Synergistic combination of document security techniques

Rudolf L. van Renesse

Conference on Optical Security and
Counterfeit Deterrence Techniques III
San Jose, California, 27 – 28 January 2000
SPIE Vol. 3314, pp. 126 – 138

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

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

Synergistic combination of document security techniques

Rudolf L. van Renesse*

ABSTRACT

The value of security features tends to decrease gradually, partly because of the continuously increasing ability of counterfeiters to counterfeit or imitate these features and partly because of the increasing capability and availability of equipment. As a countermeasure, numerous non-iridescent and iridescent optically variable devices (OVDs) are continuously being developed. The former comprise novel laser engraving techniques, the latter DOVIDs (diffractive optically variable image devices) and ISISs (interference security image structures). Although these novel techniques appear highly effective, there are indications that they are beginning to fail, not in the least because organized crime appears to have acquired some of those newer techniques. The response is the synergistic combination of those techniques, which combination expectedly remains beyond the capability of criminal organizations. This ongoing development is currently providing new and exciting security potential. Examples are combinations of diffractive and interference phenomena and of laser perforation techniques with OVDs. The latter combinations provide strong protection against counterfeiting as well as forgery.

Keywords: document security, diffraction, interference, DOVID, ISIS, laser engraving, forgery, counterfeiting.

1. INTRODUCTION

From old, valuable documents have been provided with security features based on novel techniques. This is the result of a continual race between the issuers of the valuable documents and the criminals that try to forge, imitate or counterfeit them.[1]
A series of now classic security features has come forth of this process, such as the watermark, tactile intaglio printing, the see through register, fine line structures such as guilloches, micro lettering, colored and fluorescent security fibers, and fluorescent printing. The various security properties of some of these classic features are discussed in section 3 of this paper.
Gradually the value of many of these classic security features has decreased, partly because of the continuously increasing know how of counterfeiters and partly because of continuously decreasing prices and increasing capability of the equipment available. The contemporary gamut of counterfeited bank notes is a sad demonstration of the possibilities that are available to the multitude: color copiers, desk top publishing (DTP) systems (producing so called "digifeits"), and quality screen offset and line offset printing techniques.
The response to this process has been the development of novel security features, in particular comprising DOVIDs (diffractive optically variable image devices)[2] and ISISs (interference security image structures)[2], and also a variety of laser engraving techniques.[3-6] The various security properties of some of these novel features are discussed in section 4.
Proof of the ongoing race between issuers and criminals – the latter obviously having access to more or less advanced laboratories – is the regular appearance of counterfeit DOVIDs and their increase in quality.
In this ongoing race the issue now has become to introduce anti-counterfeiting techniques that synergistically combine very diverse document security techniques, to bring them beyond the capability of the counterfeiter. The various security features of some of these combination features are discussed in section 5.

2. THE MAIN PROPERTIES OF SECURITY FEATURES

In various earlier papers the properties of classic and novel security features are treated.[7-10] The main security properties discussed are the human factors involved in the inspection of these features and the topic of verifiability versus falsifiablility.

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

2.1. Human Factors

The human factors of security features concern three fundamental questions:
(1) "is the function of the device obvious?",
(2) "is execution of the examination easy?", and
(3) "is the evaluation based on a yes/no decision?".
The answers to these questions render a qualitative measure of the ergonomics of the security feature. [7-9] If these questions can be answered affirmatively, the security examination can be considered to be executable ergonomically. If not, the examination will be rarely executed or, at best, will be executed in an inadequate manner. In these latter cases, the security feature, however advanced from a technical point of view, obviously will not fulfill its task.

2.2. Verifying versus Falsifying

The integrity of the evaluation involves the state of a security feature being either confirmable as false (negative evidence) or as genuine (positive evidence).[10]
Advanced security features that cannot possibly be expected to be faithfully originated, can sometimes be imitated with simple techniques. In that case, the difference between such "shortcuts" and the genuine feature can only be established by detailed analysis (for example with a magnifier or microscope) or in a destructive manner (for example by tearing the note at the location of a security thread). Such security features are mere falsifiers: their missing or gross deviation from expectation prove falseness, but their apparent presence or their meeting expectation does not. Contrary, the apparent presence of a verifier does proof genuineness.

3. CLASSIC SECURITY FEATURES

The human factors and security properties of various classic security features, such as the watermark, the see-through register, fine printing structures (such as micro text, guilloches and screen traps), intaglio printing, the latent image, engraved portraits, metameric color pairs, and fluorescent printing are extensively discussed in earlier papers [7-10] and, therefore, only the properties of a few are reviewed briefly in this paper, regarding concurrent counterfeits. In general, it may be concluded that many classic security features do not allow optimally ergonomic inspection and are not verifiers.

3.1 The Watermark

Originating a watermark requires a paper mill and counterfeiters rarely have that available. This principally makes the watermark a strong security feature. However, the watermark is not an ergonomic device and tends to be rarely evaluated in an adequate manner. This is because it has to be held against the light, which involves a psychological drawback, and subsequently its halftone characteristics must be adequately evaluated, which is relatively difficult and time consuming.

(a)

(b)

Figure 1 – Watermark and security thread in Italian 100.000 Lire bank note (transmission): (a) genuine watermark, (b) imitation watermark. Although there is a distinct difference in quality, the imitation watermark shows lighter and darker halftones. Also note that the imitation security thread has legible micro text.

Due to high speed paper production, resulting in inferior watermarks that do not adequately present halftones that are lighter and darker than the surrounding paper, adequate inspection is often seriously hampered. Counterfeiters make thankful use of this latter fact. Otherwise, even quality watermarks are imitated in a successful manner, showing in detail both lighter and darker halftones. Such imitations require careful examination in order to be revealed as imitations (figure 1). Consequently, unless well designed, the watermark only functions as a falsifier.

3.2 The See-through Register

The see-through register requires the counterfeiter to have front and back printing of the note in exact register. Like the watermark, the see-through register must be inspected against the light. Counterfeiters rarely care to register front and back printing, because experience teaches that the public normally does not care to investigate a note against the light. Most counterfeits therefore lack adequate front-back register, counterfeits may sometimes even have one side upside down, or may even have two identical sides.
Another problem connected to the see-through register is that it is not always designed in an ergonomic manner. The feature then shows a complete, abstract image on both sides of the note and therefore it does not adequately reveal a register of two visually different parts. Only when both sides are off-register, this becomes visible in transmission. As a result the user does not easily understand the function of the device.[7]
Otherwise, even amateur counterfeits may show a front-back print register, so that observing adequate front-back register does not prove the note to be genuine (figures 2 and 3). As a consequence, the see-through register is just a falsifier.

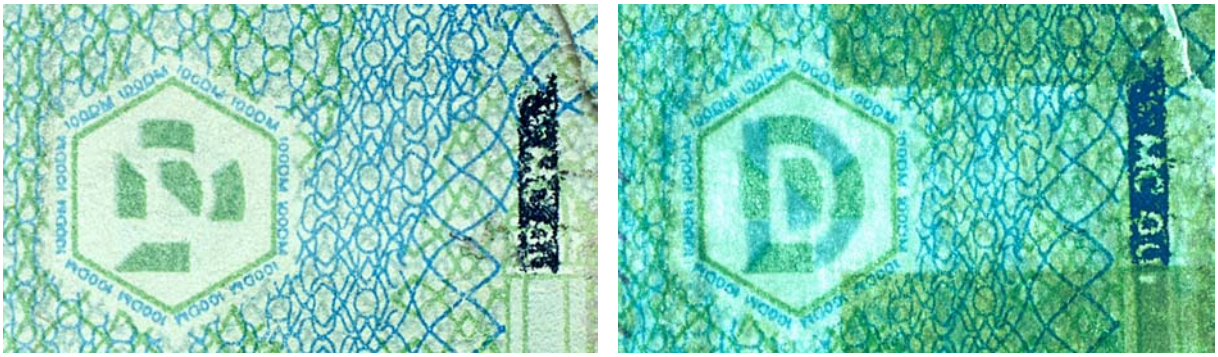
Diffuse reflection — Diffuse reflection

Transmission — Transmission

Figure 2 - Counterfeit see-through features in adequate register: (left) screen offset of the former Dutch 100 guilder note, with sub-optimal see-through design, and (right) ink jet digifeit of the Dutch 25 guilder note with optimal see-through design.

3.3 Small Lettering and Micro Text

Small lettering, micro text and other fine printing features protect against the lack of resolution of color copiers and DTP systems. The human factors of fine printing details, such as micro text, generally lack ergonomic properties, the fine features are not obvious and their inspection requires acute vision or a magnifier. Otherwise, professional line offset counterfeits provide adequate resolution to reproduce micro text (figure 3).[10]



(a) **(b)**

Figure 3 – Micro text (0.3 mm high) around see-through register on a line offset counterfeit German 100 mark note: (a) in diffuse reflection and (b) in transmission. Note the adequate front-back register and the presence of small lettering on an imitation windowed thread that is continuous in transmission.

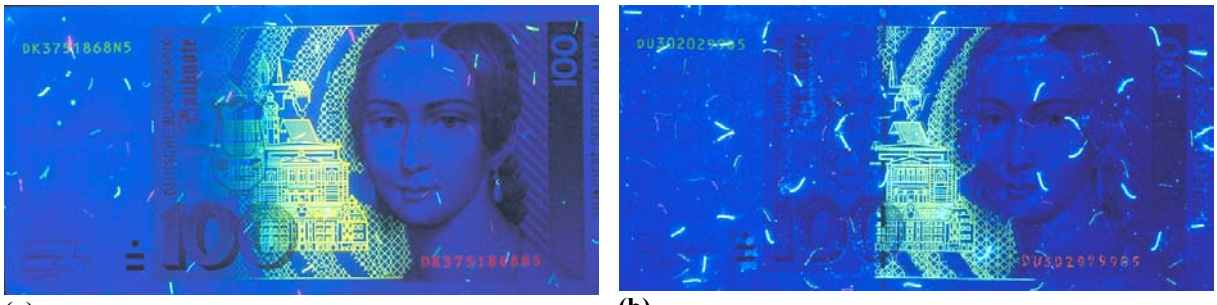
But current color copiers and DTP systems have a resolution of 600 dpi (24 dots/mm) or more, which now allows fine details being reproduced with deceptive detail (figure 4). As a consequence the appearance of legible micro text does no longer prove genuineness. In general, fine printed details only provide falsifiers.

(a) **(b)**

Figure 4 – Micro text (0.4 mm high) on a Spanish 1000 peseta bank note: (a) genuine note and (b) digifeit made with HP Scanjet 6200C scanner and tektronix phaser 740 printer.

3.4 Fluorescent Printing

In daylight or bright incandescent background light, a hand held ultraviolet source does not easily allow checking the presence of fluorescent printing. Adequate inspection is only possible at a counter where a bright enough ultraviolet source is available with sufficient shielding of background light. The issuer of counterfeits therefore may wish to avoid such places.



(a) **(b)**

Figure 5 – Fluorescent printing on a German 100 mark note: (a) genuine note and (b) line offset counterfeit note. Also note the imitation fluorescent fibers and the note number in green (top left) and red (bottom right) fluorescence on the counterfeit note.

Otherwise, fluorescent inks are widely available and their preparation is not a tour de force for the counterfeiter. The origination of fluorescent printing and the imitation of fluorescent fibers therefore is not beyond the capability of the professional counterfeiter and this reduces fluorescent features to falsifiers (figure 5).

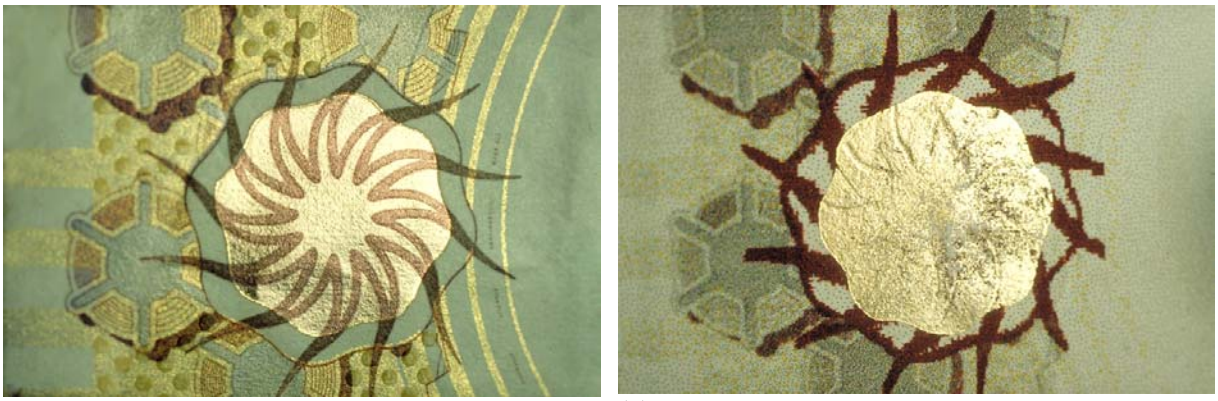
3.5 Foil Printing

The craft of metallic foil printing is mastered by many professional printers. Metallic hot stamping foils are commercially available without restriction and, as a consequence, foil printing does not offer strong security (figure 6).

(a) **(b)**

Figure 6 – Aluminum foil printing on a UK £50 note: (a) genuine note, and (b) line offset counterfeit note.

Furthermore, ordinary metallic gold or silver paints can be used more or less successfully to imitate metallic foils, and otherwise, metallic foils can be transposed from genuine bank notes, without the latter becoming valueless (figure 7).[8] Although the absence of metallic foils may indicate a counterfeit (which absence can also be caused by inadvertent laundering of the note), the presence of a metallic foil does not prove genuineness. Consequently, metallic foils merely function as falsifiers.



(a) **(b)**

Figure 7 – Metallic gold foils on DFL 100 note: (a) genuine note, and (b) ink jet digifeit with transposed foil (the foil overprinting is lost). Also note the reflection of the pearl luster printing on the genuine note.

4. MODERN SECURITY FEATURES

Various novel security features have been introduced in the last two decades, offering improved anti-counterfeiting and anti-forgery characteristics over their classic predecessors. These features comprise non-iridescent as well as iridescent Optically

Variable Devices (OVDs). Amongst the non-iridescent OVDs are laser engraved features, including lenticular tilt images (Multiple Laser Image) that – with angle of observation – can display different variable information (e.g. a portrait and an ID number), and laser perforated portraits (ImagePerf).[3-6] The iridescent OVDs that have been developed are all based on either light diffraction (DOVIDs - diffractive optically variable image devices) or light interference (ISISs - interference security image structures).[2]

Such OVDs tend to thwart counterfeiting and forgery because – in principle – they are neither easily originated nor easily imitated, while their inspection can be carried out in an ergonomic manner.

Two important counterfeiting targets are bank notes and plastic cards. The counterfeiting of these appears to be carried out in different criminal provinces, requiring different technical capabilities and offering different revenues.

4.1 Bank Note Counterfeiting

Due to the steady development of digital copying techniques, the ability to copy bank notes resulting in a deceptive counterfeit ("digifeit") has come within the reach of the multitude. Making allowance for the less than optimal functionality of classic security features, discussed above, these (occasional) "digifeiters" do not require any significant abilities but for operating widely available image processing software on a computer, connected to a quality ink jet or a dye sublimation printer. All together this low end equipment is available for a few thousands of dollars or less. Generally, the digifeiter is not a mass-producer, but their sheer number has become a considerable threat.
On the high end of the bank note counterfeiting scale, a relatively limited number of professional printers are able to mass produce counterfeits and add value to these by successfully imitating watermarks, fluorescent features, security threads and security foils, using classic printing techniques like offset, screen and foil printing.
Although DOVIDs have appeared on bank notes since 1986 (Finland), their application has only become widespread in the nineties. Therefore – until recently – neither the industrious low-end digifeiter nor the high-end professional printer have felt an incentive to get access to DOVID origination sources. Necessarily they currently revert to imitations, which tend to be poor. An example of such an imitation on a German bank note is given in figure 8b.

(a) **(b)**

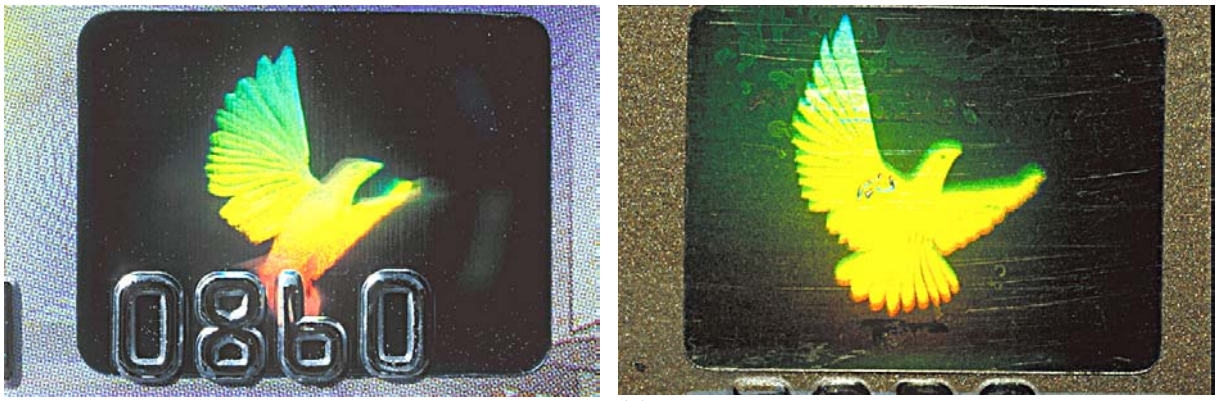
Figure 8 – DOVID (Kinegram) on a German 100 mark note: (a) a genuine Kinegram and (b) an imitation by means of commercially available diffractive foil glued to the substrate of a digifeit.

Also ISISs, such as optically variable ink (OVI) and the Canadian Optical Security Device (OSD), have been the subject of imitation, but thus far none of these imitations has displayed a convincing color change with angle of observation. Considering the above, iridescent OVDs may remain effective as verifiers against bank note counterfeiting for the years to come.
And indeed, we now see many bank notes being provided with DOVIDs (e.g. UK, Swiss and German notes), and ISISs (Canadian notes with the OSD and numerous notes with OVI printing).
Otherwise, apart from iridescent OVDs, also micro laser perforation (Microperf) is now protecting Swiss bank notes against counterfeiting.[4]

Undoubtedly, organized bank note counterfeiters will strain after obtaining or originating deceptive copies of iridescent OVDs to add to their products and – in due course – they may succeed. However, it must be borne in mind that the revenue of adding a counterfeit DOVID to a bank note is limited to even less than its face value. And, further, the higher its face value, the more difficult it generally is to pass a bank note. Expectedly, both these factors reduce the incentive to counterfeit OVDs for bank notes. However, the broad introduction of Euro notes, which will be protected by DOVIDs, may be ample incentive for their potential counterfeiters and sooner or later the security value of DOVIDs may be notably decreased.

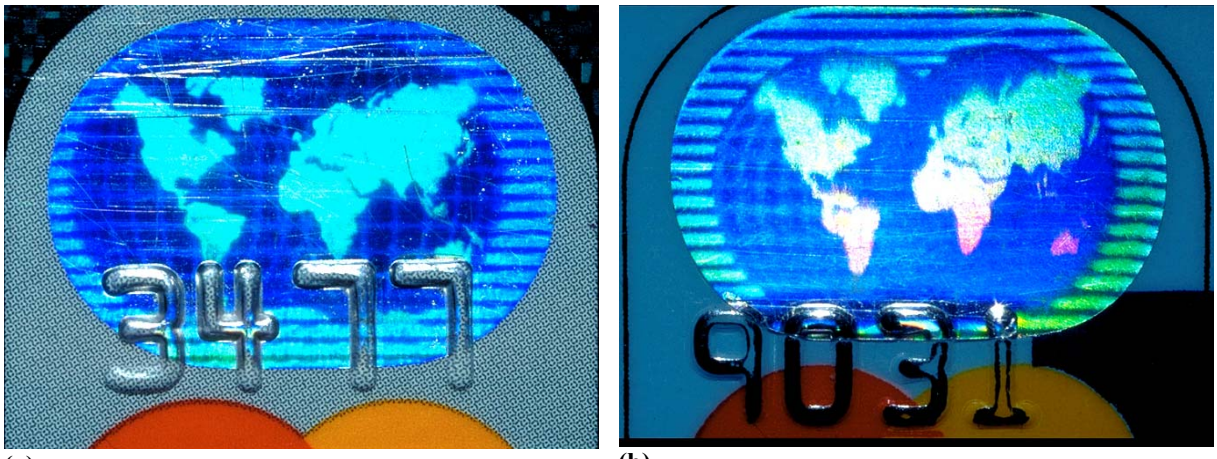
4.2 Plastic Card Counterfeiting

A wholly different picture is presented by plastic card counterfeiting. The plastic card counterfeiter is required to obtain plastic cards with magnetic stripes, print the plastic cards with screen printing or dye sublimation, skim magnetic codes from original credit cards and copy these to the magnetic stripes of the fake cards, add a passable DOVID and finally emboss or laser engrave the account number into both card and DOVID. This diverse technology is fully beyond the capability of the digifeiter and even beyond that of many classic professional printers.
The use of DOVIDs on plastic cards became common since the early eighties. Apparently, in this respect, the credit card industry is somewhat ahead of the bank note industry. As a result, the credit card counterfeiter, living in a criminal world different from that of the bank note counterfeiter, also became ahead of the latter.
The main reason for this discrepancy in time is that DOVIDs applied to plastic cards, which are stiff, have a smooth surface and are not circulated, have a considerably longer life expectancy than DOVIDs applied to paper bank notes that are pliable, have a rough surface and are heavily circulated.



(a) **(b)**

Figure 9 – Single channel VISA hologram: (a) genuine hologram and (b) counterfeit hologram.



(a) **(b)**

Figure 10 – Two channel MasterCard hologram: (a) genuine hologram and (b) counterfeit hologram.

Otherwise, plastic cards have no face value, but have an intrinsic value that may amount to tens of thousands of dollars a piece, significantly surmounting the value of any single bank note and rendering the effort per piece apparently much more rewarding.
In the not so remote past, various observers, this author included, have affirmed that counterfeit DOVIDs often were crude imitations that could be easily distinguished from the originals. These affirmations were based on a worldwide examination of counterfeit and imitation DOVIDs.[2] Since, however, criminal organizations have increasingly acquired access to (the more basic) holographic techniques.[11] Recently, for example, high quality counterfeit holograms, originating in the Far East, have appeared on fake credit cards seized by the Police Rotterdam-Rijnmond, Forensic Crime Squad (figures 9 and 10).

These quality counterfeit holograms have high diffraction efficiencies and display full three-dimensional images that, although not being fully accurate copies and lacking fine detail, very deceptively resemble the original holograms. The counterfeit VISA dove, for instance, is displayed under a different angle and the counterfeit MasterCard hologram displays no micro printing.
Although experts may easily distinguish between these counterfeits and the original holograms, cashiers – let alone lay people – expectedly require attentive comparison of the counterfeit with its original in order to adequately discriminate between the two. As a consequence, in the plastic card sector, the hologram tends to become a falsifier rather than a verifier.

5. SYNERGISTIC COMBINATION OF SECURITY FEATURES

Typically, OVDs were initially – and often still are – applied to security documents in a stand-alone manner, without any synergistic relation to other security features present on the same document. Examples are the OSD on Canadian bank notes and the Kinegram on the 500 Finnish mark. This, in principle, makes the separate features more vulnerable to counterfeiting and forgery than if they were inventively combined with others. It is the synergistic combination of security features – necessarily based on diverse technologies – that makes these features interact in a manner such that their combined security value is greater than the sum of their individual security values. Such synergism allows the secure application of existing features that, applied separately, may no longer render adequate security.
An early attempt to integrate different security measures was the embossing of account numbers through DOVIDs on plastic cards (figures 9 and 10). Of course, the efficacy of this approach is only small because the card embossing itself does not serve appreciable security.[12]
Since, a steady development of ingeniously combined security features has taken place. An early example is found on the commemorative $10 Australian polymer bank note (1988) that combines polymer technology and diffraction gratings to create a DOVID in a transparent window. Otherwise, the use of polymers potentially opens up a whole new area of combination features that allow self-authentication of valuable documents. Proposed are Fresnel lenses embossed in the polymer that allow magnified inspection of micro features, polarizers, metameric filters, and line gratings incorporated in a transparent window that induce moiré effects when laid over the printing.[13] The application of a metameric filter in bank notes is now realized in the new Romania 2000 Lei bank note. Furthermore, the integration of transmission Fourier holograms that can be viewed in transmission against a point source and be projected by a laser beam, or of circular polarizers that can interact with liquid crystal structures on the same document, are reported at this conference by Paul Zientec et al (Note Printing Australia).[14]

The latent image is a relatively early example of the combination of intaglio printing and geometrical patterns to create optically variable effects when observed under an acute angle.[15] A novel application of intaglio printing is the use of OVI to create iridescent latent images.
A further example of the combination of security features is the printing of intaglio over OVDs (the LEAD strip, amongst others, on Bulgarian and Zaire bank notes).

5.1 Combination of Liquid Crystal Interference and Diffraction Effects

Recently various researchers have succeeded to integrate ISISs with DOVIDs.
A development by NHK Spring (Japan), reported at this conference by Itsuo Takeuchi et al, integrates diffractive and interference effects to form a so called CPL-gram, wherein CPL stands for circularly polarized light.[16] A semi-transparent thin film of polymerized cholesteric liquid crystals evokes the interference effect, while embossed diffraction gratings are integrated in this liquid crystal film.

In specular reflection, the liquid crystal film acts as an efficient Bragg mirror and reflects a waveband that shifts from gold to blue-green with angle of observation. Both this Bragg reflection and the light diffracted by the embossed features are

circularly polarized and can be efficiently extinguished by a reverse circular polarizer. Various effects of the CPL-gram are illustrated in figure 11.

(a) **(b)** **(c)**

Figure 11 – Integration of thin film interference and diffraction in a CPL-gram: (a) Bragg reflection of the polymerized liquid crystal layer, (b) Bragg reflection extinguished by a right circular polarizer, and (c) diffractive effects, outside Bragg reflection, integrated within the liquid crystal layer.

Such an integration of ISISs and DOVIDs, each requiring very different and advanced production technologies and, consequently, together rendering excellent anti-counterfeiting properties, is also interesting from an inspection point of view. The security of DOVIDs is based on their image effects – such as three-dimensionality, positive-negative contrast swaps and kinematic effects – rather than on their iridescent diffraction colors which are difficult to simply define and may even distract the attention of the observer from the relevant image effects. Contrary the security of ISISs, which – apart from the volume reflection hologram – rarely display complex image effects, is based on their well definable color shift. Therefore, the ergonomic combination of well defined color shifts with distinct image effects would synergistically increase the anti-counterfeiting value of the whole. Such combinations potentially are powerful verifiers.

5.2 Combinations of Iridescent Effects and Laser Engraving

Another approach to create verifiers is to integrate iridescent effects with laser engraving.
An example is the perforation of patterns consisting of micro holes through the paper substrate as well as the attached OVD, such as the perforation of the face value in Swiss bank notes. This feature is called Microperf (Orell Füssli, Switzerland); the holes have a diameter of about 100 μm and are only visible against the light.[4,18]

But, apart from its high technology and the associated anti-counterfeiting value, laser engraving has the additional advantage that it allows writing variable information. Consequently, not only a threshold against counterfeiting is raised, but also against forgery. Examples of this application are laser ablation of account numbers through DOVIDs on plastic cards (figure 12a), and laser perforation of account numbers through checks (figure 12b). In particular the latter feature efficiently thwarts forgery because it is very difficult to substitute the perforated number by another.

A recent development in this area is Brongers'invention of *transgraving*. [3,19] This technique involves the laser engraving of variable information in an OVD in such a manner that the variable information itself is iridescent again (figure 12c). Transgraving allows all combinations of interference and diffraction effects, such as variable ISIS information in a DOVID, variable DOVID information in an ISIS, etc. The combined effect of the variability of the information and its iridescence renders an excellent threshold against counterfeiting as well as forgery and may be considered to offer a powerful verifier.

Mention must also be made of a development by Flex Products (USA) called Lightgate™, reported at this conference by Roger W. Phillips et al. Lightgate integrates light interference by vacuum deposited thin films with light diffraction by embossed gratings and laser ablated variable information.[17]

(a)

(b)

(c)

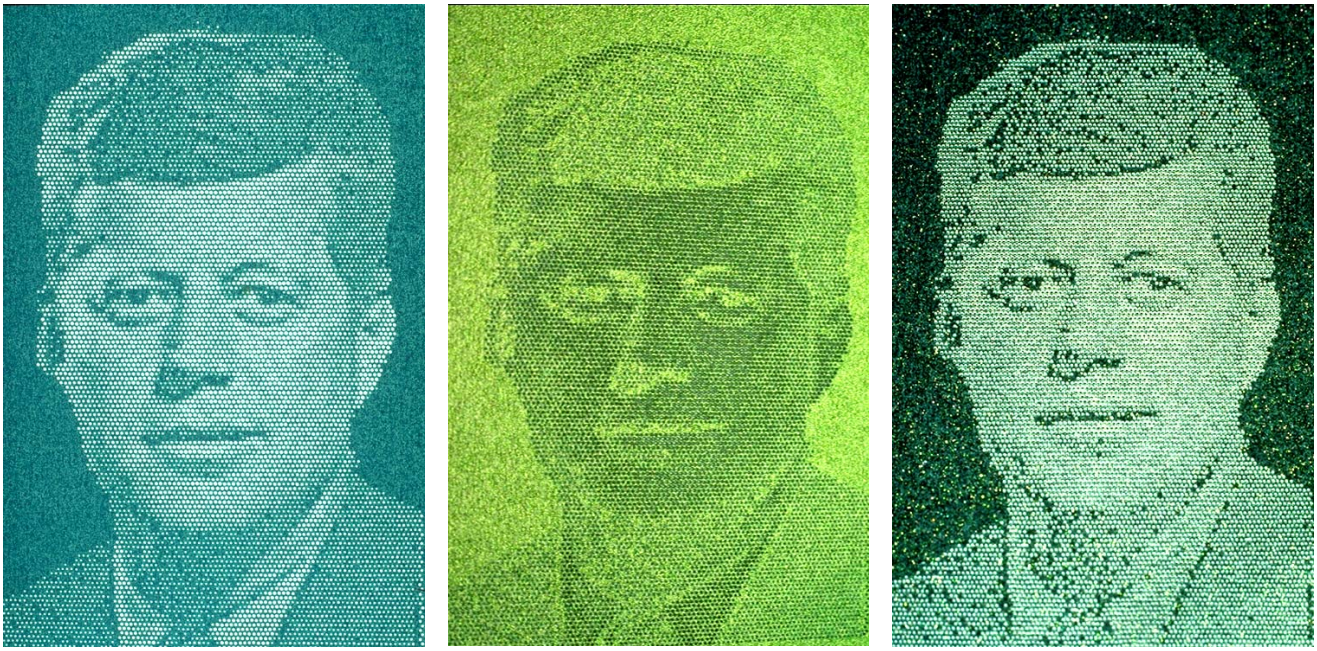
Figure 12 – Combinations of laser engraving techniques with DOVIDs:
(a) Account number engraved in the Kinegram on a Dutch guarantee card by laser ablation.
(b) Laser perforated slits (width 0.3 mm) constituting the account number through the Kinegram and the paper substrate of a Dutch Postcheque. The account number is printed directly above the perforation for easy comparison.
(c) Sample of a transgraved iridescent account number "2721978" in a Kinegram.

5.3 Combination of Iridescent Effects and ImagePerf

ImagePerf is an application of laser engraving developed by IAI (Industrial Automation Integrators, The Netherlands) especially against forgery of ID documents.[4] ImagePerf consists of a portrait perforated through the substrate of the document (e.g. plastic, paper) additional to the common portrait. The image modulation is achieved by either perforation frequency modulation or by perforation size modulation or a combination of the two. Depending on the production method, under observation in diffuse reflection, ImagePerf may be invisible or visible as a brownish negative image.
The forger that wants to (1) swap the original (integrated) portrait in the document now also must (2) remove the perforated portrait and (3) substitute it for a new perforated portrait. Although a determined forger may manage to complete these successive operations with more or less success, this is not at all a trivial matter because these require very diverse and exceptional skills, not often mastered by a single person.

However, this author is of the opinion that such a high skill forgery can be made virtually impossible by integrating ImagePerf with a suitable iridescent security feature, preferably an ISIS. In order to demonstrate the various possible optical effects, tests were carried out by applying ImagePerf in OVI (SICPA Security Printing, Switzerland), Securigrafix thin film foil, (Security Foiling, UK) and Kinegrams (OVD Kinegram Corp., Switzerland).
The perforated holes are conical in shape due to the cone shaped waist of the focussed laser beam. Thus, at the location of each perforated hole, the white substrate is well visible against the iridescent background. As a result, a few distinguished Optically Variable ImagePerf effects can be observed in combination with an ISIS:

1. Against a light background a positive image of the portrait is observed (figure 13a).
2. In specular reflection the iridescence of ISISs is brighter than the diffuse reflection of the white substrate, so that a negative image of the portrait is observed (figure 13b).
3. The negative image in specular reflection is seen against a background that shifts color with angle of observation.
4. In diffuse reflection the white of the substrate becomes brighter than the iridescent background, so that a positive image of the portrait is observed (figure 13c).



(a) **(b)** **(c)**

Figure 13 – ImagePerf portrait in a substrate printed with an OVI background: (a) positive image in transmitted light, (b) negative image in iridescent specular reflection and (c) positive image in diffuse reflection.

Obviously, for DOVIDs the second effect would not only display in specular reflection, but also in first order diffraction, while the 3rd effect is much more complicated and also involves variable image effects.

These optically variable effects are shown to their full advantage if the iridescent background is homogeneous. Therefore the ISIS type of OVD is more suitable than the DOVID type for combining iridescent effects and ImagePerf. The effects can be obtained utilizing DOVIDs, but the diffractive background must be more or less homogeneous and diffractive image effects must not confuse the OV ImagePerf effects.
The more efficient and specular the reflection of the OVD is, the more distinct the OV ImagePerf effects are with the angle of observation. Figure 14 shows the various OV ImagePerf effects for a thin film foil (Securigrafix, Security Foiling, UK).

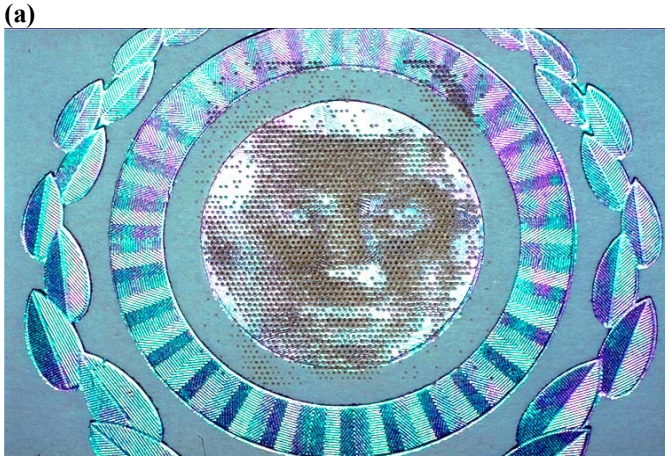
Summarizing, the combination of ImagePerf with ISISs displays a quartette of advantageous characteristics:

1. It displays a positive image in transmission. Because of the relatively large size of the perforated holes (up to 200 μm), observing this image not necessarily requires holding it against a light source. It can be simply observed by holding the feature against a white background while the image itself is less brightly illuminated.
2. It displays a well defined color shift with angle of observation (iridescence).
3. It displays a positive/negative image swap with angle of observation between diffuse and specular reflection.
4. It allows the writing of variable information that can be easily compared with information printed on the document.

These four effects of OV ImagePerf can all be observed under normal observation, depending on the background of the image and the angle of observation. Consequently, these characteristics can be inspected during normal handling of the feature.

The forger, confronted with OV ImagePerf, apart from carrying out the three diverse operations mentioned above, now also has to restore the iridescence of the originally perforated locations, in order to successfully swap the portrait. Therefore, OV ImagePerf, may be considered a powerful verifier that effectively protects against counterfeiting as well as forgery.

(a)



(b)

(c)

Figure 14 – ImagePerf portrait in a substrate with a Securigrafix thin film device:
(a) positive image in transmitted light,
(b) negative image in specular reflection, and
(c) positive image in diffuse reflection.

6. DISCUSSION AND CONCLUSIONS

The value of security features is equally based on (1) the technological threshold they raise against counterfeiting, imitation and forgery, and (2) the human factors involved with their inspection. It appears that many classic security features fail in either one or both properties. Modern security features potentially come to meet these technological and ergonomical requirements. These technological requirements are based on nano-technology that often is beyond the capability of criminal organizations, while the ergonomical requirements are based on the obvious and uncommon optical effects displayed.
Otherwise, two opposing processes are in force. One is the tendency to increase the visual complexity of DOVIDs in order to hamper counterfeiting, a measure that at the same time hampers ergonomic inspection.[20] The other is the increasing access achieved by criminal organizations to corrupt manufacturers and their equipment.
Some R&D institutions have understood the message that betting on one horse may cause unacceptable losses in the long run. Their response has been the synergistic merging of various nano-security features in order to utilize the best of all of these. Such features synergistically combine three optically variable effects: well defined color shifts, well defined variable image effects and variable personal information. If well designed, such combinations optimally comply with the requirements of high technology as well as human factors and will function as powerful verifiers against counterfeit and forgery for many years to come.

ACKNOWLEDGEMENTS

The following persons are gratefully acknowledged for their support:
J.D. Brongers (Dutch Banking Institution) for providing samples of transgraving and making counterfeit bank notes available for investigation, A. Bleikolm (SICPA Security Printing, Switzerland) for providing OVI samples, C. Hope (Security Foiling, UK) for providing Securigrafix samples, W. Hospel (Industrial Automation Integrators, The Netherlands) for laser engraving ImagePerf in various iridescent samples, Chr. Saxer (OVD Kinegram Corp, Switzerland) for providing Kinegrams, R. van Spijk (Police Rotterdam-Rijnmond, Forensic Crime Squad, The Netherlands) for making counterfeit holograms available for investigation, and T. Sugahara (NHK Spring Co., Japan) for providing CPL-grams.

REFERENCES

1. K.J. Schell, The historical development of security printing: design and technology, *Optical Document Security*, ed. R.L. van Renesse, Artech House, London/New York, 1998.
2. R.L. van Renesse, Iridescent optically variable devices, a survey, *Optical Document Security*, ed. R.L. van Renesse, Artech House, London/New York, 1998.
3. J.D. Brongers, Search for effective document security by 'inventioneering', *SPIE vol. 3314, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques II*, San José, Ca., 29-30 January, 1998, p. 29-38.
4. W. Hospel, Application of laser technology to introduce security features on security documents in order to reduce counterfeiting, *SPIE vol. 3314, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques II*, San José, Ca., 29-30 January, 1998, p. 254- 259.
5. K. Schell, LEAN, the acronym for Laser Etched Aqua Number, *SPIE vol. 3314, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques II*, San José, Ca., 29-30 January, 1998, p. 260-267.
6. J. van den Berg, New optical security features in plastic documents, *SPIE vol. 3973-18, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques III*, San José, Ca., 26-28 January, 2000.
7. R.L. van Renesse, Human factors of first line security, *SPIE vol. 3314, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques II*, San José, Ca., 29-30 January, 1998, p. 97-108.
8. R.L. van Renesse, The human factor of security, *Proc. International Conference on Document Counterfeiting Protection*, San Francisco, CA, January 28-29, 1999.
9. R.L. van Renesse, Human factors of card security, *Chip Card: Trump Card? – Consequences for investigation and prosecution*, ed. F. Knopjes and P.J. Lakeman, National Criminal Intelligence Division, The Hague, Netherlands, 1998, p. 37-58.
10. R.L. van Renesse, Verifying versus falsifying bank notes, *SPIE vol. 3314, Conference on Optical Security and Counterfeit Deterrence Techniques II*, San José, Ca., 29-30 January 1998, and p. 71-85.
11. OEM Windows 98 copied (too) soon after release, *Authentication News*, Reconnaissance International Ltd., volume 4, no. 8, November 1998, p. 1-2.
12. H.W. Nusmeier and J. Wotte, Optical Security in Laminates, *Optical Document Security*, ed. R.L. van Renesse, Artech House, London/New York, 1998.
13. P. Zientec, Polymeric self-authenticating banknotes, *SPIE vol. 3314, Conference on Optical Security and Counterfeit Deterrence Techniques II*, San José, Ca., 29-30 January 1998, and p. 272-274.
14. B. Hardwick and A. Ghioghiu, Guardian substrate as an optical medium for security devices, *SPIE vol. 3973-19, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques III*, San José, Ca., 26-28 January, 2000.
15. Robert G. Hutton and Trevor Merry, *Documents of value including intaglio printed transitory images*, American Bank Note Company*, patent number US 4,033,059*, filed 18 April 1975, published July 5, 1977.
16. Itsuo Takeuchi et al, CPL-gram: An advanced machine readable OVD that is obtained by combining diffraction gratings and liquid crystals, *SPIE vol. 3973-26, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques III*, San José, Ca., 26-28 January 2000.
17. Roger W. Phillips and Richard Bonkovski, Security enhancement of holograms with interference coatings, *SPIE vol. 3973-33, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques III*, San José, Ca., 26-28 January 2000.
18. J. Zintzmeyer and J.R. Coleman, Security document with security marking, Orell Füssli Banknote Engineering Ltd., Zürich, *patent number WO 97/18092*, publ. 22 May 1997.
19. J.D. Brongers, Method for applying a security code and article, such as a cheque, guarantee card, credit card, identity card or component of a motor or machine, ING Groep N.V. Amsterdam, *patent number EP 0868314 B 1*, filed 9 December 1996, published 4 August 1999.
20. R.L. van Renesse, Security design of valuable documents and products, *SPIE vol. 2659, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques*, San José, Ca., 1-2 February 1996, p. 10-20.