DISCRETE AND CONTINUOUS
DYNAMICAL SYSTEMS–SERIES B
Volume **8**, Number **4**, November **2007**

Website: http://AIMsciences.org

pp. **1007-1020**

HASH FUNCTION CONSTRUCTION BASED ON TIME AVERAGE MOIRÉ

Minvydas Ragulskis

Faculty of Fundamental Sciences, Kaunas University of Technology
Kaunas, LT-51368 Lithuania

Zenonas Navickas

Faculty of Fundamental Sciences, Kaunas University of Technology
Kaunas, LT-51368 Lithuania

(Communicated by Miguel Sanjuan)

Abstract. An algorithm for the construction of Hash function based on optical time average moiré experimental technique is proposed in this paper. Algebraic structures of grayscale color functions and time average operators are constructed. Properties of time average operators and effects of digital image representation are explored. The fact that the inverse problem of identification of the original grayscale color function from its time averaged image is an ill-posed problem helps to construct an efficient algorithm for the construction of a new class of one-way collision free hash functions.

1. **Introduction.** Currently there are no technically mature techniques that provide the security service of non-repudiation in an open network environment, in the absence of trusted third parties, other than digital signature-based techniques [1]. A digital signature is formed by applying a mathematical function to the electronic document [5]. The recipient of the transmitted document decrypts the message digest with the originators public key, applies the same message hash function to the document, then compares the resulting digest with the transmitted version. If they are identical, then the recipient is assured that the message is unaltered and the identity of the signer is proven.

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 [2], [15]. 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 optical digital image time averaging techniques.

2000 *Mathematics Subject Classification.* Primary: 78A05; Secondary: 94A08.
Key words and phrases. time average moiré, hash function, algebraic structure.

2. **Optical Background.** Geometric moiré [7], [9] is a classical 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, radial lines [4], [14], [8]. The gratings can be superposed by double exposure photography, by reflection, by shadowing, or by direct contact [3], [6]. Moiré patterns are used to measure variables such as displacements, rotations, curvature, and strain throughout the viewed area.

Double exposure geometric moiré techniques can be extended to time average geometric moir methods. Moiré grating is formed on the surface of elastic oscillating structure and time averaging techniques are used for the formation of patterns of fringes [11]. Dynamic displacements can be estimated from the time average fringes, whereas the fringe order no longer represents the displacement by an integer number of pitches; the intensity of the time averaged moiré pattern is governed by mathematical relationships comprising zero order Bessel function of the first kind [12].

Moiré grating on the surface of a one-dimensional structure in the state of equilibrium can be interpreted as a harmonic function [7], [10]:

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

where λ is the pitch of the grating. Such a continuous function is well applicable to digital image processing in virtual computational environments [10]. 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 [11]:

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

where s defines the displacement from the state of equilibrium at a point x. Time averaging technique can be applied for the analysis of dynamic displacements of vibrating elastic one-dimensional structure. Then the carrier fringes are contrast modulated and the color intensity of the time average geometric moir image can be described by the following relationship [12]:

$$\begin{aligned} F(x) &= \lim_{T\to\infty}\frac{1}{T}\int_0^T \cos^2\left(\frac{\pi}{\lambda}(x - s\sin(\omega t - \varphi))\right) dt \\ &= \frac{1}{2} + \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right) J_0\left(\frac{2\pi}{\lambda}s\right) \end{aligned} \tag{3}$$

where T is time of exposure; ω and φ are angular frequency and phase of structural vibrations around the state of equilibrium; J_0 is zero order Bessel function of the first kind. It can be noted that s now defines not static displacement, but the amplitude of dynamic displacement. Also, neither the angular frequency nor the phase has any effect on the formation of moiré fringes.

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 color intensity of a non-deformable one-dimensional body is $F(x)$, then its time averaged grayscale

intensity at a point x_0 is [13]:

$$\begin{aligned}\lim_{T\to\infty}\frac{1}{T}\int_0^T F(x_0 - s\sin(\omega t+\varphi))dt &= \frac{1}{\pi}\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} F(x_0 - s\sin t)dt \\ &= \lim_{m\to\infty}\frac{1}{2m}\sum_{k=-m}^{m-1} F\left(x_0 - s\sin\left(\frac{\pi k}{2m}\right)\right)\end{aligned} \tag{4}$$

where s is the amplitude of harmonic oscillations of a non-deformable body. Technique for identification of parameters of in-plane vibrations presented in [13] is based on digital image processing and can be effectively exploited for the analysis of vibrating microstructures when the surface color in the steady state $F(x)$ is known.

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 oscillates harmonically. In practice, these measurements are both incomplete (sampling) and inaccurate (statistical noise) [13]. 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. In order to cope with these difficulties, the reconstructed image is usually defined as the solution of an optimization problem. Solution of the inverse problem for identification of $F(x)$, when time average image is known, is computationally infeasible and this fact is the object of this paper.

3. **Algebraic Structure of Grayscale Functions.**

Definition 3.1. Function $f(x)$ belongs to set Φ if:

(i) $f(x)$ is defined for all $x \in R$.
(ii) $f(x)$ has only a finite number of discontinuity points.
(iii) $0 \le f(x) \le 1$ for all $x \in R$.

Then the following functions can be constructed:

(i) $\hat{f}^{(+)}(x) := \left(f(x) - \frac{1}{2}\right)\mathrm{I}\left(f(x) - \frac{1}{2}\right)$
(ii) $\hat{f}^{(-)}(x) := \left(f(x) - \frac{1}{2}\right)\mathrm{I}\left(\frac{1}{2} - f(x)\right)$
(iii) $\hat{f}(x) := \hat{f}^{(+)}(x) + \hat{f}^{(-)}(x)$
(iv) $f^{(+)}(x) := \hat{f}^{(+)}(x) + \frac{1}{2}$
(v) $f^{(-)}(x) := \hat{f}^{(-)}(x) + \frac{1}{2}$

where $\mathrm{I}(x) := \begin{cases} 0, \text{ when } x < 0 \\ 1, \text{ when } x \ge 0 \end{cases}$ is Heaviside step function. It is clear that

$$f(x) = \hat{f}(x) + \frac{1}{2} \tag{5}$$

Definition 3.2. Function $f(x)$ is a grayscale function if:

(i) $F(x) \in \{\Phi\}$
(ii) $0 \le \int_{-\infty}^{+\infty} \hat{F}^{(+)}(x)dx < +\infty$ and $-\infty \le \int_{-\infty}^{+\infty} \hat{F}^{(-)}(x)dx < 0$
(iii) Var $F(x) < +\infty$

Requirements in part (ii) of Definition 3.2 are stronger than $\int_{-\infty}^{+\infty} \left|F(x) - \frac{1}{2}\right| dx < +\infty$, which can hold true even if both integrals in (ii) diverge.

Corollary 3.1. *The following limits hold true for grayscale functions:*

$$\lim_{x\to-\infty} F(x) = \lim_{x\to+\infty} F(x) = \frac{1}{2}$$

.

If 0 corresponds to black color and 1 corresponds to white color, the "background" color at infinity is gray.

The set of all grayscale functions is denoted by Γ. It is clear that $\Gamma \subset \Phi$.

Definition 3.3. Seminorm of a grayscale function is defined as follows:

$$\| F(x) \| = \int_{-\infty}^{+\infty} \left|F(x) - \frac{1}{2}\right| dx \tag{6}$$

We will explain why $\| F(x) \|$ is a seminorm but not a norm after we introduce algebraic structure of time average operators. It can be noted that

$$\| F(x) \| = \int_{-\infty}^{+\infty} \hat{F}^{(+)}(x)dx - \int_{-\infty}^{+\infty} \hat{F}^{(-)}(x)dx < +\infty$$

if $F(x) \in \Gamma$.

Definition 3.4. Function $O(x) := \frac{1}{2}$, for all $x \in R$, is called a zero function.

It is clear that $O(x) \in \Gamma$.

Definition 3.5. Every function $F(x) \in \Gamma$ has the opposite function $\overline{F}(x)$ which is defined as:

$$\overline{F}(x) := 1 - F(x). \tag{7}$$

It is clear that $\overline{F}(x) \in \Gamma$; $\overline{O}(x) = O(x)$; $\overline{\overline{F}}(x) = F(x)$;

Definition 3.6. Arithmetic mean operator is defined for a finite set of grayscale functions $F_1(x), \ldots, F_n(x)$, $n \geq 1$:

$$[F_1(x), F_2(x), \ldots, F_n(x)]_n := \frac{1}{n} \sum_{k=1}^{n} F_k(x). \tag{8}$$

Corollary 3.2. *For all $n \in \mathrm{N}$, and $F_1(x), F_2(x), \ldots, F_n(x) \in \Gamma$ the following statements hold true:*

(i) $[F_1(x), F_2(x), \ldots, F_n(x)]_n \in \Gamma$.

(ii) permutation of grayscale functions (in the square brackets) has no effect on the resulting arithmetic mean.

(iii) $[F(x), F(x), \ldots, F(x)]_n = F(x)$.

(iv) $\lfloor F(x), \overline{F}(x) \rfloor_2 = O(x)$.

(v) $\overline{[F_1(x), \ldots, F_n(x)]_n} = \lfloor \overline{F_1}(x), \ldots, \overline{F_n}(x) \rfloor_n$.

Definition 3.7. The set of real numbers $\alpha \in [-1; 1]$ is marked as $\mathrm{S} = [-1; 1]$.

Definition 3.8. Let $\alpha \in \mathrm{S}$ and $F(x) \in \Gamma$. The product of the grayscale function $F(x)$ by the scalar α is denoted by $\alpha \otimes F(x)$ and is defined as:

$$\alpha \otimes F(x) := \alpha \left(F(x) - \frac{1}{2}\right) + \frac{1}{2}. \tag{9}$$

Corollary 3.3. *The following statements are true for all* $\alpha \in \mathrm{S}$ *and* $F(x) \in \Gamma$*:*
(i) $\alpha \otimes F(x) \in \Gamma$.
(ii) $1 \otimes F(x) = F(x)$; $0 \otimes F(x) = O(x)$; $-1 \otimes F(x) = \overline{F}(x)$.
(iii) $\alpha \otimes O(x) = O(x)$.

Lemma 3.9. *Let* $\alpha_1, \alpha_2 \in \mathrm{S}$ *and* $F(x) \in \Gamma$. *Then* $\alpha_1 \otimes (\alpha_2 \otimes F(x)) = (\alpha_1 \alpha_2) \otimes F(x)$.

Proof.

$$\alpha_1 \otimes (\alpha_2 \otimes F(x)) = \alpha_1 \otimes \left(\alpha_2 F(x) + \frac{1-\alpha_2}{2} \right)$$
$$= \alpha_1 \alpha_2 F(x) + \alpha_1 \frac{1-\alpha_2}{2} + \frac{1-\alpha_1}{2} = \alpha_1 \alpha_2 \left(F(x) - \frac{1}{2} \right) + \frac{1}{2}.$$

□

It is clear that $\alpha_1 \otimes (\alpha_2 \otimes F(x)) = \alpha_2 \otimes (\alpha_1 \otimes F(x))$.

Corollary 3.4. *Let* $\alpha\alpha_1, \ldots, \alpha_n \in \mathrm{S}$ *and* $F_1(x), \ldots, F_n(x) \in \Gamma$. *Then the following statements hold true for all* $n \in \mathrm{N}$*:*
(i) $\alpha_1 \otimes [F_1(x), \ldots, F_n(x)]_n = [\alpha_1 \otimes F_1(x), \ldots, \alpha_1 \otimes F_n(x)]_n$.
(ii) $[\alpha_1 \otimes F(x), \ldots, \alpha_1 \otimes F(x)]_n = \left(\frac{1}{n} \sum_{k=1}^{n} \alpha_k \right) \otimes F(x)$; $\left(\frac{1}{n} \sum_{k=1}^{n} \alpha_k \in S \right)$.

Corollary 3.5. *Seminorm of a grayscale function possesses the following properties:*
(i) $\| F \| = 0$ *if and only if* $F(x) = O(x)$.
(ii) $\| F \| = 2 \| [O(x), F(x)]_2 \|$ *since*

$$2 \| [O(x), F(x)]_2 \| = 2 \int_{-\infty}^{+\infty} \left| \frac{\frac{1}{2} + F(x)}{2} - \frac{1}{2} \right| dx = \int_{-\infty}^{+\infty} \left| F(x) - \frac{1}{2} \right| dx = \| F \|.$$

(iii) $\| F \| = \| \overline{F} \|$ *since* $\int_{-\infty}^{+\infty} \left| F(x) - \frac{1}{2} \right| dx = \int_{-\infty}^{+\infty} \left| \frac{1}{2} - F(x) \right| dx$.
(iv) $\| [F_1(x), \overline{F_2}(x)]_2 \| = \| [F_2(x), \overline{F_1}(x)]_2 \|$.
(v) $\| a \otimes F(x) \| = |a| \cdot \| F(x) \|$, *since* $\int_{-\infty}^{+\infty} \left| \left(a \left(F(x) - \frac{1}{2} \right) + \frac{1}{2} \right) - \frac{1}{2} dx \right| =$
$|a| \int_{-\infty}^{+\infty} \left| F(x) - \frac{1}{2} \right| dx$.

Definition 3.10. Distance between any two grayscale functions $F_1(x)$ and $F_2(x)$ is defined as follows:

$$\rho(F_1, F_2) = \| [F_1(x), \overline{F_2}(x)]_2 \| . \tag{10}$$

Definition 3.10 is correct because:
(i) $\rho(F_1, F_2)$ is a distance because $\rho(F, F) = 0$; $\rho(F_1, F_2) = \rho(F_2, F_1) \geq 0$; $\rho(F_1, F_2) = 0$ implies $F_1(x) = F_2(x)$; and the triangle inequality is in force:

$\rho(F_1, F_3) \le \rho(F_1, F_2) + \rho(F_2, F_3)$. Really,

$$\begin{aligned}
&\rho(F_1, F_2) + \rho(F_2, F_3) \\
=&\int_{-\infty}^{+\infty} \left| \frac{F_1 - F_2 + 1}{2} - \frac{1}{2} \right| dx + \int_{-\infty}^{+\infty} \left| \frac{F_2 - F_3 + 1}{2} - \frac{1}{2} \right| dx \\
=&\frac{1}{2} \int_{-\infty}^{+\infty} \left(|F_1 - F_2| + |F_2 - F_3| \right) dx \ge \frac{1}{2} \int_{-\infty}^{+\infty} |F_1 - F_2 + F_2 - F_3| \, dx \\
=&\frac{1}{2} \int_{-\infty}^{+\infty} |F_1 - F_3| \, dx = \int_{-\infty}^{+\infty} \left| \frac{F_1 - F_3 + 1}{2} - \frac{1}{2} \right| dx = \rho(F_1, F_3)
\end{aligned}$$

(ii) $\rho(F_1, F_2) \le \frac{1}{2} \left(\| F_1 \| + \| F_2 \| \right)$. From Corollary 3.5 (ii) it follows that $\| F \| = 2\rho(O, F)$. Thus, $\rho(F_1, F_2) \le \rho(F_1, O) + \rho(O, F_2) = \frac{1}{2}(\| F_1 \| + \| F_2 \|)$.

Definition 3.11. The set of grayscale functions Γ together with the operation of arithmetic mean $[F_1(x), \dots, F_n(x)]_n$ and operation of scalar multiplication $\alpha \otimes F(x)$ forms an algebraic structure of grayscale functions and is denoted by $< \Gamma; [\dots]]_n | S; \otimes >$.

It can be noted that $< \Gamma; [\dots]]_n | S; \otimes >$ is the generalization of a linear functional space where the summation is replaced with the operation of arithmetic mean and the multiplication by a scalar is replaced with the generalized operation of multiplication $\otimes$.

4. Algebraic Structure of Time Average Operators.

Definition 4.1. Time average operator H_s is defined as:

$$H_s(F(x)) := \frac{1}{\pi} \int_{-\frac{\pi}{2}}^{+\frac{\pi}{2}} F(x - s \sin t) dt, \tag{11}$$

for all $F(x) \in \Phi$ and $s \ge 0$, $s \in R$; where t is time and s is the amplitude of harmonic oscillations.

Corollary 4.1. *(i) $H_s(F(x)) \in \Gamma$, since $0 \le H_s(F(x)) \le \frac{1}{\pi} \int_{-\frac{\pi}{2}}^{+\frac{\pi}{2}} 1 dt = 1$, for $0 \le F(x) \le 1$.*
(ii) $H_s(F(x))$ is a continuous function (in terms of x), for $s > 0$.
(iii) $H_s(O(x)) = O(x)$.
(iv) $H_0(F(x)) = F(x)$.
(v) $\lim_{s \to \infty} H_s(F(x)) = O(x)$.

Definition 4.2. Operator I (unitary operator) and operator O (zero operator) are operators satisfying the following identities: $\mathrm{I}(F(x)) = F(x)$ and $\mathrm{O}(F(x)) = O(x)$.

It is clear that $\mathrm{I} = H_0$; $\mathrm{O} = \lim_{s \to \infty} H_s$.

Corollary 4.2. *(Multiplication of an operator by a scalar) $H_s(\alpha \otimes F(x)) = \alpha \otimes (H_s(F(x)))$, for all $\alpha \in S$, $s \ge 0$ and $F(x) \in \Gamma$.*

Proof.

$$\begin{aligned}
H_s(\alpha \otimes F(x)) &= \frac{1}{\pi} \int_{-\frac{\pi}{2}}^{+\frac{\pi}{2}} \left(\alpha F(x - s \sin t) + \frac{1 - \alpha}{2} \right) dt \\
&= \alpha \left(\frac{1}{\pi} \int_{-\frac{\pi}{2}}^{+\frac{\pi}{2}} F(x - s \sin t) dt \right) + \frac{1 - \alpha}{2} = \alpha \otimes (H_s(F(x))).
\end{aligned}$$

□

Corollary 4.3. $H_s([\alpha_1 \otimes F_1(x), \ldots, \alpha_n \otimes F_n(x)]_n) = [\alpha_1 \otimes (H_s(F_1(x))), \ldots, \alpha_n \otimes (H_s(F_n(x)))]_n$, *for all* $n \in N$, $s \geq 0$, $\alpha_1, \ldots, \alpha_n \in S$ *and* $F_1(x), \ldots, F_n(x) \in \Gamma$.

Definition 4.3. Superposition of time averaging operators H_{s_1} and H_{s_2} is defined as:

$$H_{s_1} \cdot H_{s_2}(F(x)) = H_{s_1}(H_{s_2}(F(x))), \tag{12}$$

for all $s_1, s_2 \geq 0$ and $F(x) \in \Gamma$.

Corollary 4.4. *The following relationships hold true, for all* $s_1, s_2, s_3 \geq 0$ *and* $F(x) \in \Gamma$*:*

(i) $H_{s_1} \cdot H_{s_2}(F(x)) = \dfrac{1}{\pi^2} \displaystyle\int_{-\frac{\pi}{2}}^{+\frac{\pi}{2}} \int_{-\frac{\pi}{2}}^{+\frac{\pi}{2}} F(x - s_1 \sin u - s_2 \sin v) du dv.$

(ii) $H_{s_1} \cdot H_{s_2} = H_{s_2} \cdot H_{s_1}$.

(iii) $H_{s_1} \cdot (H_{s_2} \cdot H_{s_3}) = (H_{s_1} \cdot (H_{s_2}) \cdot H_{s_3}$.

Lets define an operator $H_{s_1} \cdot H_{s_2} \cdot \cdots \cdot H_{s_n}$ for any $n \in N$ and$s_1, \ldots, s_n \geq 0$. Lets denote the set of such operators by $\mathbf{H}$. In other words, we construct an algebraic structure of time averaging operators $< \mathbf{H}; \cdot | \mathbf{S}; \otimes >$. Every operator $H \in \mathbf{H}$ maps the structure of grayscale functions into itself: $H :< \Gamma; [\ldots]_n | \mathbf{S}; \otimes > \rightarrow < \Gamma; [\ldots]_n | \mathbf{S}; \otimes >$. In general, the relationship between the algebraic structure of operators and the algebraic structure of grayscale functions can be expressed as:

$$< \mathbf{H}; \cdot | \mathbf{S}; \otimes > :< \Gamma; [\ldots]_n | \mathbf{S}; \otimes > \rightarrow < \Gamma; [\ldots]_n | \mathbf{S}; \otimes > . \tag{13}$$

5. **Properties and Examples.**

Example 5.1. Several grayscale functions and corresponding grayscale images are presented in Fig. 1. This is to demonstrate that $\lfloor H_s(F(x)), H_s(\overline{F}(x)) \rfloor_2 = O(x)$.

Example 5.2. Grayscale intensity functions produced by repetitive time averaging are presented in Fig. 2. Operator H_s acts over a grayscale function producing a new grayscale function $H_s(F(x))$. Then the same operator (with the same amplitude s) acts again over the newly produced grayscale function producing $H_s(H_s(F(x)))$. The process is iterated for 25 times (different figures correspond to different amplitudes s). The rectangular shape of the initial grayscale function is selected for clearness. This is to demonstrate that $H_{s_1} \cdot H_{s_2} \neq H_{s_1+s_2}$.

Theorem 5.1. *Whatever* $s \geq 0$, $\| H_s(F^{(+)}(x)) \| = \| F^{(+)}(x) \|$ *and* $\| H_s(F^{(-)}(x)) \| = \| F^{(-)}(x) \|$.

Proof. Whatever $s \geq 0$

$$\begin{aligned} \| H_s(F^{(+)}(x)) \| &= \int_{-\infty}^{+\infty} \left| \frac{1}{\pi} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} F^{(+)}(x - s \sin t) dt - \frac{1}{2} \right| dx \\ &= \int_{-\infty}^{+\infty} \left(\frac{1}{\pi} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \left(F^{(+)}(x - s \sin t) - \frac{1}{2} \right) dt \right) dx. \end{aligned}$$

On the other hand,

$$\begin{aligned} \| H_s(F^{(+)}(x)) \| &= \frac{1}{\pi} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \left(\int_{-\infty}^{+\infty} \left(F^{(+)}(x - s \sin t) - \frac{1}{2} \right) dx \right) dt \\ &= \int_{-\infty}^{+\infty} \left(F^{(+)}(x) - \frac{1}{2} \right) dx = \| F^{(+)}(x) \| . \end{aligned}$$

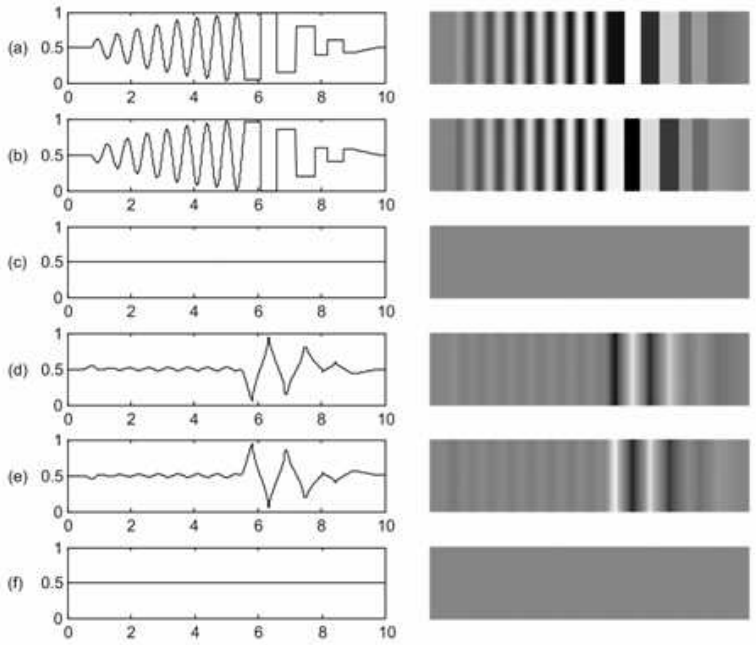

FIGURE 1. Grayscale functions and corresponding images: a) $F(x)$; b) $\overline{F}(x)$; c) $\lfloor F(x), \overline{F}(x) \rfloor_2$; d) $H_{1.5}(F(x))$; e) $H_{1.5}(\overline{F}(x))$; f) $\lfloor H_{1.5}(F(x)), H_{1.5}(\overline{F}(x)) \rfloor_2$

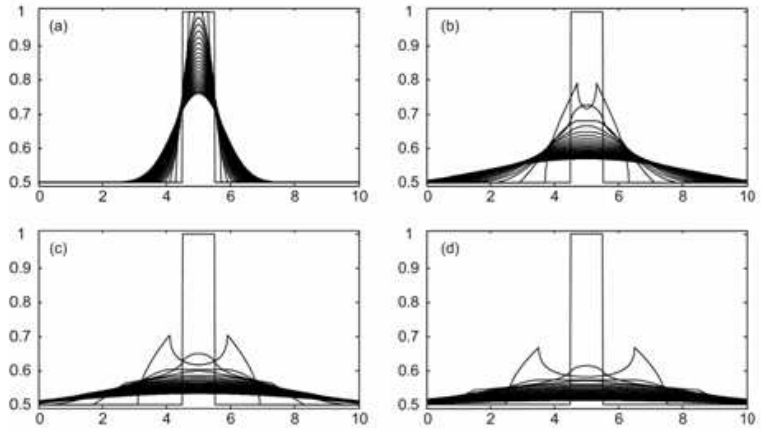

FIGURE 2. Grayscale functions produced by repetitive time averaging: a) $s = 0.2$; b) $s = 0.8$; c) $s = 1.4$; d) $s = 2.0$.

The second part of the theorem can be proved analogously. □

Now we are ready to explain why $\| F(x) \|$ is defined as a seminorm, not a norm (Definition 3.3). Let $F(x) \in \Gamma$, $\frac{1}{2} \leq F(x) \leq 1$ for all x, and $\| F(x) \| = \alpha$,

$0 < \alpha \leq +\infty$. Then, from Theorem 5.1, $\| H_sF(x) \| = \alpha$. But, from Corollary 4.1(v), $\| \lim\limits_{s\to+\infty} H_sF(x) \| = \| O(x) \| = 0$. Thus, $\lim\limits_{s\to+\infty} \| H_sF(x) \| \neq \| \lim\limits_{s\to+\infty} H_sF(x) \|$.

Corollary 5.1. *The following inequalities hold true:*

$$\begin{aligned} \| \| H_s(F^{(+)}(x)) \| - \| H_sF^{(-)}(x) \| \| \leq & \| H_sF(x) \| \\ \leq & \| H_s(F^{(+)}(x)) \| + \| H_s(F^{(-)}(x)) \|; \end{aligned} \tag{14}$$

$$\| H_{s_1+s_2}F(x) \| \leq \| H_{s_1}F(x) \|, s, s_1, s_2 \geq 0. \tag{15}$$

Theorem 5.1 provides insight into the process of time averaging and focuses on the quantity of grayscale color ("paint") on a surface. The paint is classified into "white paint" $F^{(+)}(x)$ (grayscale color intensity from 0.5 up to 1) and "black paint" $F^{(-)}(x)$ (from 0 up to 0.5). The quantity of pure paint is invariant – would the surface oscillate or not. But it turns out that if one zone of the surface is coated with "black paint" and another with "white paint", the time averaged image will not preserve the quantities of black and white paints invariant. Different paints will annihilate each other at appropriate rate which is dependent on the paint distribution and the amplitude s.

Example 5.3. The effect of annihilation is illustrated by eq. (3) and Fig. 3 – when $\frac{2\pi}{\lambda}s$ is equal to a root of zero order Bessel function of the first kind, grayscale color intensity becomes equal to 0.5. It can be noted that $\frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right) + \frac{1}{2}$ is an element of set Φ, but does not belong to set Γ. Instead, we operate with $F_0(x) = \begin{cases} \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right) + \frac{1}{2}, \text{ when } 1 \leq x \leq 9 \\ 0.5, \text{ otherwise} \end{cases}$; $F_0(x) \in \Gamma$. The effect of color annihilation can be observed at the centers of time averaged interference fringes. Nevertheless, $H_{s_i}F_0(x) \neq O(x)$ as time averaged riddles are formed around interval endpoints; where $s_i = \frac{\lambda}{2\pi}r_i$, $i = 1, 2, \ldots$ and r_i is the i-th root of zero order Bessel function of the first type.

Definition 5.2. Grayscale function $F(x)$ is not vanishing if $\| H_sF(x) \|$ for all $0 \leq s < +\infty$.

Corollary 5.2. *If $F(x) \in \Gamma$ then $F^{(+)}(x)$ and $F^{(-)}(x)$ are not vanishing.*

The proof follows from Definition 3.2 (ii), Definition 3.1 (iv) and (v) and Theorem 5.1.

Corollary 5.3. *Grayscale function $F(x)$ is not vanishing if $\| F^{(+)}(x) \| \neq \| F^{(-)}(x) \|$.*

The proof follows from inequalities $0 < \| \| H_sF^{(+)}(x) \| - \| H_sF^{(-)}(x) \| \| \leq \| H_sF(x) \| < +\infty$.

Definition 5.3. Grayscale functions $F_1(x)$ and $F_2(x)$ are no coincident if $0 < \rho(H_sF_1(x), H_sF_2(x)) < +\infty$ for any $0 \leq s < +\infty$.

Theorem 5.4. *Grayscale functions $F_1(x)$ and $F_2(x)$ are no coincident if and only if $\lfloor F_1(x), \overline{F}_2(x) \rfloor_2$ is not vanishing.*

Proof. From Corollary 4.3, $H_s\lfloor F_1(x), \overline{F}_2(x) \rfloor_2 = \lfloor H_sF_1(x), H_s\overline{F}_2(x) \rfloor_2$. But from Definition 3.10 $\rho(H_sF_1(x), H_sF_2(x)) = \| [H_sF_1(x), H_s\overline{F}_2(x)]_2 \|$, what concludes the proof. □

Corollary 5.4. *If $\| F_1(x) \| \neq \| F_2(x) \|$ then $F_1(x)$ and $F_2(x)$ are no coincident.*

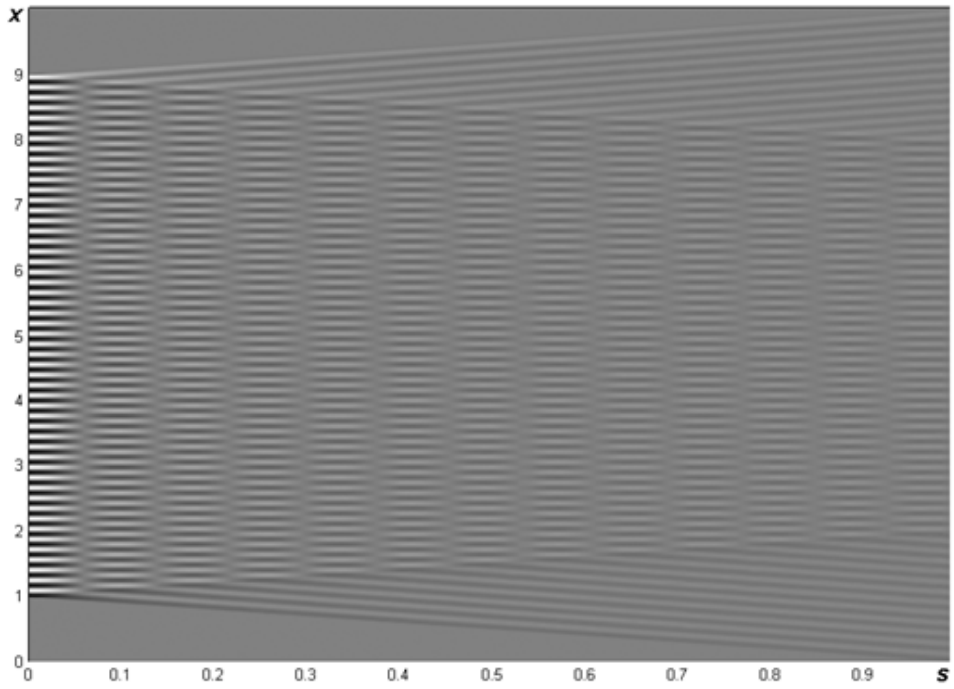

FIGURE 3. Time averaged image of $F_0(x)$ at $\lambda = \frac{\pi}{20}$

From Corollary 5.4 it follows that if $\| F_1(x) \| \neq \| F_2(x) \|$ then the following inequality holds true: $0 < [H_s F_1(x), H_s F_2(x)]_2$. This is an important conclusion which secures the collision free property of the constructed hash function. It can be noted that this property holds true when amplitude s is the same for both grayscale functions. Clearly, $0 = [H_0 F_1(x), H_s F_2(x)]_2$ if $F_1 = H_s F_2(x)$. Analogously, $0 = \left[\lim_{s\to\infty} H_s F(x), O(x)\right]_2$. Hash function must not be constructed exploiting unitary or zero operators. One has to choose some middle range of values of s instead of using extremities. That is discussed in more details in the following Section.

6. **Effects caused by digital image representation.** It is quite natural that the time averaged grayscale color intensity distribution $H_s(F(x))$ is calculated exploiting digital computational techniques. This leads to an immediate contradiction. It follows form Definition 4.1 that any time averaged grayscale function is a continuous function for $s > 0$. But it is clear that only grayscale functions with finite discontinuities at inter-pixel boundaries can be visualized exploiting digital visualization techniques. That is illustrated in Fig. 4. It is assumed that initially only 3 pixels have grayscale color intensities different from the background color (Fig. 4a). When the time average operator is applied to such a grayscale function and the amplitude s is equal to one and a half of pixel length, the theoretical color distribution in the time averaged image is presented in Fig. 4b. Unfortunately, pixel dimensions do not enable accurate reconstruction of the time averaged color intensity variation. Digital image representation implies that the image is constructed from pixels with

appropriate grayscale color intensities. Fig. 4c presents digital time averaged image where color intensities are averaged at locations of the appropriate pixels.

Moreover, calculation of the definite integral in the process of time averaging (eq. 6) is replaced with calculation of the limit sum. It can be noted that the step size of the limit sum is an important physical parameter [10]. Time step π produces double exposure (stroboscopic) geometric moiré image. Naturally, the time step should be small for time average images. The relationship between the time step and the number of correctly reconstructed fringes is analyzed in [10]. The time step (the number of discrete time moments in one half of the period of oscillation) can be one of the control (input) parameters of the hash function.

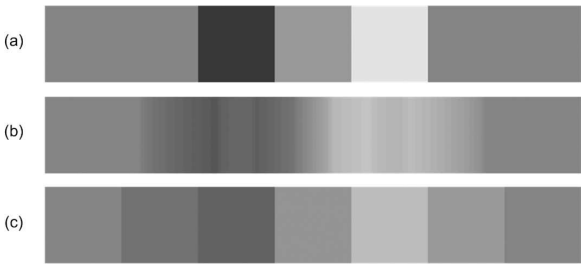

FIGURE 4. Discretisation of the time averaged function: a) initial color distribution; b) theoretical distribution of time averaged color ($s = 0.75$); c) discretised color distribution.

Another important feature of digital image processing is the fact that only a limited number of discrete grayscale intensity levels are available (usually 256 levels from 0 up to 255). Figure 4 illustrates the transitions of time averaged images at increasing values of s. Only 16 different grayscale intensity levels (from 0 up to 15) and 3 pixels are selected for clearness. Though time averaged grayscale color distribution (different from the background color) occupies more than 3 pixels at $s > 0$, only the three central pixels are visualized in Fig. 5. In fact, the original grayscale levels of these 3 pixels correspond to the ones in Fig. 4a.

In general, two slightly different finite values of s can produce the same time averaged image, especially if the number of considered pixels and the number of different grayscale levels is small and s is large. Nevertheless, appropriate discrete meshing of s-axis can help to guarantee that the hash function algorithm is collision-free. Meshing strategies depend from the number of pixels and the number of different grayscale levels and are out of scope of interest in this paper.

7. **Description of the algorithm for construction of the Hash function.** Many engineering problems are based on the reconstruction of parameters of time averaging operators. A typical example is presented in [13] where both the original grayscale function and its time averaged image are known. Then the amplitude s (and the direction of oscillations in a two-dimensional problem) can be determined solving the following optimization problem:

$$\min_{s \geq 0} \rho(F(x), H_s(F(x))). \tag{16}$$

Solution of the inverse problem when the grayscale function must be determined from its time averaged image turns out to be a much more complex problem. If

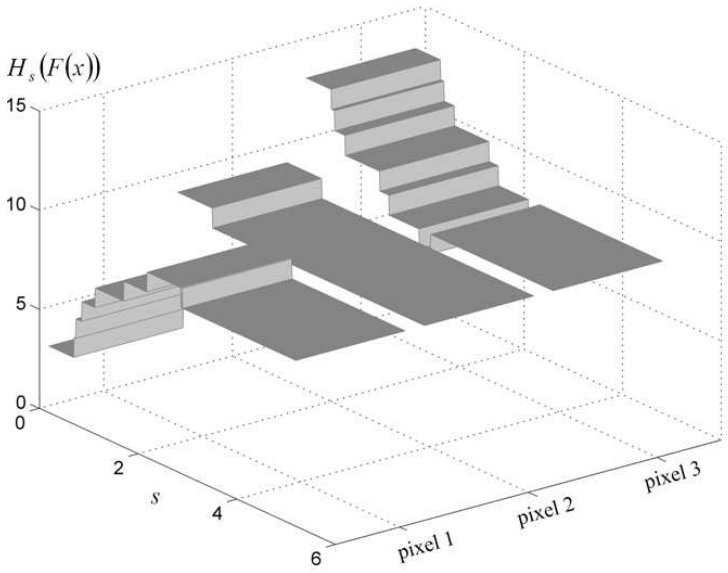

FIGURE 5. Transformation of grayscale color intensities at increasing amplitude s.

the time averaging is performed experimentally, the problem is unsolvable due to extreme sensitivity to the inevitable measurement errors; only optimization techniques can be used for approximating $F(x)$. Even if time averaging is performed using computational techniques, it is an ill-posed inverse problem and is practically unsolvable even if s is known.

Several considerations can be taken into account when constructing the Hash function. It is possible to eliminate even the theoretical possibility of reconstruction of the grayscale color invariant (Theorem 5.1). This feature would be important only if the static color distribution would fit into one of the intervals: $0 \le F(x) \le \frac{1}{2}$ or $\frac{1}{2} \le F(x) \le 1$ (what in fact is not likely). Stretching of the time averaged grayscale intensity scale to min-max color range would eliminate even this possibility.

One may also exploit the fact that $H_{s_1} \cdot H_{s_2} \ne H_{s_1+s_2}$. Double (sequential) time averaging can be applied what can be considered as the next step of algorithmic safety.

The algorithm for construction of the hash function comprises three main parts:

a) Acquisition of input data: function $F(x)$ represented as grayscale color intensities at appropriate pixels and the amplitude s.
b) Production of the intermediate result: $H_s(F(x))$ (time averaged grayscale intensities at appropriate pixels).
c) Delivery of output data: time averaged grayscale function stretched to min-max intensity levels.

This algorithm is illustrated in Fig. 6 where an input set of natural numbers (Fig. 6a) is transformed to the output set (Fig. 6d).

8. **Concluding remarks.** One may question the definition of the grayscale function (Definition 3.2). We would like to note that the original assumption that

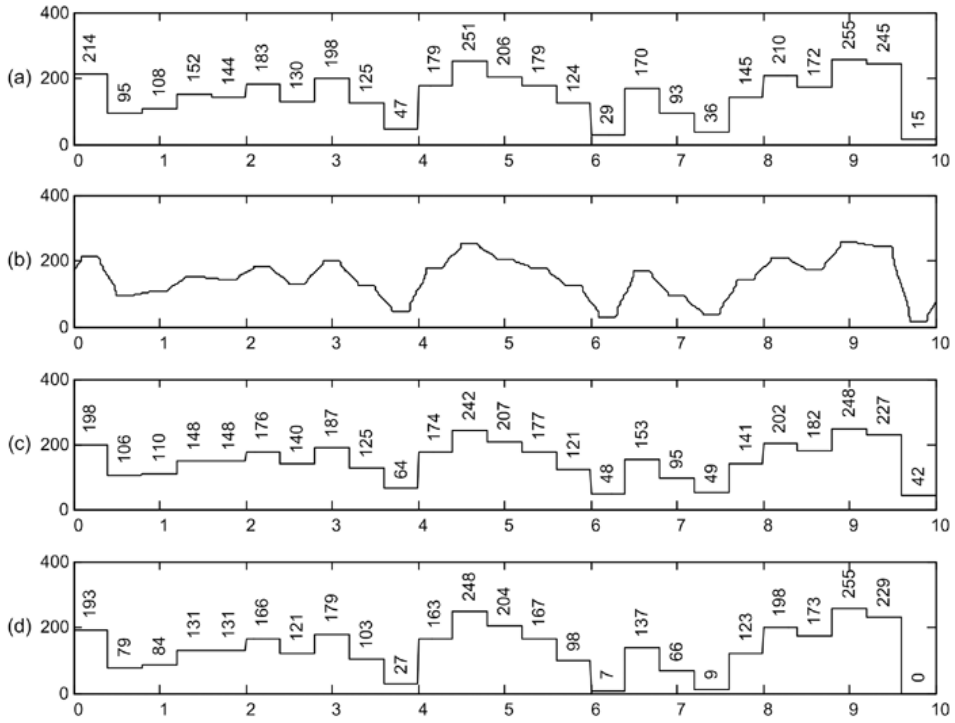

FIGURE 6. Illustration of the algorithm: a) original grayscale color distribution (width of the pixels is 0.4); b) time averaged grayscale color distribution at $s = 0.2$; c) time averaged intensity distribution averaged at appropriate pixels; d) averaged grayscale color distribution stretched to min-max levels.

$O(x) = \frac{1}{2}$ has a strong physical motivation. The observation window in realistic physical experiments is finite and the areas of the analyzed body covered by the background color (if only such areas exist at all) are far away from the observation window. Then it is natural to expect that the time averaged image will be gray (if only the original static image is not very dark or very light). That is clearly demonstrated by experimental investigations where natural stochastic grayscale structure of the surface serves as a stochastic geometric moiré grating for time average analysis [13].

Alternative definition of the grayscale function could read $\int_{-\infty}^{+\infty}(1 - F(x))dx < \infty$ resulting to $\lim_{x\to\pm\infty} F(x) = 1$ (background is white, paint is black). The seminorm then takes the following form: $\| F \| := \int_{-\infty}^{+\infty}(1 - F(x))dx$. In that case it is natural to assume that $O(x) := 1$. But the optical inverse is still the same: $\overline{F}(x) = 1 - F(x)$. Thus a generalized multiplication operation by a scalar must hold $1 \otimes F(x) = F(x)$; $0 \otimes F(x) = O(x)$; $-1 \otimes F(x) = \overline{F}(x)$ and $\alpha \otimes F(x) \in \Gamma$, for all $-1 \le \alpha \le 1$. One could suggest that $\alpha \otimes F(x) = 1 - \frac{\alpha^2+\alpha}{2} + \alpha F(x)$, but $\alpha \otimes F(x) \notin \Gamma$ for all

$-1 \leq \alpha \leq 1$ and $F(x) \in \Gamma$ (for example, $\alpha = \frac{1}{2}$ and $F(x) = 1$). Therefore, no algebraic structures can be constructed, the properties of the time average operator stay unclear and one-way collision-free hash function algorithm can not be developed.

Finally, it can be noted that the problem (and the algorithm) can be generalized to 2, 3 or even higher dimensionality and even more rich color models, what is the object of future research. But the algebraic structure of time average operators for one-dimensional grayscale problem already reveals interesting properties of time averaging process and builds the ground for development of new class of hash functions.

REFERENCES

[1] M. Bellare and P. Rogaway, *The exact security of digital signatures how to sign with RSA and Rabin*, in "Advances in Cryptology — Eurocrypt'96", Springer-Verlag, (1996), 399–414.

[2] K. Bicakci, G. Tsudik and B. Tung, *How to construct optimal one-time signatures*, Computer Networks, **43** (2003), 339–349.

[3] F.L. Dai and Z.Y. Wang, *Geometric micron-moiré*, Optics and Lasers in Engineering, **31** (1999), 191–198.

[4] J. W. Dally and W. F. Riley, "Experimental Stress Analysism 3rd ed.," McGraw-Hill, New York, 1991.

[5] S. Haber and W. S. Stornetta, *How to timestamp a digital document*, Journal of Cryptology, **3** (1991), 99–111.

[6] X. Huimin, W. Guotao, D. Fulong, Z. Guangjun, L. Xingfu, Z. Fangju, Z. et al., *The dynamic deformation measurement of the high speed heated LY12 aluminium plate with moiré interferometry*, Journal of Materials Processing Technology, **83** (1998), 159–163.

[7] A. S. Kobayashi, "Handbook on Experimental Mechanics 2nd ed.," SEM, Bethel, 1993.

[8] C. M. Liu and L. W. Chen, *Digital atomic force microscope moiré method*, Ultramicroscopy, **101** (2004), 173–181.

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

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

[11] M. Ragulskis, L. Ragulskis and R. Maskeliunas, *Applicability of time average geometric moiré for vibrating elastic structures*, Experimental Techniques, **28** (2003), 27–30.

[12] M. Ragulskis, R. Maskeliunas, L. Ragulskis and V. Turla, *Investigation of dynamic displacements of lithographic press rubber roller by time average geometric moiré*, Optics and Lasers in Engineering, **43** (2005), 951–962.

[13] M. Ragulskis, R. Maskeliunas, L. Ragulskis and V. Turla, *Identification of in-plane vibrations using time average stochastic moiré*, Experimental Techniques, **29** (2004), 41–45.

[14] P. Verleysen and J. Degrieck, *Experimental investigation of the deformation of Hopkinson bar specimens*, International Journal of Impact Engineering, **30** (2004), 239–253.

[15] D. Xiao, X. Liao and S. Deng, *One-way Hash function construction based on the chaotic map with changeable-parameter*, Chaos, Solitons & Fractals, **24** (2005), 65–71.

Received February 2007; revised May 2007.

E-mail address: minvydas.ragulskis@ktu.lt
E-mail address: zenonas.navickas@ktu.lt