Optics Communications 335 (2015) 161–167

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Image communication scheme based on dynamic visual cryptography and computer generated holography

Paulius Palevicius, Minvydas Ragulskis *

Research Group for Mathematical and Numerical Analysis of Dynamical Systems, Kaunas University of Technology, Studentu 50-147, Kaunas, LT-51368, Lithuania

ARTICLE INFO

Article history:
Received 18 July 2014
Received in revised form
11 September 2014
Accepted 14 September 2014
Available online 29 September 2014

Keywords:
Moire
Computer generated holograms
Holography

ABSTRACT

Computer generated holograms are often exploited to implement optical encryption schemes. This paper proposes the integration of dynamic visual cryptography (an optical technique based on the interplay of visual cryptography and time-averaging geometric moiré) with Gerchberg–Saxton algorithm. A stochastic moiré grating is used to embed the secret into a single cover image. The secret can be visually decoded by a naked eye if only the amplitude of harmonic oscillations corresponds to an accurately preselected value. The proposed visual image encryption scheme is based on computer generated holography, optical time-averaging moiré and principles of dynamic visual cryptography. Dynamic visual cryptography is used both for the initial encryption of the secret image and for the final decryption. Phase data of the encrypted image are computed by using Gerchberg–Saxton algorithm. The optical image is decrypted using the computationally reconstructed field of amplitudes.

1. Introduction

A diffractive optical element (DOE) is a component that modifies wavefronts by segmenting and redirecting the segments through the use of interference and phase control [1]. DOE incorporation in the optical setup allows to change and control the shape of a laser beam. It provides almost the same optical functionality as elements of the refractive optics such as optical lenses, prisms and spheres. DOEs are much smaller and lighter compared to standard elements of the refractive optics. DOEs can be implemented in the form of a transparency or a reflecting mirror. Various techniques are used for the manufacturing of DOEs such as half-tone masking technique [2], diamond turning [3], electron or ion beam writing [4,5], and other techniques. E-beam lithography is the tool of choice for such applications which require high quality and sophisticated hologram masters – even though e-beam direct writing has the disadvantage of a higher fabrication cost [6]. The use of standard electron-beam lithography for the fabrication of a computer generated hologram (CGH) is discussed in [5]. The surface structures are either etched in fused silica or embossed in various polymer materials for low-cost mass production and replication applications [4]. Most DOEs production technologies have matured from microelectronics and MEMS micro-fabrication techniques.

A CGH is different from an optical hologram in the sense that there is no need to use real objects in the recording stage. Various computational algorithms are used to design a CGH of a non-existent, synthetic or even a virtual object. The functionality of a DOE can be optimized mathematically rather than experimentally [4]. CGHs are applied in the fabrication of high spatial-frequency gratings [7], direct laser beam writing [8], gray-tone lithography [9]. An estimate of the phase hologram can be computed by using classical iterative Fourier transform algorithms such as Gerchberg–Saxton algorithm [10] or adaptive-additive algorithm [11]. The most popular method used to generate the computer generated holograms is Gerchberg–Saxton algorithm.

CGHs have been often exploited to implement various image encryption schemes. One of the examples is the method of optical image encryption with a binary CGH and pixel-scrambling technology [12]. The orders of the pixel scrambling as well as the encrypted image are used as the keys to decrypt the original image in this method. The other method allows optical color image encryption based on computer generated hologram and chaos theory [13]. The tricolor separated images of the secret image are encoded with three random phase arrays constructed by a chaotic sequence of the deterministic non-linear system in this method. Then Burch's encoding method using the modified off-axis reference beam is adopted to fabricate the CGH as the encryption image.

Optical multiple-image authentication based on modified Gerchberg–Saxton algorithm with random sampling is proposed

* Corresponding author.
E-mail addresses: paulius.palevicius@ktu.lt (P. Palevicius), minvydas.ragulskis@ktu.lt (M. Ragulskis).

http://dx.doi.org/10.1016/j.optcom.2014.09.041
0030-4018/

in [14]. It is demonstrated that such optical setup is not significantly affected by cross-talk terms and that the quality of recovered images are applicable for optical cryptography applications. A phase-modulated optical system with sparse representation for information encoding and authentication is developed in [15]. The optical cryptosystem is developed with cascaded phase-only masks, and the plaintext is encoded into the cascaded phase-only masks based on an iterative phase retrieval algorithm during the encryption. It is shown that the optical authentication operation with sparsity strategy can provide an additional security layer for the optical security system.

Dynamic visual cryptography is an optical technique based on the interplay of two apparently different methods – visual cryptography and time-averaging geometric moiré. Visual cryptography is a cryptographic technique which allows visual information (such as pictures, text) to be encrypted in such a way that a decryption can be performed by the human visual system, without the aid of computers. Visual cryptography was pioneered by Naor and Shamir [16]. They demonstrated a visual secret image sharing scheme where an image was broken up into a number of shares so that only someone with all shares could decrypt the image. Each share was printed on a separate transparency and decryption was performed by overlaying the shares. When all shares were overlaid the original image would appear. The main difference between geometric moiré and visual cryptography is that a single share is cryptographically secure in the visual cryptography setting (which in general is not true for geometric moiré). In other words, an eavesdropper having a single visual cryptography share has no possibility (visual or computational) to detect the secret image. Since 1994 many advances in visual cryptography have been made. Visual cryptography for color images has been proposed in [17,18]. Ideal contrast visual cryptography schemes have been introduced in [19]. A general multi-secret visual cryptography scheme is presented in [20]; incrementing visual cryptography is described in [21]. A new cheating prevention visual cryptography scheme is discussed in [22]. In contrast to visual cryptography, moiré pattern synthesis applications have not experienced such extensive developments (due to problems associated with cryptographic security).

Time-averaging geometric moiré is a dynamic alternative to static double exposure geometric moiré. A single moiré grating is used in time-averaging geometric moiré. A nontransparent image of the grating is printed on the surface of an oscillating body and time averaging techniques are used to record time-averaged moiré fringes [23]. Time-averaging geometric moiré can be exploited not only for the optical analysis of vibrating structures but also for the synthesis of a predefined pattern of time-averaged fringes. Such type of image hiding technique (when the secret image leaks in the form of a time-averaged moiré fringe in an oscillating non-deformable cover image) was first presented in [24]. A stochastic moiré grating is used to embed the secret image into a single cover image. The secret image can be visually decoded by a naked eye if only the amplitude of the harmonic oscillations corresponds to an accurately preselected value. The fact that a naked eye cannot interpret the secret from a static cover image makes this image hiding technique similar to visual cryptography. Special computational algorithms are required to encode the image; but the decoding is completely visual. The difference from visual cryptography is that only a single cover image is used and that it should be oscillated in order to leak a secret.

The aim of this paper is to propose a new visual image encryption scheme which is based on computer generated holography, optical time-averaging moiré techniques and principles of dynamic visual cryptography. The method proposed in [24] will be used for initial encryption of the secret image and the final decryption. The phase field of the encrypted image will be retrieved by using Gerchberg–Saxton algorithm. A computationally reconstructed amplitude field will be used to decrypt the secret image. Note that image sharing strategy is not employed in dynamic visual cryptography in contrast to classical visual cryptography schemes where the superposition of shares is required to leak the secret image.

The paper is structured as follows. Details about computer generated holography and Gerchberg–Saxton algorithm are given in Section 2. Image hiding based on optical time-averaging moiré scheme is given in Section 3. A new encryption scheme based on computer generated holography and time-averaging moire technique is proposed in Section 4. Finally, concluding remarks are given in Section 5.

2. Computer generated holography

Gerchberg–Saxton algorithm is used for the estimation of the phase field in [10]. A block diagram is presented in Fig. 1. To start the algorithm, a random number generator is used to retrieve a set of phase angles from a stochastic variable distributed uniformly in the interval $[-\pi,\pi]$. The algorithm steps are given as follows:

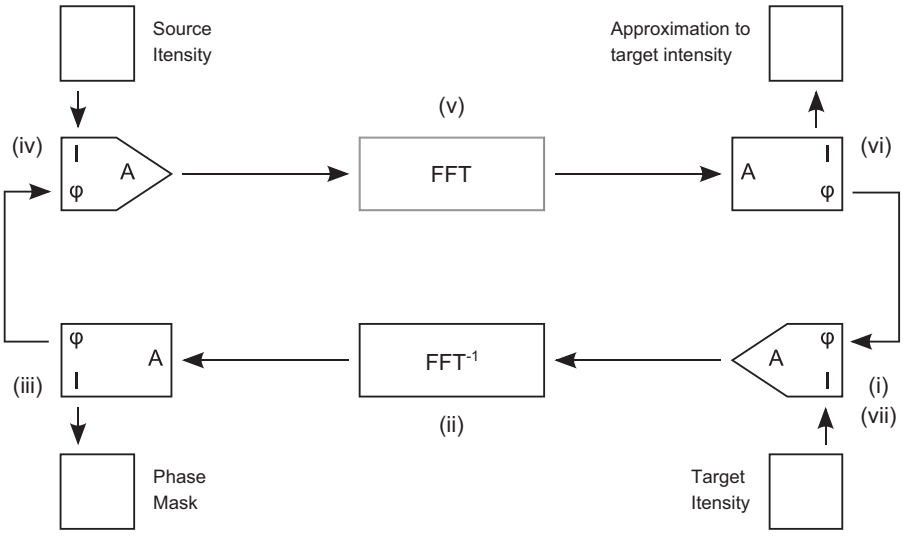

Fig. 1. A block diagram of Gerchberg–Saxton algorithm.

(i) Construct a field with an amplitude given by the square root of the expected irradiance and with a constant phase.
(ii) This field is propagated from the image-plane to the object-plane.
(iii) The amplitude information is discarded leaving only the phase information (for the phase mask).
(iv) The amplitude and phase of the illumination field are added to the phase information in order to obtain the resulting object field.
(v) This field is propagated from the object plane to the image plane.
(vi) The resulting reconstructed image (the square of the field amplitude) is compared with the expected one. The decision to terminate the process (or continue to iterate) is made by computing the correlation between both images.
(vii) The phase from the reconstructed image is combined with the field amplitude obtained from the expected irradiance. The process is repeated from step (i).

Phase distribution is obtained by performing the Fourier transform $\hat{f}$ of the function f:

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \xi}\, dx \tag{1}$$

where ξ is any real number. In this case, a discrete Fourier transform (DFT) is used:

$$\hat{f}(\xi) = \sum_{x=0}^{N-1} f(x) \exp[-2\pi i x \xi / N]. \tag{2}$$

The inverse of DFT is defined as

$$f(x) = N^{-2} \sum_{\xi=0}^{N-1} \hat{f}(\xi) \exp[2\pi i \xi x]. \tag{3}$$

DFT is computed using the fast Fourier transform (FFT) method.

3. Image hiding based on optical time-averaging moiré

Let us consider a one-dimensional harmonic moiré grating:

$$F(x) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x\right) \tag{4}$$

where λ is the pitch of the grating; 0 corresponds to the black color; 1 corresponds to the white color and all intermediate numerical values of $F(x)$ correspond to an appropriate grayscale level. Let us assume that this moiré grating is oscillated around the state of equilibrium (without being deformed), and a deflection from the state of equilibrium does not depend on x:

$$u(x,t) = u(t) = a\ \sin(\omega t + \varphi) \tag{5}$$

where ω is the cyclic frequency; φ is the phase and a is the amplitude of the oscillation. The resultant time-averaged image reads [25]

$$\begin{aligned} \overline{F}(x) &= \lim_{T\to\infty} \frac{1}{T} \int_0^T F(x - a\ \sin(\omega t + \varphi))\, dt, \\ &= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x\right) J_0\left(\frac{2\pi}{\lambda} a\right) \end{aligned}$$

where T is the exposure time and J_0 is the zero-th order Bessel function of the first kind. The original moiré grating is mapped into a time-averaged fringe ($\overline{F}(x) = 0.5$) when J_0 becomes equal to zero. In other words, the explicit relationship among the pitch of the moiré grating λ, the amplitude of harmonic oscillations a and the consecutive number of the time-averaged moiré fringe k reads:

$$\frac{2\pi}{\lambda} a_k = r_k, \quad k = 1, 2, \ldots \tag{6}$$

where r_k is the k-th root of J_0 and a_k is the discrete value of the amplitude which results in the k-th time-averaged fringe in the time-averaged image.

The construction of the image hiding scheme in dynamic visual cryptography is based on the assignment of slightly different pitches for parts of the cover image occupied by the secret and by the background. In other words, time-averaged geometric moiré fringes do leak the secret if the parameters of the oscillations are preselected according to the constitutive formation of original moiré gratings. Stochastic moiré gratings are used in order to conceal the secret in the static cover image. The phase matching algorithm is used to eliminate discontinuities at the boundaries between the background and the secret image; the stochastic initial phase deflection algorithm is used to encrypt the secret (both algorithms are described in detail in [24]). Note that a more sophisticated image hiding scheme in a deformable stochastic moire grating could be used when the cover image is not only oscillated around the state of equilibrium but is also deformed according to one of its eigenshapes. [26].

4. Encryption scheme based on computer generated holography and time-averaging moiré

A new image encryption scheme based on computer generated holography and time-averaging moiré is proposed in this section. The encryption scheme comprises the following steps:

(i) An image hiding technique based on optical time-averaging moiré is used to encrypt the secret image.
(ii) Encrypted data are used as the target image for Gerchberg–Saxton algorithm in order to obtain phase data.
(iii) Various fabrication techniques can now be used to fabricate DOE based on retrieved phase data.

The computational decryption is performed as follows:

(i) DOE is illuminated by a coherent laser beam in the virtual optical environment. Light distribution of the encrypted data is formed in the observation (or the reconstruction) plane.
(ii) Oscillation of DOE by a predefined amplitude allows to decrypt encrypted the image and to acquire the secret image.

A flow chart diagram describing the encryption and the decryption processes is illustrated in Fig. 2. Results of computational experiments illustrating the proposed scheme are shown in Figs. 4 and 5 (the secret image is shown in Fig. 3). Parts (a) and (b) in Fig. 4 show the original encrypted image (the encryption is performed according to the algorithm presented in Section 3). Two computational experiments were performed with 1×1 composite pixel size in (a) and 3×3 composite pixel size in part (b) (note that the resolution of digital images in parts (a) and (b) is different). Corresponding phase data are given in parts (c) and (d). The resulting reconstructed image is given in parts (e) and (f). The results show that 3×3 size of the composite pixel makes the algorithm less prone to noise which is induced by Gerchberg–Saxton algorithm. Fig. 5 illustrates the decryption step. Parts (a) and (b) show the results without using Gerchberg–Saxton algorithm; parts (c) and (d) show results when Gerchberg–Saxton algorithm is applied to the encrypted image; parts (e) and (f) show the contrast enhanced images of (c) and (d). A technique based on [24] can be used for the contrast enhancement.

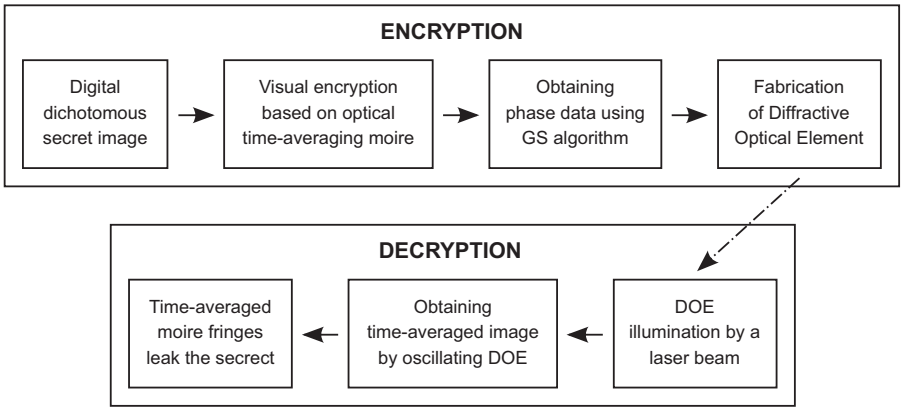

Fig. 2. The encryption and decryption processes.

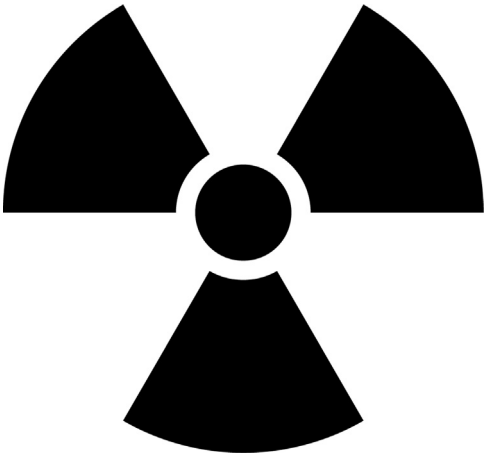

Fig. 3. The secret image.

The quality of the reconstructed secret images could be assessed using formal metrics. A PSNR type metrics is a common choice for the evaluation of the quality of the decryption algorithms [27]. However, a PSNR type metrics is not directly applicable for the proposed technique simply because the original secret digital image is a black and white image – and the reconstructed image is a grayscale image. The secret image is leaked in a pattern of time-averaged moiré fringes in a stochastic grayscale background. A direct pixel by pixel comparison between these two images is irrelevant.

The quality of the reconstruction of the secret image in our case could be evaluated by the ratio of the smoothness of areas occupied by time-averaged moiré fringes and the smoothness of the background (the smaller is this ratio, the better is visual interpretability of the decoded secret image). The standard deviation of the grayscale level around the mean grayscale level in a particular zone of the time-averaged image is introduced in [28]. Let us denote the quality parameter of the reconstruction of the time-averaged secret image Q as

$$Q = \frac{\sigma(\overline{F_S})}{\sigma(\overline{F_B})} \tag{7}$$

where σ is the standard deviation of grayscale levels of pixels in a given area; $\overline{F_S}$ denotes the area of the digital image occupied by time-averaged moiré fringes (the secret) and $\overline{F_B}$ denotes the area occupied by the background. It is clear that $0 \le Q \le 1$. The secret image is clearly seen when $Q=0$ (the secret image is revealed by ideal time-averaged moire fringes), but it is not interpretable when $Q=1$.

The computed values of the quality parameter Q for time-averaged images in Fig. 5 are listed below: $Q=0.2195$ for part (a); $Q=0.2162$ for part (b); $Q=0.6675$ for part (c); $Q=0.5806$ for part (d); $Q=0.5692$ for part (e) and $Q=0.3464$ for part (f). Note that Gerchberg–Saxton algorithm is not employed for parts (a) and (b) – the additional noise is not added to the cover moiré grating and the resulting time-averaged moiré fringes are almost ideally smooth. But the decrypted secret image is well-interpretable by a naked eye even though the values of Q are much higher for parts (c–f).

As mentioned previously, Gerchberg–Saxton algorithm does introduce additional noise to the cover image. Therefore it is important to assess the sensitivity of the time-averaged image to the noise and occlusion contaminations to the encrypted cover image. Thus, we perform a computational experiment by adding a random noise to the digital cover image illustrated in Fig. 4(b).

Fig. 6(a) shows the encrypted cover image with added noise uniformly distributed in interval $[-0.1, 0.1]$. Note that 256 grayscale discrete levels are used (0 stands for the black color; 1 stands for the white color). Each pixel of the cover image is affected by the additive noise; the pixel level is rounded to the nearest discrete grayscale level (the pixel level is set to 0 if the altered grayscale level is lower than 0; analogously the pixel level is set to 1 if the altered level is higher than 1). The time-averaged image of Fig. 6(a) is shown in Fig. 6(c).

Computational experiments are repeated with the random noise uniformly distributed in interval $[-0.2, 0.2]$; the cover image is shown in Fig. 6(b) and the time-averaged image is shown in Fig. 6(d). A naked eye confirms that the proposed optical encryption scheme is robust to noise contamination. Nevertheless, we compute the parameter of the quality of reconstruction Q for Fig. 6(c) ($Q=0.2898$) and Fig. 6(d) ($Q=0.3933$). That confirms the robustness of the system to the additive noise (the value of Q for Fig. 5(b) is 0.2162). Peak signal-to-noise ratio (PSNR) values are also computed between Figs. 5(b) and 6(c) and Figs. 5(b) and 6(c). The values are respectively PSNR$=+40.95$ dB and PSNR$=+36.21$ dB.

Note that the illustrated optical decryption scheme is implemented in a virtual optical environment. Physical realization of the decryption requires an experimental implementation of the DOE on a surface of an oscillating structure. That enables interesting potential of the proposed optical technique for image hiding and optical monitoring applications. The proposed technique can be exploited for vibration monitoring of the whole experimental setup when the reconstructed image performs oscillations around the state of equilibrium in the observation plane. Alternatively the proposed technique can be exploited for visual monitoring of the vibrations of micro-components carrying the DOE. However, in the

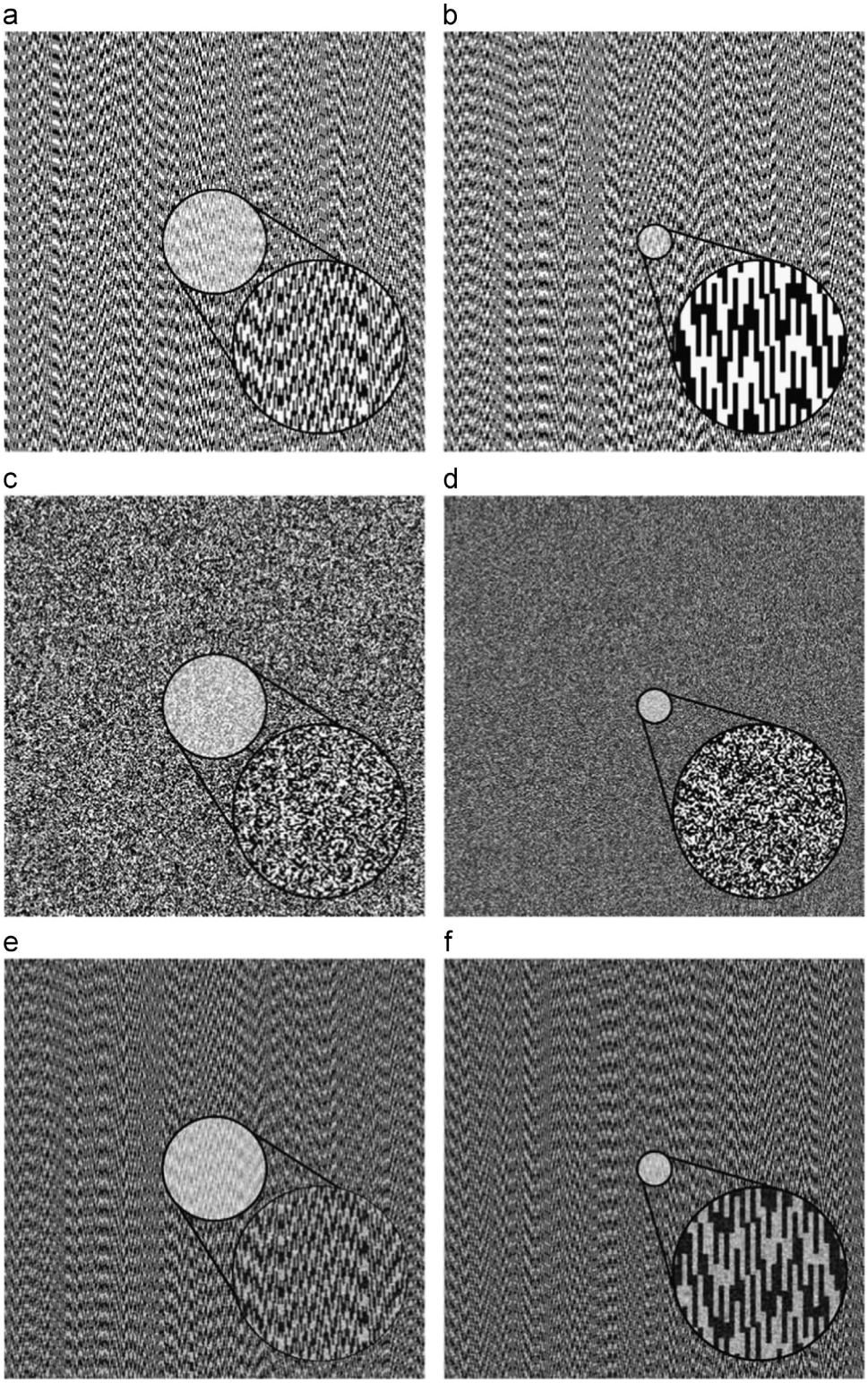

Fig. 4. Computational results for the proposed scheme – the encryption step. The original encrypted image with different composite pixel sizes is shown in (a) and (b); corresponding phase data are shown in (c) and (d); the reconstructed image is shown in (e) and (f).

later case the visual encoding scheme must account deformations happening in the cover image itself – the image hiding technique based on deformable moiré gratings [26] must be used then. In any case, we would like to stress that the main objective of this paper is to propose the fusion of dynamic visual cryptography and computer generated holography. All experimental results presented in this paper are performed in virtual optical environment.

5. Concluding remarks

An image hiding scheme based on computer generated holography and dynamic visual cryptography is proposed in this paper. The secret image is embedded into the stochastic geometric moiré cover image. Gerchberg–Saxton algorithm is used to produce phase data from the encrypted cover image and is directly incorporated into

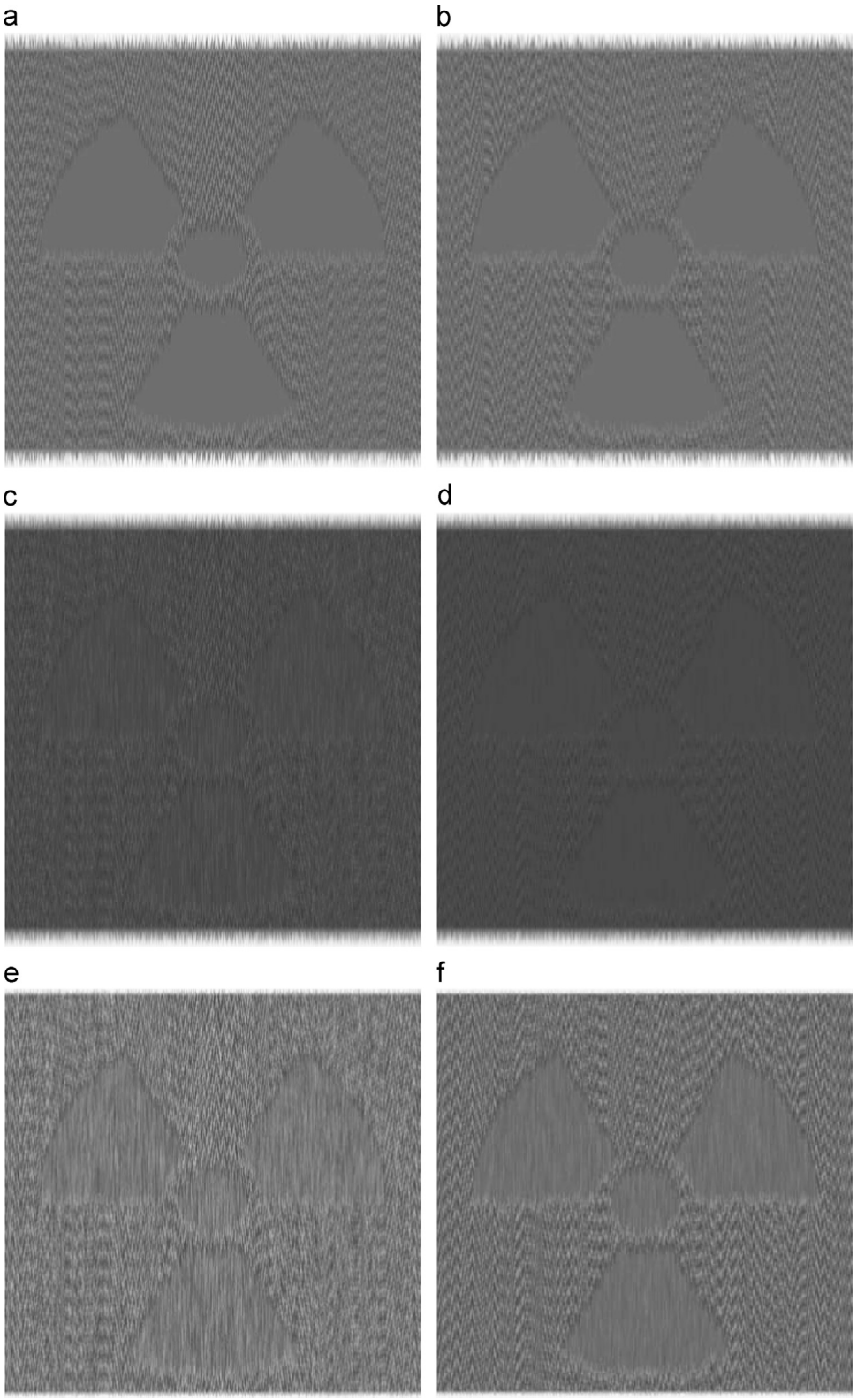

Fig. 5. Computational results for the proposed scheme – the decryption step. The results without using Gerchberg–Saxton algorithm are shown in (a) and (b); the results with Gerchberg–Saxton algorithm are shown in (c) and (d); contrast enhanced images are illustrated in (e) and (f).

CGH. The secret image is leaked from time-averaged pattern of fringes generated by an oscillating CGH image in the projection plane; the decryption is completely optical and does not require an application of a computing device. Moreover, the secret image is not shared into components – the secret is embedded into a single stochastic cover image which is directly used as a target image for the Gerchberg–Saxton algorithm.

So far only the applicability of this technique in virtual optical environments was demonstrated. However, unleashing the potential of the proposed technique in experimental applications

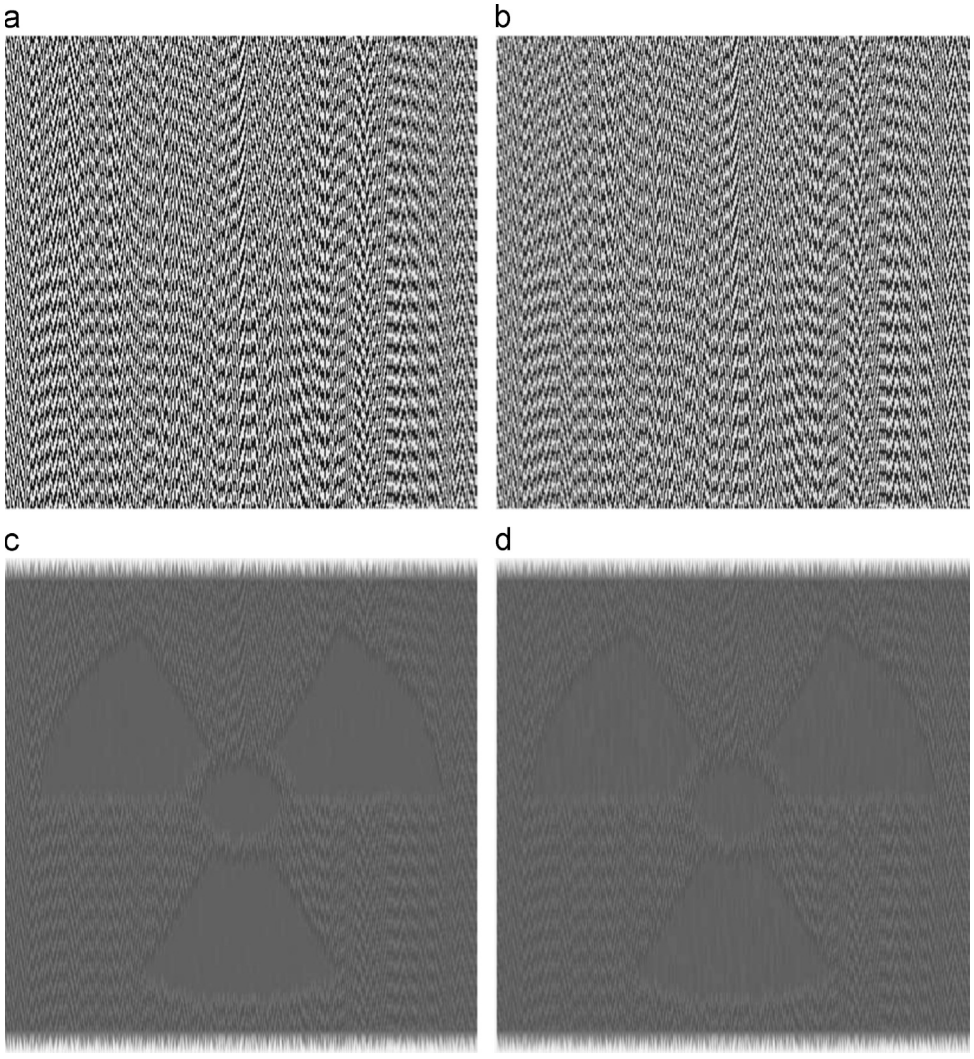

Fig. 6. The robustness of the proposed scheme to the additive noise: the encrypted cover with the added noise uniformly distributed in interval [−0.1, 0.1] is shown in (a); with the noise distributed in interval [−0.2, 0.2] is shown in (b). The decrypted images of (a) and (b) are shown respectively in (c) and (d).

(especially for optical monitoring of movable components of MEMS) remains a definite object of future research.

Acknowledgements

Financial support from the Lithuanian Science Council under Project no. MIP-100/2012 is acknowledged.

References

[1] D. Shea, Diffractive Optics: Design, Fabrication, and Test, SPIE Press, Bellingham, Washington, 2004.
[2] F. Quentel, J. Fieret, A.S. Holmes, S. Paineau, Laser Appl. Microelectron. Optoelectron. Manuf. VI, http://dx.doi.org/10.1117/12.432538, in press.
[3] D.C. Smith, Contemporary Methods of Optical Fabrication, http://dx.doi.org/10.1117/12.932733, in press.
[4] J. Turunen, Diffractive Optics for Industrial and Commercial Applications, Akademie Verlag, Berlin, 1997.
[5] J.M. Teijido, H. Buczek, D. Wuthrich, Microelectron. Eng. 9 (1–4) (1989) 255.
[6] F. Gao, J. Zhu, Q. Huang, Y. Zhang, Y. Zeng, F. Gao, Y. Guo, Z. Cui, Microelectron. Eng. 61–62 (2002) 363.
[7] T.J. Suleski, B. Baggett, W.F. Delaney, C. Koehler, E.G. Johnson, Opt. Lett. 24 (9) (1999) 602.
[8] A. Schilling, H.P. Herzig, L. Stauffer, U. Vokinger, M. Rossi, Appl. Opt. 40 (32) (2001) 5852.
[9] E.-B. Kley, L.-C. Wittig, M. Cumme, U.D. Zeitner, P. Dannberg, Micromach. Technol. Diffr. Hologr. Opt, http://dx.doi.org/10.1117/12.360513, in press.
[10] R.W. Gerchberg, W.O. Saxton, Optik 35 (1972) 237.
[11] E.R. Dufresne, G.C. Spalding, M.T. Dearing, S.A. Sheets, D.G. Grier, Rev. Sci. Instrum. 72 (3) (2001) 1810.
[12] Y.-Y. Wang, Y.-R. Wang, Y. Wang, H.-J. Li, W.-J. Sun, Opt. Lasers Eng. 45 (7) (2007) 761.
[13] J. Liu, H. Jin, L. Ma, Y. Li, W. Jin, Opt. Commun. 307 (2013) 76.
[14] W. Chen, X. Chen, Opt. Commun. 318 (2014) 128.
[15] W. Chen, X. Chen, A. Stern, B. Javidi, IEEE Photon. J. 5 (2) (2013) 6900113.
[16] M. Naor, A. Shamir, Eurocrypt '94, Lecture Notes in Computer Science, vol. 950, Visual Cryptography, Springer-Verlag, Berlin, 1995, pp. 1–12.
[17] Y.-C. Hou, Pattern Recognit. 36 (7) (2003) 1619.
[18] S. Cimato, R. De Prisco, A. De Santis, Theor. Comput. Sci. 374 (1–3) (2007) 261.
[19] S. Cimato, A. De Santis, A.L. Ferrara, B. Masucci, Inf. Process. Lett. 93 (4) (2005) 199.
[20] C.-N. Yang, T.-H. Chung, Opt. Commun. 283 (24) (2010) 4949.
[21] R.-Z. Wang, Y.-C. Lan, Y.-K. Lee, S.-Y. Huang, S.-J. Shyu, T.-L. Chia, Opt. Commun. 283 (21) (2010) 4242.
[22] Y.-C. Chen, D.-S. Tsai, G. Horng, J. Vis. Commun. Image Represent. 23 (8) (2012) 1225.
[23] C. Liang, Y. Hung, A. Durelli, J. Hovanesian, J. Sound Vib. 62 (2) (1979) 267.
[24] M. Ragulskis, A. Aleksa, Opt. Commun. 282 (14) (2009) 2752.
[25] M. Ragulskis, Z. Navickas, Exp. Mech. 49 (4) (2009) 439.
[26] R. Palivonaite, A. Aleksa, A. Paunksnis, A. Gelzinis, M. Ragulskis, J. Opt. 16 (2) (2014) 025401.
[27] S.-K. Au Yeung, S. Zhu, B. Zeng, Quality assessment for a perceptual video encryption system, in: 2010 IEEE International Conference on Wireless Communications, Networking and Information Security.
[28] M. Ragulskis, L. Saunoriene, R. Maskeliunas, Exp. Techn. 33 (2) (2009) 60.