



Image hiding based on time-averaging moiré

Minvydas Ragulskis *, Algimantas Aleksa

Research Group for Mathematical and Numerical Analysis of Dynamical Systems, Kaunas University of Technology, Studentu 50-222, Kaunas LT-51638, Lithuania

ARTICLE INFO

Article history:

Received 1 October 2008

Received in revised form 15 March 2009

Accepted 3 April 2009

Keywords:

Geometric moiré

Time-averaged fringes

Bessel functions

ABSTRACT

Image hiding based on optical time-averaging moiré technique is presented in this paper. It is a new visual decoding scheme when the secret image is embedded into a moiré grating and can be interpreted by a naked eye only when the image is harmonically oscillated in a predefined direction. The secret image is visualized at strictly defined amplitude of oscillation. Computational and experimental examples are used to demonstrate the functionality of the method.

© 2009 Elsevier B.V. All rights reserved.

1. Introduction

Geometric moiré [1,2] is a classical in-plane whole field non-destructive optical experimental technique based on analysis of visual patterns produced by superposition of two regular gratings that geometrically interfere. Examples of gratings are equispaced parallel lines, concentric circles, arrays of dots. The gratings can be superposed by double-exposure photography, by reflection, by shadowing, or by direct contact [3,4]. Moiré patterns are used to measure variables such as displacements, rotations, curvature, and strains throughout the viewed area. In-plane moiré is typically conducted with gratings of equispaced, parallel lines [2,3].

Two goals exist in moiré pattern research. The first is the analysis of moiré patterns. The task is to analyze and characterize the distribution of moiré fringes in a moiré pattern. 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. Moiré fringes in a pattern are enumerated using manual, semi-manual or fully automatic computational techniques [1].

Another goal is moiré pattern synthesis when the generation of a certain predefined moiré pattern is required. The synthesis process involves production of such two images that the required moiré pattern emerges when those images are superimposed [5]. Moiré synthesis and analysis are tightly linked and understanding one task gives insight into the other.

* Corresponding author. Tel.: +370 69822456; fax: +370 37330446.

E-mail address: minvydas.ragulskis@ktu.lt (M. Ragulskis).

URL: <http://www.personalas.ktu.lt/~mragul> (M. Ragulskis).

Moiré patterns are patterns that don't exist in any of the original images but appear in the superposition image. The topic of moiré pattern synthesis deals with creating images that, when superimposed, will reveal certain desired moiré patterns. Conditions ensuring that a desired moiré pattern will be present in the superposition of two images are pre-determined; however they do not specify these two original images uniquely. The freedom in choosing the superimposed images can be exploited to produce various degrees of visibility and ensure desired properties. Several criteria are proposed in [6,7] to resolve that freedom in moiré pattern synthesis.

Another technique based on optical moiré operations for image encryption and decryption is presented by simulation and experimentally in [8]. The moiré grating is generated by a computational algorithm as a harmonic function. The intensity of the reflectance map of the secret image is added as an argument of the harmonic moiré grating. The decryption is performed by overlapping the encrypted image with a key fringe pattern.

A technique based on optical operations on stochastic moiré patterns for image encryption and decryption is developed in [9]. In this method, an image is encrypted by a stochastic geometric moiré pattern deformed according to the image reflectance map. The decryption is performed using pixel correlation algorithm in the encrypted image and the original stochastic geometrical moiré pattern.

The object of this paper is to develop a new scheme for image hiding based not on superposition of moiré images but on time-averaging geometric moiré. A secret image can be interpreted by a naked eye only when the original encoded image is harmonically oscillated in a predefined direction. This visual decoding technique requires only one image; the encoded image looks like a random image in the state of the rest. Moreover, the secret image is visualized only at strictly defined amplitude of oscillation.

2. Optical background

One-dimensional example is analyzed for simplicity at first. Moiré grating on the surface of a one-dimensional structure in the state of equilibrium can be interpreted as a periodic variation of black and white colors:

$$M(y) = \frac{1}{2} \left(1 + \cos \left(\frac{2\pi}{\lambda} y \right) \right) = \cos^2 \left(\frac{\pi}{\lambda} y \right), \tag{1}$$

where y is the longitudinal coordinate; $M(y)$ is grayscale level of the surface at point y ; λ is the pitch of the grating. Numerical value 0 of the function in Eq. (1) corresponds to black; 1 – to white; all intermediate values – to grayscale levels.

Time-average geometric moiré is an optical experimental method when the moiré grating is formed on the surface of an oscillating structure and time averaging techniques are used for the registration of time averaged patterns of fringes [10]. Again, we will use one-dimensional model to illustrate the formation of time-averaged fringes. We assume that the deflection from state of equilibrium varies in time:

$$u(x, t) = a(x) \sin(\omega t + \varphi), \tag{2}$$

where ω is the cyclic frequency, φ is the phase and $u(x)$ is the amplitude of harmonic oscillations at point x . Then, the time averaged grayscale level can be expressed like [10,11]:

$$M_T(x, y) = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \cos^2 \left(\frac{\pi}{\lambda} (y - a(x) \sin(\omega t + \varphi)) \right) dt = \frac{1}{2} + \frac{1}{2} \cos \left(\frac{2\pi}{\lambda} y \right) J_0 \left(\frac{2\pi}{\lambda} a(x) \right), \tag{3}$$

where T is the exposure time; i is the imaginary unit; J_0 is the zero order Bessel function of the first kind. Time-averaged fringes will form at such x where $J_0 \left(\frac{2\pi}{\lambda} a(x) \right) = 0$. Now the relationship between fringe order, the amplitude of oscillations and the pitch of the grating takes the following form:

$$\frac{2\pi}{\lambda} a_i(x) = r_i, \tag{4}$$

where r_i denotes i th root of the zero order Bessel function of the first kind; a_i is the amplitude of oscillation at the center of the i th fringe.

Computationally reconstructed pattern of time-averaged fringes is presented in Fig. 1. Static moiré grating is formed in

the interval $0 \leq y \leq 5$ ($\lambda = 0.2$); white background is assumed elsewhere. It is assumed that $a(x) = x$. Therefore clear moiré grating is visible at the left part of the time-averaged image which gets blurred as the amplitude of harmonic oscillations increases. But the decline of contrast of the time-averaged image is not monotonic as the amplitude increases. It is modulated by the zero order Bessel function of the first kind (Eq. (3)). Time-averaged fringes form around the areas where the amplitude of oscillation satisfies the relationship (4). We plot zero order Bessel function of the first kind in the bottom part of Fig. 1 to give an explicit illustration of Eq. (4). It can be noted that the frequency of oscillations has no effect to the formation of fringes (Eq. (3)). Exposure time must be long enough to fit in a large number of periods of oscillations (or alternatively must be exactly equal to one period of oscillation). Plotting procedure used to construct digital time-averaged image in Fig. 1 is discussed in detail in [12].

3. Image hiding based on time-averaging geometric moiré

Illustration of the formation of time-averaged fringes is presented in Fig. 2. In contrary to Fig. 1 we now use a constant amplitude of oscillations for the whole image. Static digital image is shown in Fig. 2a. Moiré grating in the background is formed as an array of parallel lines; the pitch of the grating is $\lambda_0 = 0.2$. Three digits are formed in front of the background image. All these digits are also formed as arrays of parallel lines. Pitch of the moiré grating is $\lambda_1 = 0.143$ in the area of digit 1, $\lambda_2 = 0.131$ in the area of digit 2 and $\lambda_3 = 0.111$ in the area of digit 3.

Now we are ready to construct digital time-averaged images. We calculate integral sum instead of calculating indefinite integral in Eq.(3). Thus, time averaged one-dimensional image becomes (the amplitude a is constant in the area of the whole image):

$$M_T(x, y) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=0}^{n-1} \cos^2 \left(\frac{\pi}{\lambda} \left(y - a \sin \left(\frac{2\pi k}{n} \right) \right) \right). \tag{5}$$

In practice that means that we calculate averages of many frames where every frame represents the original static image deflected from the state of equilibrium by a certain magnitude defined by Eq. (5). Relationship between the number of correctly reconstructed interference fringes and the number of frames n in Eq. (5) is studied in [12]. We use $n = 256$ in our computational experiments what guarantees acceptable accuracy of the first 32 time-averaged fringes (in fact we will use only first three time-averaged fringes to visualize digits 1, 2 and 3).

We select such discrete amplitudes that moiré patterns in the areas occupied by appropriate digits in Fig. 2a would be transformed into gray fringes in time-averaged images. The first three roots of the zero order Bessel function of the first kind can be easily reconstructed using simple root finding algorithm: $r_1 = 2.4054$; $r_2 = 5.5201$ and $r_3 = 8.6537$. It can be noted that numerical values of these roots are intrinsic to the Bessel function. We use relationship in Eq. (4) to calculate the necessary magnitude of the amplitude a . As mentioned previously, the amplitude will be constant for the whole image which will oscillate as a solid non-deformable body. Thus, $a_1(x) = a_1 = \frac{r_1 \lambda_1}{2\pi} = 0.0547$ yields an interference fringe in the area occupied by the digit 1 (Fig. 2b), but interference fringes are not formed in the background nor in the areas occupied by digits 2 and 3 (though the original moiré gratings are of course somewhat blurred there if compared to the static image). Analogously, $a_2 = \frac{r_2 \lambda_2}{2\pi} = 0.1148$ produces interference fringe in the area occupied by the digit 2 and $a_3 = \frac{r_3 \lambda_3}{2\pi} = 0.1530$ – interference fringe in the area of the digit 3.

Clearly, Fig. 2a cannot be considered as a safe encoding of digits 1, 2 and 3 – these numbers can be interpreted by a naked eye from

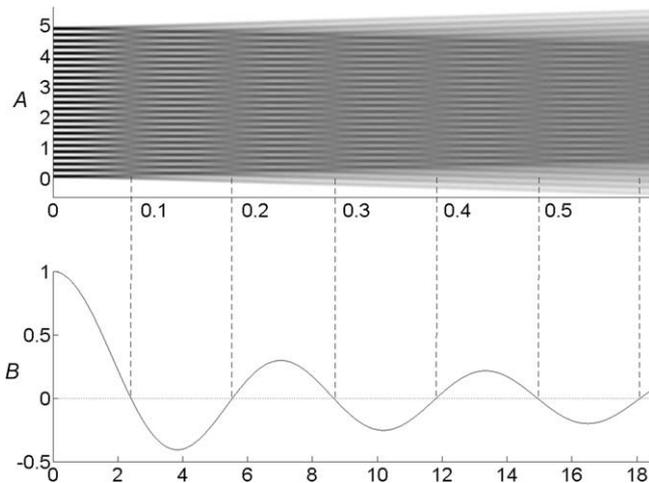


Fig. 1. Pattern of time-averaged fringes at $\lambda = 0.2$; $a(x) = x$: (A) Grayscale time-averaged image. (B) Zero order Bessel function of the first kind; dashed lines are used to interconnect the centers of time-averaged fringes and roots of the Bessel function.

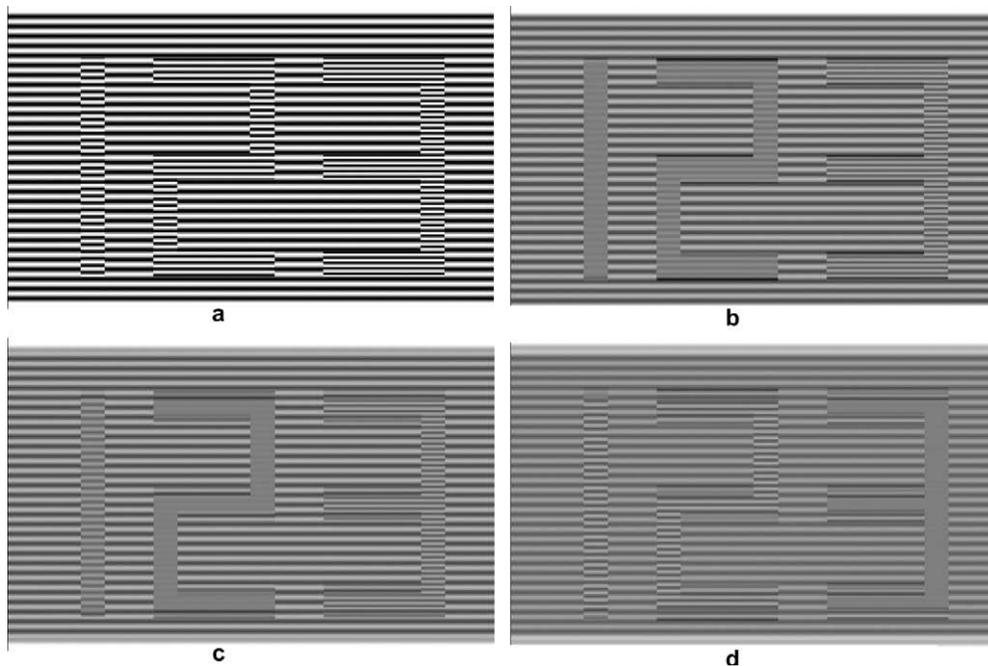


Fig. 2. Illustration of the formation of time-averaged fringes: (a) The static image; the pitch of the background is $\lambda_0 = 0.2$; the pitch in the area occupied by the digit 1 is $\lambda_1 = 0.143$; the pitch of the digit 2 is $\lambda_2 = 0.131$; the pitch of the digit 3 is $\lambda_3 = 0.111$. (b) Time-averaged image at $a = 0.0547$. (c) Time-averaged image at $a = 0.1148$. (d) Time-averaged image at $a = 0.1530$.

the static image. Special image transformation techniques are to be used before the original static image can be considered as a safe carrier of the secret information. Such transformations must preserve the basic rule – interference fringes must form in the time-averaged image of the vibrating original image in zones occupied by secret symbols. In general, there exist many different transformations which could impede direct visual interpretation of the original symbols but still preserve the afore-mentioned principle of time averaging. We will demonstrate a simple method for the construction of such a digital image.

Let's assume that a secret text "KAUNAS" should be encoded in a background moiré pattern. First of all one has to select the magnitude of the amplitude which will be used to decrypt the image. We select $a(x) = a = 0.0574$. Now, the pitch of the background image λ_0 can be selected. We select $\lambda_0 = 0.19$ what guarantees that

the background moiré grating will not disappear in the time-averaged image (the numerical value of the relationship $2\pi a/\lambda$ is far away from all roots of the zero order Bessel function of the first kind).

Next step is the selection of pitches for the encrypted text. It can be noted that different pitches can produce interference fringes at the same amplitude – the zero order Bessel function of the first kind has multiple roots (Fig. 1).

We construct the digital image as a set of vertical columns of pixels (constitutive moiré grating lines are horizontal in our experiment). Every single vertical column corresponds to a set of grayscale pixels. Variation of the grayscale level in the zone of the background image corresponds to the pitch λ_0 . Variation of the grayscale level in the areas occupied by the encrypted text must correspond to one of the pitches calculated from Eq. (4):

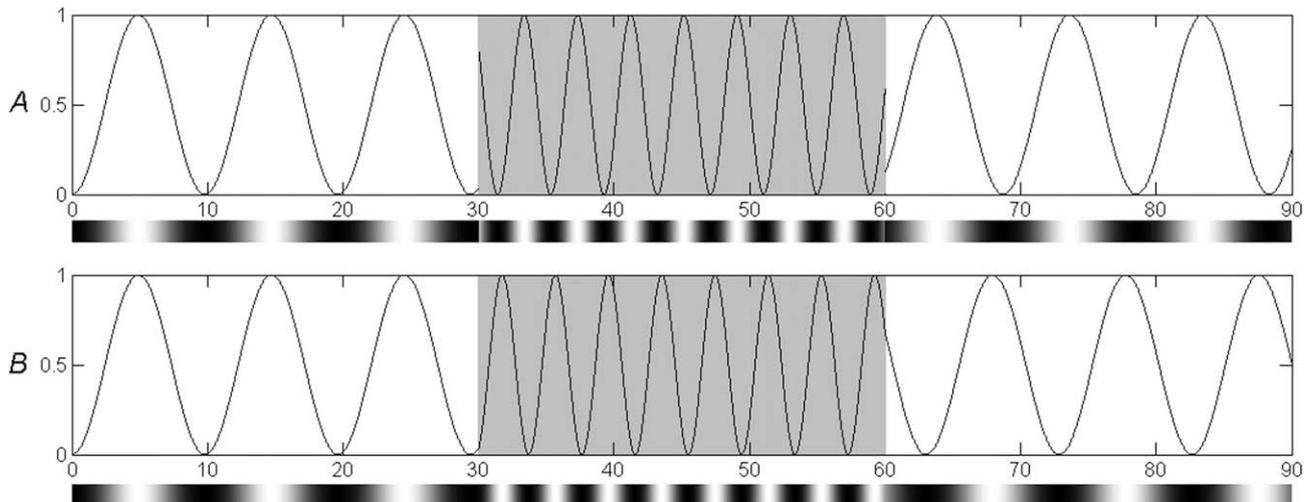


Fig. 3. Matching of phases at boundaries of the background image and the encrypted image; variations of grayscale levels before the matching (A) and after the matching (B) are shown.

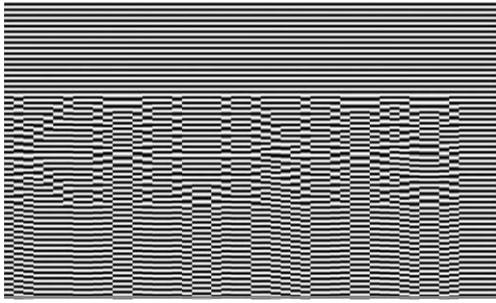


Fig. 4. Encryption of the text “KAUNAS” into a background moiré grating. Pitch of the background grating is $\lambda_0 = 0.19$; pitch at zones corresponding to the encrypted text is $\lambda_1 = 0.15$.

$$\lambda_i = \frac{2\pi a}{r_i}, \quad i = 1, 2, \dots \quad (6)$$

Moreover, we select appropriate phases of the harmonic variation of the grayscale levels in different zones of the digital image in order to avoid discontinuities (Fig. 3). We illustrate the necessity of this phase matching using both a line graph and a grayscale level map. The zone of the encrypted text is shaded for clarity. One pixel column (before and after the matching of phases) is shown. Columns are placed horizontally in order to minimize the size of the figure.

As mentioned previously, we use a rather primitive rule to embed the secret image into a moiré grating. It can be noted that the structure of the moiré grating at the bottom part of the background image is violated due to the matching of the phases (starting from the top of the image). The pitch of the moiré grating at zones corresponding to the encrypted text is $\lambda_1 = \frac{2\pi a}{r_1} = \frac{2\pi \cdot 0.0574}{2.4054} \approx 0.15$. In other words, only the first root of the Bessel function will be used to visualize the encoded text.

Simple embedding of text “KAUNAS” in a background moiré image would produce clearly an unsatisfactory result (Fig. 4) – the “secret” information can be easily recognized by a naked eye. Therefore we use stochastic phase deflection at the top of adjacent vertical columns of pixels. This procedure is illustrated in Fig. 5 where two adjacent vertical columns of pixels are presented after the initial random phase at the top of the image (at left in Fig. 5) is already assigned. Gray shaded zones in Fig. 5 are plotted different as we operate with two different columns of pixels. Phases are matched at boundaries of the background and the encoded image.

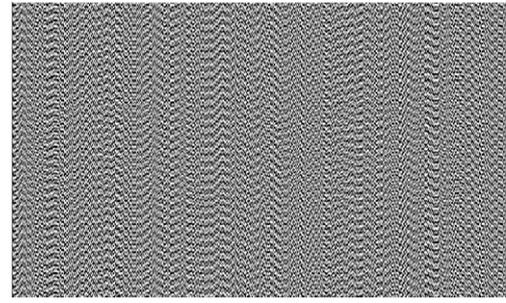


Fig. 6. Text “KAUNAS” encrypted into the background moiré grating. Pitch of the background grating is $\lambda_0 = 0.19$; the pitch at zones corresponding to the encrypted text is $\lambda_1 = 0.15$; the procedure of stochastic deflections of phases is applied.

Such random scrambling of initial phases may appear similar to the concept of stochastic geometric moiré presented in [9]. In fact, these two concepts are completely different – pixels of the background image are not shifted from their original locations in contrary to the technique exploited in [9].

Such an encoding method is relatively primitive, though it prevents direct interpretation of the secret text (Fig. 6). Nonetheless, we continue with this simple method and demonstrate the functionality of the decoding procedure in Fig. 7. The embedded text “KAUNAS” is visible as a pattern of gray time-averaged fringes in Fig. 7A (only at appropriate amplitude). The magnitude of the amplitude is pre-selected in order to transform the moiré grating into gray regions in the areas of the secret text. But the moiré grating in the background is not transformed into a gray area (Fig. 7A).

Alternatively, the background can be transformed into a gray zone at appropriate amplitude (we used only one single pitch to construct the background moiré grating). Fig. 7B shows the decoded text which can be clearly distinguished in the gray background. But visualization of the secret text is not impossible if either the zones corresponding to the secret text or the background is not transformed into a pattern of gray time-averaged fringes (Fig. 7C). The ripples at the top and the bottom of images in Fig. 7 are produced by time averaging of boundaries (similar effect can be observed in Fig. 1A). The higher is the amplitude, the wider are these ripples.

Our proposed method could be considered to be somewhat similar to the moiré cryptography method proposed by Desmedt and Van Lee [5]. But there is a principal difference between optical techniques used in [5] and in our approach. Double exposure

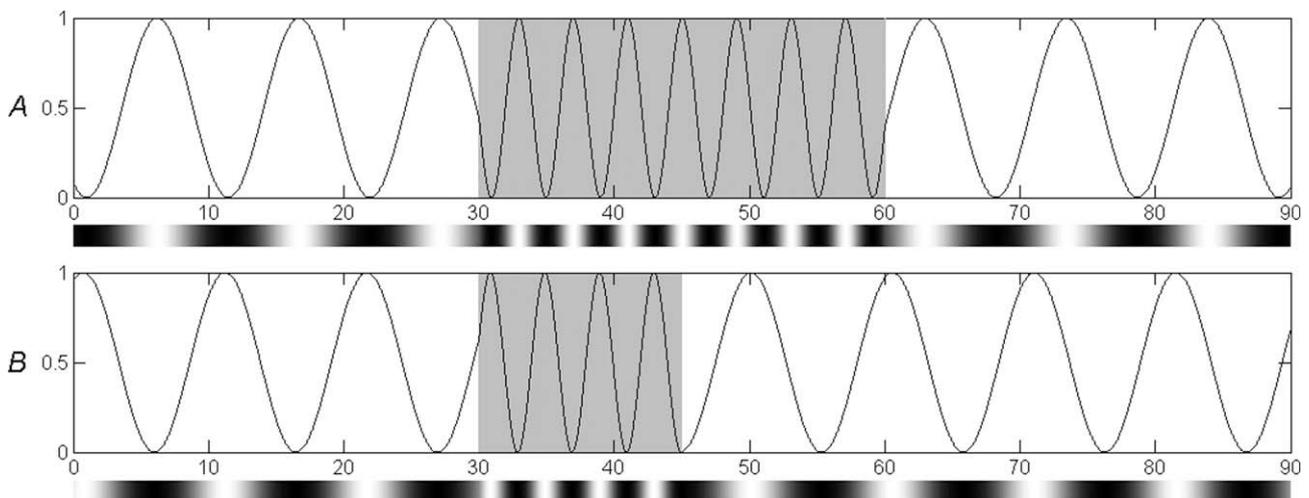


Fig. 5. Illustration of the procedure of stochastic deflection of phases for adjacent columns of pixels.

geometric moiré (a superposition of two moiré slides) is used in [5]. We use time-averaging geometric moiré optical technique. There are no 2 or n shares to superpose in our method. We use one image only. We oscillate that image in order to produce

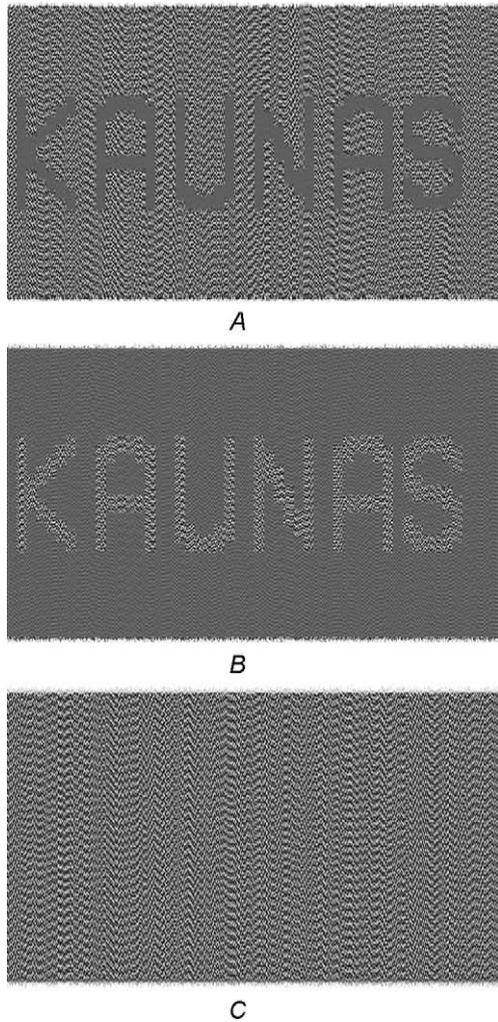


Fig. 7. Computational decryption of the encrypted text at different amplitudes of oscillations: (A) $-a = 0.0574$; (B) $-a = 0.0747$; (C) $-a = 0.1334$.

time-averaged moiré fringes. This is in contrary to interference between two static moiré gratings. The formation of time-averaged fringes is governed by different physical processes compared to double exposure fringes; motion induced blur is exploited to generate time-averaged fringes. Thus, the similarity between these two methods is only apparent; optical principles used to decode the secret are completely different.

Numerical construction of a time-averaged image when the original image performs unidirectional oscillations can be interpreted as a calculation of the integral sum when the number of nodes in the time axis tends to infinity (Eq. (5)). In fact, the integration interval can be shortened to $[-\pi/2; \pi/2]$ instead of $[0; 2\pi]$. Computational process of the formation of a time-averaged image is illustrated in Fig. 8. First of all, the time interval (the exposure time) is split into n subintervals. Then the original image is shifted from the state of equilibrium; the deflection equals to an instantaneous value of the time function $a \sin t$. Finally, all n shares (in fact the same original but shifted image) are averaged into the time-averaged image. Since we calculate an arithmetical average in the integral sum, such superposition of shares is an additive superposition [2]. On the contrary, classical visual cryptography scheme uses the overlapping of shares [13,5] (what is a geometric superposition [2]).

Experimental visualization of the secret image requires optical formation of a time-averaged image. A schematic illustration of an experimental setup is illustrated in Fig. 9. In fact, a camera is not necessary for this experimental setup; all optical effects can be clearly interpreted by a naked eye. We use a camera only to document these optical effects.

One must have the ability to control the frequency and the amplitude of the shaker. It is important that the direction of harmonic oscillations would coincide with the direction perpendicular to moiré grating lines. This would not be an easy task in practice if the picture would not be rectangular or grating lines would be inclined (the moiré grating structure is encoded using the stochastic phase deflection technique). Theoretically, the time of exposure should tend to infinity (we do not use stroboscopic illumination to single out one period of oscillations). In practice, it is enough that a large number of periods of oscillation would fit into the time of exposure [1,11]. As shown previously, the frequency of oscillations does not have any influence to the formation of the time-averaged image (Eq. (3)). Nevertheless, one must use a quite high frequency of oscillations allowing the human eye to average fast dynamical processes being not able to follow rapid oscillatory motions. In other words, visual decoding “by hands only” would be

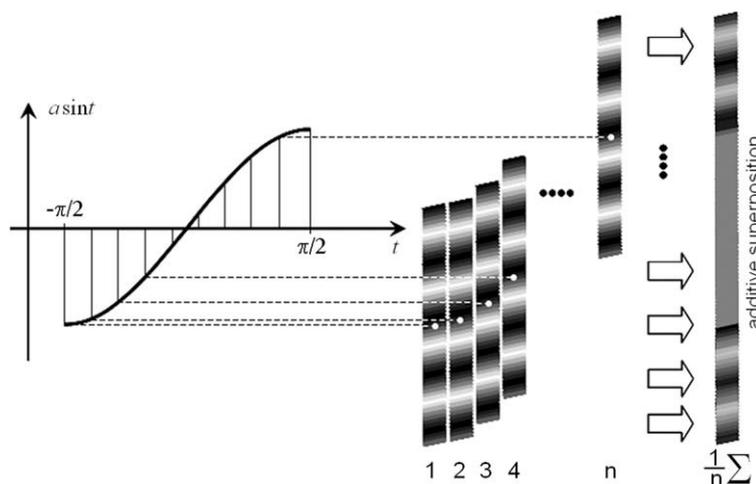


Fig. 8. A schematic diagram illustrating computational reconstruction of a time-averaged image.

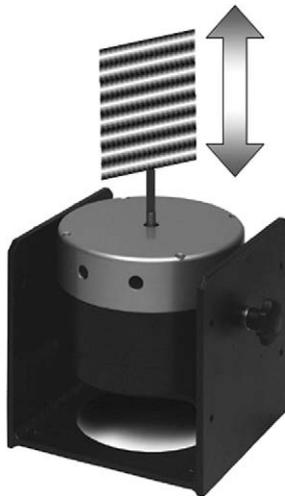


Fig. 9. A schematic diagram illustrating experimental visualization of a secret image.

almost impossible. It is difficult to shake a hand at a high frequency. It would also be extremely hard to keep constant amplitude of oscillations. It would be even more difficult to maintain unidirectional oscillations. Therefore one must use a shaker table in order to visually decode the secret.

4. Experimental validation of the decoding technique

The proposed visualization scheme is based on the optical time averaging of an image fixed onto the surface of a solid non-deformable body which performs harmonic oscillations. The experimental setup used for the implementation of this visualization technique comprises a shaker table and an ordinary optical camera (Fig. 10). The encoded image is printed using several different resolutions and glued onto the surface of a rigid structure which is fixed to the head of the shaker. We select the frequency of oscillations $\omega = 100$ Hz and the time of exposure $T = 1$ s. Thus, around 100 periods of harmonic oscillations fit into the time of exposure. If some fractional part of the period is cut out at the beginning or at the end of the exposure interval, that has a negligible effect to the process of time averaging.

The size of the encoded picture is 145 mm \times 115 mm (the left sheet in Fig. 10). Several experimental time-averaged pictures are presented in Figs. 11 and 12. Fig. 11A shows the experimentally decoded image (amplitude $a = 0.9$ mm) when the secret text is visualized as a pattern of time-averaged fringes. It can be noted that letters “KAU” are clearly visible, while the rest part of the text is



Fig. 10. A view of the experimental setup showing the shaker table, encrypted images fixed onto the surface of a rigid structure and an optical camera.

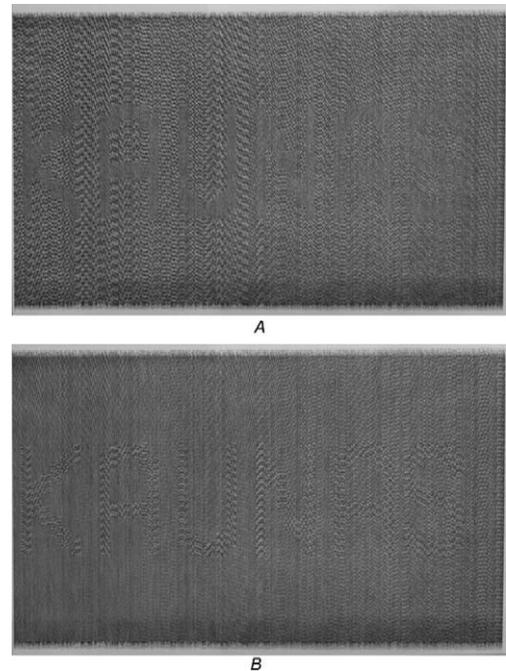


Fig. 11. Time averaged experimental images: (A) The decoded text is visualized as a pattern of interference fringes ($a = 0.9$ mm); (B) The decoded text is visualized in a blurred background ($a = 1.2$ mm).

blurred – this is due to poor fixing of the paper sheet to the vibrating steel plate.

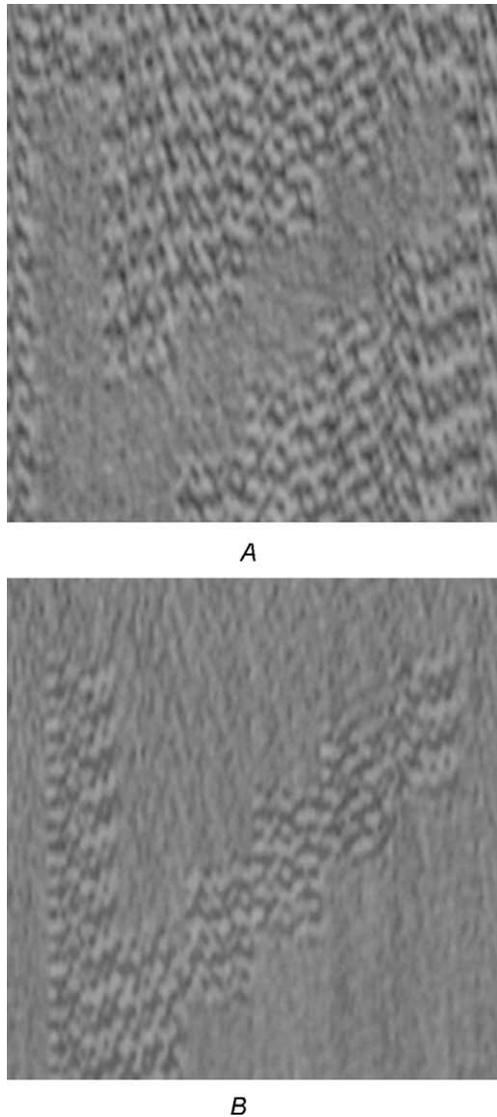
Fig. 11B shows the experimentally decoded image (amplitude $a = 1.2$ mm) when the moiré grating in the background is blurred almost to the grayscale level of an interference fringe (the secret text is visualized as a pattern of less blurred lines).

The magnified upper parts of the letter ‘K’ are shown in Fig. 12A and B in order to demonstrate the effectiveness of the experimental visualization technique. The boundaries between the zones corresponding to the secret text and the background are clearly visible there.

5. More complex encoding algorithms

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 [13]. 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. Efficient visual secret sharing scheme for color images is proposed in [14]. Halftone visual cryptography based on the blue noise dithering principles is proposed in [15]. Basis matrices free image encryption by random grids is developed in [16]. A generic method that converts a visual cryptography scheme into another visual cryptography scheme that has a property of cheating prevention is implemented in [17]. Colored visual cryptography without color darkening is developed in [18]. Secret sharing schemes based on Boolean operations without pixel expansion are proposed in [19]. Visual cryptography and polynomial-style sharing are combined in one image sharing method [20]. Sharing ability in visual cryp-



method. Now we will demonstrate a more complex (and a more secure) encoding algorithm which prevents a straightforward decoding.

We consider a rectangular picture consisting from 25 different zones (Fig. 13A). Every separate zone will be filled by a moiré grating with a particular pitch (the orientation of grating lines is the same in all zones). We construct three different non-overlapping patterns in Fig. 13B–D. Pitches of moiré gratings are pre-selected in such a way that every different pattern would be visualized in the time-averaged image at different amplitudes of oscillation. We use Eq. (6) to determine the first three pitches which form a time-averaged fringe (in practice one can use even a larger number of pitches for one fixed amplitude). Thus, λ_1, λ_2 and λ_3 are the first three pitches calculated for amplitude a_1 ; μ_1, μ_2 and μ_3 – corresponding to amplitude a_2 , and finally, ρ_1, ρ_2 and ρ_3 – to amplitude a_3 (Fig. 14). The idea of the algorithm is to select such values of a_1, a_2 and a_3 that different pitches would not coincide. Moreover, pitches inside each fixed pattern can be distributed randomly (Fig. 13A). Let’s assume that the secret pattern is shown in Fig. 13C. Then a straightforward visualization of the secret is not so simple. First of all, the whole image would be scrambled using a random initial phase (described in Section 3). Secondly, one needs to know that the picture must be vibrated if one wishes to see the secret. Finally, a trial and error method would not work. The pattern in Fig. 13B will be visualized at amplitude a_1 ; the pattern in Fig. 13C – at amplitude a_2 and the pattern in Fig. 13D – at amplitude a_3 . Which one is the secret from these three patterns?

We omit numerical experiments for brevity. Anyway, if the security of such an encoding method would be considered to be not sufficient, a classical visual cryptography image splitting scheme can be used to split the image encoded by our method into two separate shares. We split the image in Fig. 6 into two shares shown in Fig. 15A and B. Accurate overlapping of these two shares produces the original image in Fig. 6. The random nature of the visual cryptography splitting technique damages the organized structure of moiré gratings and the vibration of any of the separate shares cannot leak the secret. Time-averaged image of a vibrated share (the one in Fig. 15A) is shown in Fig. 15C at amplitude

Fig. 12. Zoomed experimental images in the area around the upper part of the letter “K”: (A) $-a = 0.9$ mm and (B) $-a = 1.2$ mm.

tography up to any general number of multiple secrets in two circle shares is proposed in [21]. Circular visual cryptography scheme for hiding multiple secret images is developed in [22]. Prioritization of the different pixel expansions for image contrast enhancement is proposed in [23]. Extended visual secret sharing schemes have been used to improve the quality of the shadow image in [24]. New progressive image sharing technique is developed in [25].

Our proposed method, strictly speaking, is not a visual cryptography scheme. Our method only resembles a visual cryptography scheme because one needs a computer to encode a secret, and one can decode the secret without a computing device. But our method generates only one picture. In fact, 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.

Also, strictly speaking, our method is not an encryption scheme. We manipulate with time-averaged moiré fringes. Of course, we can construct a very complex pattern of time-averaged fringes, but that does not increase the security of the method. As mentioned in Section 3, we have used a primitive encoding algorithm. Our objective was just to demonstrate the basic principle of the

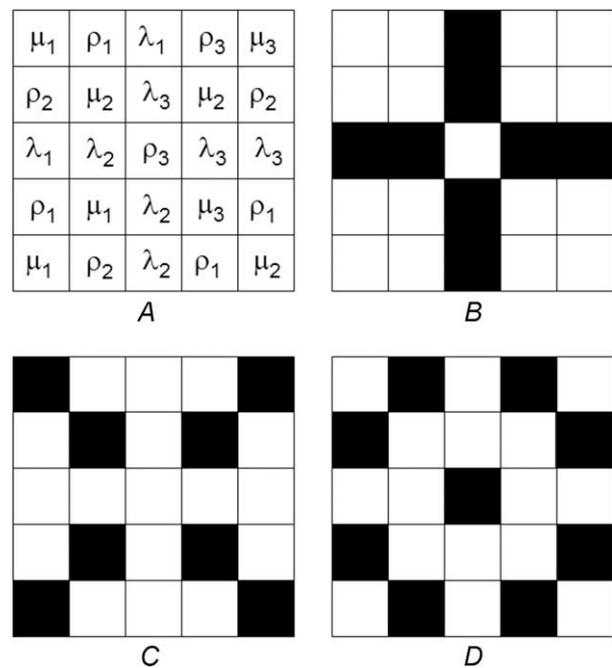


Fig. 13. Schematic illustration of a more complex encoding algorithm.

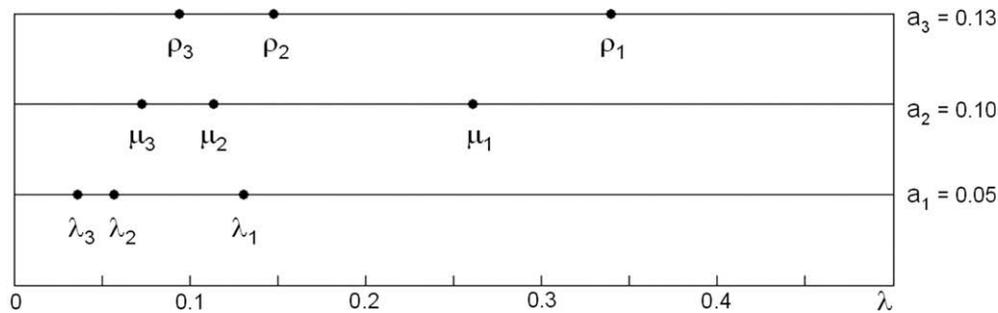
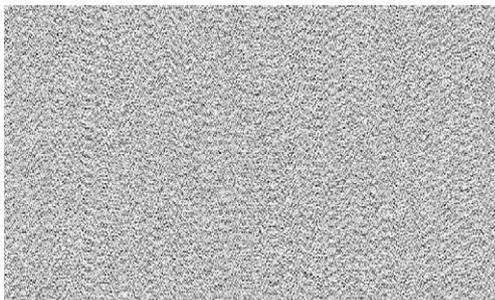
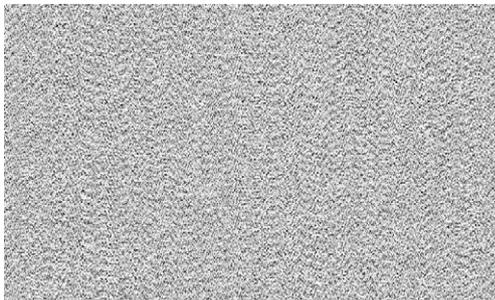


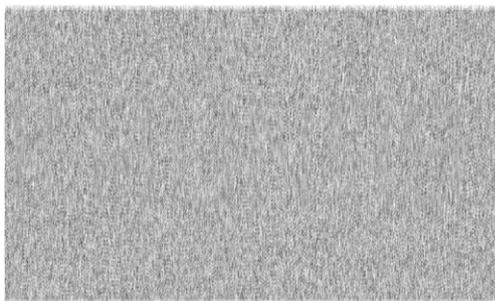
Fig. 14. A diagram illustrating the selection of different amplitudes of oscillation; distinct pitches of moiré gratings (corresponding to first three time-averaged fringes) do not overlap.



A



B



C

Fig. 15. The image in Fig. 6 is split into two shares: A and B; the image in C is a time-averaged share A at $a = 0.0574$.

$a = 0.0574$ (this is the amplitude used to visualize Fig. 7A). No secret can be visualized from one separate share.

6. Concluding remarks

We have developed a new image hiding technique based on optical time-averaging moiré. The encoded secret image is not

shared into components; this is a one image method. The secret image is embedded into the background moiré grating. Stochastic initial phase deflection, phase matching and more complex encoding algorithms help to construct a digital image which cannot be interpreted by a naked eye.

The decoding is performed by vibrating the encoded image in a predefined direction. This is an experimental technique; the decoding process is really visual. We exploit the property of the human visual system to average fast dynamical processes being not able to follow rapid oscillatory motions.

Acknowledgements

We would like to thank prof. Rimantas Maskeliunas from Vilnius Gediminas Technical University for his help with the experimental setup and both anonymous reviewers for their valuable comments which helped to improve the manuscript.

References

- [1] A.S. Kobayashi, Handbook on Experimental Mechanics, second ed., Bethel, SEM, 1993.
- [2] K. Patorski, M. Kujawinska, Handbook of the Moiré Fringe Technique, Elsevier, 1993.
- [3] D. Post, B. Han, P. Ifju, High Sensitivity Moiré: Experimental Analysis for Mechanics and Materials, Springer, Verlag, Berlin, 1997.
- [4] F.L. Dai, Z. Y Wang, Optics and Lasers in Engineering 31 (1999) 191.
- [5] Y. Desmedt, T. van Le, in: Seventh ACM Conference on Computer and Communications Security, 2000, p. 116.
- [6] G. Lebanon, A.M. Bruckstein, Journal of the Optical Society of the America A 18 (2001) 1371.
- [7] G. Lebanon, A.M. Bruckstein, Lecture Notes in Computer Science 2134 (2001) 185.
- [8] M.R.J. Apolinar, R.V. Ramon, Opt. Commun. 236 (2004) 295.
- [9] M. Ragulskis, A. Aleksa, L. Saunoriene, Opt. Commun. 273 (2007) 370.
- [10] C.Y. Liang, Y. Y Hung, A. J Durelli, J.D. Hovanesian, Journal of Sound and Vibration 62 (1979) 267.
- [11] M. Ragulskis, R. Maskeliunas, L. Ragulskis, V. Turla, Optics and Lasers in Engineering 43 (2005) 951.
- [12] M. Ragulskis, A. Palevicius, L. Ragulskis, International Journal for Numerical Methods in Engineering 56 (2003) 1647.
- [13] M. Naor, A. Shamir, Lecture Notes in Computer Science 950 (1995) 1.
- [14] S.H. Shyu, Pattern Recognition 39 (5) (2006) 866.
- [15] Z. Zhou, G.R. Arce, G. Di Crescenzo, IEEE Transactions on Images Processing 15 (2006) 2441.
- [16] S.H. Shyu, Pattern Recognition 40 (2003) 1014.
- [17] C.M. Hu, W.G. Tzeng, IEEE Transactions on Images Processing 16 (2007) 36.
- [18] S. Cimato, R. De Prisco, A. De Santis, Theoretical Computer Science 374 (2007) 261.
- [19] D.S. Wang, L. Zhang, N. Ma, et al., Pattern Recognition 40 (2007) 2776.
- [20] S.J. Lin, J.C. Lin, Pattern Recognition 40 (2007) 3652.
- [21] S.J. Shyu, S.Y. Huang Y.K. Lee, et al., Pattern Recognition 40 (2007) 3633.
- [22] H.C. Hsu, J. Chen, T.S. Chen, Imaging Science Journal 55 (2007) 175.
- [23] C.N. Yang, T. S Chen, Optical Engineering 46 (2007) 097005.
- [24] C.N. Yang, T.S. Chen, International Journal of Pattern Recognition and Artificial Intelligence 21 (2007) 879.
- [25] W.P. Fang, Pattern Recognition 41 (2008) 1410.