JOURNAL OF APPLIED FUNCTIONAL ANALYSIS,VOL.4,NO.4,611-622,COPYRIGHT 2009 EUDOXUS PRESS,LLC

CONSTRUCTION OF CRYPTOGRAPHIC HASH FUNCTIONS BASED ON TIME AVERAGE CHAOTIC MAP

M. Ragulskis[1], Z. Navickas[2], L. Saunoriene[1], K. Lukoseviciute[1]

1 – Research Group for Mathematical and Numerical Analysis of Dynamical Systems
Kaunas University of Technology
Studentu 50-222, Kaunas LT-51638, Lithuania
2 – Department of Applied Mathematics
Kaunas University of Technology
Studentu 50-325C, Kaunas LT-51638, Lithuania

Abstract. An algorithm for the construction of cryptographic hash function based on optical time average geometric moiré, chaotic dynamics and digital image processing is proposed in this paper. This algorithm is based on the fact that inverse problem for identification of the original grayscale color function from its time averaged image is an ill-posed problem. The problem becomes even more complex if a chaotic map is incorporated into the process of time averaging. The algorithm is designed to cope with any type of digital data and efficiently compresses initial information into a smaller data set.

Keywords: *Chaotic map, Hash function, Time average moiré, Inverse problem.*

1. INTRODUCTION

A hash function is a transformation that takes a digital input and returns a fixed-size string, which is called the hash value. Hash functions with just this property have a variety of general computational uses, but when employed in cryptography, the hash functions are usually chosen to have some additional properties: it must be relatively easy to compute hash values for any given inputs; hash functions must be one-way and collision-free [1, 2]. A hash function is said to be one-way if it is hard to invert, where “hard to invert” means that given a hash value, it is computationally infeasible to find the input. A hash function is said to be collision-free if it is computationally infeasible to find any two different digital inputs which hash values coincide.

We will construct a hash function exploiting physical principles of nonlinear dynamics and chaos embedded into optical digital image time averaging techniques. It must be noted that the considered optical methods are virtual optical methods and all digital algorithms can cope with any type of digital data. Recovery of original grayscale distribution from digital time averaged images is an ill-posed inverse problem. Incorporation of chaotic maps into time averaging makes the inverse problem even more complex. Nevertheless, the complexity of direct calculation of hash values is a straightforward and efficient digital procedure. The object of this paper is to propose an efficient numerical technique for implementation of a new class of hash algorithms.

2. OPTICAL BACKGROUND

Geometric moiré [3, 4] is a classical optical experimental technique based on the analysis of visual patterns produced by superposition of two regular gratings that geometrically interfere. Moiré patterns are used to measure variables such as displacements, rotations, curvature, and strain throughout the viewed area.

Moiré grating on the surface of a one-dimensional structure in the state of equilibrium can be interpreted as a harmonic function [3, 5]:

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

where λ is the pitch of the grating. Such a continuous function is well applicable to digital image processing in virtual computational environments [5]. Numerical value 0 of the function in this equation corresponds to black color; 1 – to white color; all intermediate values – to grayscale color intensity levels. The grating of a one-dimensional structure in a deformed state can be interpreted as follows [6]:

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

where s defines the deflection from the state of equilibrium.

Double exposure geometric moiré techniques can be extended to time average geometric moiré methods when the deflections from the state of equilibrium oscillate in time and long exposure times are used to average the grayscale levels [3]:

$$F(x)=\lim_{T\to\infty}\frac{1}{T}\int_{0}^{T}\left(\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}(x-s\sin(\omega t+\varphi))\right)+\frac{1}{2}\right)dt=\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)J_0\left(\frac{2\pi}{\lambda}s\right)+\frac{1}{2}, \tag{3}$$

where s now is the amplitude of dynamic deflections; ω and φ are the frequency and phase of harmonic oscillations; J_0 is zero order Bessel function of the first kind. Time averaged moiré fringes will form at such amplitudes of dynamic deflections where the argument of the Bessel function in eq. (3) becomes equal to a root of the Bessel function. Thus, an explicit relationship between the pitch of the grating, amplitude of harmonic oscillations and the order of the time averaged fringe takes the following form:

$$s_i=\frac{\lambda}{2\pi}r_i,\ i=1,2,\ldots, \tag{4}$$

where r_i is the i-th root of the zero order Bessel function of the first kind (Fig. 1).

Geometric moiré techniques have a general limitation associated with the fact that the displacements can be determined only in the direction orthogonal to the lines of the grating. Ability to exploit the natural microstructure of the surface as a stochastic grating eliminates this restraint. If the grayscale level of a non-deformable one-dimensional body is $F(x)$, then its time averaged grayscale intensity at a point x_0 is [7]:

$$\lim_{T\to\infty}\frac{1}{T}\int_{0}^{T}F(x_0-s\sin(\omega t+\varphi))dt=\frac{1}{\pi}\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}F(x_0-s\sin t)dt=H_s(F(x)), \tag{5}$$

where H_s is a generalized operator of time averaging [8].

Inverse problems involving geometric moiré are characterized by the fact that the information of interest (e.g. the distribution of grayscale color intensity on the surface of a non-deformable body) is not directly available. The imaging device (the camera) provides measurements of a transformation of this information in the process of time averaging while the body performs harmonic or chaotic oscillations. In practice, these measurements are both incomplete (sampling) and inaccurate (statistical noise) [7]. This means that one must give up recovering the exact image. Indeed, aiming at full recovery of the information usually results in unstable solutions due to the fact that the reconstructed image is very sensitive to inevitable measurement errors. In other words, slightly different data would produce a significantly different image.

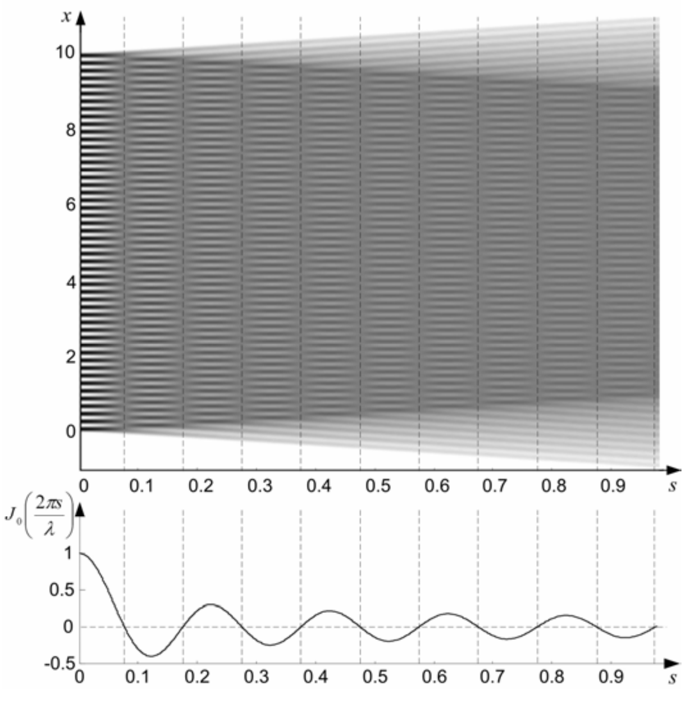

Figure 1. Time averaged moiré fringes produced by harmonic grating ($\lambda = 0.2$) at increasing amplitudes s. The graph of zero order Bessel function of the first kind is shown to illustrate the relationship between the centerlines of the fringes and roots of the Bessel function.

Solution of the inverse problem for identification of $F(x)$, when only time average image is known, is computationally infeasible and this fact is exploited for construction of hard to invert hash function.

3. TIME AVERAGING OF HARMONIC MOIRÉ GRATINGS

It is shown in [9] that it is possible to construct mathematical relationships in operator format between an original grayscale function $F(x)$ and its time average produced by harmonic oscillations around the state of equilibrium. First, function $\widetilde{F}(x) = F(x) - \frac{1}{2}$ is constructed requiring that it must be square integrable and can be expressed in a Fourrier series: $\int_{-\infty}^{+\infty} \left(\widetilde{F}(x)\right)^2 dx < +\infty$; $\widetilde{F}(x) = \sum_{n=-\infty}^{+\infty} c_n \exp\left(i \frac{n\pi}{l} x\right)$; $-l < x < l$; $l > 0$; where $c_n = \frac{1}{2l} \int_{-l}^{l} \widetilde{F}(u) \exp\left(-i \frac{n\pi}{l} u\right) du$.

Then, time averaged image can be expressed in the following form [9]:

$$HF(x) = \Phi^{-1}\left(\hat{p}(sv)\Phi\widetilde{F}(x)\right) + \frac{1}{2}, \tag{6}$$

where $p(x)$ is the distribution of the random variable which defines the displacements from the state of equilibrium during the process of time averaging; $\hat{p}(z)$ is the Fourrier transform of $p(x)$. It is clear that $p(x)$ for harmonic oscillations is an arcsine distribution. As Fourrier transform of arcsine distribution is zero order Bessel function of the first kind, the following equality holds true for harmonic oscillations:

$$H_s F(x) = \Phi^{-1}\left(J_0(sv)\Phi\widetilde{F}(x)\right) + \frac{1}{2}. \tag{7}$$

Time averaging of a grayscale function (one-dimensional image which oscillates harmonically in time) produces grayscale blur. That blur can be characterized as a convolution between the original image (function) and the point spread function which characterizes the distribution of deflections from the state of equilibrium in time.

Equation 7 is an important result which shows that the inverse problem of reconstruction of the original grayscale function is an ill-posed inverse problem.

Zero order Bessel function of the first kind has multiple roots (Fig. 1). Therefore there exists multiple divisions by zero in the kernel of the inverse problem (Eq. 7) what makes this inverse problem ill-posed. This property is illustrated by Fig. 1 where a number of time averaged interference fringes can be observed at increasing amplitude *s*.

4. DESCRIPTION OF THE ALGORITHM FOR CONSTRUCTION OF CRYPTOGRAPHIC HASH FUNCTION

The algorithm for construction of the one-dimensional hash function comprises three basic parts:

1. Acquisition of input data: amplitude *s* and grayscale function *F*(*x*).
2. Production of the intermediate result: $H_s F(x)$.
3. Delivery of output data: time averaged grayscale function stretched to min-max levels.

There three basic parts are graphically illustrated in Fig. 2. The original grayscale function *F*(*x*) is constructed as a set of random numbers evenly distributed in interval $[0,1]$. We plot the values of $H_s F(x)$ produced by harmonic oscillations at increasing *s* as *s* sweeps from 0 to 2. One can observe grayscale riddles in the upper and lower part of the digital image in Fig. 2(a) (similar to the riddles above and below time averaged fringes in Fig. 1). The hash value of the constructed hash function is the middle part of time averaged image (riddles are disregarded). Such approach enables to realize the compression of the original data into a smaller set what is a standard feature of existing hash functions. Finally, time averaged grayscale levels are stretched to min-max level range what eliminates even theoretical possibility to reconstruct the original *F*(*x*) from its time averaged image.

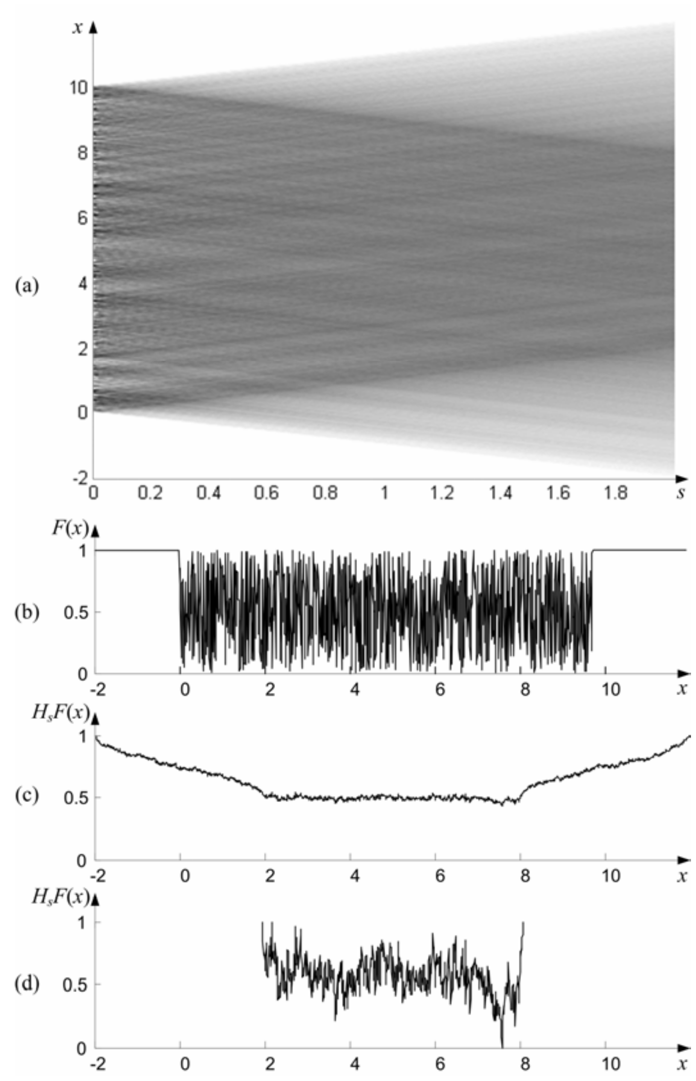

Figure 2. Graphical illustration of the three basic parts of the cryptographic algorithm: (a) $H_sF(x)$ at increasing amplitudes *s*; (b) original grayscale function as a set of random numbers evenly distributed in interval $[0,1]$; (c) grayscale levels at $s = 2$; (d) time averaged grayscale function stretched to min-max levels ($s = 2$).

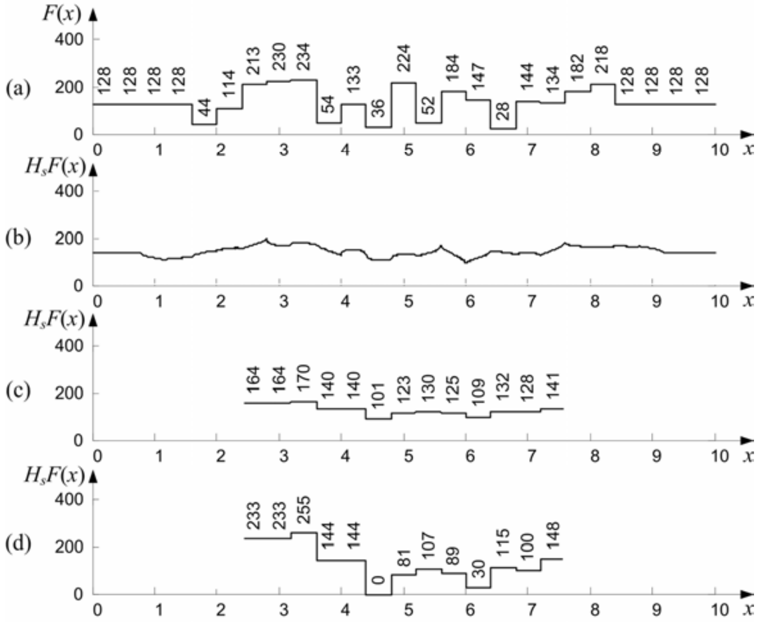

Figure 3. Illustration of the algorithm (harmonic motion): (a) original grayscale distribution (width of the virtual pixels is 0.4); (b) time averaged grayscale at s=0.8; (c) time averaged levels reconstructed at appropriate locations of virtual pixels; (d) hash value stretched to min-max levels.

As mentioned earlier, functionality of the proposed cryptographic hash function enables processing of any kind of data – not necessarily digital grayscale images. That fact is illustrated in Fig. 3 where an input set of natural numbers (Fig. 3(a)) is transformed to the output set (Fig. 3(d)); vertical integers denote virtual grayscale levels.

5. ALGORITHM FOR CONSTRUCTION OF HASH FUNCTION BASED ON THE CHAOTIC MAP

The theoretical result in eq. (6) enables use of any type of time function determining dynamic deflections from the state of equilibrium. As mentioned previously, the complexity of the problem would not decrease only if $\hat{p}(z)$ is not a trivial function (what may happen if the motion law is uni-directional motion with constant velocity). Thus we incorporate state variable defining some sort of chaotic motion assuming that it describes dynamic deflection from the state of equilibrium.

The general structure of such a modified algorithm for construction of the two-dimensional hash function is illustrated in a schematic diagram in Fig. 4. Computations required to transform the digital input into a hash value are based on chaotic dynamics, geometric optics, and digital image processing. Data base holds a collection of virtual grayscale one-dimensional images which are represented as arrays of integers. Every integer must fit into grayscale range between 0 and 255. Control parameter is used to tune the shape of chaotic attractor. Preconditioning is required to fit the amplitudes of virtual dynamic deflections to a realistic computational scenario, what can be interpreted as an additional security parameter. Other steps in Fig. 4 are discussed in the previous Sections.

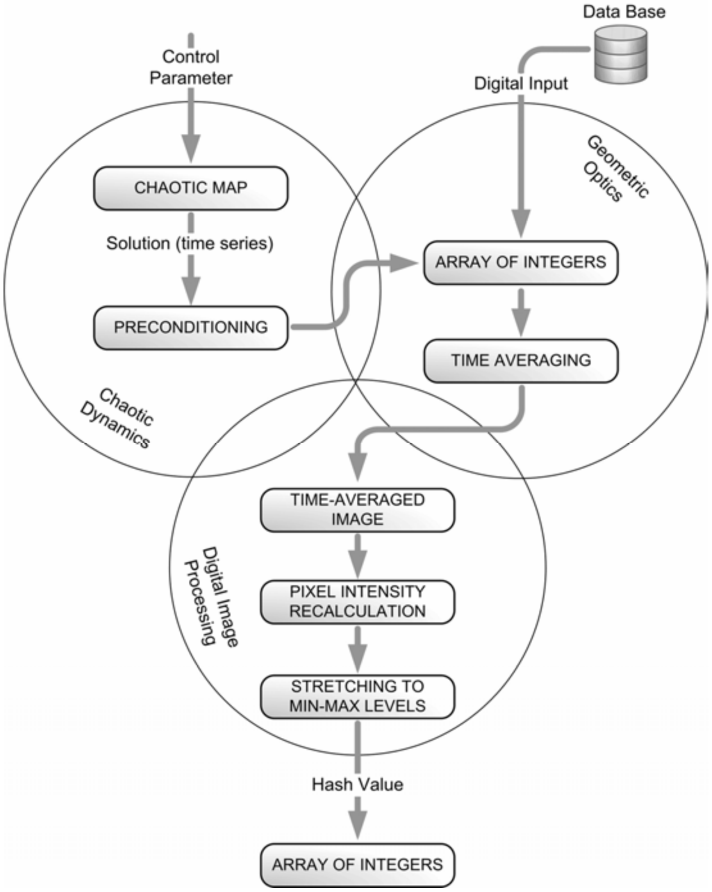

Figure 4. Schematic graphical representation of the algorithm for the construction of hash function.

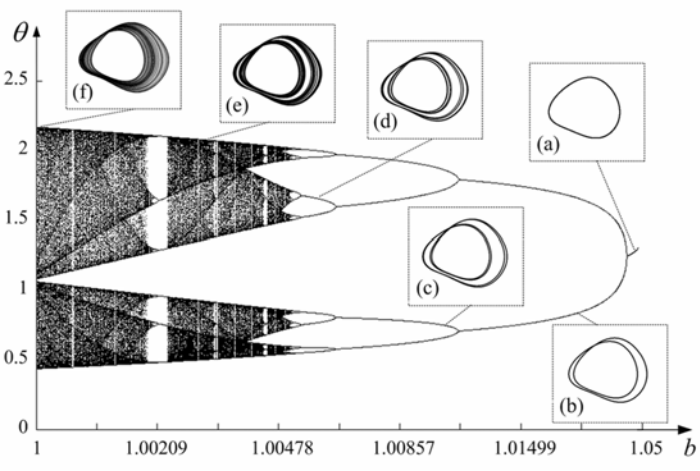

Figure 5. Bifurcation diagram for the driven damped nonlinear pendulum with parameter values *ω*=2/3; *a*=2.048, with respect to the variation of the damping coefficient *b*. The insets show phase space diagrams with orbits corresponding to specific values of the parameters

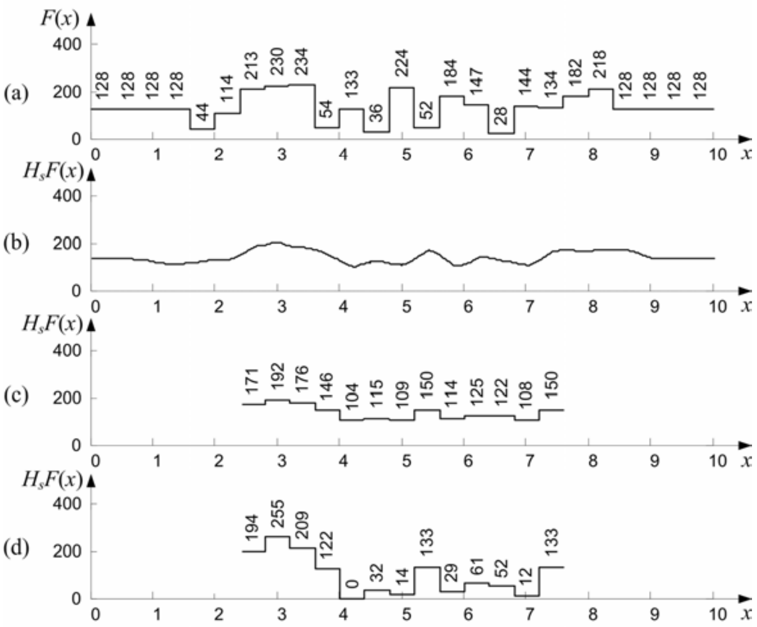

Figure 6. Illustration of the algorithm (chaotic motion): (a) original grayscale distribution (width of virtual pixels is 0.4); (b) time averaged grayscale distribution produced by chaotic oscillations; (c) time averaged grayscale distribution averaged at appropriate virtual pixels; (d) hash value stretched to min-max levels

As mentioned previously, we use a chaotic map for the construction of hash algorithm. We consider a nonlinear periodically driven damped pendulum, which is a paradigm model in the study of nonlinear dynamics. A dimensionless time evolution equation of such pendulum reads [10]:

$$\frac{d^2\theta}{dt^2} = -\sin\theta - b\frac{d\theta}{dt} + a\cos(\omega t), \tag{8}$$

where b is the damping coefficient; a is external forcing amplitude; and ω is the frequency. The driven damped pendulum with ω=2/3, b=1.0, and a=2.048 yields chaotic behavior following a period-doubling sequence of bifurcations (Fig. 5).

Phase trajectories in the insets of Fig. 5 are plotted in frames $(\theta;\dot{\theta})$ at the following values of b: (a) b=1.04; (b) b=1.025; (c) b=1.01; (d) b=1.0055; (e) b=1.003; (f) b=1.0002. Parameter b is varied following the rule $b_i = 1.05 - \frac{0.05}{\ln 201}\ln\left(1 + \frac{1000 - i + 1}{5}\right)$, i=1, ..., 1001, what helps to expand the cascade of period-doubling bifurcations.

We use parameter value b=1.0002 for construction dynamic deflections which are used for time averaging of original grayscale function (Fig. 6(b)). Hash value is produced when the averaged grayscale levels are fitted to virtual pixels (Fig. 6(c)) and stretched to min-max levels (Fig. 6(d)).

6. CONCLUSIONS

A new class of hash functions is proposed in this paper. Chaotic map is incorporated into the process of virtual time averaging. Though the inverse problem is ill posed, algorithm for calculation of hash values is efficient and straightforward. Calculations are based on the principles of virtual geometric optics, nonlinear dynamics and digital image processing. Such an approach builds prerequisites of wide potential application of the proposed hash functions.

REFERENCES

[1] Bicakci K., Tsudik G., Tung B., (2003), "How to Construct Optimal One-time Signatures", *Computer Networks*, 43, 339-349.

[2] Xiao D., Liao X., Deng S., (2005), "One-way Hash Function Construction Based on the Chaotic Map with Changeable-parameter", *Chaos, Solitons & Fractals*, 24, 65-71.

[3] Kobayashi A. S., (1993), *Handbook on Experimental Mechanics 2nd ed.*, Bethel, SEM.

[4] Post D., Han B., Ifju P., (1997), *High Sensitivity Moiré: Experimental Analysis for Mechanics and Materials,* Berlin, Springer-Verlag.

[5] Ragulskis M., Palevicius A., Ragulskis L., (2003), "Plotting Holographic Interferograms for Visualization of Dynamic Results from Finite-Element Calculations", *International Journal of Numerical Methods in Engineering*, 56, 1647-1659.

[6] Ragulskis M., Ragulskis L., Maskeliunas R., (2003), "Applicability of Time Average Geometric Moiré for Vibrating Elastic Structures", *Experimental Techniques*, 28, 27-30.

[7] Ragulskis M., Maskeliunas R., Saunoriene L., (2005), "Identification of In-plane vibrations Using Time Average Stochastic Moiré", *Experimental Techniques*, 29, 41-45.

[8] Ragulskis M., Navickas Z., (2007), "Hash Function Construction Based on Time Average Moiré", *Discrete and Continuous Dynamical Systems-Series B*, *American Institute of Mathematical Sciences*, 8, 1007-1020.

[9] Navickas Z., Ragulskis M., (2007), "Representation of the Time-averaged Vibrating Images in the Operator Format", *Journal of Vibroengineering*, 9, 1-8.

[10] Hilborn R. C. (2000), *Chaos and Nonlinear Dynamics,* Norfolk, Oxford University Press.