Published in: Anti-counterfeit Image Analysis Methods: A Special Session of ICSXII Journal of Physics: Conferences Series 77, 2007, article 012001, 10 pages

Notes:
1. This is the correct version of the present paper; the version which appears in the JOP contains corrupted figures.
2. Page 6 may take a few minutes to print.

Moiré methods for the protection of documents and products: A short survey

I Amidror, S Chosson and R D Hersch
Ecole Polytechnique Fédérale de Lausanne (EPFL), CH-1015 Lausanne, Switzerland

Abstract. Moiré effects have long been used for various applications in many different fields, including metrology, strain analysis, optical alignment, etc. In the present survey we describe some of the main applications of the moiré effect in the field of document and product security. We review the main families of moiré-based anticounterfeiting methods, compare them, and explain how they can be used for such security applications.

1. Introduction

The moiré effect is a well known optical phenomenon which occurs due to an interaction between overlaid structures (such as line gratings, dot screens, etc.). It consists of a new visible pattern which is clearly observed at the superposition of the individual structures, although it does not appear in any of the original structures themselves [1]. In the present survey we review some of the main applications of the moiré effect for the authentication of documents and products and for their protection against counterfeiters.

Counterfeiting of security documents such as banknotes, checks, certificates, travel documents etc. is becoming now more than ever a serious problem, due to the availability of high-quality and low-priced colour photocopiers and desk-top publishing systems. The same is also true for valuable products such as CDs, DVDs, software packages, medical drugs, etc., that are often marketed in easy to counterfeit packages.

Moiré-based methods offer an interesting solution to this problem, that can be easily incorporated in the document or product production process without incurring additional production costs. This is due to the fact that moiré security elements are usually print-based, i.e. they are designed and printed as part of the document itlelf. But they can be also incorporated in independent security elements such as holograms, kinegrams, non-standard inks, etc.

In the following sections we review the main moiré security methods and classify them into several families according to their properties and functionality. We also describe some of their main variants, compare their advantages, and discuss their applications in the field of anticounterfeiting.

2. Moiré inducing patterns (screen traps, scan traps)

The first family of moiré-based counterfeit deterrents, which is widely used in security documents such as banknotes, checks, etc., consists of some special repetitive patterns, usually straight or curved line families with gradually varying frequencies and orientations, that are incorporated within the design of the original document. These patterns generate strong moiré artifacts when the document is counterfeited by means of any standard halftone-based colour reproduction system such as offset printing, etc. (the halftoning technique, which is the core of most image reproduction systems, is explained, for example, in [2] or in [3]). Moiré inducing patterns are designed to interfere with the widest range of halftone screens that are being used in the printing industry, hence their popular name “screen traps”.

Similar methods are also applied to the prevention of digital photocopying or digital scanning of documents; in this case the term “scan trap” is often used. Nice examples of moiré inducing patterns can be found, for example, in [4], pp. 147–149, or in Figures 14–15 in [5].

3. Phase modulation methods (latent images)

While in the moiré inducing methods the presence of moiré patterns indicates that the document in question is counterfeit, other moiré-based methods are based on the inverse paradigm: They take advantage of the intentional generation of a moiré pattern, which can only be produced by the superposition of an appropriate revealer, and it is the appearance of the intended moiré shapes which confirms the authenticity of the document or of the product in question.

In the present section we describe the first family of such moiré-based methods. This family of methods is based on the physical presence on the document of a latent image, which is generated using a technique known as “phase modulation”. In this technique, a fine, uniform line grating or screen of dots is printed on the document, but within the pre-defined borders of the latent image the same line grating (or respectively, the same dot screen) is printed in a different phase, or possibly in a different orientation. Due to the high frequency of the lines or dots, the latent image thus printed on the document is hard to distinguish from its background. But when a reference transparency comprising an identical but unmodulated line grating (respectively, dot screen) is superposed on the document, thereby generating a moiré effect, the latent image pre-designed on the document becomes clearly visible, since within its pre-defined borders the moiré effect appears in a different phase than in the background (see pp. 187–190 in [1]; pp. 151–158 in [4]).

Figure 1 illustrates the basic principle of phase modulation methods, making use of periodic line gratings. Let A and B be two identical line gratings with a small period T. Assume that within the borders of a given shape, say, a triangle, the parallel lines of grating A are shifted by half a period (see Figure 1(a)). In reality, the period of the gratings would be much smaller than in Figure 1, so that only its general gray level would be perceived by the eye. Since the gray level outside the triangle is identical to the gray level inside it, the presence of the triangular shape within grating A is not easily detected by the eye. Now, assume that line grating B, printed on a transparency using the same period T but with no latent images (see Figure 1(b)), is superposed on top of grating A at the same angle. Figure 1(c) shows the superposition when the two gratings are superposed in-phase, and Figure 1(d) shows the superposition when grating B is shifted by half a period. As we can see, thanks to grating B the shape of the latent image hidden in grating A becomes clearly visible. However, owing to its high frequency, layer A and its latent image will be reproduced by any photocopier as a constant gray area; and when the revealing layer B is laid on a photocopy of the original document, the moiré effect will not be seen (or will be highly corrupted).

The family of phase modulation methods contains many different variants. For example, in a technique developed by Jura JSP, Hungary, the line thickness within layer A is not constant as in Figure 1 but rather varies in order to create a visible gray-level image, in addition to the latent image which is located in the same area but can only be detected using the moiré revealer [4, pp. 156–157]. Phase modulated line screens can be also combined, in different line orientations, in order to create multiple hidden images. In this case several latent images can be designed within the same area, each of which being detected by superposing the revealing layer at a different orientation [4, pp. 157–158].

In yet another variant periodic dot screens are used instead of the line gratings illustrated in Figure 1. This variant has the advantage that it can be incorporated within black and white images that are printed using the halftoning technique, where the size of the halftone dots varies according to the gray level in the different regions of the image. Since the latent image cannot be perceived in areas where the image is completely black or completely white, the visibility of the latent image can be improved by compressing the dynamic range of the printed image, for example into the range (0.2...0.8) rather than (0...1). A similar method can be also used in colour printing using the standard cyan, magenta, yellow and black halftone screens for hiding several different latent images within the same area of the document.

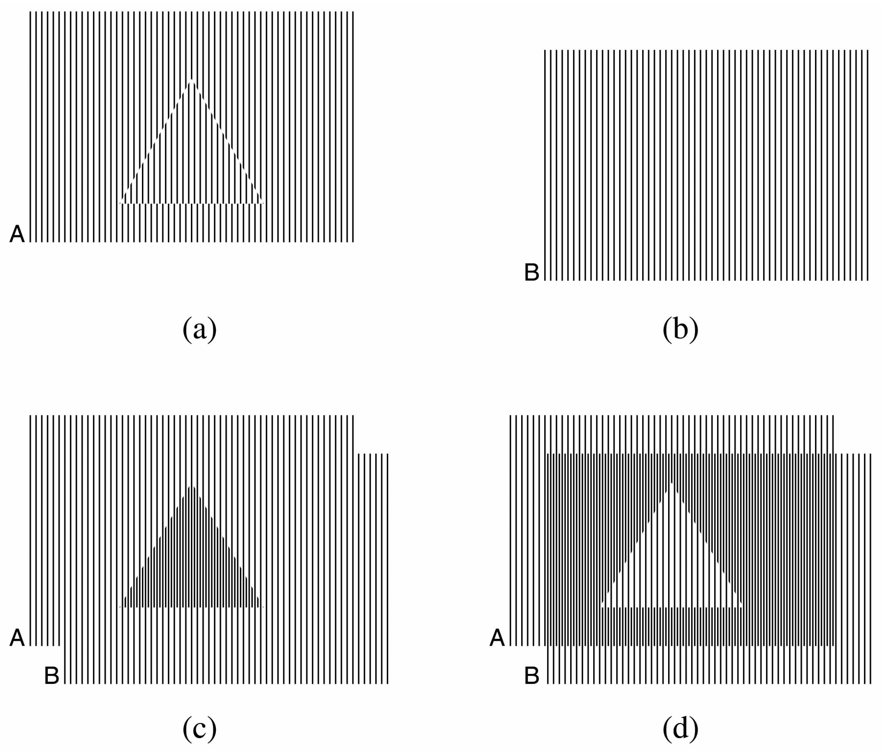


Figure 1. The basic principle of phase modulation methods, illustrated here with largely magnified line gratings. (a) Grating A and its latent image. (b) Grating B, the revealing layer. (c) In-phase superposition of grating B on top of grating A. (d) The superposition when grating B is shifted by half a period to the right.

Yet another similar method, known as *Scrambled Indicia*, has been introduced by the Graphic Security Systems Corporation [6]. This method uses as a revealer a 1D line grating rather than a two-fold periodic dot screen. Scrambled indicia have been used since 1997 by the U.S. Postal service for issuing stamps incorporating hidden text or images intended to deter counterfeiters, and to offer an interesting design element for collectors. The first stamp incorporating this feature was the 32¢ stamp issued on September 18, 1997 to commemorate the 50th anniversary of the U.S. Air Force, and it contains the hidden text "USAF". This latent text is not visible to the naked eye, but can be viewed using a special revealer, available through the U.S. Postal Service, when the revealer is positioned on the stamp at the appropriate angle. More information on this method can be found in GSSC's internet site: http://www.graphicsecurity.com.

A further variant of the phase modulation methods is based on pseudo-random dot screens rather than on periodic dot screens. This method is described in the section "Background" of [7] and illustrated in Figs. 4(a)–4(c) there.

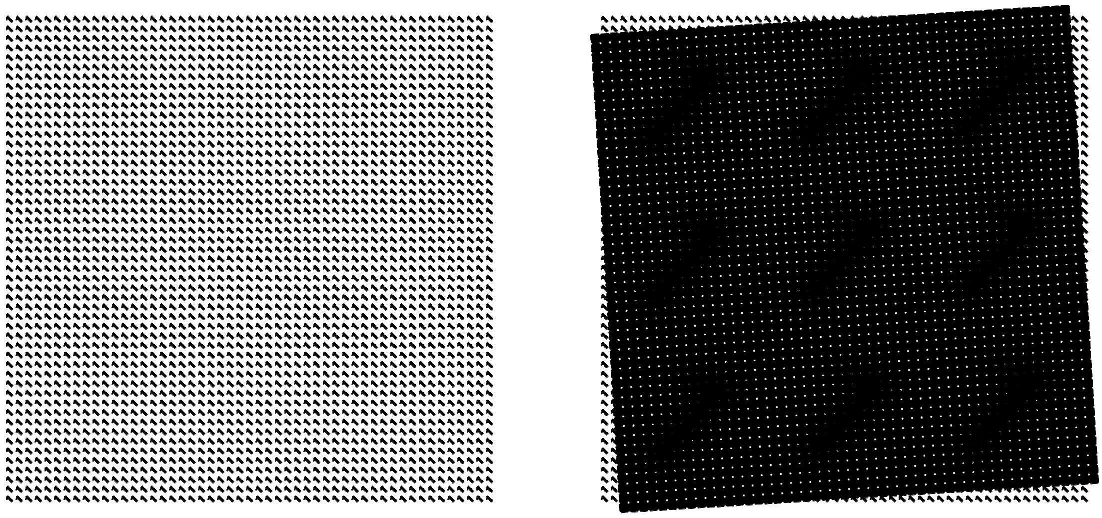
All phase modulation methods have in common some typical characteristic properties that distinguish them from the other methods. As shown in Fig. 1, when the revealer is slowly shifted along the latent image the intensities (or colours) of the foreground and of the background are rapidly and repeatedly interchanged, so that the latent image does not have a fixed, stable intensity (or colour); but the *location*, *size* and *orientation* of the latent image do not vary. Furthermore, all phase modulation methods have low tolerance to rotation, and the revealer must be aligned at a precise orientation in order to see the desired effect; this intrinsic property of phase modulation methods is due to the fact that these methods are based on a singular moiré effect (see Secs. 2.9 and 7.7 in [1]).

4. Moiré intensity profiles (2D, 1D and random)

While phase modulation methods are based on the existence of a latent image on the document, whose shape, location, size and orientation are fixed and do not change, there exist other families of moiré-based methods that do not use a fixed latent image on the document, and provide highly dynamic moiré effects. These methods are briefly reviewed in the present section.

The 2D moiré method [8, 9, 10] is based on the moiré intensity profiles which are generated between two specially designed periodic dot screens, one of which (known as the basic screen) being a microstructured halftone image that is located on the document itself, while the other (the master screen) plays the role of a revealer. Each of these periodic dot screens consists of a lattice of tiny dots, and is characterized by three parameters: its repetition frequency, its orientation, and its dot shapes. These periodic screens are similar to the dot screens which are used in classical halftoning, but they have specially designed dot shapes, frequencies and orientations. When two properly designed black-and-white or colour screens are laid on top of each other, there appears in the superposition a highly visible repetitive moiré pattern of a predefined intensity profile shape and colour (see Figure 2), whose size, location and orientation are not fixed, but rather gradually vary as the screens are rotated or shifted on top of each other. As an example, this repetitive moiré pattern may consist of any predefined letters, digits or any other preferred symbols (such as the country emblem, the currency, etc.), either in black-and-white or in colour. The theoretical explanation of this phenomenon has been presented in detail, along with numerous illustrative figures, in [11] or in Chapters 4 and 9 of [1].

It should be noted that the screen which is located on the document itself (the basic screen) needs not be of a constant halftone level. On the contrary, it may include dots of gradually varying sizes and shapes, and thus constitute a full, real halftoned image with varying tone levels (such as a portrait, a landscape, etc.), either in full gray levels or in colour (see Figure 3). Such a basic screen, made of halftone dots of varying sizes and microstructure shapes, can be generated using halftoning techniques as described in Section 3 of [10]. The revealer (master screen) may typically be a pinhole screen with the same (or almost the same) frequency as the basic screen, whose dots consist of tiny openings on a dark or opaque background. When a properly designed revealer is superposed on the corresponding basic screen, highly visible moiré shapes become visible inside the image, showing a largely magnified version of the shapes and colours of the microstructured halftone dots from which the basic screen image is composed (see Figure 4). The size and orientation of the moiré intensity profiles gradually vary as the master screen is rotated on top of the basic screen, and when the master screen is slowly shifted they rapidly scroll throughout the image. It should be mentioned that unlike in the phase modulation methods, where the shape of the moiré effects is determined by a fixed latent image that is physically located on the document, no latent images exist in the present method, and all the spatial information which is made visible by the moiré intensity profiles is encoded in the specially designed periodic tiny shapes forming the screens. As a consequence, unlike in the phase modulation methods where the moiré shape is fixed and delimited by the borders of the predefined latent image, in the present method the moiré intensity profiles are not fixed, and they gradually vary (move, rotate, or become bigger or smaller) as the screens are shifted or rotated on top of each other, generating an attractive dynamic visual effect. Furthermore, unlike in the phase modulation methods, where any slight shift of the revealing device causes a foreground / background colour inversion (for example: Swiss flag / Red-Cross flag), all colours in the present method remain stable and constant (in the example above: a Swiss flag remains a Swiss flag throughout). Another significant advantage of the present method is its much larger angular tolerance: the moiré intensity profiles remain clearly visible within a range of more than ±10°, making them much more easy to observe than in the phase modulation methods where the moiré effect is only visible when the revealer is superposed precisely at the specified angle.



(a) (b)

Figure 2: (a) A periodic dot screen consisting of tiny "1" shapes. (b) Its superposition (possibly with some angle difference) with a periodic dot screen (revealer) consisting of small pinholes on a black background gives a largely magnified periodic "1"-shaped moiré intensity profile. Both (a) and (b) are shown here largely magnified.

The fact that moiré effects generated between superposed dot screens are very sensitive to any microscopic variations in the screened layers makes any document protected using the present method very difficult to counterfeit. Any attempt to counterfeit a document produced using this method by photocopying, by means of a desk-top publishing system, by a photographic process, or by any other counterfeiting method, be it digital or analog, will inevitably corrupt the size or the shape of the tiny screen dots of the basic screen comprised in the document (for example, due to resampling, dot-gain, ink-propagation, etc.). But since moiré effects between superposed dot screens significantly increase any microscopic distortions in the screens, this makes any document protected by this method very difficult to counterfeit, and serves as a means to distinguish between an authentic document and a counterfeited one (compare Figs. 4(a) and 4(b)).

The 1D moiré method [12, 13, 14, 15] differs from the 2D moiré method described above in that it is based on 1-fold periodic line gratings rather than on 2-fold periodic dot screens. Instead of encoding the desired information in the shape of the individual dots of a periodic dot screen, the information is encoded within the individual lines of a periodic line grating, and the revealing layer being used consists of a 1-fold periodic grating made of linear slits rather than a 2-fold periodic pinhole array.

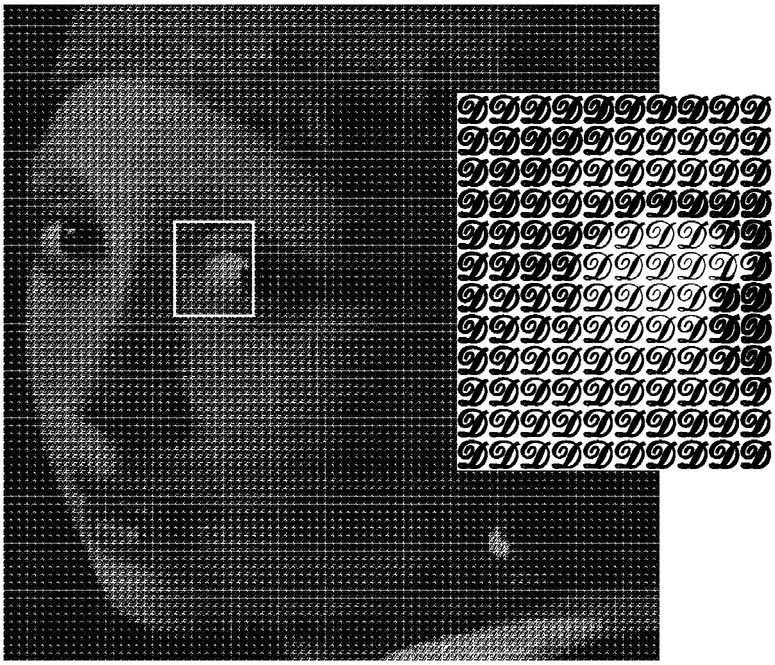
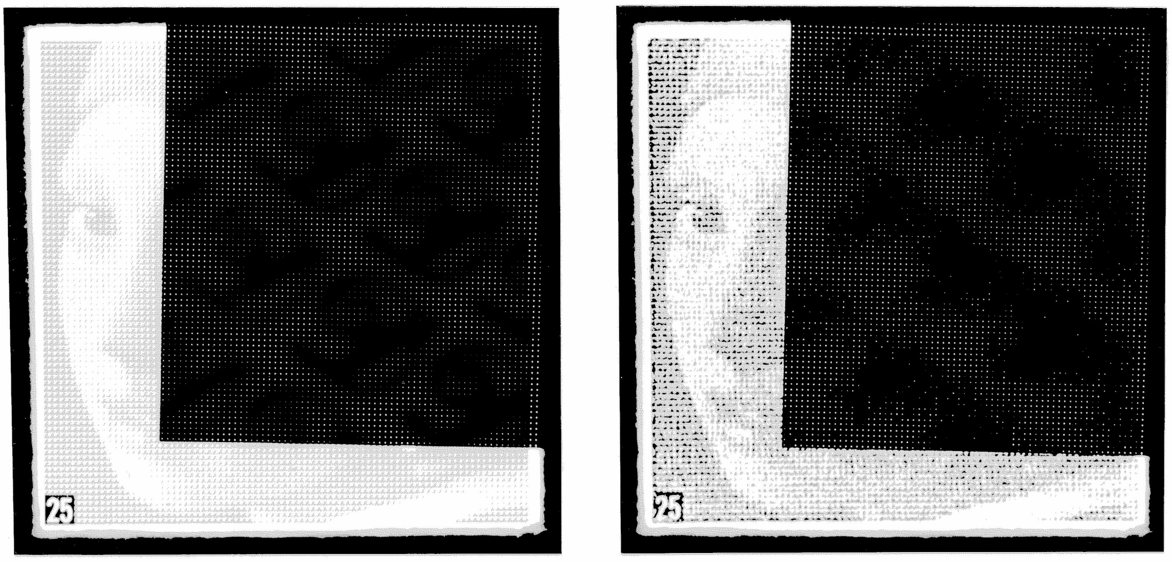


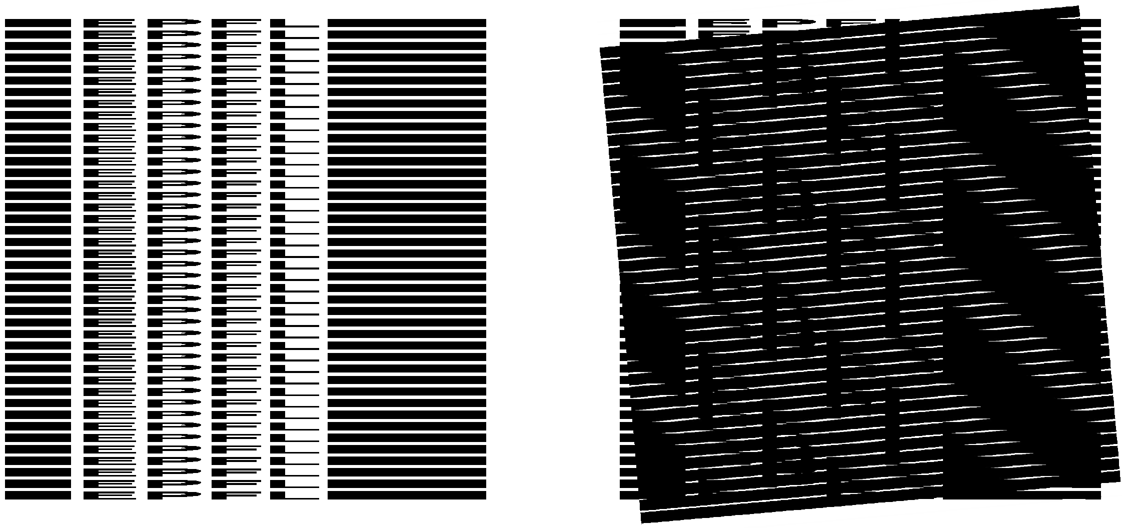
Figure 3. “Girl with a Pearl Earring” by Vermeer, halftoned with a dot screen whose microstructure elements (screen dots) consist of the letter D in a nice calligraphic font (magnified approx. 4 times). The inset shows a largely magnified detail from the eye.



(a) (b)

Figure 4. (a) Moiré intensity profiles with the shape of the calligraphic letter D which appear when a corresponding master screen is superposed on top of the halftoned image (basic screen) of Figure 3. (b) The result obtained when the same master screen is laid on a photocopy of the basic screen of Figure 3. Both (a) and (b) are magnified approx. 3 times.

When superposing two line gratings having a similar period, the resulting moiré consists of large linear bands whose properties (periodicity, orientation) depend on those of the original line gratings (see the straight moiré bands in the left and in the right parts of Fig. 5(b)). Assume, now, that we replace the simple black lines of the first grating by lines that incorporate along their main direction some predefined information (such as tiny, flattened letters or symbols), while the other grating consists of a series of linear slits (narrow transparent lines) on a dark or opaque background. As we can see in Figure 5, the superposition of these line gratings gives moiré bands whose intensity profile is a largely magnified (and possibly slanted) version of the information that is incorporated along the lines of the first grating. This interesting phenomenon is explained mathematically, along with numerous illustrative figures, in the above mentioned references.

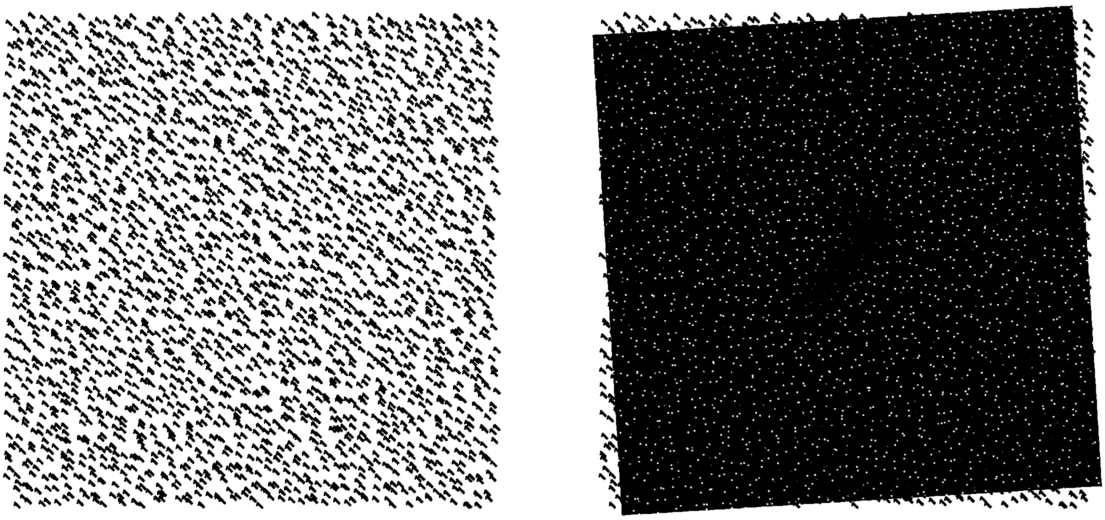


(a) (b)

Figure 5. (a) A periodic line grating whose individual lines contain a flattened version of the letters "EPFL". (b) Its superposition (possibly with a small angle difference) with a second periodic line grating (revealer) which consists of narrow slits on a black background gives a periodic moiré effect whose individual bands contain a largely stretched-out (and possibly sheared) version of the 2D information that is embedded in the individual lines of the first grating. Note that we have intentionally left the left and right parts of grating (a) non-modulated; this allows us to compare in the superposition the modulated moiré bands with the simple moiré bands that are obtained in the classical, non-modulated case.

The 1D moiré method enjoys the same advantages over phase modulation methods as does its 2D counterpart, but it also has some nice properties which make it very useful in anticounterfeiting applications. These include, notably, the larger amount of light that passes through a grating made of line slits (as compared to a 2D pinhole screen), which makes the resulting moiré more easily visible than its 2D counterpart even in difficult light conditions; and the fact that it can carry along its moiré bands information of practically any desired length. But on the other hand, the 1D method is more sensitive to layer rotations than its 2D counterpart, since such rotations do not cause a *rotation* of the resulting moiré as in the 2D case but rather a strong *shearing* effect which may distort the carried information.

Finally, there also exist *random* (or rather *pseudo-random*) variants of both the 2D and the 1D methods described above (see Section H.3 in [16]). In these variants, pseudo-random dot screens (or line gratings) are used rather than periodic ones, and as a result the moiré effect that is obtained in the superposition is no longer periodic, and consists of a single moiré shape (magnified 2D element or 1D band, respectively). Since the moiré effect is only obtained when the element locations in the revealing layer (dots or lines) are correlated with the element locations in the base layer, i.e. when both of them have been prepared using the same sequence of random numbers, these random variants offer an additional, built-in encryption that offers additional security options [17]. An example of the 2D variant is shown in Figure 6.



(a) (b)

Figure 6: (a) A pseudo-random dot screen consisting of tiny "1" shapes. (b) Its superposition (possibly with some angle difference) with a random dot screen (revealer) having the same dot locations but consisting of small pinholes on a black background gives a single largely magnified "1"-shaped moiré intensity profile. Both (a) and (b) are shown here largely magnified.

5. Variants, embodiments and applications

In addition to the moiré-based methods as described in Sections 3 and 4, there also exist several variants and embodiments that can be combined with each of these methods. For example, most of these methods can be incorporated (or dissimulated) within a real halftoned image located on the document by allowing the width of the individual lines or dots to vary according to the gray levels of the image in question. Without using the revealer, this image is clearly visible on the document; but when the appropriate revealer is superposed on top of the image, a new moiré effect becomes visible in the same area, whose properties (fixed or dynamic, constant or alternating colours, etc.) depend on the moiré method being used.

In addition, in each of these moiré-based methods, it is also possible to use as a revealer a microlens array with the appropriate frequency (1D or 2D, depending on the case) instead of the simple opaque film with transparent openings (1D slits or 2D pinholes, respectively). The main advantage of microlenses is that they allow more light to pass through the revealer, and hence they can be used in more difficult light conditions, both on transparent support, where the moiré is observed by transmission, and on opaque support, where the moiré is observed by reflection. But microlenses also offer the possibility of using a revealing layer that is fixed onto the basic layer, where the dynamics of the moiré effects are observed by means of a parallax effect that occurs when tilting the object or when one moves in front of it (rather than by moving the revealer on top of the document, as in the original methods described so far).

Another possible variant that can be used in most of these moiré-based methods consists of the application of various geometric transformations to one or both of the moiré generating layers (on the document and on the revealer). Special mathematical calculations allow to design geometrically transformed layers which, in spite of being transformed in themselves, still yield in their superposition the original, undistorted moiré effects (see, for example, Section 4 in [10] or [13]). This makes it even more difficult to counterfeit the document or to reverse engineer it, and may also serve simultaneously as a screen trap, as described in Section 2 above.

Additionally, in most of the above mentioned methods multiple layer information can be also introduced by overprinting several layers on the document, each layer having a different orientation or frequency, so that different revealers (or different orientations of the same revealer) may reveal different moiré patterns that are encoded in the different layers printed on the document.

All the moiré-based methods and variants mentioned above can be applied, alone or in combination, for the protection of security documents such as banknotes, checks, credit cards, identity cards, passports, travel documents, tickets, vouchers, or various business documents. These methods can be also used for the protection of valuable articles and products, such as CDs, DVDs, software packages, medical drugs, perfumes, personal care articles, watches, fashion articles, etc. Various embodiments of these methods can be used, for example where the revealer is incorporated in the product itself or in its package. Concrete examples of such applications are illustrated, for example, in [18] and in [14].

Because moiré methods are typically print-based authentication methods, they can be integrated in the document and printed within the standard printing process, so they do not significantly increase the production cost of the document. But on the other hand, these methods can be also advantageously incorporated within other security elements such as holograms and kinegrams (see, for example, [19] and [20]) or non-standard inks (see, for example, Section 5 in [10]).

6. Conclusions

Many different moiré-based methods for the protection of documents and products have been introduced over the years. In this short survey we review the main methods and classify them into several families according to their properties and functionality. We also describe some of their main variants, compare their advantages, and discuss their various applications in the field of anticounterfeiting. More detailed information on these methods along with many illustrations can be found in the references.

References

[1] Amidror I 2000 *The Theory of the Moiré Phenomenon* (Dordrecht: Kluwer Academic Publishers)

[2] Kipphan H 2001 *Handbook of Print Media* (Berlin: Springer) section 1.4.3

[3] Sharma G (ed.) 2003 *Digital Color Imaging Handbook* (Boca Raton: CRC Press) chapter 6

[4] van Renesse R L 2005 *Optical Document Security* (Boston: Artech House), third edition

[5] Canadian Bank Note Company Ltd. 1968 “Improvements in printed matter for the purpose of rendering counterfeiting more difficult,” UK Patent No. 1,138,011

[6] Alasia A 1998 “Digital anti-counterfeiting software methos and apparatus,” US Patent No. 5,708,717

[7] McGrew S P 1995 “Anticounterfeiting method and device using holograms and pseudo-random dot patterns,” US Patent No. 5,396,559

[8] Amidror I and Hersch R D 1999 “Methods and apparatus for authentication of documents by using the intensity profile of moire patterns,” US Patent No. 5,995,638

[9] Amidror I and Hersch R D 2001 “Method and apparatus for authentication of documents by using the intensity profile of moire patterns,” US Patent No. 6,249,588

[10] Amidror I 2002 “A new print-based security strategy for the protection of valuable documents and products using moiré intensity profiles,” *Optical Security and Counterfeit Deterrence Techniques IV*: Proceedings of SPIE Vol. 4677 (Bellingham: SPIE) ed R. L. Van Renesse pp. 89–100

[11] Amidror I 1994 “A generalized Fourier-based method for the analysis of 2D moiré envelope forms in screen superpositions,” *Journal of Modern Optics* **41** 1837–62

[12] Chosson S 2006 *Synthèse d’Images Moiré* Ph.D. Thesis No. 3434, EPFL, Lausanne (in French)

[13] Hersch R D and Chosson S 2004 “Band moiré images,” Proc. of SIGGRAPH 2004, *ACM Transactions on Graphics* **23** 239–48

[14] Hersch R D and Chosson S 2007 “Authentication of documents and articles by moire patterns,” US Patent No. 7,194,105

[15] Hersch R D and Chosson S 2006 “Model-based synthesis of band moire images for authenticating security documents and valuable products,” Published US Patent Application No. 2006/0003295

[16] Amidror I 2007 *The Theory of the Moiré Phenomenon, Volume II: Aperiodic Layers* (Dordrecht: Springer)

[17] Amidror I 2006 “Authentication with built-in encryption by using moire intensity profiles between random layers,” US Patent No. 7,058,202

[18] Amidror I and Hersch R D 2004 “Authentication of documents and valuable articles by using moire intensity profiles,” US Patent No. 6,819,775

[19] Huang P-P 1999 “Holographic anti-imitation method and device for preventing unauthorized reproduction,” US Patent No. 5,999,280

[20] Schilling A *et al* 2006 “Diffractive moiré features for optically variable devices,” *Optical Security and Counterfeit Deterrence Techniques VI*: Proceedings of SPIE Vol. 6075 (Bellingham: SPIE) ed R. L. Van Renesse pp. 60750V-1–12