Innovative approaches to the selection of banknote security features

Hans A.M. de Heij
De Nederlandsche Bank NV
Eurosystem
Amsterdam, The Netherlands

ABSTRACT

New public security feature may become successful when next to their reproducibility the following parameters are part of the selection procedure:
- time needed to verify the feature,
- the required human operation (feel, look and tilt),
- the location of the feature on the note,
- consistency within the series,
- costs.

Two stakeholders are discussed: public and retailers. What do they know? What do they want? A public person receives on average one or two banknotes a day. The probability to receive a counterfeit is low and the confidence in genuine banknotes high. The average knowledge is in the Netherlands around 2 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 5 seconds. As a consequence the counterfeiters are decreasing the quality of the public security features.
A retailer receives on average around 200 banknotes a day. The counterfeiter targets the retailer and creates counterfeits with UV features that look similar - or even better - than in a genuine euro banknote. Many Dutch retailers still rely on their UV lamp (almost 40%) and around 40% of the retailers are not using any checking devices.
A retailer does not want to receive high denominations like 100, 200 and 500 euro. A security check should be done in less than 2 seconds and should not lead to discussion with the client. Magnifying glasses or mirrors are not used at all. Central banks do not want the retailer to use a pen tests for starch content.

How to get attention of the public for the public security features? A design solution is achieved by a synthesis of several design parameters like a maximum of 3 active security features (and 3 sleeping). The features should be striking and easy to find, e.g. by a preset layout and added way finding features like the use of an icon. An eye-travel path should be designed and checked during the design process.
For the retailer the design team may achieve a synthesis by introducing new security features like e.g. taggants, which can be checked by an automatic device within 2 seconds. The device provides a signal (red or green light or a beep) and the retailer may tell the client ‘The detector does not accept this note, would you have another one for me?’

Other counterfeit models used by DNB are refreshed too, like ‘intrinsic versus extrinsic features’, ‘internal versus add-on features’ and the ‘black box model’.

Keywords

Banknote design, design methodology, public and retail security features, counterfeiting.

---

1 Email: Hans.de.Heij@dnb.nl
1. INTRODUCTION

This paper will focus on the selection of public security features for banknotes. Next to the reproducibility of a new security feature other parameters should be studied too to make a new security feature successful, like e.g. the time needed to verify the feature, the required human operation (feel, look and tilt), the location of the feature on the note and the consistency within the series.

Another purpose of this paper is to give a historical overview of the policy of De Nederlandsche Bank (DNB) regarding the introduction of new security features.

DNB’s tasks regarding counterfeit deterrence are:
- producing banknotes with adequate security features,
- keeping the retail sector and public at large properly informed,
- supporting repressive measures on the part of judicial, judiciary and police authorities against counterfeiters.

DNB prefers to present these three aspects as a triangle (see Figure 1 [99]). The focus in this paper will be on secure banknotes; law enforcement, communications and awareness are only marginally touched.

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 that counterfeiters are traced by law enforcement.

Self defending banknote versus law enforcement
A central bank may have a bias to either more secure banknotes or to law enforcement. This bias is driven by national culture. In Europe central banks relied more on ‘self defending banknotes’, while for example the Treasury of the US by tradition has an intensive cooperation with the Secret Service and also with others like e.g. Interpol (Figure 2). This bias may also explain why the euro banknotes have two additional production steps compared to the US dollar, foil and silk screen, which makes the euro notes more costly than the dollar.

Legislation and informing the public
President Lincoln explicitly gave the Secret Service also the task of counterfeit combat. First legislation on counterfeiting banknotes was done in 1697, when the British Parliament proclaimed forgery of a banknote to be a felony and punishable with death. Later, in 1800, the introduction of banknote paper with a waved line watermark, instead of straight lines, was supported by an Act of the Parliament prohibiting the manufacturing of paper with a waved line watermark [27].
Banknote strategy bias

<table>
<thead>
<tr>
<th></th>
<th>Self defending</th>
<th>Law enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banknote production cost</td>
<td>89 %</td>
<td>75 %</td>
</tr>
<tr>
<td>Communication cost</td>
<td>&lt; 1 %</td>
<td>&lt; 0.5 %</td>
</tr>
<tr>
<td>Law enforcement cost</td>
<td>10 %</td>
<td>25 %</td>
</tr>
</tbody>
</table>

Figure 2.
Two basic strategies to protect banknotes against counterfeiting. Central banks following the strategy of ‘self defending banknotes’ spend relatively more money on the security of the banknotes. Central banks opting for the strategy of ‘law enforcement’ will spend relatively more money on law enforcement. Imaginative figures.

Communication
The Swiss National Bank was the first to issue a public leaflet (1976). Before then this was considered unwanted, since informing the public is like telling the counterfeiter, so was the general opinion of central banks. 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.

Easy to explain, hard to counterfeit
Security features should be easy to authenticate and difficult to counterfeit. This is easier said than done! Indeed: ‘If you can make it, they can fake it!’; the motto of Mr. Martin Mund of the European Central Bank (ECB). In a Monthly Bulletin phrased as: ‘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.’ [62]. For the US dollar a similar policy is drawn: ‘future US dollar features should be complex yet easy to explain to the users of currency’ [77].

1.1 Public preferences
How to garner public interest in banknotes? Key here is the development process involved by such features and their introduction in new banknotes. The Bank of Canada proposed highly intuitive security features, which can be used effectively for counterfeit detection even if an individual has no prior training in how to deal with it [72]. Intuitiveness will be hard to define and jumping to conclusions is a pitfall. Still, it is becoming increasingly clear that public perception of a banknote is the key to better banknote design.
The time needed to evaluate the feature in order to establish its authenticity is a critical parameter for the Bank of Canada. This seems to be very true. The public is willing to spend about 5 seconds on a security check as will be discussed in Chapter 4 of this paper.
Features for new banknotes should not only be selected on the basis of perception, but obviously also on the basis of other studies, like
- communication strategy (e.g. motto like feel, look, tilt, retrieval path),
- capitalizing on public awareness of legacy features (e.g. no more than two new public features and improving the features that are kept),
- costs (e.g. maximum cost increase 3 %),
- resistance to counterfeiting.

In 2009, DNB conducted a survey of the Dutch public’s security feature preferences. It turned out that the location of security features on euro banknotes has the highest relative importance, followed by the number of security features. The appearance of the security features is considered less important. Security features that are verifiable at one glance will give the strongest boost to a new euro 50 banknote design (see Paragraph 8.5.2)

1.2 Shorter life cycle for banknotes?

The trend towards shorter life cycles for both banknote design and security features is a constant. The question is: are we heading for life cycles of 5, 10, 15 or 20 years?

Long life cycles for DEM and USD notes
The German Mark banknotes (DEM) first issued in 1948 circulated until the mid-1990s: a life cycle of around 35 years. At 68 years, the life cycle of 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; the application of micro-printing and security threads in the early 90s).

Shorter life cycles
DNB’s policy in the 1980s was to issue a new banknote design after every two years. This means that, with 6 denominations, a Netherlands guilder (NLG) banknote series life cycle would be around 12 years. This policy would ensure a constant work load for the central bank, designers and printing works. However, as new versions of the most counterfeited denominations, e.g. the NLG 100 note, were issued more frequently than others, like the NLG 10 note. In practice the public usually carried banknotes from different series in their wallets. For by the time a series was complete, the arrival of the first new banknote broke up the ‘series perception’.

Today even shorter life cycles are foreseen by the US Treasury. The Bureau of Engraving and Printing (BEP) writes on its website: ‘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.’ Proof for this statement is the replacement within 8 years of the USD 20 model 1996 by the 2004 model of this same denomination.
In 2003, the ECB also assumed that a new banknote’s life cycle would be around 7 years and that a further decline in lifespan was likely [32, 33]. However, the lead time to realise the second series of euro banknotes (ES2) already exceeds this 7 years. The ES2-project started in 2003 and is expected to ‘be issued in a few years time’ (2008, Annual Report ECB). Indeed, the develop time to come to a new banknote design is a lower limit to the life cycle.

Lifespan of security features
Although a security feature’s lifespan is not identical to a banknote model’s life cycle, they are evidently related. The reason behind new banknote designs is usually the introduction of new security features. However, there seems to be a contradiction. The lifespan of many security features is much longer than that of a banknote design. The first watermarks, for example, were
made in 1282 in Bologna in Italy, long before the first western banknotes appeared, which amounts to a lifespan of well over 700 years. Although back then watermarks largely consisted of lines, watermarks are still used in banknotes (Figure 3). And if we consider that copper plate engraving was first used for British pound banknotes in 1694, we are looking at a tradition spanning over 300 years! [24]. The origin of micro-printing is not exactly known, but Dutch guilder notes issued in 1860 are the first available example of the 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!

Figure 3.
(a) sketch of the first watermark made in Bologna in Italy in 1282. The first NLG notes in 1814 included such a line watermark.
(b) mould-made watermark ‘Little Owl’ by Jaap Drupsteen for DNB and produced by VHP. Fist watermark with integrated highlights applied in NLG 100/Little Owl, issued in 1993. Since 1924, NLG notes featured mould-made watermarks.
(c) mould-made watermark ‘Renaissance’ by Inge Madlé for DNB and produced by Arjo Wiggins (VHP) in 2003. The background is an innovation, a so-called ‘digitised area’.

Legal lifespan of security features is 20 years
If patented, a security feature has a legal lifespan of 20 years, the period during which the patent owner has the exclusive rights to the feature’s use. This is a reason 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. Recently, the patent on the optically variable ink (OVI) expired, giving anyone access to the production of such inks or the right to order such inks, like for example ‘metameric optically variable pairs’ presented in September 2009.
The patent on a transparent window in banknotes (Wertpapier mit Fenster) will expire in 2015, probably leading to new competitive initiatives to introduce a transparent area in a (cotton) banknote as basis for a public security feature.

Features for detectors
The same pattern is observed for machine-readable features, as presented at the ‘Banknote 2005’ conference by De Heij. The use of UV-features that, to be discerned must be evaluated using ultra-violet light, has spanned over 40 years. And features requiring the light from the infra-red section of the spectrum (IR-features) have been in use for around 30 years. The lifespan of the magnetic and spectral properties are approaching 20 years [40].

Hard to abandon features
A variable that is crucial when we break down the lifespan of security features, is their number. New banknotes contain far more features than did the first banknotes, i.e. 37 now against 3 or 4 in the 18th century [48]. It appears to be difficult to discontinue the use of features, which in turn is
problematic given that banknote dimensions have reduced over time, in some cases over 50%!
[100]. Foil and silk screen were new features introduced in the 80s to deter colour copying and were added to the existing ones like watermark, thread and gravure print. Today central banks maximise the number of security features in their banknotes to around 20, divided over several user groups [25, 48, 55], including around 6 security features for the public and 2 or 3 features for the retailer. Contrary to the past, central banks can pick from a wide variety of security features. The question is: how to make this choice?

1.3 Reactive response policy

Until the 1970s, 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 1853, when, 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). The NLG notes using this improved technique were issued in 1860 [20]. Several times over the history of Dutch banknotes such reactive decisions were made, one of the last being made in the 1970s, when the NLG 100/Michiel de Ruyter was found to be frequently counterfeited.

The (implicit) counterfeit deterrence model used by many central banks is the outcome of a design strategy based on the counterfeits received. When these counterfeits exceed a given threshold, 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 4). 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.

**Figure 4.**
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.

*Counterfeiter focus is on mid denominations*

In the past counterfeiters focussed on the highest banknote denominations. The NLG 1,000 (value 454 euro) was one of the most targeted denominations in the 1970s, although this denomination was hardly used in daily cash payments [8]. 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 and also 100).
**High denominations not used for daily payments**

Retailers do not want to take the risk of a counterfeited 200 or 500 euro notes and inform their customers by stickers (Figure 5a). At first only the 200 and 500 euro were not accepted, the euro 100 joined later (Figure 5b). If high denominations are not accepted in the shops than counterfeiters will not produce such denominations. Professor Philip Hans Franses: ‘Nine out of ten shops 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.’ [58]. Recently, however, the Dutch public’s demand for 100 euro notes has started to rise, though, and more and more ATMs in the Netherlands now contain 100 euro banknotes (Figure 5c).

![Figure 5. Communication examples on the use of high banknote denominations in the Netherlands.](a) Sorry, no change (gasoline station, 2007). (b) These banknotes are not accepted (liquor store, 2009). (c) This ATM issues also EUR 100 notes (ABN AMRO branch, 2009).

**Euro counterfeits threshold**

As far as is known, no studies are available of what would be an acceptable counterfeiting level in a cash payment system. The first system to observe a distinct threshold, an *alarm level indicator*, was the Eurosystem.

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 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. The euro zone passed the threshold in 2008. The annual report of the ECB over this year reports a total of 666,000 counterfeited euro banknotes on a circulation of 13 billion notes.

The Eurosystem has left this threshold policy in 2009, since media attention on counterfeits is depending on several aspects like perception on the counterfeits by the public.

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 counterfeits per million notes in circulation (or c/mln). Looking at the alarm level from this point of view, the threshold in 2008 was about 50 c/mln.
1.4 Proactive counterfeit models developed by DNB

Since the mid-1970s, DNB abandoned its reactive approach and developed the following three proactive counterfeit models:
- intrinsic and extrinsic security features (1976),
- black box model (1991),

These models are discussed in paragraphs 8.1, 8.2 and 8.3, respectively.

Being the only party in the banknote-chain receiving all counterfeits accepted in circulation, central banks (or in some countries the police or justice), should analyse these notes closely. Shortly after the introduction of the euro, DNB developed the so-called ‘simple model’ to analyse incoming counterfeits. The simple model focuses on the received counterfeits and classifies the reproduction of the security features in simple qualities as ‘not imitated’ (= 0 points), ‘poor imitation’ (= 1 point) or ‘good imitation’ (= 2 points). This simple counterfeit analysis model has now been in use for over 3 years.

1.5 Need for development of counterfeit models

Before issuing a new banknote, it is common practice for central banks to produce several counterfeit studies in so-called ‘reproduction research centres’ (RRC).

Counterfeit studies on isolated parts
With the help of such a RRC central banks may create their ‘self made counterfeits’ before the new banknote will be issued. Such self made counterfeits could be disclosed to retailers or to the general public. As far as known, this is has never been done.
A new feature is often studied and evaluated as an isolated part of a banknote. 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 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’. See also paragraph 8.4 Preparation of counterfeits for the Board.

Counterfeiters have a test market; central banks do not
An important - and often neglected - difference between a central bank and a counterfeiter lies in the possibility of improving a banknote while the denomination in question is in circulation. Where central banks cannot change a banknote once it is put in circulation, a counterfeiter may continuously produce and try out their products. Next to introducing technical improvements, counterfeitors can optimise their counterfeits by taking on board the response of retailers and the public at large. They anticipate on public behaviour by decreasing the quality of the public features (see paragraph 8.3) and increasing the UV quality needed to pass the notes to the retailer (see paragraph 8.5.1). Like counterfeiters, central banks could receive feedback on their new banknote design before bringing the note into circulation. Such feedback could be received by offering a testing programme to retailers and public, using self made counterfeit 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 higher than used to be the case with the old note. This
happened in Canada after the issuance of the new CAD 10 in 1999. A similar reaction by counterfeiters was recorded in the United Kingdom. Shortly after the introduction of the new GBP 20 in 2007, counterfeit figures surged to an all-time high in 2008. In the Netherlands, too, counterfeit figures increased shortly after the issuance of the NLG 25/Robin in 1989.
2. COUNTERFEIT REPORTING STYLES

Banknote counterfeiters reproduce banknotes with the intention to use them for real. They come in several categories. To this end, the US National Research Council [62] and the Bank of Canada [64] work with the following categories of banknote counterfeiters:

1) primitive or unprofessional (fantasy notes and existing notes made with off-the-shelf equipment at home or push-the-button devices like a colour copier),
2) casual counterfeiter, hobbyist, opportunist or petty criminal counterfeiter (digital publishing tools like a Personal Computer (PC), scanner, printer, editing software (i.e. Photoshop) and other desk top publishing equipment),
3) professional (specialised equipment, acquisition of special materials, organised crime),
4) state sponsored or sophisticated high level counterfeiting (access to banknote production techniques).

The ECB uses a similar classification system (unprofessional, semi-professional, professional and sophisticated).

State sponsored counterfeiting happens only occasionally, usually to destabilize hostile economies, like the attempt of the British Government to destabilise the Continental government by counterfeiting US currency during the Revolutionary War (1775 - 1783). In 1942 the Germans tried to do the same to the British. Inmates had to counterfeit the 5, 10, 20 and 50 British pound banknotes, called ‘Operation Bernhard’. A recent example is the ‘Super Dollar’. These dollar notes are printed by a real banknote printing works outside the USA and pieces are found in the dollar circulation since 1989. The US Government suspects the involvement of the North Korean government [27, 62].

2.1 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). So these counterfeits were successfully used for a cash payment. Counterfeits seized by police before the criminals could use them for payments are not part of these figures and are in general much larger quantities.

Six counterfeit levels are recognised and some countries are classified according to these levels, including the euro area (see Table 1). No case is known were over 500 c/mln have circulated. Of course, world currencies like the US dollar and the euro are more attractive for counterfeiters than the currencies of small economies.

<table>
<thead>
<tr>
<th>Counterfeit level</th>
<th>Counterfeits detected per million notes in circulation [c/mln]</th>
<th>Country/currency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>0 – 10</td>
<td>Australia, Japan, Latvia, Norway, Romania, Sweden (Netherlands before euro)</td>
</tr>
<tr>
<td>2.</td>
<td>10 - 50</td>
<td>Hungary, United States (excluding 1 USD-notes)</td>
</tr>
<tr>
<td>3.</td>
<td>50 - 100</td>
<td>Euro (average in euro area)</td>
</tr>
<tr>
<td>4.</td>
<td>100 - 200</td>
<td>Canada, United States, Euro in NL</td>
</tr>
<tr>
<td>5.</td>
<td>200 - 500</td>
<td>Canada (in 2004), Great Britain (in 2008)</td>
</tr>
<tr>
<td>6.</td>
<td>&gt; 500</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 1.

Seven levels of counterfeits and some of the countries where these levels have been established. Number of counterfeits detected per million notes in circulation [c/mln].
Increase of euro counterfeits

Euro counterfeits increased from 49 in 2007 up to 55 c/mln in 2008 and will probably reach a level of around 70 c/mln in 2009, much more than the counterfeit level of US dollars, which is believed to be around 5 c/mln in 2005 (including the USD 1).

The USD 100 has a counterfeit rate of 30 c/mln [62]. The total value of counterfeited USD-notes is less than 0.01 % of the value of currency in circulation [62, 77].

The counterfeit level in the Netherlands (NL) seems to be substantially higher than the euro area average. As the Netherlands is like a euro area ‘province’, the number of euro banknotes in circulation is not exactly known but is estimated to be approx. 350 million. It follows that at around 50,000 counterfeits a year, the counterfeit level in the Netherlands may be calculated at 143 c/mln or 0.0143 % (= 50,000/350.10^6), far above the average for the whole euro area 55 (in 2008).

However, one should be cautious, for counterfeit figures are 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) [69, 91]. Australia claims a very low counterfeit rate of just 6 c/mln. This low figure is fully attributed to the high counterfeit deterrence capability of the polymer notes [56, 62].

Rolling average number of counterfeits

Over the years 2006 - 2008, banknote counterfeiting more than doubled in the Netherlands (from 20,745 notes in 2006 to 49,294 in 2008) [90]. To overcome the high volatility in counterfeit figures, DNB prefers a reporting style on counterfeit figures based on the 12-month rolling average number of detected fake banknotes [55]. Averaging over 12 months will yield a more objective view on the trend, which for the euro notes in the Netherlands is going up appreciably (see Figure 6).

Figure 6.
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 - 2009.

2.2 Press releases by central banks

Most central banks issue 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.

<table>
<thead>
<tr>
<th>Area/country</th>
<th>Euro area</th>
<th>United States</th>
<th>United Kingdom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td>2009</td>
<td>2009</td>
<td>2008**</td>
</tr>
<tr>
<td>Reference</td>
<td>[95]</td>
<td>[96]</td>
<td>[26]</td>
</tr>
<tr>
<td>1. Increase/decrease</td>
<td>+ 17 % *</td>
<td>+ 31.5 % *</td>
<td>+ 30 %</td>
</tr>
<tr>
<td>2. Distribution: where</td>
<td>Euro area</td>
<td>Euro area</td>
<td>NL</td>
</tr>
<tr>
<td>3. Circulating: where (mainly)</td>
<td>Euro area</td>
<td>NL</td>
<td>NL</td>
</tr>
<tr>
<td>4. Note counterfeited the most</td>
<td>EUR 20</td>
<td>EUR 50</td>
<td>NLG 100</td>
</tr>
<tr>
<td>5. Percentage of most counterfeited denomination on total of counterfeits</td>
<td>48.5 %</td>
<td>82 %</td>
<td>~ 90 %</td>
</tr>
<tr>
<td>6. Other counterfeited notes</td>
<td>EUR 50, 100</td>
<td>EUR 20</td>
<td>NLG 25, 50</td>
</tr>
<tr>
<td>7. Numbers passed - absolute</td>
<td>826,000*</td>
<td>64,056*</td>
<td>16,299</td>
</tr>
<tr>
<td>- c/m</td>
<td>~ 140 ***</td>
<td>~ 10</td>
<td>between 5 and 30</td>
</tr>
<tr>
<td>- per resident</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Numbers seized</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Face value</td>
<td></td>
<td></td>
<td>USD 103 million (0,01 % of circulation)</td>
</tr>
<tr>
<td>10. Name of producing country or town</td>
<td>Bulgaria</td>
<td>Bulgaria; Utrecht (NL)</td>
<td>Colombia</td>
</tr>
<tr>
<td>11. Produced by criminal group</td>
<td>criminal group</td>
<td></td>
<td>Mafia</td>
</tr>
<tr>
<td>12. Reproduction equipment</td>
<td></td>
<td></td>
<td>digital press (61 %)</td>
</tr>
<tr>
<td>13. Police actions/arresting</td>
<td>e.g. 17 arrests</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*) These figures are simply double the figure for the first half year of 2009.
**) Period October 2007 - August 2008
****) implicitly mentioned (reader has to divide the number of counterfeits by banknotes in circulation)

Table 2.
Typical subject-matter covered by press releases of 4 central banks.
Overview of counterfeit figures in eurozone and some other countries.
Such reports have a statistical format including some legal remarks. Table 2 provides an overview of a reporting style as observed by four central banks in this context. All too often these press-releases fail to inform on technical matters like differences between the fake and original notes.

**Increase in counterfeit detection by Dutch retailers since euro introduction**

A comparison of the number of counterfeit NLG notes with that of euro counterfeits in the Netherlands (see Table 2), should take the following into account. The figures for the Netherlands were only based on the counterfeits detected there and did not include NLG counterfeits detected in other countries. The figures on the euro counterfeits in the Netherlands also include - of course - euro counterfeits coming in from other euro and non-euro countries.

Table 2 shows that Dutch retailers were since the introduction of the euro confronted with about 4 times more counterfeits in 2009. However, the total loss incurred by Dutch retailers because of shoplifting is much higher than the total value of the counterfeits, i.e. around EUR 750 million and EUR 2 million, respectively.

**Probability of receiving a counterfeit in NL**

The odds of winning a lottery are usually much higher than receiving a counterfeit in circulation. In reaction to the first increase in euro counterfeits (2004), DNB calculated the probability of receiving a counterfeit in the Netherlands. Since the circulation of euro notes in the Netherlands is unknown, the total volume of passed counterfeits was expressed in absolute numbers. Nevertheless, the following calculation can be made:

Assuming a total circulation of 13 billion euro banknotes \((13 \times 10^9)\) in 2008 and a share of 5.71 % of this total for the Netherlands (capital key of 3.99 % rebased to 100), the Dutch account for 742.3 millions of euro notes in circulation. However, the real circulation in the Netherlands is, as said before, estimated to be lower, i.e. at approximately 350 million notes. With around 50,000 counterfeits in 2008, the probability of receiving a euro counterfeit in the Netherlands will be - assuming the issuance of counterfeits are a constant flow over the whole year - about 140 counterfeits on 1 million real euro notes. The real probability will be lower, since counterfeits are not equally put in circulation. Furthermore, the calculation is only valid for the person being the last to use the counterfeited note; it presupposes that only one payment is done with the counterfeited banknote. Only the last person using a counterfeit will bear the damage of a lost value.

The probability of receiving a US dollar counterfeit note is believed to be lower, around 5 on 1 million, including one-dollar bills [62].

**Perception of 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. Entrepreneurs estimated that - within a 5-year period - 0.5 to 10 % of the euro notes in the Netherlands would be counterfeits. Consumers were expecting even much higher levels: 30 -100 % [48]. 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 [34].

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 [93]. This public perception is remarkable, since it is far above the reality of around 50 c/mln passed or 0.005 % in 2008. Based on these figures the Dutch estimated over 200 % more counterfeits in circulation as there were in reality (in 2008).
Confidence in banknotes

In addition to the cognitive average knowledge of public security features, DNB considers the Dutch citizens’ confidence in euro banknotes a relevant psychological indicator and started in 2004 to measure the public’s trust in banknotes. Figure 7 provides the confidence figures for NL and Canada.

The public’s confidence that euro banknotes in circulation are authentic is not high: around 7 on a scale from 1 to 10 [48, 55, 85]. The Bank of England has also measured aspects of public confidence since 2004, but did not publish the results. In 2004 and 2007 the ECB made a so called ‘cash handlers survey’ [34, 61]. From these two surveys it can be concluded that in both years 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. It is most probably on the basis of these surveys that the ECB reported that ‘Studies show that, in general, the more a banknote is immediately liked, the more it inspires confidence’ [66].

Figure 7.
Public confidence score for the euro (in NL) and for the Canadian dollar.

Threat indicators

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 [20].

Instead of ‘probability of a counterfeit’ or ‘confidence’, central banks have recently 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.

Recently artificial models have been developed to explain these threats, like threat assessment (Bank of Canada, 2008), analytical flow model (USA, 2007) and multi criteria decision analysis (ECB, 2007). They will be discussed in Chapter 6.
3. PUBLIC KNOWLEDGE OF SECURITY FEATURES

Sometimes, central banks are weary of the public’s apathy, as is witnessed by the following three statements made by central bank employees:

- 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) [75],
- 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) [60],
- 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 (Mr. Paramo, member of the Executive Board of the ECB, on the occasion of the first Europol congress on counterfeiting) [54].

How to garner public interest in public security features? Studies on public appreciation, knowledge, emotion and perception are necessary to arrive at more communicative banknotes. This view is shared by Dr. Hans Reckers of the Bundesbank, who finds that: “The new Euro Series 2 (ES2) should receive user friendly public security features.” [78].

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

* = corrected compared to 2007

Table 3.

All measurements are done by TNS NIPO. The answers are given ‘repeated by heart’. The type of research is periodic.
Instead, security features are getting more and more complex to evaluate. The public already has major difficulties recalling a feature. The general public is unaware of security features, as is illustrated once more by DNB's 2009 study of public knowledge of security features (see Table 3).

The group that can not tell any security feature dropped from 19 % to 7 %. Spanish researched showed that almost 1 in 5 Spanish cannot name one security feature either [73].

**Public: some qualitative, but no quantitative knowledge**

The ECB also found that the public at large has little 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. Furthermore, just a 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 [61].

So, the public knows some qualitative aspects of banknote security features, but hardly any quantitative. The relative high confidence in the euro banknotes (Figure 6) is probably one of the reasons why the public does not check banknotes on counterfeits. An other explanation is given by Ruud Van Renesse: ‘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.’ [57].

**How does the public know what to check?**

Many people will 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 what kind of images our brain stores: 95 % of what we see is recollection of old images [67]. For banknotes, this means that people will probably just look for the watermark and foil, the two best-recalled public security features. This implicit long-term memory seems to be irrelevant for a full security check, since it does not tell us *how* the feature should be checked.

Another example of banknote recollection over a period of 7 years was researched in 2009 by TNS NIPO at the request of DNB (Table 4).

<table>
<thead>
<tr>
<th>Spontaneous awareness of pictures on NLG banknotes in 2009</th>
<th>Name mentioned</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Snipe</td>
<td></td>
<td>25 %</td>
</tr>
<tr>
<td>2. Lighthouse</td>
<td></td>
<td>15 %</td>
</tr>
<tr>
<td>3. Sunflower</td>
<td></td>
<td>9 %</td>
</tr>
<tr>
<td>4. Other bird</td>
<td></td>
<td>5 %</td>
</tr>
<tr>
<td>5. A head of a person</td>
<td></td>
<td>5 %</td>
</tr>
<tr>
<td>6. Named colour</td>
<td></td>
<td>4 %</td>
</tr>
<tr>
<td>7. Michiel de Ruyter</td>
<td></td>
<td>2 %</td>
</tr>
<tr>
<td>8. Frans Hals</td>
<td></td>
<td>2 %</td>
</tr>
<tr>
<td>7. Others</td>
<td></td>
<td>~ 10 %</td>
</tr>
<tr>
<td>8. Do not know</td>
<td></td>
<td>22 %</td>
</tr>
</tbody>
</table>

*Table 4.*

After 7 years the Dutch recall the image of a snipe best, followed by the lighthouse and sunflower.
The Dutch public was asked which images of former guilder banknotes they could remember. The ‘Snipe’, as the then circulating NLG 100 bill was popularly referred to, was mentioned by far the most, followed by the ‘Lighthouse’ and ‘Sunflower’. Only a few people recalled historical persons like Michiel de Ruyter (2 %) and Frans Hals (2 %). Men proved better able to recall pictures on guilder banknotes than 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 %) [86].

Banknote perception

Besides the overlooked new ‘haircut’, other examples were given in the second ‘public feedback’ paper [55]. There is a difference between removing an element (a birthmark or a moustache) and adding one (start wearing glasses). This might also apply to the perception of banknotes. Leaving out the watermark or a secure ink may go unnoticed, while something added like a stamp or writing on a banknote will definitely not be overlooked. This explains why counterfeiters can permit themselves to leave out some security features as we will see in paragraph 8.3 DNB Model 3: Simple method.

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, as we will see in paragraph 8.5.4 Communication of security features.

Does the counterfeiter make use of the public’s knowledge?

Why do counterfeiters focus on certain features and widely ignore others? 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 3 for optimising their bogus notes?

To answer this question we need statistics on how often security features are reproduced. Such statistics are only incidentally made. Table 5 provides on the one hand the public knowledge of security features and on the other hand an estimation of the presence of public security features in counterfeits.

<table>
<thead>
<tr>
<th>Public feature in euro</th>
<th>Public knowledge (NL, 2009)</th>
<th>Imitated in some form in euro counterfeit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Watermark</td>
<td>76 %</td>
<td>Frequently</td>
</tr>
<tr>
<td>2. Hologram/silver foil</td>
<td>55 %</td>
<td>Almost all</td>
</tr>
<tr>
<td>3. Security thread</td>
<td>15 %</td>
<td>Frequently</td>
</tr>
<tr>
<td>4. See-through register</td>
<td>9 %</td>
<td>Frequently</td>
</tr>
<tr>
<td>5. Tactility</td>
<td>8 %</td>
<td>Some</td>
</tr>
<tr>
<td>6. Colour changing ink (OVI)</td>
<td>3 %</td>
<td>Frequently</td>
</tr>
<tr>
<td>7. Glossy gold stripe</td>
<td>2 %</td>
<td>Frequently</td>
</tr>
</tbody>
</table>

Table 5.
Relation between public knowledge of public security features and the presence of such features in counterfeited euro banknotes (common class, frequency).
Vicious circle: public - counterfeiter - central bank
Judging by Table 5, there is a relation. It seems that counterfeitors are doing more than is necessary for public acceptance! This is in line with the observation that the quality of counterfeits seems to be declining (see Paragraph 8.3).
Counterfeits do not have to be very close to the original to be accepted by the public, is how counterfeitors seem to reason. Here the vicious circle becomes clear (Figure 8). The public pays no attention to the notes they receive, since the probability on receiving a counterfeit is low and the confidence in genuine euro banknotes is relative high. 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!
When the number of counterfeits is increasing, like is the case in the Netherlands, people know more public security features (2.5 in 2009 versus 1.9 in 2007) and also the group that can not recall a single security feature decreased from 20 % in 2007 to 7 % in 2009 (Table 3). If the public becomes more alert, the vicious circle may be broken.

![Figure 8.](image)
How to break the vicious circle? Make designs that get attention of the public!

Focus from public to retailer?
Central banks’ focus in this context should be shifted towards retailers, since they are the key persons in accepting counterfeits. While the average consumer makes cash payments once or twice a day [38], retailers receive on average 200 notes a day [48].
Most Dutch retailers (41 %) do not check a banknote for genuineness; at least not without the help of a device. Fortunately, the category that uses a device is growing (see Table 6) [79].

<table>
<thead>
<tr>
<th>Retail device</th>
<th>Used by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2007</td>
</tr>
<tr>
<td>1. UV lamp</td>
<td>35 %</td>
</tr>
<tr>
<td>2. Auto detection</td>
<td>16 %</td>
</tr>
<tr>
<td>3. IR viewer</td>
<td>4 %</td>
</tr>
<tr>
<td>4. Different</td>
<td>3 %</td>
</tr>
<tr>
<td>5. Magnifier or mirror</td>
<td>0 %</td>
</tr>
<tr>
<td>6. None</td>
<td>45 %</td>
</tr>
<tr>
<td>Total</td>
<td>100 %</td>
</tr>
</tbody>
</table>

Table 6.
Overview of the use of retail devices in the Netherlands (2007 and 2008) [55, 79].
These results qualitatively match the data for the Netherlands as reported in the 2007 ‘Cashier Survey’ of the ECB except for the pen tests for starch content (see Table 7) [61]. 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.

<table>
<thead>
<tr>
<th>Retail device</th>
<th>NL</th>
<th>Euro Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ultraviolet lamp</td>
<td>44%</td>
<td>26%</td>
</tr>
<tr>
<td>Euro ‘pens’ indicating whether the banknote paper is genuine</td>
<td>10%</td>
<td>9%</td>
</tr>
<tr>
<td>Infrared viewer</td>
<td>9%</td>
<td>7%</td>
</tr>
<tr>
<td>Authentication device/equipment</td>
<td>22%</td>
<td>3%</td>
</tr>
<tr>
<td>The till/equipment you use automatically checks all banknotes</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td>You don’t use any tools (spontaneous)</td>
<td>18%</td>
<td>55%</td>
</tr>
<tr>
<td>Other tool (spontaneous - specify)</td>
<td>4%</td>
<td>1%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>2%</td>
<td>1%</td>
</tr>
</tbody>
</table>

Table 7.
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 2007, ECB.

A similar 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 proffer to pay for a purchase; but on the other hand 41% are annoyed by it [73].

Automatic devices are preferred
There are two types of device for retailers:
1) The type of device letting the retailer decide whether the note is genuine or not, e.g. UV lamps, IR viewers, magnifiers and mirrors (for the colour-changing features when the note is tilted).
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).

The second option is preferred and advised by DNB. Research conducted by DNB in 2006 showed that UV light checks on banknotes are often not properly conducted. This explains why so many counterfeits with a limited UV imitation are not rejected. That is why DNB discourages the use UV lamps (see paragraph 8.5.1). Auto detection devices on the other hand provide the retailer with an easy argument to ask: ‘The detector does not accept this note, would you have another one for me?’

Develop features to assist retailers
It is known that retailers do not wish to spend more than 2 seconds on a security feature [48]. Central banks could be of assistance here to retailers, for example, by:
- ensuring that in the next generation of banknotes all retail features are on one side,
- developing tools, e.g. a barcode scanner, that also check a banknote for genuineness (Figure 9).
- developing a marker and/or taggant readers (see Paragraph 7.1).
Figure 9.
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, or any other. Metameric inks are explained in paragraph 8.2.
4. TIME REQUIRED TO CHECK 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.

_Flash second_

When the payer hands over the note, the acceptor only gets to see a glimpse of the banknote since the payer's fingers and thumb partly cover the note (Figure 10).

![Figure 10](image)

Banknotes are often used without being seriously checked. The flash second is important. Drawing by author (1984).

In this instant, the value must be verified. The receiver, usually a retailer, will need to assess if she or he is getting the right value, while the payer must determine whether she took the right denomination from her wallet. This explains also the research results of both the US Treasury and the ECB that the touch of the banknote is the most important trigger on counterfeits. In 2002 the US Treasury 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) [29]. The 2007 Cash handling survey of the ECB reported that the most common security feature checked is tactility for 70% of the cashiers [61].

**Maximum time spent on checking security features: 5 seconds**

The author’s paper entitled ‘Public feedback for better banknote design’ provides data regarding the time needed to check a security feature [48]. From DNB research, the total time to settle a cash payment transaction is known to be 19 seconds [36]. 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 8 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 [52].

Five seconds also seems to be the limit of what is socially acceptable to check a received banknote without being impolite.
CASH SETTLEMENT - break down

<table>
<thead>
<tr>
<th>Step</th>
<th>Estimated time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Payer becomes conscious of the amount to be paid</td>
<td>1 s</td>
</tr>
<tr>
<td>2. Payer searches cash and takes his/her wallet (or from pocket)</td>
<td>2 s</td>
</tr>
<tr>
<td>3. Payer selects right cash amount (banknote(s) and coin(s))</td>
<td>2 s</td>
</tr>
<tr>
<td>4. Payer hands over the cash to the receiver</td>
<td>1 s</td>
</tr>
<tr>
<td>5. Receiver checks the value of the received cash</td>
<td>1 s</td>
</tr>
<tr>
<td>6. Receiver may check the authenticity of the received cash</td>
<td>5 s</td>
</tr>
<tr>
<td>7. Receiver calculates the change (if any)</td>
<td>1 s</td>
</tr>
<tr>
<td>8. Receiver searches for change</td>
<td>2 s</td>
</tr>
<tr>
<td>9. Receiver hands over change to payer</td>
<td>1 s</td>
</tr>
<tr>
<td>10. Payer checks on the amount of change</td>
<td>1 s</td>
</tr>
<tr>
<td>11. Payer may check the change for authenticity</td>
<td>0 s</td>
</tr>
<tr>
<td>12. Payer stores the change in his/her wallet or pocket</td>
<td>2 s</td>
</tr>
<tr>
<td><strong>Total settlement time</strong></td>
<td><strong>19 seconds</strong></td>
</tr>
</tbody>
</table>

Table 8.
Breakdown in time of a cash settlement between a payer (public) and a receiver (retailer). Estimation by author, based on the reported total time to settle a cash transaction.

*How much time is needed to check a banknote?*

On the website of the ECB the following statement is made: ‘It only takes a few seconds to check a banknote.’ The question is if this can be verified. First answer would be that the estimated 5 seconds are not enough to check all public features in a euro 50 banknote. To check all 6 public features would take an estimated time of 16 seconds, as reported in Table 9. Usually central banks advise the public to check 3 security features, which altogether would take about 5 seconds (3 x max 2 seconds = max 6 seconds).

<table>
<thead>
<tr>
<th>Euro 50 – Public security features</th>
<th>Estimated time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Tactile relief</td>
<td>2 s</td>
</tr>
<tr>
<td>1.2 Nail scratch</td>
<td>2 s</td>
</tr>
<tr>
<td>2. Watermark</td>
<td>2 s</td>
</tr>
<tr>
<td>3. Security thread</td>
<td>1 s</td>
</tr>
<tr>
<td>4. See-through</td>
<td>2 s</td>
</tr>
<tr>
<td>5. Colour changing ink (OVI)</td>
<td>3 s</td>
</tr>
<tr>
<td>6. Hologram.</td>
<td>4 s</td>
</tr>
<tr>
<td><strong>Total to check all public features</strong></td>
<td><strong>16 seconds</strong></td>
</tr>
</tbody>
</table>

Table 9.
Estimated time to check the public security features in a EUR 50 banknote.

*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 (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. 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 %) [61].

*No nested features*

There is a clear trend that central banks expect the public to pay more attention, in casu more time, to security features. The reason is the trend of so called ‘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 11). 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.

![Droste-effect](image1)

![Original public feature](image2)

![Original feature with 3 nested features. One nested feature has two more 'nest levels'.](image3)

*Figure 11.*

Principle of nested features. On the left: ‘Droste effect’. In the middle the original basic feature. On the right the basic feature with 3 nested features in it. One nested feature contains two more levels of nested features.

![A switch from dark to light within the renaissance window is seen when the hologram on the euro 50 banknote is tilted.](image4)

*Figure 12.*

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

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 (see Figure 12). Also the numeral ‘50’ may be seen (feature 2.3).

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). Micro-lettering on a security thread is also seen as a nested feature, just as a feature which becomes discernable when held under UV-light with a long (around 365 nm) or a short (around 254 nm) wavelength.

**Change blindness**
The switch from dark to light within the Renaissance window of the hologram on the euro 50 (Figure 12) reminds of a change blindness test done with 20 US dollar banknotes. The two images of Figure 13 are used in an animation movie showing each 1.5 second a switch from one image to the other. Most people do not notice that the background behind the portrait changes from dark to light. Tilting the euro 50 hologram will also be hindered by change blindness. So called ‘achromatic holograms’ switch from light to dark and will experience similar perception problems.

Figure 14 is also a variant on change blindness. Mirroring the portrait of the well known one dollar banknote is not noticed by most people [80].

![Figure 13.](image)
Change blindness illustrated by US dollar 20 banknote. When the above images are shown on a screen most people will not notice the 2 second switch in the background to Jackson from dark to light.

![Figure 14.](image)
Which is the correct USD banknote? [80].

**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 may be demanding too much from 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 [27].

In fact, central banks should see the banknote as a whole, as one feature (the banknote) with six nested public features in it, all on nest level 1. 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 15 and the DNB-patent ‘Authenticity Mark’ [46]. As reading eyes typically focus on sizes of about 30 mm x 15 mm, these dimensions might serve as guidelines for the dimensions of public security features [67].

Figure 15.
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, like e.g. overprinting with offset.

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 like the colour changing element (OVI) and the watermark. Such ‘island features’ should be avoided since they make life easier for the counterfeiter.

Multi-level security features
One should be careful with features serving several user groups. A security thread for the public that may also be used as a detector feature in the central bank’s sorting machines is an example of a ‘multi-level feature’. Such feature might lead to sub optimization for one or more of the relevant user groups. Ideally each feature should serve just one user group.

User requirements
Time seems to be the most important user requirement for a public security feature, but there are more, as listed in ‘Public feedback for better banknote design’ papers [48, 55]. Table 10 provides an overview of these user requirements, including the new introduced ‘no nested features’ requirement. As an example the table is filed in for the euro 50 note.

Scoring of public features in the EUR 50 note is simply done by a Yes or No.
The features best fulfilling the user requirements are:
- nail scratch feature (or ‘ISARD’), 7 out of 7
- security thread, 5 out of 7
- see-through register, 5 out of 7

The features that do not match the user requirements are:
- hologram, 1 out of 7
- OVI, 2 out of 7.
Table 10.
Scoring the public security features in the EUR 50 note against the user requirements.
Y = Yes, meeting the requirement. N = No, not meeting the requirement.

Transparent window takes at least 9 seconds
In 2005 the Varifeye feature was presented, a clear window in a cotton paper. To check this feature would take around 2 seconds:
- view against white background - in transmission 1 s
- view against dark background - in transmission 1 s
  --- + 2 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) [84]. 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.

OVI and SPARK
More and more central banks are growing convinced that Optically Variable Ink (OVI) is not a strong feature. After DNB and Romania, similar findings are reported by Banco de España. Just as in the Netherlands, the optically variable ink mark is the least familiar public security feature, known by 11 % of the Spanish (and 3 % of the Dutch). The OVI on the dollar notes is also not popular in the United States. The NRC in their NextGen book writes that ‘color-shifting inks are rarely used by the general public’[62]. Dr. Hans Reckers (Bundesbank) is one of the criticasters
of OVI because of its ‘astonishingly’ easy reproducibility [78]. Vladimir Finogenov of the Russian Central Bank agrees: ‘OVI are reproduced with rather high quality’ [76].

With Spark, the next generation of OVI features, a third, motion-based, ‘nest level’ was introduced, in addition to the gloss and a colour (Figure 16). The order of checking the Spark feature will be:
- motion,
- colour switch,
- gloss.

![Figure 16. The first banknote to feature the Spark is the Chinese 10 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.](image)

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. If it sees motion in a counterfeited Spark-feature, the public might take it for real. Since the OVI patent has expired, another drawback is the free production by any company of two elements of the Spark: the gloss and colour switch.

And there are other hurdles for a Spark feature to be successful. The limited range of colours that are suitable for the purpose is another weak aspect, also from counterfeiter’s point of view. Once the good colour flop imitation is found, it may be used for many banknotes, both within the series and internationally.

![Figure 17. Colour concept for a banknotes series. Easy to communicate: all colours turn to gold.](image)
From the customers’ point of view central banks will opt for a colour-scheme as provided in Figure 17, where seven different colours all change to the same hue of gold. Such a proposal is in line with the advice given 2007 to develop security features much more on colour concepts, like e.g. partly coloured foil stripes [55]. 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 features [48]. Finally, the Spark feature is expensive, making up 15 to 20 % of a banknote’s production costs.
5. SUPPLIERS TOO FAR REMOVED FROM CUSTOMERS

Usually the printer is the contractor for a new banknote. The printer’s customer is the central bank, not the public or the retailer. Semi-finished product suppliers are even further removed from the final users of the banknotes (see Figure 18). This situation may be explained by the controversy between technology push (the suppliers) and technology pull (the central banks).

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.’ [82].

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.’[83].

The new 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 i.e. it the consumer (in the end of the day the user of banknotes).’ [92].

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 [65].

What should be developed?
Since there is only one feel feature available (ink relief) central banks are especially in need for more feel features. Tilt features - and especially colour switching features - are less popular than feel and look features as is concluded in the first paper on ‘Public feedback for better banknote
design’ [48]. Also user requirements for public features are defined in this paper, like a checking
time less than 3 seconds. Further more new retail features are needed as follow up for the
magnifying glass and the UV lamp.

**Printer is contractor**
It seems that the central banks should develop themselves much more as knowledgeable on the
subject banknotes and should increase their development work, starting first of all to understand
their customers better, especially the retailers and the general public (Figure 19).

---

**Figure 19.**
Schematic view of the estimated input in banknote development by 5 disciplines (estimation is subjective,
made by author). Suppliers dominate banknote development process.

**Example**
Often developers of security features expect that public and retailers will recognise small design
deviations in a counterfeit. Having a good idea of what a document should look like is essential to
detecting irregularities so is the idea of many suppliers. This may be questioned. Even if a large
element like the main image on the euro notes is altered, as in Figure 20, this is not noticed by
more than 80 % of the people [86, 87 90, 100].

---

**Figure 20.**
Change blindness for euro banknotes. Which are the correct notes?
6. MODELS USED TO ANALYSE COUNTERFEIT BANKNOTES

Wouldn’t it be fantastic if we could say: ‘The counterfeit resistance of a foil is 134 % of a watermark?’ Unfortunately it is not that simple to compare security features with each other. Recently, three reports were published on models for analysing public security features and their counterfeiting resistance. The first was the report by the National Research Council in 2007 [62], followed by a report by the Bank of Canada in 2008 [64]. The third method is developed by the ECB and deals with a method to rank ‘human sense’ security features on the basis of their counterfeit resistance. The target of these three models is not exactly the same, as is illustrated in Table 11.

6.1 National Research Council

In 2007, the report ‘A Path to the Next Generation of U.S. Banknotes’ was published. Commissioned by the Bureau of Engraving and Printing from the National Research Council (NRC), this study provides an extensive analysis of who is counterfeiting what. Around 80% of the lower US dollar denominations are mostly counterfeited by opportunistic (or casual counterfeiter) and petty criminals, while the USD 100 is mostly reproduced by professional criminals and even state-sponsored criminals (around 85%). Most counterfeits are ink-jet printed (mostly lower denominations) and offset (USD 100) [62].

The NRC chose for an ‘analytical flow model’ after their conclusion that all features were assigned about the same scores (mean score 1.9 +/- 0.1, maximum 2.1, minimum 1.7). Counterfeits should be removed from circulation when passing sophisticated authentication detectors [63]. A feature that prevents reproduction is less effective than a feature that prevents passing, their conclusion reads. The future they see is a world using many more devices to check banknotes.

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 blue-shift in the colours [62].

6.2 Bank of Canada

All R&D projects for new security features are conducted through a ‘stage/gate’ process and reviewed by a panel of experts. The development phases of a security feature are:
- design,
- proof of design,
- prototype,
- pilot scale-up,
- production scale-up.

Since the inception of the programme, more than 300 prospective designs have been reviewed (not only security features). To date, just one project pertaining to security features has reached the pilot scale-up phase. The intention is to maintain projects running on a continual basis at various stages of maturity.

Several projects have been designed to predict the effectiveness of banknote security features. For this purpose, information about how well users can authenticate notes or features has been collected from direct observations using human perception experiments [82].

The criteria for passing on to the next phase of the stage/gate process are partly based on a ‘Technology Scan and Threat Analysis’. The focus is on the different users of banknotes like...
‘human’, ‘automatic’ and ‘forensic’. ‘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) [64].

### MODELS USED TO ANALYSE COUNTERFEIT BANKNOTES

<table>
<thead>
<tr>
<th>Institute</th>
<th>National Research Council USA</th>
<th>Bank of Canada</th>
<th>European Central Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currency symbol</td>
<td>USD</td>
<td>CAD</td>
<td>EUR</td>
</tr>
<tr>
<td>Year</td>
<td>2007</td>
<td>2008</td>
<td>2007</td>
</tr>
<tr>
<td>Methodology</td>
<td>Analytical flow model</td>
<td>Stage/Gate process (Technology Scan and Threat Analysis)</td>
<td>Ranking counterfeit resilience</td>
</tr>
<tr>
<td>Target</td>
<td>Forecasting which technologies are favourable for new security features</td>
<td>Selection of designs of security features for development by the central bank</td>
<td>Ranking of old and new public human sense security features</td>
</tr>
<tr>
<td>Criteria</td>
<td>5 criteria per counterfeit class (excellent, good, easy, somewhat, blank)</td>
<td>3 ‘in’ criteria and 7 ‘out’ criteria</td>
<td>14 criteria (subdivided in totally 57 descriptors) and 4 indicators.</td>
</tr>
<tr>
<td>Arithmetic operations</td>
<td>Not found useful</td>
<td>Dynamic Selection Process (ranking table)</td>
<td>Multi-criteria decision analysis</td>
</tr>
<tr>
<td>Judgement</td>
<td>By Committee (NRC)</td>
<td>Central bank experts</td>
<td>Central bank experts</td>
</tr>
<tr>
<td>Public testing /input</td>
<td>No</td>
<td>Yes, some human perception experiments</td>
<td>No</td>
</tr>
<tr>
<td>Measurements</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Complete note or single features</td>
<td>Single features</td>
<td>Single features</td>
<td>Single features</td>
</tr>
<tr>
<td>Time needed by counterfeiter</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Costs made by counterfeiter</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Final output</td>
<td>Development programme; technological directions where to search for new features</td>
<td>Stage-gate process, &gt; 300 at start; still 8 projects running for new features</td>
<td>Resilience Grade 1 - 6 (best - worst feature)</td>
</tr>
</tbody>
</table>

Table 11. Overview of three models.

### 6.3 European Central Bank

At the Euro-conference in 2007 the ECB presented the ‘counterfeit resilience assessment of security features’, a method which allows for a classification of public security features reflecting their counterfeit resilience.
The ranking of counterfeit resilience by the ECB is based on 8 criteria:

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

A distinction is made between a feature reproduction made by emulation and one made by simulation. When an original security feature may be reproduced close to the original by commercially available techniques this is called emulation. If a reproduction is made with materials that are basically not suitable for recreating the original, this is called simulation.

The simulated counterfeit attacks are ranked ‘good’, ‘mediocre’ or ‘poor’. The method provides for several steps to arrive at ‘Robustness Grades’ (RG), ranging from RG 1 to RG 6; RG1 for the highest resilience and RG6 for the lowest.

It seems that the ECB experiences the same difficulty as the NRC. Finally, the difference between the features scored is quite small; from the 6 RG-levels just 3 are used.

6.4 Some observations

On the basis of a study of and comparison of the three models, 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;
- 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 on their experts’ view instead of also the public’s comments (except the Bank of Canada);
- fail to conduct measurements on the genuine feature versus counterfeited variants.
7. COUNTERFEIT DETERRENT SYSTEMS (CDS)

Counterfeit Deterrent Systems (CDS) are generally aimed at preventing counterfeiting by the use of standardized off-the-shelf reproduction techniques. In 1990 the Bank for International Settlements (BIS) took the initiative to develop such systems.

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 feature is directed against the casual counterfeiter trying to manufacture counterfeits at home and introduced in the euro banknotes in 2002. Both CDS-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. Thus, in October 2007 [60], 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.’

Counterfeit deterrence systems are an element of law enforcement rather than part of a self-defending banknote strategy (see Figure 2). With the introduction of the euro in 2002 the central banks in Europe, including the ECB, gained interest in counterfeit deterrence systems but kept spending money also on more secure banknotes by applying e.g. holographic foil and OVI in silk screen. Evidently, CDS has had a considerable impact, since home counterfeiting has come down: toner copies have fared badly thanks to CDS. In 2006 only 3.3 % of total quantities recovered by the Eurosystem were toner copies.

Too much space and pale banknotes
CDS features are in need of space. DNB calculated in 2005 that over 50 % of the euro 50 note surface is occupied by [65] which has a clear negative effect on the overall perception of the banknote. The space attributed to CDS limits the surface for public security features, being 15 % of the surface of the euro 50 note. Its large space requirements give the banknote a rather blurred and pale impression. Now the public is known to disapprove of pale banknotes [48, 55]. Indeed, they may accept a more colourful counterfeit note for the real thing!

If the graphic 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 21.
Figure 21.
Conceptual banknote 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. Background could be used for other security features. Design by author (2009) [55].
8. COUNTERFEIT MODELS DEVELOPED BY DNB

In 1814 DNB commissioned its first banknotes from Messrs. Johannes Enschedé in Haarlem because they owned many unique letter types for letterpress printing cut by Fleischman. Letter types were very difficult to reproduce for it required other type cutters to reproduce the types by hand.

Around 1850, the new technology of photography triggered illegal banknote reproduction, also in the Netherlands. In 1860, a new series of NLG banknotes including improved gravure print provided the answer. Counterfeits kept coming, however, and 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. 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 1000 issued in 1929!

Portraits on banknotes
In the 1920s DNB held the statement that banknotes should have a historical portrait on the note, 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.’ The portrait of William of Orange appeared on the new NLG 25 issued in 1921 [20]. The reasoning behind this choice may be questioned, but it can be seen as the first step towards a proactive anti-counterfeit strategy. For a long period 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 is different from the counterfeit. People are expert in recognizing other people, especially by the eyes, so was the philosophy. With the issuance of the NLG 100/Snipe, a banknote depicting a bird, DNB was in 1981 the first to leave portraits on banknotes behind. At international meetings DNB received some sarcasm like ‘Please, can you tell us what the facial expression of a snipe is?’

8.1 DNB Model 1: Intrinsic and extrinsic security features

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. Intrinsic banknote features mentioned by Koeze were, among others: X-ray fluorescence, absorption of electro magnetic micro waves and Electron Spin Resonance (ESR). Another feature mentioned also was based on laser Raman spectroscopy (in the infrared spectrum).

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 [2].

Machine readable features based on counterfeit policy
The model was first applied in 1979 in the development policy concerning machine readable features. One intrinsic and one extrinsic feature were proposed for both the paper and the print: c 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) [3].

Finally the new 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 22). The ink of the banknote number could be either magnetic or non-magnetic.

\[\text{ISARD} \quad \text{AQUs}\]

*Figure 22.*
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.

**ISARD and AQUs**
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 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 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’!).

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 [13]. 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 extrinsic 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 'nail scratch feature' on the euro series [48]. 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 23.
Figure 23.
Left: conceptual proposal for a so called ‘free intaglio detector’. Instead of the fixed intaglio line element shown in Figure 22 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 [31].
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 Wiggins (2004). Based on DNB EU patent on BCWM (2003) [30].

Internal and add-on features
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. Under this definition, the AQUUS and the ISARD now became - confusingly! - internal features (instead of extrinsic). Next to watermark and intaglio printing a new unmistakeable example of an internal feature was born in the early 1990ths: the micro perforation of a banknote, first used in Swiss banknotes (CHF 50, 1995). The optical thin-film patch on the Canadian banknotes first issued in 1989, applied by a special cold transfer technique, is an other example of an internal feature.

Internal features still preferred
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 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.
Overt versus covert

Intrinsic/extrinsic and internal/add-on features should not be confused with overt and covert features. Until 1980, security features were kept secret, because in banking circles the notion reigned that to tell the public was to tell the counterfeiter[s] [68]. 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 [6]. Of course, public features should be evident, even striking, while features for sorting machines should be undetectable to the human eye.

As stated in the Introduction of this paper, the Swiss National Bank was the first with a public leaflet in 1976.

Considering the trend that counterfeiters mainly try to fool the retailer and the public and therefore mainly imitated retail and public features, a constant development of improved and new retail and public security features should receive priority. It would seem that the security industry focuses too much on add-on technologies as is suggested by Table 12.

<table>
<thead>
<tr>
<th>Banknote production process</th>
<th>Security features</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Internal</td>
</tr>
<tr>
<td>1. Paper</td>
<td>mass variations within the paper (watermark, barcode watermark),</td>
</tr>
<tr>
<td>2. Foil (hot stamping)</td>
<td>glue, special unique colours, additional layers, nanotechnology, e-beam made holograms (high resolution)</td>
</tr>
<tr>
<td>3. Thin-foil (cold transfer technique)</td>
<td>patch changing colour</td>
</tr>
<tr>
<td>4. Silk screen/rotogravure</td>
<td>extremely small two dimensional signatures</td>
</tr>
<tr>
<td>5. Offset</td>
<td>spectral values (layers of ink), small silicon printed on wafer *</td>
</tr>
<tr>
<td>6. Intaglio</td>
<td>ink mass variations</td>
</tr>
<tr>
<td>7. Numbering</td>
<td>number + database</td>
</tr>
<tr>
<td>8. Perforations</td>
<td>(micro)perforation patterns through finished banknote</td>
</tr>
<tr>
<td>9. Cutting</td>
<td>shape of edges, notches</td>
</tr>
</tbody>
</table>

Table 12.
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.
**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. Taggants 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). The typical structure of cotton makes every banknote unique and could also be seen as a marker.

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 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.

### 8.2 DNB Model 2: System approach

In 1991 DNB presented a second counterfeit model, based on the principle that a reproduction of an original banknote will never be identical to the original. The counterfeiter has no access to the banknote security industry and have to use reproduction tools of the graphic industry, as indicated in Figure 24. The quality of the reproduction will look poor - although sometimes enriched! - beside 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 paragraph 8.2.1. 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, a note well protected against colour copying, issued in 1993 [16].
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.’ [19]. Over the years the system was developed further [22, 25, 43, 87] and today the model may be described as shown in Figure 25. The six key dimensions are specified in more detail in Table 13.

![Diagram](image)

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

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

Table 13.
Overview of the six dimensions used in the system approach and the corresponding units (overview of units is not exhaustive).

Reporting on banknotes based on black box approach
The black box approach enables reporting on banknotes in terms of the six dimensions described above. Table 14 is an example based on the public security features in the euro series 2002. According to this method the see-through register is rather weak and watermark quite strong. The black box approach also permits real measurements between original and counterfeits. An example of this is provided in Table 15.
Counterfeited public security feature in euro banknotes

<table>
<thead>
<tr>
<th></th>
<th>Watermark</th>
<th>Foil/hologram</th>
<th>Security thread</th>
<th>See-through register</th>
<th>Colour: iridescence/OVI</th>
<th>Tactility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colour</td>
<td>o</td>
<td>o</td>
<td>-</td>
<td>o</td>
<td>+</td>
<td>o</td>
</tr>
<tr>
<td>Density</td>
<td>+</td>
<td>o</td>
<td>+</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Resolution</td>
<td>+ +</td>
<td>+</td>
<td>+</td>
<td>o</td>
<td>o</td>
<td>+</td>
</tr>
<tr>
<td>Geometry</td>
<td>+</td>
<td>+</td>
<td>0</td>
<td>+</td>
<td>0</td>
<td>+ 2)</td>
</tr>
<tr>
<td>Mass</td>
<td>- 1)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Material</td>
<td>o</td>
<td>o</td>
<td>+</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
</tbody>
</table>

Table 14.
Strength-weakness analysis of the 6 public features of the euro series 2002 according to the black box model or system approach. Original compared to counterfeit:
+ + = original much better than counterfeit, + = original better, o = original and counterfeit quite similar,
- = counterfeit slightly better, - - = counterfeit is better than original. N/A = not applicable.
1) because paper weight is similar to standard in copy machines, 2) for nail scratch element.

Gloss

<table>
<thead>
<tr>
<th>original hologram</th>
<th>Reproduction</th>
<th>Gloss reproduced hologram</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>Sample A</td>
<td>283</td>
</tr>
<tr>
<td></td>
<td>Sample B</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>Sample C</td>
<td>709</td>
</tr>
</tbody>
</table>

Table 15.
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' [41, 43].

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 (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 26.
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.’ [89]. 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. 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 (first banknote gravure: 1732).

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. Table 16 provides a short and incomplete historic overview of counterfeit threats and the reaction of central banks and indicating the dimension on which the new protection may be reduced, like resolution, geometry or colour.

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!
### Historical counterfeit threats and the reactions of central banks

<table>
<thead>
<tr>
<th>Threat</th>
<th>Year</th>
<th>Central bank’s reaction</th>
<th>Dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>1282</td>
<td>Watermark</td>
<td>Density</td>
</tr>
<tr>
<td></td>
<td>1661</td>
<td>First banknote with watermark (Stockholms Banco)</td>
<td>Density</td>
</tr>
<tr>
<td></td>
<td>1694</td>
<td>Marbled paper (GBP)</td>
<td>Material</td>
</tr>
<tr>
<td></td>
<td>1694</td>
<td>Gravure printing using copper plates, maximum 10,000 passes (GBP)</td>
<td>Geometry</td>
</tr>
<tr>
<td>Changing value of real notes</td>
<td>1797</td>
<td>Anti erasure feature: an elaborate £-sign in front of the amount (GBP)</td>
<td>Geometry</td>
</tr>
<tr>
<td>Carving</td>
<td>1809</td>
<td>First forgeries. Number by letter press (GBP)</td>
<td>Geometry</td>
</tr>
<tr>
<td>Original banknotes not uniform</td>
<td>1819/1836</td>
<td>Plate Transfer Method (hardened steel mother plate) invented by Jacob Perkins</td>
<td>Geometry</td>
</tr>
<tr>
<td></td>
<td>1839</td>
<td>Electotype invented by Boris Jakobi</td>
<td>Geometry</td>
</tr>
<tr>
<td>Photography</td>
<td>ca. 1850</td>
<td>Introduction of colour</td>
<td>Colour</td>
</tr>
<tr>
<td></td>
<td>1855</td>
<td>Shaded watermark (GBP)</td>
<td>Density</td>
</tr>
<tr>
<td></td>
<td>1867</td>
<td>Security thread (silk), Crane</td>
<td>Material, density</td>
</tr>
<tr>
<td></td>
<td>1876</td>
<td>First photographic forgery discovered (GB)</td>
<td>-</td>
</tr>
<tr>
<td>Offset printing</td>
<td>ca. 1920</td>
<td>Line printing in alternating colours (up to 3 lines)</td>
<td>Geometry</td>
</tr>
<tr>
<td></td>
<td>ca. 1925</td>
<td>First see-through register (RZ press)</td>
<td>Geometry</td>
</tr>
<tr>
<td></td>
<td>1928</td>
<td>First banknote introducing colour, red for 10 shilling, green for 1 pound (GBP)</td>
<td>Colour</td>
</tr>
<tr>
<td></td>
<td>ca. 1960</td>
<td>Simultan press (see-through register)</td>
<td>Geometry</td>
</tr>
<tr>
<td></td>
<td>ca. 1970</td>
<td>Introduction UV features</td>
<td>Colour</td>
</tr>
<tr>
<td></td>
<td>ca. 1980</td>
<td>Magnetic particle printing (e.g. in number)</td>
<td>Material</td>
</tr>
<tr>
<td></td>
<td>ca. 1980</td>
<td>Introduction IR features</td>
<td>Colour</td>
</tr>
<tr>
<td>Colour copy machines</td>
<td>1988</td>
<td>Polymer banknote with transparent window and foil with pixelgram, ASD 10</td>
<td>Material, density</td>
</tr>
<tr>
<td></td>
<td>1989</td>
<td>Foil with hologram. ATS 1,000</td>
<td>Material, density</td>
</tr>
<tr>
<td></td>
<td>1989</td>
<td>First OVI in intaglio, THB 60, commemorative note, issued 1989</td>
<td>Colour change</td>
</tr>
<tr>
<td></td>
<td>1989</td>
<td>Thin-film patch (OSD) by cold transfer technique, turning from gold to green (CAD 50, issued 1989)</td>
<td>Density, colour</td>
</tr>
<tr>
<td></td>
<td>1990</td>
<td>Windowed thread (Stardust), GBP 5, 20</td>
<td>Geometry, density</td>
</tr>
<tr>
<td></td>
<td>1991</td>
<td>Spectral features (M-feature), DEM 10</td>
<td>Material</td>
</tr>
<tr>
<td></td>
<td>ca. 1994</td>
<td>Common Mark/Security Circles to prevent from copying</td>
<td>Geometry, density</td>
</tr>
<tr>
<td>Home scanners</td>
<td>ca. 1990</td>
<td>Counterfeit Deterrence Systems</td>
<td>Geometry</td>
</tr>
<tr>
<td></td>
<td>1992</td>
<td>Simultan presses with 4/4, usually 3 plates dry offset and one wet.</td>
<td>Resolution</td>
</tr>
<tr>
<td></td>
<td>1992</td>
<td>Silk screen, pearl lustre, NLG 100, 1992</td>
<td>Density</td>
</tr>
<tr>
<td></td>
<td>1995</td>
<td>Micro perforations, CHF 50, 1995</td>
<td>Geometry</td>
</tr>
<tr>
<td>All in one devices</td>
<td>ca. 2000</td>
<td>Transparent window in cotton banknotes, BGL 100, commemorative note, issued 2005</td>
<td>Material, geometry, density</td>
</tr>
<tr>
<td></td>
<td>2009</td>
<td>Watermark with large highlight area (pixel area), MXN 200 com. note, issued 2009</td>
<td>Geometry, density</td>
</tr>
<tr>
<td></td>
<td>2009</td>
<td>Hybrid banknote paper: film-cotton-film SLZ 100 and 200, commemorative note, 2009</td>
<td>Material</td>
</tr>
<tr>
<td></td>
<td>2010</td>
<td>Hybrid paper: paper-polymer-paper (CHF 50)</td>
<td>Material</td>
</tr>
</tbody>
</table>

*Table 16.*

Overview of several historical threats and the reaction 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.

*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 27).

![Wings security thread](image)

*Figure 27.*
The Wings security thread shows up quite differently in reflection and in transmission (Goznak, 2007).

Also, the real security of the Motion feature is not only the lenticular lenses (geometry), but especially the high resolution of the electro-graphical printing underneath these lenses. A transparent window in a paper banknote is mainly a matter of material and optical density (Figure 28). 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.

![Characterising Motion](image)

*Figure 28.*
Characterising Motion and transparent window with the system approach.
System approach applied on Counterfeit Deterrence Systems

The principle of Counterfeit Deterrence Systems (CDS) may also be explained by the system approach, as is done in Figure 29. An intrinsic feature, such as a taggant might be an option for such systems, since high-speed detection is not required. Taggants are not visible and therefore inconspicuous. Furthermore taggants take no space.

Figure 29.
Basic principle of prevention of banknote reproduction: no output.

Not all eggs in one basket
The selection of security features for a new banknote may profit from this system approach. The central bank could select the features on the principle of ‘not all eggs in one basket’ and could opt for a strategic spread of the features over the six dimensions (Figure 30).

Figure 30.
Selection of security features for a new banknote could be based on the policy ‘do not put all your eggs in one basket’.

8.2.1 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 graphic 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. A resolution of 360 dpi is equivalent to 6.6 lp/mm.

**Eigenfrequency**

Over the decades several security features were developed based on printed lines, such as lines in alternating colours, as will be explained in Section 8.2.2 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 [28]. 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 found that for being effective, the line width of the printed and the unprinted line should be exactly the same [4]. 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 which trigger the public’s attention. Today such features are not considered to be public features, but trigger features (or level 0). Such trigger features make the counterfeited note look blurred or brownish, which triggers people to check for example the watermark and other public security features [48, 55].

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 31). Disturbance by interference (moiré patterns) or by aliasing effects (i.e. eigenfrequency) would disturb the homogenous circle so was the design idea.

![Image of banknotes with screen and scan traps](image)

*Figure 31.*

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.

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 32). 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 32). 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).

![Diagram](Figure 35. 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 \( \alpha_o \) and C is contrast.

Table 17 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).

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

Table 17. Characterisation of reproduction systems by resolution in terms of line pairs per millimeter.
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’ [7]. 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 31).

Another clear example of the black box model was the introduction of intaglio micro printing for that same note. According to the printer, the 0.2 mm letter height proposed by DNB could not be achieved, but DNB proved that it could, with the letter font shown in Figure 33 a) and b) [10].

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 33 c) and d) may be used to create new images and so may go down better with the public.

Figure 33.

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).

8.2.2 Dry offset printing

This paragraph is specifically dedicated to dry offset Simultan printing, a banknote printing technology which is outdated, in the author’s opinion, 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. As said in the introduction of this Chapter, the answer for DNB was the introduction of two-colour offset presses (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 34. 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 in Figure 35.
Security principle of alternating line colours, based on two colours (left, since around 1925) and based on three colours (right, since around 1960).

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).

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 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 images are printed in one run - simultaneously - on both the front and the reverse of the banknote paper.

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. The presses had another property unavailable in the outside graphic industry: one plate on the front could be printed in perfect register with one plate on the reverse (+/- 0.10 mm).
To date 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 35). Also the fit of the front and the reverse, the see-through register, no longer provides a defence against current reproduction techniques. Its main drawback is its low resolution (around 8 lp/mm); most commercial presses can do better. Also the line broadening because of the slight relief of the dry offset plates is today a disadvantage for a security product like 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 36). The MVC is a smart construction making use of the high registration between the three offset plates. The MVC feature shows all kind of rainbow colours when the banknote is tilted.

**Figure 36.**
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.

### 8.2.3 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 37). 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 31 for an example from the NLG 250/Lighthouse).

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 experiment was carried out by DNB with the green NLG 1,000/Lapwing as shown in Figure 38b and reported in 1996 [23]. 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.
Figure 37.
Development model for security features based on density. Tonal range of perfect (A) and imperfect (B) graphic reproduction.

Figure 38.
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).

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 located next to an area with high single-print density. The difference in density must be visible in the original but not in a graphic reproduction. For this purpose a grey scale from 90 - 100 % could be suitable. The same colour was used for both the intaglio print and the offset print. Figure 38c show an application of this principle. The high density properties were used again in the NLG 10/Kingfisher, issued in 1997.
8.2.4 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. 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 euroscale colour reproduction standard. The bright orange colour, showing up brown in a reproduction, was first introduced on the NLG 50/Sunflower issued in 1982.

In 1986 some more design studies on colours outside the euroscale were performed. One idea that came out of this study was to print a reference next to the colour outside the euroscale. This reference was the colour the ‘outlier’ colour would show up as in 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 39 explains the principle and provides some examples.

![Figure 39](image.png)

*Figure 39.* Study of colours outside the euroscale reproduction standard, 1986 [9, 11].

a) Basic principle. The colour B’ will be reproduced as colour B, which ideally should be similar to colour A). Within the ellipse humans will perceive no colour difference between A and B.

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.
Metameric colours

An other example of a colour pair based on the ‘colour dimension’ are so-called metameric colours also recommended by the NRC in their NextGen report [62]. 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 40). In the years that followed some more metameric studies were done by DNB and Joh. Enschedé. One example is shown in Figure 41. 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 40). In 2001 DNB proposed a metameric barcode for the euro banknotes (see Figure 9).

Figure 40.

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).

Figure 41.

Design study on metameric colours by Joh. Enschedé, based on designs made by Hans Kruit. On the left the original (here of course reproduced) and on the right a contemporary colour-copied reproduction (ca. 1986).
8.3 DNB Model 3: Simple method

Up to 2002, classifying 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 (NAC). 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 Mr. Marco Wind (DNB) a new, simple method was developed and introduced in DNB’s monthly report 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 42 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

![Counterfeit scoring examples](image)

Figure 42.
Six examples of counterfeited public security features in euro banknote forgeries and the assignment of points according to the simple method.
Maximum score = 12
Euro banknotes have 6 public features, so the maximum counterfeit quality score is 12. Figure 43 is taken from the report on banknote counterfeit quality in the Netherlands as measured in September 2009.

![Graph of counterfeit quality scores.](image)

Figure 43.
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.

Two interesting conclusions were drawn immediately:
- not one euro counterfeit received 12 points; the maximum score to date is 10 points (euro 200p3),
- the average quality score is around 6.5 points.

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.’ [94].

Quality of counterfeits in NL
If all scores for one denomination are grouped, the ‘average public score’ may be calculated, as shown in Figure 44. This is the average quality of the ten most frequently found counterfeits in the Netherlands in the January 2008 - September 2009 period. Note that in the Netherlands, euro 50 counterfeits have the highest occurrence rate: some 80% of all counterfeits are euro 50s, which is why there are several euro 50 counterfeit types (indicatives) represented. The euro 20 makes up about 12 % 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).
Figure 44.
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).

This exercise yields an interesting conclusion: the quality of counterfeits is not rising, but declining. From the graph in Figure 44 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 (!, since it is the most used denomination in NL).

Quality of counterfeited public security features
The simple method also delivers the individual quality of each public feature as provided in Table 18, 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 feature seems to be the strongest public security feature.

<table>
<thead>
<tr>
<th>Quality of counterfeited public security features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public feature</strong></td>
</tr>
<tr>
<td>1. Watermark</td>
</tr>
<tr>
<td>2. See-through register</td>
</tr>
<tr>
<td>3. Foil</td>
</tr>
<tr>
<td>4. Security thread</td>
</tr>
<tr>
<td>5. Tactile effect intaglio</td>
</tr>
<tr>
<td>6. Iridescence/OVI</td>
</tr>
<tr>
<td><strong>Retail feature</strong></td>
</tr>
<tr>
<td>1. UV</td>
</tr>
<tr>
<td>2. IR</td>
</tr>
</tbody>
</table>

*Table 18.*
Quality of counterfeited public security features in euro banknotes, based on the 10 most frequently received counterfeit types in the Netherlands (April 2009 figures).
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 [50].

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.

The method was also validated during a research project in which it was tested how well the public and retailers could distinguish counterfeits from genuine notes (see paragraph 8.5.1 Discrimination of counterfeits by public and retailers). 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. Deviation in correlation found may be attributable to the fact that the paper quality ‘feel’ is not accounted for. Further research is needed to fine tune the method.

8.4 Preparation of counterfeits for 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. These first ‘self made counterfeits’ were printed by the colour copy machine at security printer Enschedé. In 1995 DNB travelled for the first time to Copenhagen, to the Reproduction Research Centre (RRC), to prepare such self made counterfeits. Figure 45 shows two examples. The RRC is an initiative of Denmark’s national bank and is established on 1 December 1989.

![Figure 45.](image)

Colour copy reproductions of NLG 1,000/Lapwing made by DNB at the RRC in Copenhagen in 1995.

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 19 presents an imaginary example of such a method, reporting on the time, expertise and investment needed to reproduce a newly designed banknote.
### COUNTERFEIT INVESTMENTS

<table>
<thead>
<tr>
<th></th>
<th>Time</th>
<th>Expertise</th>
<th>Cost in EUR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A. COPY</strong> - pre press</td>
<td>Push-the button: 1 s</td>
<td>Primitive</td>
<td>0</td>
</tr>
<tr>
<td>- pre press</td>
<td>100 hour</td>
<td>Primitive</td>
<td>100</td>
</tr>
<tr>
<td>- production</td>
<td>1 day</td>
<td>Casual, hobbyist</td>
<td>~ 1,000</td>
</tr>
<tr>
<td><strong>B. INK JET</strong> - pre press</td>
<td>10 hour</td>
<td>Primitive</td>
<td>~ 100</td>
</tr>
<tr>
<td>- pre press</td>
<td>1 week</td>
<td>Professional</td>
<td>~ 10,000</td>
</tr>
<tr>
<td>- production</td>
<td>3,000/hour</td>
<td>Casual, hobbyist</td>
<td>~ 50,000</td>
</tr>
</tbody>
</table>

**Table 19.**
Overview of the time, expertise and investments needed by the counterfeiter to make a reproduction. Expertise subgroups correspond to those defined in Chapter 2 (primitive, hobbyist, professional and state-sponsored). The figures mentioned are estimations. A reference is needed to judge if the counterfeit resistance of the new note is poor, medium or good.

**Evaluation of research results**

A research team studying a new or improved security feature might present its results as shown in Table 20. 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 the preferred foil design [37, 41, 43].

<table>
<thead>
<tr>
<th>Ordinal ranking of foil/hologram samples</th>
<th>Public preference</th>
<th>Counterfeit resistance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. A</td>
<td>1. I</td>
<td></td>
</tr>
<tr>
<td>3. C</td>
<td>3. F</td>
<td></td>
</tr>
<tr>
<td>4. D</td>
<td>4. B</td>
<td></td>
</tr>
<tr>
<td>5. E</td>
<td>5. C</td>
<td></td>
</tr>
<tr>
<td>6. F</td>
<td>6. D</td>
<td></td>
</tr>
<tr>
<td>7. G</td>
<td>7. J</td>
<td></td>
</tr>
<tr>
<td>8. H</td>
<td>8. K</td>
<td></td>
</tr>
<tr>
<td>10. J</td>
<td>10. L</td>
<td></td>
</tr>
<tr>
<td>12. L</td>
<td>12. A</td>
<td></td>
</tr>
<tr>
<td>13. LD original</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 20.**
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, difficult to counterfeit. Yellow = medium, Red = poor, rejected by public, easy to counterfeit.
8.5 DNB Researches

Since the introduction of the euro in 2002, DNB performed several research studies. The following relevant studies are reported here:

8.5.1 Discrimination of counterfeits by public and retailers (2005),
8.5.2 Marketing approach: what does the public want? Conjoint research. (2009),
8.5.3 Marketing mix of public security features (2007),
8.5.4 Communication of public security features (2007, 2009).

8.5.1 Discrimination of counterfeits by public and retailers

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, but here technical aids provided useful services. Practice with the help of the CD-ROM turned out to benefit untrained consumers in particular. They soon managed to bring their performance up to the level of experienced cash handlers [47]. The findings were also reported at the Banknote 2006 conference.

Correlation

Analysing the data of the study mentioned above, Tom Buitelaar (DNB) reported in 2007 that the majority of respondents were not fooled by the imitations. The maximum acceptance rate found is 37.5% for counterfeits having three good imitated public features. Furthermore, a correlation was found between the public acceptance of the counterfeits presented and the quality of the imitated security features. The highest correlation was found for intaglio relief, security thread and watermark, meaning that the public prefers these features in checking euro banknotes on 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 [59]. Except for the foil/hologram these findings match qualitatively with the public awareness of security features as reported in Table 3.

UV feature not reliable

The UV features in the counterfeited euro notes are imitated so well that UV light did not contribute to correct identification by the retailers for which this feature was intended (Figure 46). 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 public. Washed genuine banknotes on the other hand will light up under UV light because of the bleaching agents in some detergents and may be misjudged as a counterfeit.

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. Some UV imitations are hard to distinguish from the real thing. The Bank of Russia agreed that ‘the counterfeiters reproduced the UV feature of banknotes well enough. In this way they practically invalidated such devices as the UV lamp.’ [76]. The Russian Ministry of Internal Affairs holds...
the same opinion ‘The luminescence of the counterfeit is poor, yet close to that of the genuine note.’ [94].

Figure 46. Banknotes under UV light. Because of the brighter reflection of the UV features in the counterfeited note, many people accept this note as real.

**DNB’s policy with respect to UV**
Since 2006 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.

**Short and long UV**
The response of the security industry 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’). This response using ‘double’ UV features applies the (undesired) nested feature approach and creates features that take too long to check. An automatic UV detector detecting within 2 s whether a note is forged could be attractive to retailers.

8.5.2 Marketing approach: what does the public want?

In 2009, at the request of DNB, TNS/NIPO researched the public preference for different sets of security features [86]. 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, six different attributes of the security features of a banknote were distinguished, each with 2 or 3 levels as shown in Table 21.

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.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Attribute level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Location of security feature</td>
<td>Everything on the front</td>
</tr>
<tr>
<td></td>
<td>Everything on the back</td>
</tr>
<tr>
<td></td>
<td>Partly on the front and partly on the back</td>
</tr>
<tr>
<td>2. Number of security features</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>6</td>
</tr>
<tr>
<td>3. Degree of conspicuousness</td>
<td>Should be noticed at first glance</td>
</tr>
<tr>
<td></td>
<td>Should be somewhat concealed</td>
</tr>
<tr>
<td>4. Degree of complexity</td>
<td>Should be verifiable at one glance</td>
</tr>
<tr>
<td></td>
<td>Should need an effort to verify</td>
</tr>
<tr>
<td>5. Pictorial element used for security feature</td>
<td>Figurative: clear and recognisable images (for example flowers, animals, buildings)</td>
</tr>
<tr>
<td></td>
<td>Number: value of the banknote (for example 5, 10, 20, 50)</td>
</tr>
<tr>
<td></td>
<td>Abstract: combined, no obvious depiction (for example lines and compartments)</td>
</tr>
<tr>
<td>6. Appearance of security feature</td>
<td>Technically improved, but with the same appearance as the current security features</td>
</tr>
<tr>
<td></td>
<td>Technically improved, and with a modern, state-of-the-art appearance</td>
</tr>
</tbody>
</table>

*Table 21.*
Overview of the six attributes of the security features of a banknote and their levels used in the conjoint analysis 2009.

*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 22.

<table>
<thead>
<tr>
<th>Euro banknote characteristic</th>
<th>Score in %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of security feature</td>
<td>30</td>
</tr>
<tr>
<td>Number of security features</td>
<td>23</td>
</tr>
<tr>
<td>Type of image</td>
<td>18</td>
</tr>
<tr>
<td>Degree of complexity</td>
<td>13</td>
</tr>
<tr>
<td>Degree of conspicuousness</td>
<td>9</td>
</tr>
<tr>
<td>Appearance of security features</td>
<td>6</td>
</tr>
</tbody>
</table>

*Table 22.*
Relative importance of the characteristics of the security features on euro banknotes.

*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.’ [60].

The graph in Figure 47 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. In fact, it is by far the strongest boost that can be given, it would become possible to check the soundness of the note at one glance.

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 several attribute levels mentioned. The model will tell the user the level of public acceptance relative to another concept, e.g. the existing euro 50.

8.5.3. Marketing mix of public security features
Analysing the considered security features by a marketing approach is an other vital aspect of the feature selection. The new features should fit in a balanced mix of old and new public security features, a ‘marketing mix’ which results in fact in a gradual approach. The first item to decide upon is the number of public security features (PSF). Since the public will not recall more than
four security features, it seems that four features is enough [25, 48]. However, central banks may want to incorporate more than four PSF and opt for a mix of active and sleeping public security features. Three features will be actively communicated, while three public features are kept sleeping. Sleeping features will be awakened - some or all - when one or more of the other features are heavily counterfeited.

In the example of Table 23 a total of six PSF, three active and three sleeping, is divided over the front and the reverse. However, different concepts are possible.

<table>
<thead>
<tr>
<th>Divide security features over feel - look - tilt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
</tr>
<tr>
<td>Feel</td>
</tr>
<tr>
<td>Look</td>
</tr>
<tr>
<td>Tilt</td>
</tr>
</tbody>
</table>

+ = active public security feature, to be communicated

o = sleeping public security feature

Table 23.
Marketing mix of six public security features divided over ‘feel, look and tilt’ and over front and reverse.

Keep ‘gold’ features from previous series
Issuing a new series of banknotes using only completely new public security features is a risky policy. Do not alter or leave out features to which the public has grown accustomed! Bear in mind that it takes a long time before the public will be able to recall new features; public knowledge of security features should be cherished like gold! Existing features enjoying high public awareness should be cherished like gold, since it is a proven fact that the public is very hard to familiarise with new security features. A fine example of a traditional feature is the watermark. Used for the first time over 300 years ago, it is still the most popular banknote security feature!

A gradual approach, using also improved versions of the best PSF of the previous series is accepted best practice. The basic change policy regarding banknote features would therefore be, in the case of six PSF:
1) Keep, but improve, 2 - 4 features,
2) Introduce 2 - 4 new features.

This principle is illustrated in Figure 48 [65]. Table 24 indicates which features of the old banknote series are most widely known and should return - improved - in the next series.

<table>
<thead>
<tr>
<th>OLD SERIES</th>
<th>+</th>
<th>NEW FEATURES</th>
<th>=</th>
<th>NEW SERIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 - 4 PSF</td>
<td></td>
<td>2 - 4 PSF</td>
<td></td>
<td>6 PSF</td>
</tr>
</tbody>
</table>

Figure 48.
Example of the gradual approach applied to the selection of 6 PSF for the new series: 2 - 4 public features are retained from the previous series and 2 - 4 new features are added.
PSF = Public Security Feature(s).
RANKING OF PUBLIC SECURITY FEATURES

<table>
<thead>
<tr>
<th>PSF in euro series 2002</th>
<th>Public knowledge in NL (2009)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Watermark</td>
<td>76 %</td>
</tr>
<tr>
<td>2. Hologram/silver foil</td>
<td>55 %</td>
</tr>
<tr>
<td>3. Security thread</td>
<td>15 %</td>
</tr>
<tr>
<td>4. See-through register</td>
<td>9 %</td>
</tr>
<tr>
<td>5. Raised ink, relief</td>
<td>8 %</td>
</tr>
<tr>
<td>6. Special ink (iridescent ink/OVI)</td>
<td>2 - 3 %</td>
</tr>
</tbody>
</table>

Table 24.
Keep the best-known features. Cherish familiarity with security features in old series like gold! Public awareness of existing features is taken from Table 3.

Policy ECB
At the Currency Conference 2007, the ECB presented the desired number of security features for the next series of euro banknotes (Table 25), based on work done in 2004 -2005 [53, 70, 88].

<table>
<thead>
<tr>
<th>User group</th>
<th>Number</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1 Public</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Level 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) Retailers – human</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>b) Retailers – automatic device</td>
<td></td>
<td>At least 4</td>
</tr>
<tr>
<td>c) Third-party sorting machines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 3 Central bank sorting machines</td>
<td>4 to 6</td>
<td>2 or 3 in substrate and 2 or 3 applied in printing works</td>
</tr>
</tbody>
</table>

Table 25.
Overview of the proposed number of security features in the Euro Series 2.

The proposed mix of public features may be completed by dividing the 6 features over the *Feel Look Tilt* motto. Within each of these three categories, the best known features from the previous series could be kept. In case of six public features a total of three new features are needed, preferably also divided over *Feel Look Tilt* and would lead to a marketing mix as first suggested in 2007 by De Heij, in this paper reproduced as Table 26 [55].

<table>
<thead>
<tr>
<th>Public use</th>
<th>Public security feature</th>
<th>Public knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEEL</td>
<td>1. previous (e.g. improved tactility)</td>
<td>8 %</td>
</tr>
<tr>
<td></td>
<td>2. new (e.g. nail scratch element)</td>
<td>-</td>
</tr>
<tr>
<td>LOOK</td>
<td>- through</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- at</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. previous (e.g. improved watermark)</td>
<td>76 %</td>
</tr>
<tr>
<td></td>
<td>4. new (e.g. secure window)</td>
<td>-</td>
</tr>
<tr>
<td>TILT</td>
<td>5. previous (e.g. hologram)</td>
<td>55 %</td>
</tr>
<tr>
<td></td>
<td>6. new (e.g. floating image or colour shifting feature)</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 26.
An example of a set of public security features based on a ‘marketing mix’.
Selection strategy for groups of security features

Individual security features should not be selected at random. It is logical to start with the selection of retail and public features, since they will dominate the banknote design. Features for detectors usually have a large ‘design freedom’ and there is much more choice. Figure 49 provides such a strategy.

![Figure 49](image)

Strategy for selection order of security features. First the retail and public features should be selected, since they are dominating the design. Machine readable features have a larger ‘design freedom’ and there is much more choice.

Selection of retail features

Existing retail features (level 2a) are detected with an UV lamp, IR viewer or a magnifying glass. In some cases a mirror is used to check the colour changing feature (OVI). The last decades the magnifying glass is hardly used and has become obsolete (see also Tables 6 and 7). From a marketing point of view there is a need for a follow up of the magnifying glass. Features based on filter seem to full fill the user requirements and therefore such ‘filter’ features could be selected, like for example a polarisation filter. The IR viewer is not much used, but does not yet disappear from the shops (Table 6). Instead auto detection, often (partially) based on IR properties (level 2b) is growing in popularity.

Future development

The ‘marketing method’ may be further developed by creating banknote concepts based on different sets of 20 to 25 security features each. In case of NLG notes the total number of features was limited to 20 [25]. Central banks and manufacturers are getting aware to limit the number of security features in a banknote: ‘As we continue to develop security features, we need to ensure we do not overcomplicate banknotes for the public.’ a statement made by a well known security printer on the Currency Conference 2008 [74].

Central banks may want to develop different packages of security features before a choice is made. A template is provided in Table 27, showing three different feature sets for Models A, B and C. In 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 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, one would create a complete prototype of each feature set and test these packages for public and retailer preference.
**THREE SETS OF SECURITY FEATURES**

| Cost increase to previous | Model A  
+ 0 % | Model B  
+ 5 % | Model C  
+ 10 % |
|---------------------------|---------|---------|---------|
| **Trigger**  
**level 0**  
| | 2. Grey colour | 2. Different paper tints | 2. Different paper tints |
| | 3. Screen and scan traps | 3. Screen and scan traps | 3. Screen and scan traps |
| **Public**  
**level 1**  
| | 5. Feel: nail scratch area | 5. Feel: embedded tactility | 5. Feel: thermo chromic |
| | 7. Look: full embedded security thread, e.g. Wings | 7. Look: windowed thread colour switch | 7. Look: ‘secure window’ die cutting |
| | 8. Tilt: foil/hologram, continuous stripe, 10 mm | 8. Tilt: foil/hologram, registered stripe, 12 mm | 8. Tilt: foil/hologram registered stripe, 20 mm |
| **Retailer ‘human’**  
**level 2a**  
2/3 | 10. Glue of foil in note colour | 10. Multi colour UV image | 10. IR-image |
| | 12. UV-fibres bi-colour | - | 12. UV short/long wave bi- or tricolour images |
| **Retailer device**  
**level 2b, 2** | 13. | 12. | 13. |
| **Third party sorting**  
**level 2c, 1** | 15. | 14. | 15. |
| **Central bank**  
**level 3**  
2 | 16. | 15. | 16. |
| | 17. | 16. | 17. |
| | 18. | 17. | 18. |
| **CDS**  
**level 4**  
3 | 19. | 18. | 19. |
| | 20. | 19. | 20. |
| **Forensic**  
**level 5 1/2** | 21. nano lettering | 20. botanical DNA | 21. botanical DNA |
| | - | 21. UV-fibres extrusion | 22. nano lettering |
| **TOTAL** | 21 | 21 | 22 |

*Table 27.*  
Example of three conceptual banknotes A, B and C with different cost prices and different sets of security features. In this example a total 21 or 22 security features are foreseen. CtIP = Computer to Intaglio Plate. Retailer ‘human’ are features were some aid is need like a polarisation filter or UV lamp and the decision is human.
8.5.4 Communication of public security features

This chapter ends with a section on the communication of security features and should perhaps be the very first paragraph instead of the last. The message of the central bank does not come across to the public as stipulated before. Figure 50 describes the basic communication model ‘sender-receiver’.

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

Let us start with the following statement by the ECB 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.’ [60]. This policy should be the starting point for a new series of banknotes, rather than being developed once the note is ready for issue. A communication strategy should already be part of the design process as described in ‘Public feedback for better banknote design 2’ [55].

**Series concept**

The communication strategy should first of all cover the complete series. A generic strategy is required, leaving freedom to individual communication concepts for each denomination [25]. The euro banknotes have a so-called *split* between low (5, 10 and 20 euro) and high denominations (50, 100, 200 and 500), each subset having partly different security features. Different public features for low and high denominations make it more difficult to explain and to communicate. ECB research reported in 2004 that close to 70% of the cash handlers did not know that there were two groups of euro banknotes: the low and the high denominations, bearing different security features [34]. Research by DNB in 2007 reported a similar conclusion: ‘The distinction between low and high euro denominations is not effective as it leaves both the public and retailers confused about the security features, besides making the public information tools too complex.’ [48].

A split is not appreciated and it is advisable to apply the same security features throughout the series. For reasons of communication all features should be on the front of the banknote, making a communication concept even stronger. The recent conjoint analysis indicated that people prefer public features both on the front and on the reverse. On the other hand, time spent on the reverse - if at all - is limited to around 1.5 seconds.

For a new banknote series a central bank should decide between better public recognition (all features the same) and higher counterfeit resilience, which always is a trade-off as shown in Figure 51.
Figure 51.
Trade-off between similar security features in all denominations and simple or more complex information tools (e.g. front side of one note explains all). The design of the features can be different, but based on the same technique.

Since the public is quite unaware of security features, it seems that central banks should focus on ‘better public recognition’. This argues in favour of using the similar technique for each public feature throughout a series and incorporating all features on the front. Each denomination within a series could be presented in different designs, such as different watermarks, different paper tints and different foil elements.

Tell a little story
The optimal banknote design uses features that are easy to remember but still difficult to counterfeit. In several publications De Heij plead for a little story as was the case for the Dutch guilder notes [25, 48, 55]. Based on this design philosophy an example was prepared for the Central Bank of Aruba in 2007. In Table 28 the letters A-R-U-B-A tell a little story about the island, for each denomination a different story.

<table>
<thead>
<tr>
<th>Florin</th>
<th>Watermark</th>
<th>See through (offset)</th>
<th>Relief print (intaglio)</th>
<th>Colour crypt (silk screen)</th>
<th>Colour shifting wide thread</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
<td>R</td>
<td>U</td>
<td>B</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Portrait of Indian</td>
<td>Turtle</td>
<td>Dolphin</td>
<td>Shell</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Donkey</td>
<td>Rattle Snake</td>
<td>Iguana</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Pelican</td>
<td>Owl</td>
<td>Butterfly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>Palm tree</td>
<td>Dividive (tree)</td>
<td>Cactus, Aloe,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>Willem III tower</td>
<td>Bird painting from cave</td>
<td>Old coin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>500</td>
<td>Carnival feather</td>
<td>Group of people in carnival-like clothing</td>
<td>Masque</td>
<td>5 continuous silhouettes: fish, flower, bird, tree, persons head, carnival element</td>
<td></td>
</tr>
</tbody>
</table>

Table 28.
A first proposal for design/communication of 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 is kept the same for each denomination.
The 10 Florin tells about the animals in the sea and the theme of the 20 is about animals on land. Animals of the air are found on the 50 animals and the 100 tells us about the typical plants on the island. Old and new architectural elements are used on the 200 and on the highest banknote people are filling the carnival theme. To illustrate this concept further a conceptual banknote design is made for the 100 (Figure 52).

Figure 52.
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 was focussed on banknote identity, in this case by following design elements of banknote designs of European Union, Netherlands, Caribbean area, South America and USA. Design by author (2007), published with permission of Central Bank of Aruba.
9. FUTURE COUNTERFEIT MODEL: PERCEPTION APPROACH

The last chapter of this extensive paper explores a novel research area, an area very much in movement: brain processing of information (perception). As stated in Chapter 5, people do not notice minor changes in banknotes, contrary to what is assumed by the security industry. In this respect it seems that counterfeiters understand the perception of banknotes better than central banks. The application of ‘evidence-based design’ raises questions such as:
- How to draw the attention of both the public and retailers to security features?
- Where and how to mobilize the storage of related information in the brain/memory?
- How to retrieve security feature information from a banknote by just looking at it?

Some first suggestions were made in the ‘Public Feedback’ papers [48, 55], such as way finding features, the retrieval path and the preset lay-out (‘all features in a row’). Other perception examples are those where the mind completes the offered images or optical illusions (ambiguous images, multi stable perception etc.) illustrating that brain processing is only partly understood. An example is Ames room, invented by Adelbert Ames in 1934. This room is a distorted room that is used to create an optical illusion. As a result of the optical illusion a person standing in one corner appears to the observer to be a giant, while the person standing in the other corner appears to be a dwarf. If you want or not, it is impossible to pass the information from your brains: it is impossible to see both persons of equal length! This is what banknote designers would be looking for: an inescapable force to pass the public security features when accepting a banknote!

In this chapter one more step in the pre-design process is added, namely the study of human sensory perception and the storage of perceptions in memory. This approach is called ‘Multi Sensory Design’ (MSD). All human senses are involved and human intuition is exploited. To date, no readily applicable MSD method appears to be available.

9.1 Perception of a euro 20 banknote

According to Colin Ware, if we think of a euro 20 banknote, nothing resembling a picture of a banknote exists in our head. What does exist is more like 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, one note [67]. Figure 53 illustrates how, according to Ware, a EUR 20 note is stored in our visual memory.

![Figure 53](image)

*Figure 53.* Representation of a euro 20 banknote in the visual working memory. Only a few features of the banknote (colour, hologram, numeral and flag) are linked to the knowledge we have about banknotes. Based on the example of a dog in Visual Thinking for Design [67].
The following is based on the perception of a dog as described by Colin Ware, applied by your author to a banknote. Let us take the situation where we accept a banknote in return at the supermarket checkout counter. How do we perceive the change? Assume the change is one 20 euro banknote and some coins. Our rapid eye movements (or saddic eye movements) capture the banknote. From the retinal image some features are captured and processed bottom-up. The captured features could be the ones we know from recollection: colour, denomination numeral, flag and hologram. These two or three features are low-level features, matched by the brain to relevant patterns (a crude map) and finally to an object (a banknote). This object is not simply an image of the banknote. The rest of the banknote features are not yet activated, as illustrated in Figure 53.

<table>
<thead>
<tr>
<th>Phase</th>
<th>What is active?</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Eye movements</td>
<td>Occurs whenever our eyes alight (0.04 s).</td>
</tr>
<tr>
<td>2</td>
<td>Eye movement catches a banknote</td>
<td>Banknote image falls on fovea to be analysed by the brain (0.04 s).</td>
</tr>
<tr>
<td>3</td>
<td>Inferotemporal cortex (IT)</td>
<td>In the IT cortex neurons respond to meaningful patterns, e.g. a banknote or a car. Rapid characterisation of the banknote, categorical judgements. Sub area ‘banknote’ found in 0.1 s.</td>
</tr>
<tr>
<td>4</td>
<td>Cognitive cycle(s) or brain paths</td>
<td>A banknote is a strong gist that will increase the number of cognitive cycles concerning the banknote.</td>
</tr>
<tr>
<td>5</td>
<td>Geon (structured objects)</td>
<td>Three-dimensional shapes or skeletons are stored in the brain. Example: 2D images with shades.</td>
</tr>
<tr>
<td>6</td>
<td>V1, V2, V4, LOC</td>
<td>Pop-up differentiators in V1 (colour, shape, texture, motion, depth). V2’s neurons respond to slightly more complex patterns, based on the processing already done in V1. In V4 more complex compound shapes are identified from patterns of features.</td>
</tr>
<tr>
<td>7</td>
<td>Back to IT, working memory</td>
<td>The banknote image is processed in both the verbal and visual working memory (0.1 s – 1 s, max 2 s). Limitation: up to 3 items.</td>
</tr>
<tr>
<td>8</td>
<td>Linguistic/semantic judgement</td>
<td>Are we looking for denomination, public security features (PSF) or something else?</td>
</tr>
<tr>
<td>9</td>
<td>Search PSF</td>
<td>Orientation and navigation: way finding features, retrieval path, pre-set lay outs.</td>
</tr>
<tr>
<td>10</td>
<td>Motto</td>
<td>Link visual information to verbal working memory. E.g. <em>Feel-look-tilt</em> or <em>Look for Yvonne</em>.</td>
</tr>
<tr>
<td>11</td>
<td>Check PSF</td>
<td>Identification, information: either on colour, geometry, resolution, etc.</td>
</tr>
<tr>
<td>12</td>
<td>Cognitive thread</td>
<td>On going chain reaction towards higher levels of pattern recognition.</td>
</tr>
<tr>
<td>13</td>
<td>Decision on first PSF</td>
<td>Feature OK. Check more.</td>
</tr>
<tr>
<td>14</td>
<td>Check next PSF</td>
<td>Recollection of: ‘check more than one feature!’</td>
</tr>
<tr>
<td>15</td>
<td>Return to phase 9</td>
<td>Repeat motto. Etceteras.</td>
</tr>
</tbody>
</table>

*Table 29.*
Schematic breakdown of the brain process involved in checking a banknote, based on the theory described by Colin Ware. Best guess by author!
At the same time the banknote is processed bottom-up, the brain also processes the note top-down. Top-down processes (or high-level attention) reinforce relevant information, causing a bias in favour of the signals we are looking for. If we are looking for the banknote’s value then the colour and denomination numeral will signal louder. If we are looking for the public security features, then the watermark and the hologram will have their signals enhanced. This biasing in favour of what we are seeking or anticipating occurs at every processing stage. Telling the banknote’s value is accomplished by an iterative process of linking and re-linking visual and non-visual information about the banknote. Because of the very limited capacity of the visual working memory, most information about the 20 euro banknote will be lost as we trace out the coins. We will most probably not check if the received note is genuine.

Table 29 presents a first attempt to make a breakdown of the brain process involved in checking a banknote, based on the book by Colin Ware. More study is clearly needed.

9.2 Designing new banknotes on the basis of eye movement planning

Every day people are working on new banknote designs. What can they already do today? A first recommendation is to start with eye movement planning. Begin by designing an eye tracking path, a further development of pre-set layouts such as ‘all features in a row’ or ‘all features in a circle’ [55]. Eye tracking paths are dependent on the instruction given, e.g. ‘check three public security features’. An eye tracking path should work as a ‘follow me’ instruction. Figure 54 presents such a design. Once the eye tracking path is designed, the features may be worked out in further detail. During the design phase, verify regularly whether the eye tracking path is working. Eye tracking instruments are nowadays made widely available by universities, institutes or commercial parties.

![Figure 54. Example of eye movement planning (‘follow me’) for 6 public security features on a banknote. The feature in the top right corner is ignored.](image)

**Lessons to be learned from information leaflets**

As proposed in paragraph 8.5.4 a security feature communication plan should be ready before the banknote is designed and printed. It is useful to look at banknotes reproduced in public instruction leaflets. Figure 55 shows three examples. Note how symbols such as numbers or letters are used to identify the security features. Banknote design could be explored further on the basis of such symbols. DNB has developed way-finding icons to mark public security features. Apart from alphanumeric information, way-finding icons indicate whether a feature should be checked by feeling, looking or tilting [48]. Figure 56 presents an example, a dummy note prepared in 2003.
Figure 55.
Explaining security features by marking them in the information leaflet. Why not do this on the banknote itself?
(a) image of HKD 1,000 as used in leaflet of the Hong Kong Monetary Authority (around 1995).
(b) image of ZAR 20 as used in leaflet of the South African Reserve Bank (around 2005).
(c) Information tool on credit card size by ECB using numbers to indicate the public security features (2007).

Figure 56.

Figure 57.
Communication symbols introduced by the Bank of Canada early 2008. The design is based on the way-finding 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.
The developed way-finding icons became quite popular as a communication tool. After DNB had used them on its CD-ROM Genuine or counterfeit in 2002, several others adopted them, such as the European Central Bank (2003) and the central banks of South Korea (2006), Chili (2006), Mexico (2007) and Canada (2008) [55]. Often the symbols were modified, as in Canada (see Figure 57). Despite the copyright aspects this is a peculiar habit, since the altered symbols are not tested on their comprehensibility like is the case for the original proposed symbols [44].

Public security features indicated by a letter
Whereas way-finding icons are used in communication tools around the world, the idea of printing them on banknotes has met with resistance, although it has been proved that doing so will increase the average number of public security features recognized from around 2 to 4.7 [55]. However, alternative design solutions have been developed as shown earlier in Figure 52. All five public security features are simple to find, just follow the letters A-R-U-B-A. The same concept may be used for a euro 50 banknote as shown in Figure 58. Here the word E-U-R-O-P-A is indicating six public security features. The basic idea behind these concepts is to find first a meaningful word, supporting the philosophy of the playing man (for the Dutch: *humo ludens*), and subsequently detect the public security feature for each letter.

![Figure 58.](image)
Conceptual banknote EUROPA with six public features E, U, R, O, P and A. People are invited to find all features and works as a memory aid. The letters will also be understood by other cultures as (compare the gate letters at airports. In international championships Greek football players have their names in Latin writing. In Russia the plate numbers on cars are in Latin, not Cyrillic.

Two variants are possible: the currency code E-U-R (three active features on the front) or E-U-R-O (four features on the front). Design by author.
10. CONCLUSIONS

10. General

10.1.1 Public perception of counterfeits in circulation is far above the reality; people overestimate the reality by 200% (NL, 2008).

10.1.2 To assist the selection of security features for new banknotes a model is required. However, there is no such proven model available. Recently some models have been developed by central banks, but these models are not (yet) mature.

10.1.3 Different selection models lead to different preferred features as shown in Table 30. Selection of security features should be done by using different selection models.

<table>
<thead>
<tr>
<th>Feature selection model</th>
<th>Public security features (in euro)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Watermark</td>
</tr>
<tr>
<td>1. User requirements</td>
<td>+</td>
</tr>
<tr>
<td>2. Public knowledge</td>
<td>+</td>
</tr>
<tr>
<td>3. Intrinsic/extrinsic</td>
<td>+</td>
</tr>
<tr>
<td>4. System approach</td>
<td>++</td>
</tr>
<tr>
<td>5. Simple method</td>
<td>-</td>
</tr>
<tr>
<td>6. Public testing (DNB, 2006)</td>
<td>+</td>
</tr>
<tr>
<td>7. Marketing mix</td>
<td>o</td>
</tr>
<tr>
<td>8. Communication</td>
<td>o</td>
</tr>
</tbody>
</table>

Table 30.
Overview of the appreciation of the public security features in the euro 50 banknote, showing 9 different feature selection models.

10.1.4 Dedicated research of central banks will lead to public and retail security features better serving the needs of these user groups. Central banks should write the requirements, the industry should develop.

Worldwide banknotes receive similar public security features, because the introduction of new security features in banknotes is often triggered by suppliers and early adopters.

10.1.5 New features are usually a dedicated barrier against the counterfeits coming in (photography 1850s, colour copiers 1980s, home scanners 1990s). New security features should be a barrier against the new threats. After 30 years of overwhelming innovations in the graphic and information technology industry, there seem to be no new (technical) threats on the horizon.

10.1.6 While the market is offering more and more add-on security features, the choice of internal security features is limited. Yet, if a choice can be made, internal features are preferred over semi-finished features, because they can only be created inside a paper mill or banknote security printing works. By principle internal features are more secure.
10.1.7  The focus of counterfeit reports is often on statistical data and counterfeits seized, illustrated with anecdotic stories, usually about the organisation of the criminals. Studies on counterfeits should be more analytical from the perspective of:
- the range of the dimensions of the reproduction equipment, like resolution, colour, opacity, geometry, mass and material,
- counterfeiter, like production time, skills and investment costs.

10.1.8  The public is not interested in public security features since the probability to receive a counterfeited banknote is very low. This explains why the quality of the counterfeited euro banknotes is relatively low (6.4 on a scale of 0 - 12). Probably this quality will decline further. Central banks are right that the difference between a real and a counterfeited note is easy to see, but their message does not come across to the public.

10.1.9  Instead central banks should focus on the retailer, who is the target of the counterfeiter. The retailer is key in the combat against the acceptance of banknote counterfeits. New banknote designs should assist first of all the retailer.

10.1.10 Public interest in public security features is key to get public attention. Develop a slogan, or keep the one that is successful (e.g. feel-look-tilt). Give the new note a name. All within an attractive design.

10.1.11 From guilloches to holograms; every generation of banknote developers joins in at a new security technology and seems to forget about the old one.

10.2 Feature selection for the public

10.2.1  Fix the total number of public security features required (e.g. 6). Fix also the total number of security features, divided over the user groups (e.g. 20).

10.2.2  Keep the best known public security features from the previous series (e.g. keep 4 of 6).

10.2.3  Make a list of the new public and retail features. Select the features taking less than 2 seconds to verify.

10.2.4  Divide these pre-selected features over 6 dimensions: resolution, colour, opacity, geometry, mass and material.

10.2.5  Divide these pre-selected features over the human operations feel, look and tilt.

10.2.6  Prefer internal features (made in house) over add-on ones (like semi-finished products).

10.2.7  Prefer features with a high ‘design freedom’ (i.e. size, shape, colours).

10.2.8  Prefer features with ‘design variety’ (i.e. available in different colours).

10.2.9  Prefer features that may be combined (‘integrated’) with other banknote design elements (i.e. partly overlap, avoid island features).

10.2.10 Avoid nested features.

10.2.11 Avoid multi level features.
10.3 Banknote series design

10.3.1 A public security features should full-fill all user requirements: fast (< 2 s), easy to use, discreet, reliable (e.g. durable), striking, univocal, easy to communicate and no nested features.

10.3.2 Public security features should have a similar authentication procedure on all denominations; probably, but not necessarily based on the same technology. Avoid denominations within a series bearing different public security features like a split in low and high denominations.

10.3.3 Throughout the series public security features should always be on the same location.

10.3.4 Develop a slogan, or keep the one that is successful (e.g. Feel-look-tilt, Look for Yvonne or E-U-R-O-P-A).

10.3.5 Within the individual banknotes the design theme of the public security features can be different (tell within each note a little story using the colour of the note, the name of the note or something else).

10.3.6 The public will take about 5 seconds to check a banknote (although usually they will not check at all).

10.3.7 Three features should be checked, so 1 to 2 seconds per feature.

10.3.8 Divide the public features (i.e. 6) in active and sleeping features (i.e. 3 active and 3 sleeping).

10.3.9 Active features are promoted. Once a preset threshold level is passed, the sleeping public features could be promoted.

10.3.10 All active public features should be on the front for two reasons:
- preference of the public: in general people do not look at the reverse,
- communication: one poster showing the front of one note is representative for the complete series.

One or two sleeping public security features could be on the reverse. All ‘human detectable’ retail features could also be positioned on the reverse.

10.3.11 Public features based on similar human operations like feel, look or tilt could be grouped together so that these features may be checked in one glance. This is especially true for tilt and look-through features.

10.3.12 Pictorial elements like way finding features or letters will help the public to trace the security features.

10.3.13 Start the design process of the individual banknotes with the development of an ‘eye travel path’. Start with the public and retail security features (there is more design freedom for detector readable features).
10.4 Retailer

10.4.1 A retail feature should full fill all user requirement, like a total authentication time < 2 s.

10.4.2 Retailers do not use a magnifying glass (neither does the public). From a marketing point of view there is a need for a follow up. Features based on a polarisation filter seem to full fill the user requirements of the retailers.

10.4.2 Counterfeits have good imitated UV features, often even brighter than the ones in the real notes. The retailer should not rely on a human operational check under a UV lamp.

10.4.3 Detectors telling ‘yes-or-no the note can be accepted’ are preferred over detectors that need an interpretation by the retailer.

10.4.4 Maximum 3 features for retailers, based on different dimensions. A taggant could used, since the detection speed can be slow.

10.4.5 All human detectable retail features on one side (reverse).

10.5 Counterfeit Deterrence Systems (CDS)

10.5.1 Instead of adding CDS-features once the design is ready, such CDS-features should become part of the design process. Therefore specifications are needed.

10.5.2 CDS-features reduce the design quality of a banknote. Such features require too much space and provide the note with a blurred and pale look.

10.5.3 An intrinsic and invisible feature using the complete banknote surface would be an optimal CDS-feature (like e.g. a spectral property or a special fibre added to the substrate).

10.6 Forensic features

10.6.1 Since forensic features are small, some forensic features could be introduced like e.g. a taggant, fibres with an extrusion profile and a nano-text (letter height 2 µm).

10.7 Test on counterfeit resistance

10.7.1 Tests on counterfeit resistance should be done on the complete new banknote.

10.7.2 Tests on counterfeit resistance should be reproducible by third party and should also report on needed skills, investments and time.

10.7.3 Self made counterfeits of the new note should be tested with retailers and public (providing feedback on the banknote design and its features).

10.7.4 Proposing proof prints of the new banknote to the Board should include two self made counterfeits: a push the button copy and a counterfeit on a professional level.
10.8 Reporting on counterfeits in circulation

10.8.1 Reporting on counterfeits should be done by counterfeits detected per million notes in circulation (counterfeits passed in c/mln).

10.8.2 Information about counterfeits in circulation to the public is fragmented and unclear, leaving the public with a passive attitude and negative feeling. Central banks report in a statistical and juridical way on their counterfeited banknotes and i.e. not in a more informative manner like reporting on:
- the chance to receive a counterfeited note,
- public confidence,
- the difference between genuine and most counterfeited notes.

10.8.3 Central banks do not collect information on how often a security feature is faked. Such information is valuable feedback for the design process of a new banknote.

10.9 Counterfeits in NL

10.9.1 Since the introduction of the euro banknotes in 2002 Dutch retailers are confronted with about 4 times more counterfeits in 2009.

10.9.2 Best known public security features in the Netherlands are watermark, hologram/foil and the security thread.

ACKNOWLEDGEMENT

This paper is part of the fieldwork of my PhD-study ‘Key elements in banknote design’ at the Delft University of Technology, Faculty of Industrial Design Engineering. The paper is a first investigation of this research area and will be discussed with my tutors and supervisor and investigated further.

Several people have contributed so far 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:

- Ms. Jolanda Hijlkema - Duikers (DNB),
  - Mr. Marco Wind (DNB),
  - Dr. Peter Koeze (DNB, retired),
  - European Central Bank.

Further thanks go to Mr. Jan Binnekamp, head of the Currency Policy Department (DNB), for making this paper possible and to Mr. Fred Collens (DNB) and Mr. René Kupershoek (DNB) for editing my English.
REFERENCES

   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.
   Also issued in French: ‘Des caractères lisibles’ Volume 4, Issue 87, Antwerpen, April 1987
32. ‘Next generation of euro banknotes will be different’ interview with Antti Heinonen, Keesing’s Journal of Documents, Issue 3, Amsterdam 2003.
38. ‘The second series of euro banknotes’ Annual Report, European Central Bank, Frankfurt 2005
39. ‘Life cycle analysis of security features in banknotes; from central bank to retailer’.
40. De Heij, Hans A.M.; ‘Life cycle analysis of security features in banknotes; from central bank to retailer’.
41. ‘Counterfeit Report Foil with public appeal’ De Nederlandsche Bank NV, prepared for the European Central Bank, Amsterdam 23 March 2005
47. 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
49. unused reference number
50. Van Haeften, Ewout; ‘Counterfeit threat assessment. A methodology approach’ power point presentation to the Counterfeit Working Group (ESCB), De Nederlandsche Bank NV, October 2006.


52. 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.


56. ‘Increases all round for Australia’ Currency News Volume 5, Number 9, Shepperton September 2007.


58. Dinjens, Marlies; ‘Winkeliers doen biljet van 100 euro in de ban’ Volkskrant, Amsterdam 12 September 2007.


69. 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.


88. ‘Towards the second series of euro banknotes’ interview with Antti Heinonen, Banknotes of the World No. 6, Moscow, June 2009.


92. ‘Currency provides anything but a tall order for De La Rue’s new CEO’ Currency News, Vol 7, No 6, Shepperton June 2009.


94. ‘Do not look down on counterfeits’ Banknotes of the World, Number 7, July 2009 Moscow.

95. ‘Biannual information on euro banknote counterfeiting’ press release ECB, 13 July 2009.


98. Balueva, Tatiana; ‘In search of new images’ interview with Hans de Heij, Watermark, Number 5, St. Petersburg 2009.
