Commun Nonlinear Sci Numer Simulat 19 (2014) 112–120

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 11 June 2013

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

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

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].