We continue informing our readers about the results of the latest research in counterfeit deterrence and the development of the currency industry. This paper will focus on counterfeit analysis of banknotes. In a second article public knowledge and perception of banknotes will be the subject. The two articles are a summary of the materials that Hans de Heij of De Nederlandsche Bank (DNB) used in his presentation entitled ‘Innovative approaches to the selection of security features’, presented in January 2010 at the Conference on Optical Security and Counterfeit Deterrence in San Francisco. Mr. De Heij is one of the developers of banknote design and security at the Cash Policy Department of DNB. Mr. De Heij managed the introduction of five Dutch banknotes during the period 1981–1997. Currently, he uses his vast practical and scientific experience in creating universal models to improve banknote security and provide for counterfeit deterrence.

A central bank has to keep track of improved and/or new technologies. This is an ongoing process. The last three decades have delivered overwhelming innovations. Since the introduction of ‘digital presses’, ‘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.

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 1 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.

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 and

<table>
<thead>
<tr>
<th>Digital presses</th>
<th>1990</th>
<th>Computer to plate</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home scanners</td>
<td>1990</td>
<td>Counterfeit Deterrence Systems</td>
<td>Geometry</td>
</tr>
<tr>
<td></td>
<td>1992</td>
<td>Silk screen, pearl lustre, NLG 100</td>
<td>Resolution</td>
</tr>
<tr>
<td></td>
<td>1992</td>
<td>Iridescent planchettes, NLG 100</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>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>2012</td>
<td>Hybrid paper: paper-polymer-paper (new Swiss banknotes)</td>
<td>Material</td>
</tr>
</tbody>
</table>
the Bank of Canada 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. Photo-
toshop) and other desk top publishing equipment),

3) professional (specialised equipment, acquisition of
special materials, organised crime),

4) state sponsored or sophisticated high level counter-
feiting (access to banknote production techniques).

The ECB uses a similar classification system (unpro-
fessional, semi-professional, professional and sophisti-
cated).

State sponsored counterfeiting happens only occasionally,
usually to destabilize hostile economies, like the attempt
of the British Government to destabilise the Continental gov-
ernment by counterfeiting US currency during the Revolu-
tionary 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 circula-
tion since 1989. The US Government suspects the involve-
ment of the North Korean government.

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 counterfeiters were suc-
cessfully 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 recognized and some countries
are classified according to these levels, including the euro
area (Table 2). 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.

Increase of counterfeits

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. 650 million. It follows that at around
50,000 counterfeits a year, the counterfeit level in the Nether-
lands may be calculated at around 80 c/mln, above the av-
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).
Australia claims a very low counterfeit rate of just 6 c/mln.
This low figure is fully attributed to the high counterfeit de-
terrence capability of the polymer notes.

Vicious circle: public – counterfeiter – central bank

It seems that counterfeiters are doing more than is nec-
essary for public acceptance! This is in line with the obser-
vation that the quality of counterfeits seems to be declining.
Counterfeits do not have to be very close to the original to
be accepted by the public, is how counterfeiters seem to
reason. Here the vicious circle becomes clear. The public
pays no attention to the notes they receive, since the proba-
bility 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 se-
curity features (2.5 in 2009 versus 1.9 in 2007) and also the
group that cannot recall a single security feature decreased
from 20 % in 2007 to 7 % in 2009. If the public becomes
more alert, the vicious circle may be broken.

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 pay-
ments once or twice a day, retailers receive on average 200
notes a day.

In the Netherlands most retailers use the UV-lamp, far
more than the average for the Euro Area, as is shown in
Table 3. There is a large group of retailers (18 % in NL,
2007) that do not use any authentication device.

<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), Euro in NL, Brazil, Canada, USD (including 1 USD-notes)</td>
</tr>
<tr>
<td>4</td>
<td>100 – 200</td>
<td>Canada</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>

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).
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 of UV lamps. 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

Probably retailers do not wish to spend more than 2 seconds on a security feature.

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 (Figure 1),
- developing tools, e.g. a barcode scanner, that also check a banknote for genuineness,
- developing a marker and/or taggart readers.

The general public would like to have all security features on the front. A concept for 5 features is provided on the (image on the left). To be sure that banknotes are also looked at from the reverse, the (human assisted) retail features may be positioned on the reverse (image on the right).

Approaches to counterfeit deterrence

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.

Self defending

![Figure 2](image)

<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 3

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.

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>

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. Today every central bank makes an effort to familiarize the public with the (public) security features because communication costs are relatively low.
Reactive versus proactive counterfeit models

Reactive response policy to fight counterfeiting

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 (Figure 3). 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.

Counterfeiter focus is on mid denominations

In the past counterfeiters focused on the highest banknote denominations. For instance, 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. 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).

Euro counterfeits threshold

As far as is known, no studies are available on 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 about 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.

Counterfeit models

The use of artificial models to underpin the selection of security features is a trend. Examples are robustness grades (European Central Bank, 2007), secure calc (Federal Reserve System, USA, 2009) and security effectiveness (Bank of Canada, 2009). Most models use algorithms to aggregate criteria to a single value level or a set of values. However, as they are complex and so far have not yielded a proper selection of new features, none of these models has been validated. Only the Canadian security effectiveness method includes the use of real counterfeits.

Comparing these 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.

Since the mid-1970s, DNB developed the following three proactive counterfeit models:

- intrinsic and extrinsic security features (1976),
- black box model (1991),

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.

**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: 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).

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 (Figure 4). The ink of the banknote number could be either magnetic or nonmagnetic.

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. 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. The bar watermark in the euro is quite different from the Dutch AQUS. It takes much more space and doesn’t use the density graduation 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 5.

**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. Un-
der this definition, the AQUIS and the ISARD now became confusingly! – internal features (instead of extrinsic). Next to watermark and intaglio printing a new unmistakable 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 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 resistances 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. 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.

**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 counterfeiters have no access to the banknote security industry and have to use reproduction tools of the graphic industry. The quality of the reproduction will look poor - although sometimes enriched! – beside the original.

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

**DNB Model 3: Simple method**

Based on an idea of Mr. Marco Wind (DNB) a new, simple method was developed and introduced in DNB’s monthly report on the banknote circulation of January 2006. The idea underlying the method is to take the most recent counterfeits and monitor their quality. Instead of monitoring all counterfeits, this ‘simple method’ considers only the 10 types most frequently accepted by retailers and the public.

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

Euro banknotes have 6 public features, so the maximum counterfeit quality score is 12. Euro banknotes have 6 public features, so the maximum counterfeit quality score is 12.

Two interesting conclusions were drawn immediately:

- not one euro counterfeit received 12 points; the maximum score to date is 10 points,
- the average quality score is 6.4 points.

If all scores for one denomination are grouped, the ‘average public score’ may be calculated, as shown in Figure 7.

![Figure 7](image-url)

**Figure 7**

Weighted average score of the quality of counterfeit euro banknotes in NL since 1 January 2006.

The quality of counterfeit euro banknotes in NL is declining. This is especially true of the euro 50 counterfeiters (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 6 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 counterfeiters in general is stable if not slightly declining,
- the euro 50 has the poorest quality (remarkable, since it is the most used denomination in NL).

This is the average quality of the ten most frequently found counterfeits in the Netherlands in the January 2006 – September 2009 period. Note that in the Netherlands, euro 50 counterfeiters 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).
Counterfeit deterrent systems  (CDS)

Counterfeit Deterrent Systems (CDS) are generally aimed at preventing counterfeit use by standardization of the shelf reproduction techniques. In 1990 the Bank for International Settlements (BIS) took the initiative to develop such systems. Such systems are typically part of a ‘law enforcement strategy’ as presented in Figure 2.

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 centres 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, 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. Nowadays, approximately half the counterfeits detected and withdrawn from circulation were produced with fewer than ten distinctly identifiable sources of traditional printing technology.’

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 copying or printing banknotes at home.

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 8.

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 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. Indeed, they may accept a more colourful counterfeit note for the real thing!

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, counterfeiters can optimize their counterfeits by taking on board the response of retailers and the public at large. They anticipate on public behavior by decreasing the quality of the public features and increasing the UV quality needed to pass the notes to the retailer. 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.


To be continued.
Innovative Approaches to the Selection of Banknote Security Features: public knowledge and note design

In this article two stakeholders are discussed: public and retailers. 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 in the Netherlands is 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. The Dutch public have a high confidence in euro banknotes; people trust the banknotes coming out of the ATM and they also trust the banknotes they get in return from the retailers. They do not see the need to verify the authenticity of the euro banknotes.

A retailer receives on average around 200 banknotes a day. 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. The counterfeiter targets the retailer and creates counterfeits with UV features that look similar – or even better – than in a genuine euro banknote.

Magnifying glasses or mirrors are not used at all. Central banks do not support use of a pen tests for starch content; such a test is not reliable. Many Dutch retailers still rely on their UV lamp (almost 40 %) and around 40 % of the retailers are not using any checking devices.

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.

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 1 for optimizing their bogus notes? It seems that counterfeiters have their own opinion and do not follow the presented statistics, although there is some correspondence. The explanation is the ‘heuristic quality’ of a banknote. When a banknote feels limp or looks blurred or pale, or if a banknote is heavily damaged and repaired with cello tape we hesitate to accept such a note. These are all examples of the heuristic quality, the overall and implicit quality standards of the note. The foil stripe is also a fine example. The counterfeiter will always include a foil stripe in a counterfeited euro 20, although in many counterfeits just a commercial available foil stripe is used, which does not match at all with the original one! An authenticity check of the foil stripe is a ‘rule based quality’ of the banknote, just as the use of the other public security features. The conclusion is that a counterfeiter pays more attention to the heuristic quality (overall impression) than to the rule based quality (security features) of the counterfeited banknote.
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 receiver, usually a retailer, will need to assess if she or he is getting the right value, while the payer must determine whether the right denomination is taken from the wallet. Our vision, including our brain processing, is fully occupied with the cash transaction itself. In parallel our tactile senses become active and the touch of the banknotes becomes the most important trigger on counterfeits. This explanation is supported by research done in 2002 by the US Treasury. They reported that 25 % of the cash handlers only check the just received banknote if it feels suspicious (against 6 % of the general public, the consumers). Similar findings are reported by the ECB in 2007: the most common security feature checked is tactility for 70 % of the cashiers.

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 2. 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).

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%).

User requirements

Time seems to be the most important user requirement for a public security feature, but there are more, as listed in both ‘Public feedback for better banknote design’ papers published by DNB in respectively 2006 and 2007.

Below is the scoring of public features best fulfilling the user requirements. (The scoring of public features in the euro 50 note is simply done by a Yes or No):

- nail scratch feature (or ‘ISARD’), 7 out of 7
- security thread, 5 out of 7
- see-through register, 5 out of 7
- colour changing ink (OVI) 3 % Frequent
- glossy gold stripe 2 %

The features that do not match the user requirements are:

- hologram, 1 out of 7
- OVI, 2 out of 7.

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.

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:
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). 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

Total: 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. The OVI is often the least familiar public security feature, known by 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’. Similar findings are reported by the central banks of Spain and Romania.

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

- motion,
- colour switch,
- gloss.

The question is whether it will be successful. Motion is registered more quickly and in a different part of the brain than colour differences. People will focus on motion rather than colour change and/or gloss. 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 counterfeiters’ point of view. Once the good colour flop imitation is found, it may be used for many banknotes, both within the series and internationally.

SUPPLIERS TOO FAR REMOVED FROM CUSTOMERS

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 Program of Requirements the central bank may inform the private sector.

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’. Also user requirements for public features are defined in this paper, like discrete and univocal. Further more new retail features are needed as follow up for the magnifying glass and the UV lamp.

Often developers of security features expect that public and retailers will recognize 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 1, this is not noticed by more than 80% of people.

Discrimination of counterfeiters by public and retailers (2005)

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

- Discrimination of counterfeiters by public and retailers (2005),
- Marketing mix of public security features (2007),

Figure 1

Change blindness for euro banknotes. Which is the correct note?

DNB Researches

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 recognizing 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).

Recognizing 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. The findings were also reported at the Banknote 2006 conference.

**Correlation**

Analyzing 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.

**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 2).

The UV fluorescence of the counterfeited notes is often stronger than that of the original, making the counterfeit look ‘more real’ and misleading to the retailer. These brighter reflections of the inks and fibres under an UV lamp are another example of the importance of the heuristic quality of a banknote. In this case the counterfeiter exaggerates the original features. For the girl behind the counter: this note looks very bright, it must be a real one! Or it could be a washed genuine banknotes. Some of the retailers might know that washed genuine banknotes might light up under UV light because of the bleaching agents in some detergents.

The increase of UV imitations has also been recognized 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. 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.’

**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.

**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. It was the first ranking based on public preference.

**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 3.

<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>
</tbody>
</table>

Table 3
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.'

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

Marketing mix of public security features (2007)

Analyzing the considered security features by a marketing approach is another 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 are enough. 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 4 a total of six PSF, three active and three sleeping, is divided over the front and the reverse. However, other different concepts are possible. Look could be subdivided in look-at and look-through.

Table 4

<table>
<thead>
<tr>
<th>Action</th>
<th>Front</th>
<th>Reverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feel</td>
<td>+</td>
<td>0</td>
</tr>
<tr>
<td>Look</td>
<td>+</td>
<td>0</td>
</tr>
<tr>
<td>Tilt</td>
<td>+</td>
<td>0</td>
</tr>
</tbody>
</table>

+ – active public security feature, to be communicated
0 – sleeping public security feature

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. Existing features enjoying high public awareness should be cherished like gold, since it is a proven fact that the public is very hard to familiarize 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.

Policy ECB

At the Currency Conference 2007, the ECB presented the desired number of security features for the next series of euro banknotes (Table 5), based on work done in 2004–2005.

Table 5

<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>

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

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. From a marketing point of view there is a need for a follow up of the magnifying glass. Features based on filter seem to fulfill the user requirements and therefore such ‘filter’ features could be selected, like for example a polarization filter. The IR viewer is not much used, but does not yet disappear from the shops. Instead auto detection, often (partially) based on IR properties (level 2b) is growing in popularity.
PERCEPTION APPROACH

The last chapter of this extensive paper by Hans de Heij explores a novel research area, an area very much in movement: brain processing of information (perception). People do not notice minor changes in banknotes, contrary to what is assumed by the security industry. As said before, 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?

Communication of public security features (2007, 2009)

Every day people are working on new banknote designs. What can they already do today?

One of the recommendations 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’. Eye tracking paths are dependent on the instruction given, e.g. ‘check three public security features’ or follow the letters ‘E-U-R-O-P-A’. An eye tracking path should work as a ‘follow me’ instruction.

*Figure 3* is an illustration of the eye tracking path. 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 4* are two examples of a conceptual design using the letters of the word Europa as a lead to find the public security features.

CONCLUSIONS

General

Below you may find the combined conclusions of both articles in Banknotes of the World #8 and #9, using the publication of Mr. De Heij’s ‘Innovative Approaches to the Selection of Banknote Security Features’.

New features are usually a dedicated barrier against the counterfeiters 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.

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.

The focus of counterfeit reports is often on statistical data and counterfeiters seized, illustrated with anecdotic stories, usually about the organization of the criminals. Studies on counterfeiters 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.

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.

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.

Public interest in public security features is essential to get public attention. Attention is driven by emotions. So create more emotional content. Introduce for example living creatures like humans, animals or flora to the euro banknotes. Develop a slogan (e.g. ‘E-U-R-O-P-A’ or ‘follow the fish’), or keep the one that is successful (e.g. Feel Look Tilt). Give the new note a name. All within an attractive design.

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

**Feature selection for the public**

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).

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

Analyse the remaining features over the human operations feel, look-at, look-through and tilt. Search for new features in the required human action (e.g. search for feel and look-at features).

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

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

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

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

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

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

**Banknote series design**

Central banks should focus more on the overall quality (heuristic quality) of the banknote, next to their attention for the security features (rule based quality).

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

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.

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

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

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

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

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

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.

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.

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).

**Retailer**

A retail feature should fulfill all user requirements, like a total authentication time < 2 s.

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 polarization filter seem to full fill the user requirements of the retailers.

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.

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

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

All human detectable retail features on one side (reverse).
Counterfeit Deterrence Systems (CDS)

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

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.

Forensic features

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

Test on counterfeit resistance

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

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

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

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.

Reporting on counterfeits in circulation

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

Information about counterfeits in circulation to the public is fragmented and unclear, leaving the public with a passive attitude and negative feeling. Public perception of counterfeits in circulation is far above the reality; people overestimate the reality by 200 % (NL, 2008). 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 counterfeit,
- public confidence,
- the difference between genuine and most counterfeited notes.


This and other documents can be found on the website of DNB: http://www.dnb.nl/en/z-onderzoek/researchers/personal-pages/auto184528.jsp or Google: Hans de Heij DNB.