Near-Optimal Time Function for Secure Dynamic Visual Cryptography

V. Petrauskiene[1], J. Ragulskiene[2], E. Sakyte[1], and M. Ragulskis[1]

[1] Research Group for Mathematical and Numerical Analysis of Dynamical Systems, Kaunas University of Technology, Studentu 50-222, Kaunas LT-51368, Lithuania
[2] Kauno Kolegija, Pramones 20, Kaunas LT-50468, Lithuania

Abstract. The strategy for the selection of an optimal time function for dynamic visual cryptography is presented in this paper. Evolutionary algorithms are used to obtain the symmetric piece-wise uniform density function. The fitness function of each chromosome is associated with the derivative of the standard of the time-averaged moiré image. The reconstructed near-optimal time function represents the smallest interval of amplitudes where an interpretable moiré pattern is generated in the time-averaged image. Such time functions can be effectively exploited in computational implementation of secure dynamic visual cryptography.

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. An efficient visual secret sharing scheme for color images is proposed in [2]. Halftone visual cryptography based on the blue noise dithering principles is proposed in [3]. Basis-matrices-free image encryption by random grids is developed in [4]. A generic method that converts a visual cryptography scheme into another visual cryptography scheme that has a property of cheating prevention is implemented in [5]. Colored visual cryptography without color darkening is developed in [6]. Extended visual secret sharing schemes have been used to improve the quality of the shadow image in [7].

Geometric moiré [8,9] is a classical in-plane whole-field non-destructive optical experimental technique based on the analysis of visual patterns produced by superposition of two regular gratings that geometrically interfere. Examples of gratings are equispaced parallel lines, concentric circles or arrays of dots. The

G. Bebis et al. (Eds.): ISVC 2011, Part II, LNCS 6939, pp. 300–309, 2011.

gratings can be superposed by double exposure photography, by reflection, by shadowing, or by direct contact [10,11]. Moiré patterns are used to measure variables such as displacements, rotations, curvature and strains throughout the viewed area. Two basic goals exist in moiré pattern research. The first is the analysis of moiré patterns. Most of the research in moiré pattern analysis deals with the interpretation of experimentally produced patterns of fringes and determination of displacements (or strains) at centerlines of appropriate moiré fringes [8]. Another goal is moiré pattern synthesis when the generation of a certain predefined moiré pattern is required. The synthesis process involves production of two such images that the required moiré pattern emerges when those images are superimposed [12]. Moiré synthesis and analysis are tightly linked and understanding one task gives insight into the other.

The image hiding method based on time-averaging moiré is proposed in [13]. This method is based not on static superposition of moiré images, but on time-averaging geometric moiré. This method generates 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 a strictly defined amplitude of oscillation. Only one picture is generated, and the secret is leaked from this picture when parameters of the oscillation are appropriately tuned. In other words, the secret can be decoded by trial and error-if only one knows that he has to shake the slide. Therefore, additional image security measures are implemented in [13], particularly splitting of the encoded image into two shares.

The image encoding method which reveals the secret image not only at exactly tuned parameters of the oscillation, but also requires that the time function determining the process of oscillation must comply with specific requirements is developed in Ref. [14]. This image hiding method based on time-averaging moiré and non-harmonic oscillations does not reveal the secret image at any amplitude of harmonic oscillations. Instead, the secret is leaked only at carefully chosen parameters of this specific time function (when the density function of the time function is a symmetric uniform density function).

The main objective of this manuscript is to propose such a time function (used to decrypt the secret image) which would ensure the optimal security of the encoded image. The security of the encoded image is measured in terms of the local variation of grayscale levels in the surrounding of a time-averaged fringe which is exploited to reveal the secret.

This paper is organized as follows. Initial definitions are presented in section 2; the optimization problem is discussed in section 3; computational experiments and concluding remarks are given in section 4.

2 Initial Definitions

A one-dimensional moiré grating is considered in this paper. We will use a stepped grayscale function defined as follows [14]:

$$F(x) = \begin{cases} 1, \text{ when } x \in \left[\lambda j; \lambda\left(j+\frac{1}{2}\right)\right] \\ 0, \text{ when } x \in \left[\lambda\left(j+\frac{1}{2}\right); \lambda(j+1)\right] \end{cases}, \quad j = 0, \pm 1, \pm 2, \ldots \tag{1}$$

and λ is the pitch of moiré grating.

Definition 1. Time averaging operator H_s reads [15]:

$$H_s(F; \zeta_s) = \lim_{T\to\infty} \frac{1}{T} \int_0^T F(x - \xi_s(t))\, dt; \tag{2}$$

where t is time, T is exposure time, $\xi_s(t)$ is a function describing dynamic deflection from state of equilibrium, $s \geq 0$ is a real parameter; $x \in \mathbf{R}$.

Definition 2. The standard of a time-averaged grayscale grating function reads [14]:

$$\sigma(s) = \sigma(H_s(F(x), \xi_s)) = \sqrt{\frac{1}{\lambda}} \int_0^\lambda (H_s(F(x), \xi_s) - E(H_s(F(x), \xi_s)))^2 \tag{3}$$

We will consider a piece-linear function $\xi_s(t)$ as a realization of ξ_s; its which density function $p_s(x)$ satisfies following requirements:

(i) $p_s(x) = 0$ when $|x| > s$; $s > 0$;
(ii) $p_s(x) = p_s(-x)$ for all $x \in \mathbf{R}$.

We will assume that the density function $p_s(x)$ comprises $2n$ equispaced columns symmetrically distributed in the interval $[-s; s]$ (Fig. 1). Due to the symmetry we will consider the vector $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ representing the right half of the density function (γ_i denotes the area of the ith column).

Corollary 1. The Fourier transform of a piece-wise uniform density function reads:

$$P_s(\Omega) = \frac{2n}{\Omega \cdot s} \cdot p_1(\Omega); \tag{4}$$

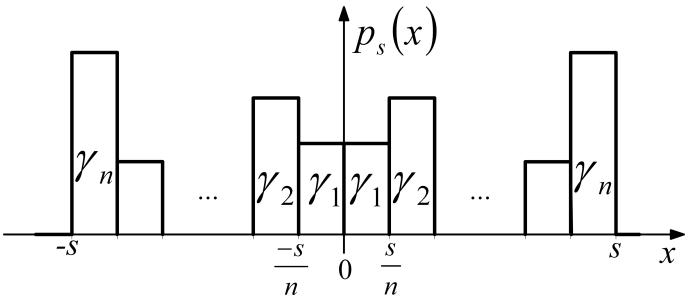

Fig. 1. A piece-wise uniform density function comprising $2n$ equispaced columns. The density is described by the weight-vector $(\gamma_1, \gamma_2, \ldots, \gamma_n)$; γ_i is the area of the i-th column.

where

$$p_1(\Omega) = (\gamma_1 - \gamma_2)\sin\left(\frac{s\Omega}{n}\right) + (\gamma_2 - \gamma_3)\sin\left(\frac{2s\Omega}{n}\right) + \ldots$$
$$+(\gamma_{n-1} - \gamma_n)\sin\left(\frac{(n-1)s\Omega}{n}\right) + n\gamma_n \sin(s\Omega).$$

The derivative of the Fourier transform $P_s(\Omega)$ with respect to amplitude s reads:

$$P_s'(\Omega) = \frac{2}{s} \cdot p_2(\Omega) - \frac{2n}{\Omega s^2} \cdot p_1(\Omega); \tag{5}$$

where

$$p_2(\Omega) = (\gamma_1 - \gamma_2)\cos\left(\frac{s\Omega}{n}\right) + (\gamma_2 - \gamma_3)\cos\left(\frac{2s\Omega}{n}\right) + \ldots$$
$$+(\gamma_{n-1} - \gamma_n)\cos\left(\frac{(n-1)s\Omega}{n}\right) + n\gamma_n \cos(s\Omega).$$

Corollary 2. If a periodic grayscale function can be expanded into a Fourier series:

$$F(x) = \frac{a_0}{2} + \sum_{k=1}^{\infty}\left(a_k \cos\frac{2k\pi x}{\lambda} + b_k \sin\frac{2k\pi x}{\lambda}\right), \quad a_k, \quad b_k \in \mathbf{R}, \tag{6}$$

then, according to [14]

$$H(F(x), \zeta_s(t)) = \frac{a_0}{2} + \sum_{k=1}^{\infty}\left(a_k \cos\frac{2k\pi x}{\lambda} + b_k \sin\frac{2k\pi x}{\lambda}\right) P_s\left(\frac{2k\pi}{\lambda}\right). \tag{7}$$

Elementary transformations help to compute the average of a time-averaged grayscale grating function:

$$E(H(F(x), \xi_s(t))) = \frac{a_0}{2}; \tag{8}$$

its standard:

$$\sigma(H_s(F(x), \xi_s)) = \frac{\sqrt{2}}{2}\sqrt{\sum_{k=1}^{\infty}(a_k^2 + b_k^2) \cdot P_s^2\left(\frac{2k\pi}{\lambda}\right)}; \tag{9}$$

and the derivative of the standard which is used as a measure of the encryption security (detailed reasoning is given in the next section):

$$\sigma_s'(H_s(F(x), \xi_s)) = \frac{\sqrt{2}}{2}\frac{\sum_{k=1}^{\infty}\left(a_k^2 + b_k^2\right) \cdot P_s\left(\frac{2k\pi}{\lambda}\right) \cdot P_s'\left(\frac{2k\pi}{\lambda}\right)}{\sqrt{\sum_{k=1}^{\infty}(a_k^2 + b_k^2) \cdot P_s^2\left(\frac{2k\pi}{\lambda}\right)}}. \tag{10}$$

3 The Construction and Solving of Optimization Problem

It is well known [14] that time-averaged moiré fringes do not develop when a stepped moiré grating is oscillated harmonically. On the other hand, time-averaged fringes do form when a stepped moiré grating (1) is oscillated by a time function which density function is a piece-wise uniform function comprising $2n$ equispaced columns. The clearest moiré fringe formes at the amplitude of oscillations corresponding to the first root of Fourier transform of the density function [14]. The first time-averaged moiré fringe formes at $s = \lambda/2$ for the uniform density function: the standard of the time-averaged moiré grating is equal to zero then. The roots of the Fourier transform (eq. 4) of the piece-wise uniform density function are spread out periodically as well. Then the following question arises: which density function – uniform or piece-wise uniform – is better in respect of the security of information encryption? It is clear that the magnitude of the derivative of the standard at the amplitude corresponding to the formation of the first moiré fringe can be considered as a measure of the encryption security.

Thus, the following problem of combinatorial optimization is considered: find a vector $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ maximizing the target function

$$\left|\sigma_s'\left(s=\frac{\lambda}{2}\right)\right| = \left|\frac{\sqrt{2}}{2}\frac{\sum\limits_{k=1}^{\infty}\left(a_k^2+b_k^2\right)\cdot P_s\left(\frac{2k\pi}{\lambda}\right)\cdot P_s'\left(\frac{2k\pi}{\lambda}\right)}{\sqrt{\sum\limits_{k=1}^{\infty}\left(a_k^2+b_k^2\right)\cdot P_s^2\left(\frac{2k\pi}{\lambda}\right)}}\right|, \tag{11}$$

with the following constraints $\sum\limits_{i=1}^{n}\gamma_i = \frac{1}{2}$ and $\gamma_i > 0$; $i = 1, 2, \ldots, n$ in force.

In order to reduce the computational costs of the problem we analyze an integer programming problem instead: we seek integer values of $\gamma_1, \gamma_2, \ldots, \gamma_n$ and then normalize them with respect to $2 \cdot \sum\limits_{i=1}^{n}\gamma_i$: $\frac{1}{2\cdot\sum\limits_{i=1}^{n}\gamma_i}(\gamma_1, \gamma_2, \ldots, \gamma_n)$.

The sum $H = \gamma_1 + \gamma_2 + \ldots + \gamma_n$ is fixed (following the properties of the density function) what yields :

$$\left|\sigma_s'(s=\frac{\lambda}{2})\right| = \left|\frac{\sqrt{2}}{2}\cdot\frac{\sum\limits_{k=1}^{\infty}\left(a_k^2+b_k^2\right)\cdot P_s\left(\frac{2k\pi}{\lambda}\right)\cdot P_s'\left(\frac{2k\pi}{\lambda}\right)}{\sqrt{\sum\limits_{k=1}^{\infty}\left(a_k^2+b_k^2\right)\cdot P_s^2\left(\frac{2k\pi}{\lambda}\right)}}\right| \to \max, \tag{12}$$

$$\text{at } \sum_{i=1}^{n}\gamma_i = H; \tag{13}$$

$$\gamma_i > 0,\ i = 1, 2, \ldots, n. \tag{14}$$

where γ_i, $i = 1, 2, \ldots, n$; $H \in \mathbf{N}$.

It can be noted that the quantity of vectors $(\gamma_1, \gamma_2, \ldots, \gamma_n)$, satisfying 13 and 14 constrains is equal to $N_\gamma = \frac{(H-n+1)(H-n+2)}{2}$.

We will use evolutionary algorithms for solving the problem 12-14. Every chromosome represents a vector $(\gamma_1, \gamma_2, \ldots, \gamma_n)$. The length of each chromosome is 12 and the sum $H = 60$, i.e. a gene is the integer between 1 and 49. The width of the columns is fixed, thus the magnitude of a gene is proportional to the height of a corresponding column. The fitness of the chromosome is estimated by $\left|\sigma'_s\left(s = \frac{\lambda}{2}\right)\right|$.

The initial population comprises N randomly generated chromosomes. Each chromosome in the initial population was generated in such way that 13 and 14 requirements hold true. All chromosomes $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ lie on hyperplane, described by equation 13 and inequalities 14. The procedure of generation of the chromosomes is following:

- generate an integer γ_1 distributed uniformly over the interval $[1; H - n + 1]$;
- generate an integer γ_2 distributed uniformly over $[1; H - n + 1 - \gamma_1]$;
- ...
- generate γ_{n-1} distributed uniformly over $\left[1; H - n + 1 - \sum_{i=1}^{n-2} \gamma_i\right]$;
- calculate the gene $\gamma_n = H - n + 1 - \sum_{i=1}^{n-1} \gamma_i$.

Replications are allowed in the initial population. Therefore chromosomes $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ are distributed uniformly over the hyperplane, described by eq. 12 and eq. 14 and the probability for all chromosomes to be selected into the initial population is uniform and equals to $\frac{1}{H-n+1} \cdot \frac{1}{H-n} \cdot \ldots \cdot \frac{1}{2} \cdot 1 = \frac{1}{(H-n+1)!}$.

The fitness of each chromosome is evaluated and an even number of chromosomes is selected to the mating population (the size of the mating population is equal to the size of initial population). We use a random roulette method for the selection of chromosomes; the chance that a chromosome will be selected is proportional to its fitness value. All chromosomes are paired randomly when process of mating is over.

The crossover between two chromosomes is executed for all pairs in the mating population. We use one-point crossover method and the location of this point is random. We introduce a crossover coefficient κ which characterizes a probability that the crossover procedure will be executed for a pair of chromosomes. If a chromosomes violates condition 13 after crossover, a norming procedure is applied:

$$(\gamma'_1, \gamma'_2, \ldots, \gamma'_n) = \left(round\left(\frac{H \cdot \gamma_1}{\sum_{i=1}^{n} \gamma_i}\right), round\left(\frac{H \cdot \gamma_2}{\sum_{i=1}^{n} \gamma_i}\right), \ldots, round\left(\frac{H \cdot \gamma_n}{\sum_{i=1}^{n} \gamma_i}\right)\right). \quad (15)$$

If the new chromosome $(\gamma'_1, \gamma'_2, \ldots, \gamma'_n)$ violates condition 14, it is rounded to the nearest $(H - n + 1)$-digit number from n columns.

In order to avoid the convergence to one local solution a mutation procedure is used. The mutation parameter μ $(0 < \mu < 1)$ determines the probability for a chromosome to mutate. The quantity of $round\,(\mu \cdot N)$ chromosomes is randomly selected to expose to the mutation and one gene of each chromosome is changed by adding a random number distributed uniformly over the interval $[1; H - n + 1]$. The norming procedure is applied for the mutated chromosomes.

The following parameters of the evolutionary algorithms must be pre-selected: the crossover coefficient κ, the mutation parameter μ and the size of the population N.

In order to tune the parameters κ and μ we construct an artificial problem – we seek a best density function comprising 6 columns (the length of a chromosome is 3) and $H = 15$. The optimal (full sorting) solution for this problem is the vector $(1; 1; 13)$ and its fitness equals to $\left|\sigma_s'\left(s = \frac{\lambda}{2}\right)\right| = 0.656506722318812$. Now evolutionary algorithms are commenced for the same problem; the population size is set to $N = 20$, what correspond to $\frac{N}{N_\gamma} = \frac{20 \cdot 2}{(15-3+1)(15-3+2)} = \frac{40}{182} \approx 22.99\%$ of all chromosomes.

We select the parameters κ and μ according to the frequency of optimal solution $(1; 1; 13)$ in the population and according to the mean value of the fitness function. Three independent trials of evolutionary algorithms containing 5 generations were executed.

The number of successful trials and the mean value of the fitness function of the population is highest at $\kappa = 0.6$ and $\mu = 0.05$. Thus we fix these parameter values of the evolutionary algorithm and we seek a piece-wise uniform density function comprising 24 columns with $H = 60$ (it is unrealistic to solve such a problem using brute-force full sorting strategies). The number of possible solutions is $N_\gamma = \frac{(60-12+1)(60-12+2)}{2} = 1225$. The size of the population is N=300 which comprises $\frac{N}{N_\gamma} = \frac{300}{1225} \approx 24.49\%$ of all chromosomes. The number of generations is set to 50 and the evolutionary algorithm is executed 5 times. The near-optimal set of $\gamma_k, k = 1, 2, \ldots, 12$ reads $[1; 1; 1; 1; 1; 1; 1; 1; 2; 1; 1; 48]/120$; the near-optimal time function $\xi\,(t)$ is shown in Fig. 2.

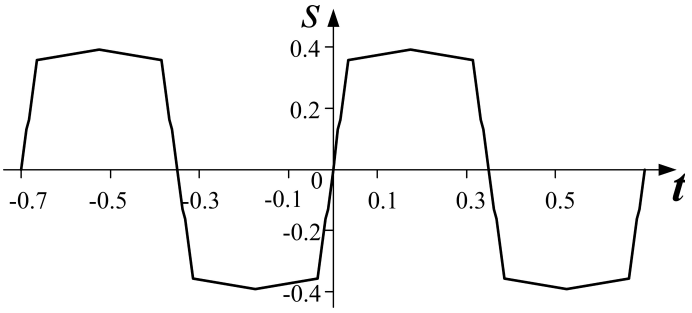

Fig. 2. The near-optimal time function $\xi\,(t)$ as a realization of the near-optimal density function comprising 24 columns at H=60

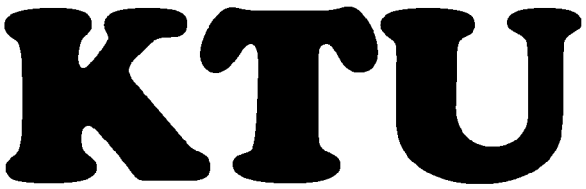

Fig. 3. The secret image

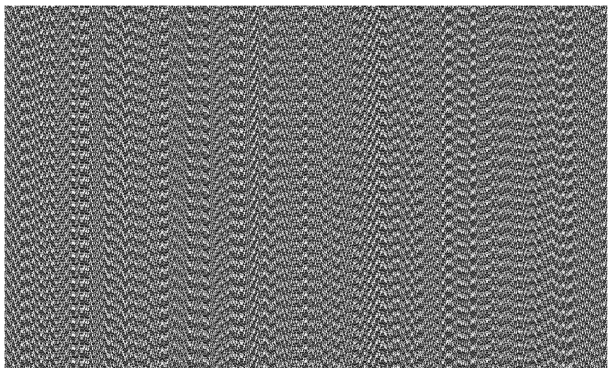

Fig. 4. The secret image encoded into the background moiré grating

Computational results show that the optimal density function gains maximal values at $x = s$ and $x = -s$. In the limiting case the optimal density function reads:

$$p\left(x\right) = \frac{1}{2} \cdot \delta_{-s}(x) + \frac{1}{2} \cdot \delta_{s}(x) \tag{16}$$

where $\delta_{x_0}(x)$ is a delta impulse function at x_0. It can be noted that then

$$P_s\left(\Omega\right) = \int_{-\infty}^{+\infty} \frac{1}{2} \left(\delta_s\left(x\right) + \delta_{-s}\left(x\right)\right) e^{-ix\Omega} dx = \cos\left(s \cdot \Omega\right),$$

and the first time averaged fringe will form at $s = \lambda/4$.

4 Computational Experiments and Concluding Remarks

Computational experiments using the optimal time function with the proposed scheme of dynamic visual cryptography are performed using a secret image shown in Fig. 3. The secret image is encoded into a stepped stochastic moiré background using phase regularization and initial phase randomization algorithms [13]. The secret image can be decrypted using the optimal time function show in Fig. 2

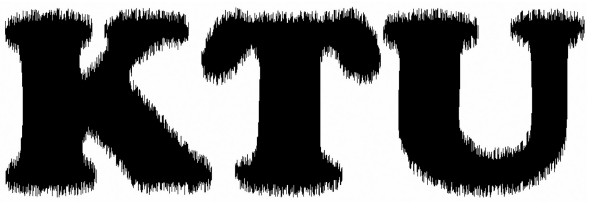

Fig. 5. Contrast enhancement of the decrypted image

at $s = \lambda/4 = 0.39$ mm (contrast enhancement algorithms [16] have been used to make the decrypted image more clear).

An optimal time function ensuring the highest security of the encoded image in the scheme based on dynamical visual cryptography is proposed. The optimality criteria is based on the derivative of the standard of the time averaged image. It is shown that interplay of extreme deflections from the state of equilibrium can be considered as a near-optimal realization of the decoding phase and can be effectively exploited in computational implementation of secure dynamic visual cryptography.

Acknowledgments. Partial financial support from the Lithuanian Science Council under project No. MIP-041/2011 is acknowledged.

References

1. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
2. Shyu, S.: Efficient visual secret sharing scheme for color images. Pattern Recognit. 39, 866–880 (2006)
3. Zhou, Z., Arce, G., Crescenzo, D.: Halftone visual cryptography. IEEE Trans. Image Process. 15, 2441–2453 (2006)
4. Shyu, S.: Image encryption by random grids. Pattern Recognit. 40, 1014–1031 (2007)
5. Hu, C., Tseng, W.: Cheating prevention in visual cryptography. IEEE Trans. Image Process 16, 36–45 (2007)
6. Cimato, S., De Prisco, R., De Santis, A.: Colored visual cryptography without color darkening. Theor. Comput. Sci. 374, 261–276 (2007)
7. Yang, C.N., Chen, T.S.: Extended visual secret sharing schemes: improving the shadow image quality. Int. J. Pattern Recognit. Artificial Intelligence 21, 879–898 (2007)
8. Kobayashi, A.S.: Handbook on Experimental Mechanics, 2nd edn. SEM, Bethel (1993)
9. Patorski, K., Kujawinska, M.: Handbook of the moiré fringe technique. Elsevier, Amsterdam (1993)
10. Post, D., Han, B., Ifju, P.: High sensitivity moiré: experimental analysis for mechanics and materials. Springer, Berlin (1997)

11. Dai, F.L., Wang, Z.Y.: Geometric micron moiré. Opt. Laser Eng. 31, 191–208 (1999)
12. Desmedt, Y., Van Le, T.: Moiré cryptography. In: 7th ACM Conf. on Computer and Communications Security, pp. 116–124 (2000)
13. Ragulskis, M., Aleksa, A.: Image hiding based on time-averaging moiré. Optics Communications 282, 2752–2759 (2009)
14. Ragulskis, M., Aleksa, A., Navickas, Z.: Image hiding based on time-averaged fringes produced by non-harmonic oscillations. J. Opt. A: Pure Appl. Opt. 11, 125411 (2009)
15. Ragulskis, M., Navickas, Z.: Hash functions construction based on time average moiré. J. Discrete and Continuous Dynamical Systems-Series B 8, 1007–1020 (2007)
16. Ragulskis, M., Aleksa, A., Maskeliunas, R.: Contrast enhancement of time-averaged fringes based on moving average mapping functions. Optics and Lasers in Engineering 47, 768–773 (2009)