau-Giori, a well known company in the security printing industry. This press collects the print of several separate images – all images on one side – on a rubber 'blanket'. The same is done for several separated images on the reverse side of the banknote. The registration of the offset plates within one side is high, today less than 3 µm. Next these collected

Figure A4.13



Two examples of line work in banknotes.
Left: typical detail of line work, including guilloches, in NLG 10/Greybeard, issued in 1934 (design by C.A. Lion Cachet).
Right: typical detail of line work in EUR 50, issued in 2002 (design by Robert Kalina).

Figure A4.14

a) Sight NLG 1,000 b) Puzzle number CAD 100 c) Puzzle number EUR 10

Three designs of a see-through register.
a) See-through register, variant *sight of a weapon,* NLG 1,000/Lapwing, issued in 1994. The overlap of the egg of the lapwing between the front and reverse is camouflaged by the lines in the visor.
b) See-through register, variant *puzzle number*, CAD100, issued in 2004. The overlap between the front and the reverse is clearly visible (first issue was CAD 10 in 2001).
c) See-through register, variant *puzzle number*, EUR 10, issued in 2002. The overlap between the front and the reverse is clearly visible.

images are printed in one run – *simultaneously* – on both the front and the reverse of the banknote paper, creating a 'perfect' register between front and reverse. This register between front and reverse could not be made with other commercial available presses. In fact one plate on the front is printed in register with one plate on the reverse with a tolerance of +/- 0.10 mm (so not in 'perfect register' as often declared by central banks).

The see-through register is a typical geometry feature and was designed as a sight in the Dutch banknotes since 1980 (see Figure A4.14). The see-through registers in the Canadian dollar banknotes and in the euro banknotes received a similar design (Figure A4.14b and A4.14c).

Dry offset has lost its value
In traditional offset printing, ink separation is based on the repulsion between ink and water (or *wet offset*). The printing plates of these new Simultan presses did not use water, but separated ink and non-ink areas by using a slight relief, in fact a variant of letterpress. Therefore the Simultan printing technique was called *dry offset*. This slight relief creates *line broadening* (or *dot gain*).
These days the Simultan press has lost its added value. Lines in alternating colours and iris print, the two typical dry offset features, are no longer a hurdle for the counterfeiter and are less used (e.g. Figure A4.13, right hand side, detail of the euro 50 banknote). Also the fit of the front and the reverse, the see-through register, no longer provides a defence against current reproduction techniques.
The main drawback of the Simultan press is its low resolution (around 8 lp/mm); most commercial presses can do better. Also the line-broadening because of the slight relief of de dry offset plates is today a disadvantage for a security product like

Figure A4.15

Muti Variable Colour (MVC) security feature in Russian rouble banknotes, introduced in 2004. When tilted, rainbow colours appear in the area printed under the denomination numeral.

a banknote. As a consequence there are no new public features using the techniques of the Simultan press, except the Multi Variable Colour feature.

Multi Variable Colour
In 2004 a new public security feature was introduced using the three offset plates of the Simultan press. The feature is called Multi Variable Colour (MVC) and is part of the Russian 100 rouble banknote (Figure A4.15). The MVC is a smart construction making use of the high registration between the three offset plates (on one side of the banknote). The MVC feature shows all kind of rainbow colours when the banknote is tilted.
A variant of MVC is offered in 2010 by Giesecke and Devrient. Instead of lines, dots are printed in close register. Embossing is added to the feature in a second step, creating the so called 'PEAK pixel' feature.

Vertical and horizontal iris-printing
To create new added value for Simultan printing, Koebau-Giori has developed a new Super Simultan 5 press (2009). This press is larger and uses more printing plates (up to 6 on the front and 4 plates on the reverse). More colours can be created, coming closer to commercial printing presses. The old Simultan press could create so called *vertical iris printing* (or *vertical rainbow printing* or *split fountain printing*), a typical banknote feature where two different colours (inks) fuse together creating a gradual transition from one colour into the other. This transition is best perceived in solid printing, in full surface, without any dot or line screens. The new developed press can print both vertical and horizontal rainbow printing, named '3D iris feature'. So the improvement would, from a system approach point of view, be in the geometry of the rainbow-printing (vertical and horizontal against only vertical). Also the line broadening is reduced, which leads to a higher resolution. Still the

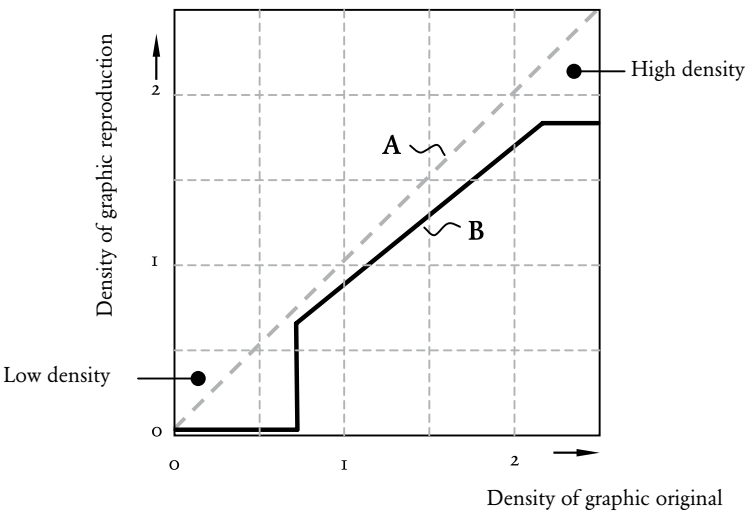
added value of this new press may be questioned, because it doesn't create new security features. People will also perceive the notes coming from this new press as closer to standard offset printing.

A4.3 **Density and tonal range**

The system approach also sparked inspiration for some new features based on colour density. The tonal range characterizes the density reproduction capacity of a graphic process (see Figure A4.16).
The upper (light) and lower (dark) boundaries of this range serve to test the quality of the reproduction process. A graphic original can be optimized to emphasize the difference between the density ranges of the original and the graphic reproduction. Lightly tinted banknote paper is a well known security feature based on low density. Other features covering the low end of the density range may use pastel tints or grey scales ranging from 0 to 5%. A typical Dutch low-density feature was the 'fading to zero' first applied on the reverse of the NLG 100/Snipe issued in 1981 (see Figure A4.9 for an example on the NLG 250/Lighthouse).

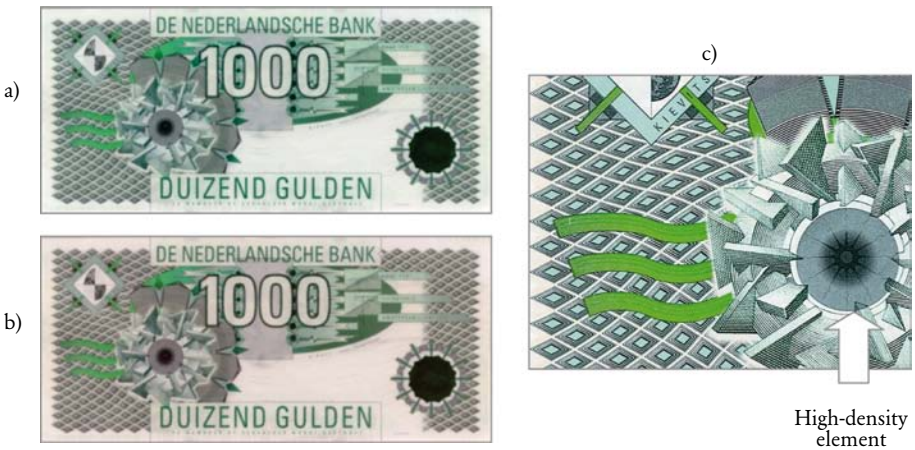
Light-red paper tint for a green banknote?
What if the colour chosen for the paper tint is complementary to the dominant banknote colour? Are people more likely to notice, for example, the absence, in a green counterfeit, of a faint red paper tint than a slightly green paper tint? An

Figure A4.16



Development model for security features based on density. Tonal range of perfect (A) and imperfect (B) graphic reproduction.

Figure A4.17



Examples of features based on low and high density.
a) Original NLG 1,000/Lapwing on white paper (issued in 1994).
b) NLG 1,000/Lapwing printed on slightly red paper (1993).
c) High density element printed in NLG 1,000/Lapwing (dark solid offset area with on top dark intaglio).

experiment was carried out by DNB with the green NLG 1,000/Lapwing as shown in Figure A4.17b and reported in 1996 [41]. Although the reddish tint was absent in standard colour copies, the idea was abandoned because the graphic designer Jaap Drupsteen did not like it. It delivers the design an old fashioned look.

High density features
Also high density features will contribute to the security of a banknote. The difference in the density must only be seen in the original and not in its graphic reproduction. Differences at the high end of the density range may be introduced for example by designing an area with overlay printing. For this purpose a grey scale from 90-100% could be suitable. The difference in density must be visible in the original but not in a graphic reproduction. The solution was found in using the same colour for both the intaglio print and the offset print. Figure A4.17c show an application of this principle. The high density properties were used again in the NLG 10/Kingfisher, issued in 1997.

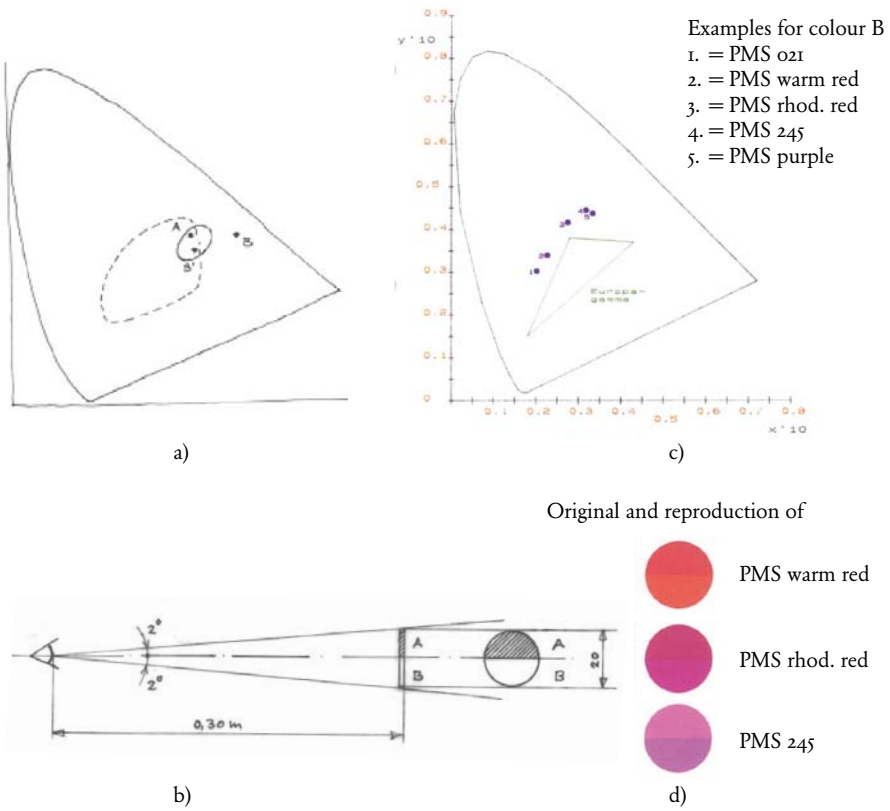
A4.4 **Colour**

The system approach also yielded some security features based on colour. Since 1850, unsaturated colours have been used in many banknote designs, including the Dutch (see e.g. Figure 58). Such colours were often based on unique ink recipes. The well known Dutch artist Anton Pieck worked and lived in Haarlem, also the

residence of security printer Joh. Enschedé. In the 1950s he regularly visited the printer because he loved all the nice dark brown ink varieties he could find there.

In 1980, unprecedented in banknote printing, a very bright colour, a highly saturated orange ink, was developed. The idea was to use a colour outside the *euro scale* colour reproduction standard. The euro scale is a standardised method for printers to reproduce a coloured picture using yellow, cyan and magenta. Black is used as a fourth printing ink.

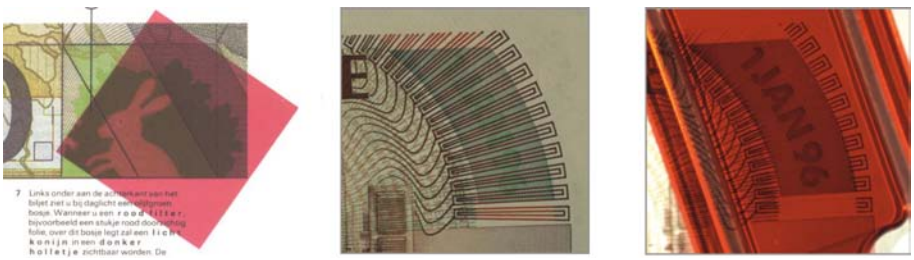
Figure A4.18



Study of colours outside the euroscale reproduction standard, 1986 [19, 21].
a) Basic principle. Within the ellipse humans will perceive no colour difference between A and B[1]. The colour B outside the ellipse will be reproduced as colour B[1], which ideally should be similar to colour A.
b) The human eye will see two different colour areas (A and B) if the diameter of such an area is about 10 mm, corresponding to an angle of vision of ca. 2° at reading distance.
c) The colours developed, plotted in a CIE-diagram.
d) Samples of the colours developed.

Figure A4.19

a) Metameric rabbit in NLG 25 b) Original SGD 25 c) One of the metameric colours becomes visible using a red filter

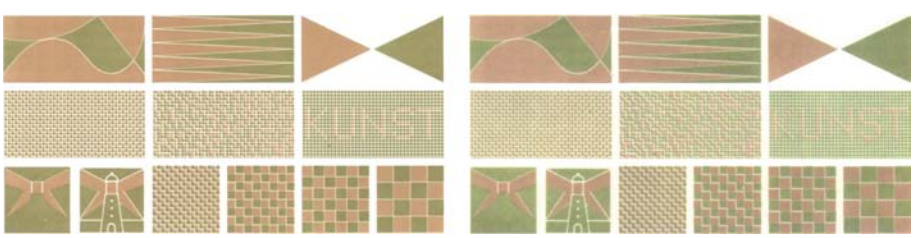


a) Metameric rabbit explained in the leaflet of the NLG 250/Lighthouse (1986).
b) Metameric security feature in Singapore SGD 25. A third brown pattern is used as camouflage.
c) Under a red filter the text 1JAN96 becomes visible (SGD 25).

The bright orange colour, showing up brown in a reproduction, was first introduced on the NLG 50/Sunflower issued in 1982. The same orange colour was used on the front of the euro 200.
In 1986 some more design studies on colours outside the euro scale were performed. One idea that came out of this study was to print a reference next to the colour outside the euro scale. This reference was the 'outlier' colour showing up in a reproduction. In an original note, the idea ran, the two colour areas should look different, while in a reproduction they would look the same. Figure A4.18 explains the principle and provides some examples.

Figure A4.20

Original Colour copy



Design study on metameric colours by Joh. Enschedé, based on designs made by Hans Kruit. On the left the original (here of course mimicked) and on the right a contemporary colour-copied reproduction (ca. 1986).

Metameric colours
An other example based on the 'colour dimension' are so-called metameric colours also recommended by the NRC in their NextGen report [102]. Metameric colours are two colours (a colour pair) that are perceived as similar under one light source, e.g. daylight, and as differently under another, e.g. neon light. Infra red (IR) images are also referred to as 'IR metameric ink', since under daylight two inks will look the same, while with an IR viewer one ink becomes visible (absorbent in IR spectrum) and the other ink is not visible (transparent in IR spectrum).

Metameric design in Dutch guilder notes
A green metameric colour pair was designed and introduced in the NLG 250/Lighthouse intended for use by retailers. Seen through a red filter, a rabbit would show (Figure A4.19a). In the years that followed some more metameric studies were done by DNB and Joh. Enschedé. One example is shown in Figure A4.20. An other metameric colour pair, in the shape of a fish, was introduced in the NLG 25/Robin issued in 1990. This was to be the last banknote model DNB incorporated colour pairs in, because the design suffered of a lack of colours in the area of the metameric colour pair and the feature never became popular. In 1996 Singapore issued a commemorative banknote of SGD 25 using metameric colours (Figure A4.19). In 2001 DNB proposed a metameric barcode for the euro banknotes (see Figure 15). The barcode would represent the denomination, like e.g. 50.

Unique foil colours
Also in the two latest guilder banknotes the colour parameter was used on purpose. Special colours were proposed for the foil on these banknotes. A special green on the NLG 1,000 and a unique blue for the NLG 10. With the manufacturer it was agreed not to sell these colours to others.

A4.5 **Preparation of counterfeits by central bank**

Before issuing a new banknote, it is common practice for central banks to produce several counterfeit studies in a so-called 'Reproduction Research Centre' (RRC). In 1995 DNB travelled for the first time to the RRC in Copenhagen, to prepare such self made counterfeits of the new NLG 1,000. With the help of such a RRC central banks may create their 'self made counterfeits' before the new banknote will be issued.

RRC Copenhagen
'We will learn most about own banknotes when we attempt to counterfeit them.' This was the basic thought behind the establishment of the RRC at Denmark's central bank in Copenhagen on 1 December 1989. At that juncture, scanners and colour copiers were quite expensive. The first scanner at the RRC was a Crosfield drum scanner including a unit for image editing. The price was around euro 265,000

(price in 1989). It was also a large machine, it needed around 10 m². The price of the first colour laser copier of photographic quality from Canon, just introduced, was at that time around euro 40,000.
As it was not feasible or sensible to purchase such expensive reproduction machines individually, a group of central banks concentrated their forces. In total, eight European central banks joined and gladly accepted the offer of Danish central bank to host the RRC. Spacious and secure rooms were made available and the first equipment was ordered. Also an experienced operator was engaged. The concept was very successful. The low costs for carrying out tests justified the centre's existence. DNB followed in 1995 and in 2010 there are 13 members from all over the world, including world currencies.
The central bank of France has its own reproduction research centre called 'Counterfeit Resilience Center'.

Testing of single (island) features
A new feature is often studied and evaluated in the RRC as an isolated part of a banknote. This is not following to the system approach, since the input should be a complete banknote. Still, such single features could be tested, but their reproductions will be made with less effort. The evaluation of such a study is quite often by the person producing the counterfeit. Such evaluation could become more objective if the counterfeit resistance is determined with the aid of a model, by recording and reporting for example time and expertise required to reproduce a complete new design. Also the counterfeit study could be reproduced by a third party to verify the conclusions. Finally the methods used in ranking features for counterfeit deterrence can be improved and made more objective to overcome statements like 'this version will be more resilient to counterfeit attacks than the previous sample'.

Figure A4.21

Standard colour copy CLC 700
Production time: 2 minutes

Optimized colour copy CLC 700 plus foil
Production time: 2.5 hours

Colour copy reproductions of NLG 1,000/Lapwing made by DNB at the RRC in Copenhagen in 1995.

Table A4.5

		Counterfeit investment		
		Time	Expertise	Cost in EUR
A. Copy	- pre press	Push-the button: 1 s	Primitive	0
	- production	100 hour	Primitive	100
B. Ink Jet	- pre press	1 day	Casual, hobbyist	~ 1,000
	- production	10 hour	Primitive	~ 100
C. Offset	- pre press	1 week	Professional	~ 10,000
	- production	3,000/hour	Casual, hobbyist	~ 50,000

Characterisation of reproduction systems by resolution in terms of line pairs per millimetre.

Presentation to the Board

When in the 1990s a new banknote design was submitted to the Board of DNB, the presentation also included specially prepared counterfeits, which were the best reproductions the banknote developers of DNB were able to make, including a 'just push the button' colour copy.

Table A4.6

Public preference	Counterfeit resistance
1. A	1. I
2. B	2. H
3. C	3. F
4. D	4. B
5. E	5. C
6. F	6. D
7. G	7. J
8. H	8. K
9. I	9. E
10. J	10. L
11. K	11. G
12. L	12. A
13. LD original	

Overview of the public preference for 13 hologram designs and the quality of the counterfeits. The results are part of a DNB study 'Foil with public appeal' prepared for the ECB in 2004/2005.
Green = good, favoured by public, proved difficult to counterfeit, Yellow = medium, Red = poor, rejected by public proved to be easy to counterfeit.

These first 'self made counterfeits' were printed by the colour copy machine at the RRC in Copenhagen. Figure A4.21 shows two examples.

A further development of this exercise would be to test such counterfeits on an external panel. Retailers, law enforcers and consumer organisations could be invited to sit on such a panel. The test report could also be part of the presentation to the Board.

Track of the time, expertise and investment
The report to the Board would be even more informative if it also included time, expertise and investment needed to reproduce the freshly designed banknote. Table A4.5 presents an imaginary example of such a method, reporting on the time, expertise and investment needed to reproduce a newly designed banknote.

Evaluation of research results
A research team studying a new or improved security feature might present its results according to the lines as shown in Table A4.6. This method was developed in 2004, in the context of a foil research project by DNB at the request of the ECB. For the first time both 'public preference' and 'counterfeit resistance' are researched to underpin the selection of one of the samples produced. Remarkably, the hologram preferred by the public (A) showed the lowest counterfeit resistance. Sample B received the highest ranking on both parameters and would be the preferred foil design [63, 70, 72].

Appendix 5
Simple method (2006)

Up to 2002, classifying of and reporting on NLG counterfeits were not a high priority of DNB. With the introduction of the euro banknotes all central banks of the Eurosystem implemented a National Analysis Centre or NAC (see also Chapter 6). The principal aim of the centres is to keep track of counterfeit euro notes. Counterfeits within the Eurosystem are therefore classified in a standardized way and information is centrally gathered.
The coming of the Dutch NAC at DNB brought counterfeit analysis to a higher level of sophistication. DNB began to prepare monthly reports on counterfeited euro banknotes. The first, internal, reports were mainly statistical and did not tell much about a trend. The question for DNB was: how to get more feedback from counterfeited security features as input for future banknote designs?

Simple method
Based on an idea of Marco Wind (DNB) a new, *simple method* was developed by Hans de Heij and Jolanda Hijlkema-Duikers (both DNB) and introduced in DNB's monthly report on the banknote circulation of January 2006. The idea underlying the method is to take the most recent counterfeits and monitor their quality. Instead of monitoring all counterfeits, this simple method considers only the 10 types most frequently accepted by retailers and the public.
Figure A5.1 shows some examples of counterfeit scoring. For each of the six public security features in a euro banknote, counterfeit quality is simply scored as:

0 point = no imitation,
1 point = poor imitation,
2 points = good imitation.

These findings lend support to the well-known rule of thumb stating that 'less than 10% of counterfeits are good reproductions'. They also support statements made by the Russian Ministry of Internal Affairs: 'No counterfeiter will try to imitate all security features on a note; they will go for the necessary minimum.' [142].

Quality of counterfeits in NL
The average quality of counterfeited euro banknotes circulating in the Netherlands in September 2009 is 6.4 as provided in Figure A5.2. If all scores for one denomination are grouped, the 'average public score' may be calculated, as shown in Figure A5.3.

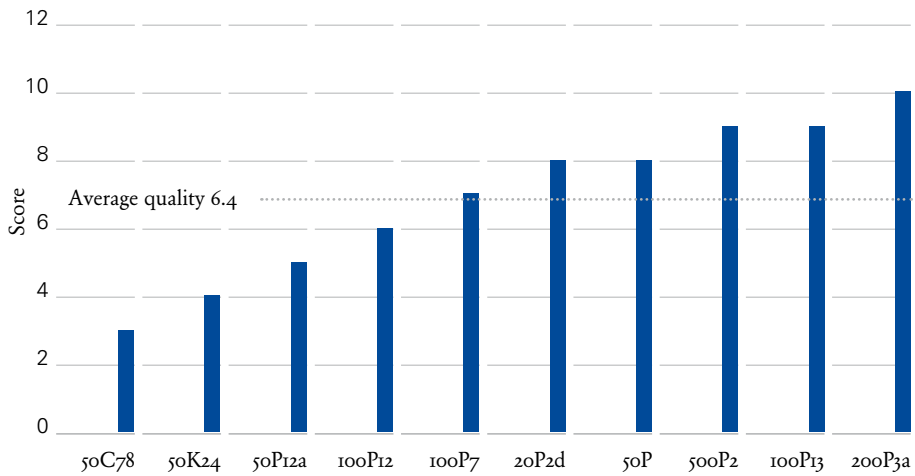
Figure A5.1

Six examples of counterfeited public security features in euro banknote forgeries and the assignment of points according to the simple method.

This is the average quality of the ten most frequently found counterfeits in the Netherlands in the January 2006 - September 2009 period. Note that in the Netherlands, euro 50 counterfeits have the highest occurrence rate: over 70% of all counterfeits are euro 50s, which is why there are several euro 50 counterfeit types (indicatives) represented. The euro 20 makes up about 5% of the number of counterfeits found in NL, but within this denomination there are several variants. This is why there is only one euro 20 counterfeit in the top 10, which is also the most common one in NL (indicative 20P2d).

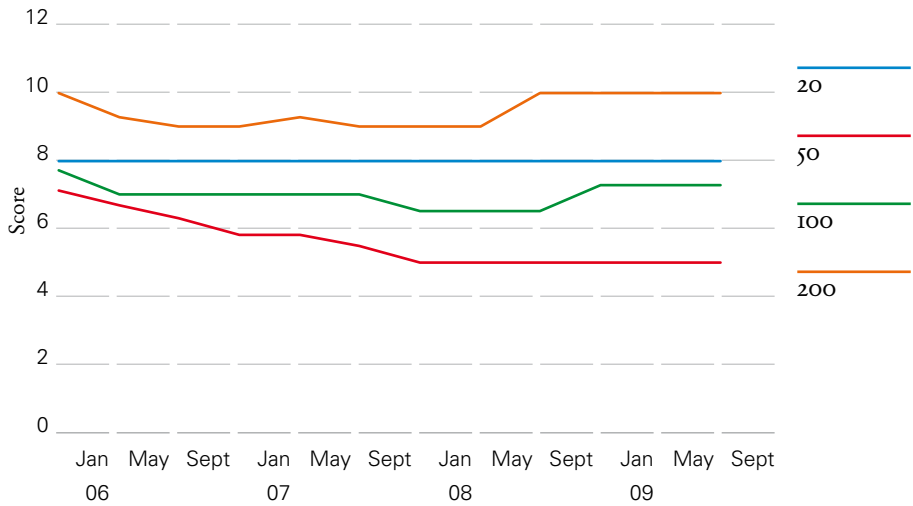
This exercise yields an interesting conclusion: the quality of counterfeits is not rising, but declining. From the graph in Figure A5.3 it can be concluded that:
- There is a difference in quality per denomination,
- The quality of the most frequently counterfeited note, the euro 50, is declining,
- The quality of counterfeits in general is stable if not slightly declining,
- The euro 50 has the poorest quality (remarkable, since it is the most used denomination in NL).

Figure A5.2



Quality of euro counterfeits in September 2009, ranked according to the simple method. The 200P3 has the highest quality (10 points) and the 50C78 the lowest (3 points). The average counterfeit quality in this month is 6.4 points.

Figure A5.3



Weighted average score of the quality of counterfeit euro banknotes in NL since 1 January 2006. The quality of counterfeited euro banknotes in NL is declining. This is especially true of the euro 50 counterfeits (from 7 down to 5 points).

Table A5.1

Quality of counterfeited euro security features

Public feature	Score (2 points max)
1. Watermark	1.7
2. See-through register	1.5
3. Foil	1.4
4. Security thread	1.3
5. Tactile effect intaglio	0.7
6. Iridescence/OVI	0.3
Retail feature	
1. UV	0.8
2. IR	0.1

Quality of counterfeited public security features in euro banknotes, based on the 10 most frequently received counterfeit types in the Netherlands (April 2009 figures).

Quality of counterfeited public security features
The simple method also delivers the individual quality of each public feature as provided in Table A5.1, including the two retail security features.
Clearly the watermark is the weakest feature, in this perspective, since it is imitated 'most and best'. The iridescent and OVI features seem from this perspective to be the strongest public security features.

Evaluation of the simple method
The simple method provides a better view on developments and is indeed simple to apply. Scoring the features seldom requires discussion, so is the experience of DNB, also because of the limited classes (0, 1 or 2). Therefore DNB presented the method in 2006 to the Counterfeit Working Group of the Eurosystem [85]. The method was made public by DNB in 2010 [156, 175].
One disadvantage has already been mentioned: the limitation to the 10 most frequently detected variants. If within one denomination, e.g. euro 20, one indicative is predominant, the counterfeit quality will appear stable, since no other variants are shown.

It turns out that the simple method has a high correlation with deceptiveness, i.e. the higher the score according to this method the more deceptive the note will be to public and retailers.

Appendix 6
Time required checking a banknote

When a cash transaction between two persons is settled, one person is the payer and the other the receiver. The payer has to search in her/his wallet or pocket, and recognises a banknote usually by its borders. Within this *flash second* people will only verify the notes value, its denomination. A security check is only done if the note is not trusted. These two subjects of time spend on a banknote are discussed in two sections:

A6.1 Value recognition: flash second,
A6.2 Security check: about 6 seconds.

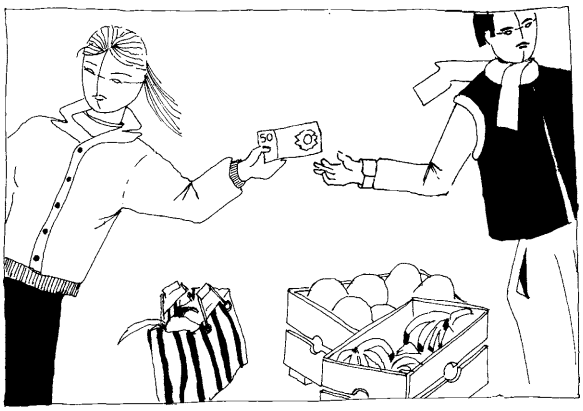
A6.1 **Value recognition: flash second**

In principal there are two different user situations, one person is the payer and the other the receiver, in this case the retailer. The payer has to search in their wallet and recognises a banknote usually by its borders. In this case an image will not contribute much to the value determination. This is the reason why the pattern on the last DNB banknote designs by Jaap Drupsteen was uncluttered visible at all four banknote borders (see Figure 48).
For the retailer the situation is different. The retailer holds the banknotes usually in the drawer of the cash register. The same denominations are grouped together, the low denominations on the left. The retailer sees the banknotes usually in a portrait position.

When the payer hands over the note, the acceptor often only gets to see a glimpse of the banknote since the payer's fingers and thumb partly cover the note (Figure A6.1). This is the instant moment that value verification should take place. For the payer: did I take the right denomination from my wallet or cash register? For the receiver: do I take the right value, is it enough? This very first moment is the *flash second*. A single fixation of the eye takes about 0.01 s. A cluster of several fixations will take 0.05 s or more. The presumed flash second for three well known banknotes is provided in Figure A6.2.

The study 'Banknote design for the visually impaired' [148] describes that value recognition of a banknote is determined by several design parameters like:

Figure A6.1



Illustrations of the flash second; banknotes are often used without being seriously checked. Drawing by De Heij (1984).

1) Colour,
2) Value numerals,
3) Main image, the picture,
4) Dimensions.

When the order of these design parameters of a given banknote would be known, a new banknote design could be improved. Which parameters would deliver most to instant value recognition? What triggers the public first? What comes second and what is third? If such analysis would be available before a new banknote design starts, the graphic designer would know what prevails and could anticipate with an appropriate design proposal. This is relevant if the central bank wants to minimise

Figure A6.2

Overview of the presumed time needed for the public to recognise the value of a banknote when taken from a third party.

the time needed for the public to denominate a banknote. Within this flash second people will only verify the note's value, its denomination.

The flash seconds as provided in Figure A6.2 are a best guess, but are based on an analysis of the design parameters of these three banknotes. The sequence of the parameters is for each banknote different, as is shown in Table A6.1. Below this sequence will be reasoned.

Colour
Euro banknotes are first of all recognised by its colour. The latest dollar designs show more colour, but these colours are not dominant over the portrait image or the numerals.
The bird image of the NLG 100/Snipe prevails over the brown colour; changing the colour of the snipe would not have brought the Dutch people to other thoughts: this is the 100 guilder bird.

Picture
When asked to recall by heart what is on the euro banknotes, less than 5% of the people answer a door, gate or window. Nobody knows that these windows and gates belong to a certain style period (e.g. Renaissance for the euro 50) [94]. With the US dollar bills we see the same. The portraits are too similar and do not contribute to a (quick) value recognition. At the time of the NLG 100/Snipe 68% (1989) people spontaneously recalled Snipe, when they were asked to tell by heart what is on the 100 guilder note. This figure went up to 84% when also the answer 'bird' is added.

Snipe, lighthouse and sunflower used on the NLG banknotes had their own discriminating silhouette and were selected from different categories: a bird, a tower and a flower. Different brain paths become active, which seems not the case with the euro banknotes.

Table A6.1

Design parameters value recognition

NLG 100/Snipe	EUR 50	USD 20 (2004)
1. Picture	1. Colour	1. Numerals
2. Colour	2. Numerals	2. Picture
3. Numerals	3. Dimensions	3. Colour
4. Dimensions	4. Picture	4. Dimensions

Overview of the *estimated* sequence of simular design parameters for three different banknotes.

Figure A6.3

A 'zero USD banknote' as provided by the website www.zerocurrency.org (2010). Replacing the numerals by zero makes it hard to tell the value of this note.

Denomination numerals
Since the sizes of the US dollar notes are the same, the numerals are contributing most to value recognition for these banknote designs.
After the colour, the large numerals on the euro banknotes will assist value recognition over the main image, so is the assumption. Figure A6.3 provides same proof. Large numerals could also be found on the NLG notes and will contribute more to instant value recognition than the dimensions of the NLG notes.

Sizes
All US dollar notes have the same dimensions and are as a consequence not providing any information on its value. The height of the NLG notes is for all denominations the same, but its length increased 6 mm. The euro banknotes have both a length and a height increment. This is the reason why the dimensions of the euro banknotes are put thirdly in Table A6.2. People probably would react sooner to a smaller euro note – must be the 5 – as to the arch.

What can the central bank do with these analyses?
To increase instant value recognition, the European Central Bank could focus first on the pictures on the front of the euro banknotes. In case of a new dollar design the Federal Reserve Bank could opt first of all for changes in colour and dimensions.

A6.2 **Security check: about 6 seconds**

Once people have determined the notes value, they might decide to operate a security check. Such a check is unusual and is triggered by the heuristic quality of the note, registered first of all by the following two human senses: tactility and sight (and in some cases also by our ears). If this implicit quality is found below

Table A6.2

Cash settlement - break down	Estimated time
1. Payer becomes conscious of the amount to be paid	1 s
2. Payer searches cash and takes wallet (or from pocket)	2 s
3. Payer selects right cash amount (banknote(s) and coin(s))	2 s
4. Payer hands over the cash to the receiver	1 s
5. Receiver checks the value of the received cash	1 s
6. Receiver may check the authenticity of the received cash	5 s
7. Receiver calculates the change (if any)	1 s
8. Receiver searches for change	2 s
9. Receiver hands over change to payer	1 s
10. Payer checks on the amount of change	1 s
11. Payer may check the change for authenticity	0 s
12. Payer stores the change in wallet or pocket	2 s
Total settlement time	**19 seconds**

Breakdown in time of a cash settlement between a payer (public) and a receiver (retailer). Estimation by De Heij, based on the reported total time to settle a cash transaction.

standards, the receiver of the note might decide to execute an explicit quality check. All these decisions are taken by the brain within fractions of a second. But once decided to do a security check this will take much more time! See also Subsection 4.1.1 on heuristic and rule based banknote quality.

From DNB research, the total time to settle a cash payment transaction is known to be 19 seconds [62]. Unfortunately, it was not documented what exactly is included within this time. Therefore, we have to live with the breakdown of 19 seconds as assumed in Table A6.2 until more studies on time become available.

From this breakdown, it may be deduced that the total time to check a banknote is probably around 5 seconds. This is also consistent with the study initiated by the ECB in 2007 to analyse how people handle banknotes. The total handling time was 5 seconds on average, 3.5 seconds of which was spent on exploring the front and the remaining 1.5 seconds on checking the reverse. After 10 seconds the test terminated [91, 94].
Five seconds also seems to be the limit of what is socially acceptable to check a received banknote without being impolite.
Five seconds is also close to the 6 seconds needed for a security check of 3 features (3 x 2 s = 6 s).

Figure A6.4

DKK 100 (2010), front

Micro-optics on reverse

New Danish 100 krone banknote with on the reverse side a micro-optic thread (issued in 2010). The design is perceived as 'empty', so the public will focus on the security features, so is the assumption.

Not much attention for reverse side

Checking features on the reverse side takes additional awareness that is usually lacking and is therefore often not done. Turning the euro note and tilting it for the special inks features is probably found to be too time-consuming, although ECB research showed that on average people spent 1.5 seconds on checking the reverse side. It may be questioned if this suffices to verify the optically variable ink on the euro 50 and higher denominations (or the iridescent stripe on the low euro denominations). Furthermore, this check is often hindered by the thumb or other fingers covering the feature when the note is being turned. It is therefore interesting to follow the response to the recently introduced 'motion thread' on the reverse of the new 50 Danish krone banknote issued in August 2009 (see Figure A9.3 and Figure A6.4 for the DKK 100). Will it be successful?

Other ECB research done in 2007 reported that the majority of the *cash handlers* check banknotes on both sides (64%) with just over a quarter only the front (27%) [100].

Transparent window takes at least 9 seconds

In 2005 the Varifeye feature was presented, a clear window in a cotton paper [94]. To check this feature would take around 2 seconds:

- View against white background - in transmission 1 s
- View against dark background - in transmission $\frac{1\text{ s}}{2\text{ s}}+$

Today commercial companies propose a clear window in a banknote which should be viewed first from the front (viewed in *reflection*) and subsequently should be *looked-through*. As a next step, the public should turn the note and check the same feature from the reverse (e.g. reVIEW and recolor) [131]. The time to check such a

single feature would be at least 9 seconds instead of the requisite maximum of 3 seconds:

- View note from front - in reflection 3 s
- View note from front - in transmission 3 s
- Turn note and view from reverse - in reflection 3 s

9 s +

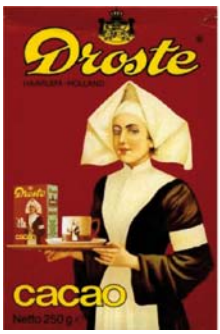
This leads to serious doubt if such features will be used by the public. Most likely, the public may use it partly, e.g. will view it from the front in transmission.

Appendix 7
Nested features

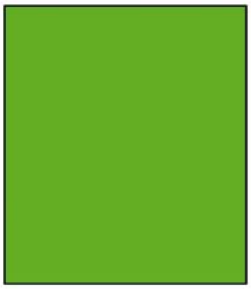
Nested features are based on the principle of a feature within a feature, reminding of the well-known Dutch example of the Droste Cacao box (Figure A7.1a). The first image, a nurse holding a tray with a cup of cacao and a Droste Cacao pack on it, is interminably repeated in that Droste box. An example will explain the nested feature principle. The first security thread was developed in 1867 by Crane (see Table A4.3). The original feature, e.g. a plain security thread, receives a micro-text (nest level 1). New developed public features often follow this principle and have several *nest levels*. This principle is explained in Figure A7.1b and c.
Next to nest levels, user groutp levels are discriminated. The security thread was originally intended to be recognised by the cashiers, but they have evolved to include security features that can be read by high-speed sorting machines. Instead of one user group (cashiers) the thread is used by two user groups (cashiers plus sorting machines).
Thread development is continued and today security threads are available in many variants like e.g. thread with different colour changing effects, thread in two or

Figure A7.1

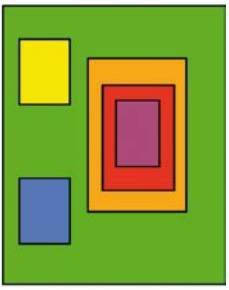
a) Droste-effect



b) Original feature



c) Nested features



Principle of nested features.
a) A box in a box in a box etceteras ('Droste effect').
b) Original, basic security feature.
c) Basic feature with 3 nested features in it; one nested feature contains two more levels of nested features.

even more special colours, all kind of holographic threads, threads with 3 levels of demetallisation making tonal variations possible ('Picture Thread') and threads with different magnetic codes.

Holograms are multi nested features
A hologram is such a nested feature: a plain foil (main feature) is provided with a hologram (nested feature 1), mini-text (nested feature 2), micro-text (3) and, from the reverse, a perforation (4). The hologram itself shows the image of a gate switching from 'positive' (feature 2.1) to 'negative' (feature 2.2) on being moved (e.g. Figure 52). Also the numeral '50' may be seen (feature 2.3) and 'pumping effects' like rainbow colours (feature 2.4).
Another example of a nested feature is a mark in glossy ink (main feature) showing a colour-shift (nested feature 1) and movement (nested feature 2). Features which become discernable when held under UV light with a long (around 365 nm) or a short (around 254 nm) wavelength are also a variant of nested features.

Nested public features are too difficult to explain
In banknote design such nested features are unwanted, because they involve explaining and checking several features, instead of just one. This seems to be too demanding for the public in terms of time and knowledge. A plea for simple design was already given by the Bank of England in the 18th century: the best defence against forgery lies in three key features: watermarked paper, good quality ink and a simple design [46].
In fact, central banks should see the banknote as a whole, as one feature (the banknote) with nested public features in it, all on nest level 1.
Nest level 2 and higher may be included in the feature, but not for public use. Such higher levels are forcing the counterfeiter to layer their work. This should be realised by the design: level 1 for the public and the higher levels are there for the counterfeiter (see section 4.1, the paradox on holographic foil).

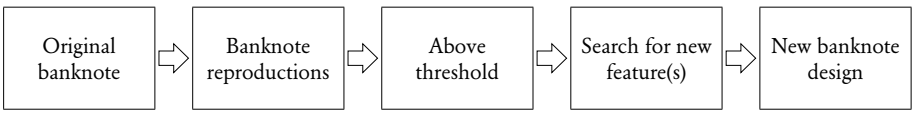
Appendix 8
Response policies of central banks on counterfeited banknotes

The number of counterfeits received is an (implicit) counterfeit deterrence model used by many central banks. The central bank speeds up the search for new security features, when counterfeit levels exceed such threshold values. Table 7 serves as a model to set such limits for the number of counterfeits to be found acceptable. A central bank could formulate a response strategy to initiate a new banknote design as follows: 'There are less than 30 counterfeits per one million notes in circulation during the first two years of issue. After this period a maximum of 50 c/mln is accepted.' While the threshold value marking the moment from which new features must be developed may be a quantitative value, it is usually of a subjective kind, such as complaints or a (perceived) high counterfeit volume.

First counterfeit threat was in 1849
The first counterfeit threat in Europe was already recognised in 1849 by the Académie Internationale des Sciences. Banknotes could be reproduced using 'palaeography'. Palaeography employs both lithographic and photomechanical techniques. Such techniques became available with the invention of the photography in 1825 by Nièpce and by Daguerre in 1837. Because of this counterfeit warning, in the 1850s the black print on the Belgium banknotes was replaced by a more secure blue tint [35].

First counterfeited NLG banknotes
For a long period DNB's response policy with respect to counterfeited NLG banknotes was reactive. When the public lost confidence in certain denominations and avoided using these notes in daily payments, DNB responded by developing a new banknote design. The first time was in 1836 and DNB responded by replacing the watermark, but did not change the print.
Around 1850, the new technology of photography triggered illegal banknote reproduction, also in the Netherlands. Counterfeits were made and after the discovery of a batch of counterfeit NLG notes in London, the board of DNB decided to give the development of new banknotes priority. One of the DNB board members, Willem Cornelis Mees, personally led the research for new security elements. The final choice went to an improved intaglio gravure (a small blue-green security text was already printed by gravure on the guilder notes between 1814 and 1837). In 1860, a new series of NLG banknotes including enhanced gravure print provided the first reactive response. Counterfeits kept coming, however, and

Figure A8.1



Process traditionally preceding the production of a new banknote model in a particular denomination in reaction to a high incidence of counterfeits of that denomination.

once more necessitated the introduction of new features and production machines around 1920. The single grey colour of the NLG 1,000 note issued in 1921 was quickly imitated. This time (part of) the response was found in the introduction of *iris-print* (or *rainbow-print*, see Appendix 4, Section A4.2). A two-colour press by Roland, the Roland Zwei Farben Presse (RZ press) was installed and ready for use in 1926. The iris print technique was introduced in the upgraded NLG 1,000, issued three years later in 1929 [34, 55].

Counterfeit thresholds
How many counterfeits in circulation are acceptable? As far as is known, no studies are available of what would be an acceptable counterfeiting level in a cash payment system. For many central banks the number of counterfeits should not exceed 50 counterfeits per million notes in circulation (c/mln). If this figure would rise above 100 c/mln this is seen as an alarm level. When such a given threshold is exceeded, the central bank speeds up the search for new security features. Once such features have been developed, the central bank commissions a new banknote design (see Figure A8.1) [156, 175].

Since the mid-1970s, DNB abandoned its reactive approach and developed the following proactive counterfeit models like intrinsic and extrinsic security features (1976), internal and ad on (1985), system approach (1991) and simple model (2006). These models are discussed in Appendix 2, 3, 4 and 5, respectively.

Euro counterfeits threshold
The counterfeit threshold for the Eurosysteem was set in 2002 at 50,000 counterfeited banknotes a month. The reasoning was the following. Before the introduction of the euro, the total number of counterfeits detected in the 12 countries that converted to the euro was around 600,000. This was found acceptable by the Eurosystem and that is why, in 2002, the threshold for euro counterfeits was set at a maximum of 50,000 notes per month for all denominations. Action is triggered when that limit is reached and when each month during a period of three months in a row over 50,000 counterfeits are detected. A denomination should be replaced with a new

design if the number of counterfeits of that banknote accepted in one year exceeds 75,000.
If the 9 billion notes issued at the introduction of the cash euro in 2002 is divided into the above threshold of 600,000 counterfeits per year, we arrive at a threshold of 70 c/mln. This level was reached in 2009, the year the Eurosystem has left this threshold policy, with the argument that attention on counterfeits is depending on several aspects like perception on the counterfeits by the public. Looking at the alarm level from this point of view, the euro counterfeits increased from 49 c/mln in 2007 up to 55 c/mln in 2008 and reached (the former threshold) level of around 70 c/mln in 2009.

Threat indicators
Instead of 'probability of a counterfeit' or 'confidence', central banks have started looking for ways to create 'threat indicators', just as in 1849. Such indicators intend to create a signal, e.g. on a scale of 1 to 5, that indicates what kind of response is necessary. This signal could be based on a variety of aspects like: increase in counterfeits since previous quarter, counterfeit percentage in total banknote circulation, deceptiveness, average counterfeit value or financial damage.

Press releases by central banks
Expressions of a reactive response strategy are the central bank's annual or biannual press releases containing the latest counterfeiting figures. Such press releases and the subsequent articles in the media – often copy-and-paste jobs from the original press release – cover a fixed range of items:
- Numbers,
- In- or decreases in the number of fake banknotes,
- The places where the counterfeits were distributed and/or circulate,
- The denominations that are counterfeited (the most),
- Face value,
- The places where the counterfeits were produced and by whom or which criminal group.

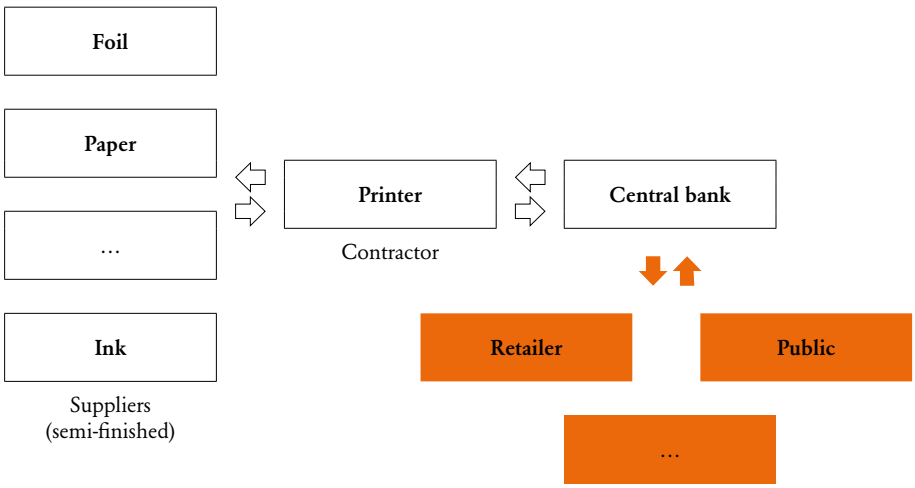
Such reports have a statistical format including some legal remarks. An overview of reporting style as observed by four central banks was provided in 2010 [156]. All too often these press releases fail to inform on technical matters like differences between the fake and original notes. If there is a problem it is helpful for the public to be aware of it and look out for counterfeits. A study to the effect on the public perception of press releases on counterfeits would be useful.

Appendix 9
Which features should be developed?

Security features proposed by the security industry, may be explained by the controversy between *technology push* (the suppliers) and *technology pull* (the central banks). It seems that the central banks do not exercise sufficient 'pull' and should develop themselves much more as knowledgeable on the subject of banknotes as well as stepping up their development efforts, starting first of all by learning to understand their customers better, especially the retailers and the general public.
One of the central banks commenting on this issue is the Bank of Canada. 'The approach of the private sector, because it is largely driven by profit motives and short term timelines, is not completely suitable for the Bank of Canada. (…) Working through an internal research and development program allows the Bank of Canada to test concepts that fall outside the core capabilities of the traditional suppliers. Such exploration allows the Bank to progress toward features targeted to specifically meet the needs of the Canadian currency user.' [129].
An even stronger quote comes from Julian Ashbourn: 'Suppliers are convincing central banks of the merits of their particular features, spiced with some attractive sounding theoretical benefits, couched in the language of the organisation being targeted. With good marketing and publicity a steamroller effect is created and, with the help of conferences and workshops to reinforce the message, consumers dutifully start adopting the sales-speak.'[130].
The CEO of DeLaRue is aware of, and even accepts, this criticism when he tells that the security industry is suffering from complacency. 'I think there is a real concern that this is becoming an introverted, narrow and incestuous industry which forgets the outside world, be it the consumer (in the end of the day the user of banknotes).' [140].

The banknote industry cannot develop optimal banknotes for lack of input from the retailers and public. Central banks should provide this input. The central bank is, in modern management terms, the *chain director* and should do the consumer research. By means of a Programme of Requirements the central bank may inform the private sector [108, 170].
Semi-finished product suppliers are even further removed from the end users of the banknotes (see Figure A9.1).

Figure A9.1



Supplier (too) far from final customers [134]. The central bank should take care of their stakeholders like retailers and public and inform the private sector by means of a Programme of Requirements.

Central banks would like to have far more options. Since there is only one feel feature available (ink relief), central banks are especially in need of more feel features. Secondly, far more look-at features are required.
Tilt features – and especially colour switching features – are less popular than feel and look features, as concluded in the first paper, 'Public feedback for better banknote design' [81]. New retail features are needed as a follow-up to the magnifying glass and the UV lamp.
Central banks would also like to have more choice in design variants of new features, like e.g. more colours. Foil stripes all come in silver and the colour-changing features have a limited colour range.

Feel feature
There is evidence that merely touching a banknote may trigger alertness to a counterfeit note, especially among cash handlers like retailers. A recent ECB survey confirms that for 70% of the cashiers, tactility is the security feature most commonly noticed. 'Tactility here is a collective term for feel of the paper, properties you can feel and raised print' [100]. To increase counterfeit detection, the design of banknotes should thus take into account this important haptic interaction. By reviewing relevant haptic sensory mechanisms, research should serve as a basis for identifying new feel features that will increase the haptic detection of genuine banknotes. The feel sense is much broader than tactility restricted to relief, and there are more ways to gain the public's attraction. The feel sense can be explored

by using different surface boundaries, by contrasting rough-shiny, smooth-sharp, stiff-weak, simple-complex and narrow-broad. Also nail scratch elements producing a specific sound could be explored.

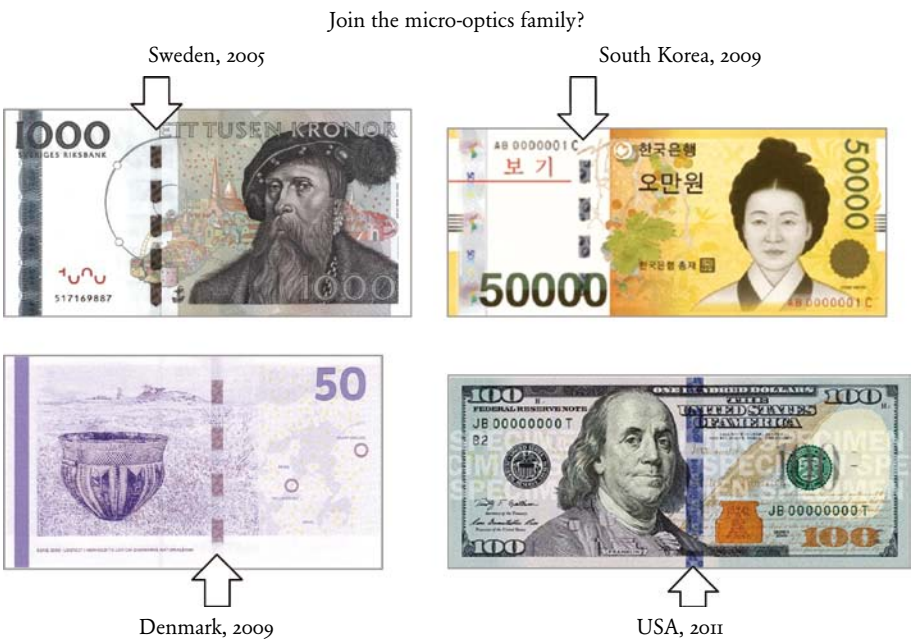
Foil feature familiarity
The glossy, silver foil stripes are dominant design elements and catch the human eye. Banknotes with such a foil stripe have something in common; they belong to the foil stripe family (Figure A9.2). Foil stripes became popular in the 1990s. For the public the holographic images in the foil are too complex and there is a need for foils that match the user requirements, especially on 'understandable' and 'univocal' (see Section 4.1.7 on User requirements public). Introducing additional colour to these silver stripes will create more design variety (and will increase the counterfeit-resistance) [94].

Banknotes with micro-optics
A new family of banknotes connected by a security feature is born in 2005: the micro-optics family (Figure A9.3). This striking feature is applied on a wide windowed security thread, which makes this security feature prototypical. For central banks the question is, just as with the foil stripes, how to design this feature so that it will match the user requirements? Again 'understandable' and 'univocal' seem to be the two critical user requirements.

Figure A9.2

The foil stripe is a prototypical design element of these four banknotes, making them belong to the foil stripe family.

Figure A9.3



The wide windowed security thread with micro-optics is a prototypical design element of these four banknotes, making them belong to the micro-optics family.

Floating images receive usually a high score on user requirement 'striking' (see Section 4.1.7.8). Even higher scores may be reached when a short film would be printed on a banknote, like was done for the first time on a postage stamp issued in the Netherlands in 2010 (Figure A9.4). It seems a matter of time to reduce the thickness of this stamp (around 150 µm) to a thickness suitable for a banknote (around 50 µm). The film is hard to reproduce!

Banknotes with transparent windows

In April 2007 the first banknote with a transparent window named 'Optiks' was issued by the central bank of Fiji. The Opiks feature is a 18 mm wide security band and is an invention of De La Rue. In the centre of the band there is a transparent area not covered with paper fibres. As a result an elliptical transparent area can be seen.

There are also other technical solutions to come to a transparent area in a banknote, like using a registered foil stripe as shown in Figure A9.5.

Figure A9.4

b) One of the 30 originals

a) 3 of the 30 images

c) Scanned image, only one will be selected!

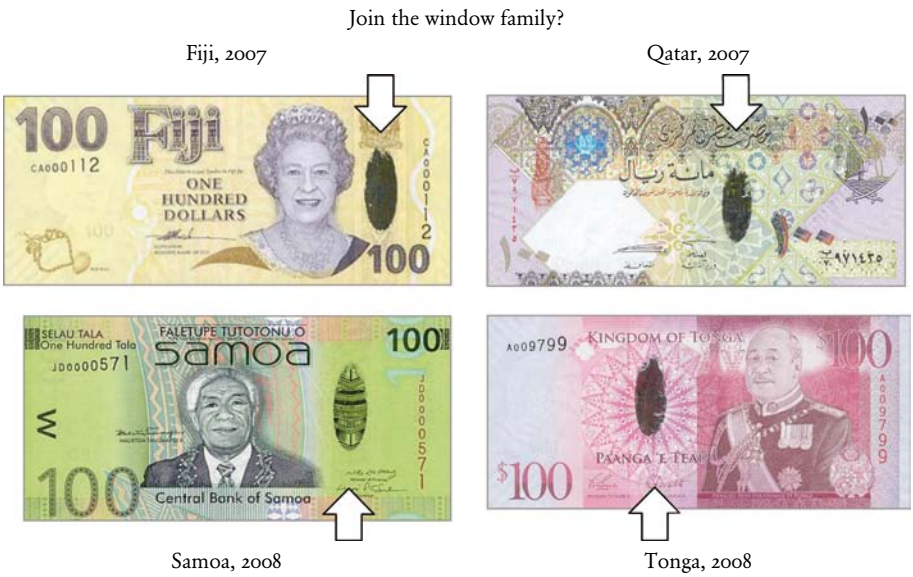
Innovative postage stamp 5 (value euro 2.20) issued in the Netherlands in September 2010. The stamp shows a one second film of a woman biting a finger. The film is made up of 30 different images called stills. Stills become visible because of a special lenticular print.
Production: TNT (350.000 stamps). Concept: KesselsCramer. Film director: Anton Corbijn. Actrice: Carice van Houten.
a) Three of the 30 stills making up the short film.
b) One of the original stills to be reproduced.
c) Depending on the scanning angle, the scanner will just reproduce one of the 30 stills. Secondly, the reproduced image is blurred and out of colour because of the lenticular lens.

Improved OVI: Spark

Since the improved OVI receives so much attention from central banks and is incorporated in several recently issued banknotes, somewhat more attention is given to this feature. More and more central banks are growing convinced that Optically Variable Ink (OVI) is not a strong feature. After DNB and the Central Bank of Romania, similar findings are reported by Banco de España [117]. Just as in the Netherlands, the optically variable ink mark is the least familiar public security feature, known by 11% of the Spanish public (and 3% of the Dutch). The OVI on the dollar notes is not popular in the United States either. The NRC in their NextGen book writes that 'color-shifting inks are rarely used by the general public'[102]. Dr. Hans Reckers (Bundesbank) is among the criticasters of OVI because of its 'astonishingly' easy reproducibility [123]. Mr. Vladimir Finogenov of the Russian Central Bank agrees: 'OVI are reproduced with rather high quality' [120].

In 2006, the next generation of OVI features was introduced, named Spark (Figure A9.6). The OVI pigments received a metal kernel. During the printing process the

Figure A9.5



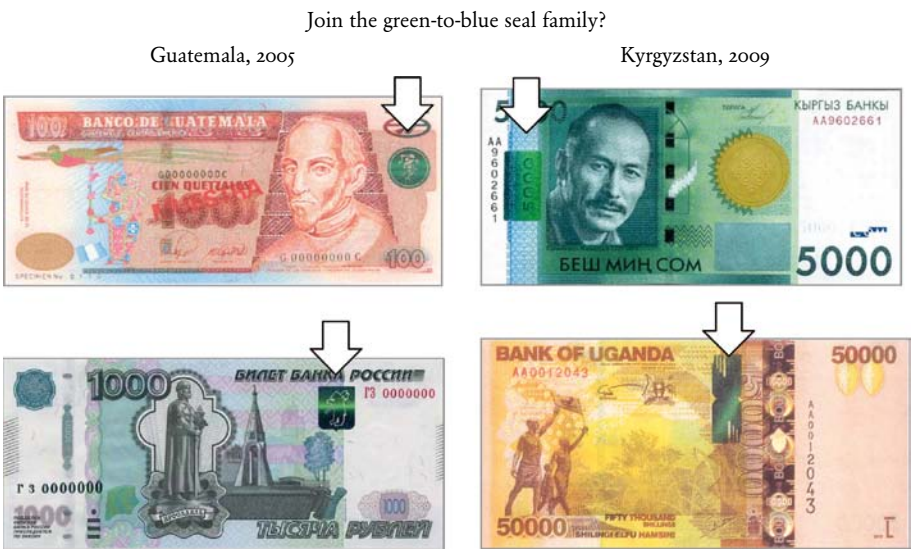
Four banknotes with the window feature 'OPTIKS' by De La Rue, creating a family of transparent windows.

ink pigments are being oriented by a magnetic field. The advantage of this method over the existing OVI is that thus a dynamic effect can be created, e.g. the so-called *rolling bar*. Spark is therefore considered an improved OVI and not a really new

Figure A9.6

The first banknote to feature the Spark is the Chinese 19 Yuan (print run 6 million), issued by the People's Bank of China in 2008 on the occasion of the Olympic Games in Beijing in 2008. Picture published by Getty Images.

Figure A9.7



The glossy seal-type element using the same green-blue colours is a prototypical design element of these four banknotes, making them belong to the green-to-blue seal family (or rolling bar or Spark family).

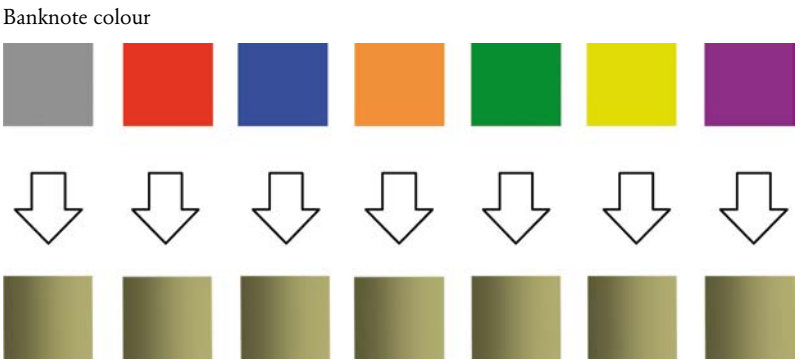
feature. In fact, a third, motion-based, nest level was introduced, in addition to the gloss and a colour. The order of operating the Spark feature will be:

- Motion,
- Colour switch,
- Gloss.

The question is whether it will be successful. Motion is registered more quickly and in a different part of the brain than colour differences. People will focus on motion rather than colour change and/or gloss. When discerning motion in a counterfeit Spark-feature, the public might take it for real. Since the OVI patent has expired, another drawback is that any enterprise is free to produce the Spark's gloss and colour switch features.
Figure A9.7 provides an overview of banknotes issued with the spark-feature.

Alternative colour switching scheme
From the customers' point of view, central banks will opt for a colour-flop scheme, which consists of seven different colours that all change to the same hue of gold (see Figure A9.8). The design of the colour-moving features should be extra appealing, since the public in general is not keen on having to tilt banknotes in order to check

Figure A9.8



Innovative colour concept for a banknotes series. Easy to communicate: all colours turn to gold. Concept by De Heij [134].

features [81]. And further more, as reported by De Heij in 2009, the colour-blind people are not able to see (most of) the colour switches [148].
Also from counterfeiters' point of view the Spark feature is a hurdle. Once the good colour flop imitation is found, it may be used for many banknotes, both within the series and internationally. An other drawback is the limitation of colours: just two colours are available. Sicpa announced that two more colours will become available in 2011.

Appendix 10
Conjoint research
What does the public want?

At the request of DNB, TNS/NIPO researched in 2009 the public preference for different sets of security features [133, 156]. It was the first ranking based on public preference. The perceived relative importance of security features was determined by using a marketing research method called *conjoint analysis*. Conjoint analysis is also called multi-attribute compositional models analysis and is a statistical technique that originates in mathematical psychology. It analyses the relative importance of attributes or components. In this case, 6 different attributes of the security features of a banknote were distinguished, each with 2 or 3 levels as shown in Table A10.1.

Table A10.1

Attribute	Attribute level
1. Location of security feature	Everything on the front,
	Everything on the back,
	Partly on the front and partly on the back.
2. Number of security features	2
	4
	6
3. Degree of conspicuousness	Should be noticed at first glance,
	Should be somewhat concealed.
4. Degree of complexity	Should be verifiable at one glance,
	Should need an effort to verify.
5. Pictorial element used for security feature	Figurative: clear and recognisable images (for example flowers, animals, buildings),
	Number: value of the banknote (for example 5, 10, 20, 50),
	Abstract: combined, no obvious depiction (for example lines and compartments).
6. Appearance of security feature	Technically improved, but with the same appearance as the current security features,
	Technically improved, and with a modern, state-of-the-art appearance.

Overview of the six attributes of the security features of a banknote and their levels used in the conjoint analysis 2009.

Table A10.2

Euro banknote characteristic	Score in %
Location of security feature	30
Number of security features	23
Pictorial element (type of image)	18
Degree of complexity	13
Degree of conspicuousness	9
Appearance of security features	6

Relative importance of the characteristics of the security features on euro banknotes.

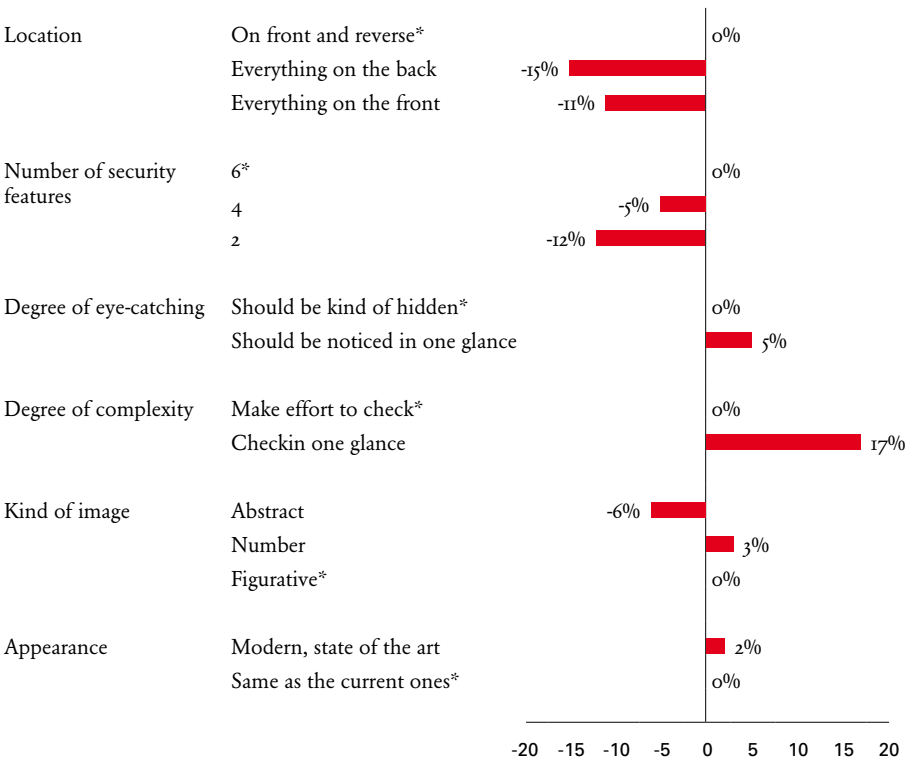
The respondents were asked to indicate which they found more important: the *number* of features or their *location* on the banknote. They were given three options to choose from: 2, 4 or 6 features all placed on the front of the note, all placed on the reverse of the note or divided over both the front and the reverse. Other considerations concerned the design of the features (figurative, numerals or abstract), the degree of complexity, conspicuousness and the appearance of the features.
Each participant was offered two different sets and asked to choose between them. In total, 36 combinations were offered.

Location of feature most important
It turns out that the location of the security features on the euro banknote is given the highest relative importance, followed by the number of security features. The appearance of the security features turns out to be of least relative importance, as shown in Table A10.2.

Checkable at one glance
Based on the conjoint analysis done, the effect of making changes to the security features of the euro 50 banknote can be predicted. The Dutch fully agree with the October 2007 Report of the ECB: 'The public seems to experience some difficulties in locating the security features on the banknotes. Therefore, communicating on the security features of the banknotes is an important and ongoing challenge. It can be aided by a user-friendly banknote design.' [99].

The graph in Figure A10.1 shows the results. The attribute levels of the current euro 50 banknote are marked with an asterisk. It is clear that a change in the degree of complexity will give a strong boost. If security features are verifiable at one glance will give the strongest boost to a new euro 50 banknote design and is in fact by far the strongest boost that can be given.

Figure A10.1



Relative importance of the characteristics of the security features on euro banknotes. People would like to see features that can be checked in one glance.

To men, the location and the number of security features are slightly more important. To women, the degree of complexity is slightly more important. Youngsters find the number of security features most important, as opposed to the elderly, who find the type of image used for the security feature is most important.

Operational model

The conjoint analysis is a working model. The model is filled with the data obtained in 2009 and provided on a CD-ROM. The model accepts variable input, simulating different banknote concepts put together using the various attribute levels mentioned. The model will tell the user the level of public acceptance relative to another concept, e.g. the existing euro 50.

Appendix 11
All-in-one method applied to retail features in euro banknotes

Chapter 3 describes the all-in-one method as applied to the retail features of the euro banknotes. Detailed information on how the criteria are scored is not part of Chapter 3 and is provided in this Appendix. The user of the all-in-one methodology might come up with different results by scoring the criteria differently; of course, one may lay down other thresholds than the ones proposed.
The structure of the all-in-one method is followed:

A11.1 Defining tool-feature matrix,
A11.2 What goes out? - retail features euro,
A11.3 What can be improved? - retail features euro,
A11.4 What comes in? - retail features euro.

A11.1 Defining tool-feature matrix

A far-reaching adaptation of the retail features is required, as analysed in Chapter 2. We opt in this theoretical exercise for a tool-feature matrix based on the generic security matrix as proposed in Table 12.

A11.2 What goes out? - retail features euro

There are several criteria to audit the retail security features of the euro banknotes. The first is the retailers' knowledge.

Retail knowledge of security features
The data found to judge the knowledge criteria is reported in Table A11.1. In general the knowledge on retail features is poor and seems to confirm that retailers rather do not check banknotes.

Specific dedicated research to *cash handlers* is done by the ECB known as the 'Cash Handler Surveys' [60, 100, 151]. Which devices retailers are using and what their knowledge is on security features is the subject of this research.
An overview of the collected data is provided in Appendix A1. Best known are the fibres visible under UV light (16%).

Table A11.1

Retail security features euro series 2002	Knowledge ECB 2009	Knowledge DNB 2009
UV light		
1. Front and reverse: dull paper	9%	3%
2. Front: fibres visible in three colours (red, blue and green)		16%
3. Reverse: fibres visible in three colours (red, blue and green)		5%
4. Front: two inks are fluorescent (e.g. EU flag, signature)		3%
5. Reverse: one ink is fluorescent (e.g. map of Europe, bridge)		
IR viewer		
6. Front: right part of building visible	4%	3%
7. Reverse: numeral on the right is visible		
Magnifier		
8. Front: micro-text	8%	6%
9. Reverse: micro-text		
Mirror		
10. OVI numeral on reverse (high denominations)	-	-
Pen		
11. Starch content	-	-

Knowledge of retail features in the euro area by ECB (2009) and in the Netherlands by DNB (2009).
The Opticial Variable Ink feature (OVI) is a public security feature, that could also be checked with a tool, with a mirror. The pen test is used to indicate starch content.
This feature is not advised, as reported in Section 3.1.4 .
Left column: Cash Handler Survey, ECB, 2009 [151].
Right column: Public survey, DNB, 2009 [133].

Criterion
Green: Score retail knowledge > 50%.
Red : Score retail knowledge < 10%.

Reduced communication
Since 2006 DNB no longer advises to use an UV lamp to verify euro banknotes. A magnifier is never actively promoted as a tool to be used by the retailers. It could be used at the back-office of a store. These two tools, UV lamp and magnifier, receive respectively a red and yellow flag and should be discontinued (Table A11.5).

User requirements
In general the retail features full fill the user criteria (Table A11.2).
Using an IR viewer to verify a banknote takes time. The retailer has to put the note under the camera, which usually activates the screen, which takes one or two seconds. All together a judgement by a retailer will need over 3 seconds.

Table A11.2 What goes out?

Retail security features euro series 2002	UV light					IR viewer		Magnifier	
Criteria	1. UV dull paper	2. Fibres front	3. Fibres reverse	4. Reflection inks front	5. Reflection ink reverse	6. Building front	7. Banknote number reverse	8. Micro-text front	9. Micro-text reverse
User requirments (RH)									
1. Time (< 2 s)									
2. Easy to find									
2.1 Space									
3. Understandable									
4. Univocal									
5. Single user group									
6. Nest levels ≤ 1									
7. Delicate									
8. Striking									
9. Durable									

Human assisted retail features in the euro banknotes scored against the user requirements.
Scored by De Heij.

UV features received a yellow score on being durable. If banknotes are washed the UV properties change as bleaching agents in the washing powder make the cotton paper reflecting under an UV lamp instead of dull.
IR features are influenced by dirt, which is often IR absorbent. Using an IR viewer will show different images on respectively clean and soiled banknotes, indicating a yellow score too.

Counterfeit analysis
Retail features have a poor resistance to counterfeiting, especially when the system approach is applied (Table A11.5).

Threshold levels used for the criteria on counterfeit frequency are:
Green: Imitated feature is present in some (< 10%) of the counterfeit banknotes.
Red : Imitated feature is found in almost all (> 80%) of the counterfeit banknotes.

Since around 1995 standard paper in copy and other reproduction machines is often recycled paper and is UV dull. This is the reason why the watermark received a red flag on criterion 'density' of the system approach.

Costs

Traffic lights representing the costs of the retail features are provided in Table A11.3. Retail features are specified in detail; all three colours of the fibres on both front and reverse are listed. Instead of one, all different types of micro-texts (5) are specified. All features, except the micro-text on the foil, receive a green light, because all are produced for less than 5% of the total banknote cost (based on a total of 37 features). The cost of the foil exceeds the threshold.

Table A11.3

Production step	Cost in euro-cent per feature – euro 50 note	Retail security feature
		1. Dull paper front (UV)
		2. Red fibres front (UV)
		3. Blue fibres front (UV)
		4. Green fibres front (UV)
		5. Dull paper reverse (UV)
1. Paper	0.11	6. Red fibres reverse (UV)
		7. Blue fibres reverse (UV)
		8. Green fibres reverse (UV)
		9. Micro-text thread seen from front
		10. Micro-text thread seen from reverse
		11. Mini-text thread seen from front
2. Foil stripe (10 mm)	0.55	12. Micro-text foil
		13. Micro-text offset (front)
		14. Micro-text offset, positive (reverse)
3. Print - offset	0.07	15. Micro-text wet offset, negative (reverse)
		16. Reflecting ink 1 front (UV)
		17. Reflecting ink 2 front (UV)
		18. Reflecting ink reverse (UV)
		19. Micro-text (intaglio)
4. Print - intaglio	0.13	20 Building front (IR)
5. Numbering	0.2	21. Banknote number (IR)

Overview of the costs of the retail security features in the euro banknotes per production step (based on Table 31).

Table A11.4

Retail security features euro series 2002	Surface in euro 50	In mm²
UV light		
1. Dull paper	140 mm x 77 mm (x2)	21,560
2. Fibres front	average 3 mm x 15 fibres	45
3. Fibres reverse	average 3 mm x 15 fibres	45
4. Reflecting inks front	about 1/6 x 10,780 mm²	1,800
5. Reflecting ink reverse	about 1/5 x 10,780 mm²	2,200
IR viewer		
6. Building front	50 mm x 20 mm	1,000
7. Numeral reverse	30 mm x 3 mm	90
Magnifier		
8. Micro-text front	about 1/50 x 10,780 mm²	200
9. Micro-text reverse	about 1/50 x 10,780 mm²	200

Retail security features in a euro 50 banknote and the space they occupy.
The euro 50 measures 140 mm x 77 mm = 10,780 mm².

Criterion

Green: Feature cost is < 0.35 eurocent (or 5% of average note price of one euro 50 banknote).

Red : Feature cost is > 0.7 eurocent (or 10% of average note price of one euro 50 banknote).

Life span

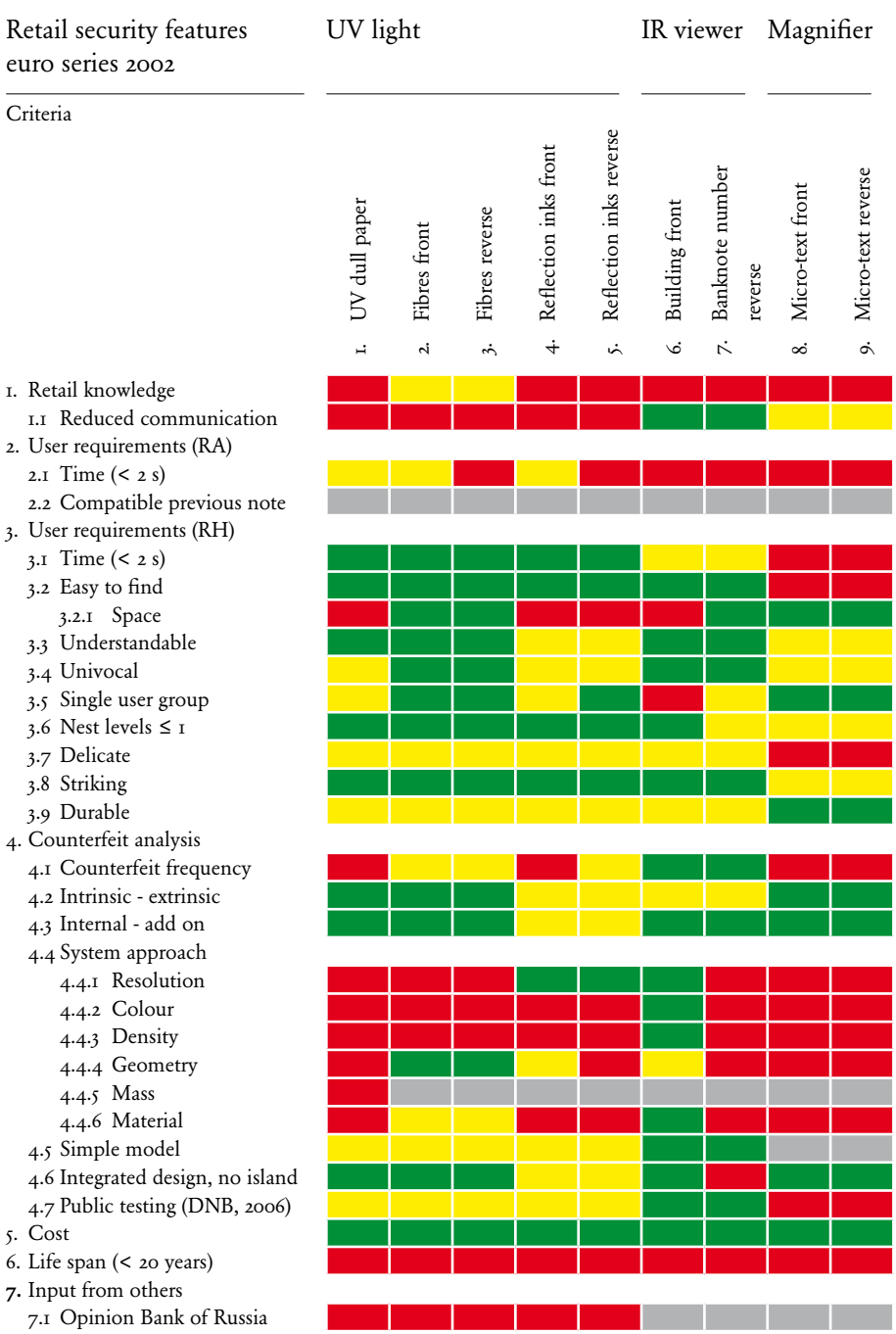
The life span of a security feature should be set at 20 years, the period after which a patent will expire. The ages of the retail features used in the euro series all exceed 20 years: UV over 50 years, IR is used over 25 years and the first micro-text in banknotes are first used over 200 years ago (Tabel A11.5).

Space

In 2008 DNB published an analysis of the use of space for public security features in the euro banknotes [108]. Similar to this analysis Table A11.4 lists the space occupied by the retail features in a euro 50 banknote.

Several retail features recieved a red flag on space because they are too large. Several other retail features recieved a grey colour because for these features space is not relevant (e.g. fibres, micro-texts).

Table A11.5 What goes out?



Theoretical exercise of the tool/retail criteria-feature matrix *What goes out?* Overview of all criteria used on all retail security features in the euro series 2002. The user of the all-in-one methodology might come up with very different results by coding the criteria differently. Scored by De Heij.

Table A11.6 What can be improved?

Retail security features euro series 2002	IR viewer	
Criteria	1. Building front	2. Banknote number
1. User requirements (RA)		
1.1 Time (< 2 s)		
1.2 Compatible previous note		
2. User requirements (RH)		
2.1 Time (< 2 s)		
2.2 Easy to find		
2.2.1 Space		
2.3 Understandable		
2.4 Univocal		
2.5 Single user group		
2.6 Nest levels ≤ 1		
2.7 Delicate		
2.8 Striking		
2.9 Durable		
3. Counterfeit analysis		
3.1 Counterfeit frequency		
3.2 Intrinsic - extrinsic		
3.3 Internal - add on		
3.4 System approach		
3.4.1 Resolution		
3.4.2 Colour		
3.4.3 Density		
3.4.4 Geometry		
3.4.5 Mass		
3.4.6 Material		
3.5 Integrated design, no island		
3.6 Integrated design, no island		
4. Life span (< 20 years)		

Theoretical exercise of the tool/retail feature-criterion matrix *What can be improved?*. Scored are the expected options on improvement on both design and technology. Scored by De Heij.

Input from others

The Bank of Russia evaluated their existing banknotes in 2008 and reported that 'the counterfeiters reproduced the UV feature of banknotes well enough. In this way they practically invalidated such devices as the UV lamp.' [120]. The Russian

Table A11.7 What comes in?

Retail security features new banknote series	Automatic device			Human assisted		
Criteria	Botanic DNA in paper	Thin steel fibres in paper	Metameric code	Polarisation in foil	Liquid crystal-based polarisation	Laser pen and opaque white boll
1. User requirements (RA)						
1.1 Time (< 2 s)						
1.2 Compatible previous note						
2. User requirements (RH)						
2.1 Time (< 2 s)						
2.2 Easy to find						
2.2.1 Space						
2.3 Understandable						
2.4 Univocal						
2.5 Single user group						
2.6 Nest levels ≤ 1						
2.7 Delicate						
2.8 Striking						
2.9 Durable						
3. Counterfeit analysis						
3.1 Intrinsic - extrinsic						
3.2 Internal - add on						
3.3 System approach						
3.3.1 Resolution						
3.3.2 Colour						
3.3.3 Density						
3.3.4 Geometry						
3.3.5 Mass						
3.3.6 Material						
3.5 Integrated design, no island						
4. Life span (< 20 years)						

Theoretical exercise of the tool/retail criteria-feature matrix *What comes in?* Overview of all criteria used in making a selection out of 5 innovative retail security features. Scored by De Heij.

Ministry of Internal Affairs holds the same opinion 'The luminescence of the counterfeit is poor, yet close to that of the genuine note.' [142].

Overall table'what goes out?

Table A11.5 presents the outcome, the final result of the method applied to the retail features in the euro banknotes. All retail features of the euro series 2002 have shortcomings (red lights); not a single feature is without any disadvantages.

A11.3 What can be improved? - retail features euro

Table A11.6 indicates which retail features of the existing euro banknote series have better options to return – improved – in the next series. Improvements can be made on both design (perception, e.g. easy to understand and univocal) and technology (e.g. two different inks with different spectral curves in the IR part of the spectrum).

A11.4 What comes in? - retail features euro

Three new retail features are scored on the criteria in Table A11.7. Botanic DNA and thin steel fibres are discussed in Appendix 4. A polarisation filter is described in the study 'Public feedback for better banknote design 2 [94] and shown in Figure 14. A laser pen and opaque white boll is described in the paper 'Life cycle analysis of security features of banknotes'[69].

Appendix 12
All-in-one method applied to public features in euro banknotes

Chapter 4 describes the all-in-one method as applied to the public features of the euro banknotes. Detailed information on how the criteria are scored is not part of Chapter 4 and is provided in this Appendix. The user of the all-in-one methodology might come up with very different results by coding the criteria differently; of course, one may lay down other thresholds than the ones proposed.
The structure of the all-in-one method is followed:

A12.1 Defining action-feature matrix,
A12.2 What goes out? - public features euro,
A12.3 What can be improved? - public features euro,
A12.4 What comes in? - public features euro.

A12.1 Defining action-feature matrix

The action-feature matrix with a disruptive human action was proposed in Table 23.

A12.2 What goes out? - public features euro

There are several criteria to audit the public security features of the euro banknotes. The first is the public knowledge.

Public knowledge of security features
In general the knowledge on public features is limited. A large group is not aware of any security feature (Appendix A1).
Table A12.1 indicates that the watermark and the hologram/silver foil are the public features in the euro banknotes most widely known and should from this view return – improved – in the next series.

Criterion
Green: Score public knowledge > 50%.
Red : Score public knowledge < 10%.

Table A12.1

Public security features euro series 2002	Public knowledge in NL (2009)
1. Watermark	76%
2. Hologram/silver foil	55%
3. Tactility (raised ink, relief, paper)	22%
4. Security thread	15%
5. See-through register	9%
6. Special ink - 6.1 Colour-changing number (OVI)	3%
- 6.2 Glossy gold stripe (iridescent)	2%

Ranking of public security features on the basis of public knowledge in the Netherlands in 2009. In the euro series, the security features in the low denominations (5, 10 and 20 euro) differ from those in the high denominations. The low ones have glossy gold stripes (iridescent ink) on the reverse side, while the high denominations (50, 100, 200 and 500) colour-changing numbers. Furthermore, the foil stripe occurs on the low denominations, ands the foil patch on the high ones, but both features are judged as being similar from a security printing point of view.

Table A12.2

Euro 50 - Public security features	Estimated time
1. Watermark	4 s
2. Hologram/silver foil	3 s
3. Tactile properties	
3.1 Tactile relief	1 s
3.2 Scratch	1 s
4. Security thread including text	3.5 s
5. See-through register	5.5 s
6. Special ink	
6.1 Colour-changing number	3 s
6.2 *Glossy gold stripe*	*(2 s)*
Total to check all public features (excl. 6.2)	**21 s**

Estimated time for checking public security features in a euro 50 banknote. Not being part of the euro 50 banknote, the glossy gold stripe is not included in the total time. The estimation uses data of Bank of Canada as provided in Table 19.

User requirements
The user requirements are listed in Chapter 4, including the proposed audit criteria. Data concerning the user requirement 'time' is provided in Table A12.2. Checking all 6 public features in a euro 50 banknote would take an estimated 21 seconds.

Criterion
Green: Operation time < 2 s.
Red : Operation time > 4 s.

Counterfeit analysis
The results on the counterfeit analyses are provided in Table A12.3. The counterfeiter is very well able to imitate the watermark and see-through register. According to the simple method these features received the highest scores.

The paper weight of the euro banknotes is 85 g/m² and comes close to standard paper in copy machines or other printers, which is 80 g/m². Being of more importance is

Table A12.3 What goes out?

Public security features
euro series 2002

Criteria	Watermark	Hologram/foil	Rubbing finger	Nail scratch	Security thread	See-through register	Colour changing ink	Glossy gold stripe
Counterfeit analysis								
1. Counterfeit frequency								
2. Intrinsic - extrinsic								
3. Internal - add on								
4. System approach								
4.1 Resolution								
4.2 Colour								
4.3 Density								
4.4 Geometry								
4.5 Mass								
4.6 Material								
5. Simple model								
6. Public testing (DNB, 2006)								
7. Integrated design, no island								

Overview of the counterfeit analysis of the public features in the euro banknotes.Theoretical exercise. Scored by De Heij.

Table A12.4

Production step	Cost in euro-cent per feature – euro 50 note	Public security feature
Paper	0.11	1. Multi tone watermark with highlight
		2. Security thread
Foil stripe (10 mm)	0.55	3. Foil stripe with hologram
Print - offset	0.07	4. See-through register
Print - intaglio	0.13	5. Tactile properties (rub text, nail scratch)
Silk screen (OVI)	1.0	6. Special ink OVI
Iridescent band	0.3	6. Special ink iridescent band

Overview of the costs of the public security features in the euro banknotes per production step (based on Table 31).

the colour of the standard copy paper. This off-white, yellowish tint is quite close to the paper tint of the euro 50 and is UV dull. Since the paper tints of the euro series are all different the judgement on the colour of the watermark is flagged yellow (and red for the 50 euro).

Cost
The cost of the OVI exceeds the 10% threshold on the cost criterion (Table A12.4).

Criterion
Green: Feature cost is < 0.35 eurocent (or 5% of average note price of one euro 50 banknote).
Red : Feature cost is > 0.7 eurocent (or 10% of average note price of one euro 50 banknote).

Life span
The life span of a security feature should be set at 20 years, the period after which a patent will expire. Some features may have an additional nest level which might still be protected by a patent while the patent on the original feature has expired. The two special colours in the euro series (iridescence and OVI) receive a red score on life span, because today they are purchasable within the public domain.

Space
Table A12.5 provides a breakdown of the space used for the different features in a euro 50 banknote. Just 15% of the total surface of a euro 50 banknote is covered with public security features [108].

Table A12.5

Public feature in euro series 2002	Surface in euro 50	In mm²
1. Watermark	36 mm x 20 mm (x 2)	1.440
2. Hologram/silver foil (patch)	20 mm x 16 mm	320
Foil stripe (in euro 50)	12 mm x 77 mm	924
3. Tactility - rub (text)	32 mm x 2 mm	64
- scratch	14 mm x 5 mm	70
4. Security thread	12 mm x 77 mm (x 2)	1.848
5. See-through register	10 mm x 10 mm (x 2)	200
6. Colour-changing ink (OVI)	17 mm x 12 mm	204
7. Glossy gold stripe (in euro 50)	10 mm x 77 mm	770

Public security features in a euro 50 banknote and the space they occupy. The thread is 1.2 mm-wide, but the so-called wandering zone (movement area) is 12 mm (2 x 6 mm), enough to prevent bumps forming in a pile of sheets.

Watermark and security thread receive a red score on space because they are too large, while rub and scratch tactility receive a red flag for being too small.

Input from others

Two central banks have evaluated their existing banknotes, using different methods:

- ECB: Resilience Grades (2007),
- Bank of Canada: feature effectiveness (2010).

Table A12.6

Public feature in euro series 2002	Resilience grades
1. Multitone watermark and electrotype	
2. Security thread	
3. Foil stripe (with hologram)	
4. Intaglio	
5. Iridescent stripe	
6. Foil patch (with hologram)	
7. OVI	
8. See-through register	

Resilience scores of the public security features in the euro series 2002. The following thresholds are laid down by De Heij (red < 40 RG points and green > 50 RG points).

Table A12.7

Public feature in CAD 100	Security effectiveness
1. Foil stripe (with hologram)	
2. Security thread	
3. Watermark	
4. See-through register	

Feature effectiveness of a CAD 100 banknote according to Bank of Canada.

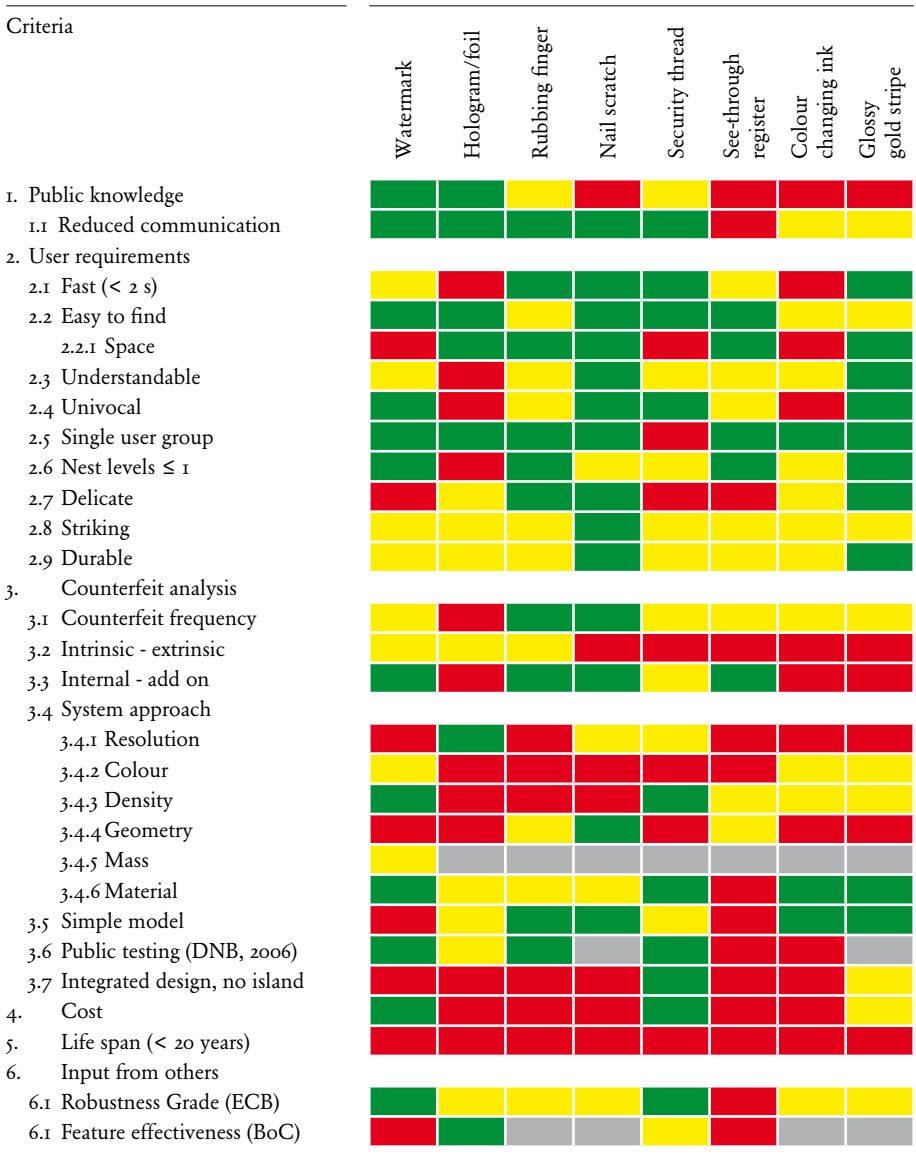
In 2008, the ECB ranked the public security features of the euro banknotes according to their Resilience Grades (RG). Watermark and security thread are found to be the most robust. The see-through register received the lowest score as is shown in Table A12.6.

Bank of Canada: feature effectiveness
Just as in the ECB study, the see-through register is found not effective according to the Bank of Canada. The best score is for the foil stripe (Table A12.7).

Overall table
Table A12.8 is the final result: a complete feature-criterion matrix 'what goes out?'. All public features of the euro series 2002 have shortcomings (red lights); not a single feature is without any disadvantages. This exercise on the euro banknotes is an example, illustrating the method, while a scoring procedure involving more people is a recommended option. Adding or removing criteria is also up to your consideration. Analysing Table A12.8 one may conclude the following and, again, others may arrive at different conclusions:
Out:
1) See-through register,
2) Colour-changing ink,
3) Holographic foil,
Dubious:
4) Watermark,
In:
5) Tactility,
6) Security thread,
7) Glossy gold stripe.

Table A12.8 What goes out?

Public security features
euro series 2002



Theoretical exercise of the public features-criterion matrix *What goes out?*. Overview of all criteria used on all public security features of the euro banknotes. Scored by De Heij.

Table A12.9 What can be improved?

Public security features euro series 2002	Feel		Look-through		Tilt	
Criteria	Rub (with CtIP)	Scratch (with CtIP)	Innovative watermark	Windowed security thread	Strong iridescent colour	Improved OVI (Spark)
1. User requirements						
1.1 Fast (< 2 s)						
1.2 Easy to find						
1.2.1 Space						
1.3 Understandable						
1.4 Univocal						
1.5 Single user group						
1.6 Nest levels ≤ 1						
1.7 Delicate						
1.8 Striking						
1.9 Durable						
2. Counterfeit analysis						
2.1 Intrinsic - extrinsic						
2.2 Internal - add on						
2.3 System approach						
2.3.1 Resolution						
2.3.2 Colour						
2.3.3 Density						
2.3.4 Geometry						
2.3.5 Mass						
2.3.6 Material						
2.4 Integrated design, no island						
3. Cost						
4. Life span (< 20 years)						

Theoretical exercise of the public feature-criterion matrix *What can be improved?*. Scored are the expected options on improvement on both design and technology. The innovative watermark (Figure 2) is included for illustrative reasons. Scored by De Heij.

A12.3 What can be improved? - public features euro

Tactility, security thread and glossy gold stripe are the public features retained, forming the basis for Table A12.9. In that table, the top row indicates the required human actions 'feel, look-through and tilt' (there is no look-at feature in the euro

banknotes). Technical proposals are entered in the second row, like CtIP and windowed security threads. Two more improved features have been added: strong iridescent ink with a more powerful effect and an improved OVI called Spark. The innovative watermark (Figure 2) is also included for illustrative reasons.

Looking at Table A12.9 most green lights are given for:
- Feel: nail scratch feature,
- Look-through: windowed security thread,
- Tilt: strong iridescent colour.

A12.4 What goes in? - pubic features euro

The all-in-one method is continued with step 4, in which the focus is on what goes in. In case of the public features we are looking for 3 new features (next to 3 features that have to be improved):
- One feel feature,
- One look-at feature,
- One tilt feature.

Looking at Table 25 the following features received most green lights:
- 3D foil image (e-beam based foil image),
- Piezochemistry,
- Mobile phone, camera feature (e.g. based on an IR image).

A feature without any red lights is:
- New feel feature (tactile elements inside paper).

Reference (Chronological)

1. Ebbinghaus, Hermann; 'Über das Gedächtnis' (1865). Translated by Henry A. Ruger & Clara E. Bussenius to 'Memory: A Contribution to Experimental Psychology', Teachers College, Columbia University, New York, 1913
2. 'Moiré, interferentieverschijnselen bij rasterdruk', Instituut voor Grafische Techniek, Amsterdam, 1945
3. Miller, G.A.; 'The magical number seven, plus or minus two: Some limits on our capacity for processing information' Psychological Review 63, page 81-97, 1956
4. Bloom, Murray Teigh; 'The Man Who Stole Portugal' Scribner, New York, 1966
5. Peek, J.; 'Plaatjes in leerprocessen (Research on pictures in learning)' PhD Study, University of Utrecht, Drukkerij Elinkwijk, Utrecht, 8 December 1972
6. Koeze, P.; 'Fysische eigenschappen van papier en andere materialen' De Nederlandsche Bank NV, Amsterdam, 24 June 1976 - internal document
7. Koeze, P.; 'Beveiligende kenmerken van bankbiljetten' De Nederlandsche Bank NV, Amsterdam, 30 March 1979 - internal document
8. Koeze, P.; 'A graphic method of predicting and constructing moiré patterns', published in Optica Acta, Vol. 29, No. 5, 1982, page 595-610. Also issued as 'DNB Reprint No. 80'.
9. Koeze, Peter; 'Printed matter having elements to indicate counterfeiting, and method for manufacturing such printed matter', De Nederlandsche Bank NV, European Patent Application, published 24 February 1982 This patent application is also filed as US Patent office - patent 292 381 (13 August 1981) and Canada patent 384 219 (19 August 1981). The outcome of the examination of 28 January 1983: Canadian patent 1 070 731 granted on 29 January 1980 appears similar to the DNB patent application. This was later agreed by DNB (by letter of 16 March 1983), and all 3 patent applications were withdrawn in 1983.
10. Koeze, Peter; 'Mechanical sorting, data processing and security against counterfeiting' De Nederlandsche Bank NV, presented at Banknkote Printers' Conference, Helsinki, 1982
11. Bloom, Murray Teigh; 'Money of Their Own: the True Story of the World's Greatest Counterfeiters' ISBN 0931960096, BNR Press, Port Clinton, Ohio, 1982
12. Bloom, Murray Teigh; 'The Brotherhood of Money. The Secret World of Banknote Printers' ISBN 0931960126, BNR Press, Port Clinton, Ohio, 1983

13. De Heij, H.A.M. and P. Koeze; 'Detailweergave element' De Nederlandsche Bank NV, Amsterdam, 9 November 1984 - internal document
14. Boeschoten, W.C. and P.D. van Loo; 'Valsemunterij: algemene aspecten en de betekenis in Nederland' Reprint 123, De Nederlandsche Bank NV, Amsterdam, December 1984
15. 'Advanced Reprographic Systems: Counterfeiting Threat and Deterrent Measures' National Materials Advisory Board, National Academy of Press, Washington DC, 1985
16. De Heij, H.A.M. and P. Koeze:'Echt of namaak? Van 4 naar 20 echtheidskenmerken' De Florijn, De Nederlandsche Bank NV, Volume 9, Number 1, Amsterdam, January 1986
17. De Heij, H.A.M.; 'Selecteren van produktvoorstellen' De Ingenieur, Volume 98, Issue 12, The Hague, December 1986
Also issued as 'DNB Reprint No. 163'.
18. Fase, M.M.G, J.R. Steinhauser and Joh. de Vries; 'Het Nederlandse bankbiljet in zijn verscheidenheid' Monetaire Monografieën Nr. 6, De Nederlandsche Bank NV, Kluwer, Deventer, 1986
19. De Heij, H.A.M. and P. Koeze; 'Vormgeving kleuren buiten de Europaschaal' De Nederlandsche Bank N.V., Amsterdam, 7 April 1986 - internal document.
20. De Heij, H.A.M. and P. Koeze; 'Leesbare letters' Compres, Volume 12, Issue 6, 17 March 1987. Also issued as 'DNB Reprint No. 176' and printed in Cicero, Volume 4, Issue 87, Antwerpen, April 1987. Also issued in French: 'Des caractères lisibles' Volume 4, Issue 87, Antwerpen, April 1987
21. Lemmers, J.J.; 'Proef - kleuren buiten de Europaschaal - II' Joh. Enschedé en Zonen Grafische Inrichting BV, Haarlem, 30 September 1987
22. De Heij, H.A.M.; 'Principe oplossingen grijstrap in bankbiljetten' De Nederlandsche Bank NV, Amsterdam, 20 October 1987 - internal document.
23. De Heij, H.A.M.; 'Banknote paper identification with a waternumber', De Nederlandsche Bank NV, presented at BPC Paper Committee, London, 1987
24. Biederman, I.; 'Recognition by components: A theory of human image understanding', Psychological Review, 92(2) page 115 - 147, 1987
25. 'Counterfeit Threats and Deterrent Measures' National Materials Advisory Board, National Academy of Press, Washington DC, 1987
26. Hewitt, V.H. and J.M.Keyworth; 'As Good as Gold; 300 Years of British Bank Note Design' ISBN 0 7141 0868 5, British Museum Press, London, 1987
27. Lemmers, J.J.; 'Densiteitsverlopen als beveiliging tegen namaak', Joh. Enschedé en Zonen Grafische Inrichting BV, Haarlem, 30 June 1988
28. De Heij, H.A.M.; 'Beveiliging bankbiljetten tegen kleurenkopieermachines', policy document to Board of DNB, Afdeling Bankbiljetten-technische ontwikkeling, De Nederlandsche Bank NV, Amsterdam, 2 November 1989 - internal document

29. Van Erve, P.C.J.F.; 'Voorlichting over (valse) bankbiljetten' Bank- en Effectenbedrijf (39)3 (DNB Overdruk 259), Amsterdam, March 1990
30. De Heij, Hans; 'Dakpansgewijs met behoud van serie-indruk - De opdracht voor een serie-ontwerp' De Florijn, Jaargang 13, Nummer 3, De Nederlandsche Bank NV, Amsterdam, March 1990
31. Van Gelder, Ed; 'Papier…'om te rouleren voor en in stede van contant geld' Bührmann-Ubbens Papier BV, Zutphen, 1990
32. Kranister, Willibald; 'The Moneymakers International' ISBN 0 9514522 0 7, Probus Pub Co, March 1991
33. De Heij, H.A.M.; 'Market-based strategy for the development of new security features for banknote paper' De Nederlandsche Bank NV, presented at BPC Paper Committee, Copenhagen, 27-28 May 1991
34. Grolle, J.J.; 'Geschiedenis van het Nederlandse bankbiljet' Laurens Schulman BV, ISBN 90-74162-01-0, Bussum, 1991
35. Schaap, C.D., B. van Vliet; 'Vals geld bestrijding' Uitgeverij J.B. van den Brink & Co, Lochem, 1991
36. 'Counterfeit Deterrent Features for the Next-Generation Currency Design' National Research Council, Publication NMAB-472 National Academy Press, Washington DC, 1993
37. De Heij, H.A.M.; 'Market-based strategy for the development of new security features for banknote paper' De Nederlandsche Bank NV, presented at the BPC General Meeting, Amsterdam, 18-21 May 1992
38. Byatt, Derrick; 'Promises to Pay: The First Three Hundred Years of Bank of England Notes' ISBN 0907605508, Spink & Son Ltd, London, 1994
39. Herman, Jürgen; 'Wertpapier mit Fenster' Patent Application DE 43 34 848 C1, Deutsches Patentamt, 5 January 1995
40. Carter, Rita; 'Mapping the mind' Weidenfeld & Nicolson, London, 1998
41. De Heij, H.A.M.; 'An experiment with red tinted paper in a green printed note' De Nederlandsche Bank. NV, presented at BPC Paper Committee, Amsterdam, 15-17 April 1996
42. French, John; 'On the right wavelength - magnetic particle printing' based on a presentation made by John French, Product & Image Security, 1997
43. Bolten, Jaap; 'Dutch Banknote Design 1814 – 2002' including 'Catalogue of Dutch banknotes 1814 - 2002' by J.J. Grolle en P. Koeze, ISBN 90-804784-2-3 De Nederlandsche Bank NV, Primavera Press, Leiden, 1999
44. De Heij, H.A.M.; 'The design methodology of Dutch banknotes', Optical Security and Counterfeit Deterrence Techniques III, Proceedings of SPIE Vol. 3973 (ISBN 0 - 8194 - 3591- 0), San Jose, California USA 27-28 January, 2000
45. Bakker-Rijnbeek, L.M.; 'Jaarverslag falisificaten 2000', De Nederlandsche Bank NV, Amsterdam, 6 September 2001 - internal document
46. Keyworth, John; 'Forgery. The Artful Crime. A brief history of the forgery of Bank of England notes' Bank of England Museum, London, 2001

47. Drazen Prelec and Duncan Simester; 'Always Leave Home Without It: a Further Investigation of the Credit-Card Effect on Willingness to Pay', Marketing Letters 12(1), page 5-12, Kluwer Academic Publishers, 2001
48. Brion, René and Jean-Louis Moreau:'A Flutter of Banknotes ; From the First European Paper Money to the Euro' Mercatorfonds, ISBN 90 6153 5131, Antwerp, 2001
49. De Heij, H.A.M.; 'A method for measuring the public's appreciation and knowledge of banknotes' Optical Security and Counterfeit Deterrence Techniques IV, Proceedings of SPIE Vol. 4677 (ISBN 0-8194-4417-0), San Jose, California USA, 23-25 January 2002
50. 'Intaglio. The Handbook' Giesecke & Devrient GmbH, KBA-Giori SA, Sicpa SA, 2002
51. Van Renesse, Rudolf; 'Hidden and scrambled images - a review' Proceedings SPIE, 4677 (ed. R. van Renesse), 2002, pages 333-348
52. Lyutov, V.V. and A.V. Yurov; 'Experience of application of security features for banknotes of the Bank of Russia' St. Petersburg, 2002
53. De Heij, H.A.M., Lisa a. DiNunzio and Olivier Strube; 'Comparence EUR - USD Banknotes Public's Appreciation and Knowledge' De Nederlandsche Bank NV, US Treasury BEP and European Central Bank, presented at Banknote 2003, Washington DC, USA, 2-5 February 2003
54. De Heij, Henricus A.M. and Thomas Buitelaar; 'Series of security documents provided with a watermark in the form of a barcode' EP 1 273 461 A3, European Patent Office, 5 March 2003
55. Koeze, Peter; 'Het watermark in het Nederlandse bankbiljet 1814-2002', De Nederlandsche Bank NV, Amsterdam, unpublished, 24 March 2003
56. De Heij, Hans and Ton Roos; 'Free Intaglio Detector', letter to De La Rue Currency, De Nederlandsche Bank NV, Amsterdam, 27 March 2003
57. 'Next generation of euro banknotes will be different' interview with Antti Heinonen (ECB), Keesing's Journal of Documents, Issue 3, Amsterdam, 2003
58. 'R&D Plans for new Euro Unveiled' interview with Brian Dennis (ECB), Currency News, Volume 1, No 5, Shepperton, May 2003
59. 'Euro banknote design exhibition' European Central Bank, ISBN 92-9181-393-1, Frankfurt, September 2003
60. 'Quantitative survey 'Professional cash handlers' by TNS/NIPO, prepared for the European Central Bank, Frankfurt, 7 February 2004
61. Church, S. and L. Setlakwe; 'Analysis of counterfeits and public survey results as design input' Proceedings SPIE, 5310 (ed. R. van Renesse), 2004, pages 63-73
62. 'Betalen kost geld', Werkgroep Kostenonderzoek Toonbankbetaalproducten, Maatschappelijk Overleg Betalingsverkeer, De Nederlandsche Bank NV, March 2004. A summery 'The cost of payments' can be found in the Quarterly Bulletin of DNB, March 2004

63. De Heij, Hans; 'Foil with public appeal (for new designs of euro banknotes)' De Nederlandsche Bank NV, prepared for the European Central Bank, Amsterdam 9 June 2004 - confidential
64. De Heij, Hans and Jeanine Kippers; 'Efficient cash payments with euro coins and banknotes in the Netherlands', De Nederlandsche Bank NV, presented at Banknote Printers' Conference, Dresden, 6-9 September 2004
65. Mooij, Joke and Ton Dongelmans; 'Mogen wij even afrekenen? Twee eeuwen betalen in Nederland', ISBN 90 5352 981 0, Boom, Amsterdam, 2004
66. 'Recycling of euro banknotes: framework for the detection of counterfeits and fitness sorting by credit institutions and other professional cash handlers'; European Central Bank, Frankfurt, January 2005
67. Gentaz, E.; 'Evalutation of multi-sensory training in the detection of counterfeit banknotes for retail cashiers in Europe' Centre Nationale de la Recherche Scientifique, Université Pierre Mendès France, Grenoble, France, 17 January, 2005
68. 'The second series of euro banknotes' Annual Report, European Central Bank, Frankfurt, 2005
69. De Heij, Hans A.M.; 'Life cycle analysis of security features in banknotes; from central bank to retailer' De Nederlandsche Bank NV, presented at Banknote 2005, Washington, 20-23 February 2005
70. De Heij, Hans and Javier Gamo; 'Counterfeit report foil with public appeal' De Nederlandsche Bank NV, prepared for the European Central Bank, Amsterdam, 23 March 2005 - confidential
71. 'The euro banknotes: developments and future challenges' Monthly Bulletin, European Central Bank, Frankfurt, August 2005
72. De Heij, Hans; 'Evaluation of counterfeits, development of methodology' De Nederlandsche Bank NV, presented at RRC Users Meeting, Ottawa, Canada, 28-29 September 2005
73. Jonker, Nicole; 'Payment Instruments as Perceived by Consumers - a public survey' DNB Working Paper No. 53, De Nederlandsche Bank NV, Amsterdam, September 2005
74. Schmitz, Stijn; 'Nieuwe echtheidskenmerken, nieuwe octrooien' P-Florijn, Issue 19, De Nederlandsche Bank NV, Amsterdam, 6 October 2005
75. 'Nachrichten aus Euro-Land: Neue Euro-Scheine bis 2010?' Münzen & Sammeln, Regenstauf, November 2005
76. De Heij, H.A.M. and T.R. Stange; 'Authenticity mark' Deutsches Patent- und Merkenamt, DE 60 2005 000 658 T2 2007.11.15. European Patent Office, EP 1 607 235 BI. Date of filing: 21 December 2005. Date of publication and mention of the grant of the patent: 7 March 2007.
77. Van Renesse, Rudolf L.; 'Optical Document Security' (Third Edition), Artech House ISBN 1-58053-258-6, Boston London, 2005
78. Schaede, Johannes, Volker Lohweg; 'The mechanism of human recognition as a guideline for security feature development' KBA-Giori SA, Optical

Security and Counterfeit Deterence Techniques VI, Proceedings of SPIE Vol. 6075 (ISBN 0-8194-6115-6), San Jose, California USA, 17-19 January 2006
79. Lancaster, Ian M.; 'Use and Efficacy of DOVIDs and other Optical Security Devices', Optical Security and Counterfeit Deterence Techniques VI, Proceedings of SPIE Vol. 6075 (ISBN 0-8194-6115-6), San Jose, California USA, 17-19 January 2006
80. Jonker, Nicole, Bram Scholten, Marco Wind, Martijn van Emmerik and Marike van der Hoeven; 'Counterfeit or genuine: can you tell the difference?' DNB Working Paper 121, De Nederlandsche Bank NV, Amsterdam, 2006
81. De Heij, H.A.M.; 'Public feed back for better banknote design' DNB Working Paper No. 104, De Nederlandsche Bank NV, Amsterdam, June 2006
82. De Heij, Hans and Alwin van Gelder; 'Numbers on Banknotes. What is their use?' Keesing Journal of Documents & Identity, Issue 20, Amsterdam, 2006
83. De Heij, Hans and Alwin van Gelder; 'Numbers on Banknotes. What is their use? Part II' Keesing Journal of Documents & Identity, Issue 21, Amsterdam, September 2006
84. Boersema, Theo; 'Comprehensibility of graphical symbols for clarifying security features' in D. de Waard, K.A. Brookhuis and A. Toffetti (Eds), 'Developments in Human Factors n Transportation, Design, and Evaluation, Shaker Publishing Maastricht, 2006, page 333 - 344
85. Van Haeften, Ewout; 'Counterfeit threat assessment. A methodology approach' power point presentation to the Counterfeit Working Group (ESCB), De Nederlandsche Bank NV, Frankfurt, October 2006
86. Van Gelder, Alwin; 'Euro Counterfeits in the Netherlands' De Nederlandsche Bank NV, presented at RRC User's Meeting, Oslo, 2006
87. Verstraten, Frans; 'Psychologie in een notendop' Uitgeverij Bert Bakker, ISBN 90 351 2905 9, Amsterdam, 2006
88. Van Renesse, R.L; 'What is "funny"about Funny Money?' Keesing Journal of Documents & Identity, Issue 20, Amsterdam, 2006
89. Bear, M., B.W. Connor and M. Paradiso: 'Neuroscience - Exploring the brain' Lippincott Williams & Wilkins, 3th edition, 2006
90. Bender, Klaus W.; 'Moneymakers The Secret World of Banknote Printing' Wiley-VCH Verlag Gmbh & Co, KGA,Weinheim 2006 (original edition 'Geldmacher' was published in 2004)
91. Lingnau, A., Francesco Pavani and Jens Schwarzbach; 'How do People Manipulate Banknotes?' Study for ECB, Center for Mind/Brain Sciences, University of Trento, Italy, April 2007 - confidential
92. Heinonen, Antti; 'The euro banknotes: recent experiences and future challenges', Currency Conference, Bangkok, 6-9 May 2007
93. 'First International Conference on the Protection of the Euro against Counterfeiting: The euro is in safe hands' Press release European Central Bank, The Hague, The Netherlands, 16 May 2007

94. De Heij, Hans; 'Public feedback for better banknote design 2', Occasional Studies, Volume 5, Number 2, De Nederlandsche Bank NV, Amsterdam, September 2007
95. 'Increases all round for Australia' Currency News Volume 5, Number 9, Shepperton, September 2007
96. 'More variations on opals for security' Currency News Volume 5, Number 9, Shepperton, September 2007
97. Dinjens, Marlies; 'Winkeliers doen biljet van 100 euro in de ban' Volkskrant, Amsterdam, 12 September 2007
98. Buitelaar, Tom; 'Counterfeit Threat Assessment' De Nederlandsche Bank NV, presented at RRC User Meeting, Lausanne, 25-26 September 2007
99. 'Circulation and supply of euro banknotes and preparations for the second series of banknotes' ECB Monthly Bulletin, European Central Bank, Frankfurt, October 2007
100. 'Survey Among Cash Handlers in the Euro Area', TNS prepared for European Central Bank, Frankfurt, November 2007
101. Moxley, Jill, Helen Meubus, and Maura Brown: '*The Candadian Journey*: An Odyssey into the Complex World of Bank Note Production' Bank of Canada Review, Bank of Canada, Ottawa, Autumn 2007
102. 'A Path to the Next Generation of U.S. Banknotes: Keeping them Real' US National Research Council, Committee on Technologies to Deter Currency Counterfeiting, The National Academic Press, ISBN 0-309-10575-7, Washington, 2007
103. Baddeley, A.; 'Working memory, thought and action' Oxford University Press, Oxford, 2007
104. Galán Camacho, Jorge Eduardo and Miguel Sarmiento Paipilla; 'Banknote Printing at Modern Central Banking: Trends, Costs, and Efficiency' Banca de Republica Colombia, Borradores de Economía Issue 476, Bogota, 2007
105. Schell, Karel Johan; 'History of Document Security' in 'The History of Information Security: A Comprehensive Handbook' by Karl de Leeuw and Jan Bergstra, ISBN 9780444516084, Elsevier Amsterdam Oxford, 2007
106. Holm, Elizabeth; 'A flow model for banknote feature evaluation' Sanda National Laboratories, 'The Conference on Optical Security and Counterfeit Deterrence', San Francisco, 23-25 January 2008
107. Church, S., T. Granzotis, M. Lacelle and A. Firth; 'Methodology for establishing bank note security requirements' Bank of Canada, 'The Conference on Optical Security and Counterfeit Deterrence', San Francisco, 23-25 January 2008
108. De Heij, Hans A.M.; 'Programme of Requirements: a powerful tool to develop new, secure banknotes' De Nederlandsche Bank NV, 'The Conference on Optical Security and Counterfeit Deterrence', San Francisco, 23-25 January 2008

109. 'How the euro became our money' European Central Bank, ISBN 92-9181-985-9, Frankfurt, 2007
110. Ware, Colin; 'Visual thinking for Design' Elsevier, ISBN 978-0-12-370896-0, Amsterdam, 2008
111. 'Optical document security - past, present and future' Currency News Vol. 6, No. 2, Shepperton, February 2008
112. De Heij, Hans; 'Banknote opinion polls: a method for collecting customer feedback on banknote design' DNB Cash Seminar 2008, De Nederlandsche Bank NV, Amsterdam, 28-29 February 2008
113. 'Dramatic Fall in Counterfeits Brings Canada Close to Target' Currency News, Vol. 6 No. 3, Shepperton, March 2008
114. '€50 leads the way for 2nd series' Currency News, Vol. 4, No. 4, Shepperton, April 2008
115. 'Euro banknotes - a tangible symbol of integration' Monthly Bulletin, 10th Anniversary of the ECB, European Central Bank, Frankfurt, May 2008
116. 'Security Feature (Usability Quadrant) Perception Study', by Daniel Smilek, Kelly A. Malcolmson & Jonathan S.A. Carriere, Bank of Canada, presented at RRC User Meeting, Lausanne, 2 July 2008 - confidential
117. Negueruela, Darió J. and Maria José Fernández; 'Have people learned to love euro banknotes yet?', power point presentation, Banco de España, Currency Conference Prague, 12-15 October 2008
118. Thick, Jacqui; 'The Curse of Complexity' power point presentation, De La Rue Currency, Currency Conference Prague, 12-15 October 2008
119. Pacreu, Jaime; 'Interview with Thomas A. Ferguson, former Director of the Bureau of Engraving and Printing of the United States', Billetaria, No. 4, Madrid, October 2008
120. 'Main trends in counterfeit deterrence in the banking system of the Russian Federation', Banknotes of the World, No. 10, Moscow, October 2008
121. 'NexGen 100-Dollar Note Will Become a New Stage in the Long History of US Money', interview with Larry Felix, Banknotes of the World, Number 8, Moscow, October 2008
122. 'Het mooie van geld' Blauw, Year 3, Issue 2, Blue Sky Group, Amstelveen, October 2008
123. Geldsammler 2008/11, November 2008
124. 'HBD Monitor Betalingsverkeer 2008', Hoofdbedrijfschap Detailhandel, Den Haag, 2008
125. Alter, Adam L. and Daniel M. Oppenheimer; 'Easy on the Mind, Easy on the Wallet: The Roles of Familiarity and Processing Fluency in Valuation Judgments' Princeton University, 2008
126. Summers, Ian R. Richard J. Irwin and Alan C. Brady; 'Haptic discrimination of paper' in Human Haptic Perception Basics and Applications, edited by Grunwald, Martin (Ed.), Birkhäuser, ISBN 978-3-7643-7611-6, 2008

127. Wijnen, Frank and Frans Verstraten (red.); 'Het brein te kijk. Verkenning van de cognitieve neurowetenschap' Pearson Assesment and Information BV, Edition 4 (revised), ISBN 978 90 265 1807 2, Amsterdam, 2008
128. 'Currency Counterfeiting on the Rise' Currency News, Vol. 7 No. 1, Shepperton, January 2009
129. Firth, Andrea V. and Sara E. Church; 'Building better banknotes. The role of scientific research at the Bank of Canada' Journal of Documents & Identity, Keesing Reference Systems, Issue 28, Amsterdam, 2009
130. Ashbourn, Julian; 'Documented thoughts' Journal of Documents & Identity, Keesing Reference Systems, Issue 28, Amsterdam, 2009
131. Schilling, Andreas; 'Diffractive OVDs and banknote windows' Keesing Journal of Documents & Identity, Issue 28, Amsterdam, 2009
132. 'The Bank Note Confidence Survey', web site Bank of Canada. Purchased 20 February 2009
133. Visser, Julie and Judith Sonke; 'Euro Banknotes. A study about awareness and recognition of euro banknotes among the Dutch' report by TNS NIPO prepared for De Nederlandsche Bank NV, Amsterdam, 24 March 2009
134. De Heij, Hans; 'Innovative approaches to banknote design' De Nederlandsche Bank NV, power point presentation, presented at Watermark Conference, Kazan, 23-25 June 2009
135. Garic, Natali; 'Where Security Meets Durability' Crane Currency, power point presentation, presented at Watermark Conference, Kazan, 23-25 June 2009
136. 'Towards the second series of euro banknotes' interview with Antti Heinonen, Banknotes of the World No. 6, Moscow, June 2009
137. Van Roon, Joost; 'Contemporary passport design' Journal of Documents & Identity, Issue 29, ISSN 1571-0564, Amsterdam, 2009
138. 'Latest developments in payment and settlement systems' Quarterly Bulletin, De Nederlandsche Bank NV, Amsterdam, June 2009
139. 'Surge in Bank of England Counterfeits' Currency News, Volume 7, Number 6, Shepperton, June 2009
140. 'Currency provides anything but a tall order for De La Rue's new CEO' Currency News, Vol 7, No 6, Shepperton June 2009
141. Kersten, Jason; 'The Art of Making Money -The Story of a Master Counterfeiter' Gotham-Penguin, ISBN 1592404464, June 2009
142. 'Do not look down on counterfeits' Banknotes of the World, Number 7, Moscow, July 2009
143. 'Biannual information on euro banknote counterfeiting' press release ECB, Frankfurt, 13 July 2009
144. 'Meer valse eurobiljetten onderschept in Nederland' press release DNB, Amsterdam, 13 July 2009
145. Infosecura, 13th year, number 40, July 2009

146. Balueva, Tatiana; 'In search of new images' interview with Hans de Heij, Watermark, Number 5, St. Petersburg, 2009
147. Van den Kommer, Esther; 'Communication on euro banknotes', De Nederlandsche Bank NV, presented at Cash Seminar, Budapest, 7 October 2009
148. De Heij, Hans; 'Banknote design for the visually impaired' De Nederlandsche Bank NV, Occasional Study 2009 Volume 7, Number 2, Amsterdam, October 2009
149. McCallum, Allister; 'The Eurosystem's Approach to Quantifying the Threat Posed by Counterfeiting' European Central Bank, presented at Banknote 2009, Washington 6 - 9 December 2009
150. Meyers, Judith Diaz; 'Development of Security Features for the Next Generation of U.S. currency' U.S. Bureau of Printing and Engraving, presented at Banknote 2009, Washington 6-9 December 2009
151. 'Survey on cash handlers in euro area countries 2009' TNS Opinion, prepared for the European Central Bank, Frankfurt, December 2009
152. 'HBD Monitor Betalingsverkeer 2009', Hoofdbedrijfschap Detailhandel, Den Haag, 2009
153. 'Payment behaviour in Germany' Deutsche Bundesbank, Frankfurt, 2009
154. 'The National Retailer Research Program Results for Q4 2009' Bank of Canada (website), 2010
155. Balodis, Erik and Andrea Firth, Daniel Smilek and Kelly Malcolmson; 'A Method for Quantitatively Determining the Security Effectiveness of Bank Note Security Features and Whole Notes' Bank of Canada and University of Waterloo, presented at 'The Conference on Optical Security and Counterfeit Deterrence', San Francisco, 20-22 January 2010
156. De Heij, Hans A.M.; 'Innovative approaches to the selection of banknote security features' De Nederlandsche Bank NV, presented at 'The Conference on Optical Security and Counterfeit Deterrence', San Francisco, 20-22 January 2010
157. Lohweg, Volker and Johannes Schaede:'Document Production and Verification by Optimization of Feature Platform Exploitation' Ostwestfalen-Lippe University of Applied Sciences, Institute Industrial IT and KBA - Giori SA, presented at 'The Conference on Optical Security and Counterfeit Deterrence', San Francisco, 20-22 January 2010
158. 'Public perceptions to Banknote Design' summary of presentation 'Innovative Approaches to the Selection of Banknote Features' by Hans de Heij at the Optical Document Security Conference, Currency News Volume 8, Number 2, Sunbury (UK), February 2010
159. Pryazhnikova, Lyudmila; 'We expect the new $100 note to enter circulation in late 2010' (interview with Michael Lambert), Banknotes of the World, Issue #2, InterCrim Press, Moscow, February 2010

160. Biederman, Irving, website http://geon.usc.edu/~biederman, purchased 6 April 2010
161. Hymans, Jacques E.C.; 'East is East, and West is West ? Currency iconography as nation-branding in the wider Europe' Elsevier, Political Geography 29, 2010, page 97 -108
162. Kosse, Anneke; 'The safety of cash and debit cards: a study on the perception and behaviour of Dutch consumers' Working Paper No. 245, De Nederlandsche Bank NV, Amsterdam, April 2010
163. 'Annual Report 2009' De Nederlandsche Bank NV, Amsterdam, April 2010
164. 'Banken, OM en politie binden samen strijd aan tegen skimming' Press release Nederlandse Vereniging van Banken, Amsterdam, 7 April 2010
165. Tolsma, Ellen; 'Op weg naar het perfecte bankbiljet' DNB Magazine, Number 2, De Nederlandsche Bank NV, Amsterdam, April 2010
166. De Heij, Hans; 'Counterfeit analysis: do we target the right user group?' De Nederlandsche Bank NV, power point presentation, presented at 'European Banknote Conference, Materials Committee, Lisbon, 17-20 May 2010
167. Cleland, Victoria; 'Banknotes meeting demand' Bank of England, Speech given at the European ATM Conference London, 11 June 2010
168. Hoffmann, Andreas; 'Deutsche Bundesbank cash study - Payment behaviour in Germany' Deutsche Bundesbank Payment Markets Theory, Evidence and Policy, Granada (Spain), 21-22 June 2010
169. 'Nationaal onderzoek winkelcriminaliteit 2010' Detailhandel Nederland, Leidschendam, June 2010
170. De Heij, Hans; 'Key elements in banknote design; part 1: the product perspective' Keesing Journal of Documents & Identity, issue 32, Amsterdam, June 2010
171. Esselink, Henk; 'The development of euro banknotes in circulation' European Central Bank, power point presentation, presented at 3rd ECB Central Bank Seminar on Banknotes, Frankfurt, 29 June - 2 July 2010
172. Gilles, Jean-Claude; 'Tracking banknote observation' European Central Bank, power point presentation, presented at 3rd ECB Central Bank Seminar on Banknotes, Frankfurt, 29 June-2 July 2010
173. De Heij, Hans; 'Public perception of banknotes - DNB Approach' De Nederlandsche Bank NV, power point presentation, presented at 3rd ECB Central Bank Seminar on Banknotes, Frankfurt, 29 June - 2 July 2010
174. 'Biannual information on euro banknote counterfeiting' press release European Central Bank, Frankfurt, 19 July 2010
175. 'Innovative Approaches to the Selection of Banknote Security Features: counterfeit analysis'; Banknotes of the World, Issue #8, InterCrim Press, Moscow, August 2010 (a summary of De Heij, Hans A.M.; 'Innovative approaches to the selection of banknote security features' De Nederlandsche Bank NV, presented at 'The Conference on Optical Security and Counterfeit Deterrence', San Francisco, 20-22 January 2010)

176. De Heij, Hans; 'Banknote identity', De Nederlandsche Bank NV, power point presentation presented at the First International Banknote Designers Conference, Geneva, 5-8 September 2010
177. 'Innovative Approaches to the Selection of Banknote Security Features: public knowledge and note design'; Banknotes of the World, Issue #9, InterCrim Press, Moscow, September 2010 (a summary of De Heij, Hans A.M.; 'Innovative approaches to the selection of banknote security features' De Nederlandsche Bank NV, presented at 'The Conference on Optical Security and Counterfeit Deterrence', San Francisco, 20-22 January 2010)
178. website Swiss National Bank (SNB), costs, 27 September 2010
179. Google: 'cost of banknotes'; calculation based on Annual Report of Bank of England 2004/2005 and 2005/2006, 27 September 2010
180. website Wikipedia, subject 'Federal Reserve Note', 27 September 2010
181. De Heij, Hans; 'Key elements in banknote design; part 2: the process perspective' Keesing Journal of Documents & Identity, Issue 33, Amsterdam, October 2010

Several banknote images were taken from the website of Ron Wise (http://aes.iupui.edu/rwise/notedir).

Publications in this series as from January 2003

Vol.1/No.1 (2003) Requirements for successful currency regimes:
The Dutch and Thai experiences
Robert-Paul Berben, Jan Marc Berk, Ekniti Nitihanprapas, Kanit Sangsuphan, Pisit Puapan and Piyaporn Sodsriwiboon

Vol.1/No.2 (2003) The blurring of distinctions between financial sectors: fact or fiction?
Annemarie van der Zwet

Vol.1/No.3 (2003) Intermediation, integration and internationalisation: a survey on banking in Europe
Jaap Bikker and Sandra Wesseling

Vol.1/No.4 (2003) A Survey of Institutional Frameworks for Financial Stability
Sander Oosterloo and Jakob de Haan

Vol.2/No.1 (2004) Towards a framework for financial stability
Aerdt Houben, Jan Kakes and Garry Schinasi

Vol.2/No.2 (2004) Depositor and investor protection in the Netherlands: past, present and future
Gillian Garcia and Henriëtte Prast

Vol.3/No.1 (2005) Labour market participation of ageing workers
Micro-financial incentives and policy considerations
W. Allard Bruinshoofd and Sybille G. Grob

Vol.3/No.2 (2005) Payments are no free lunch
Hans Brits and Carlo Winder

Vol.4/No.1 (2006) EUROMON: the multi-country model of De Nederlandsche Bank
Maria Demertzis, Peter van Els, Sybille Grob and Marga Peeters

Vol.4/No.2 (2006) An international scorecard for measuring bank performance: The case of Dutch Banks
J.W.B. Bos, J. Draulans, D. van den Kommer and B.A. Verhoef

Vol.4/No.3 (2006) How fair are fair values? A comparison for cross-listed financial companies
Marian Berden and Franka Liedorp

Vol.4/No.4 (2006) Monetary policy strategies and credibility – theory and practice
Bryan Chapple

Vol.4/No.5 (2006) China in 2006: An economist's view
Philipp Maier

Vol.4/No.6 (2006) The sustainability of the Dutch pension system
Jan Kakes and Dirk Broeders

Vol.5/No.1 (2007) Microfinanciering, deposito's en toezicht: de wereld is groot, denk klein!
Ronald Bosman en Iskander Schrijvers

Vol.5/No.2 (2007) Public feedback for better banknote design 2
Hans de Heij

Vol.6/No.1 (2008) Towards a European payments market: survey results on cross-border payment behaviour of Dutch consumers
Nicole Jonker and Anneke Kosse

Vol.6/No.2 (2008) Confidence and trust: empirical investigations for the Netherlands and the financial sector
Robert Mosch and Henriëtte Prast

Vol.6/No.3 (2008) Islamic Finance and Supervision: an exploratory analysis
Bastiaan Verhoef, Somia Azahaf and Werner Bijkerk

Vol.6/No.4 (2008) The Supervision of Banks in Europe: The Case for a Tailor-made Set-up
Aerdt Houben, Iskander Schrijvers and Tim Willems

Vol.6/No.5 (2008) Dutch Natural Gas Revenues and Fiscal Policy: Theory versus Practice
Peter Wierts and Guido Schotten

Vol.7/No.1 (2009) How does cross-border collateral affect a country's central bank and prudential supervisor?
Jeanette Capel

Vol.7/No.2 (2009) Banknote design for the visually impaired
Hans de Heij

Vol.7/No.3 (2009) Distortionary effects of crisis measures and how to limit them
Jan Willem van den End, Silvie Verkaart and Arjen van Dijkhuizen

Vol.8/No.1 (2010) The performance of EU foreign trade: a sectoral analysis
Piet Buitelaar and Henk van Kerkhoff

Vol.8/No.2 (2010) Reinsurers as Financial Intermediaries in the Market for Catastrophic Risk
John Lewis

Vol.8/No.3 (2010) Macro-effecten van hogere kapitaal- en liquiditeitstandaarden voor banken
Robert-Paul Berben, Beata Bierut, Jan Willem van den End and Jan Kakes

Vol.8/No.4 (2010) Banknote design for retailers and public
Hans de Heij