Ordering the Order

A survey of optical document security features

Rudolf L. van Renesse

SPIE Conference on Practical Holography IX
San Jose, California, 5-10 February 1995
paper # 2406-33

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

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

Ordering the order - a survey of optical document security features

Rudolf L. van Renesse*

ABSTRACT

Until the appearance of the colour copier, security features were optically invariable devices (OIDs). Nowadays, deceptive colour copies of OIDs can be made. Optical variability however, is unattainable by the colour copier. Optically variable devices (OVDs) are either based on specular reflection (metallic foils), diffraction (holograms, etc.) or interference (thin films, Bragg structures, etc.). A classification of OIDs and OVDs is presented. It is proposed that the degree of microstructural order of an optical feature is an approximate measure of its practical value for document security.

Keywords: valuable document, document security, security device, optically variable device, OVD.

1. INTRODUCTION

From of old issuers of valuable documents have sought to secure these against forgery and counterfeit by utilising security features that revealed such violations at a glance. With the rise of technology, security devices advanced and their number grew steadily. But the craft of the criminal developed with it. The history of document security is one of a continuous struggle to stay one step ahead of the fraud.[1] The wax seal of a document with a unique emblem is an early mediaeval example of document security, the watermark and intaglio printing are more recent examples and iridescent features like holograms form the latest sprout on the ever growing security branch. The number of document security features thus has become virtually countless and their survey would fill several books. As many of these features are of an optical nature, even the confinement to optical security features leaves us with an abundance of devices that can be applied to the paper of the document or can be printed or otherwise adhered thereon.[2]

Until the appearance of the colour copier, based on the subtractive mixture of yellow, magenta, cyan and black pigments, all security features were optically invariable devices (OIDs), i.e more or less diffusely reflecting devices, mostly being independent of the angle of illumination and observation. Such OIDs are generally copied most easily by advanced colour copiers and other four colour reproduction systems. In principle however optical variability, like specular reflection and iridescence, is unattainable by four colour copy techniques. In the last few decades a profusion of optically variable devices (OVDs) was developed to thwart four colour copy fraud, embossed holograms being the first. Since, many different kinds of OVDs have been developed and applied to valuable documents. They are all based on either specular reflection (metallic foils), diffraction (holograms, kinegrams, pixelgrams, etc.) or interference (thin films, Bragg structures and liquid crystals).
This wealth of both OIDs and OVDs raises a difficulty for the manufacturer of valuable documents, who has to make an intelligent choice in order to attain optimal document security. To sustain security design, security models of the document must be developed and a security analysis performed. A further organisation of security features with respect to their benefit for document security appears to rely on on their structural order. In this paper it is proposed that the degree of structural order incorporated by an optical security feature is a rough measure of its security value.

To appreciate the concept *security value*, or *degree of security*, it must be realised that security involves the total of three domains: the security product, the message it conveys and its inspection. Each of these domains is covered by various disciplines as schematically illustrated in figure 1. Only if all three domains are adequately dealt with, security will be optimum. In the following the subject will be treated with first line inspection in mind, that is inspection performed merely with the sense-organs without additional tools. An example is the inspection of a bank note by the-man-in-the-street. Once utensils are required, the inspection is considered second line.

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

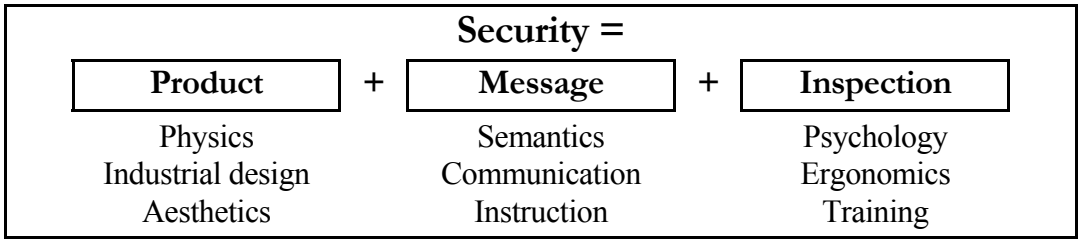


Figure 1 - Security as a total of three domains.

2. ORDERING THE ORDER

A quick look at the extensive gamut of security devices reveals great differences in the fineness of their structural order. On the low end we find coloured images, printed with diffuse pigments, which are only ordered in the visual millimetre scale and, on a microscopic scale, have no order at all. On the high end we find optically variable devices that are highly ordered on a submicron scale. As the fineness of the structural order increases, not only do the optical effects become more conspicuous, but also the degree of security tends to increase. This approximate rule is illustrated in the security-order space of figure 2. In the following a representative gamut of optical security devices will be discussed in order to support this first line inspection rule.

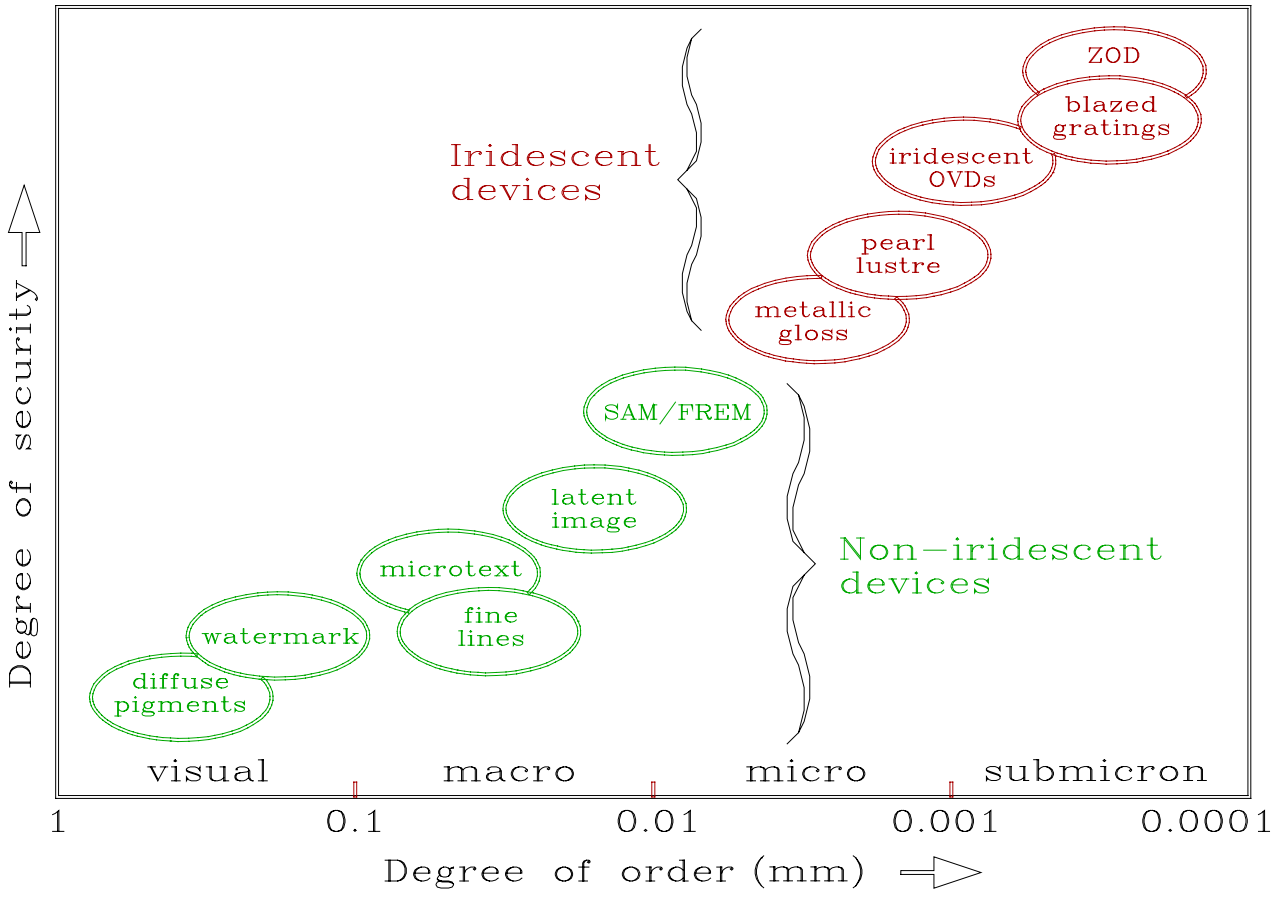


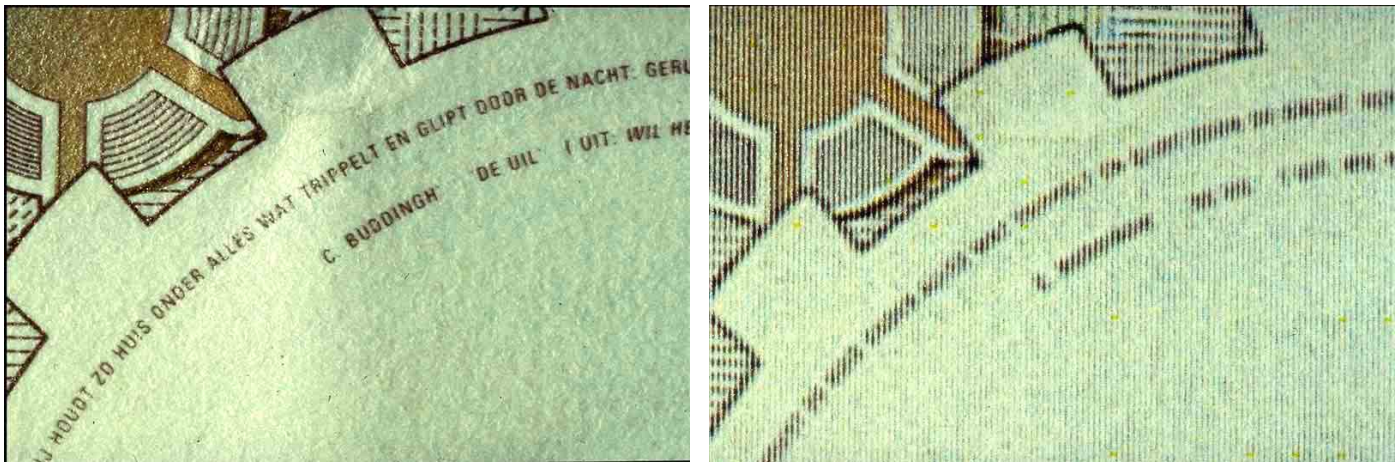
Figure 2 - The security-Order space

2.1 Non-iridescent security devices

Diffuse colour printing - In former days counterfeiting valuable documents demanded a certain know how and specialist equipment. Unfortunately, from a security point of view, nowadays each lay person, in a trice, can manufacture deceptive colour imitations of documents. Although colour can be well communicated as well as inspected, as a security product coloured images have therefore become of very low value. This value can be related to the low order that coloured images possess in the spatial frequency domain.

Watermark - The mould-made watermark is a continuous tone image that can be viewed in transmitted light. It consists of low spatial frequency variations in paper thickness and density, which create an image integrated in the paper mass of the document. The diffuse reflection of the watermark is visible as a negative image because the thick portions of the paper have a higher diffuse reflection than the thin portions. The watermark has therefore been considered as the first OVD invented.[3] Of old, the positive/negative switching continuous tone watermark image has proved markedly counterfeit resistant, and the watermark still is considered an excellent security product. The essential continuous tone properties of the watermark, however, appear to be difficult to communicate. Even poor imitations tend to be accepted by the public. The security value of the watermark is further degraded by what has been called the *embarrassment factor*.[4] Consider the embarrassing situation of the 'man at the counter' manifestly holding up a security document against the light in order to view the watermark; such handling will probably be considered an offense by the customer. Therefore, document inspection generally has to be casual and more or less unobtrusive. For such psychological reasons advanced security devices like the watermark appear to be virtually ineffective.[5] In spite of its high security potential the watermark, for psychological reasons, has a relatively low first line security value. However, once suspicion arises and thus the embarrassment factor is eliminated, the watermark will prove to be an excellent security hallmark. The question remains: "what will arouse the suspicion of the recipient?". Obviously not the highly valued watermark.

Microtext - Microtext consists of very small lettering, beyond the 300-600 dpi resolution of the usual scanner and colour copier. Figure 3a gives an example of microtext on a Dutch one hundred guilder note. The height of the letters is only 0.3 mm, so the spatial frequency of this feature belongs to the macro domain. Figure 3b shows the colour copy, with the microtext having become completely illegible.



(a) (b)

Figure 3 – (a) Microtext and fine lines in a detail of a DFL 100 note and (b) a copy made on a high-resolution colour copier.

Again, like the watermark, microtext as such may be considered an excellent security feature, that can be easily communicated. However, a message consisting of 0.3 mm letters is below the resolving power of human vision and its verification therefore requires a magnifier. This makes microtext a second line security feature with a security value comparable to that of the watermark.

Fine lines, guilloches - Fine line security patterns are ornaments that, like microtext belong to the macro domain. The complexity of fine line and guilloche patterns aims at hampering counterfeiting. Their fineness is beyond the resolution of the usual scanner, as becomes evident from figure 3. As such, these features serve security well, but from a communication standpoint they offer little or nothing: their ornamental intricacy contradicts adequate communication. Moreover, their inspection requires a magnifier. This is why

these structures are ranked below microtext in the security-order space.

(a)

(b)

(c)

Figure 4 - a) Austrian 5000 Schilling bank note, b) Enlargement of the latent image, c) latent image under oblique observation.

Latent image - Intaglio printing consists of tactile, raised lines of which the ink is transferred to the document under enormous printing pressure. It is a craft confined to security printers so that the chance on intaglio counterfeiting is remote. The latent image (not to be confused with the photographic latent image) consists of a fine intaglio pattern that renders the printing non-iridescent optical variability.[6] The effect is based on the distinct relief of the intaglio lines. A latent image may consist of a foreground of parallel lines and a similar background being aligned perpendicularly to the foreground. The separate lines will not be resolved by the human eye, so that under normal observation both foreground and background merge into a uniformly coloured ornament. An enlarged example is presented in figure 4b.

Under oblique observation, foreground and background separate in contrast because the raised lines of one pattern shield the white paper from view while between the lines of the other pattern the paper remains visible (figure 4c). Thus, depending on the orientation of the pattern to the observer, the foreground will be darker than the background or vice versa. The intaglio relief cannot be copied and thus copies will entirely lack the optically variable effect. The latent image therefore is an excellent security feature, while the optically variable effect can be well communicated. Inspection can be performed in first line, without additional tools. The disadvantage, however, of the latent image is, that its inspection will tend to evoke the embarrassment effect. This is why the latent image does not score very much higher on the security scale than microtext or fine lines.

SAM/FREM - The function of the combination of Screen Angle Modulation (SAM) and Frequency Modulation (FREM) has been described[7,8] and illustrated[8] comprehensively elsewhere.

SAM is a composition of minimal lines, with a spatial frequency of about 4 lines per millimetre and an angular rotation that is a function of the density of the original image. As an example figure 5a shows an enlarged part of a continuous tone original, while figure 5b presents its SAM counterpart: horizontal lines correspond to black, vertical lines to white, intermediate densities are represented by corresponding angular rotations.

The spatial frequency of SAM causes aliasing (moiré interference) with the spatial frequency of photodiode arrays of common scanners so that gross disturbances will appear in a copy. These disturbances may take the form of an obvious message like "void" or "false". To have an optimum effect, SAM images require wet offset printing with printing accuracy in the micro range. This is why a one-on-one SAM example cannot be reproduced in these proceedings. However, certain digital filter operations (uniform filtering), also available on colour copiers, allow the elimination of these intended disturbance effects. This is why SAM is preferably combined with FREM. A frequency-modulated image of figure 5a is presented in figure 5c. It consists of randomly distributed minimal dots, having a spatial frequency that is a function of the original density. Application of uniform digital filters, to avoid the 'SAM effect', will markedly deteriorate the FREM image, so that the fraudulent operation becomes obvious to those well informed of the expected image degradations. The SAM/FREM combination is effective against occasional fraud, the message it communicates is obvious in first line, while its inspection does not evoke the embarrassment effect. This is why SAM/FREM is ranked on top of the non-iridescent security devices in the security-order space.

(a)

(b)

(c)

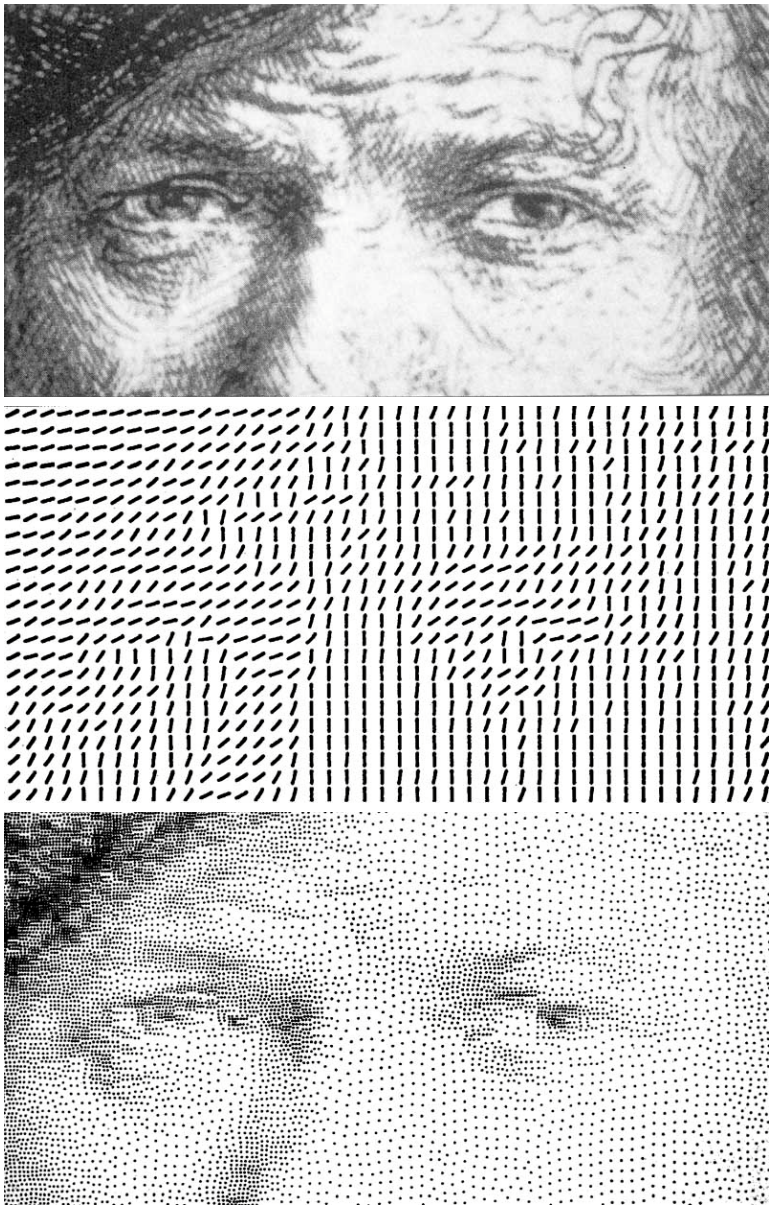


Figure 5 - a) continuous tone, b) SAM, c) FREM. (From S. Spannenburg[8])

2.2 Iridescent security devices

As soon as the structure of matter becomes ordered on the scale of the wavelength of light, optically variable effects like metallic gloss and iridescent effects result. Iridescent colours vary with the angle of observation and illumination like the colours of a soap bubble, an oil film or a peacock feather. The colour copier, or any other four-colour reproduction system, is by no means a match for such lustrous and iridescent effects. Iridescent colours may come about by two different phenomena; *light diffraction* at regularly ordered, fine line structures (gratings) and *light interference* at regularly ordered stacks of layers. Figure 6 gives a schematic overview of these effects as they occur in nature and as they are applied to document security.

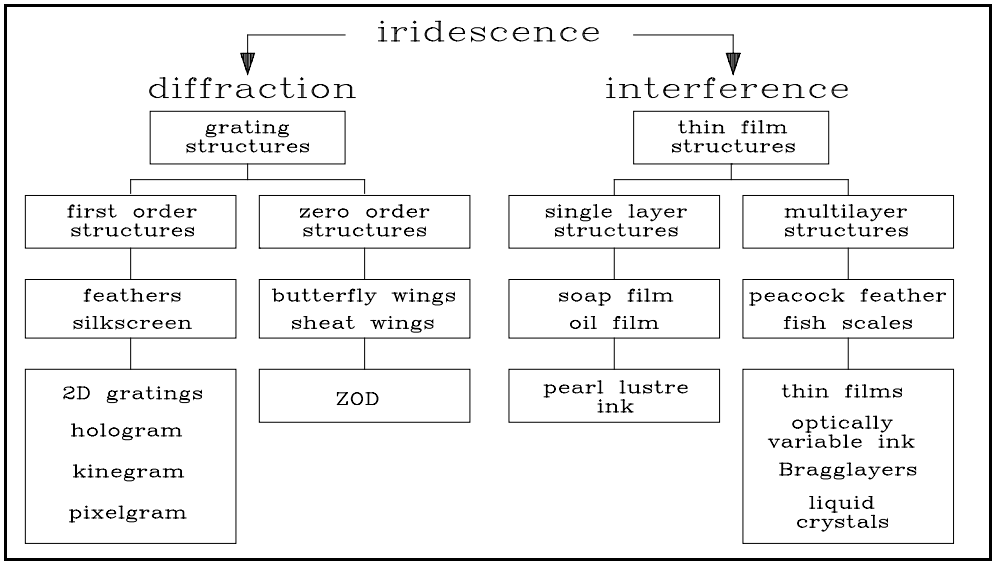


Figure 6 - Iridescence in nature and applied to document security.

Metallic gloss - Examples of metallic foil printed ornaments are found on the new English £50 (silver) and Dutch *f*100 (gold) bank notes. Other examples are the silvery lustrous window threads on German bank notes. The sheen of these features is rather conspicuous and requires no second glance in first line inspection. Moreover, the characteristics of these features can be well communicated. However, metallic foils are commercially available without restriction while foil printing does not require great skill. This is why metallic gloss is ranked lowest in the iridescent area of the security-order space.

Pearl lustre - Pearl lustre inks are composed of a transparent varnish to which tiny mica flakes are added that carry a single thin interference film of TiO_2. A layer of Fe_2O_3 or Cr_2O_3 may be applied, either singly or in combination with TiO_2, to produce bronze and gold effects. The high refractive index of the TiO_2 film renders the ink a relatively high reflection, but at the same time this causes the optical variability of the interference colours to be negligible: a variation in angle of illumination or observation has no appreciable effect.[9,15] If it is further taken into consideration that pearl lustre pigments are commercially available without restriction and that such inks can be easily composed and printed by simple means, it will be appreciated that pearl lustre printing does not rank very much higher in the security-order space than metallic devices.

Iridescent OVDs - As it appears from figure 6, a large range of iridescent OVDs exists: diffractive as well as interference types. Except pearl lustre, all of these have a prominent optical variability in common, which makes them deviate manifestly from ordinary printing, but also from metallic features.
The diffractive type, such as the hologram[10,11,15], is found on a variety of credit cards and other valuable documents. Other examples are the kinegram[11,12,15], amongst others found on the Austrian 5000 Schilling and the 500 Finnish Mark, and the prototype of the pixelgram[11,15] (Catpix I) on the commemorative $10 Australian plastic bank note.
The multi-layer interference type is represented by several security features. Thin film devices are applied to Canadian bank notes ($20, $50. $100, $1000), British Columbia drivers' licences and identity cards.[13-15] Optically Variable Ink (OVI)[11] consists of a transparent carrier to which microscopic flakes of thin interference film stacks are added. Examples of OVI are found on the German DM500 and DM1000 notes and the French FF50 note. Another multi-layer example is the Bragg structured liquid crystal polymer device, which has found applications on passports, visa, ID cards, etc.[16] In general these highly iridescent security features are available only for registered security applications and their origination requires considerable technical know how.
If it is taken into account that inspection of such features, if well designed, will only take a glance, it will be understood why iridescent OVDs are ranked high in the security-order space.

Blazed gratings - It is known that holographic copies of diffractive devices like holograms can be made. Various defences against this type of counterfeiting have been proposed and realized.[17-19] An interesting defence is based on the fact that holographic copies will necessarily result in grating reliefs having a more or less sinusoidal cross section. Such gratings will diffract light into plus and minus first orders of equal intensity. Asymmetrical gratings, e.g. blazed gratings, however, will display plus and minus first orders of greatly differing intensities. This effect can be advantageously made operational for security designs by combining 'left' and 'right' blazed gratings, as illustrated in figure 7.
For instance a pictorial design consisting of a left blazed foreground and a right blazed background, will display a positive-negative contrast conversion if rotated over 180° (see figure 7).

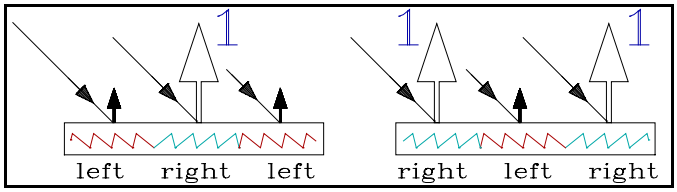


Figure 7 - Asymmetric first order device: effect on first order diffraction by 'left' and 'right' blaze.

Such gratings may be manufactured by various techniques, like chemical differential etching, ion beam etching and electron beam lithography.[12] It is impossible to create such asymmetric images by common holographic techniques and holographic copies will likewise lack the effect. Obviously the blaze renders the grating submicron detail, which shifts this device to the right in the security-order space, while its unique asymmetric behaviour renders these non-holographic devices increased security in first line. The mass production, however, of gratings with submicron detail will require great proficiency of the embosser. Up to the present a successful application of asymmetric gratings to security documents has not been reported.

Zero order devices - Common diffractive devices require inspection of their first order diffraction using light sources of limited extension. Under completely diffuse illumination, like an overcast sky, such devices do no longer show any three-dimensional or iridescent effects because all diffraction orders will overlap to result in a fuzzy, white reconstruction. This may be considered a particular drawback of all first order devices.
A diffractive device that displays a completely different behaviour is the zero-order device (ZOD).[20]

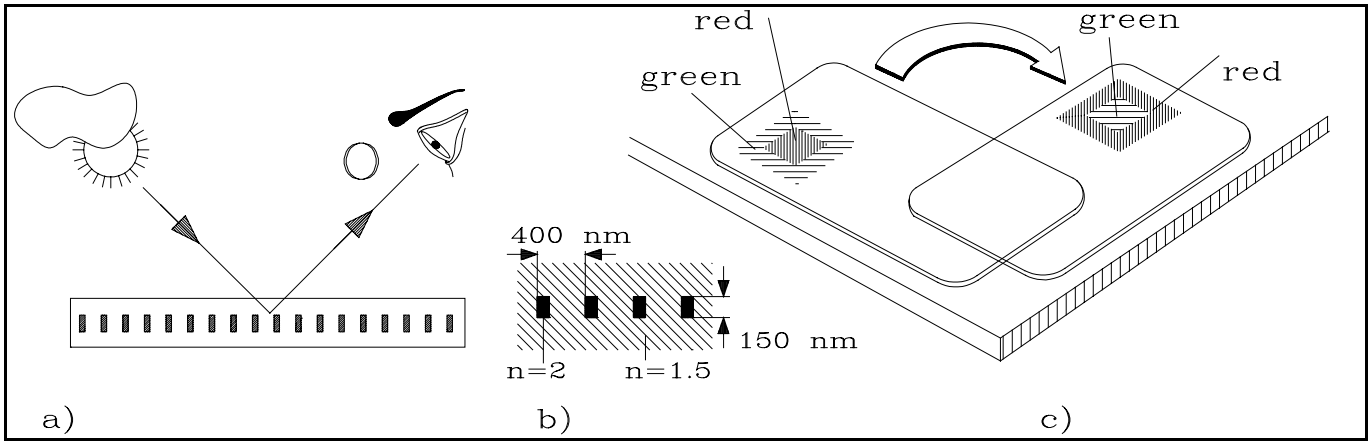


Figure 8 - a) Zero order reflection, b) typical grating dimensions, c) anisotropic performance. (After Gale[20])

The ZOD grating period typically is so small ($<\lambda$) that no first orders exist at normal incidence illumination (figure 8a). At non-normal illumination a first order reflection may be displayed at angles far removed from the zero order. The ZOD consists of a three-dimensional high refractive index structure embedded within a low refractive index matrix (figure 8b). Holographic copying of such structures is not possible because this does not reconstruct the typical three-dimensional properties of the submicron grating. Mass production of the ZOD involves high resolution laser interference lithography, dry etching techniques to manufacture the embossing shim, the continuous embossing of plastic film, deposition of the high index material and overcoating with a transparent polymer film. Examples of natural ZODs are the iridescent colours on the wings of the Morpho butterfly and on the sheat wings of some beetles, like the scarabea.
The ZOD shows strong polarisation and bright anisotropic iridescent behaviour in zero order observation (specular reflection): when rotated over 180° in its own plane, for instance a red metallic reflection may change into a green reflection and vice versa (figure 8c). The ZOD reflection is very bright and well visible under diffuse illumination as well as under illumination from a point source. As no metal is present in the structure, outside the reflection waveband the ZOD is completely transparent and it may therefore be applied as a security overlay combining a high transmission as well as a strong iridescent reflection. Due to the combination of a sophisticated production process which renders the ZOD high anti-counterfeiting resistance, highly unique and conspicuous iridescent effects and a high transparency, this security device ranks highest in the security order space. The submicron details will require great proficiency of the embosser. No commercial application of the ZOD to security documents has yet been reported.

3. DISCUSSION

An aspect that is not investigated, but nevertheless of great importance, is the price/performance ratio of a security feature. If this ratio can be established and is taken into account, a different ranking may result.
Naturally the order discussed is no more than a semi-quantitative one, a general trend rather than an exact classification. In order to really establish the value of a security feature it must be evaluated as it is integrated with other elements in a specific valuable product. Such an evaluation of a security design demands at least a fraud risk analysis, a list of requirements, a security model and adequate experiments; together these allow to establish if the product meets the requirements.[21]

Finally, it may be mentioned that an entirely different type of security features exists: random devices. These combine a complete lack of order with a high degree of security and hence find a place in the upper left corner of the security-order space. Many are based on random fiber or particle distributions incorporated in the valuable product or on its unique random surface texture. An interesting, recently invented example of random security features makes use of a three-dimensional nonwoven fibre structure.[22-24] By nature, random devices are of the second line, machine readable type and they cannot be simply compared with the first order devices discussed above.

4. REFERENCES

1. Schell, K.J., "Security printing, a part of optical security systems or vice versa?", Symposium Optical Security Systems, Zurich, Switzerland, October 14-16, 1987.
2. Renesse, R.L. van (ed.), Optical Document Security, Artech House, London/ Norwood 1994, ISBN: 0-89006-619-1.
3. Camus, M., e.a., "Security papers and special effects", ref. 2, chapter 5.2.2.
4. Cassidy, J.F., "Authentification without embarrassment - a unique, novel, paper-based method of document verification", Intergraf International Security Printers Conference, Vouliagmeni, Sicily, 6-8 June 1991.
5. Renesse, R.L. van, e.a., "Detection and integration of security devices in documents", SPIE vol. 1210 - Proc. of the Symposium on Optical Security and Anticounterfeiting Systems, 15-16 January 1990, Los Angeles, California.
6. Renesse, R.L. van, "Noniridescent Optically Variable Devices", ref. 2, chapter 15.2.2.
7. Spannenburg, S, "Frequency modulation of printed gratings as a protection against copying", SPIE vol. 1509, Holographic Optical Security Systems, 14-15 March 1991, The Hague, The Netherlands, p. 88-104.
8. Spannenburg, S., "Modulation of printed gratings as a protection against copying", ref. 2, chapter 7.
9. R.L. van Renesse, Introduction to optical document security, ref. 2, chapter 3.3.2.
10. Colgate, G. "Document protection by holograms", ref. 2, chapter 8.
11. Renesse, R.L. van, "Iridescent optically variable devices: a survey", ref. 2, chapter 11.
12. Moser, J.-F., "Document protection by Optically Variable Graphics (Kinegram)", ref. 2, chapter 9.
13. Dobrowolski, J.A., Ho, F.C., and Waldorf, A.J., "Research on Thin Film Anticounterfeiting Coatings at the National Research Council of Canada", Applied Optics, vol. 28, no. 14, p. 2702-2717, 1989.
14. Dobrowolski, J.A., "Optical thin-film security devices", ref. 2, chapter 12.
15. Original samples of pearl lustre print, hologram, pixelgram, kinegram and thin film features are added to the appendix of ref. 2.
16. Renesse, R.L. van, "Liquid crystal security devices", ref. 2, chapter 13.
17. Colgate, G., "Document protection by holograms", ref. 2, chapter 8.
18. McGrew, S.P., "Hologram Counterfeiting, Problems and Solutions", SPIE vol. 1210, Optical Security and Anticounterfeiting Systems, 15-16 January 1990, Los Angeles, California, p. 66-76.
19. Wood, G.P. and Woodd, P.H.L., "The Williams and Clapper effect in anti-counterfeit security holograms", OSA Annual Meeting, Dallas, Texas, October 2-7, 1994.
20. Gale, M.T., "Zero-order grating microstructures", ref. 2, chapter 10.
21. Tadema Wielandt, R, "The evaluation of document fraud resistence", ref. 2, chapter 2.
22. Renesse, R.L. van, "3DAS - Identification and Verification of Cards and Labels", Intergraf Conference, Prague, 12-14 May 1994.
23. Renesse, R.L. van, "Noniridescent Optically Variable Devices", ref. 2, chapter 15.3.3.
24. Renesse, R.L. van, "3DAS: a 3Dimensional structure Authentication System", Proceedings of ECOS95 European Convention on Security and Detection, 16-18 May 1995, Brighton, UK.