Paper based document security - a review

Rudolf L. van Renesse

ECOS 97
European Conference on Security and Detection
Commonwealth Institute, London, 28 – 30 April 1997
Conf. Publ. no. 437, pp. 75 – 80

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

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

PAPER BASED DOCUMENT SECURITY - A REVIEW

ECOS 97, London, 28 – 30 April 1997

Rudolf L. van Renesse*

1 INTRODUCTION

The list of paper based valuable documents is nearly interminable and extends from *high security* passports, shares and bonds via *medium security* stadium admission tickets and gift vouchers to *low security* purchase authorisations, management stationery, receipts and bank forms. Otherwise, the fact that some types of document are considered 'low security' does not mean that their abuse is not likely to result in considerable profit for the criminal as well as substantial damage for the rightful owner of such documents.

Apart from the security categories high, medium and low, categories of value may be distinguished [1]:

- *Direct value* of documents that have an unconditional and immediate value, like banknotes and gift vouchers.
- *Indirect value* of documents that serve to support a transaction or a right, like passports and diplomas.
- *Conditional value* of documents that become negotiable only after performing mandatory inspections, like cheques, trading stamps and admission tickets.
- *Informative value* of documents like confidential reports and examination papers.
- *Fictitious value*, for instance the value of stationery of recognised institutions and companies.

The security approach not only depends on the security category, but also on the category of value of the document to be protected. In the case of direct value, security measures are mainly applied to the document itself. Protection of documents with conditional value depends on the relationship between document and inspection. Documents with indirect value or informative value will mostly be inspected upon issue. The fictitious value of documents can only be (partly) protected by appropriate security management. It may be worthwhile to consult the book "Security documents" [1] on these matters.

Of old, ingenious countermeasures are taken against abuse of valuable documents. Extensive studies are devoted to the enormous variety of existing security features and security measures [2-5], including a growing number of biometric techniques [6] while various relevant periodicals appear [7-9]. Unfortunately, the list of methods in which valuable documents are abused seems at least as long as the list of existing countermeasures.

Inspection of documents and valuable products for authenticity can be divided into three categories:

First line inspection - The inspection of the document or product with the human senses only without additional equipment. First line inspection is aimed at unveiling counterfeits and forgeries (alterations) using *public security features* like watermarks, tactile intaglio printing, etcetera.

Second line inspection - The inspection of the document or product with the means of additional tools like a magnifier, an ultra violet source, a bar code reader, etc. In these cases the second line inspection requires a human inspector to judge the results of the inspection. In the case of automatic teller machines (ATMs) and suchlike equipment, the inspection is fully automated.

Third line inspection - The inspection of the document or product in laboratory conditions, using advanced know how, sophisticated means (spectrometers, microscopes, infrared radiation, etc.) and dedicated inspection facilities. Third line inspection is mainly limited to forensic laboratories and only of practical value once suspected documents have been seized.

It can be argued that first line inspection has a few psychological drawbacks [10] and that machine inspection grants considerably higher security. This may be true, but a major drawback of machine inspection is the current lack of standardisation and it cannot be conceived how the many ingenious systems that have been invented can be put to general use. Obvious exceptions are the magnetic stripe and the chip card. However, there is little refuge in providing valuable documents and products

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

with hightech and highly secure machine readable features if not, first of all, their first line public defence is adequately covered. Claiming ultimate security based on second line technology is of limited value. Whether we will see the much debated cashless community or not, this thesis will hold. First line security, therefore, will be the main subject of this paper.

2 PAPER SECURITY

First line security may be embedded in the paper (section 2.1), integrated in the printed artwork (section 2.2) or appended to the document as metallic or iridescent features (section 2.3).

2.1 security features embedded in the paper mass

Paper security may be achieved by the addition of certain products to the paper during its manufacture. A review on security papers is given in reference [11]. The classic example is the *watermark*, consisting of thick and thin areas in the paper that, in transmission, respectively appear darker and lighter than the surrounding paper. Coloured *security fibres* embedded in the paper (e.g. US$ 100) are another example. Security fibres may otherwise be metallic or photochromic.

Relatively new are *security threads* completely embedded in the paper and only visible in transmission as well as the so called *window thread* which is partly embedded in the paper mass and partly appears at the paper surface as a metallic feature (e.g. German banknotes). A small feature of a few millimeters diameter, held by the surface fibres of the paper mass is the *planchette*, either coloured as on Canadian banknotes or iridescent as on the new Dutch 100 and 1000 guilder banknotes. Features like security fibres, threads and planchettes may also be luminescent under ultraviolet radiation. Microprinting may be added to security threads and planchettes in order to enable second line inspection on authenticity.

The paper embedded features discussed above are primarily aimed at raising counterfeit resistance. In order to raise thresholds against forgery (alteration), chemicals may be added to the paper that serve as an indicator of chemical and solvent attacks.
A chemical attack (chemical erasure) may be aimed at bleaching information so that false information can be unobtrusively substituted. A series of inorganic oxidising agents is at the service of the forger to allow effective bleaching of various types of ink, like that of ballpoints, fountain pens, and felt-tipped pens. Such bleaching agents are widely available. Certain chemical indicators deposited in the paper mass provide a defence. These indicators react to oxidising agents to form an indelible stain of the paper that acts as a clear indication of tamper. The stain response should be resistant against chemical removal with reducing agents.
A solvent attack may be aimed at completely washing out certain types of print (like name, address and other variable information on cheques) with the aid of a variety of organic solvents. *Solvent indicators* may be added to the paper that react to give a strongly coloured bleeding of a dyestuff in the paper. Such reactants must obviously withstand attempts to washing with an excess of solvent.
Adding a coating to the paper that contains encapsulated chromogens and colour developers such as in self-copying paper may expose mechanical erasure of information by scratching and rubbing. When pressure is applied, the capsules break and a coloured reaction between chromogen and developer results. A disadvantage of such *pressure indicators* is that they may react to give false stains when inadvertent mechanical pressure is applied to the paper. Another method to expose mechanical erasure is to create a thin zone in the paper that is vulnerable to mechanical attacks, for instance at the location of the payable amount of a cheque. Mechanical erasure will likely result in local destruction of the paper. Again another way to hamper mechanical erasure is to make the paper fluffy, so that the paper surface becomes easily disrupted.
In some cases the document is predisposed to an attack by *paper splitting*. This is particularly the case with laminated documents. A possible defence comprises of the implementation of weak parts in the paper. These may consist of patterns of thin paper zones or of patterns slit nearly through the thickness of the paper. These weak zones may react to splitting attempts by irreparable paper tears.
The perforation of paper is utilised to permanently mark the paper, like numbers are perforated in many passports. A laser perforated account number, for instance, is found through the kinegram on the Dutch Postcheque.

2.2 security features in the printed artwork

The printing of a large variety of patterns and substances on the surface of the paper may result in additional security against counterfeiting as well as forgery (alteration). Some of these printings can penetrate the paper mass to add further security.

2.2.1 anti-counterfeiting printed patterns. The number of printed security patterns is abundant.
Some patterns protecting documents against counter-feiting are based on *intaglio printing*, a technology restricted to security printers. Sensing the tactility of intaglio printing is a means of authenticating secured documents. Such a tactile pattern may also be effectively machine read [12,13]. The three-dimensional charac-teristic of intaglio printing can be put to use in so called *latent images*, revealing document authenticity at acute angles of observation [13]. A peculiar measure against counterfeiting is the application of intaglio ink that comes

off to leave traces of ink when rubbed against a white piece of paper. Such *staining ink* is printed on the Swiss 50 frank note in position C. Otherwise, the security rendered by intaglio printing has been defiled by corrupt nations, abusing this technology to counterfeit foreign documents.

From of old, intricate patterns have been printed on documents to thwart counterfeiting. Guilloche patterns are an early and well-known example. The current rise of digital scanning technology, however, has severely reduced their value. Modern examples of anti-counterfeit patterns comprise digital scan traps like *screen angle modulation* and *dot frequency modulation* [14,15]. This new type of security printing aims at exposing digital scanning techniques by the moiré-interference between the original printed pattern and the scanning frequency. The interference between printed pattern and scanning pattern renders deviating motifs, clearly discernible by the naked eye.

The printing of patterns that cannot be resolved by either the naked eye or common scanning equipment add to second line security. Examples are *µSAM* [15] and *Isocheck/Isogram* [16]. These features respectively require a line or a dot pattern to be laid over the printed pattern in order to reveal a distinct visible image. Again the visible image is generated by moiré between the printed pattern and the overlay pattern. A comparable technique is *optical encoding of images* [17-20] like the scrambled indicia technique [21-22]. The optical encoding technique requires a matrix of lenslets, for instance an array of fine cylindrical lenses (a lenticular array), to be placed over the printed pattern in order to reveal a distinct visible image. The latter technique allows encoding a set of two or more images that appear subsequently when the document is tilted. An example of such a *tilt image* is found on the reverse of the Swiss ID card, alternately displaying the card number and date of expiring [23]. Although this latter example is not paper based, the lenticular array technique can be well applied to paper printed patterns, witness the many postcards that have been issued with such tilt images.

Micro text and *fluorescent printed patterns* further add to thwarting counterfeiting in second line.

Recently developed printing inks allow the printing of iridescent designs on paper and plastic substrates. An example is intaglio or silkscreen printing in *optically variable ink* (OVI). OVI printing shows a conspicuous palette of fluctuating interference colours when tilted, for instance from magenta to green or from gold to green [24,25]. Examples are found on many banknotes like the French 50 frank note (green to dark blue) and the Swiss 50 frank note (green to purple; position E). The ink is manufactured by SICPA (Lausanne, Switzerland) and is strictly reserved for high security documents. Furthermore, *pearl lustre ink* displays a coloured sheen in reflection while otherwise being completely transparent [26]. Pearl lustre ink does not change colour with the angle of observation. It has become widely used on valuable documents like banknotes and driving licences. Examples are the golden sheen on the Dutch 100-guilder note and the greenish sheen of the cipher 50 in position A on the Swiss 50 frank note. Pearl lustre ink is commercially available and inexpensive (Mearl, Merck).

2.2.2 anti-tamper printed patterns. Fine *background security patterns* are offset printed on valuable documents like cheques in order to hamper mechanical erasure of variable information and substitution of fraudulent information. Scraping the written or printed ink off the surface of the paper without the damage becoming easily noticeable is thus made rather cumbersome. Care must be taken by the issuer not to use printing that merely sits on the paper without sufficiently penetrating it. Such printing is easily removed without noteworthy damage to the printed background. An extreme countermeasure is the use of printing that completely penetrates the depth of the paper. Such a *penetrating ink* withstands even the most careful scratching and does completely prevent the unobservable mechanical erasure of the information. An example is found on the Euro cheque which has the bank account number printed in such a penetrating ink. A penetrating ink may be printed, from a ribbon, black on the face of a document and bleeding through the paper to produce a red colour at the back [27]. Care must be taken to make these inks invulnerable to chemical erasure or, alternatively, to add suitable chemical indicators to the paper.

Apart from precluding mechanical erasure, the successful use of ink solvents can be made difficult by using *fugitive printing*. The application of solvents to erase the variable information will thus result in the obvious fading of the adjacent printing as well. Many invisible fluorescent printing inks are soluble in organic solvents as well. Apart from inks that reveal the action of inorganic solvents, water fugitive inks are sometimes printed to reveal an attack with watery solutions.

2.3 features appended to the paper

Modern security features comprise labels that can be firmly appended to the document by self-adhesion or hot foil printing. They comprise purely metallic foils as well as iridescent foils. Iridescent security features have proven to be of paramount importance in precluding current counterfeit techniques. Such features may be based on either diffraction or interference effects. Security features based on diffraction have been coined *Diffractive Optically Variable Image Device* (DOVID), while those based on interference are referred to as *Interference Security Image Structure* (ISIS). Figure 1 presents a schematic survey of iridescent security features. First order type DOVIDs are best-known and found as holograms, dot matrix devices, kinegrams, etc. on valuable documents like credit cards, banknotes and cheques. First order devices are best inspected under

point source illumination; in diffuse illumination their iridescent effects vanish. Next to these first order devices a zero order type DOVID has been developed [28]. It is inspected in zero order reflection and can be inspected in diffuse as well as point source illumination.

Apart from OVI and pearl lustre ink, the ISIS type feature is less widespread. Contrary to the DOVID, which consists of microscopic line patterns, the ISIS consists of a stack of thin films. The ISIS can be inspected in diffuse as well as point source illumination with the exception of deep Bragg-holograms, also called *volume reflection holograms*, that become fuzzy when illuminated with extended light sources. Bragg type security holograms are put on the market by Krystal Holographics [29]. Thin film features are found on Canadian banknotes and the British Columbia driving licence [30].

Bragg type structures consist of a stack of tens or even hundreds of dielectric layers that slightly alternate in refractive index. Each layer has an optical thickness of one half wavelength of the colour reflected. Bragg structures therefore display a monochromatic reflection when illuminated with white light. Other Bragg type features are the iridescent planchette and the *polymerised liquid crystal*, such as the Advantage seal [31].

In general security labels aim at protection against counterfeiting. They may be totally reflective or semitransparent. The latter type can be used as a security overlay protecting vital information against forgery. *Anti-tamper security labels* can be produced that are destroyed when peeled off, thus presenting clear evidence of the tamper attempt. Iridescent features are treated extensively in various chapters of reference [2].

For the sake of completeness, mention is made of 3M semi-transparent *retro-reflective foils* that are inspected in second line using a retro-viewer [32].

Currently, a tendency exists to produce DOVIDs displaying very complex images, with numerous image elements, kinematic and tilt effects in order to defeat counterfeiting. It can be argued on ergonomic grounds that such complex iridescent features are counterproductive from a first line inspection point of view. Although image complexity is a valid approach to producing features that protect against re-origination, such complex images are difficult to inspect and adequate inspection may even require an expert. Contrary, the development and application of document security features that derive their protection of highly complex micro and sub-micron structures, while otherwise displaying uncomplicated, recognisable images that are easy to remember, will be beneficial from a first line security point of view [33].

3 REFERENCES

[1] B. van den Assem, D. Brongers, J. Rath, R.L. van Renesse, K. Schell, D. Schuurman and S. Tuinstra, Security Documents - Practical guide for the security documents printing sector, Sdu Publishers, The Hague, The Netherlands (1994), ISBN 90 12081289 (out of print).

[2] Optical Document Security, ed. R.L. van Renesse, 2nd edition, publ. Artech House, Boston/London (1998), ISBN 0-89006-982-4.

[3] Holopack.Holoprint GuideBook (1995), ed. Ian Lancaster, publ. Reconnaissance Holographics, Runnymede Malthouse, Egham, Surrey TW20 9BD, England. Guidebook to sourcing and using holographic materials.

[4] Product & Image Security - A Techno-Economic Review and International Directory of Anti-Counterfeiting, Forgery, Theft, Tampering and Product and Image Security Technologies, 1st ed. March 1995. Publ. Labels and Labelling Data & Consultancy Services Ltd, The White House, 60 High Street, Potters Bar, Herts EN65AB, UK, and Label & Tag Security International, 28 Barn Lane, Oakley, Basingstoke, Hants RG23 7HT, UK.

[5] 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.

[6] The Biometrics Report (1995), Fingerprint, hand, eye, face, voice, signature; A research Report on Systems, Equipment, Costs, Advantages and Markets, by Emma Newham, ISBN 190018 00 9, 1995, 303 pages. Published by:
Europe: S.J.B. Services, London House, Broad Street, Somerton, Somerset, UK TA11 7NH.
North America: S.J.B. Services, 576 Fifth Ave., Suite 1103, New York, NY 10036, USA.

[7] Holography News and Authentication News, ed. Ian M. Lancaster, publ. Lewis T. Kontnik, Reconnaissance Holographics Ltd.,
Europe: Runnymede Malthouse, Egham, Surrey TW20 9BD, England,
North America: 825 East Tufts Avenue, Cherry Hills Village, CO 80110, USA

[8] Biometric Technology Today, ed. Emma Newham, S.J.B. Services, PO Box 20, Somerton, Somerset, England TA11 7YY.

[9] Product and Image Security, ed. J.J. Plimmer, publ. Label & Tag Security Int., 28 Barn Lane, Oakley, Basingstoke, Hants RG23 7HT, UK.

[10] R.L. van Renesse, Ordering the order - a survey of optical document security features, Conference on Practical Holography IX, San Jose, CA, USA, February 5-10, 1995, SPIE vol. 2406, p. 268-275.

[11] M. Camus et al, Security papers and special effects, reference [2], chapter 5.

[12] R.L. van Renesse, Optical inspection techniques for security instrumentation, Conference on Optical Security and Counterfeit Deterrence Techniques, San José, CA, USA, 27 Jan - 2 Febr. 1996, SPIE vol. 2659, p. 159-167.

[13] R.L. van Renesse, Noniridescent optically variable devices, reference [2], chapter 9.

[14] S. Spannenburg, Digital copying security elements, reference [2], chapter 8.

[15] S. Spannenburg, Optically and machine detectable copying security elements, Conference on Optical Security and Counterfeit Deterrence Techniques, San José, CA, USA, 27 Jan - 2 Febr. 1996, SPIE vol. 2659, p. 76-96.

[16] Aestron Almanac, Aestron Security Design BV, Zeverijnstraat 12, 1216 GK Hilversum, The Netherlands. Inclusive the Encyclopedia of Printed Security, eds. R.L. van Renesse, TNO Institute of Applied Physics, Delft, Netherlands and K.J. Schell, Schell Consulting, Noordwijk zh, The Netherlands (out of print).

[17] Robert J. Meltzer, Optical encoding of images for ID security, Proceedings of the Society of Photo-optical instrumentation Engineers (SPIE) seminar on Solving Problems in Security, Surveillance and Law Enforcement with Optical Instrumentation, 20-21 September 1972, New York, NY, USA, p. 149-153.

[18] John T. Ferris and Robert J. Meltzer, Optical cryptographic devices, Bausch & Lomb Inc. Rochester, NY, USA, patent number US 3,178,993, April 1965.

[19] Y. Ikegami and A. Miyauchi, Information storage and retrieval, Fuji Photo Film Co., Japan, US patent 3,922,074, November 25, 1975.

[20] Warren J. Ungerman, Indicia encoding system, West Point Industries, Pa, USA, US patent 4,023,902, May 17, 1977.

[21] A.V. Alasia, Process of coding indicia and product produced thereby, US Patent 3,937,565, published Febr. 10, 1976.

[22] A.V. Alasia, Encoding System, US Patent 4,092,654, published May 30, 1978.

[23] Becker, W. et al, "Datenträger mit einem optischen Echtheitsmerkmal sowie Verfahren zur Herstellung und Prüfung des Datenträgers", GAO mbH, München, Germany, patent number EP 219 012, US4-765656, April 22, 1987.

[24] Haim Bretler, Thin film devices in security printing inks, SPIE vol. 1210, Optical Security and Anticounterfeiting Systems, 15-16 Jauary 1990, Los Angeles, CA, USA, p. 78-82.

[25] J.A. Dobrowolski, Optical thin-film security devices, reference [2], chapter 13.

[26] R.L. van Renesse, Introduction to optical document security, reference [2], chapter 4.

[27] Cobra Imaging Products, 902 Linwood Ave, St. Paul, MN, USA.

[28] M.T. Gale, Zero-order microstructures, reference [2], chapter 12.

[29] Holography News, vol. 10, nr. 5, October 1996, Krystal enters security market with photopolymer, p. 12.
Krystal Holographics International Inc., 555 West 57th street, New York, NY 10019, USA.

[30] Identicard Ltd., 89 Galaxy Blvd., Unit 8, Rexdale, Ontario, Canada M9W 6A4.

[31] Advantage Technology Inc., 1809 Old Homestead Lane, P.O. Box 10155, Lancaster, Pennsylvania 17601, US.
This product is also put on the market by Identilam Ltd. under the name "Identiseal".

[32] J.E. Cook, Retroreflective security devices, reference [2], chapter 16.

[33] R.L. van Renesse, Security design of valuable documents and products, Conference on Optical Security and Counterfeit Deterrence Techniques, San José, CA, USA, 27 Jan - 2 Febr. 1996, SPIE vol. 2659, p. 10-20.

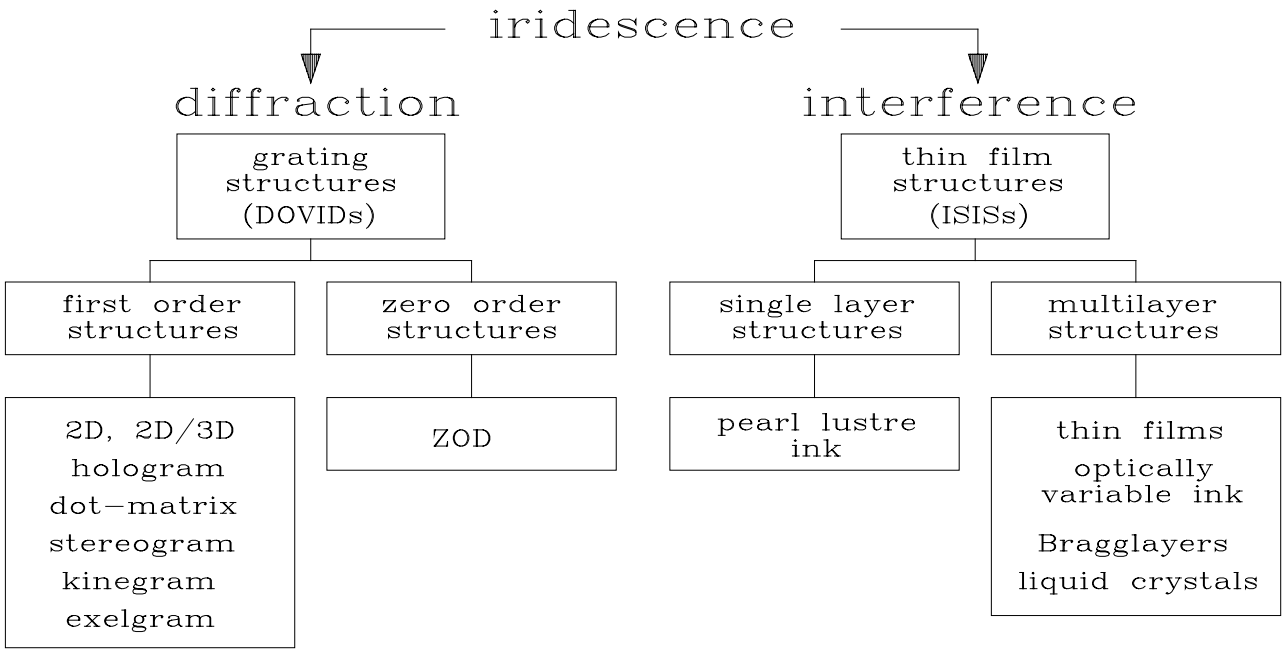

Figure 1 – Iridescence applied to document security