Near-optimal pitch of a moiré grating for image hiding applications in dynamic visual cryptography

Loreta Saunoriene[1], Sandra Aleksiene[2], Jurate Ragulskiene[3]
Research Group for Mathematical and Numerical Analysis of Dynamical Systems,
Kaunas University of Technology, Kaunas, Lithuania
[1]Corresponding author
E-mail: [1]*loreta.saunoriene@ktu.lt*, [2]*sandra.aleksiene@ktu.lt*, [3]*jurate.ragulskiene@ktu.lt*

Received 30 August 2017; accepted 31 August 2017
DOI https://doi.org/10.21595/vp.2017.19031

Check for updates

Abstract. Dynamic visual cryptography is based on hiding of a dichotomous secret image in the regular moiré grating. One pitch of the moiré grating is used to represent the secret image and a slightly different pitch of another moiré grating is used to form the background. The secret is decoded in the form of a pattern of a time-averaged moiré fringe when the cover image is oscillated according to a predefined law of motion. The security of the encoding and the sharpness of the decoded secret are mostly influenced by the selection of the pitches of moiré grating. This paper proposes scheme for the determination of near-optimal pitches of the moiré grating for image hiding in dynamic visual cryptography.

Keywords: dynamic visual cryptography, harmonic oscillation, moiré grating.

1. Introduction

Visual cryptography (VC) is a special encryption technique used to hide visual information in a way that it can be decrypted purely by the human visual system and no computational techniques are required. First introduced by Moni Naor and Adi Shamir [1] in 1994, VC is based on the division of the original image into several semi-transparent shares. Each share individually does not reveal the secret, but if all these shares are overlaid at the right position, a secret message appears [2]. Recently many advances have been done in visual cryptography: visual cryptography of gray-level and color images was introduced in [3]; probabilistic visual secret sharing scheme for grey-scale and color images was presented in [4]; letter-based VC scheme where pixels are replaced by letters in the share images was proposed in [5], sharing of multiple secrets in visual cryptography was discussed in [6]; security of visual cryptography schemes was analysed in [7-9].

Geometric moiré is a classical optical experimental technique based on analysis of visual patterns formed as a superposition of two regular gratings that geometrically interfere [10, 11]. Geometric moiré techniques can be extended to time-average geometric moiré methods. If moiré grating is formed on the surface of oscillating structure and time-averaging techniques are applied, pattern of time-averaged fringes emerges [12].

The concept of dynamic visual cryptography was first introduced in [13]. This method is based not on static superposition of shares like in VC, but on the time-averaging techniques applied for a single encoded image. The secret image is embedded into the moiré grating in such a way, that one pitch of the moiré grating is used to form the background of the secret image and a slightly different pitch of another moiré grating is used to represent the secret. Phase scrambling completely hides the secret and a naked eye cannot interpret the secret from the stationary cover image. The secret is decoded in a form of a pattern of time-averaged moiré fringe when the cover image is oscillated according to a predefined law of motion. Furthermore, the amplitude of the harmonic oscillations must be set to a preselected value in order to leak the secret. The security of the encoding and the sharpness of the decoded secret are mostly influenced by the selection of the pitches of moiré grating. Pitches of the grating representing the secret image and the background cannot differ very significantly – otherwise, encoded secret could be seen by a naked eye in a static share. At the same time, the difference between the pitches should ensure the sufficient contrast between secret and background areas in time-averaged image. This paper proposes

scheme for the determination of near-optimal pitch of the moiré grating for image hiding in dynamic visual cryptography.

2. Optical background

One-dimensional harmonic moiré grating reads [10, 11]:

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

where x is the longitudinal coordinate, λ is the pitch of the moiré grating. The numerical value 0 of function $F(x)$ corresponds to black color, 1 – to white color, all values between 0 and 1 correspond to the appropriate greyscale levels.

Let us suppose that the moiré grating (Eq. (1)) is formed on the surface of one-dimensional non-deformable body and is harmonically oscillated around the state of equilibrium according to harmonic function: $a \cdot \sin(\omega t + \varphi)$, where a is the amplitude of harmonic oscillations, ω is the frequency and φ is the phase. Then grey-scale level of moiré grating at coordinate x at time moment t can be expressed [12]:

$$F(x,t) = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x - a\sin(\omega t + \varphi))\right). \tag{2}$$

Greyscale level of time-averaged geometric moiré can be obtained averaging Eq. (2) in time [12]:

$$F_t(x) = \lim_{T\to\infty}\frac{1}{T}\int_0^T F(x,t)dt = \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)J_0\left(\frac{2\pi}{\lambda}a\right), \tag{3}$$

where T is the exposure time used for the time-averaging, J_0 is the zero order Bessel function of the first kind. Note, that oscillation frequency ω and phase φ have no influence on the formation of time-averaged image [11, 12]. Time-averaged image becomes continuously grey at the roots of $J_0\left(\frac{2\pi}{\lambda}a\right)$:

$$\frac{2\pi}{\lambda}a = r_i, \quad i = 1,2,..., \tag{4}$$

where r_i is the ith root of the zero order Bessel function of the first kind.

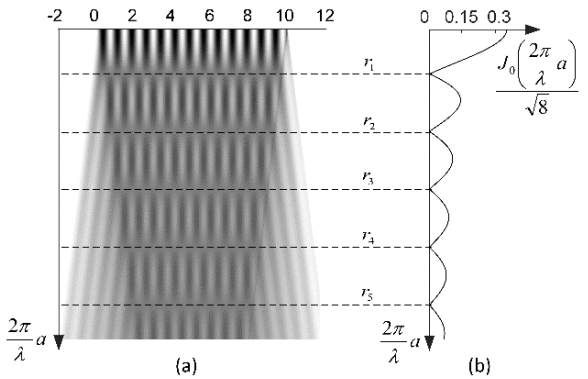

Fig. 1. Time-averaged moiré at $\lambda = 0.75$: a) one-dimensional time-averaged moiré in case of harmonic oscillations at increasing amplitudes a; b) standard deviation of time-averaged moiré

It can be noted, that standard deviation of time-averaged image, described by Eq. (3), is calculated as follows [14]:

$$S\left(F_t(x)\right) = \frac{\left|J_0\left(\frac{2\pi}{\lambda}a\right)\right|}{\sqrt{8}}. \tag{5}$$

Fig. 1(a) provides one-dimensional time-averaged moiré image at increasing amplitudes. It is clear that time-averaged fringes form at amplitudes corresponding to the Eq. (4). Fig. 1(b) shows the variation of the standard deviation of the time-averaged moiré at increasing amplitudes. Value of the standard deviation within the time-averaged image depends on a blur level in time-averaged moiré grating: sharp structure of the grating ensures sufficiently high standard deviation. Note that standard deviation is equal to zero at the centers of time-averaged fringes.

3. Estimation of near-optimal pitch of a moiré grating

The main idea of hiding a secret in the dynamic visual cryptography is to encode this secret image into moiré grating: one pitch of the moiré grating is used to form the background of the secret image and a slightly different pitch of another moiré grating is used to represent the secret. Let the pitch of the grating in the area of secret information be denoted λ_s, the pitch of the grating in the background – λ_b. Pitches of the grating λ_s and λ_b cannot differ very significantly $|\lambda_s - \lambda_b| \leq \varepsilon$, otherwise the encoded secret could be seen by a naked eye in a static share. Simultaneously, the difference between λ_s and λ_b should ensure the sufficient contrast between secret and background areas in time-averaged image.

The secret information is leaked if only the cover image is oscillated harmonically. Secret appears as a uniformly grey area in time-averaged image while background contains slightly blurred pattern of the cover image.

Let the standard deviations of the secret and background areas in time-averaged image be denoted as σ_s and σ_b respectively. Values of σ_s and σ_b are calculated as [14]:

$$\sigma_s = \frac{\left|J_0\left(\frac{2\pi}{\lambda_s}a\right)\right|}{\sqrt{8}}, \quad \sigma_b = \frac{\left|J_0\left(\frac{2\pi}{\lambda_b}a\right)\right|}{\sqrt{8}}. \tag{6}$$

Sufficient contrast between the leaked secret and the background in the time-averaged cover image is obtained if only $|\sigma_s - \sigma_b| \geq \delta$. The graphical representation of standard deviations σ_s and σ_b is proposed in Fig. 2.

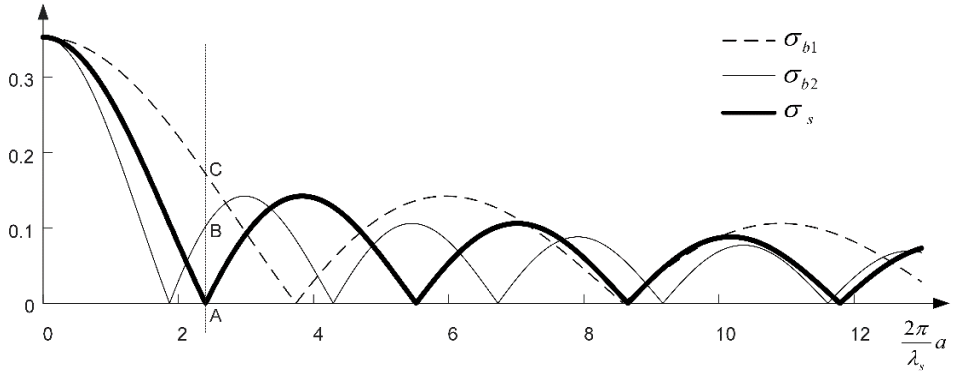

Fig. 2. Variation of standard deviations of time-averaged moiré. Thick solid line stands for standard deviation of the secret σ_s at $\lambda_s = 0.45$; thin solid and thin dashed lines represent standard deviations of the background σ_{b1} and σ_{b2} at $\lambda_{b1} = 0.7$, $\lambda_{b2} = 0.35$ accordingly

As it is mentioned in Eq. (4), the area of the secret information in time-averaged image becomes uniformly grey if only the amplitude of oscillations a is equal to $a = \frac{\lambda_s}{2\pi} r_i$, $i = 1,2, \ldots$. It is clear that standard deviation of uniformly grey area is equal to 0, thus $\sigma_s = 0$ if only the amplitude of oscillations is equal to $\frac{\lambda_s}{2\pi} r_1$. Therefore, the contrast between the secret and the background depends on the value of σ_b only (note that distance AC in Fig. 2 is equal to $|\sigma_{b1} - \sigma_s| = \sigma_{b1}$ and distance AB is equal to $|\sigma_{b2} - \sigma_s| = \sigma_{b2}$ at the point where $\frac{2\pi}{\lambda_s} a = r_1$).

Let us assume that the contrast of the leaked secret in time-averaged cover image is sufficient, if standard deviation σ_b is equal or exceeds threshold δ :

$$\frac{\left|J_0\left(\frac{2\pi}{\lambda_b} a\right)\right|}{\sqrt{8}} \geq \delta, \tag{7}$$

whereas amplitude of oscillation is preset to $a = \frac{\lambda}{2\pi} r_1$, Eq. (7) yields:

$$\frac{\left|J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right)\right|}{\sqrt{8}} \geq \delta. \tag{8}$$

The inequality Eq. (8) is visualized in Fig. 3 when λ_s is fixed. Striped intervals on the graph show the intervals of λ_b for which the inequality $\left|J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right)\right| / \sqrt{8} \geq \delta$ holds true. Zeroes of the function $J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right)$ are located at $\lambda_b = \lambda_s \frac{r_1}{r_i}$, $i = 1,2, \ldots$.

Function $J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right)$ can be approximated by its tangent in the root surrounding if the threshold δ is relatively small. It is known, that $J_0'(x) = -J_1(x)$, where $J_1(x)$ is first order Bessel function of the first kind. Therefore, the slope of tangent line at point $\lambda_b = \lambda_s$ is $k_1 = J_0{}'(r_1) = \frac{r_1}{\lambda_s} J_1(r_1)$.

Analogously the slope at point $\lambda_b = \lambda_s \frac{r_1}{r_2}$ reads $k_2 = J_0{}'(r_2) = \frac{r_2^2}{r_1 \lambda_s} J_1(r_2)$. Now Δ_i, $i = 1,2, \ldots$ (Fig. 3) can be approximated as $\Delta_i = \frac{\delta}{k_i}$.

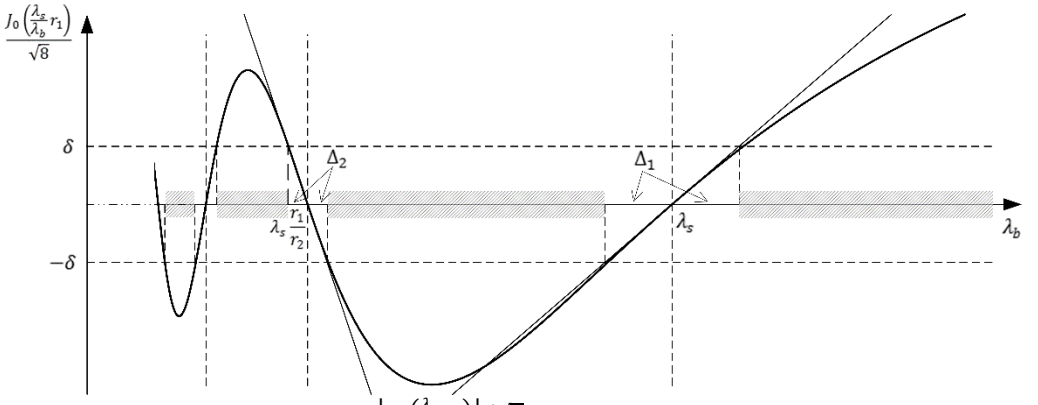

Fig. 3. Visualization of the inequality $\left|J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right)\right| / \sqrt{8} \geq \delta$ in the interval $(0.2\lambda_s; 1.5\lambda_s)$. Thick solid line represents the variation of $\left|J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right)\right| / \sqrt{8}$; tangents at points λ_s and $\lambda_s \frac{r_1}{r_2}$ are displayed by thin lines

Finally, the approximate solution of inequality in Eq. (8) if δ is relatively small can be written

as:

$$\begin{cases} \lambda_b \geq \lambda_s \left(1 + \dfrac{\delta}{r_1 J_1(r_1)}\right), \\ \lambda_s \left(1 - \dfrac{\delta}{r_1 J_1(r_1)}\right) \geq \lambda_b \geq \lambda_s \dfrac{r_1}{r_2}\left(1 + \dfrac{\delta}{r_2 J_1(r_2)}\right). \end{cases} \quad (9)$$

Computational solutions of inequality in Eq. (8) are presented in Fig. 4: all λ_b located in the uniformly grey and striped grey areas fit the inequality at the predefined values of δ. Black lines show the boundaries of the approximate solution in Eq. (9).

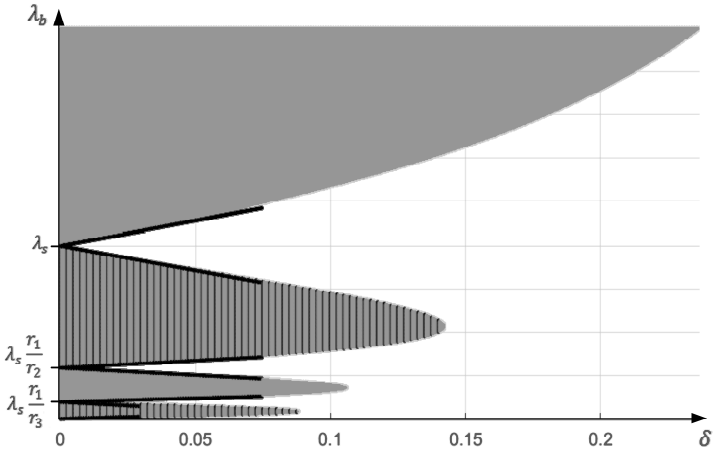

Fig. 4. Solutions of the inequality $\left|J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right)\right| / \sqrt{8} \geq \delta$: grey color indicates areas where $J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right) / \sqrt{8} \geq \delta$, striped grey areas – where $J_0\left(\frac{\lambda_s}{\lambda_b} r_1\right) / \sqrt{8} \leq -\delta$, black lines corresponds to the boundaries of the approximate solution in Eq. (9)

If we want to obtain sufficient predetermined contrast between secret and background areas ($\sigma_b = \delta$), it would be optimal to choose such values λ_b that lye on the contours of the grey and striped grey areas in Fig. 3, or, if δ is small, the approximate optimal solution is:

$$\lambda_b = \lambda_s \left(1 + \frac{\delta}{r_1 J_1(r_1)}\right) \quad \text{or} \quad \lambda_b = \lambda_s \left(1 - \frac{\delta}{r_1 J_1(r_1)}\right). \quad (10)$$

Note, that the difference between values λ_s and λ_b still should be small enough in order to ensure the safety of the visual encoding scheme.

4. Conclusions

The secure encryption and successful decryption of the secret information in dynamic visual cryptography is generally based on the correct determination of the moiré grating parameters. This paper proposes the graphical scheme as well as the approximate solutions for the preselection of the near optimal pitches of moiré grating. The pitch standing for the secret information should ensure uniformly grey secret area in the time-averaged image (standard deviation of the area is equal to zero). The pitch of the background should guarantee high enough standard deviation in the time-averaged background. Such near-optimal pair of the pitches of moiré grating provides sufficient contrast of the decoded image and ensures that no secret information is visible in the

static cover image.

References

[1] **Naor M., Shamir A.** Visual cryptography. Eurocrypt'94 Proceedings LNCS, Vol. 950, 1995, p. 1-12.
[2] **Verheul E. R., Van Tilborg H. C. A.** Constructions and properties of k out of n visual secret sharing schemes. Design Codes and Cryptography, Vol. 11, Issue 2, 1997, p. 179-196.
[3] **Hou Young Chang** Visual cryptography for color images. Pattern Recognition, Vol. 36, Issue 7, 2003, p. 1619-1629.
[4] **Wang Daoshun, Yi Feng, Li Xiaobo** Probabilistic visual secret sharing schemes for grey-scale images and color images. Information Sciences, Vol. 181, Issue 11, 2011, p. 2189-2208.
[5] **Lin Hsiao Ching, Yang Ching Nung, Laih Chi Sung, Lin Hui Tang** Natural language letter based visual cryptography scheme. Journal of Visual Communication and Image Representation, Vol. 24, Issue 3, 2013, p. 318-331.
[6] **Shyu Shyong Jian, Huang Shih Yu, Lee Yeuan Kuen, Wang Ran Zan, Sharing Kun Chen** multiple secrets in visual cryptography. Pattern Recognition, Vol. 40, Issue 12, 2007, p. 3633-3651.
[7] **Horng Gwoboa, Chen Tzungher, Tsai Du Shiau** Cheating in visual cryptography. Designs, Codes and Cryptography, Vol. 38, Issue 2, 2006, p. 219-236.
[8] **Lin Pei Yu, Wang Ran Zan, Chang Yu Jie, Fang Wen Pinn** Prevention of cheating in visual cryptography by using coherent patterns. Information Sciences, Vol. 301, 2015, p. 61-74.
[9] **Bert Leung W., Felix Ng Y., Duncan Wong S.** On the security of a visual cryptography scheme for color images. Pattern Recognition, Vol. 42, Issue 5, 2009, p. 929-940.
[10] **Kobayashi A. S.** Handbook on Experimental Mechanics. Second Edition, SEM, Bethel, 1993.
[11] **Patorski K., Kujawinska M.** Handbook on the Moiré Fringe Technique. Elsevier, Amsterdam, 1993.
[12] **Ragulskis M., Ragulskis L., Maskeliunas R.** Applicability of time-average geometric moiré for vibrating elastic structures. Experimental Techniques, Vol. 28, 2004, p. 27-30.
[13] **Ragulskis M., Aleksa A.** Image hiding based on time-averaging moiré. Optics Communications, Vol. 282, Issue 14, 2009, p. 2752-2759.
[14] **Ragulskis M., Saunoriene L., Maskeliunas R.** The structure of moiré grating lines and influence to time-averaged fringes. Experimental Techniques, Vol. 33, Issue 2, 2009, p. 60-64.