Public Education by Central Banks on the Internet[**]

Rudolf L. van Renesse, VanRenesse Consulting,
Willem de Zwijgerlaan 5, 2582 ED The Hague, The Netherlands[*]

ABSTRACT

The Internet is the most powerful information providing medium today and it has great potential in conveying pictorial information in the form of still images, video clips and applets. Obviously, central banks can make use of the Internet to efficiently provide information for the public on the anti-counterfeiting features of their currency.
An investigation was carried out of the information provided by 133 Central Banks on the public security features of their currency. Many central banks appear to provide no information at all, many only provide written information and many indeed provide illustrations. An overview is presented of the various errors that central banks make when presenting illustrated information and illustrated examples are given. It appears that even illustrated information often lacks the most elementary requirements: obviousness, clarity and adequate visual representation of the relevant optical effects. As a result, the information made available on the internet by many banknote issuing authorities remains largely ineffective and – on occasion – even assumes silly proportions.

Keywords: banknote security; public education; Internet; human factors, Counterfeit Deterrence System

1 INTRODUCTION

From a human factors point of view, the most efficient way to educate the public on banknote authentication is to have the security features speak for themselves without the need for explicit lengthy explanations and illustrations. First-line inspection of security features involves the use of the human senses only, without the application of tools like magnifiers, ultraviolet sources, retro viewers, bar code readers, etc. Public security features depend on first-line inspection. It is in the interest of the issuing authorities as well as the public that a clear and truthful mental image of the available public security features and their handling can be acquired. If this image cannot be adequately created by the information radiated by the banknotes as such, the issuing authorities can revert to distributing brochures, broadcasting TV-spots and even providing the necessary information on the Internet. Meanwhile, many central banks have started providing information on the Internet of the security features of their currency. This information can be purely in writing and it can be additionally illustrated. The proverb says "A picture is worth a thousand words", and written information therefore is not as educational and efficient as illustrated information can be. This investigation shows that many central banks provide illustrated information on security features that can hardly, if at all, be expected to significantly attribute to the clear understanding of the public. Additionally, the accessibility of the information often appears to be inadequate.

2 HUMAN FACTORS

Human factors play a paramount role in conveying information and this also counts for information regarding public security features on banknotes. The subject of human factors in de context of document security is discussed in several publications [1-4] and here it suffices to note a few basic aspects.
Reference is made to the action cycle, associated with the general theory of industrial product design, and illustrated in Figure 1. This action cycle is derived of Donald Norman's work [5] and it illustrates the interaction between the examiner (subject) and the security device (object). The action cycle comprises two stages: (1) the development and execution of a strategy (input), and (2) the observation and evaluation of the result (output). In order to properly operate the security device, the user must gain adequate knowledge (information) about the way it functions or else make either errors in

[**] Conference on Optical Security and Counterfeit Deterrence Techniques VI, 17-19 January 2006, San Jose, CA. USA, SPIE Vol. 6075.
[*] email: ruud_van_renesse@zonnet.nl, phone +31 70 3540333, mobile +31 (0)6 23415493.

operating it or in judgment. Insufficient or inadequate information may result in cycling through the action cycle several times, possibly without conclusive results or with incorrect results. In case of complete lack of knowledge, the security function will not be operated at all.

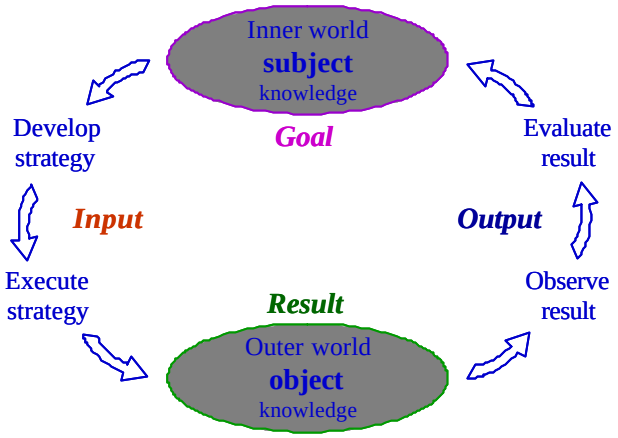


Figure 1 – The action cycle: interaction between subject and object.

Apparently, the required knowledge is twofold:

1. knowledge about the required action (input), and
2. knowledge about the expected result of that action (output).

Norman rightfully argues that industrial products must themselves provide this knowledge (not by a manual or a brochure!) in order to adequately meet human factors design and Norman calls this "knowledge in the world". Contrary, requiring the public to remember this information (*à priori* "knowledge in the head") will rarely be successful because people are not generally inclined to remember more or less trivial information, unless it is of paramount importance for them in daily life. Issuers of banknotes often attempt to educate the user about the existing security measures and the way to verify or falsify them. To this end brochures and posters are issued and even TV spots are broadcasted and currently the Internet is chosen as a medium to convey this knowledge. Note that these media do not bring information in the world, they aim at bringing it in the user's head.

Nevertheless, the Internet is a very powerful source of information, and it allows the display of visual information in a very efficient manner, not only by still images, but also by video clips, virtual tours and applets (programs that are automatically downloaded and run on the user's computer). Therefore, once central banks use the Internet as a medium to educate the public, optimal use of its potential seems indicated. With reference to Figure 1, this implies that the strategy to be followed by the inspector, and the results to be observed and evaluated must be presented in a clear and comprehensible manner. In particular because the inspection of security features often involves more or less complex handling, the use of animations and video clips can be instructive. Obviously, the handling of the website itself should also meet human factors requirements, in particular where it regards the accessibility of the information provided; accessibility related problems are discussed in Section 3.1.

3 CENTRAL BANK INTERNET EDUCATION

A list of 159 central bank internet sites can be found on the website of the Bank for International Settlements: http://www.bis.org/cbanks.htm. The European Union covers thirteen *euro states*, the BCEAO (Banque Centrale des Etats de l'Afrique de l'Ouest) covers eight *franc CFA*[1] *states*, and the BEAC (Banque des Etats de l'Afrique Centrale) covers six *franc CFA*[2] *states*. The list also includes two USA banking institutions: The Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System (Washington). This leaves a total of 133 websites, involving different currencies, available for an investigation of the information offered by the issuing authorities.

The general results of the investigation are summarized in Figure 2. Because internet information tends to be somewhat volatile, it must be borne in mind that these results are valid per November 2005.

[1] "Franc de la Communauté Financière Africaine" for members of UEMOA (l'Union Economique et Monétaire Ouest Africaine).
[2] "Franc de la Coopération Financière en Afrique Centrale" for members of CEMAC (Communauté Economique et Monétaire de l'Afrique Centrale).

It is striking that the majority (90) of central banks (67.7%) does not provide any illustrated internet information on the authentication features of their currency. On the other hand 89 central banks (66.9%) do indeed provide written or illustrated information. In Section 3.1 - 3.4 the results of this investigation are discussed in more detail.

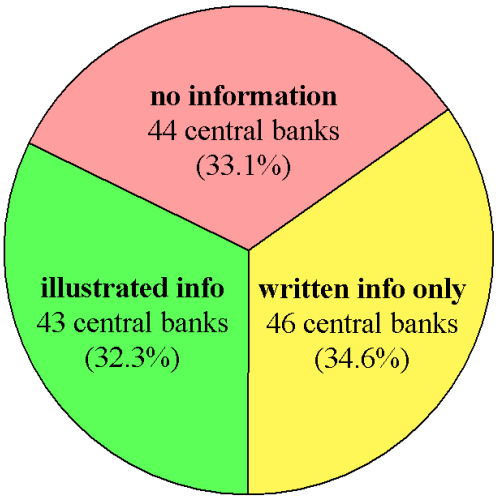


Figure 2 – Overview of information on banknote security features provided by 133 central banks.

3.1 Accessibility of central bank websites and security information

For a visitor of a central bank home page it appears sometimes obscure where to look for information on the authentication features of banknotes[3] (if available at all), and the visitor must then revert to a blind search. In other cases information is only available on the website in the local language, which is not always understandable for foreigners: 19 central banks provide no information on banknote security in English. In some cases the information on websites is difficult to find because it is introduced in odd places or only found after consulting the site map (Bank Negara Malaysia). Examples of websites with such "hidden information" on security features are those of Bank Al-Maghrib, which gives banknote images under "banknotes and coins", and written security information under "printing plant", and of the Bank of Papua New Guinea which gives banknote images under "currency/notes" and written security information under "currency history", both without any cross references between relevant pages. The Central Bank of Kuwait unexpectedly provides illustrated information under "CBK Gallery/Issues" and the Saudi Arabian Monetary Agency under "Currency Museum". On various occasions during this investigation the conclusion was initially drawn that a central bank did not provide information on security features, until an extended investigation was carried out on pages that were initially considered unlikely to provide such information.

Another accessibility problem encountered is that the information is located in too deep a level of the site. Furthermore, finding and browsing through the relevant information sometimes requires an inordinate amount of mouse clicks and waiting for illustrations to load, which inconvenience could be cured by designing these sites in a more user friendly manner.

Access to information sometimes is also made difficult because the relevant web pages load extremely slowly[4]. In other cases security information is only made available as downloadable pdf files, in which the informational power of the Internet is partly lost.

In several cases the relevant page "e.g. banknotes and coins" consistently cannot be opened (Barbados, Samoa), or the page seems to be under construction forever (Guatemala) and the request "please come back soon" after a while makes an odd impression. In one noteworthy case the complete central bank website is protected by a password (the South Pacific island nation of Vanuatu).

These experiences show that designing and maintaining websites knows many pitfalls, which appear not always avoided by even professional website designers for central banks. In all these cases, even if the information provided were of high quality, it will not likely reach many members of the public. Efforts invested in setting up a website will remain

[3] For instance: Banco de la Republica Colombia, Reserve Bank of India, Central Bank of Libya, State Bank of Pakistan, Monetary Authority of Singapore, Bank of Tanzania, Central Bank of Yemen, Reserve Bank of Zimbabwe.

[4] For instance the websites of the Bank of Botswana, the National Bank of the Republic of Macedonia and the Bank Negara Malaysia.

largely fruitless if the accessibility of the information provided, however instructive this information may be, does not meet human factors requirements.

3.2 No information on security features

In 33.1% of the cases (44 central banks) no information on the security features is provided at all (see Figure 2). In quite a few cases (16 central banks), images of the currency in circulation are shown indeed, but security information remains absent. Images of banknotes vary widely in quality between central banks. For instance the Bank Al-Maghrib (Morocco) provides very low quality banknote images having a size of only 120 x 59 pixels (Figure 3). The Bank of Sierra Leone, possibly for even greater security, illustrates low resolution images of banknotes photographed under an angle (Figure 4). Central Banks like those of Nicaragua and the United Arab Emirates present reasonably good quality images of their currency (note width 452 and 480 pixels respectively). Otherwise, the images of the latter bank are denied copying via right mouse clicking, a futile security measure because no defense exists against simply copying such images from the screen with widely available and cheap software. Apparently, central banks desire to prevent abuse of their images by counterfeiters, a subject that is further discussed in Section 4.3 of this paper.

Figure 3 – Internet illustration of Moroccan 10 Dirham note (note width 120 pixels).

Figure 4 – Internet illustration of Sierra Leone 500 Leones note (note width 296 pixels).

3.3 Only written information on security features

In 47 cases (35.3%) central banks only give written Internet information on the security features of their currency (see Figure 2). Images of the currency in circulation are made available in almost all cases –sometimes with annoyingly low resolution– but information on security features remains limited to written descriptions. In 11 cases banknote images are provided with arrows pointing at the location of the security features, like is often done in brochures. An example is given in Figure 5. It goes without saying that this is not an optimal use of the illustrative power of the Internet. Because this approach does not really illustrate the security features as such; it remains essentially written information.

Figure 5 – Internet illustration of Bahrain 1 Dinar note (note width 257 pixels) with arrows pointing at the locations of security features as well as non-security design elements. The image is apparently copied from a brochure.

The Banco Central de Bolivia presents images of the currency in circulation, containing various rectangular areas in a deviating color, marked with an obvious, moving striped circumference (see Figure 6). When the cursor is moved to these areas, brief descriptions of the security features appear in a caption below the image. Although this type of illustration is interactive, this approach with "interactive arrows" is not essentially different from the regular pointing arrow method, and thus the information on the security features cannot be considered as illustrated information.

Figure 6 – Central Bank of Bolivia: 10 Bolivianos note with "interactive arrows" indicating the locations of security features.

3.4 Illustrated information of security features

In 43 cases (32.3%; see Figure 2) central bank websites provide separate images of security features of their currencies'. Again, the quality of the illustrations provided differs greatly between central banks and appears generally inferior. In many cases the illustrations do not contribute at all to a better understanding because they are essentially void of relevant information. Good examples are shown in Figure 7 with details of a South Korean 10,000 Won note windowed thread and optically variable ink (OVI): the windowed thread does not show at all in the illustration, while the OVI is only shown in one single (vague) color. A frequently occurring image quality problem is that only minute images are published, such as found on the website of the Central Bank of the Republic of Argentina (see Figure 8).

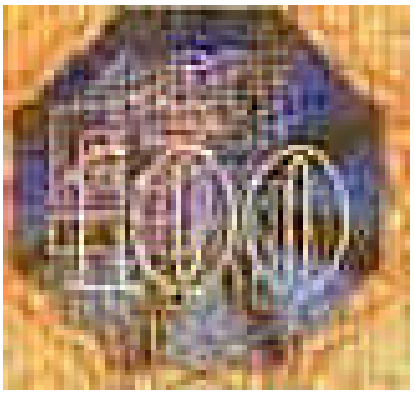
Figure 7 – Bank of Korea 10,000 Won note: Internet illustration of 99 x 101 pixel details of windowed thread (left) and optically variable ink (right).

Figure 8 – Central Bank of the Republic of Argentina 20 Pesos note (width 285 pixels): Internet illustrations of 65 x 65 pixel details of latent image (top right) and security thread (bottom right). The former detail is incomprehensible and the latter is illegible.

The Bank of the Netherlands Antilles on their website also illustrates security features. The images of front and back of a 100 guilder note (note width 221 pixels) contain arrows pointing at eight pictures as small as 48 x 48 pixels, without giving any additional explanation (Figure 9). The image looks like being copied from a brochure and it is left to the visitor of the site to deduce what the pictures mean.

Figure 9 – Bank of the Netherlands Antilles 100 guilder note: 48 x 48 pixel Internet illustrations of security features without additional explanation.

The Singapore $10 note serves as the Internet example for the security features incorporated in the currency of the Monetary Authority of Singapore. Two of the minuscule images provided of the various security features are shown in Figure 10. These images of the Kinegram (OVD Kinegram Corporation, Switzerland) and the micro printing, exemplify the ineptness of the information presented. Apart from the fact that the images are void of useful information, it is interesting to note that the Kinegram image is accompanied with a 91 word intricate description (Figure 10). It will expectedly remain obscure to the public what is meant with the larger part of this description. One may wonder what happened to the proverbial "A picture is worth a thousand words"? This is most unfortunate, considering the closing statement: "These features are unique properties to the Kinegram and cannot be replicated.", which statement emphasizes the importance of the optical effects referred to. The question remains unanswered what exactly cannot be replicated.



91 word Kinegram description on the website:

"The Kinegram appears as an octagonal foil on the front of the notes. It contains an image of the denomination numeral which shifts as the note is tilted. On varying the viewing angle, one can also see the logo of BCCS transforming into the letters "BCCS". The background of the Kinegram is composed of shapes representing electron orbitals which change from bright to dark as the notes are rotated. This background shimmers in an array of colors when rotated. These features are unique properties to the Kinegram and cannot be replicated."

Figure 10 – Internet illustrations of details of the Singapore $10 note: kinegram top left (80 x 77 pixels), its description in writing top right and the (150 x 19 pixels) image provided of micro printing (bottom).

Of course, (animated) illustrations of sufficient resolution can simply and much more adequately clarify the various optical effects referred to in this elaborate 91 word description. It is noteworthy in particular that this Kinegram displays achromatic images of "electron orbitals"[5], which are composed of low frequency (160 lines per mm) left and right blazed gratings. As a result the plus and minus first order diffractive images are different, which appears when the hologram is illuminated from the left and from the right respectively, as shown in Figure 11. Such achromatic grating structures are described by Staub [6]. Because the inspection of this effect is not particularly difficult and the counterfeit resistance attached to the structure is high, the website should at least have offered adequate illustrations of this effect.

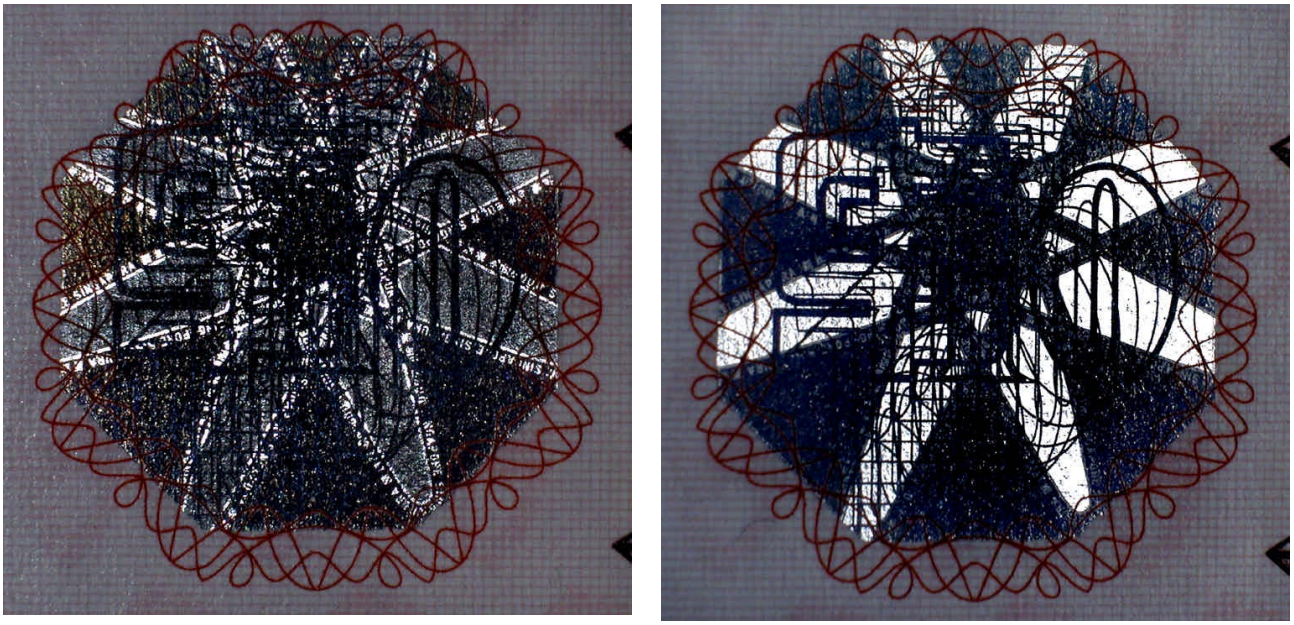


Figure 11 – Singapore $10 note kinegram with achromatic images illuminated from the left and from the right.

[5] It may be doubted that many members of the public will understand what is meant by "electron orbitals".

Only few central banks[6] make use of animations and video clips to clarify the effects to be observed, although this opportunity is one of the significant benefits of the Internet. However, it is striking that even those central banks that seem to recognize these benefits, sometimes present animations of inadequate resolution and lack of clarity of the optical effects expected to be observed. The flash animations of the Kinegram stripe and the OVI on the website of the European Central Bank are examples. The most prominent characteristic of the Kinegram stripe is that –on tilting about a horizontal axis– it alternately shows the value numeral and the euro symbol in several places. Figure 12 shows four consecutive frames of a flash animation, which obviously fails to adequately demonstrate this effect. Two European Union central banks (National Bank of Belgium and the Bank of Spain) present 2-frame animations (150 x 113 pixels) that are devoid of any relevant information, as shown in Figure 13.

The ECB video clips of the Alphagram patches (Hologram Industries, France) on the higher euro denominations, although having very little resolution (the patches as such measure 72 x 72 pixels), perform better. For further instruction the ECB gives a comparison between a genuine and a counterfeit Alphagram patch on a euro 50 note. As Figure 14 shows, these still images are largely useless as educational material and the difference will likely remain obscure to the public. A good quality video clip of the features while tilting would have been more instructive indeed.

The OVI on the higher euro denominations shifts from magenta over gold to green in glossy reflection. OVI is designed to be observed in glossy reflection, but the ECB only presents flash animations of this phenomenon showing the feature to shift from bright magenta to dark brown (Figure 15). This misrepresentation is due to the fact that the feature is mistakenly tilted from glossy reflection to diffuse reflection. Reference is made to the excellent website of the Central Bank of Russia, which presents an adequate resolution mpeg video (384 x 288 pixels) of the OVI detail on the 1000 ruble note, which video correctly displays the magenta to green shift [7]. Otherwise, the site of the ECB is exemplary with respect to accessibility.

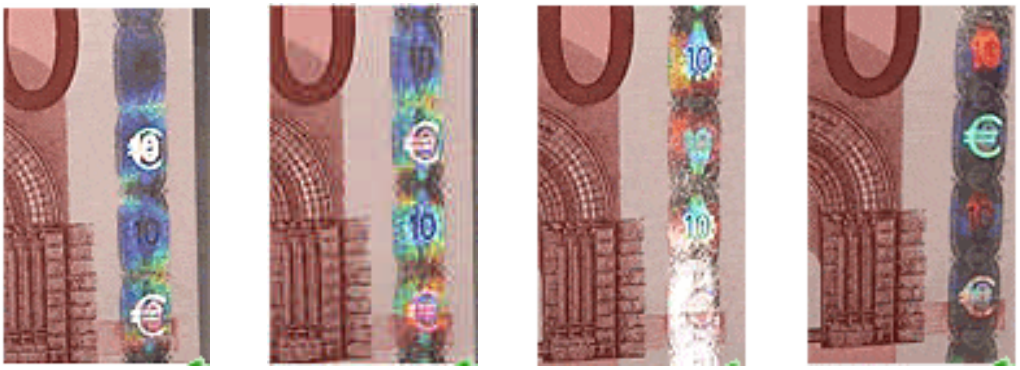


Figure 12 – European Central Bank: 4 frames (82 x 141 pixels) of a tilted Kinegram strip on a euro 10 note.

Figure 13 – Two-frame animation (150 x 113 pixels) of Kinegram stripes presented by several European Union Central Banks.

[6] Chile, Denmark, European Union, Nigeria, Russia, Serbia, United Kingdom, United States.

Figure 14 – European Central Bank: comparison between a genuine and a counterfeit Alphagram (72 x 72 pixels) on euro 50 notes.

Figure 15 – European Central Bank: 4 movie frames (107 x 152 pixels) of a tilted OVI feature on a euro 100 note: the OVI print in the movie shifts from bright magenta to dark brown, while the actual color shift is from magenta over gold to green, when correctly displayed.

Other examples of inferior illustrations of security features are found on the website of the National Bank of Serbia. Images of security features (as small as 48 x 48 pixels) are presented –some of which are animated– to which pop up descriptions are attached of only one or a few words; no further description is provided on the website (see Figure 16).

Figure 16 – Illustration of security features by the National Bank of Serbia of a 500 dinar note: from left to right 48 x 48 pixel details with pop-up descriptions: “see-through picture” (animated), “security fibers”, “micro lettering”, “micro lettering”, “serial number”, “security thread”, “watermark”, “optically variable feature” (animated), and “raised intaglio print” (animated).

Of the 43 central banks that provide images of security features, 25 central banks (58%) can be considered to provide illustrated information on security features that ranges from inferior to below average, while 18 banks (42%) provide illustrated information quality that ranges from average to excellent; the latter group comprises only a disappointing 14% of all 133 central banks investigated.

Central Banks that provide excellent still photographs and animated information on the security features of their currencies are Chile (only in Spanish), Denmark, Russia, the United Kingdom, and the United States. Central banks that offer good to excellent still images of their security features are those of Belarus, Colombia (only in Spanish), Czech Republic, Peru, and Slovakia. However, the accessibility of the information on these websites is not always optimal.

4 DISCUSSION

The problems encountered with many websites of central banks are twofold: poor accessibility (Section 3.1) and poor quality of the information (Sections 3.2 - 3.4). Only very few of the central banks investigated appear to adequately deal with both these problems. Although finding the causes of these shortcomings is largely a matter of conjecture, the following discussion tries to identify a few. It goes without saying that many other websites also suffer suchlike shortcomings, but considering the resources of central banks one would expect more advanced results. After all, central banks tend to invest significantly in issuing banknotes with high counterfeit resistance security features and stimulating optimal use of these security features by adequately educating the public would seem a logical follow-up.

4.1 Human factors of websites

The ease of handling a website is also a matter of human factors design (Section 2). Website design requires professional web designers that have acquired adequate insight in the structure of the information that a central bank desires to make available, and the priorities involved. As becomes obvious in Section 3.1, in many cases this requirement is not met. Can it be concluded that public education is not generally a priority of central banks? An astonishing large percentage (33%) of central banks investigated publish no Internet information on the security features of their currency at all. However, the remaining 67% of these central banks do provide either written or illustrated information, which indicates that the majority of central banks indeed desires to educate the public, although this may not be their first priority. The often poor accessibility of the information on security features must probably be attributed to unawareness of the human factors involved in designing a website. This is suggestive of both the lack of professional skill of the web designers involved and the limited interest of central banks in the functionality of their websites.

4.2 Comprehensibility of information

The clarity and comprehensibility of the pictorial (and written) information are a separate issue. On numerous occasions images on central bank websites are made available that simply do not convey adequate information and a few of the many examples are given in Section 3.4. In particular where the representation of the optical effects to be observed is poor, it can be suspected that the reasons for these inadequate results are a lack of the photographer's insight in the intended function of the security feature, which may originate in a lack of clear instructions, or a lack of professional photographic skill. Images of OVI that do not display the intended shift of colors (Figure 7, Figure 15) or diffractive elements that do not display the intended image animations (Figure 12, Figure 13) are probable examples. In other cases the images are of poor quality but do not seem to be a sign of lack of insight or poor photographic skills, but rather seem the result of limited awareness of, or limited concern for human factors requirements; probable examples of which are shown in Figure 8 through Figure 10.

4.3 The Counterfeit Deterrence System

The often poor image resolution and the abundant occurrence of the conspicuous overprinting "specimen" or "sample" demonstrate the desire of the issuing authorities to not make digital images useful for would-be counterfeiters. However, these measures seem to ignore the fact that high resolution, clear and undistorted physical banknote images are abundantly available, issued by the central banks themselves: currency. Because acquiring high resolution digital scans of these physical images currently is a trivial matter, would-be counterfeiters cannot be expected to be the least interested in the use of banknote images available on the Internet. Therefore, such security measures appear to be futile.

For this reason the Central Bank Counterfeit Deterrence Group (CBCDG), a working group of 27 central banks and note printing authorities, erected in 1993, has developed the *Counterfeit Deterrence System* (CDS) [8 - 10]. The CDS is based on covert digital watermarking: the embedding of imperceptible identifying codes into images and other media content. Such codes can be detected by dedicated software, which subsequently prevents a suspicious image from being processed. The CDS detection software is provided to manufacturers and since January 2004, several graphics software and hardware manufacturers (including Adobe Photoshop, JASC Paint Shop Pro, HP Printers and Canon scanners) have voluntarily integrated the CDS in their products. The potential of digital watermarking in the battle against counterfeiting is obvious: rather than adding features that are difficult to faithfully reproduce, hidden codes are embedded in the printing of banknotes, allowing image processing software to flag an attempt to capture or process the image and then abort it. The CDS does not track the use of a personal computer or digital imaging equipment, but refers the user to the website www.rulesforuse.org, which has links to the guidelines for the reproduction of banknotes of many banknote issuing authorities. According to such guidelines, the reproduction of currency is legal under certain conditions. Consequently, it has annoyed users that the CDS unconditionally cancels the processing of CDS encoded currencies, even for legal purposes. However, central banks, in order to meet the need of the graphic professional, will provide

images for reproduction that meet their guidelines. The ECB, for instance, makes 72 dpi color images –marked "specimen"– of fronts and backs of all EU currency freely available for downloading. These images are significantly unsharpened. For users who have a legitimate interest in reproducing euro banknote images, the ECB has produced CDS-disabled high resolution digital images (300 dpi; TIFF format and marked "Specimen"), which do not trigger the CDS [11]. To obtain such images, the user must:

- require the banknote images for professional purposes
- have a personal computer or digital imaging software which includes the CDS
- sign a Confidentiality Declaration.

Otherwise, it can be maintained that high resolution images and video clips of small parts of banknotes, illustrating security features, constitute no security threat whatsoever because these cannot reasonably be combined to form a complete high resolution image of a banknote. Therefore, the omission of high resolution educational illustrations of security features seems to serve no purpose.
Finally, taking into consideration that the CDS can also be added to digital images on the Internet, there appears not to exist a logical reason why central banks should not provide unrestricted educational imagery with adequate resolution.

Meanwhile, the ECB has requested that the Commission for European Communities initiate legislation making it mandatory to incorporate CDS technology into products produced, imported or distributed in the European Union (EU), capable of handling digital images. The ECB's request is based on the insight that "given the size of this market segment, concluding separate agreements with all of the undertakings concerned" is not a workable option [12].

REFERENCES

1. van Renesse, R.L., "Security design of valuable documents and products", *Proc. Conf. on Optical Security and Counterfeit Deterrence Techniques*, SPIE vol. 2659, pp. 10 – 20, San Jose, CA, 27 Jan - 2 February 1996.
2. van Renesse, R.L., "Human factors of first-line security", *Proc. Conf. on Optical Security and Counterfeit Deterrence Techniques II*, SPIE vol. 3314, pp. 97-108, San José, CA, 29 - 30 January 1998.
3. van Renesse, R.L., "The Human Factor of Security", *Proc. Int. Conf. on Document Counterfeiting Protection*, Reconnaissance International/PIRA, San Francisco, CA, 28-29 January, 1999.
4. van Renesse, R.L., "Human factors of card security", *Chip Card: Trump Card? - consequences for investigation and prosecution*, ed. F. Knopjes and P .J. Lakeman, pp. 37-58, National Criminal Intelligence Division, Netherlands, 2nd edition 1999.
5. Norman, Donald A., *The Psychology of Everyday Things*, Basic Books, New York, 1988.
6. Staub, R. and W.R. Tompkin, "Non-standard Diffraction Structures for OVDs", *Proc. Conf. on Optical Security and Counterfeit Deterrence Techniques II*, SPIE vol. 3314, pp. 194 – 202, San Jose, CA, 28 - 30 January 1998.
7. Central Bank of the Russian Federation, Banknotes and Coins, Banknotes, Bank of Russia Banknotes of 1997 Issue (modified of 2004), 1000-ruble banknote (modified of 2004), click color shifting ink patch, select video, http://www.cbr.ru/eng/bank-notes_coins/bank-notes/main.asp?file=priznak_2004_eng/Opisan_1000R_eng.htm, last visited 7 December 2005.
8. Bank for International Settlements, "Central Banks and Technology Industry Join to Combat Banknote Counterfeiting", http://www.bis.org/press/p040309.htm, 9 March 2004, last visited 26 November 2005.
9. Central Bank Counterfeit Deterrence Group, "Banknotes & Counterfeit Deterrence, http://www.rulesforuse.org/pub/index.php?currency=cad&lang=en, last visited 24 November 2006.
10. van Renesse, R.L., "The Secrets that Lie Within", *Currency News*, October 2004, Vol. 2, No. 10, pp.4-5.
11. Website of the ECB, "High-resolution Banknote Images for Professional Users", http://www.ecb.int/bc/html/hires.en.html, last visited 6 December 2005.
12. European Central Bank, "Consultation Announcement Regarding Possible Legislation on the Incorporation of Counterfeit Deterrence Technology in Products Capable of Handling Digital Images", Official Journal of the European Union, 24 October 2003, C 255/13, http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/c_255/c_25520031024en00080008.pdf, last visited 27 November 2005.