Available online at www.sciencedirect.com
ScienceDirect
Optics Communications 273 (2007) 370–378
OPTICS COMMUNICATIONS
www.elsevier.com/locate/optcom

Improved algorithm for image encryption based on stochastic geometric moiré and its application

Minvydas Ragulskis, Algiment Aleksa, Loreta Saunoriene *

Department of Mathematical Research in Systems, Kaunas University of Technology, Studentu 50-222, LT-51368 Kaunas, Lithuania

Received 25 November 2006; received in revised form 13 January 2007; accepted 13 January 2007

Abstract

A technique based on optical operations on moiré patterns for image encryption and decryption is developed. In this method, an image is encrypted by a stochastic geometric moiré pattern deformed according to the image reflectance map. The decryption is performed using pixel correlation algorithm in the encrypted image and the stochastic geometrical moiré pattern. The proposed technique has a number of advantages over existing encryption techniques based on moiré gratings. No original moiré grating can be reconstructed only from the encrypted image. Stochastic moiré grating can be deformed in any direction what is an important factor of encryption security. Finally, the quality of the decrypted image is much better compared to decryption methods based on the superposition of the regular and deformed moiré gratings. The proposed technique has a great potential, because the process is performed using computational algorithms based on optical operations and optical components are avoided.

Keywords: Moiré grating; Image encryption; Reflectance map

1. Introduction

Information security deals with several different aspects of information and its protection. Information security covers not just information but all infrastructures that facilitate its use – processes, systems, services, technology, etc. Three widely accepted elements of information security are confidentiality, integrity and availability.

Images are widely used in different engineering, industrial, medical processes. Image security is an important element of general information security in such applications. Different optical methods have been proposed for image encryption and decryption [1–15]. The use of optical signal processing in the field of image encryption typically involves the use of optical transforms representing quadratic phase systems, to implement the optical Fourier transform (OFT), the optical fractional Fourier transform (OFRT), the Fresnel transform (FST) and the general linear Canonical transform (LCT) [1]. Random phase keys or random shifting stages can be applied after transformation and the process can be repeated for deeper encryption. In general the encrypted field is complex and recording must be carried out using a holographic material or using digital holographic methods. The matrices associated with the effect of a LCT can provide an efficient method for finding the position, spatial extent, spatial frequency extent and the space bandwidth product of the encrypted signal [1]. That can help to identify necessary parameters of the optical set-up like the minimum size of lens apertures and the need for magnification stages at critical stages in the optical system.

Novel volume-hologram encryption system is proposed in [2], the encryption is done by overlapping two holograms in the same volume of the crystal; one is the hologram of the original binary image and the other is that of the complementary image. A multiple image cryptosystem based on different apertures in an optical set-up under a holographic arrangement is proposed in [3]. Based on this

* Corresponding author.
E-mail address: loreta.saunoriene@ktu.It (L. Saunoriene).

0030-4018/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2007.01.055

approach multiple encryption is achieved by changing the pupil aperture mask arrangement of the optical system among exposures. Optical image encryption algorithm based on extended fractional Fourier transform and digital holography technique is proposed in [4]. The encrypted data is stored as a digital hologram by use of an interference with a wave from a random phase mask. The data retrieval is operated by all-digital means.

A number of method have been recently proposed for the encryption of 2-D images using optical systems based on the fractional Fourier transform (FRT) [5]. A novel encryption for optical image based on multistage fractional FRT and pixel scrambling technique is presented in [6]. The principle of pixel scrambling and an optical approach to realize the pixel scrambling and decoding is proposed.

Fractional convolution operation is exploited for optical image encryption in [7]. The algorithm convolves the primary image with the randomly encoded mask in the fractional Fourier domain with the fractional orders as additional keys. Image encryption method based on the fractional wavelet transform (FWT) is proposed in [8] where the image is encrypted by two fractional orders and a series of scaling factors. The optical implementation is suggested and some numerical simulations prove its possibility.

An optical encryption method based on geometrical phase, which is originated from polarization manipulation is presented in [9]. The decrypted picture is retrieved by measuring the polarization of the beam emerging from the encrypted element. The encrypted element is achieved by using a computer-generated space-variant subwavelength dielectric grating. A method of image encryption and watermarking by random phase matching based on the idea of double phase encoding and the wave field superposition is proposed in [10]. The encryption approach based on the double random pure-phase enciphering method is proposed in [11]. Phase conjugation operation is conducted in the reconstruction stage with the aid of a photorefractive crystal which stores the encrypted information.

A new encryption scheme using modified exclusive-XOR rules and a phase-wrapping technique is proposed in [12]. For image encryption, a gray image is sliced into binary images, which have the same pixel number, and these images are encrypted by the modified XOR rules with bipolar random images. The decryption process is simply implemented by a phase-visualization system. Hybrid image cryptosystem based on the holographic interference and dyadic permutations is presented in [13]. First, the phase and amplitude of the Fourier transform of an input image are recorded as the intensity information via the holographic interference. The extracted phase is then processed via dyadic permutations by applying the exclusive-OR (XOR) operations to a user key and phase information addresses, while an asymmetric process is used for the decryption. A lensless optical security system based on computer generated phase only masks is proposed in [14]. These masks are located at determined positions along the direction of propagation so as to decrypt the target image. These positions coordinates are used as encoding parameters as well as the wavelength in the encryption process.

Applicability of image encryption technique based on moiré pattern is presented in [15]. This technique encrypts an image by a fringe pattern which is generated by a computational algorithm as a cosine function with shifted argument according to the intensity of the encrypted image. It can be noted that this encryption technique possesses a number of inherent drawbacks. The first one is immunity to breach. The encrypted image contains a well defined structure of grating lines. Though the grating lines are deformed, it is quite easy to calculate the average density of the grating lines (which is constant for the original grating without an encrypted image). Thus anyone can computationally construct the original grating and then the decryption of the encrypted image is a standard and easy computational task. Moreover, rough details of the secret encrypted image can be observed even with a naked eye in the deformed pattern of the grating lines.

The second drawback of the technique proposed in [15] is that the grating lines can be shifted only in the orthogonal direction. Geometric moiré gratings formed from arrays of parallel lines are sensitive only to in-plane deflections in the orthogonal direction to the direction of the grating [16]. Again, one can easily detect the direction of grating from the encrypted image (other grating directions except vertical are not discussed in [15]). Definitely, that is also a facilitating factor for breaking the encryption rule.

The third drawback is the low quality of the retrieved original image. Clearly, the quality of the decrypted image depends from the pitch of the original grating. A finer grating should produce better results. But here comes the fourth embedded drawback – the pitch of the original grating must be large enough to allow the shift (which is proportional to the grayscale intensity of the encrypted image) to fit into one pitch. This drawback will be discussed in detail in the following section.

This paper proposes a new image encryption algorithm based on stochastic geometric moiré.

2. One-dimensional example

A one-dimensional system is analyzed for simplicity. Geometric moiré grating in the state of equilibrium can be interpreted as a harmonic function

$$I_1(x) = \cos^2\left(\frac{\pi}{\lambda}x\right), \tag{1}$$

where λ is the pitch of the grating. Numerical values of the function I_1 represent grayscale color levels; 0 corresponds to black, 1 – to white color. Moiré grating in the deformed state can be expressed as [15,17]

$$I_2(x) = \cos^2\left(\frac{\pi}{\lambda}(x - f(x))\right), \tag{2}$$

where $f(x)$ is the deflection from the state of equilibrium at point x.

If the grating in the state of equilibrium I_1 is superposed with the negative copy of the deformed grating I_2 (subtractive superposition), the intensity of the produced moiré image $I_d(x)$ can be expressed as

$$I_d(x) = \frac{1}{2}(I_1(x) + \overline{I_2}(x)) = \frac{1}{2} - \frac{1}{2}\sin\left(\frac{2\pi}{\lambda}\left(1 - \frac{f(x)}{2x}\right)x\right)\sin\left(\frac{\pi}{\lambda}f(x)\right), \quad (3)$$

where $\overline{I_2}(x) = 1 - I_2(x)$. The envelope function of the produced moiré pattern represents the inverse approximation of the original deflection function $f(x)$

$$\frac{1}{2} \pm \frac{1}{2}\sin\left(\frac{\pi}{\lambda}f(x)\right). \quad (4)$$

It can be noted that the shape of the envelope function corresponds to the original deflection function $f(x)$ if and only if the numerical value of $f(x)$ (deflection) at any point x does not exceed the half of the pitch of the geometric moiré grating in the state of equilibrium [16]

$$f(x) \leqslant \frac{\lambda}{2}. \quad (5)$$

So the pitch of the grating must be pre-chosen in accordance with the function $f(x)$ in order to assure its correct reconstruction. Alternatively, function $f(x)$ can be digitally multiplied by a constant c before the encryption process in order to fulfill the requirement of Eq. (5). If the values of $f(x)$ vary between 0 and 1, the best contrast of the reconstruction is obtained when the multiplicative constant c is equal to $\frac{\lambda}{2}$. The envelope function then becomes $\frac{1}{2} \pm \frac{1}{2}\sin\left(\frac{\pi}{2} \cdot f(x)\right)$.

This paper proposes a technique for decryption of $f(x)$ without limitations to the pitch of grating or to the multiplicative constant c. This technique is based on correlation analysis of pixels' intensity in the images of deformed and original grating. The basic principle of this technique is illustrated in Fig. 2. Its computational implementation can be illustrated by the following algorithm (adapted for one-dimensional vectors $I_1(x)$ and $I_2(x)$):

```
STEP 0 Read master grating I1 and encrypted
       image I2; distance between adjacent
       pixels h; number of pixels m in I2;
       Select c, ε;
       Define L as a logical variable;
STEP 1 Repeat for i = round (1 + c/h) to m
         Compute j = round (i − c/h);
         Assign L = false;
         Repeat while not L, for k = i downto j
           if I2(i) − I1(k) = 0
             then
               Compute f(i) = (i − k) * h/c;
               Assign L = true;
             end;
           if |I2(i) − I2(i − 1)| >= ε
             then
               Assign L = false;
             end;
       end;
     end.
```

Such decryption algorithm possesses a number of advantages over algorithms which are based only on simple evaluations of the envelope functions [15]. The main advantage is the accuracy of the reconstruction what is illustrated in Fig. 3. It can be noted that the results in Fig. 3 are produced from the signals (a) and (c) presented in Fig. 1. Optical moiré principles are used to encrypt the secret signal. But its decryption is performed already in pure computational environment and is based on correlation analysis between the original and deformed gratings. The quality of the results is incomparable with

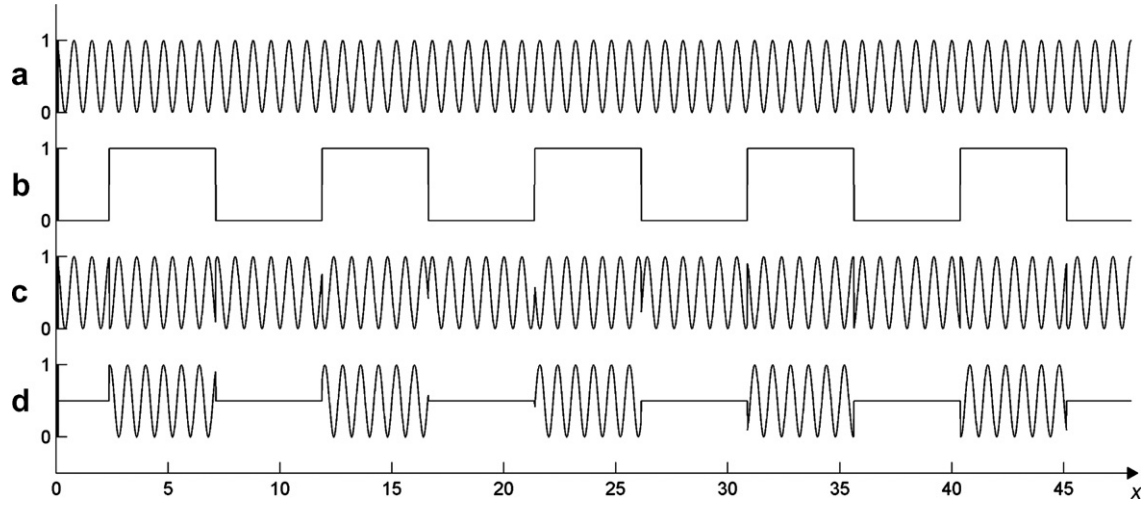

Fig. 1. Encryption; regular moiré grating: (a) regular grating I_1; $\lambda = 0.8$; (b) secret function $f(x)$ to be encrypted; (c) encrypted image – regular grating in the deformed state I_2; $c = 0.4$; (d) envelope function $(I_1 + \overline{I_2})/2$.

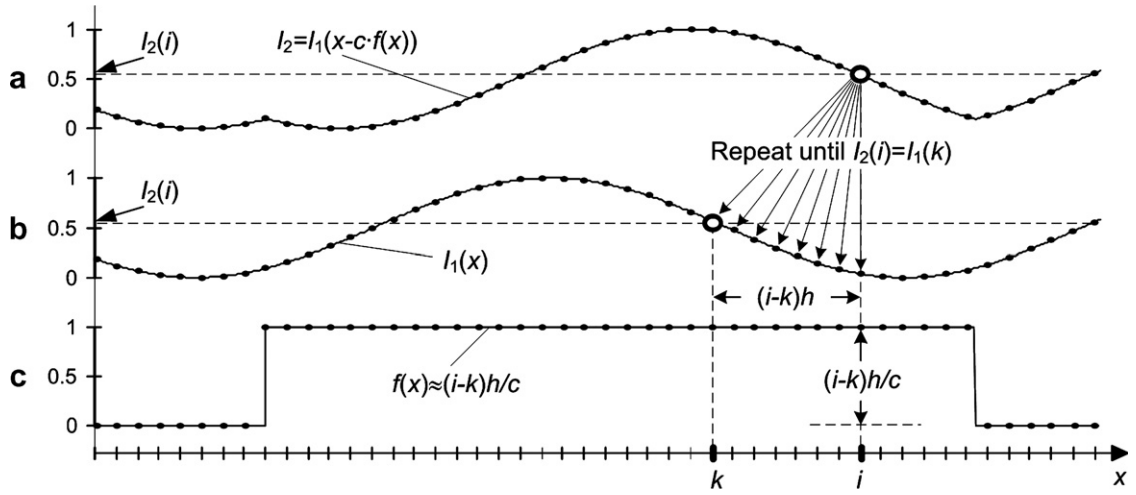

Fig. 2. Decryption of the intensity of the ith pixel of $f(x)$: (a) grating in the deformed state I_2 (encrypted image); (b) original grating I_1; (c) decrypted function $f(x)$.

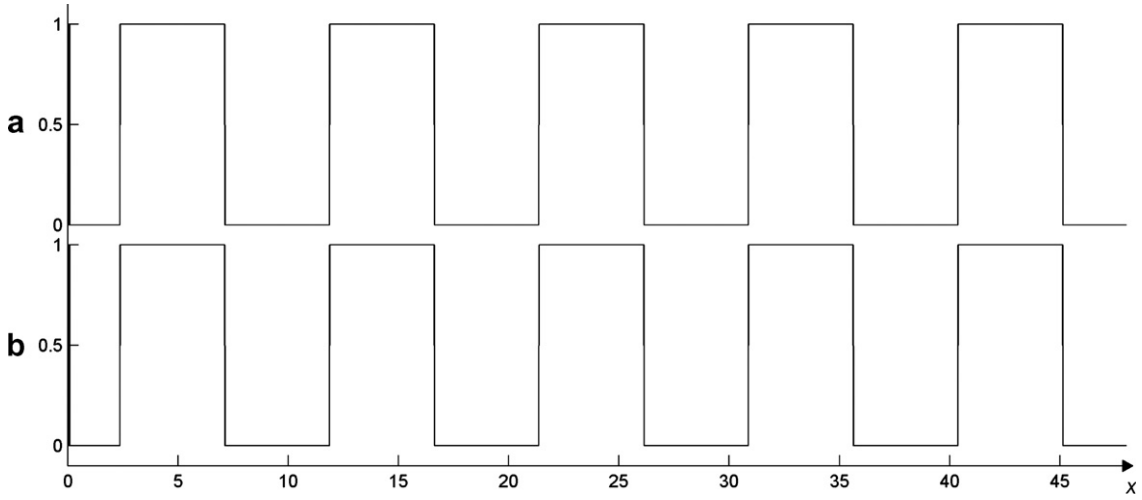

Fig. 3. Decryption; regular moiré grating: (a) secret function $f(x)$; (b) decrypted signal.

the results produced by any approximations of the envelope functions. The decrypted signal can be even digitally filtered to produce even better results (what is unnecessary for example in Fig. 3).

3. One-dimensional stochastic grating

Geometric moiré is a powerful experimental technique with numerous applications [16]. One of the drawbacks of this method is that regular geometric moiré gratings can detect displacements or strains only in the direction orthogonal to the master grating lines. Alternatively, stochastic grating exploiting natural stochastic microstructure of a surface does not possess the abovementioned limitation [17]. Moreover, stochastic geometric moiré has substantial advantages over regular geometric moiré if the safety of encryption is considered.

If one-dimensional stochastic (stationary in time) grayscale color intensity distribution (stochastic master grating) is $I_1(x)$ and the secret signal to be encrypted is $f(x)$, then the encrypted signal is produced exploiting classical relationship of geometric moiré

$$I_2(x) = I_1(x - cf(x)), \tag{6}$$

where c is the multiplicative constant. Clearly, Eq. (6) is generalization of Eq. (2). The encryption algorithm then becomes straightforward:

STEP 0 Read master grating I_1 and secret signal f; distance between adjacent pixels h; number of pixels m in I_1; Select c;

STEP 1 Repeat for $i = \mathrm{round}(1 + c/h)$ to m
$I_2(i - \mathrm{round}(c/h)) = I_1(i - \mathrm{round}(c * f(i)/h))$;
end.

The process of encryption of one-dimensional signal into a stochastic moiré grating is illustrated in Fig. 4. One of the main advantages of stochastic geometric moiré

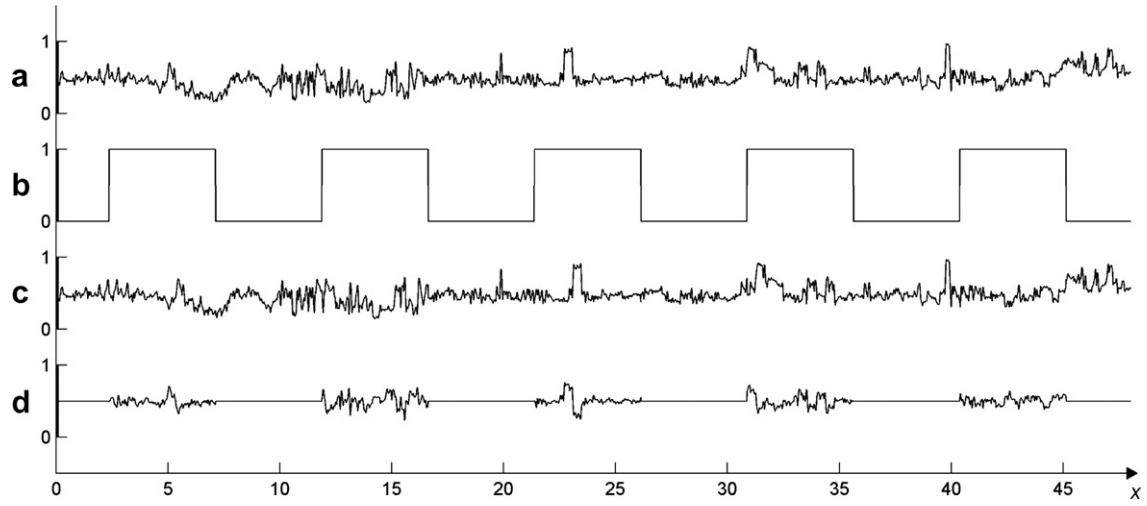

Fig. 4. Encryption; stochastic moiré grating: (a) stochastic grating I_1; (b) secret function $f(x)$; (c) encrypted image – stochastic grating in the deformed state I_2 at $c = 0.4$; (d) envelope function $(I_1 + \bar{I}_2)/2$.

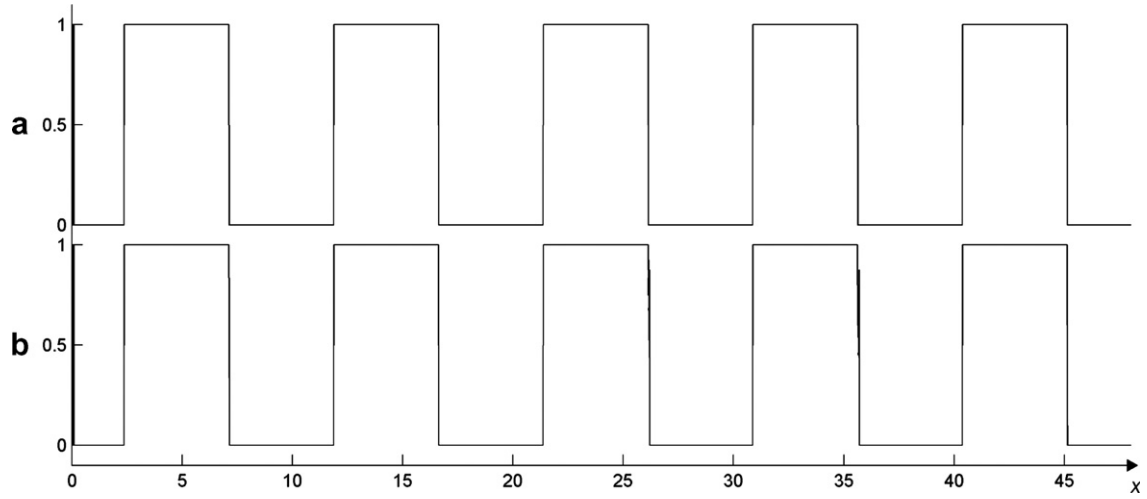

Fig. 5. Decryption using stochastic moiré grating: (a) secret function $f(x)$; (b) decrypted signal.

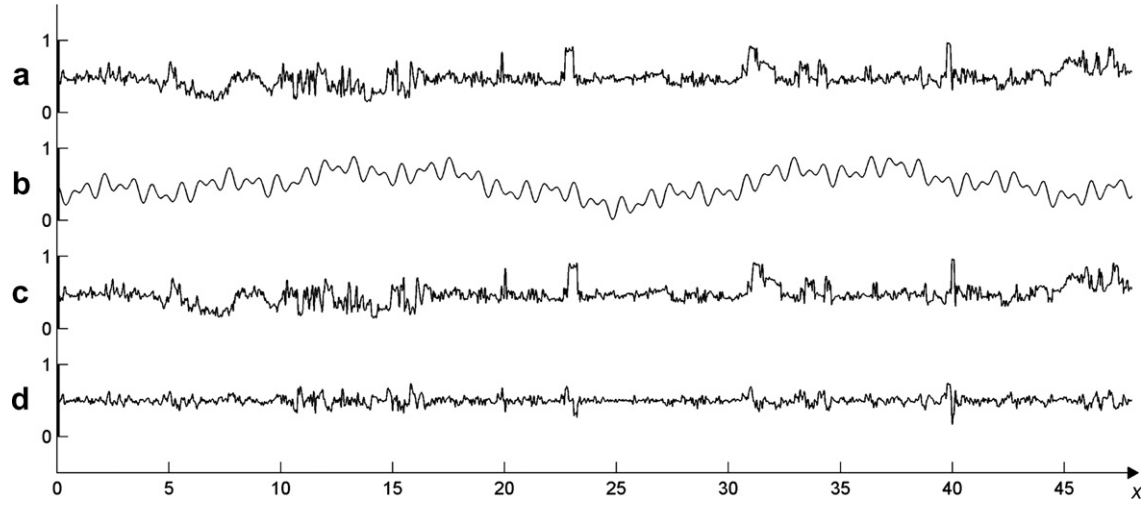

Fig. 6. Encryption using stochastic moiré grating: (a) stochastic grating I_1; (b) secret function $f(x)$; (c) encrypted image – stochastic grating in the deformed state I_2 at $c = 0.4$; (d) envelope function $(I_1 + \bar{I}_2)/2$.

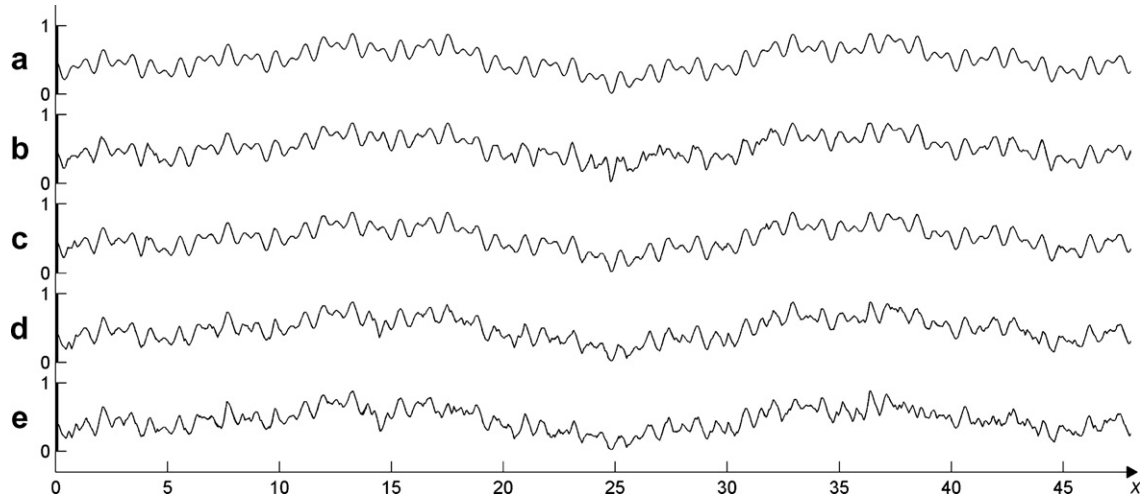

Fig. 7. Decryption using stochastic moiré grating: (a) secret function $f(x)$; (b), (c), (d) and (e) – decrypted signals at $\varepsilon = 0.005$; 0.05; 0.25 and 0.5 respectively.

is clear from Fig. 4c – it is simply impossible even to guess the details of the secret image from the encrypted image (compare to Fig. 1c). Although it can be noted that the construction of the envelope function is very easy when the original stochastic grating is know (Fig. 4d).

Though the envelope function in Fig. 4d characterises the nature of the secret function, it would be very hard to determine its shape just from the approximation of the envelope function. But the application of the decryption algorithm presented in the previous section produces astonishingly good results (Fig. 5), though few irregularities can be noted in the decrypted signal around the breaking points.

Clearly, secret function $f(x)$ can be much more complex that the one used in Figs. 1 and 3–5. That is illustrated in Fig. 6 where the original stochastic grating is the same as in Fig. 4a, but the secret function is much more intricate. Careful shape analysis is required before one could find differences between the original stochastic grating and the encrypted image (Fig. 6a and c), whereas the envelope function (Fig. 6d) is in fact useless.

Nevertheless, decryption algorithm produces excellent results, though it is sensitive to ε (Fig. 7). It can be noted that the best quality of decryption is achieved when ε is equal to 0.05 (Fig. 7c). The choice of the constant ε depends on the function which is encrypted. It must be small enough for rather smooth, slightly varying functions. Whereas the decryption of violently varying function requires relatively large values of ε. Numerical values of constants c and ε can be preselected for typical stochastic gratings and secret functions.

4. Two-dimensional stochastic image encryption

The most simple two-dimensional harmonic moiré reference grating comprising an array of parallel lines can be obtained as

$$I_1(x,y) = a + b\cos^2\left(\frac{\pi}{\lambda}x\right), \tag{7}$$

where $a(x,y)$ and $b(x,y)$ are the background intensity and contrast of the grayscale grating, respectively. Moiré grating deformed by an intensity function $f(x,y)$ is described as

$$I_2(x,y) = I_1((x - f(x,y)),y) = a + b\cos^2\left(\frac{\pi}{\lambda}(x - f(x,y))\right). \tag{8}$$

For an ideal computational environment $a(x,y) = 0$, $b(x,y) = 1$ and the intensity range [0; 1] is subdivided into 256 subintervals producing 256 discrete grayscale intensity levels.

In general case the stochastic moiré grating $I_1(x,y)$ can be represented as a grayscale image comprised of a two-dimensional array of pixels. Then the secret image $f(x,y)$ is encrypted into the stochastic grating $I_1(x,y)$ which is deformed in accordance to $f(x,y)$. As a stochastic grating can be deformed in any direction (not necessarily in the direction perpendicular to the grating lines) [17], the encrypted image reads

$$I_2(x,y) = I_1((x - \cos(\alpha)f(x,y)),(y - \sin(\alpha)f(x,y))), \tag{9}$$

where α is the direction of deflection of the stochastic moiré grating.

The image to be encrypted and decrypted is represented in gray level. The formation of the image to be encrypted is based on reflectance map [15], whose intensity is captured by a CCD camera and the optical process of encryption and decryption is performed using computational algorithms. These computational algorithms are based on optical concepts. In this manner optical components are avoided, which means that it is a virtual optical method.

The set-up used to encrypt and decrypt an image is analogous to the arrangement discussed in [15] and comprises a computer, CCD camera and frame grabber. CCD camera captures the reflected light intensity and an image is formed

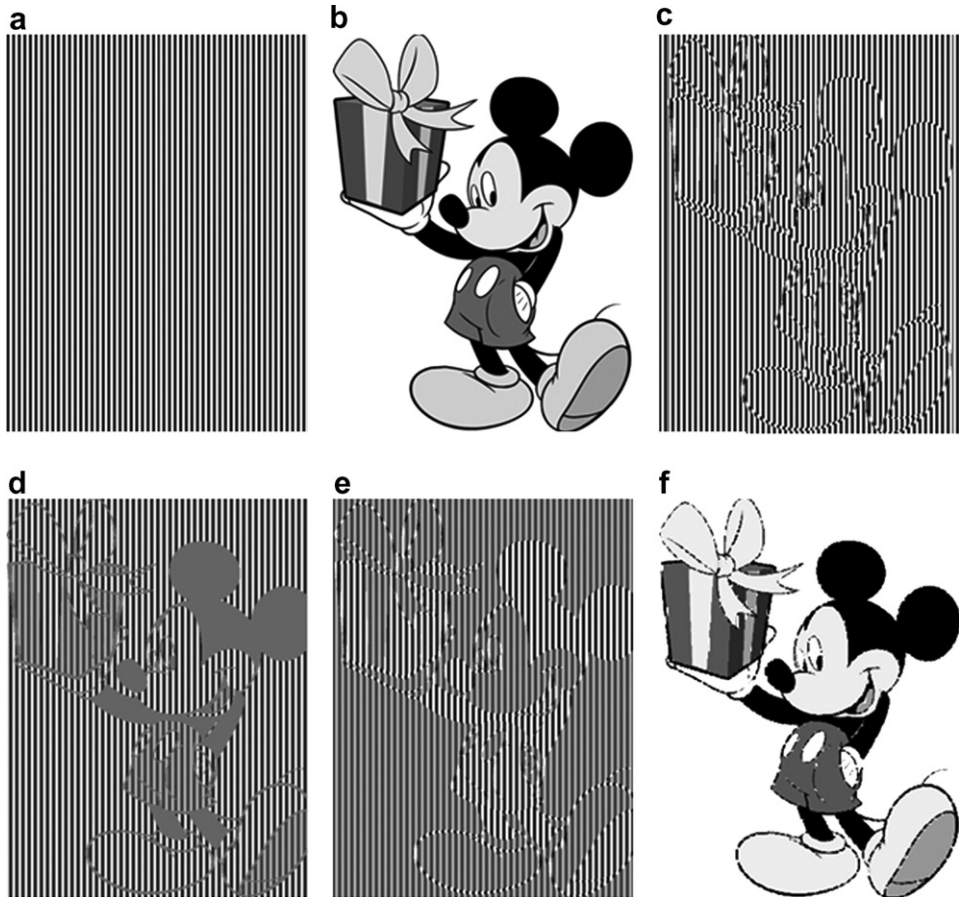

Fig. 8. Image encryption and decryption using regular moiré grating: (a) regular moiré grating; (b) secret image; (c) encrypted image; (d) subtractive superposition of the regular grating and encrypted image; (e) additive superposition of the regular grating and encrypted image; (f) decrypted image produced by the improved algorithm.

in the CCD array. The frame grabber converts electrical signals to a file with gray level values which corresponds to a two-dimensional secret image $f(x,y)$. This image is used to encrypt its information by stochastic moiré pattern for sharing data storage and transmission in electronic way.

Visual cryptography is a powerful method for sharing and encrypting information, especially images [18]. In this technique, the secret image to be encrypted is the reflectance map. Under certain reflection properties, an image can be represented as reflectance map which can be interpreted as a function of three angles $f(i,e,g)$ [15]. The angle i is the angle between the incident ray and the surface normal, the angle e is the angle between the emergent ray and the surface normal, and the angle g the angle between the incident and the emergent ray. An approximation of the reflectance function can be represented by [19]

$$f(i,e,g) = I_0\rho\cos(i), \tag{10}$$

where ρ is the albedo of reflectance factor, I_0 is the incident light intensity and the cosine of the incident angle represents the foreshortening of the surface from the direction of the source. The image intensity is equivalent to the reflectance map

$$f(x,y) = f(i,e,g). \tag{11}$$

Therefore the digital grayscale image represents a reflected intensity map of the secret image. This reflectance map $f(x,y)$ is used to generate the encrypted pattern. The computational algorithms used for image encryption and decryption are analogous to the ones described for one-dimensional grating, though some adaptation is necessary to cope with the arbitrary selected angle of deflection α.

5. Experimental results

The experimental set-up is a computational process. It is a method of virtual optics and uses optical concepts to perform image encryption. The basic set-up is analogous to computational set-up presented in [15] and comprises a CCD camera which captures the image to be encrypted and computer which performs the encryption and decryption process. The major difference though is in the computational algorithms used for the encryption and decryption of the secret images.

First of all, a more advanced optical concept is exploited for image encryption (stochastic geometric moiré instead of regular geometric moiré). Secondly, a much more advanced algorithm is used for image decryption. We use pixel based

color intensity reconstruction algorithm. Its functionality and the quality of the decrypted image are better by far than additive (or subtractive) superposition of the regular and deformed gratings and subsequent low pass filtering [15]. Thirdly, the immunity of our technique against breach is incomparably better – exploitation of stochastic gratings for image encryption in fact eliminates the possibility of visual perception of the encrypted image.

Image encryption and decryption using regular geometric moiré is presented in Fig. 8. The image to be encrypted (Fig. 8b) is downloaded from http://www.magicalears.com. The encrypted image (Fig. 8c) can hardly be considered as a safe method for transmitting secret information. Moreover, subtractive and additive superposition of the encrypted image and the original grating produces images of poor quality (Fig. 8d and e). Decryption techniques based on superposition [15] require complex image filtering techniques; nevertheless the quality of the decrypted image is low. Our proposed improved algorithm works much better, though still some noise can be detected in the decrypted image (Fig. 8f).

Our proposed encryption technique can encrypt images not only into regular moiré gratings, but also into any gray-scale image. This is illustrated in Fig. 9. Stochastic moiré grating is produced by cutting a section out of the image used for encryption (Fig. 9c). The cutting procedure is an additional security factor. The location and the angle of the cut section can be selected without limitations except one – the size of the image representing stochastic moiré grating must correspond to the size of the image to be encrypted.

Only a very close look at Fig. 9d (encrypted image) can detect differences from Fig. 9c (stochastic moiré grating). That is one of the greatest advantages of the proposed method. The quality of the decrypted image (Fig. 9e) confirms the applicability of the proposed technique in different engineering and scientific applications.

We calculate the root mean square error (rms) to evaluate the error of the decrypted image in respect to the original image

$$\mathrm{rms} = \frac{1}{256}\sqrt{\frac{1}{nm}\sum_{i=1}^{n}\sum_{j=1}^{m}(O_{ij} - D_{ij})^2}, \tag{12}$$

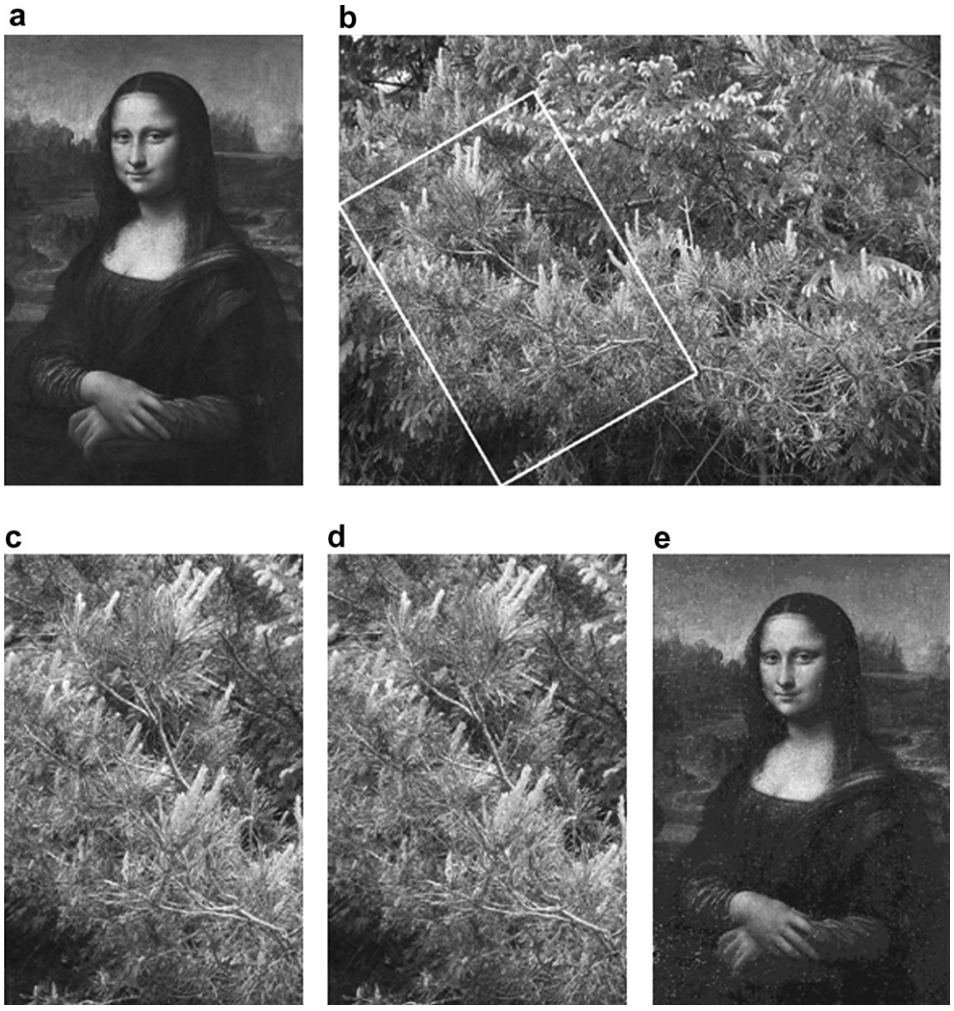

Fig. 9. Image encryption and decryption using stochastic moiré grating: (a) secret image to be encrypted; (b) image used for encryption; (c) stochastic moiré grating produced by cutting a section out of the image used for encryption; (d) encrypted image; $c = 1$; (e) decrypted image.

where n and m are the numbers of pixels in the horizontal and vertical direction of the image accordingly; O_{ij} and D_{ij} are the grayscale intensity of a pixel at position (i, j) in the original and the decrypted images accordingly; 256 stands for the number of discrete grayscale intensity levels. The rms error of the decrypted image in Fig. 9e is 0.0706 what is a very good result if compared with analogous decryption techniques [15].

6. Conclusions

A technique for image encryption and decryption based on stochastic moiré is presented in this paper. The described technique provides a valuable tool for sharing and storing images in electronic way. This technique is a virtual optical process, whose optical operations are performed by computational algorithms. The encryption is performed by deforming a stochastic moiré grating in accordance to the grayscale intensities of the encrypted image. The decryption is performed by correlating pixel intensities in the encrypted image and the original stochastic moiré grating. The presented technique shows excellent repeatability and introduces low error in the decrypted image in respect of the original image.

References

[1] B.M. Hennelly, J.T. Sheridan, Opt. Commun. 247 (4–6) (2005) 291.
[2] H. Kim, Y.H. Lee, Opt. Commun. 258 (1) (2006) 9.
[3] J.F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, Opt. Commun. 261 (1) (2006) 29.
[4] X. Wang, D. Zhao, L. Chen, Opt. Commun. 260 (2) (2006) 449.
[5] B.M. Hennelly, J.T. Sheridan, Optik – Int. J. Light Electron. Opt. 114 (6) (2003) 251.
[6] J. Zhao, H. Lu, X. Song, J. Li, Y. Ma, Opt. Commun. 249 (4–6) (2005) 493.
[7] B. Zhu, S. Liu, Opt. Commun. 195 (5–6) (2001) 371.
[8] L. Chen, D. Zhao, Opt. Commun. 254 (4–6) (2005) 361.
[9] G. Biener, A. Niv, V. Kleiner, E. Hasman, Opt. Commun. 261 (1) (2006) 5.
[10] M.Z. He, L.Z. Cai, Q. Liu, X.C. Wang, X.F. Meng, Opt. Commun. 247 (1–3) (2005) 29.
[11] J.F. Barrera, R. Henao, M. Tebaldi, R. Torroba, N. Bolognini, Opt. Commun. 260 (1) (2006) 109.
[12] C.M. Shin, S.J. Kim, Opt. Commun. 254 (1–3) (2005) 67.
[13] Y.C. Chang, H.T. Chang, C.J. Kuo, Opt. Commun. 236 (4–6) (2004) 245.
[14] G. Situ, J. Zhang, Opt. Commun. 232 (1–6) (2004) 115.
[15] J.A. Munoz-Rodriguez, R. Rodriguez-Vera, Opt. Commun. 236 (2004) 295.
[16] A.S. Kobayashi (Ed.), Handbook on Experimental Mechanics, second ed., SEM, 1993.
[17] M. Ragulskis, R. Maskeliunas, L. Saunoriene, Exp. Techn. 29 (6) (2005) 41.
[18] M. Naor, A. Shamir, Advances in Cryptography – Euracrypt 94 950 (7) (1995) 1.
[19] K.R. Castelan, Digital Image Processing, Prentice-Hall, USA, 1979.