Commun Nonlinear Sci Numer Simulat xxx (2013) xxx–xxx

Contents lists available at SciVerse ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

Dynamic visual cryptography based on chaotic oscillations

Vilma Petrauskiene, Rita Palivonaite, Algiment Aleksa, Minvydas Ragulskis *

Research Group for Mathematical and Numerical Analysis of Dynamical Systems, Kaunas University of Technology, Studentu 50-222, Kaunas LT-51368, Lithuania

ARTICLE INFO

Article history:
Received 13 September 2012
Accepted 1 June 2013
Available online xxxx

Keywords:
Visual cryptography
Time average moiré
Chaotic oscillations

ABSTRACT

Dynamic visual cryptography scheme based on chaotic oscillations is proposed in this paper. Special computational algorithms are required for hiding the secret image in the cover moiré grating, but the decryption of the secret is completely visual. The secret image is leaked in the form of time-averaged geometric moiré fringes when the cover image is oscillated by a chaotic law. The relationship among the standard deviation of the stochastic time variable, the pitch of the moiré grating and the pixel size ensuring visual decryption of the secret is derived. The parameters of these chaotic oscillations must be carefully preselected before the secret image is leaked from the cover image. Several computational experiments are used to illustrate the functionality and the applicability of the proposed image hiding technique.

1. Introduction

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography was pioneered by Naor and Shamir in 1994 [1]. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n-1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

Since 1994, many advances in visual cryptography have been done. Visual cryptography scheme for grey level images is introduced in [2]. An extended visual cryptography scheme to encode n images is proposed in [3], moreover, after the original images are encoded they are still meaningful, that is, any user will recognize the image on his transparency. Three methods for visual cryptography of gray-level and color images are presented in [4]. Visual secret sharing scheme that encodes n of secrets into two circle shares is proposed in [5], n secrets can be obtained one by one by stacking the first share and the rotated second share with n different rotation angles. Multi secret visual cryptography sharing scheme is introduced in [6–8]. An incrementing visual cryptography scheme using random grids is proposed in [9]. Visual cryptography scheme with reversing is shown in [10]. A new method to achieve progressive image sharing is proposed in [11]. A new two-in-one image secret sharing scheme by combining visual cryptography scheme and polynomial-based image secret sharing scheme is introduced in [12]. A new secret image sharing scheme for true-color secret images is presented in [13]. New algorithms by using random grids to accomplish the encryption of the secret gray-level and color images are presented in [14].

An alternative image hiding method based on time-averaging moiré is proposed in [15]. This method is based not on the static superposition of shares (or geometric moiré images), but on time-averaging geometric moiré. This method generates

* Corresponding author. Tel.: +370 69822456; fax: +370 37330446.
E-mail addresses: vilma.petrauskiene@ktu.lt (V. Petrauskiene), rita.palivonaite@ktu.lt (R. Palivonaite), algiment.aleksa@ktu.lt (A. Aleksa), minvydas.ragulskis@ktu.lt (M. Ragulskis).
URL: http://www.personalas.ktu.lt/~mragul (M. Ragulskis).

1007-5704/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cnsns.2013.06.002

only one picture; the secret image can be interpreted by the naked eye only when the original encoded image is harmonically oscillated in a predefined direction at strictly defined amplitude of oscillation. This dynamic visual cryptography scheme requires a computer to encode a secret, but one can decode the secret without a computing device. Only one picture is generated, and the secret is leaked from this picture when parameters of the oscillation are appropriately tuned. Additional image security measures are implemented in [16] where the secret image is not leaked at any parameters, at any directions of the harmonic oscillation – additional requirements are raised for the time function determining the process of oscillation. Particularly, the secret image can be interpreted by a naked eye in [16] only when the time function describing the oscillation of the encoded image is a triangular waveform (the density function of the time function is a symmetric uniform density function).

The shape of the waveform is optimized in [17] where the criterion of optimality was based on the magnitude of the derivative of the standard at the amplitude corresponding to the formation of the first moiré fringe. The standard is computed as the variation of grayscale levels around the mean grayscale level in the time averaged image while the derivative of the standard in respect to the amplitude of a piece-wise uniform waveform defines the applicable interval of amplitudes for visual decryption of the secret image.

The applicability of dynamic visual cryptography based on time-averaging geometric moiré for experimental control of vibrating systems is discussed in [18]. But experimental implementation of a complex periodic waveform can be a challenging task from the technological point of view (especially if the frequency of oscillations must be kept high). Thus, the main objective of this paper is to investigate the feasibility of chaotic dynamic visual cryptography where the time function determining the deflection of the encoded image from the state of equilibrium is a Gaussian process with zero mean and predetermined variance.

2. Optical background

One-dimensional moiré grating is considered in this paper. We will use a stepped grayscale function defined as follows

$$F(x) = 0.5 + 0.5sign\left(\sin\left(\frac{2\pi}{\lambda}x\right)\right) \tag{1}$$

where λ is the pitch of the moiré grating; the numerical value 0 corresponds to the black color; 1 corresponds to the white color and all intermediate values (which occur in the time-averaged images) correspond to an appropriate grayscale level. $F(x)$ can be expanded into the Fourier series:

$$F(x) = \frac{a_0}{2} + \sum_{k=1}^{+\infty}\left(a_k \cos\left(\frac{2\pi kx}{\lambda}\right) + b_k \sin\left(\frac{2\pi kx}{\lambda}\right)\right) \tag{2}$$

where $a_k, b_k \in R$; $a_0 = 1$; $a_1, a_2, a_3, \ldots = 0$; $b_k = \frac{1+(-1)^{k+1}}{k\pi}$; $k = 1, 2, \ldots$

Let us consider a situation when the described one-dimensional moiré grating is oscillated in the direction of the x-axis and time-averaging optical techniques are used to register the time-averaged image. Time-averaging operator H_a describing the grayscale level of the time-averaged image can be defined as [19]:

$$H_a(x|F;\xi_a) = \lim_{T\to\infty}\frac{1}{T}\int_0^T F(x - \xi_a(t))dt \tag{3}$$

where t is time; T is the exposure time; $\xi_a(t)$ is a function describing dynamic deflection from the state of equilibrium; $a \geqslant 0$ is a real parameter; $x \in R$. It is shown in [16] that if the density function $p_a(x)$ of the time function $\xi_a(t)$ does satisfy the following requirements:

$$p_a(x) = 0 \text{ when } |x| > a;\ p_a(x) = p_a(-x) \text{ for all } x \in R;\ a > 0 \tag{4}$$

then the time-averaged image of the moiré grating oscillated according to the time function $\xi_a(t)$ (as the exposure time T tends to infinity) reads:

$$H_a(x|F;\xi_a) = \frac{a_0}{2} + \sum_{k=1}^{+\infty}\left(a_k \cos\left(\frac{2\pi kx}{\lambda}\right) + b_k \sin\left(\frac{2\pi kx}{\lambda}\right)\right)P_a\left(\frac{2\pi ka}{\lambda}\right) \tag{5}$$

where P_a denotes the Fourier transform of the density function $p_a(x)$. In other words, the time-averaged image can be interpreted as the convolution of the static image (the moiré grating) and the point-spread function determining the oscillation of the original image [20,21].

As mentioned previously, the main objective of this paper is to construct an image hiding algorithm based on the principles of dynamic visual cryptography where the time function describing the oscillation of the encoded image is chaotic. In other words, the decryption of the embedded secret image should be completely visual, but the decoding should be possible only when the encoded image is oscillated chaotically. Note that harmonic oscillations cannot be used for visual decryption of the secret image if it is embedded into a stepped moiré grating due to the aperiodicity of roots of the zero order Bessel function of the first kind [16].

Please cite this article in press as: Petrauskiene V et al. Dynamic visual cryptography based on chaotic oscillations. Commun Nonlinear Sci Numer Simulat (2013), http://dx.doi.org/10.1016/j.cnsns.2013.06.002

3. Theoretical relationships

It is well known that the motion of the registered object (or the registering camera) causes the motion-induced blur [22,23]. Gaussian blur is one of the common factors affecting the quality of the registered image in an optical system [24]. And though the computational deblurring of contaminated images (and of course computational introduction of the Gaussian blur to original images) is a well-explored topic of research, our approach is different from the cryptographic point of view. We will use Gaussian blur to decrypt encoded images. Since such an approach requires the development of specialized encoding algorithms, we will concentrate on the effects taking place when the motion blur is caused by chaotic oscillations. The latter fact requires detailed analysis of time-averaging processes occurring during the Gaussian blur; such simplified approaches when contributions of pixels outside the 3σ range around the current pixel are ignored [25] cannot be exploited in the present computational setup.

Let us assume that $\xi_\sigma(t)$ is a Gaussian normal ergodic process with zero mean and σ^2 variance. Note that the standard deviation σ is used in the subscript instead of the parameter a in Eq. (5). Then, the density function $p_\sigma(x)$ reads:

$$p_\sigma(x) = \frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{x^2}{2\sigma^2}\right) \tag{6}$$

and the Fourier transform of $p_\sigma(x)$ takes the following form:

$$P_\sigma(\omega) = \exp\left(-\frac{1}{2}(\omega\sigma)^2\right) \tag{7}$$

Then, the time-averaged image of the moiré grating oscillated by a Gaussian time function reads [26]:

$$H(x|F;\xi_\sigma) = \frac{1}{2} + \sum_{k=1}^{+\infty}\left(a_k\cos\left(\frac{2\pi kx}{\lambda}\right) + b_k\sin\left(\frac{2\pi kx}{\lambda}\right)\right)\exp\left(-\frac{1}{2}\left(\frac{2\pi k\sigma}{\lambda}\right)^2\right) \tag{8}$$

Eq. (8) describes the formation of the time-averaged image as the exposure time tends to infinity and the oscillation of original moiré grating is governed by the function $\xi_\sigma(t)$. But one must keep in mind that experimental implementation of such oscillations on a digital computer screen would cause a lot of complications. First of all, digital screens are comprised from an array of pixels – thus interpretable deflections from the state of equilibrium must be aliquot to the size of a pixel. Secondly, digital screens have finite refresh rates – thus infinite exposure times cannot be considered as an acceptable option. In that sense, the simulation of optical effects caused by chaotic oscillations is much more difficult compared to harmonic (or periodic) oscillations where a finite number of steps per period of oscillation can be considered as a good approximation of the time-averaging process [15]. Therefore, a detailed investigation of time-averaging processes caused by chaotic oscillations is necessary before the algorithm for the encoding of a secret image can be discussed.

3.1. Computational representation of chaotic oscillations

A Gaussian process can be approximated by a discrete scalar series of normally distributed numbers:

$$\theta(t_j) \sim N(0,\sigma^2), \quad j = 1,2,\ldots \tag{9}$$

where the density function of the Gaussian distribution (Eq. (6)). As mentioned previously, the stepped moiré grating $F(x)$ can be displaced from the state of equilibrium by a whole number of pixels only. Let us denote the size of the pixel as ε ($\varepsilon > 0$). We also assume that the refresh rate of the digital screen is m Hz. Then, each instantaneous image of the displaced moiré grating will be displayed for $\Delta t = \frac{1}{m}$ s. The schematic diagram of the computational realization of discrete chaotic oscillations is shown in Fig. 1 where t denotes time; x denotes the longitudinal coordinate of the one-dimensional moiré grating; empty circles show the distribution of $\theta(t_j)$ (a new random number is generated at the beginning of every discrete time interval); ε denotes the height of the pixel; thick solid lines in the right part of the figure show the deflection of the moiré grating from the state of equilibrium; columns $h_\varepsilon(k)$ illustrate discrete probabilities of the deflection from the state of equilibrium.

Since the distribution of $\theta(t_j)$ is Gaussian, the height of the kth column $h_\varepsilon(k)$ reads:

$$h_\varepsilon(k) = \frac{1}{\sqrt{2\pi}\sigma}\int_{k\varepsilon-\frac{\varepsilon}{2}}^{k\varepsilon+\frac{\varepsilon}{2}}\exp\left(-\frac{x^2}{2\sigma^2}\right)dx \tag{10}$$

Note that $h_\varepsilon(k) = h_\varepsilon(-k)$. Thus the value of the discrete density function governing the statistical deflection from the state of equilibrium is equal to zero everywhere except points $k\varepsilon$; $k \in Z$.

As mentioned previously, it is necessary to compute the discrete Fourier transform of $p_\sigma(x)$ in order to construct the time-averaged image of the moiré grating deflected by such a discrete Gaussian law. Thus,

$$\widetilde{P}_\sigma(\omega) = \sum_{k=-\infty}^{+\infty} h_\varepsilon(k)\exp(-i\omega k\varepsilon) = \sum_{k=-\infty}^{+\infty} h_\varepsilon(k)(\cos(\omega k\varepsilon) + i\sin(\omega k\varepsilon)) = h_\varepsilon(0) + 2\sum_{k=1}^{+\infty} h_\varepsilon(k)\cos(\omega k\varepsilon) \tag{11}$$

where $\widetilde{P}_\sigma(\omega)$ denotes the discrete analogue of $P_\sigma(\omega)$ (Eq. (7)).

Please cite this article in press as: Petrauskiene V et al. Dynamic visual cryptography based on chaotic oscillations. Commun Nonlinear Sci Numer Simulat (2013), http://dx.doi.org/10.1016/j.cnsns.2013.06.002

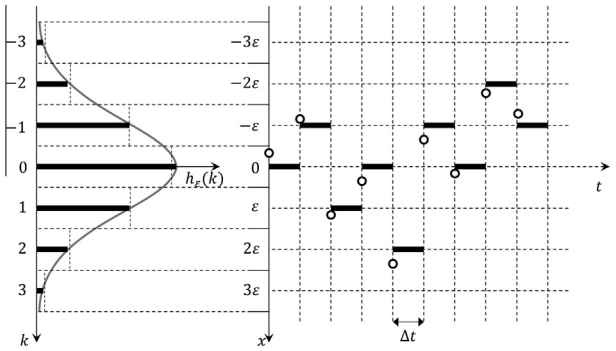

Fig. 1. The schematic diagram of the computational realization of discrete chaotic oscillations: t denotes time; x denotes the longitudinal coordinate of the one-dimensional moiré grating; empty circles show the distribution of $\theta(t_j)$ (a new Gaussian random number is generated at the beginning of every discrete time interval Δt); ε denotes the height of the pixel; thick solid intervals in the right part of the figure illustrate the deflection of the moiré grating from the state of equilibrium; columns $h_\varepsilon(k)$ illustrate discrete probabilities of the deflection from the state of equilibrium.

3.2. Considerations about the size of the pixel

First of all we will investigate the relationship in Eq. (11) when the size of the pixel tends to zero ($\varepsilon \to 0$) and the standard deviation σ is fixed.

According to the mean value theorem for the definite integral:

$$h_\varepsilon(k) = \frac{1}{\sqrt{2\pi}\sigma}\int_{k\varepsilon-\frac{\varepsilon}{2}}^{k\varepsilon+\frac{\varepsilon}{2}} \exp\left(-\frac{x^2}{2\sigma^2}\right)dx = \frac{\varepsilon}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(k\varepsilon)^2}{2\sigma^2}\right) + o(\varepsilon) \tag{12}$$

where $\lim_{\varepsilon\to 0}\frac{o(\varepsilon)}{\varepsilon} = 0$. Therefore,

$$\widetilde{P}_\sigma(\omega) = \frac{\varepsilon}{\sqrt{2\pi}\sigma}\sum_{k=-\infty}^{+\infty}\exp\left(-\frac{(k\varepsilon)^2}{2\sigma^2} - i\omega k\varepsilon\right) + \sum_{k=-\infty}^{+\infty} o(\varepsilon)\exp(-i\omega k\varepsilon) \tag{13}$$

But,

$$\lim_{\varepsilon\to 0}\sum_{k=-\infty}^{+\infty}\exp(-i\omega k\varepsilon)\varepsilon\cdot\frac{o(\varepsilon)}{\varepsilon} = \lim_{A\to+\infty}\int_{-A}^{A}\exp(-i\omega x)dx\cdot\lim_{\varepsilon\to 0}\frac{o(\varepsilon)}{\varepsilon} = 0 \tag{14}$$

because $|\exp(-i\omega k\varepsilon)| = 1$ and $\left|\int_{-A}^{A}\exp(-i\omega x)dx\right| < +\infty$ (note that $\left|\int_{-A}^{A}\exp(-i\omega x)dx\right| \leqslant \sqrt{\left(\int_{-A}^{A}\cos(\omega x)dx\right)^2 + \left(\int_{-A}^{A}\sin(\omega x)dx\right)^2} < M < +\infty$ for all A).

Therefore,

$$\lim_{\varepsilon\to 0}\widetilde{P}_\sigma(\omega) = \frac{\varepsilon}{\sqrt{2\pi}\sigma}\sum_{k=-\infty}^{+\infty}\exp\left(-\frac{(k\varepsilon)^2}{2\sigma^2} - i\omega k\varepsilon\right) = \frac{1}{\sqrt{2\pi}\sigma}\int_{-\infty}^{+\infty}\exp\left(-\frac{x^2}{2\sigma^2} - i\omega x\right)dx = \exp\left(-\frac{\omega^2\sigma^2}{2}\right) \tag{15}$$

This is an important result stating that $\widetilde{P}_\sigma(\omega)$ converges to $P_\sigma(\omega)$ as the size of the pixel tends to zero. Nevertheless, it is important to take into account the value of ε when chaotic oscillations are simulated on a particular computer display.

Alternatively, it is possible to check the opposite limit when $\varepsilon \to +\infty$ (at fixed σ).

It is clear that $\lim_{\varepsilon\to+\infty} h_\varepsilon(0) = 1$ and $\lim_{\varepsilon\to+\infty} h_\varepsilon(k) = 0$ for $k = \pm1, \pm2, \ldots$ Thus,

$$\lim_{\varepsilon\to+\infty}\widetilde{P}_\sigma(\omega) = \lim_{\varepsilon\to+\infty}\sum_{k=-\infty}^{+\infty} h_\varepsilon(k)\exp(-i\omega k\varepsilon) = 1 \tag{16}$$

All generated discrete random numbers $\theta(t_j)$ will fall into the central pixel of the stationary moiré grating if the size of the pixel is large compared to the standard deviation σ. Then the moiré grating will remain stationary at the state of equilibrium and the time-averaged image will be the image of the stationary grating (the characteristic function modulating time-averaged fringes is equal to one then).

3.3. Considerations about the standard deviation σ

We will consider the situation when $\sigma \to 0$ (at fixed ε). Now, $\lim_{\sigma\to 0} p_\sigma(x) = \delta_0$ where $\delta_0(x) = \begin{cases} +\infty, & x = 0 \\ 0, & x \neq 0 \end{cases}$ and $\int_{-\infty}^{\infty}\delta_0(x)dx = 1$. Thus,

$$\lim_{\sigma\to 0}\widetilde{P}_\sigma(\omega)=\int_{-\infty}^{\infty}\delta_0(x)\exp(-i\omega x)dx=\exp(-i\omega 0)=1 \tag{17}$$

The moiré grating will not be displaced from the state of equilibrium if the standard deviation σ is so small that all random numbers fall into the vicinity of the central pixel of the stationary grating.

Finally, we will consider the situation when $\sigma\to+\infty$ (at fixed ε). Now,

$$\lim_{\sigma\to+\infty}h_\varepsilon(k)=\lim_{\sigma\to+\infty}\frac{1}{\sqrt{2\pi}\sigma}\int_{k\varepsilon-\frac{\varepsilon}{2}}^{k\varepsilon+\frac{\varepsilon}{2}}\exp\left(-\frac{x^2}{2\sigma^2}\right)dx=0 \tag{18}$$

Therefore, $\lim_{\sigma\to+\infty}\widetilde{P}_\sigma(\omega)=0$. Instantaneous displacements of the moiré grating from the state of equilibrium will be very large then. Thus the moiré grating will be evenly blurred along the whole axis of the displacements and the time-averaged image will become gray ($\lim_{\sigma\to+\infty}H_\sigma(x|F;\xi_\sigma)=0.5$).

3.4. Simulation of chaotic oscillations on a realistic computer screen

It is important to test if a realistic computational setup is applicable for the simulation of chaotic oscillations on the computer display. We use HP ZR24w digital display; the physical height of the pixel is 0.27 mm (the one-dimensional moiré grating is placed in the vertical direction). We use 20 pixels to represent one pitch of the moiré grating (10 pixels are black and 10 pixels are white). Thus, the pitch of the one-dimensional moiré grating is 5.4 mm in the vertical direction. The theoretical envelope function which modulates the first harmonic of the moiré grating $F(x)$ is described by Eq. (7). We will use Eq. (13) to simulate the shape of the envelope function $\widetilde{P}_\sigma(\omega)$ (note that ω is replaced by $\frac{2\pi}{\lambda}$ for the first harmonic of the moiré grating):

$$\widetilde{P}_\sigma\left(\frac{2\pi}{\lambda}\right)=h_\varepsilon(0)+2\sum_{k=1}^{+\infty}h_\varepsilon(k)\cos\left(\frac{2\pi}{\lambda}k\varepsilon\right) \tag{19}$$

The shape of the envelope function $\widetilde{P}_\sigma(\omega)$ is numerically reconstructed for $\varepsilon=0.27$, 1.5, 2.8, 4.1 and 5.4 (Fig. 2). Note that all computations are performed at $\lambda=5.4=20\varepsilon$. A naked eye cannot see any differences between the envelope function $\widetilde{P}_\sigma(\omega)$ and the theoretical envelope function at $\varepsilon=0.27$ (Fig. 2). For example, the difference $|P_\sigma(\omega)-\widetilde{P}_\sigma(\omega)|=0.00191$ at $\varepsilon=0.27$ and $\sigma=1$. Thus, we may conclude that $\varepsilon=0.27$ is sufficiently small for the simulation of chaotic oscillations if only the pitch λ is not smaller than 20ε.

4. Dynamic visual cryptography based on chaotic oscillations

The concept of dynamic visual cryptography introduced in [15] and is based on the formation of time averaged moiré fringes in zones occupied by the secret image when the cover image is oscillated in a predefined law of motion. This concept cannot be exploited for dynamic visual cryptography based on chaotic oscillations due to the reason that time-averaged fringes do not form when the cover image is oscillated chaotically (Eq. (8)) – the image is continuously blurred as the standard deviation σ increases.

Therefore we need to employ other techniques which would enable visual decryption of the secret from the cover image. We will keep the encryption method used in [16] where one-dimensional moiré gratings with the pitch $\lambda_0=20\varepsilon=5.4$ mm is used in the regions occupied by the background and the pitch $\lambda_1=22\varepsilon=5.94$ mm is used in the regions occupied by the secret image. In other words, we predetermine the direction of deflections of the cover image from the state of equilibrium – all deflections must be uni-directional and that direction must coincide with the longitudinal axis of the one-dimensional moiré grating. Stochastic initial phase deflection and boundary phase regularization algorithms [15] are used to encode the secret image into the cover image.

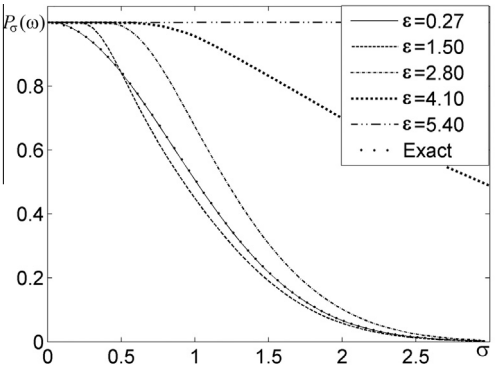

Fig. 2. Numerically reconstructed envelope functions $\widetilde{P}_\sigma(\omega)$ for different pixel sizes: $\varepsilon=0.27$, 1.5, 2.8, 4.1, 5.4.

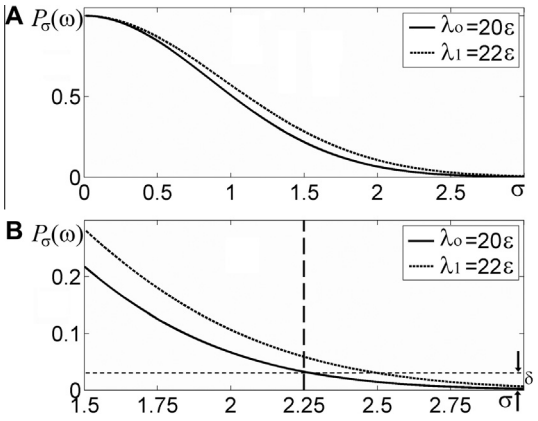

Fig. 3. Image hiding based on chaotic oscillations: envelope functions are illustrated in part A at $\lambda_0 = 20\varepsilon$ and at $\lambda_1 = 22\varepsilon$. The zoomed image in part B illustrates the optimal standard deviation σ (marked by the vertical dashed line) when the secret is interpreted as an almost developed time-averaged moiré fringe, while the background is still interpreted as a stochastic moiré grating (δ = 0.03 guarantees the satisfactory interpretation of a time-averaged moiré fringe).

Fig. 4. The secret image.

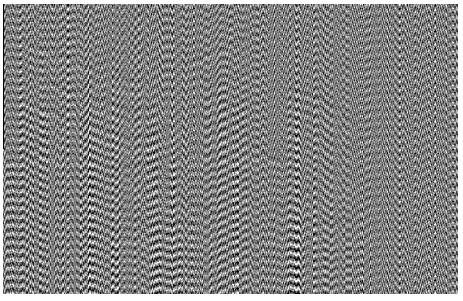

Fig. 5. The secret image encoded into cover moiré image.

4.1. Visual decryption of the secret image

As mentioned previously, chaotic oscillations do not generate time-averaged moiré fringes; the image becomes blurred at increasing standard deviation. But the slope of the envelope function governing the process of chaotic blurring (Eq. (8)) depends on the pitch of the grating (Fig. 3(A)). Thus, it is possible to find such standard deviation σ that the value of $P_\sigma(\omega)$ becomes lower than δ for $\lambda_0 = 20\varepsilon$ but remains higher than δ for $\lambda_1 = 22\varepsilon$ (Fig. 3(B)). The value of δ describes such situation when a naked eye interprets the time-averaged moiré image as an almost fully developed time-averaged fringe [18]. Strictly speaking, the particular value of δ should be preselected individually and may depend on many different factors as the experimental set-up and the quality of the static moiré grating. We select δ = 0.03 which can be considered as a safe margin for the satisfactory interpretation of a time-averaged moiré fringe [18]. The vertical dashed line in Fig. 3(B) denotes the optimal standard deviation σ which should result into the best visual decryption of the secret image when the cover image is oscillated chaotically – the secret image should be interpretable as a time-averaged fringe, while the background should still be visible as an undeveloped fringe.

Please cite this article in press as: Petrauskiene V et al. Dynamic visual cryptography based on chaotic oscillations. Commun Nonlinear Sci Numer Simulat (2013), http://dx.doi.org/10.1016/j.cnsns.2013.06.002

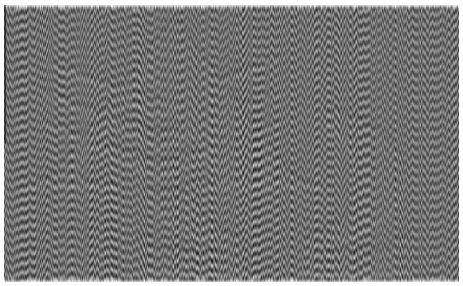

Fig. 6. The time-averaged cover image at $\sigma = 1.2$ does not leak the secret.

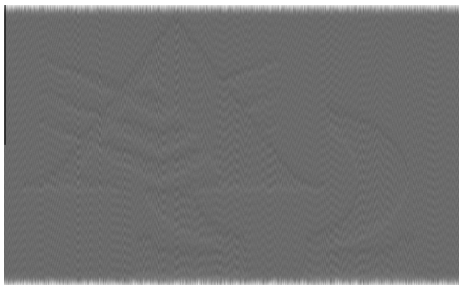

Fig. 7. The time-averaged cover image at $\sigma = 2.25$ leaks the secret; the exposure time is $T = 1$ s; $\Delta t = \frac{1}{60}$ s.

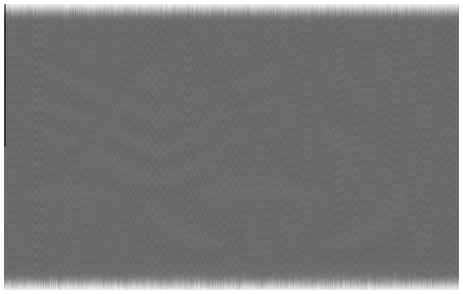

Fig. 8. It is hard to interpret the secret from the time-averaged cover image at $\sigma = 3.1$.

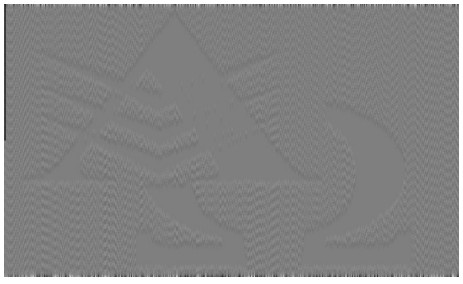

Fig. 9. The time-averaged cover image leaks the secret as the exposure time tends to infinity; $\sigma = 2.25$.

4.2. Computational experiments

First of all we select the secret image to be encoded into the background moiré grating (Fig. 4). We employ the encoding algorithms described in [15,16]; the encoded cover image is shown in Fig. 5. Next, we generate discrete random numbers $\theta(t_j) \sim N(0, \sigma^2)$ and plot time-averaged images at $\sigma = 1.2$ (Fig. 6; the standard deviation is too small to ensure visual decryp-

Please cite this article in press as: Petrauskiene V et al. Dynamic visual cryptography based on chaotic oscillations. Commun Nonlinear Sci Numer Simulat (2013), http://dx.doi.org/10.1016/j.cnsns.2013.06.002

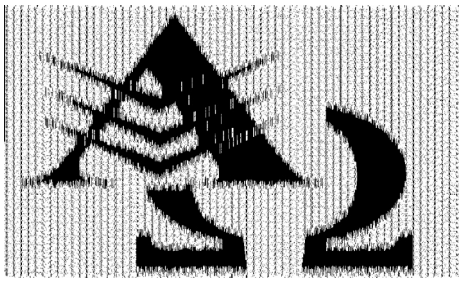

Fig. 10. Contrast enhancement helps to highlight the secret image.

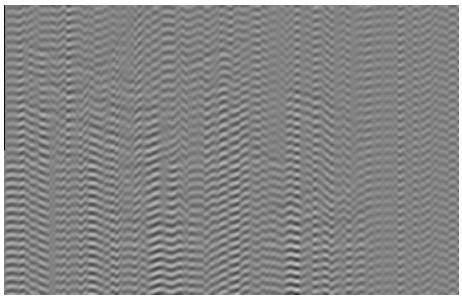

Fig. 11. Isotropic Gaussian blur cannot be used to reveal the secret because the geometric structure of moiré grating lines is damaged in the process.

tion of the secret image); at $\sigma = 2.25$ (Fig. 7; the standard deviation is optimal for visual decryption of the secret image) and at $\sigma = 3.1$ (Fig. 8; the standard deviation is too high to ensure visual decryption of the secret image).

Note that the time averaged image in Fig. 7 does not reveal the secret image in the form of a time-averaged moiré fringe. This optical effect can be explained by the fact that the exposure time was limited to 1 s (the length of the discreet set of random numbers used to construct the time-averaged image is 60). The secret image becomes well-interpretable in the stochastic moiré background as the exposure time tends to infinity (the length of the discrete set of random numbers is 6000 in Fig. 9); the secret image can be highlighted using digital enhancement techniques for the visualization of time-averaged moiré fringes [26] (Fig. 10).

Finally it can be mentioned that simple computational blur (a standard image editing function in such packages as Photoshop) cannot be used to reveal the secret from the cover image. We select $3\sigma = 6.75$ isotropic Gaussian blur (Fig. 11) – but the blurred image does not reveal the secret because the geometric structure of moiré grating lines is damaged in the process.

5. Concluding remarks

The proposed dynamic visual cryptography scheme based on chaotic oscillations can be considered as a safer image hiding scheme if compared to analogous digital image hiding techniques where the secret image can be visually decrypted as the cover image is oscillated by a harmonic, a rectangular or a piece-wise continuous waveform. The proposed image hiding algorithm does not leak the secret if the cover image is oscillated at any direction and at any amplitude of the harmonic waveform, for example. This technique requires sophisticated encoding algorithms to hiding the secret image, but the decryption is completely visual and does not require a computer.

The potential applicability of the proposed technique is not limited by different digital image hiding and communication scenarios. Interesting possibilities exist for visual control of chaotic vibrations. Dynamic visual cryptography is successfully exploited for visual control of harmonically oscillating structures and surfaces. But it is well known that complex nonlinear systems exhibit chaotic vibrations even at harmonic loads. Moreover, complex loads in aerospace applications rarely result in harmonic structural vibrations. Therefore, the ability of direct visual interpretation of chaotic vibrations would be an attractive alternative for other control methods. One could print the encrypted cover image and glue it in the surface which vibrations should be controlled. No secret image could be interpreted when the surface is motionless. The digital image encoding scheme can be preselected in such a way that the secret image (for example two letters "OK") would appear when the parameters of chaotic vibrations would fit into a predetermined interval of acceptable values. Such experimental implementation of the dynamic visual cryptography based on chaotic oscillations remains an actual topic of future research.

Acknowledgment

Financial support from the Lithuanian Science Council under project No. MIP-100/12 is acknowledged.

Please cite this article in press as: Petrauskiene V et al. Dynamic visual cryptography based on chaotic oscillations. Commun Nonlinear Sci Numer Simulat (2013), http://dx.doi.org/10.1016/j.cnsns.2013.06.002

References

[1] Naor M, Shamir A. Visual cryptography. Lect Notes Comput Sci 1994;950:1–12.
[2] Blundo C, De Santis A, Naor M. Visual cryptography for grey level images. Inform Process Lett 2000;75:255–9.
[3] Ateniese G, Blundo C, De Santis A, Stinson D. Extended capabilities for visual cryptography. Theor Comput Sci 2001;250:143–61.
[4] Hou YC. Visual cryptography for color images. Pattern Recognit 2003;36:1619–29.
[5] Shyu SJ, Huang SY, Lee YK, Wang RZ, Chen K. Sharing multiple secrets in visual cryptography. Pattern Recognit 2007;40:3633–51.
[6] Yang CN, Chung TH. A general multi-secret visual cryptography scheme. Opt Commun 2010;283:4949–62.
[7] Feng JB, Wu HC, Tsai CS, Chang YF, Chu YP. Visual secret sharing for multiple secrets. Pattern Recognit 2008;41:3572–81.
[8] Shyu SJ, Chen K. Visual multiple secret sharing based upon turning and flipping. Inform Sci 2011;181:3246–66.
[9] Wang RZ, Lan YC, Lee YK, Huang SY, Shyu SJ, Chia TL. Incrementing visual cryptography using random grids. Opt Commun 2010;283:4242–9.
[10] Cimato S, De Santis A, Ferrara AL, Masucci B. Ideal contrast visual cryptography schemes with reversing. Inform Process Lett 2005;93:199–206.
[11] Fang WP. Friendly progressive visual secret sharing. Pattern Recognit 2008;41:1410–4.
[12] Yang CN, Ciou CB. Image secret sharing method with two-decoding-options: lossless recovery and previewing capability. Image Vision Comput 2010;28:1600–10.
[13] Tsaia DS, Horngb G, Chenc TH, Huangb YT. A novel secret image sharing scheme for true-color images with size constraint. Inform Sci 2009;179:3247–54.
[14] Shyu SJ. Image encryption by random grids. Pattern Recognit 2007;40:1014–31.
[15] Ragulskis M, Aleksa A. Image hiding based on time-averaging moiré. Opt Commun 2009;282:2752–9.
[16] Ragulskis M, Aleksa A, Navickas Z. Image hiding based on time-averaged fringes produced by non-harmonic oscillations. J Opt A-Pure Appl Opt 2009;11:125411.
[17] Sakyte E, Palivonaite R, Aleksa A, Ragulskis M. Image hiding based on near-optimal moiré gratings. Opt Commun 2011;284:3954–64.
[18] Petrauskiene V, Aleksa A, Fedaravicius A, Ragulskis M. Dynamic visual cryptography for optical control of vibration generation equipment. Opt Laser Eng 2012;50:869–76.
[19] Ragulskis M, Navickas Z. Hash function construction based on time average moiré. Discrete Contin Dyn-B 2007;8:1007–20.
[20] Fujii H, Asakura T. Effect of the point spread function on the average contrast of image speckle patterns. Opt Commun 1977;21:80–4.
[21] Braat JJM, van Haver S, Janssen AJEM, Dirksen P. In: Wolf Emil, editor. Assessment of optical systems by means of point-spread functions. New York: Elsevier; 2008. p. 349–468.
[22] Peng Z, Guo-Qiang N, Ting-Fa X. Image restoration for interlaced scan CCD image with space-variant motion blurs. Opt Laser Technol 2010;42:894–901.
[23] Meyer T, Meyer C. Creating motion graphics with after effects. 4th ed. Elsevier; 2008. pp. 126–33.
[24] Vairy M, Venkatesh YV. Deblurring Gaussian blur using a wavelet array transform. Pattern Recognit 1995;28:965–76.
[25] http://en.wikipedia.org/wiki/68-95-99.7_rule (last access 2012-09-10).
[26] Ragulskis M, Sanjuan M, Saunoriene L. Applicability of time-average moiré techniques for chaotic oscillations. Phys Rev E 2007;76:036208.

Please cite this article in press as: Petrauskiene V et al. Dynamic visual cryptography based on chaotic oscillations. Commun Nonlinear Sci Numer Simulat (2013), http://dx.doi.org/10.1016/j.cnsns.2013.06.002