# Hidden and scrambled images – a review

Rudolf L. van Renesse

Conference on Optical Security and
Counterfeit Deterrence Techniques IV
San Jose, California, 27 – 28 January 2002
SPIE Vol. 4677, pp. 333 – 348

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

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

# Hidden and scrambled images – a review

Rudolf L. van Renesse*


## ABSTRACT

This paper reviews *screen-decoded images*, images that are invisible or illegible to the naked eye but that are visualised or decoded by means of periodic phenomena, such as an absorptive grating, a lenticular screen or the sampling frequency of a copying system. Two basic types are distinguished: *carrier screen images* and *scrambled images*. Carrier screen images consist of periodical arrays of screen elements, such as dots and lines, which serve as a carrier on which the encoded information is modulated. The counterpart of the carrier screen image is the scrambled image, which consists of numerous separate dissections of the original image. A classification of screen-decoded images by the type of carrier screen is presented in an attempt to clear up the existing confusion in nomenclature.


**Keywords**: Carrier screen, hidden image, moiré, aliasing, latent image, image scrambling, image dissection.

## 1 INTRODUCTION – A CLASSIFICATION OF SCREEN-DECODED IMAGES

This paper reviews *screen-decoded images*, images that are invisible or illegible to the naked eye but that are visualised or decoded by periodic phenomena: a matching screen such as an absorptive grating or a lenticular lens array (lenticular screen), or the sampling frequency of a copying system. As Figure 1 shows, two basic types of security features meet this definition: *carrier screen images* and *scrambled images*.

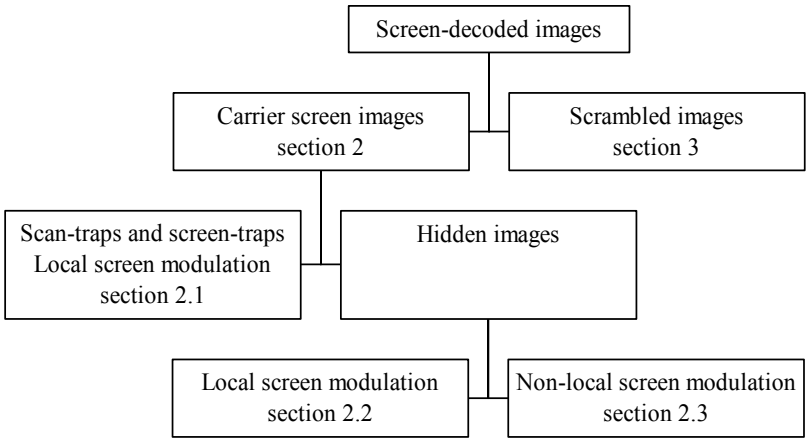



**Figure 1 –** Classification of screen-decoded images.

Carrier screen images consist of periodical screens of image elements (such as dots and lines) that serve as a carrier for the encoded information (section 2). The information modulated on the carrier screen is invisible to the naked eye. Carrier screen images can be further divided into *screen-traps* and *scan-traps*, which serve first line inspection (section 2.1), and *hidden images*, which serve second line inspection. (First line inspection merely involves the human senses, second line inspection requires tools.) Finally, hidden images can be divided into *local screen modulation images*, which display static moiré effects (section 2.2) and *non-local screen modulation images*, which display dynamic moiré effects (section 2.3). The counterpart of the carrier screen image is the scrambled image, which consists of numerous individual dissections of the original image (section 3). The scrambled image also serves second line inspection. The scrambled information is illegible to the naked eye. Hidden and scrambled images offer protection against various forms of counterfeiting because they tend to be difficult to copy or to reproduce. The application of screen decoded images against alteration of variable information is discussed in section 5 of this paper.

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

## 2 CARRIER SCREEN IMAGES

A variety of types of carrier screen images is known in the art of document security [1-10]. They have in common that the hidden information is modulated on a printable carrier such as a line screen or a dot screen. If the spatial carrier frequency is sufficiently high, the naked eye does not resolve the carrier screen so that a uniform field is observed. Furthermore, visible images may be added to the carrier screen by modulating the line width or dot size of the carrier. The hidden information becomes overt when the printed carrier is made to interfere with periodic phenomena, of which three are distinguished:

1. Interference with an overlay matching screen, the decoding screen. The interference effect is referred to as *moiré* and it serves second line inspection.
2. Interference with colour separation screens in the screen offset process. In this case the original image functions as a *screen-trap*. The resulting moiré effect is visible in first line inspection.
3. Interference with the scanner sampling band. This interference effect is referred to as *aliasing* [1-3] and the printed image functions as a *scan-trap*. The effect is visible in first line inspection.

Modulated carrier screens consist of screen elements such as lines and dots that may take arbitrary shapes. Carrier screens can be modulated by phase, frequency, angle, size/width, shape and colour (density is either modulated by size/width or frequency). Table 1 lists examples of scan-traps, screen-traps and hidden images as a function of five of these modulation parameters. The overview is not meant to be complete.

**Table 1 – Examples of carrier screen images**

| Image type | Element | Phase | Frequency | Shape | Angle | Size/width |
|---|---|---|---|---|---|---|
| *Screen -traps and scan–traps serving first line inspection* | | | | | | |
| **Concentric screens** | Lines | | (Variable) | | Variable | Variable |
| **SAM** | Minimal lines | | | | Variable | Variable |
| **FREM** | Minimal dots | | Variable | | | |
| **LIFT** | Lines | | Variable | | | Variable |
| **BrainBlock** | Dots | | | Variable | | |
| *Application of line screens and lenticular screens in second line inspection* | | | | | | |
| **Latent image** | Lines | | | | 90° clipped | (optional) |
| **µSAM** | Minimal lines | | | | Variable | |
| **Isogram** | Dots | Variable | | | | Variable |
| **HIT** | Lines, dots | Variable | | | | Variable |
| **Moiré intensity profiles** | Dots, shapes | | | Variable | | Variable |

### 2.1 Local screen modulation: scan-traps and screen-traps

The production of screen offset requires screens for digitising and colour separating continuous tone images. As a countermeasure against screen offset counterfeiting, the original image may contain printed structures, so called screen-traps, which interfere with these screens to create moiré fringe patterns in the reproduction. Likewise, digital scanners sample the original image with a certain frequency and this frequency may interfere with specific printed patterns that function as scan-traps to form aliasing effects. The hidden information, if any, forms a foreground that is locally modulated as a function of original image density on the carrier screen that serves as a background.

Screen-traps and scan-traps are not visualised by placing a decoding screen over the image, they serve first line detection of counterfeits. The aliasing effect caused by scan-traps can be suppressed by using “soft focus” settings of the copier or by various image-processing operations. The Internet provides various procedures to reduce moiré effects in scanned images. Nevertheless, scan-traps raise a barrier for the casual counterfeiter.

### 2.1.1 Concentric screen elements

Concentric screen traps do not contain any hidden information, they simply serve to generate visible moiré patterns in various types of copies. The concentric arrangement of the screen elements serves trapping functionality under all reproduction angles. Early concentric traps are found on the older issues of the DFL 100 ('snipe' 1981) and DFL 50 ('sun-flower' 1982). They consist of concentric circles with a variable spatial frequency in order to trap screens and scans of various frequencies[1]. Illustrations of aliasing and moiré fringes in counterfeits are found in [11][2]. The U.S. new currency design contains a single frequency scan-trap shown in Figure 2.

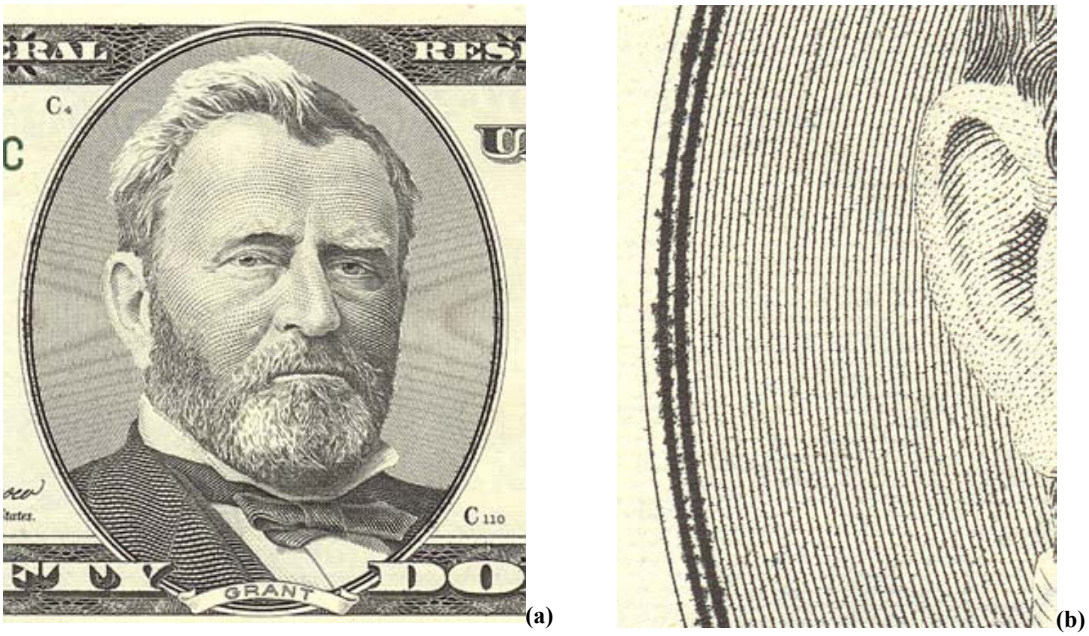



**Figure 2 –** Moiré fringes in the screen/scan-trap on the U.S. new currency design (a) and (b) detail of scan-trap intaglio lines (right). The line frequency is about 102 lines per inch.

### 2.1.2 Minimal line angle modulation

*Screen Angle Modulation* (SAM) is a scan-trap developed by Joh. Enschedé MatheGraphics (Haarlem, The Netherlands). SAM elements are very fine lines, called *minimal lines*, of which the angular orientation is modulated as a function of the original density of the encoded (covert) image. Due to aliasing, the encoded image becomes visible in a copy and displays a sensible message rather than a senseless moiré fringe pattern. Figure 3 shows an example of SAM and its effect. Additionally the line width can be modulated to create a visible image in the SAM field (Figure 3c). The background of the invention is presented in [1-3].

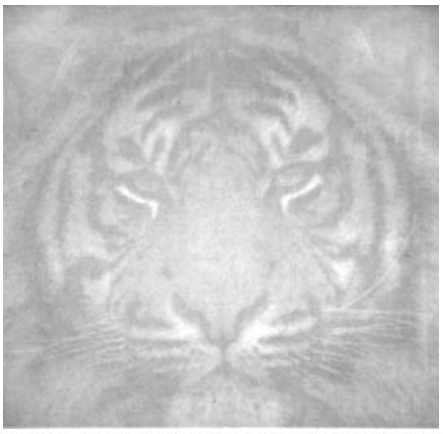
### 2.1.3 Dot frequency modulation

Because casual counterfeiters may make use of various ”sharpness low” methods to suppress the aliasing effects of scan-traps, Joh. Enschedé MatheGraphics developed frequency modulation (FREM) of minimal dots (Figure 4). The image tone rendition is achieved by modulating the spatial dot frequency rather than the dot size. High densities correspond to high dot frequencies and vice versa [1,13]. The dot frequency modulated image tends to fade if the resolution is decreased. The combination of FREM with a scan-trap such as SAM is meant to counter “sharpness low attacks”.

---

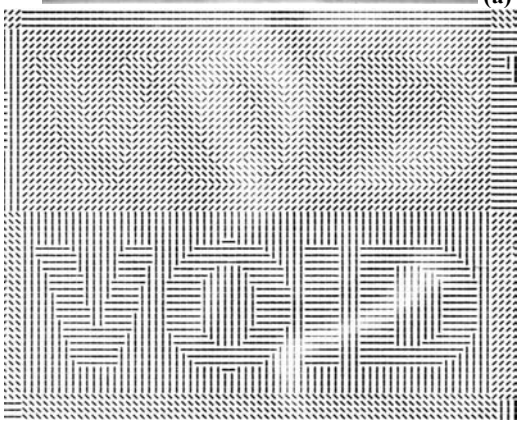
[1] These circles were coined *Koeze circles* after Peter Koeze of the National Bank of the Netherlands who introduced them on these two Dutch bank notes.

[2] Scanned images containing aliasing effects in Koeze circles are also found on Ron Wise’s website http://aes.iupiu.edu/rwise/: Europe, The Netherlands; P96 - 50 gulden (1982) and P97 - 100 gulden (1981).



(a)


(b)

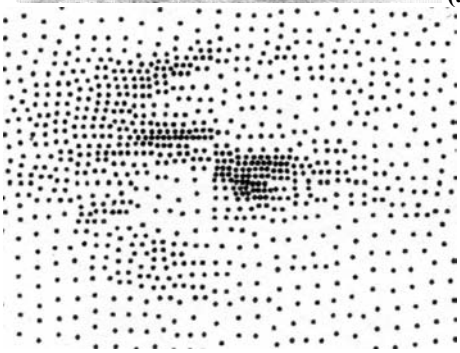


(c)

**Figure 3** – Screen Angle Modulation (SAM) functioning as a scan-trap: (a) original image, (b) copy of original image, (c) detail of original image (the lion's left eye) showing angular modulation of minimal lines to form the words "void".
In this example the maximum frequency of the minimal lines is about 76 lines per inch. The line angle modulation is 45°, 135° (c-top) and 0°, 90° (c-bottom).

(a)

(b)



(c)

**Figure 4** – Frequency modulation (FREM).
(a) original image, (b) image scanned in low resolution mode, and (c) detail showing minimal dots. The dot diameter is about 60 microns.

### 2.1.4 Line frequency modulation

Again another type of scan-trap is the *line frequency trap* (LIFT), developed by Aestron Design BV (Hilversum, The Netherlands), now part of Joh. Enschedé Holding BV. LIFT serves the same purpose as SAM, but the design is based on frequency modulation of a carrier line screen, whereby the line width is modulated to render a visually uniform field [13]. LIFT does not offer the addition of visible images by line width modulation as SAM does.
Figure **5** shows the message LIFT displays on a copy.

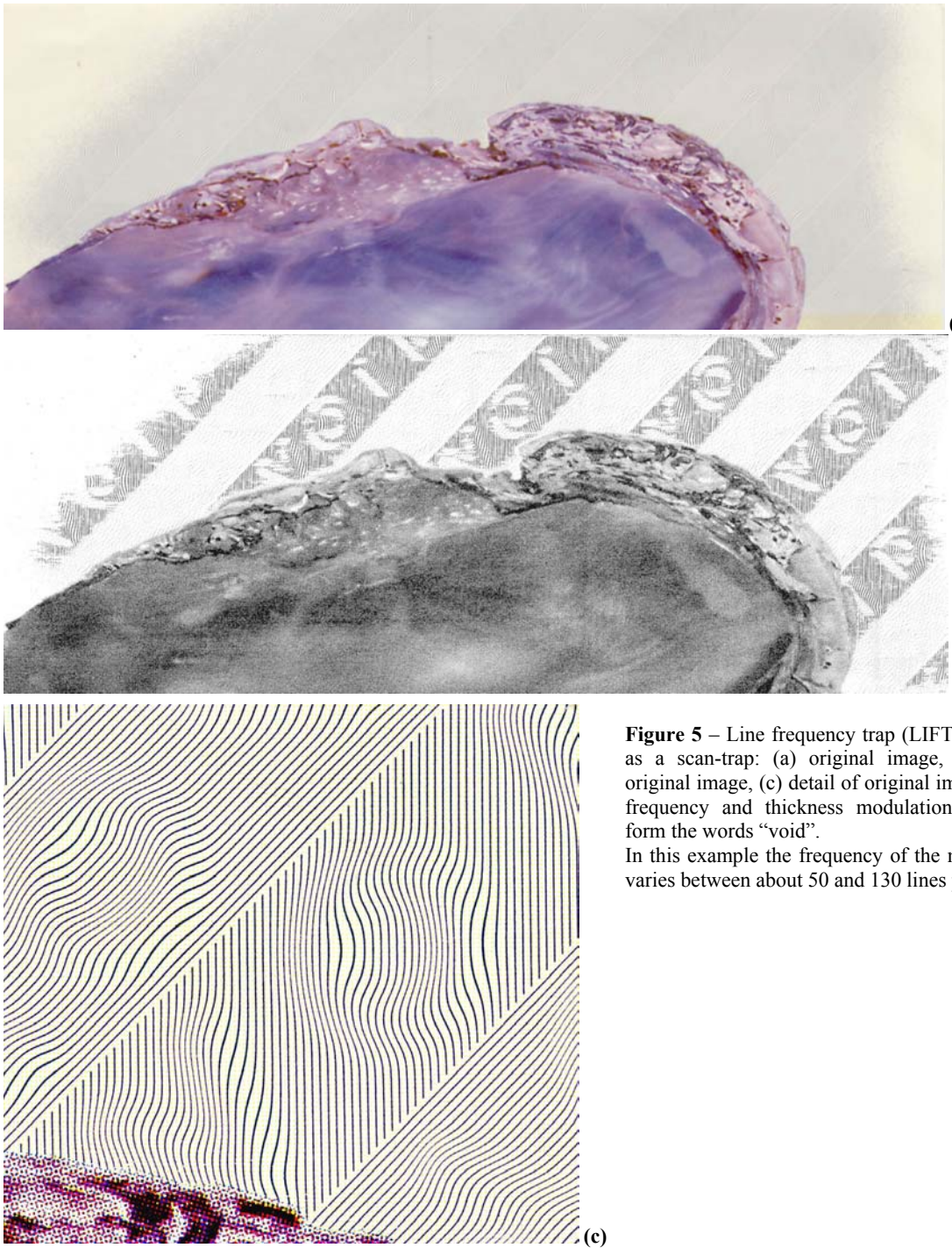



**Figure 5** – Line frequency trap (LIFT) functioning as a scan-trap: (a) original image, (b) copy of original image, (c) detail of original image showing frequency and thickness modulation of lines to form the words “void”.
In this example the frequency of the minimal lines varies between about 50 and 130 lines per inch.

### 2.1.5 Dot shape modulation

An example of a scan trap based on dot shape modulation is BrainBlock, developed by SBI (Lelystad, Netherlands). Screen elements representing high density and screen elements representing low density differ in shape according to the grey wedge represented in Figure 6.

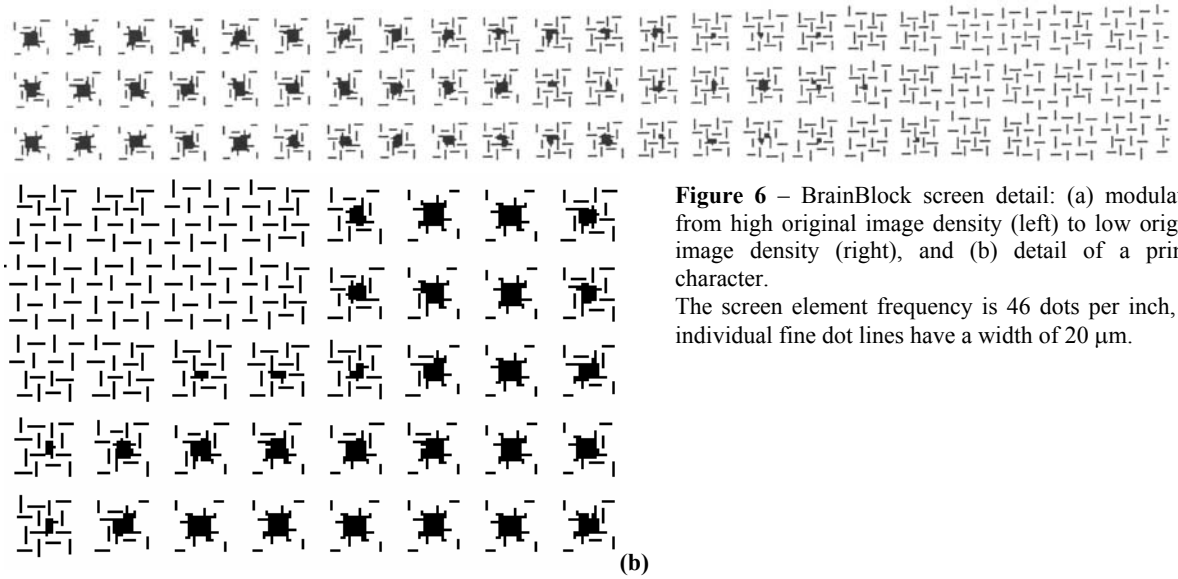



**Figure 6** – BrainBlock screen detail: (a) modulation from high original image density (left) to low original image density (right), and (b) detail of a printed character.
The screen element frequency is 46 dots per inch, the individual fine dot lines have a width of 20 µm.

When printed in high resolution, to the naked eye, such a wedge is a uniform area. But copying systems tend to reproduce the compact high-density screen elements and the exploded low-density screen elements with different densities. As a result the carrier screen image becomes visible in a copy either dark on a lighter background or in reverse contrast.

## 2.2 Local screen modulation: static moiré images

While scan-traps and screen-traps serve detection of counterfeits in first line, alternative carrier screen images allow verification in second line by the use of decoding screen overlays that generate moiré effects. Such decoding screens may be absorptive type line screens (*finding screens*) or lenticular screens. Obviously, lenticular screens will render brighter moiré patterns because they do not absorb the light (compare Figure 11 and Figure 12), but they are much more expensive than line screens. Like in scan-traps and screen-traps, the hidden information forms a foreground that is locally modulated as a function of original image density on the carrier screen that serves as a background. As a result, the displayed moiré images are local events with a fixed outline. Typical for such moiré patterns is that, depending on the adjustment of the screen overlay or the viewing angle, they appear either dark on a light background or in reverse contrast. This is demonstrated in various illustrations in section 2.2. This type of hidden image generally presents a monochrome moiré display but it could be designed to present multiple colours.

### 2.2.1 Line angle modulation in intaglio relief latent images

In the security printing art the term *latent image* commonly refers to grating patterns printed in intaglio relief. The latent image consists of a foreground of parallel lines in one angular orientation and a background of parallel lines in an orientation generally perpendicular to the foreground lines. Because of the relief of the intaglio print, shadows are cast between the lines if the patterns are illuminated and observed under an oblique angle and the encoded image is thus revealed. Latent images together with transient images are so-called transitory images, which change appearance with the angle of observation and illumination [14-17]. Latent images are examples of carrier screen images that can also be visualised by a decoding screen. Figure 7 and Figure 8 show an example and Figure 9 shows the intaglio line pattern in detail.


**Figure 7** - One hundred Intis Peru bank note (1987) with latent image on the bottom left.


**(a)**


**(b)**

**Figure 8** – A decoding lenticular screen, matching the printed line frequency, reveals the latent image on a one hundred Intis Peru note: (a) positive image under normal observation, (b) negative image observed under a slight angle.

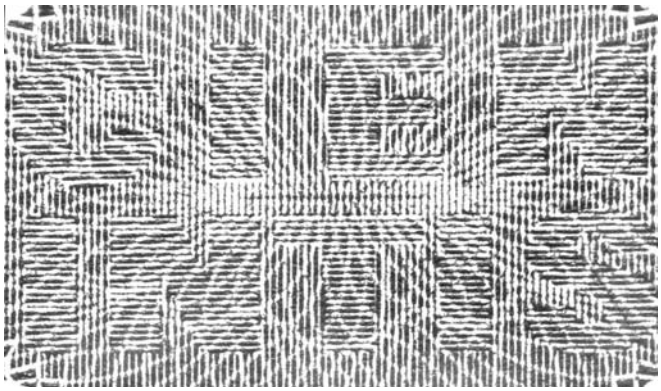


**Figure 9 –** Detail of the latent image in Figure 8, showing the orientation of horizontal foreground lines "CIEN INTIS" and vertical background lines.
Line width modulation additionally creates a visible guilloche pattern within the latent image.
The printed line frequency is 152 lines per inch.

Latent images can otherwise be produced by blind embossing or by white ink intaglio printing on a white background. In these cases even the presence of the carrier pattern becomes inconspicuous and only oblique observation reveals their presence.
Confusingly, the term "latent image" is also used for line phase modulated hidden images (section 2.2.4) that do not consist of a relief pattern and thus have no transitory characteristics.

### 2.2.2 Minimal line angle modulation

Joh. Enschedé Security Solutions developed μSAM as a second line feature against digital colour copying by casual counterfeiters [2]. The feature is based on SAM but it is printed in finer detail. The encoded image is visualised by a decoding line screen. In a copy no aliasing effects will appear but, due to lack of resolution, no moiré image will result when the decoding line screen is placed over the copy. A μSAM decoding screen has been printed in the transparent window of the 2001 Australian $5 and 2000 New Zealand $10 note as a self-authentication feature: folding the μSAM screen over the other side of the note reveals the image encoded in the printing. The function of the decoding screen can also be carried out in software, so that machine-scanned documents can be automatically checked for the presence of μSAM.

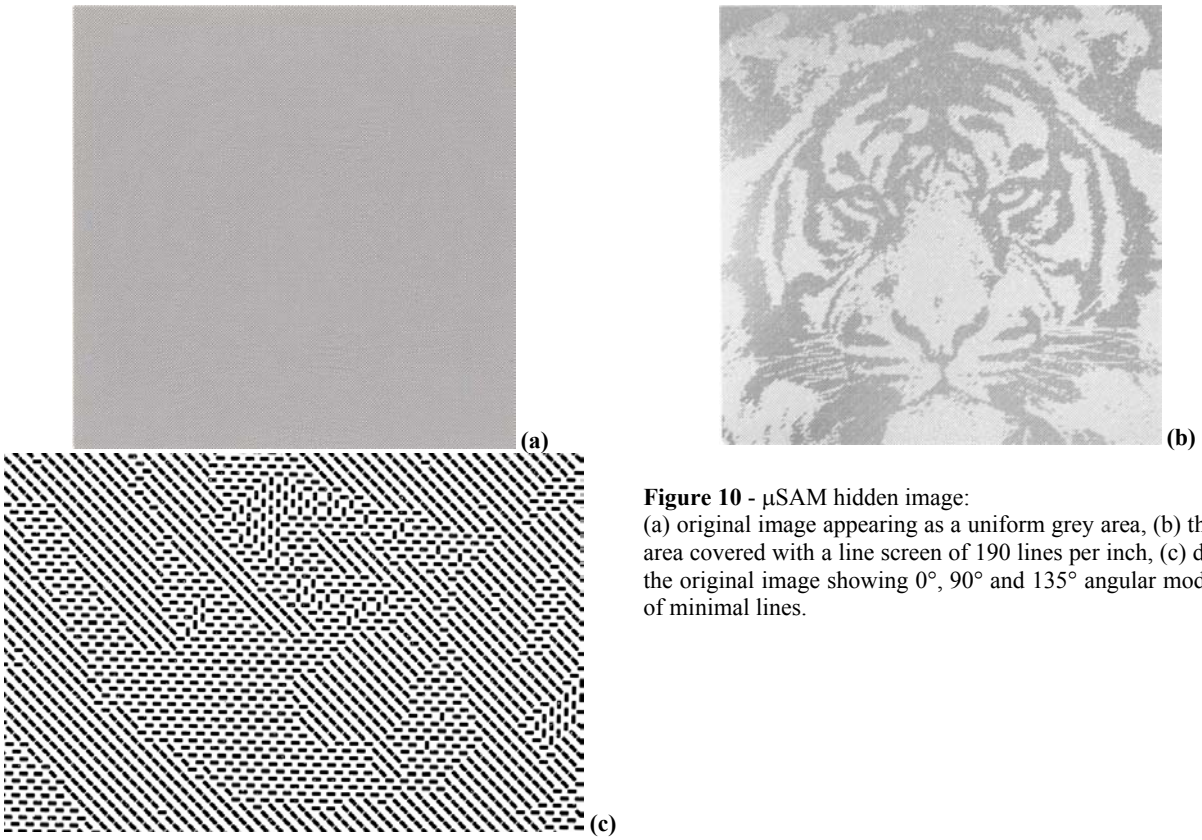


**Figure 10** - μSAM hidden image:
(a) original image appearing as a uniform grey area, (b) the same area covered with a line screen of 190 lines per inch, (c) detail of the original image showing 0°, 90° and 135° angular modulation of minimal lines.

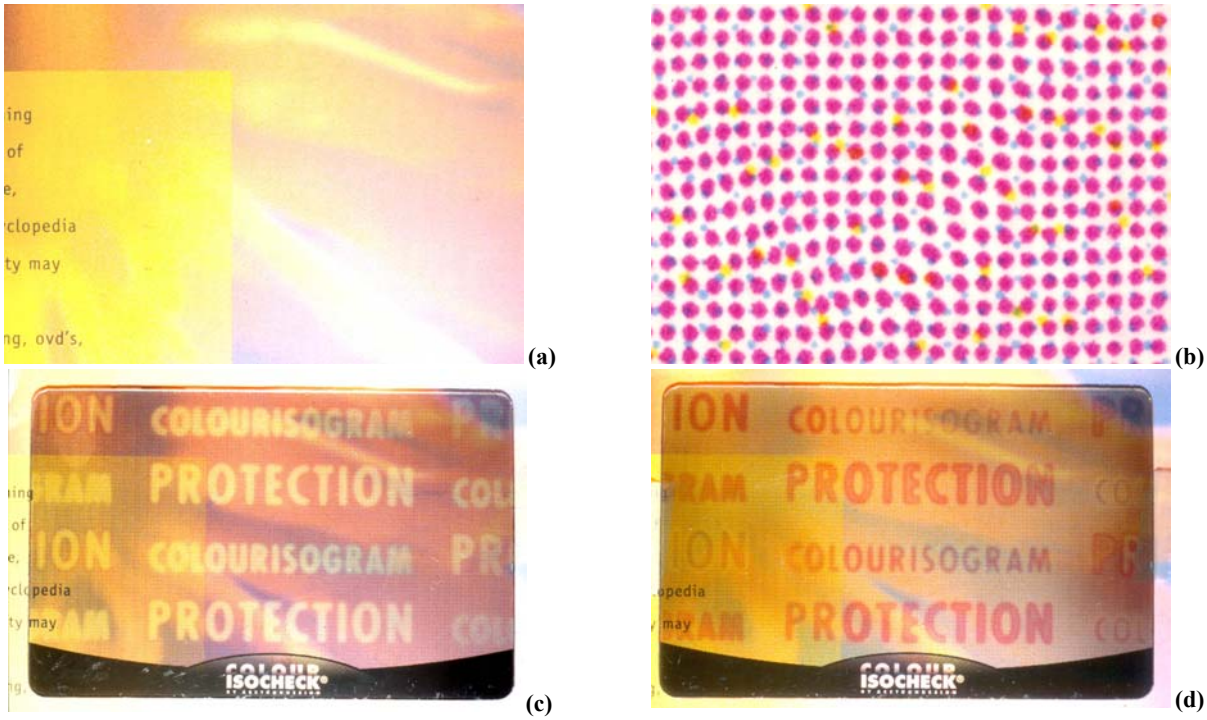



**Figure 11** – Isogram hidden image: (a) original image, (b) detail of original image showing phase and size modulation of dots, (c) negative image and (d) positive image, depending on the positioning of the dot overlay screen. In this example the frequency is about 180 dots per inch.

### 2.2.3 Dot phase modulation

The *Isogram* is an example of dot phase modulation of a black and white or multi-colour dot screen offset image. Dot size modulation renders a visible image. The Isogram was developed by Aestron Design BV (Hilversum, The Netherlands), now part of Joh. Enschedé Holding BV (Haarlem, The Netherlands). The phase encoded information is visualised by adjusting a decoding dot screen over the original image (Figure 11). Like μSAM, the Isogram allows machine authentication.

### 2.2.4 Line phase modulation

Merry refers to hidden images based on line phase modulation as *line deflection images* in 1979 [4] and *latent images* in 1984 and 1993 [5,6]. The latter term must not be confused with the intaglio printed transitory type of latent image described in section 2.2.1 which was already defined as a "latent image"[3] by Hutton in 1977. Even more confusing is the inapt use of the term *scrambled indicia* by Hackwood in 1986 for phase modulated line screens [7]. First, because phase modulation (or any other type of modulation) involves no scrambling of information and second, this term was already adopted in 1976 for images optically scrambled by the use of lenticular screens[4]. As is shown in section 3 scrambled images do not contain hidden information modulated on a carrier screen, characteristic for hidden images, but consist of separate, dissected image elements. In section 4 it is further shown that scrambled images and hidden images constitute mutually exclusive techniques.

A typical example of line phase modulation is *Hidden Image Technology* (HIT) developed by Jura JSP Ltd. (Budapest, Hungary). As is illustrated in Figure 12a, HIT is decoded by means of a lenticular screen. The carrier screen is phase modulated to create the hidden image, while line thickness modulation serves the creation of a visible image (Figure 12b, see also Figure 3c and Figure 9 for line thickness modulation).

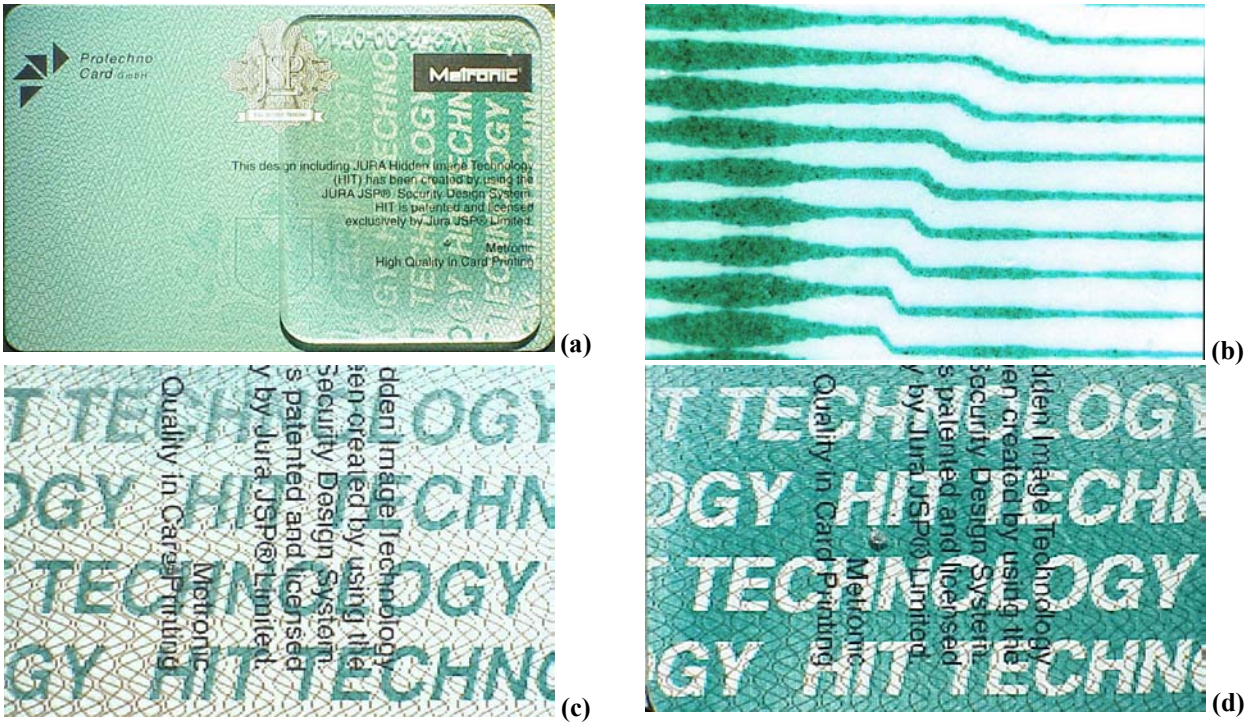



**Figure 12 –** Line phase modulation (Jura HIT): (a) plastic card with lenticular screen placed on top of it, (b) detail showing typical phase and width modulation of screen lines, (c) a positive image or (d) a negative image depending on the positioning of the lenticular screen. In this example the frequency is about 150 lines per inch.

[3] Hutton: "Such an image, appearing only when the imprint is seen at an acute angle of view, is herein termed a latent image." [15]

[4] The relevant patent on *scrambled indicia* opens with the line: "This invention relates to coding and decoding of indicia and more particularly to a system for producing scrambled or coded indicia, typically in printed form, and for decoding same." and the patent repeatedly uses the term "scrambled indicia." [28].

Phase modulated line screens may be also combined to create *multiple hidden images* [5,6]. To this end the gratings may be intertwined parallel or they may be superimposed at an angle. An example of parallel phase modulated gratings is derived of reference [6] and illustrated in Figure 13a. An example of perpendicularly crossed phase modulated gratings is found on the left front of the Guatemala ½ Quetzal note (1989 issue)[5], see Figure 13b.

**(a)**

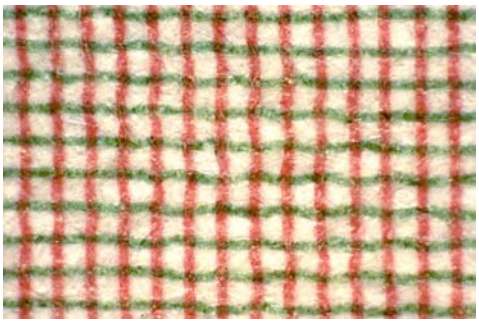

**(b)**

**Figure 13** – Line phase modulation in multiple hidden images:
(a) parallel micro text lines [6]; the finding screen must be shifted vertically to show 2 different images.
(b) Crossed lines in ½ Quetzal note (vertical lines red; horizontal lines green); the lenticular screen must be rotated over 90° to show 2 different images (138 lines per inch). Depending on the orientation of the lenticular screen, a portrait of the national hero Tecun Uman or the words "cincuenta centavos de quetzal" are displayed.

### 2.3 Non-local screen modulation: dynamic moiré images

Reference is made to the work of Amidror (EPFL, Switzerland) on security applications of *moiré intensity profiles*, published in this volume [9]. The carrier screen is dot shape modulated, building a dot screen of alpha-numerical or any other preferred symbols or shapes, either in black-and-white or in various colours. When a matching decoding pinhole screen is placed over the dot screen, a repetitive moiré pattern having the shape and colour of the screen dots appears, whose size, location and orientation are not fixed but vary dynamically as the screens are mutually rotated or shifted (Figure 14). Instead of a pinhole screen a two-dimensional lens array can be used to give brighter moiré patterns.
Contrary to local screen modulated images, described in the sections 2.1 and 2.2, in this case the hidden information is not localised in specific areas of the carrier screen (no foreground/background screen patterns). Moreover, the dot shape may vary per image element or may (gradually) vary over the total design and, consequently, the resulting moiré phenomena will change depending on the spatial characteristics of the dot screen design. Contrary to the dot shape modulation discussed in section 2.1.5, such variations in dot shape modulation do not encode any hidden information but are intended to yield artistic moiré effects. While the local screen modulation features discussed in section 2.2 display distinct foreground-background contrast inversions depending on the positioning of the decoding screen (see Figure 8, Figure 11, and Figure 12), non-local screen modulation features do not display such positive-negative contrast inversions. Non-local screen modulation can be divided into *global screen modulation* (the dot shape is fixed over the design, the size varies) and *semi-global screen modulation* (the dot shape and size vary over the design).
Another characteristic of these moiré intensity profiles is that they are visible within a large range of angles between the two screens, while local screen modulation features and scrambled images require a closer angular match between screens to become legible. The invention provides detecting and assessing moiré intensity profiles by machine reading [10]. The mathematical theory of these phenomena is treated in [18].

[5] Canadian Bank Note Co. printed the note and produced the lenticular screens.

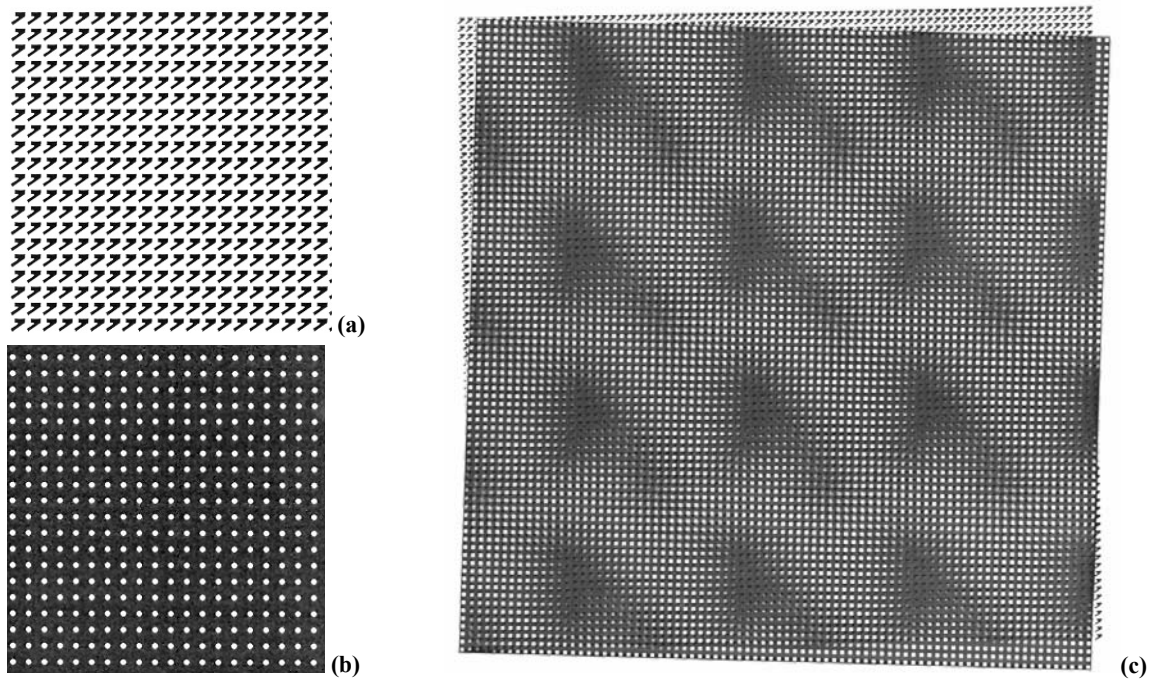



**Figure 14 –** Moré intensity profiles: (a) detail of dot screen, (b) detail of decoding pinhole screen, (c) pinhole screen placed over dot screen, displaying enlarged images of dot screen elements [19].

It is noted that, due to the high sensitivity of the moiré magnification effect, this effect has been used in industrial inspection to detect slight distortions in fine regular structures such as printing screens, woven fabric, TV phosphor screens and electric razor foils [11]. Further application areas are strain analysis, optical alignment, moiré topography, vibration analysis, etc [18].

## 3 SCRAMBLED IMAGES

Image scrambling involves splitting up (dissecting, sectionalising) an original image into many slices or patches, each of which is subsequently spatially distorted. This process can be carried out with the aid of one or two-dimensional lens arrays. The optical decoding process simply involves the ray reversal of the scrambling process using identical optics, as is explained in section 3.2. The image scrambling process can also be carried out by digital image processing.

### 3.1 History

The literature [20-30] on the optical scrambling of images for document security goes back to Avakian, et al [20] in 1960. Their technique involves *scrambling, disguising, concealing and or encoding* information and *the unscrambling, revelation or decoding thereof*, by the use of line screens, grids consisting of opaque and transparent lines, that the inventors call *sectionalising screens*. The purpose of the invention is to secure confidential information on documents from misuse by unscrupulous persons through converting this information into a *scrambled image*.

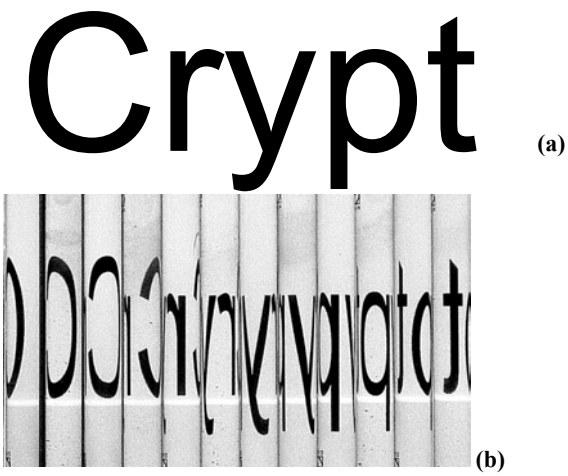
Brown, et al [21], in 1963, are the first to propose spherical and cylindrical lens arrays as optical encoders for this purpose. Subsequent patents use terms like *cryptographic security using screens of cylindrical lenticles as optical image dissectors* (1965) [22,23], *making reproducibly indiscernible or intangible documents, drawings, signature cards, etc.* utilising *a lens plate having a plurality of lenses* (1971) [24], and *a multiple array lens, otherwise known as a fly's eye lens, for scrambling the data to be encoded and also for unscrambling or decoding the data* (1972) [25].

In 1972 Meltzer [26] publishes a review article on the optical coding of images for ID security using an *array of cylindrical lenses* for the production of a *scrambled signature*. Ikegami, et al in 1974 publish a method to create a *scrambled image* using *lenticular plates*, additionally disclosing how different scrambled images can be merged to form multiple scrambled images [27].

In 1976 Alasia [28] publishes an optical scrambling technique based on lenticular screens, a technique that became known as *scrambled indicia* (see foot-note 4, section 2.2.4).

### 3.2 Principle of scrambling

Essentially, except for [20] where an absorptive line screen is proposed, these inventions are all based on scrambling an image by a lenticular screen and subsequently unscrambling it by inversion of the light rays using an identical screen. The principle can be elegantly demonstrated by using an array of test tubes filled with water serving as a large lenticular screen (Figure 15). From Figure 15 it appears that, in order to adequately scramble an image, there must be a certain relation between image size and pitch of the dissecting screen. If these two parameters are not adequately adjusted to each other, scrambling efficiency will be poor and the original information will remain more or less legible.




(a) (b) (c)

**Figure 15 –** Optical scrambling or image dissection:
(a) original object, (b) object scrambled by an array of water filled test tubes, (c) unscrambling of the scrambled image by observing the scrambled image through the same test tube array.

### 3.3 Applications of scrambled images

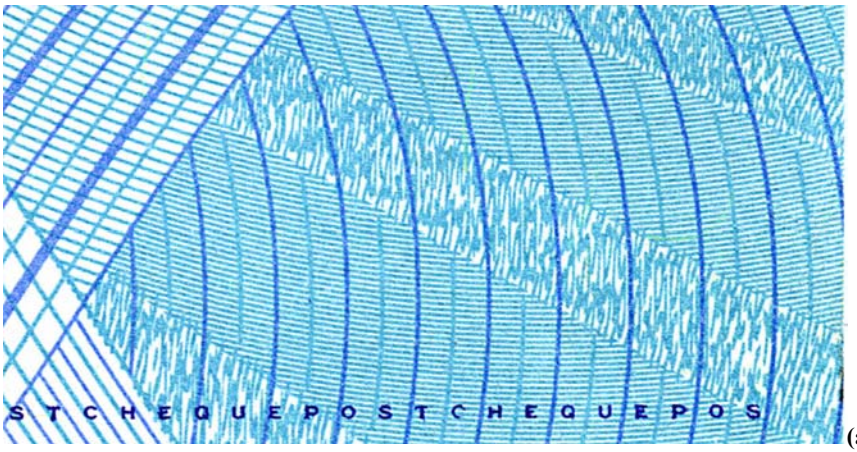
Two obvious security applications for the scrambling of information are the encryption of information and counterfeit protection. The first application does no longer seem very interesting in view of contemporary methods to optically [31-36] and digitally encrypt information. The second application is based (1) on the potential difficulty to adequately re-originate the scrambled information and (2) on the fineness of the printed detail that may be beyond the resolution of copying systems available to the casual counterfeiter.
An example of scrambled indicia is shown in Figure 16. Here it appears that the scrambling efficiency is somewhat inadequate, because the original text "Banco de España" is more or less legible on the original.


(a) (b)

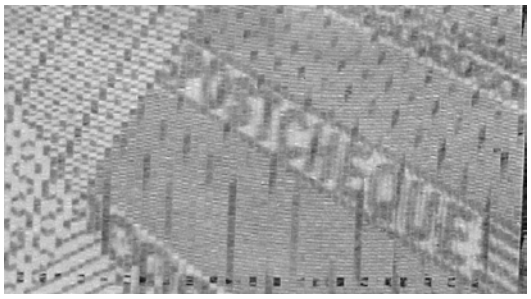
**Figure 16 -** Spanish 1000 peseta note (1992): the scrambled indicia area, printed on the right edge, is marked with a rectangle. The feature is 28 mm wide and contains 143 segments per inch.
(a) Detail of scrambled indicia.
(b) Detail showing scrambled indicia unscrambled by a lenticular screen.

It is possible to merge several scrambled images, as was proposed by Ikegami et al in 1975 [27]. This was demonstrated in 1988 by means of computer aided scrambling, coined "Line encryption", by the former Staatsdrukkerij (The Hague,

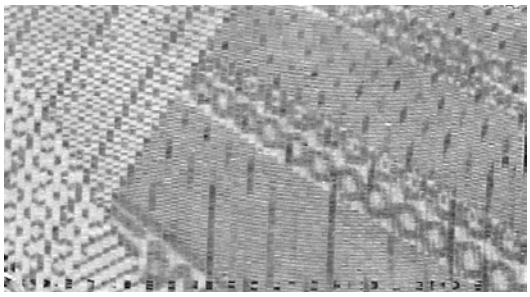
The Netherlands) on the Postbank's "Postcheque" (Figure 17). The two separate images are displayed by adjusting the position of the lenticular screen or slightly changing the viewing angle.




**(a)**



**(b)**



**(c)**

**Figure 17** – Multiple scrambled image: (a) 24 x 12 mm detail of "Postcheque" with line encryption bands and a line of 0.35 mm microtext, (b) unscrambling by a lenticular screen of the word "Postcheque" and (c) unscrambled guilloche bands.

## 4 HIDDEN IMAGES VERSUS SCRAMBLED IMAGES

Hidden images and scrambled images have in common that they are both decoded by the use of screens, either absorptive screens or lenticular screens. It is interesting to note that hidden images and scrambled images appear to constitute opposite phenomena in a number of essential aspects, being summed up in Table 2.

**Table 2 –** Scrambled images and hidden images constitute opposite phenomena

| **Scrambled images** | **Hidden images** |
|---|---|
| No carrier screen exists. | The image is modulated on a carrier screen. |
| The information is scrambled into a multitude of fractions or segments (image dissection). | The information remains an unscrambled whole. |
| The presence of the scrambled information is overt because it stands out with respect to the neighbouring design. | The presence of the information is covert because foreground and background cannot be distinguished (local modulation) or do not exist (non-local modulation). |
| **Scrambled images** | **Locally modulated hidden images** |
| Only positive contrast is displayed through the decoding screen. | Positive or negative contrast is displayed through the decoding screen, depending on its spatial adjustment or the viewing angle. |
| The size of the information depends on the period the decoding screen. | The size of the hidden information is independent of the period of the decoding screen. |

As Table 2 shows, image scrambling and hidden image techniques are mutually exclusive and it can therefore be maintained that the term "scrambled indicia" for carrier screen images is a misnomer. This was already observed in section 2.2.4 with reference to Hackwood's use of the term for phase modulated carrier screens [7] where it was observed that no type of screen modulation involves the scrambling of information.

## 5 DISCUSSION AND CONCLUSION

A variety of hidden images exists, based on modulation of information on carrier screen images. Decoding takes place with the aid of absorptive line screens or lenticular screens. Likewise, scrambled images, created by optical or digital image dissection, are unscrambled by the use of absorptive screens or lenticular screens. Although both techniques have opposite characteristics, they share potential applications: (1) hiding or encrypting information, (2) protection against copying, (3) protection against re-origination and (4) protection against alteration of variable information.

1. Successful protection of encoded information against disclosure by rendering it illegible depends on two factors: (1) the decoding screens must remain unavailable to unauthorised persons and (2) the hidden images must be designed so that it is difficult if at all possible to extract the hidden information by image analysis. This will hamper the re-engineering of such structures. This application appears obsolete, considering the fact that other optical encoding methods are now available that protect against disclosure more efficiently [31-36].
2. Protection against copying is at the mercy of the resolution of copying systems available to the casual and semi-professional counterfeiter. It must be borne in mind that, although the frequencies of the printed structures discussed in this paper all remain below 200 lines per inch, the detail modulated on the carrier frequency is much finer. It can be demonstrated however, that professional counterfeiters can copy these fine printing details using contemporary scanning and printing systems and that the copies will sufficiently reconstruct the encoded information by the use of a decoding screen. There appears no reason to be optimistic in this respect, considering the fact that printers with a resolution of 1200 dpi are currently available at no prohibitive cost.
3. Protection against re-origination depends on the remaining of necessary equipment and software unavailable for the counterfeiter. In that case it will be difficult, if at all possible, to produce printed details that will adequately reconstruct information with the use of the required finding screen. Obviously, an advantage of all screen-decoded images over old fashioned guilloche structures is, that deviations in counterfeited guilloche structures cannot be easily recognised, while a finding screen allows exact examination of the minute properties of screen-decoded images. Deviations of screen-decoded images will be revealed by disfigured moiré images if moiré effects are displayed at all. Eventually, it will appear to be more attractive for the counterfeiter to resort to copying the relevant structures from the original.
4. Protection against alteration is based on integrating hidden images or scrambled images as variable information of the holder (such as name or document number) into ID-documents (e.g. in the passport photo). A lenticular screen will simply enable the inspector to check for this variable information to match the regular holder ID information. Obviously the fraud can no longer resort to copying information because he needs to also alter it. This approach requires advanced digital encoding and printing techniques, which are expectedly beyond the reach of the semi-professional or maybe even beyond that of the professional counterfeiter and thus this approach also protects against re-origination. The machine reading potential of hidden images ads further value to this application.
   This approach is based on the general concept of combining fundamentally different techniques to add variable information to valuable documents in order to make alteration and re-origination difficult.

Summarising, the ultimate usefulness of the techniques described in this paper may rest upon the use of appropriate software combined with modern digital printing techniques to add variable information to individual valuable documents.

## 6 ACKNOWLEDGEMENTS

The author acknowledges the invaluable contributions of Isaac Amidror (Ecole Polytechnique Fédérale de Lausanne, Switzerland) and Steven Tuinstra (SBI, Lelystad, The Netherlands) to his understanding of screen-decoded images.

# 7 REFERENCES


1. Sijbrand Spannenburg, Digital copying security elements, chapter 8 in *Optical Document Security*, 2nd edition, ed. R.L. van Renesse, Artech House, London/New York (1998).
2. Sijbrand Spannenburg, Optically- and machine-detectable copying security elements, *SPIE vol. 2659, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques*, San José, CA, 1-2 February 1996, p. 76-96.
3. Sybrand Spannenburg, Developments in digital document security, *SPIE vol. 3973, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques III*, San José, CA, 27-28 January, 2000, p. 88-98.
4. Trevor Merry, *Photographic simulation of density differences as changes of line direction*, Canadian Bank Note Company, Ottawa, Ontario, Canada, patent number CA 1066109, filed 12 November 1975, issued 13 November 1979.
5. Trevor Merry, *Multiple superimposed latent images*, Canadian Bank Note Company, Ottawa, Ontario, Canada, patent number CA 1172282, filed 21 September 1981, issued 7 August 1984.
6. Trevor Merry, *Latent images comprising phase shifted micro printing*, Canadian Bank Note Company, Ottawa, Ontario, Canada, patent number US 5,178,418, filed 25 June 1991, publ. 12 January 1993.
7. Roger Hackwood and G.L. Howles, *Security documents*, Kenrick & Jefferson Ltd., West Bromwich, UK, patent number EP 0 256 176 A1, filed 7 August 1986, publ. 24 February 1988.
8. Richard Steenblik, *Optical image encryption and decryption processes*, Virtual Image Group, Roswell, GA, USA, patent number WO 93/09525, filed 18 August 1992, publ. 13 May 1993.
9. Isaac Amidror, A new print-based security strategy for the protection of valuable documents and products using moiré intensity profiles, *SPIE vol. 4677, Proc. Conf. on Optical Security and Counterfeit Deterrence Techniques IV*, San José, CA, USA, 23-25 January 2002, paper 4677-07.
10. Isaac Amidror et al, *Methods and apparatus for authentication of documents by using the intensity profile of moiré patterns*, Ecole Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, U.S. patent 5,995,638, publ. November 30, 1999.
11. Phillip Hill, Novelty effects find industrial applications, Opto &Laser Europe, issue 7, 1 February 2000, p. 24-26.
12. R.L. van Renesse, Verifying versus falsifying bank notes, *SPIE vol. 3314, Proc. Conference on Optical Security and Counterfeit Deterrence Techniques II*, San José, CA, USA, 29-30 January, 1998, p. 71-85.
13. Rudolf L. van Renesse (ed.), Karel Schell and Steven Tuinstra (co-ed.), *The Aestron Encyclopedia of Printed Security*, CD-ROM attached to *Optical Document Security*, 2nd edition, ed. R.L. van Renesse, Artech House, London/New York (1998).
14. Rudolf L. van Renesse, Noniridescent optically variable devices, chapter 9 in *Optical Document Security*, 2nd edition, ed. R.L. van Renesse, Artech House, London/New York (1998).
15. Hutton, R.G., and Merry, T., *Documents of value including intaglio printed transitory images*, American Banknote Company, New York, U.S. Patent 4,033,059, publ. July 5, 1977.
16. Rinaldo Castagnoli, *Papier valeur*, De La Rue Giori, Lausanne, Switzerland, patent number EP 0 146 151, filed 16 November 1983, publ. 26 June 1985.
17. Colin Shenton, *Security device*, The De La Rue Company Plc., London, GB, patent number WO 90/02658, filed 9 September 1988, publ. 22 March 1990.
18. Isaac Amidror, *The theory of the moiré phenomenon*, Kluwer Academic Publishers, Dordrecht/Boston/London (2000).
19. Isaac Amidror, *A didactical downloadable moiré demonstration kit,* downloadable from the Internet at: lspwww.epfl.ch/books/moire/kit.html.
20. E.A. Avakian, et al, *Cryptic grid scrambling and unscrambling method and apparatus*, patent number US 2,952,080, filed 12 September 1957, publ. 13 September 1960.
21. Laurence R. Brown, Drexel Dynamics Corp., Philadelphia, PA, USA, *Coding apparatus*, patent number US 3,084,453, filed August 31, 1960, publ. April 9, 1963.
22. Corwin H. Brumley, *Optical cryptographic device*, Bausch & Lomb Inc. Rochester, NY, USA, patent number US 3,166,625, filed February 7, 1960, publ. January 19, 1965.
23. John T. Ferris and Robert J. Meltzer, *Optical cryptographic devices*, Bausch & Lomb Inc. Rochester, NY, USA, patent number US 3,178,993, filed October 7, 1960, publ. April 20, 1965.
24. Ataka, H, *Method and device for recording characters or symbols in a reproducibly indiscernible manner*, K.K. Ricoh, Tokio, Japan, patent number US 3,609,035, filed December 17, 1969, publ. September 28, 1971.

25. George L. Mayer Jr., and David L. Dobbins, *Data encoding and decoding apparatus and method*, Coded Signatures Inc., New Orleans, LA, USA, patent number US 3,676,000, filed December 31, 1970, publ. July 11, 1972.
26. Robert J. Meltzer, Optical coding 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.
27. Yoshizo Ikegami and Akio Miyauchi, *Information storage and retrieval*, Fuji Photo Film Co., Japan, Jap. Appl. Prior, Sept. 25, 1972, patent number US 3,922,074, filed September 24, 1973, publ. November 25, 1975.
28. A.V. Alasia, *Process of coding indicia and product produced thereby*, patent number US 3,937,565, filed June 3, 1974, publ. February 10, 1976.
29. Warren J. Ungerman, *Indicia encoding system*, West Point Industries, Pa, USA, US patent 4,023,902, May 17, 1977.
30. Bryne E. Heniger and Philip B. Sullivan, *Lenticular security screen production method*, Dittler Brothers Inc., Atlanta, GA, USA patent number US 5,034,982, filed January 3, 1989, publ. July 23, 1991.
31. B. Javidi, Optical Information Processing for security and encryption systems, *Optics and Photonics News Magazine*, no. 3, March 1997.
32. B. Javidi and A. Ahouzi, Optical security system using Fourier plane phase encoding, *Journal of Applied Optics*, vol. 37, p. 6247-6255, September 10, 1998.
33. T. Nomura and B. Javidi, Polarization multiplexing for information security systems, *Proceedings of the Annual Meeting of the IEEE Lasers Electro-optical Society (IEEE LEOS)*, San Francisco, California, November, 1999**.**
34. T. Nomura and B. Javidi, Information security using digital holography, *Journal of Optics Letters*, January 1, vol. 25, 2000.
35. B. Javidi and T. Nomura, Polarization encoding for optical security systems, *Optical Engineering*, vol. 39, p. 2439-2443, September 2000.
36. E. Tajahuerce, J. Lancis, B. Javidi, and P. Andres, Optical security and encryption with totally incoherent light, *Journal of Optics Letters*, vol. 26, p. 678-681, May 15, 2001.