The Human Factor of Security

Rudolf L. van Renesse

International Conference on
Document Counterfeiting Protection
Argent Hotel, San Francisco, California, USA
January 28-29, 1999

organised by
Reconnaissance International
&
PIRA

VanRenesse Consulting
Willem de Zwijgerlaan 5
2582 ED The Hague
The Netherlands

Phone   +31 70 3540 333
Email   ruud_van_renesse@zonnet.nl

The Human Factor of Security

Rudolf L. van Renesse*

International Conference on Document Counterfeiting Protection
January 28-29, 1999
San Francisco, California, USA

Abstract
Human inspection of security features without the use of tools, so called first line inspection, deals with two fundamental security design aspects:
1. The ergonomics of the inspection.
2. The integrity of the inspection's result.
Both aspects of security design are discussed in this article, and the watermark, the windowed thread, metallic foils and iridescent OVDs are presented as examples.

1 Ergonomics

The ergonomics of inspection involve the interaction between subject (the inspector) and object (the feature to be inspected). As is set forth in earlier publications [1-3] this process involves the *action cycle* which is associated with the general theory of industrial product design. This action cycle, derived of the lucid work of the industrial designer Donald Norman [4] is depicted in figure 1.

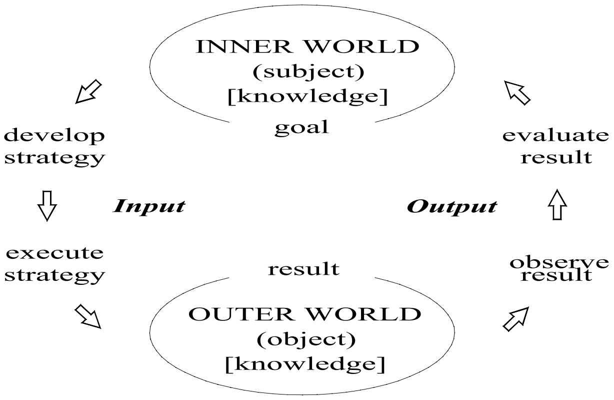

Figure 1 - The action cycle

In order to adequately operate an object, such as a security device, the examiner must develop and execute a strategy. Subsequently, the result of this action must be evaluated on the basis of what is observed and a conclusion must be drawn with respect to the status of the device: genuine or counterfeit, in other words true or false. In order to properly operate the security device, the user must have adequate knowledge about its various functions or else make either errors in operating it or make errors in judgement. Insufficient information tends to result in cycling through the action cycle several times, possibly without any conclusive result. In the worst case of ignorance, the particular security function will not be operated at all. Apparently, the required knowledge is essentially twofold.
(1) knowledge about the required action (input), and
(2) knowledge about the expected result of that action (output).

This twofold information may be either in the world, that is, provided by the product itself (not by a manual or a brochure!), or it may be in the user's head for future recollection. The structure of the action cycle raises five pertinent questions about the functionality of security devices from a viewpoint of human factors design (ergonomics):

* VanRenesse Consulting, Willem de Zwijgerlaan 5, 2582 ED The Hague, The Netherlands
Telephone +31 70 3540 333, ruud_van_renesse@zonnet.nl

How easily can the examiner:

1. Determine and understand the function of the device?

⇩ ⇧

2. Tell what actions are required? 5. Compare the observed results with the expected results and draw correct conclusions?

⇩ ⇧

3. Execute the actions? ⇨ 4. Observe the results?

Examples of assessing security features with the use of these five questions are presented in [1]. For the sake of simplicity, these five basic questions can be reduced to three fundamental questions:

1. Is the function of the device obvious? Or else, is it standardised? (People tend to avoid handling obscure or unknown devices)
2. Is execution of the examination easy? Does it evoke embarrassment? (People tend to avoid effort as well as embarrassment)
3. Is the evaluation based on a yes/no decision? (People prefer simple yes/no decisions and tend to avoid sophisticated judgements)

2 Integrity of the inspection's result

Apart from the ergonomics of security features, their state of being confirmable as either false or genuine is of importance [5]. The output of the interaction cycle in figure 1, the evaluation of the status of the device - genuine or false - may be based on two opposite types of knowledge about the security feature. Security features make the document either *falsifiable*, that is capable of being proved false, or *verifiable*, that is capable of being proved genuine.

2.1 Falsifiers

Intricate production processes do not guarantee the integrity of a document, if the applied security features can be imitated successfully and with relative ease, without the need for the original high-grade production methods. Consequently, the (seeming) presence of such falsifiable features does not confirm genuineness. Only, their absence or their striking deviation from normal prove falseness. Such features are referred to as *falsifiers*, and confidence in the genuineness of the product is only established after inspection of a sufficient number of - technologically different - falsifiers. In daily practice, this requires the scrutiny of at least two but generally four or even more falsifiers. The primary question "*is the document genuine?*" is not answered by a single falsifier.

This approach is based on the anticipated inability of the criminal to master a significant number of sufficiently different technologies. However justified this approach may be, first line inspection involving the search for absence of deviations, is - in principle - an inefficacious procedure. Of course, the combination of technologically dissimilar security elements is highly desirable to deter fraud and to sustain dependable scrutiny in case of suspicion. However, if mere falsifiers are used to achieve this, it is questionable if this is a suitable approach to first line inspection.

2.2 Verifiers

Genuineness can only be readily established by the inspection of a security feature that is truly verifiable. The issue is to explain what features to look for that verify a document, rather than describing the many possible deviations that may falsify it. *Verifiers* are based on virtually inimitable technologies that produce unique, easily observable effects that cannot be simply imitated. The obvious presence of such an effect reliably confirms the genuineness of the feature. Consequently, verifiability is to be greatly preferred over falsifiability.

The potential security value of verifiers has a twofold base:

1. The unique optical effects displayed are obvious, and allow simple, fast and unambiguous inspection (ergonomics).
2. The technology involved makes successful forgery, counterfeit or simulation highly improbable (verifiability).

3 Application to security features

The above considerations can be applied to all first line security features and even to second line security features that require human inspection. In the following a few examples are given of this approach to the ergonomics and integrity of security features: the watermark, the windowed thread, metallic foil printing, and iridescent optically variable devices.

3.1 Watermark

The cylinder mould watermark is present in almost all banknotes and in many other security documents on a world-wide scale. It is a renowned security feature that has been with us since handmade papers were produced in Italy at the end of the thirteenth century [6]. As a consequence it has become a standard. It is regarded by paper makers as the primary and most secure feature, and one of the main barriers against counterfeiting [7-10]. In how far this assessment is correct may ensue from the following.

3.1.1 Ergonomics of the watermark

To what extent the watermark is an ergonomic security feature may become clear by considering the three fundamental questions posed in section 1. As it appears, the watermark is not at all an ergonomic feature. Its complex optical characteristics and its non-normal manner of inspection contribute to this unfavourable ergonomic properties.

1. Is the function of the device obvious?

Under normal observation the watermark tends to hardly visible. The examiner must know it is there, and only knows this because it is standard on many banknotes, mostly in a blank area. For the same reason the function of the watermark is well known: verifying or falsifying the document by looking for the presence of the watermark and its typical characteristics in transmitted light: continuous tone, visible as lighter and darker elements of the image, as shown in figure 2. These characteristics are typical of the mould made watermark, but the public is generally unaware of them (not in the head), and neither is this information provided by the watermark itself (not in the world).

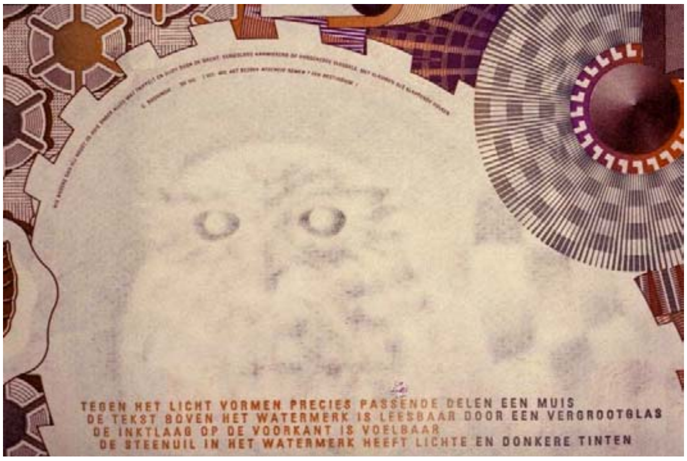
TEGEN HET LICHT VORMEN PRECIES PASSENDE DELEN EEN MUIS
DE TEKST BOVEN HET WATERMERK IS LEESBAAR DOOR EEN VERGROOTGLAS
DE INKTLAAG OP DE VOORKANT IS VOELBAAR
DE STEENUIL IN HET WATERMERK HEEFT LICHTE EN DONKERE TINTEN

Figure 2 - Mould made watermark in the DFL 100 note, showing image elements that are darker and lighter than the background.

2. Is execution of the examination easy?

From a physical standpoint this action is simple, but it is associated with an important psychological drawback: embarrassment. "The general public appears to be reluctant to observe and confront, and hence the chances are good that a banknote will only undergo a cursory inspection at the first encounter" [6]. A cursory inspection, however, is insufficient to evaluate a watermark.

3. Is the evaluation based on a yes/no decision?

If well designed and implemented, the mould made watermark allows unambiguous observation of its typical characteristics. However, the characteristics of the mould made watermark are somewhat complicated, so that their observation requires mindful attention and experience. Moreover, many watermarks hardly display clear lighter/darker image elements, and, in that case, evaluation becomes awkward (figure 3a). Therefore, fast evaluation of a watermark resulting in a yes/no decision is often infeasible.

3.1.2 falsifiability versus verifiability of the watermark

The mould made watermark is difficult to originate unless a paper manufacturing plant is available or the original paper can be stolen. This makes the watermark, potentially, a very strong security feature. Thus, the presence of a mould made watermark is a strong indication of genuineness. However, its inspection must be carried out with attention, employing a certain experience and knowledge. The watermark therefore is suited as a security feature in case suspicion is raised. It is not an ideal public security feature because it is not inspectable in an ergonomic manner. If, as is often the case, the lighter/darker halftone characteristics are not well visible in the original watermark, distinguishing it from imitations requires expertness beyond the capability of the layperson (figure 3).

It is concluded that, although the absence of a watermark is a certain indication of a counterfeit, its (seeming) presence does not prove genuineness unless the original is very well designed and implemented. Therefore - in principle - the watermark is a verifier, though - in practice - it will often merely function as a falsifier.

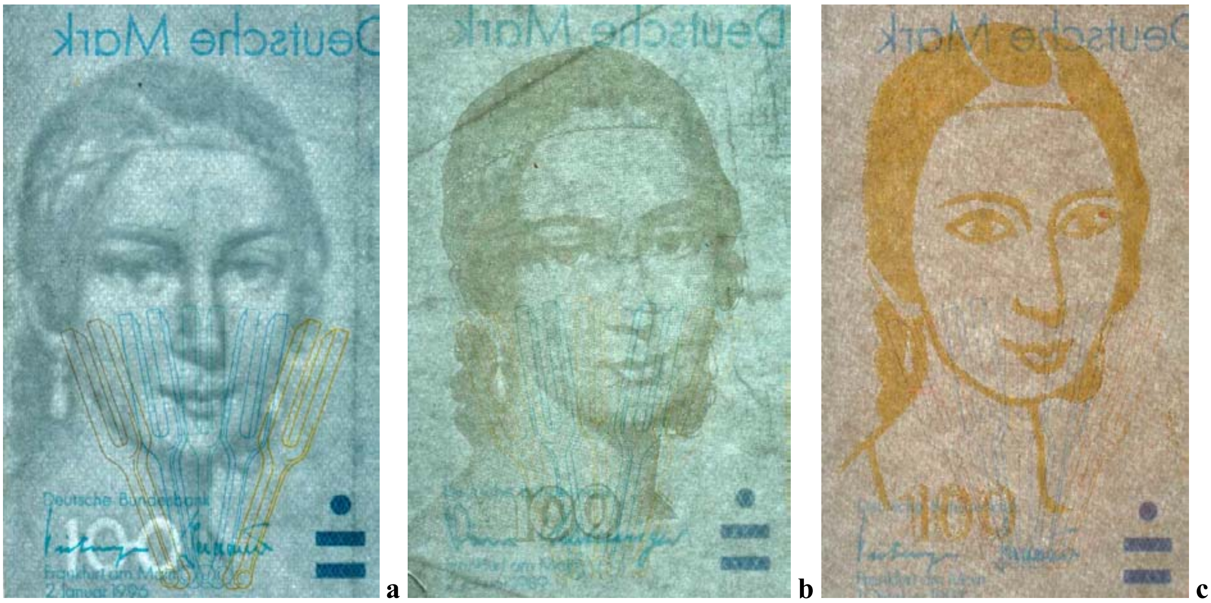

Figure 3 - watermark in DM 100 note: (a) authentic watermark, (b) half tone imitation, (c) single tone imitation.

3.2 Windowed thread

The windowed security thread is a development of Portals (UK) which is applied in banknote paper as a security feature (for instance in UK, German, Swiss and Czech notes). It is not a standard security feature. The windowed thread generally has a metallic reflection and is alternately embedded in the paper mass and visible on its surface (with a cycle of about 10 mm). As a result, and contrary to its predecessor the fully paper embedded security thread, the windowed thread is partly visible under normal observation. In transmission the thread appears as a continuous ribbon against a watermark bar pattern of darker sections at the places where the thread is embedded. Figure 4 illustrates the reflective and transmissive properties of the windowed thread. Often, the thread is provided with small lettering, visible in reflection as well as in transmission (e.g. German notes). On genuine banknotes the thread is overprinted.

3.2.1 Ergonomics of the windowed thread

By considering the three fundamental questions posed in section 1, it appears that the windowed thread is not an ergonomic feature in all aspects of its inspection. Its not being a standard, its rather complex optical characteristics, and its non-normal manner of inspection contribute to its unfavourable ergonomic properties.

1. Is the function of the device obvious?

The windowed thread is a security device that must be inspected under normal observation as well as in transmission. The complete function of the windowed thread is not obvious, and, since the device is not a standard, its full function will expectedly remain largely unknown: the required information is neither in the head nor in the world. The required actions are twofold: (1) under normal observation check for an interrupted thread with metallic reflection, being overprinted, and (2) in transmission check for a continuous dark thread against a watermark bar pattern. As the function of the device is not clear in the first place, the examiner cannot tell what characteristics to look for and how to inspect them unless *à priori* knowledge is available. In fact, the layperson confronted with an interrupted reflective ribbon may, mistakenly, expect the ribbon to be interrupted in transmission as well. The latter appears the case for the many German counterfeits, that merely carry an interrupted reflective imitation thread.

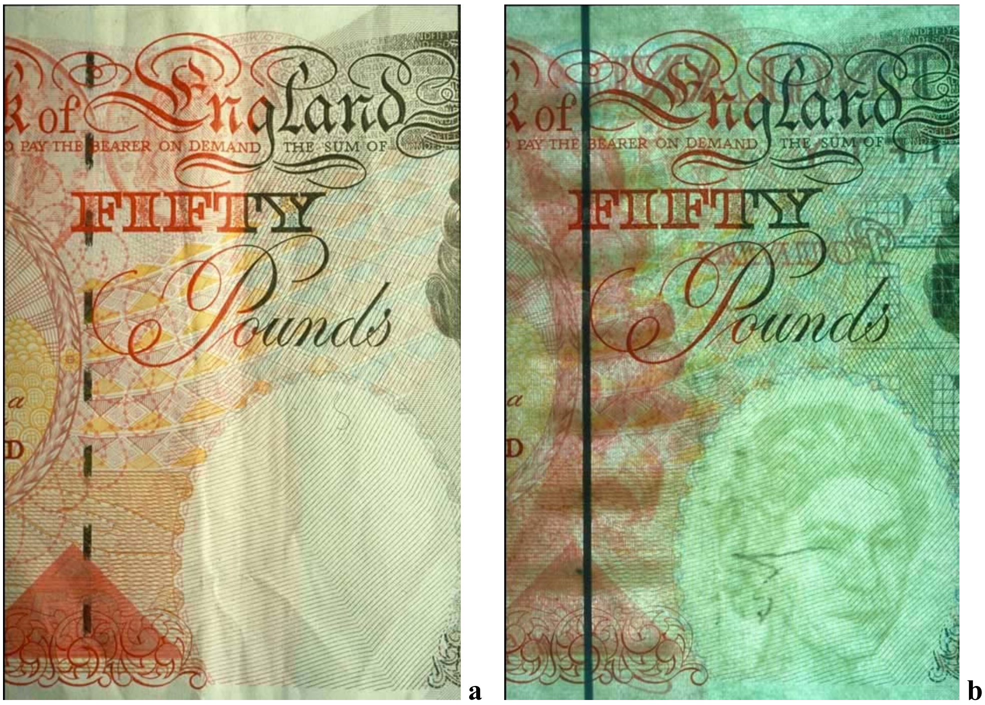

Figure 4 - The windowed thread on a genuine UK £50: (a) in diffuse reflection, and (b) in transmission (note the watermark bar pattern).

2. Is execution of the examination easy?

Normal inspection of metallic reflectivity is fast and uncomplicated, as is the check for a continuous thread in transmission. However, the combination of both these checks slightly complicates and slackens the process. Moreover, inspection in transmission is associated with embarrassment. Observing the watermark bar pattern in transmission and the printed design continuing over the thread in diffuse reflection requires sharp attention and adds to the complexity of the inspection.

3. Is the evaluation based on a yes/no decision?

The check for interrupted metallic reflection, and the continuity of the thread in transmission - on themselves - allow easy comparison with the expected result. This simpler evaluation is already based on a pair of yes/no decisions. Additionally observing the printed design continuing over the thread and the watermark pattern, expands the inspection of the windowed thread into a series of decisions that can hardly be considered a single yes/no decision.

3.2.2 falsifiability versus verifiability of the windowed thread

The origination of a windowed thread is beyond the capability of the counterfeiter, because this requires mastering an intricate paper making process. However, contrary to the watermark, this does not potentially make the windowed thread a strong security feature. Counterfeiters have found relatively simple methods to put together various deceptive imitations of the windowed thread, some being of professional quality others being of "home-made" quality but still sufficiently passable. Such shortcuts considerably lower the security value of the windowed thread. Figure 5 presents an illustration of a professional imitation in reflection and in transmission.

Discovering the deceit requires accurate scrutiny, for instance by noticing the absence of the watermark bar pattern. But it appears that counterfeiters also imitate this particular characteristic, which tends to degrade this characteristic to a falsifier. The lack of print over the thread is another falsifier, because if desired, print could also be applied over the thread as a last step. But in practice, examiners often destructively investigate the note by partly tearing it at the location of the thread; a procedure that is neither highly ergonomic nor entirely desirable.

It is concluded that, although the absence of a windowed thread, or the discontinuity of the thread observed against the light, are certain indications of a counterfeit, the (seeming) presence of a windowed thread with interrupted metallic reflectance, and appearing continuous against the light does not prove genuineness. Therefore, the windowed thread only functions as a falsifier.

It is noted that novel windowed threads that are provided with optically variable effects of the diffractive or interference type are an exception, because these iridescent effects do not allow easy imitation. But because the narrow windowed thread generally presents a rather small surface, these iridescent effects tend to be less obvious.

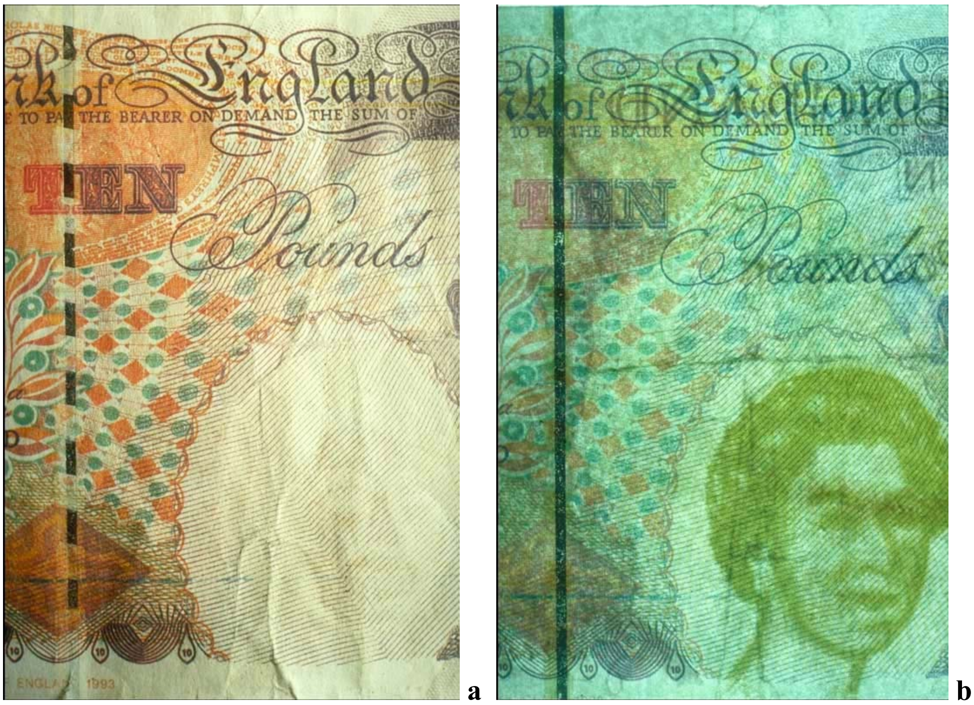

Figure 5 - Counterfeit UK £10 with imitation windowed thread: (a) in diffuse reflection, (b) in transmission (note the absence of the watermark bar pattern).

3.3 Metallic foils

Metallic foils are adhered to the substrate by hot foil blocking. Of old, they have been used by printers to embellish packaging such as cigar boxes. Metallic foils can be considered non-iridescent optically variable devices (OVDs) because they strongly change appearance with angle of observation, but do not display iridescent colour changes. It would appear that metallic foils efficiently hamper counterfeiting by the use of scanners in colour copiers and desk top publishing (DTP) systems: their metallic gloss reproduces as a black blot in colour copy and DTP counterfeits (see figure 6). As a result metallic foils frequently appear on bank notes and other valuable documents as an anti-copy feature.

3.3.1 ergonomics of metallic foils

By considering the three fundamental questions posed in section 1, it appears that foil printing is an ergonomic feature in all aspects of its inspection. The strong optical variability of metallic foils largely contributes to this favourable property.

1. Is the function of the device obvious?

The function of the metallic foil is to allow checking for its obvious metallic reflection. If covering a sufficient area, the metallic foil stands out brightly in the design and thus attracts attention while its absence tends to arouse suspicion. This is why the device, although not a standard, tends to be self-evident and communicate its function to the public without prior communication; in other words, the required knowledge tends to be in the world.

2. Is execution of the examination easy?

By slightly tilting the document, the optical variability of the metallic reflection becomes apparent. The required change in angle of observation is achieved by normal handling of the document. As a result, the metallic effect is easily observed under normal observation.

3. Is the evaluation based on a yes/no decision?

The reflective properties of the metallic foil are unambiguous and little doubt remains to what should be actually observed. Therefore, an evaluation of the feature based on a yes/no decision is well feasible.

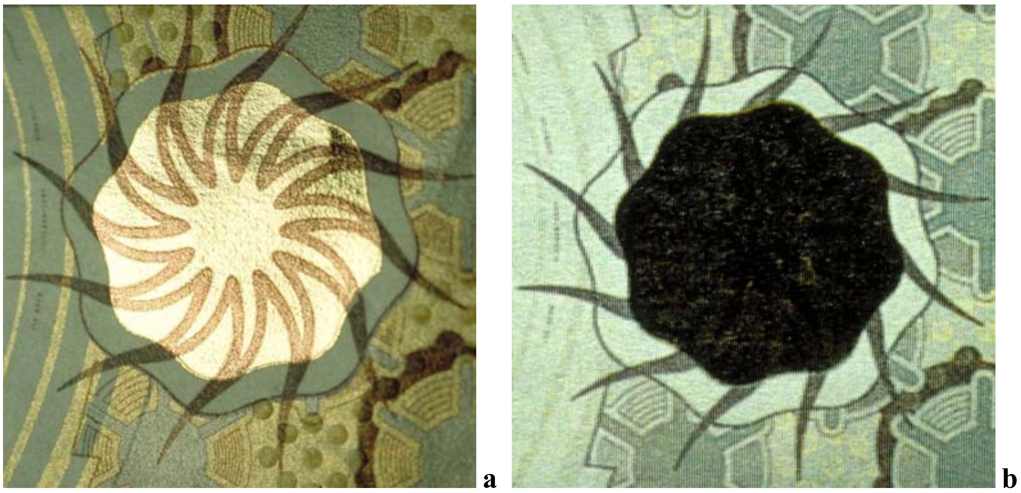

Figure 6 - Metallic “gold” foil on a DFL 100 note: (a) genuine note, and (b) a colour copy. The diameter of the foil is 14 mm.

3.3.2 falsifiability versus verifiability of metallic foils

The craft of metallic foil printing is an old one, mastered by many professional printers. Metallic hot stamping foils are commercially available without limitation and, as a consequence, foil printing does not offer strong security. This is illustrated by figure 7, showing metallic foil printing on a genuine UK £50 note and on a counterfeit UK £50 note.

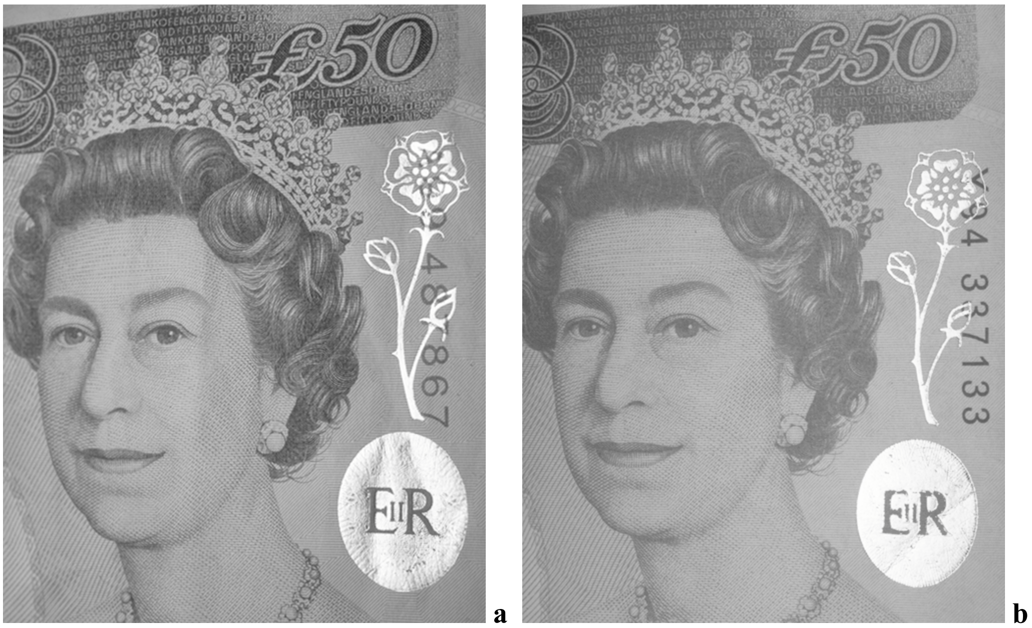

Figure 7 - Aluminium foil printing on a UK £50 note: (a) genuine note, and (b) counterfeit note printed in offset.

Furthermore, it appears that metallic foils are transposed from genuine banknotes, as shown in figure 8a and, furthermore, metallic foils can be more or less successfully imitated by the use of ordinary metallic paints, as shown in figure 8b.

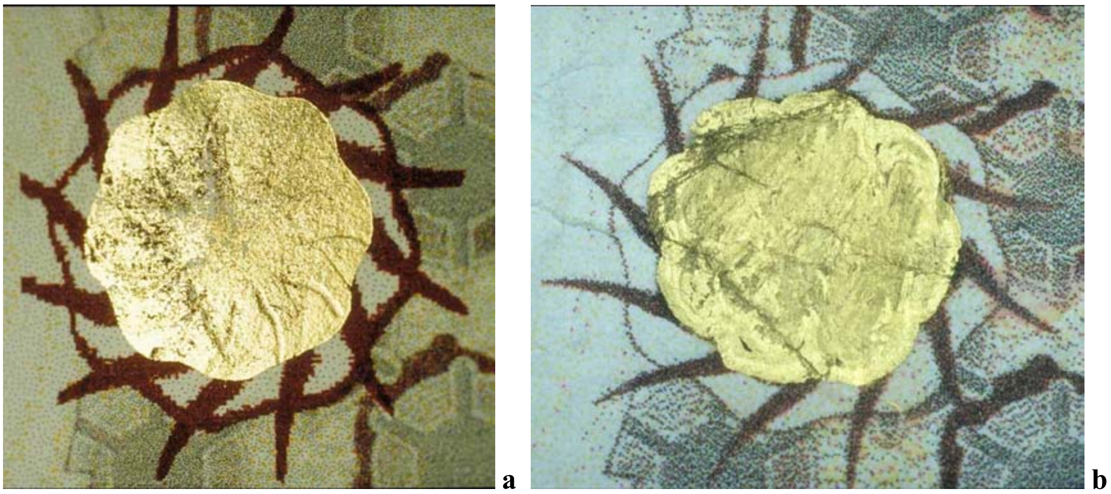

Figure 8 - Counterfeit DFL 100 note: (a) transposed metallic foil on an ink jet counterfeit, and (b) gold paint imitation on an ink jet counterfeit. The diameter of the foil is 14 mm.

Contrary to what is stated in an earlier publication [5], this means that the metallic foil does neither present a strong defence against the opportunistic counterfeiter practising his modest home-industry.
It is concluded that, although the absence of metallic foils presents a certain indication of a counterfeit, this may also be caused by prolonged soaking in water or by laundering. The (seeming) presence of a metallic foil does not prove genuineness. Consequently, the metallic foil merely functions as a falsifier of mediocre value.

3.4 Iridescent optically variable devices

Iridescent optically variable devices (iridescent OVDs) are either based on light diffraction by fine grating structures or on light interference by thin film structures. The diffractive type is coined as *diffractive optically variable image device* (DOVID), while the interference type is referred to as *interference security image structure* (ISIS).

In the evolution of document security iridescent OVDs are relatively novel developments, increasingly applied as security features on banknotes and other valuable documents and products. Examples of DOVIDs are the hologram of the VISA dove and the kinegram on Swiss banknotes. Examples of ISISs are optically variable ink (OVI) found on many banknotes, the thin film *optical security device* applied to Canadian banknotes, and pearl lustre ink. The latter ink typically displays one single interference colour in reflection, to become colourless and transparent outside specular reflection. DOVIDs and ISISs are extensively treated in reference [11].

3.4.1 ergonomics of iridescent optically variable devices

The unique optical effects displayed by iridescent OVDs tend to be obvious, and allow simple, fast and unambiguous inspection. However, as the gamut of optical effects of OVDs is extremely diverse, their ergonomic aspects can only be discussed in the broadest sense, assuming that their ergonomic potential is optimally utilised. Alas, taking into consideration the many intricate OVD-designs that embroider current valuable documents, it appears that this assumption is not always justified [2]. DOVIDs are often rendered extremely dense optically variable detail and designers seem to be fascinated by packing their OVDs with such detail in order to create petite ornamental masterpieces. Alternatively, these complex adornments may be the outcome of imperative instructions by customers, who erroneously hold the view that image complexity is a counterfeit deterrent. Unfortunately, it is often overlooked that this approach rather is an inspection deterrent.

ISISs generally are much simpler in design and tend to perform better than DOVIDs in this respect.

1. Is the function of the device obvious?

The function of OVDs is to allow checking for specific iridescent effects. Colour changes are only useful for inspection if these can be easily communicated. This is the case for ISISs (and zero order devices), which show consistent colour shifts highly independent of lighting. Contrary, colour changes of (first order) DOVIDs tend to be intricate and are highly dependent on lighting. For ergonomic inspection DOVIDs have to rely on imagery, including kinematic effects and positive-negative contrast swaps. Because, all these effects are not standardised, they must necessarily convey a functional message to the user. Only if this is a simple and obvious message, the user will understand and recall it.

The optical effects of OVDs can be simple and obvious. Consequently, OVDs potentially allow placing the required knowledge in the world so that their function can be grasped, virtually without foreknowledge. As their optical effects unfold by observing OVDs under different angles, the required actions are almost automatically performed by common handling of the documents. Consequently, the required tilt actions can be more or less self-evident.

2. Is execution of the examination easy?

Iridescent effects of OVDs unfold under normal observation by slightly tilting the document. This handling tends to be easy and inconspicuous, and does not evoke embarrassment. The changes of image and colour tend to attract attention and, if the feature is well designed, these can be easily observed. However, under diffuse illumination the kinematic effects of (first order) DOVIDs blend into one another and become practically invisible. Contrary, the iridescent effects of ISISs can be observed under diffuse illumination as well as under illumination by point sources.

The positive/negative contrast swap illustrated in figure 9 - characteristic for kinegrams - requires an in plane rotation of the document over 180° [11,12]. Although this way of handling is both conspicuous and relatively complex, this particular feature supports inspection under completely diffuse illumination.

3. Is the evaluation based on a yes/no decision?

Changes of colour and image in OVDs can be unique and unambiguous so that no misunderstanding will arise with respect to what should be observed. In case the feature is ergonomically designed, examination will be easy and the iridescent effects will, potentially, allow an evaluation based on a yes/no decision.

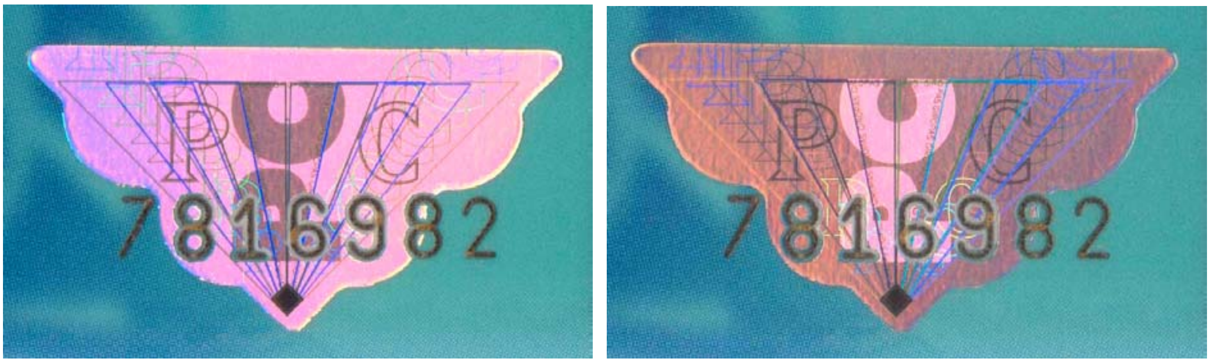

Figure 9 - Kinegram on the Dutch Giropas with laser engraved account number. The contrast reverse of the letters "PC" with the background comes about by rotating the kinegram over 180° in its own plane, or by changing the angle of illumination from left to right. The laser engraved digits through the kinegram have a height of 3 mm.

3.4.2 falsifiability versus verifiability of iridescent optically variable devices

On the one hand the potential security value of iridescent OVDs is based on the unique and obvious optical effects displayed, allowing simple, fast and unambiguous inspection. This is the ergonomic aspect of document security. On the other hand the complex technology involved tends to make successful forgery, counterfeit or simulation improbable.

However, it is noted that the technique of optical replication and holographic production of classic first order DOVIDs has progressively become widespread. This entails the threat of originating more or less deceptive counterfeits. As is derived from earlier information of the International Holographic Manufacturers Association (IHMA) and various other sources, only crude counterfeit holograms were discovered [13, 14]. The IHMA, though, warned against complacency: "Both Visa and MasterCard have stated publicly that they have a problem with counterfeit cards and counterfeit holograms. A store clerk is unlikely to check the holograms carefully, so the problem is real for the credit card issuers." [14]. The acuteness of this problem emanates from a recent news issue on counterfeit Microsoft Windows '98 holograms, denoted as appearing "very irregular and rough", a vague notification that can be hardly called ergonomically functional [15]. It is now envisaged that classic holograms will gradually shift from being verifiers to being falsifiers in the not too remote future.

This is the aspect of verifiability.

Ergonomics and verifiability are the two pillars of document security. Nano-technology in particular aids in erecting these pillars and has rendered what has been referred to as nano-security [5]. Nano-security involves the production of complex sub-micron structures that cannot be (re)produced with classic and widely available holographic means [16-19]. Examples are first order DOVIDs with blazed gratings, blazed achromatic gratings, gratings with continuous variation of depth, and superposed gratings (figure 9 in this paper, and the specimens in the figures A.7 and A.8 in Optical Document Security) [12,13,16,17]. Other examples are the zero order device (ZOD) [18], and ISISs, such as optically variable ink (OVI) [19] and the thin film device on the new Canadian banknote series [20] (see also the figures A.12-A.14 in Optical Document Security).

It is noted that not all types of iridescent OVD perform equally well in these respects. For example, the security value of pearl lustre ink and Bragg type iridescent planchets may be questioned [5]. Pearl lustre pigment is inexpensive and widely available as a raw material and printable pearl lustre inks can be easily composed. Iridescent planchets, often added to security paper during paper manufacture, consist of co-extruded multilayers, a material that is also inexpensive and widely available.

It is concluded that numerous types of iridescent OVDs can be created with characteristics that essentially make them verifiers. Obvious optical effects, beyond the capability of counterfeiters and forgers, inimitable by the application of simpler processes (shortcuts), play the key role.

4. Discussion

In this paper a limited number of security features is discussed from the viewpoint of their human factors as well as their verifiability. Some of these aspects were discussed for other security features in earlier publications [1,3,5].

It is maintained that the complexity of the manufacturing process of a security feature, being far beyond the capability of the counterfeiter, cannot be put forward as a guarantee for security. Some of these features only serve as falsifiers: only too often the inventive criminal finds efficient shortcuts to deceptively imitate these highly esteemed features. This pronouncement may seem like forcing an open door, but it cannot be denied that falsifiers are still frequently put to use on valuable documents. The presence of such falsifiers may be even detrimental to the security level of the document because they attract undeserved attention, offer a false sense of security, while the additional inspection of other features - which again may be falsifiers - is required. This makes the inspection process an uncertain one and unnecessarily slows it down. Security is not served by stacking falsifiers on documents with the purpose to raise as many thresholds as possible. It is of utmost importance that the verificatory properties of security features are evaluated before they are put to use to protect our documents. These properties are based on the nano-complexity of the security structure, not *per se* on the complexity of the manufacturing process or on the visual complexity of the design.

But even the most reliable verifier does not fulfil its promise if optimal human factors design has not been implemented. People avoid handling obscure features, tend to avoid effort and embarrassment, and prefer simple yes/no decisions over sophisticated judgements.

5. References

[1] R.L. van Renesse, Human factors of first line security, Conference on Optical Security and Counterfeit Deterrence Techniques II, San José, Ca., 29-30 January, 1998, *Proceedings SPIE*, vol. 3314, p. 97-108.

[2] Renesse, R.L. van, Security design of valuable documents and products, *Optical Document Security*, 2nd ed., chapter 2, Publ. Artech House, London/New York (1998).

[3] Renesse, R.L. van, Human factors of card security, chapter 4, *Chip Card: Trump Card?*, eds. A. Knopjes and P. Lakeman, CRI theme book, National Criminal Intelligence Division (September 1998).

[4] Norman, Donald A., *The psychology of everyday things*, Basic Books, New York (1988).

[5] Renesse, R.L. van, Verifying versus falsifying banknotes, Conference on Optical Security and Counterfeit Deterrence Techniques II, San José, Ca., 29-30 January 1998, *Proceedings SPIE*, vol. 3314, p. 71-85.

[6] *Counterfeit Deterrent Features for the Next-Generation Currency Design*, National Materials Advisory Board, Commission on Engineering and Technical Systems, National Research Council, 1993, Publication NMAB-472, National Academy Press, chapter 5, p. 91.

[7] Camus, M., et al, Security papers and special effects, *Optical Document Security*, 2nd ed., chapter 5, Publ. Artech House, London/New York (1998).

[8] Acland, N.A.B., Cylinder mould made paper for non-banknote applications, *Proc. Int. Conf. of Security Printers*, Vouliagmeni (Greece), 6-8 June 1991.

[9] Schneider, Walter, New security features and substrates in ID and passport paper, *Addendum to Proc. Int. Conf. of Security Printers*, Lisbon (Portugal), 5-7 October 1995.

[10] Hofstetter, Bruno K., Counterfeit protection in the digital age, *Proc. Int. Conf. of Security Printers*, Seville (Spain), 15-17 May 1997.

[11] Renesse, R.L. van, Iridescent optically variable security devices, *Optical Document Security*, 2nd ed., chapter 15, Publ. Artech House, London/New York (1998).

[12] Moser, J-.F., Document protection by optically variable graphics (kinegram), *Optical Document Security*, 2nd ed., chapter 11, Publ. Artech House, London/New York (1998).

[13] Renesse, R.L. van, Iridescent optically variable devices, *Optical Document Security*, 2nd ed., chapter 15, Publ. Artech House, London/New York (1998).

[14] Moyes, Robert F., Techniques used by forgers of banknotes and travel documents as seen in Canada - opinions on proven techniques to combat forgers and counterfeiters, *Proceedings of the International High Security Printers' Meeting*, May 14 1997, Seville, Spain.

[15] OEM Windows 98 copied (too) soon after release, Authentication News, Reconnaissance International Ltd., volume 4, no. 8, November 1998, p. 1-2.

[16] Staub, R., Tompkin, W.R., Moser, J.-F., Combination gratings, *Proceedings SPIE*, vol. 2689, p. 292-299 (1996).

[17] Staub, R. and Tompkin W. R., Non-standard diffraction structures for OVDs, Conference on Optical Security and Counterfeit Deterrence Techniques II, San José, Ca., 29-30 January 1998, *Proceedings SPIE*, vol. 3314, p. 194-202.

[18] Gale, M.T., Zero-order grating microstructures, *Optical Document Security*, 2nd ed., chapter 10, Publ. Artech House, London/New York (1998).

[19] Phillips, Roger W., and Bleikolm, Anton F., Optical coatings for document security, *Applied Optics*, vol. 35, no. 28, 1 October 1996, p. 5529-5534.

[20] Dobrowolski, J.A., Optical thin-film security devices, *Optical Document Security*, 2nd ed., chapter 13, Publ. Artech House, London/New York (1998).