Design and implementation of coupled chaotic maps in watermarking

S. Behnia [a,*], S. Ahadpour [b], P. Ayubi [c],

[a] *Department of Physics, IAU, Urmia, Iran.*

[b] *Department of Physics, Mohaghegh Ardabili University, Ardabil, Iran.*

[c] *Department of computer, IAU, Iran.*

Abstract

We propose a multidimensional coupled chaotic map as a pseudo random number generator. Based on the introduced dynamical systems, a robust watermark scheme for copyright protection is proposed. By modifying the original image in transform domain and embedding a watermark in the difference values between the original image, the proposed scheme overcomes the weak robustness problem of embedding a watermark in the spatial domain. Besides, the watermark extraction does not require the original image so, it is more practical in real applications. This algorithm tries to improve the problem of failure of encryption in small key space, encryption speed and level of security.

Key words: Chaotic map, Coupled map lattice, Pseudo random sequence, Ergodic theory, Digital watermarking, Robustness.
PACS: 05.45.Jn, 05.45.Ra, 05.45.Xt, 65.40.Gr

1 Introduction

The development of compression technology allows the widespread use of multimedia applications. Protection of multimedia information, especially its copyright, is of extensive interest. There is a strong need to keep the distribution of digital multimedia works profitable for the owner as well as reliable for the customer. In this way, digital watermarking emerges as one possible and popular solution. Watermarking, also called tamper-proofing or content

* Corresponding author.
Email address: s.behnia@iaurmia.ac.ir (S. Behnia).

verification, hides a secret and personal message to protect the copyright or to demonstrate the data integrity. In contrast with cryptography, which immediately arouses suspicion of something secret or valuable, the watermark hides a message within digital media without noticeable changes to the host. The majority of watermarking schemes proposed to date, use watermarks generated from pseudo random number sequences [13]. Chaotic functions such as Markov Maps, Bernoulli Maps, Skew Tent Map, Logistic Map have been widely used to generate watermark sequences [3,20,21]. These types of watermark generation schemes require two values,(the initial value and the function seed), to recreate the same watermark at a later stage. An advantage of these watermarks is the possibility to analyze and control their spectral properties. In this paper, we concentrated on the security (key space) [9,16].
We propose a secure watermarking scheme based on spatiotemporal chaos. In order to enhance the security, spatiotemporal chaos is employed to select the embedding positions for each watermark bit and for watermark encryption. In this article, a watermarking algorithm based on a multidimensional coupled chaotic map is proposed. The dimension of the introduced dynamical system by considering the level of the security selected, also the extra dimension can be used to apply many logo in watermarking process. We have also verified that the proposed scheme is robust against various attacks using common signal processing and geometric transformations. The rest of the Letter is organized as follows. Section 2 describes chaotic maps and the location of embedding position of watermark. Section 3 presents the synchronization condition and the ergodicity of the introduced model, Also the chaotic domain of the introduced model studied via Lypaunov exponents in order to generate the key space. The watermarking scheme based on chaotic maps is proposed in Section 4. Also, the selected example and simulation results are discussed in Section 4 and Section 5. Section 6 concludes the Letter.

2 Definition of model

The chaotic sequences exhibit some important characteristics. Some chaotic maps such as Logistic and Chebyshev maps can produce white-noise-like sequences whatever the controlling parameter takes [16,6,17]. For enhancing the security of discrete chaotic watermarking we introduce for the first time, the concept of using multidimensional coupled chaotic map with an invariant measure in watermarking [12]. Some points make this new watermark distinctive and advantageous compared to the other schemes.

- A very large number of fully developed chaotic maps defined in two intervals $x\varepsilon[0,1]$ and $x\varepsilon[0,1)$.
- High complexity due to high dimensionality and chaoticity.
- Large key space; It is obvious that the attack complexity is determined by

the size of the key space and the complexity of the verification of each key.
- The flexibility of attributing different values to the control parameters and coupling parameter.

The multidimensional coupled chaotic map can be defined as:

$$\Phi = \begin{cases} X_1 = F(x_1, ..., x_n) = \epsilon_1 f_1(x_1) + \epsilon_2 f_2(x_2) + ... + \epsilon_N f_N(x_N) \\ \vdots \\ X_N = F(x_1, ..., x_n) = \epsilon_1 f_1(x_N) + \epsilon_2 f_2(x_1) + ... + \epsilon_N f_{N-1}(x_{N-1}) \end{cases} \quad (1)$$

where, ϵ is the strength of the coupling $\{\epsilon_1 + ... + \epsilon_n = 1\}$. We introduce our map ensemble $\{f\}$ based on the one-parameter families of chaotic maps $\Phi_N(x, \alpha)$ of the interval $[0, 1]$ with an invariant measure, which can be defined as the ratio of polynomials of degree N (See Appendix A). Obviously, We have a multidimensional dynamical system associated with the coupled map with the property of possessing an invariant measure at synchronized state [12,11].

3 Key space

key space could be generated by considering the initial condition, coupling and control parameter. Many properties of the chaotic systems have their corresponding counterparts in traditional cryptosystems, such as: ergodicity and confusion, sensitivity to initial conditions, control parameter, and diffusion [19,18]. Here in this section we study the ergodicity condition by regarding the invariant measure and the chaotic domain for coupled map studied by lyapunov exponent. By transfer the multidimensional coupled chaotic map to chaotic domain the key space arranged. One possibility to have a ergodic coupled map is to synchronize the model.
Synchronization of two (or more) chaotic dynamical systems (starting with different initial conditions) means that their chaotic trajectories remain in step with each other during the temporal evolution. In this field, the key concept of complete synchronization refers to a state where the trajectories of dynamical systems approach each other[2,22]. In this study, we introduce the system has fast speed and robust synchronization properties.

3.1 Invariant measure

For multidimensional coupled chaotic map, we have tried to describe ergodicity from the invariant measure point of view [10,7]. The measure which describes

the ergodic properties with respect to the typical initial conditions is usually called SRB measure [10,8]. The difficulty in proving rigorously that a given coupled map exhibits spatio-temporal chaos lies in the finding of such an SRB measure. Each symmetric transformation for generic model Eq. (1) should be satisfying in the invariant measure. The suitable condition for the presentation of the invariant measure of the synchronized coupled map is choosing a one-dimensional map with an invariant measure as we introduced in our previous work [12]. We could rewrite the Frobenius-Perron (FP) integral for multidimensional coupled chaotic map as follows [10,8]:

$$\mu(x_1(n+1),...,x_N(n+1)) = \int dx_1 ... \int dx_N \delta\left(x_1(n+1) - F_1(x_1(n),...,x_N(n))\right)$$

$$...\delta(x_N(n+1) - F_N(x_1(n),...,x_N(n)))\mu(x_1(n),..,x_N(n)),$$

We will show that the invariant measure at synchronized state has the following form:

$$\mu(x_1,...,x_N) = \delta(x_2 - x_1)....\delta(x_N - x_1)\mu(x_1) \tag{2}$$

Relation 2 shows invariance under the permutation of synchronization coordinate $(x_1, x_2, ...)$, therefore, The measure is invariant at transverse direction and the stable direction follows $\mu(x_1)$. By considering the complete synchronization condition in (FP) integral for multidimensional coupled chaotic map:

$$\mu = \int dx_1 .. \int dx_N \; \delta\left(x_1(n+1) - F_1(x_1(n),..,x_N(n))\right) \delta(x_N(n+1) - F_N(x_1(n),..,x_N(n)))$$

$$\times\delta(x_2(n) - x_1(n))....\delta(x_N(n) - x_1(n))\mu(x_1),$$

which reduces to:

$$\mu = \delta(x_2(n+1) - x_1(n+1))..., \delta(x_N(n+1) - x_1(n+1))$$

$$\times \int dx_1 \delta(x_1(n+1) - F_1(x_1(n),..,x_1(n)))\mu(x_1(n)),$$

Now, if the one-dimensional map $x(n+1) = F(x_1(n),...,x_1(n))$ possesses the invariant measure $\mu(x_1(n))$, that is, it satisfies:

$$\mu(x(n+1)) = \int \delta(x(n+1) - F(x_1(n),...,x_1(n))d\mu(x_1), \tag{3}$$

Then, we have:

$$\mu(x_1(n+1),...,x_N(n+1)) =$$

$$\delta(x_1(n+1) - x_2(n+1)),..., \delta(x_N(n+1) - x_1(n+1))\mu(x_1(n+1)). \tag{4}$$

3.2 Lyapunov exponent spectra

The following properties make a deterministic algorithm suitable to generate a pseudo random sequence of numbers: high value of entropy, high dimensionality of the parent dynamical system, and very large period of the generated sequence [15,14,5]. There is a close correlation between the Lyapunov exponent of the underlying chaotic map and the "randomness". Since randomness is desired to be seen on a random number generator clearly, it must be correlated to the diverging nature of the trajectories of a chaotic map, which is tied to the existence of a positive Lyapunov exponent.
A spectrum of all the Lyapunov exponents with respect to the synchronization solution, can be evaluated in a fashion similar to that of one-dimensional local maps [11,10]. At synchronized state, the Lyapunov exponents Λ_k of multidimensional coupled chaotic map described by the Eq. (1) are defined as, $\lim_{n\longrightarrow\infty}\frac{1}{n}|\lambda_k(x_1,...,x_N)|$, where $\lambda_k=\sum_{k=1}^{N}h_k(x_1,...,x_N)$ are eigen states of the matrix:

$$\left[\begin{array}{ccc} \frac{\partial\overbrace{FoFo...F}^{n}(x_1(0),...,x_N(0))}{\partial x_1(0)} & \cdots & \frac{\partial\overbrace{FoFo...oF}^{n}(x_1(0),...,x_N(0))}{\partial x_N(0)} \\ \vdots & & \\ \frac{\partial\overbrace{FoFo...F}^{n}(x_N(0),..,x_{N-1}(0))}{\partial x_1(0)} & \cdots & \frac{\partial\overbrace{FoFo...F}^{n}(x_N(0),..,x_{N-1}(0))}{\partial x_N(0)} \end{array}\right]_{|x_1(0)=,...,=x_N(0)} =$$

$$\left[\begin{array}{ccc} \frac{\partial X_1}{\partial x_1} & \cdots & \frac{\partial X_1}{\partial x_N} \\ \vdots & & \\ \frac{\partial X_N(k)}{\partial x_N} & \cdots & \frac{\partial X_N}{\partial x_{N-1}} \end{array}\right]_{|x_1=...=x_N} = \left[\begin{array}{cccc} h_1(x_1,...,x_N) & h_2(x_1,...,x_N) & ... & h_N(x_1,...,x_N) \\ h_2(x_1,...,x_N) & h_3(x_1,...,x_N) & ... & h_1(x_1,...,x_N) \\ & \vdots & & \\ h_N(x_1,...,x_N) & h_1(x_1,...,x_N) & ... & h_{N-1}(x_1,...,x_N) \end{array}\right]$$

and $x_k=\overbrace{FoFo..F}^{k}(x_0,x_0,...,x_0)$. Now, in the case of ergodic one-dimensional map $X=F(x,x,...x)$, the Lyapunov exponents can be written as:

$$\Lambda_k(\text{syn})=\lim_{n\to\infty}\frac{1}{n}\ln|\lambda_k(x_n)|$$

$$=\lim_{n\to\infty}\frac{1}{n}\ln|\lambda_k(\overbrace{FoFo..F}^{n}(x_{1_0},x_{1_0},...,x_{1_0}))|=\lim_{n\to\infty}\frac{1}{n}\sum_{k=0}^{n}\ln(|\sum_{i=1}^{N}h_i(x_{1_k},...,x_{N_k})|)$$

$$\Lambda_k(\text{syn})=\int dx\mu(x)\ln(|\sum_{i=1}^{N}h_i(x_{1_0},...,x_{N_0})|). \tag{5}$$

Therefore, the ergodicity of one-dimensional map $X = F(x, x, ..., x)$ implies the ergodicity of symmetric multidimensional coupled chaotic map (Eq. (1)) at unstable synchronized state (synchronized state is stable for negative critical exponent Λ_k). Obviously, the non-ergodic choice of $X = F(x, x, ..., x)$ will lead to the non-ergodicity at synchronized state. There is a close correlation between the Lyapunov exponent sign of the maps and the efficiency of the extracted data in forming a good set of pseudo random numbers.

4 Watermark embedding and extraction

Watermark provides a natural link between chaotic dynamics and information theory on which, the recent idea of utilizing chaotic systems in encoding digital information is based. The proposed Watermarking consists of multidimensional coupled chaotic maps which are used along with a single chaotic map.
In order to clarify the performance of the introduced model (Eq. (1)) in watermarking process by considering our improved model of logistic map [12], the simple two-dimensional model for watermarking is built, as follows. At synchronized state $x_1 =, ..., = x_N = x$, the coupled map Eq. (2) regarding (A.4), reduces to:

$$X = F(x, ..., x) = \bar{a}(\epsilon_1, ..., \epsilon_N, a_1, ..., a_N) \tan^2(N \arctan(\sqrt{x})) \tag{6}$$

with $\bar{a}(\epsilon, a_1, a_2, ..., a_N) = (\sum_{i=1}^{N} \epsilon_i a_i)$. As it is shown in (See Appendix B), this map possess the invariant measure of the following form:

$$\mu(x_1, x_2, ..., x_N) = \delta(x_2 - x_1)...\delta(x_N - x_1)\frac{\sqrt{\beta}}{\sqrt{x}(1 + \sqrt{\beta}x)}. \tag{7}$$

provided that we choose the constant β as one of the positive roots of the following equation:

$$\bar{a}(\epsilon_1, \epsilon_2, ..., \epsilon_N, a_1, a_2, .., a_N) = \left(\frac{\sum_{k=0}^{[\frac{N}{2}]} C_{2k}^{N} \beta^{-k}}{\sum_{k=0}^{[\frac{N-1}{2}]} C_{2k+1}^{N} \beta^{-k}} \right)^2 \tag{8}$$

In our introduced example, the Lyapunov exponents are (See Appendix B):

$$\Lambda_k = \lim_{n \to \infty} \frac{1}{n} \ln |\lambda_k(x_{1,k}, ..., x_{N,k})|$$

$$= \ln|(1-\epsilon)a_1 - \epsilon a_2| + \ln|\sum_{k=1}^{N} \epsilon_k \omega^{k-1} a_k| + \Lambda\left[(\sum_{k=1}^{N} \epsilon_k a_k) g'(x_{1,k}, ..., x_{N,k})\right] \quad (9)$$

Noting $N = 2$, Eq. (6) reduces to the following two-dimensional chaotic maps:

$$X = F(x, x) = \bar{a}(\epsilon, a_1, a_2) \tan^2(2 \arctan(\sqrt{x})). \quad (10)$$

which is used in watermarking process. The last part of the encryption is followed by:

$$X = \frac{1}{a_3^2} \tan^2(2 \arctan \sqrt{x}). \quad (11)$$

At the second stage, we select the key. A positive way to describe the key space [4] might be in terms of positive Lyapunov exponents. Since it was proved that the introduced map has an invariant measure, by refereing to analytically calculated Lyapunov exponents, we select a suitable control parameter domain for the key space (see Fig. 1(a) and (b)). Key space size in our introduced example, (Eqs. (10) and (11)) consists of coupling parameter and three-control parameters and three initial conditions.
Watermark embedding process is described as follows. We assume that the original image of the size $n \times n$ be denoted as $\Phi = \{\Phi(x_1, x_2), 1 \leq x_1, x_2 \leq n\}$ and the binary watermark (logo) of size $m \times m$ be denoted by $\phi = \{\phi(i, j), 1 \leq i, j \leq m\}$, where $(i, j)((x_1, x_2))$ represent the pixel coordinate of binary watermark image and the original host image.
Watermark bits (1 bit per pixel) are embedded to the host image according to the following process. Using the coordinate (i, j) of watermark pixel as the initial condition and the control parameter of the coupled map (see Fig. (1)), the coupled map is iterated after which, the embedding position of pixels from watermark image to host image can be obtained. The watermark pixels will get different embedding positions, so the embedded watermark pixels will spread in host image randomly.
This process follows the iteration of the third map (Eq. (11)) to determine the bit of host image pixels in watermark embedding. Accounting for the chaotic domain of the third map, (See Fig 1(b)) the truly random sequence is generated which is distributed in the interval ($[0, 1]$ or $[0, \infty)$) then, the interval can be divided into several subintervals ($[0, \acute{x}_1]$, $[\acute{x}_1, \acute{x}_2], \ldots$) which correspond to different pixel bits for watermark embedding [1,23]. As it was discussed by dividing the sub domain corresponding to the $\mathbf{k^{th}}$ bit of host image, ($[0, \acute{x}_1] \rightarrow k_3$,$[\acute{x}_1, \acute{x}_2] \rightarrow k_4$, $\ldots$) the watermark pixel is embedded to the $\mathbf{k^{th}}$ bit of pixel $(\acute{x}_1, \acute{x}_2)$ in host image.
The embedded watermark pixel is denoted as $\Phi(x_1, x_2)$. If $\phi(i, j)$ is the same as the $\mathbf{k^{th}}$ bit of $\Phi(x_1, x_2)$, then $\phi(x_1, x_2) = \Phi(x_1, x_2)$, i.e., the pixel value is

kept unchanged; otherwise, the $\mathbf{k^{th}}$ bit of $\Phi(x_1, x_2)$ is substituted by $\phi(i, j)$. The flowchart of the overall solution algorithm is shown in figure 2. Watermark extraction is just the inverse process of the above embedding algorithm. In the process of extraction, one needs to know the key parameters. Since both decryption and encryption procedures have similar structure, they have essentially the same algorithmic complexity and time consumption.

5 Experimental results

This section will present and discuss the experimental results of our proposed scheme. To demonstrate the effectiveness of the proposed algorithm, MATLAB simulations are performed by using 256×256 pixel gray level "MADINEH" image and 64×64 pixel binary watermark logo "FATIMA". Fig. 3 demonstrates the invisibility of watermark. Figs. 3(a) and 3(b) show the original host image and watermark logo ,respectively. Figs. 3(c) and 3(d) show the water-marked image and the extracted watermark logo "FATIMA", respectively. The watermark embedding process is said to be imperceptible if the original data and watermarked data cannot be distinguished . To quantitatively evaluate the performance of the proposed scheme, the peak signal-to-noise ratio (PSNR) was adopted to measure the image quality of a watermarked image which is given by:

$$\begin{aligned} PSNR &= 10 \times \log_{10} \tfrac{255^2}{MSE}(dB), \\ MSE &= \tfrac{1}{M \times N} \textstyle\sum_{i=1}^{M} \sum_{j=1}^{N} (H_{i,j} - \acute{H}_{i,j}). \end{aligned} \tag{12}$$

Where $H_{i,j}$ and $\acute{H}_{i,j}$ indicate the pixel values in the location (i, j) of the original host image and the watermarked image, respectively, while $M \times N$ is the image size. In this study, reliability was measured as the bit error rate (BER) of extracted watermark through this formula:

$$BER = \frac{B}{M \times N} \times 100 \tag{13}$$

Where, B is the number of erroneously detected bits, and $M \times N$ is the extracted watermark image dimensions. The PSNR for the watermarked image is 48.82 dB, and the BER of the extracted watermark is zero. Therefore, there is no obvious perceptual distortion between watermarked image and original one; the embedded watermark does not degrade the quality of original host image. To test the robustness of our proposed method, we applied several attacks

to the watermarked image including JPEG compression, Salt & Pepper noise, Gaussian noise, Gaussian low-pass filter, gamma correction, histogram equalization, sharpening, Rotation, motion blur, Complement, Cropping and Median Filtering. Fig. 4 shows an example of a watermarked image attacted with the listed attacks. The corresponding best extracted watermarks are shown in Fig. 5.The test results for "MADINEH" image are shown in table 1.
Key space size is the total number of different keys that can be used in the encryption. Cryptosystem is completely sensitive to all secret keys. The order of time complexity for watermark extraction in our proposed method is computed below:

$$\theta(\epsilon \times x_0^3 \times iter \times a^3) \tag{14}$$

Where $\epsilon \; \varepsilon \; [0,1]$, $x_0 \; \varepsilon \; [0,1](x_0 \; \varepsilon \; [0,\infty))$, and $a \; \varepsilon \; [\frac{1}{N},\infty)$. Apparently, the key space is large enough to resist all kinds of brute-force attacks.

6 Concluding remarks

We propose a novel watermarking scheme for image authentication based on spatiotemporal chaos. The scheme is specially designed for image, thus, enabling various network multimedia applications. Spatiotemporal chaos is applied to design the selection scheme for watermark embedding. We have used symmetric multidimensional coupled chaotic maps to increase both the number of keys (control parameters) and complexities involved in the algorithm. This algorithm tries to address the shortcoming of watermarking such as small key space, watermarking speed and level of security. Without the correct initial condition, the watermark cannot be successfully detected. In general, the method is suitable for image authentication with application in law, commerce, defence, medical databases and journalism. The security of watermarking is greatly improved when chaos is administered. The goal is to realize a watermarking method with a private code. Further studies must be started to develop watermarking methods with a public key.

7 Acknowledgments

The authors would like to express their heartfelt gratitude to Mr. Wiria Soltanpoor for the nice editing of their paper - this has certainly improved its readability.

A One-parameter family of chaotic maps

We present a brief review of one-dimensional chaotic maps which are going to be used. One-parameter families of chaotic maps $\Phi_N(x,a)$ of the interval $[0,1]$ with an invariant measure, which can be defined as the ratio of polynomials of degree N [12]:

$$\Phi(x,a) = \frac{a^2(T_N(\sqrt{x}))^2}{1+(a^2-1)(T_N(\sqrt{x}))^2}, \tag{A.1}$$

As an example, some of these maps are given below:

$$\Phi_2(x,a) = \frac{a^2(2x-1)^2}{4x(1-x)+a^2(2x-1)^2}, \tag{A.2}$$

$$\Phi_3(x,a) = \frac{a^2x(4x-3)^2}{a^2x(4x-3)^2+(1-x)(4x-1)^2}, \tag{A.3}$$

It is shown that these maps have an interesting property, that is, for even values of N, the $\Phi(a,x)$ maps have only one fixed point attractor at $x=1$ provided that their parameter belongs to the interval (N,∞) while, at $a \geq N$ they bifurcate to chaotic regime without having any period doubling or period-n-tupling scenario and remain chaotic for all $a \in (0,N)$. However, for odd values of N, these maps demonstrate a different behavior; within $a \in (\frac{1}{N},N)$, they have a fixed point attractor only at $x=0$; they bifurcate to a chaotic regime at $a \geq \frac{1}{N}$ and remain chaotic for $a \in (0,\frac{1}{N})$, but, eventually, they bifurcate at $a=N$ to have $x=1$ as fixed point attractor for the whole range of $a \in (\frac{1}{N},\infty)$ (See Fig. (3)). In this paper, we are concerned with their conjugate maps which are defined as:

$$\Phi_N(x,a) = h \circ \Phi_N(x,a) \circ h^{-1} = \frac{1}{a^2}\tan^2(N\text{arc}tan\sqrt{x}). \tag{A.4}$$

Conjugacy means that the invertible map $h(x) = \frac{1-x}{x}$ maps $I=[0,1]$ into $[0,\infty)$. In order to simplify the calculation in this paper, we denote "$\tan^2(N\arctan\sqrt{x})$" with $g(x)$.

B Invariant measure & Lyapunov exponents of selected example

According to the introduced hierarchy of one-parameter families of ergodic maps as a multidimensional coupled chaotic, in this section, we evaluate its invariant measure and Lyapunov exponents:

- Invariant measure:
  At synchronized state $x_1 =, ..., = x_N = x$, the coupled map Eq. (2) on account of (A.4), reduces to:

$$X = F(x, ..., x) = \bar{a}(\epsilon_1, ..., \epsilon_N, a_1, ..., a_N) \tan^2(N \arctan(\sqrt{x})) \tag{B.1}$$

  with $\bar{a}(\epsilon, a_1, a_2, ..., a_N) = (\sum_{i=1}^{N} \epsilon_i a_i)$. As it is shown in Ref. [12], this map possesses an invariant measure of the following form:

$$\mu(x) = \frac{\sqrt{\beta}}{\sqrt{x}(1 + \sqrt{\beta}x)}, \tag{B.2}$$

  provided that we choose the constant β as one of the positive roots of the following equation:

$$\bar{a}(\epsilon_1, \epsilon_2, ..., \epsilon_N, a_1, a_2, .., a_N) = \left(\frac{\sum_{k=0}^{[\frac{N}{2}]} C_{2k}^{N} \beta^{-k}}{\sum_{k=0}^{[\frac{N-1}{2}]} C_{2k+1}^{N} \beta^{-k}} \right)^2$$

  where [ ] means the greatest integer part. Now, by substituting the invariant measure of one-dimensional maps $(B.2)$ in the relation (4), we get the following expression for the invariant measure of multidimensional coupled chaotic map Eq. (10):

$$\mu(x_1, x_2, ..., x_N) = \delta(x_2 - x_1)...\delta(x_2 - x_1) \frac{\sqrt{\beta}}{\sqrt{x}(1 + \sqrt{\beta}x)}. \tag{B.3}$$

- Lyapunov exponents:
  In order to calculate the Lyapunov exponents of multidimensional coupled chaotic at synchronized state, we need to calculate the characteristic roots of the matrix:

$$\prod_{k=1}^{n-1} \begin{vmatrix} h_1(x_{1,k}, ..., x_{N,k}) & h_2(x_{1,k}, ..., x_{N,k}) & ... & h_N(x_{1,k}, ..., x_{N,k}) \\ & \vdots & & \\ h_N(x_{1,k}, ..., x_{N,k}) & h_1(x_{1,k}, ..., x_{N,k}) & ... & h_{N-1}(x_{1,k}, ..., x_{N,k}) \end{vmatrix} =$$

$$\begin{pmatrix} \epsilon_1 a_1 & \epsilon_2 a_2 & ... & \epsilon_N a_N \\ \vdots & & & \\ \epsilon_N a_N & \epsilon_1 a_1 & ... & \epsilon_{N-1} a_{N-1} \end{pmatrix}^{n+1} \prod_{k=0}^{n} \left[(\sum_{k=1}^{N} \epsilon_k a_k) g'(x_k) \right] =$$

$$(F \begin{pmatrix} \sum_j \epsilon_j a_j & & \\ & \ddots & \end{pmatrix} F^{-1})^{n+1} \prod_{k=0}^{n} \left[(\sum_{k=1}^{N} \epsilon_k a_k) g'(x_k) \right] =$$

$$\begin{pmatrix} \sum_j \epsilon_j a_j & & & \\ & \sum_j \epsilon_j \omega^{j-1} a_j & & \\ & & \ddots & \\ & & & \sum_j \epsilon_j \omega^{(j-1)(N-1)} a_j \end{pmatrix} \prod_{k=0}^{n} \left[(\sum_{k=1}^{N} \epsilon_k a_k) g'(x_k) \right]$$

where:

$$F = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega & \dots & \omega_{N-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \omega_1^{(N-1)} & \dots & \omega_{N-1}^{(N-1)} \end{pmatrix}$$

which yields:

$$\lambda_k(x_{1,k}, ..., x_{N,k}) = \prod_{k=0}^{n} \left[(\sum_{k=1}^{N} \epsilon_k a_k) g'(x_{1,k}, ..., x_{N,k}) (\sum_{k=1}^{N} \epsilon_k \omega^{(k-1)} a_k) \right] . \quad \text{(B.4)}$$

Hence, we have:

$$\Lambda_k = \lim_{n \to \infty} \frac{1}{n} \ln |\lambda_k(x_{1,k}, ..., x_{N,k})| =$$

$$\ln |(1-\epsilon) a_1 - \epsilon a_2| + \ln |\sum_{k=1}^{N} \epsilon_k \omega^{(k-1)} a_k| + \Lambda \left[(\sum_{k=1}^{N} \epsilon_k a_k) g'(x_{1,k}, ..., x_{N,k}) \right]$$

References

[1] A. Mooney, J. G. Keating, D. M. Heffernan, A detailed study of the generation of optically detectable watermarks using the logistic map, Chaos, Solitons & Fractals 30 (2006) 1088-1097.

[2] A. Shabunin, V. Astakhov, Quantitative analysis of chaotic synchronization by means of coherence, Phys. Rev. E 72 (2005) 016218-28.

[3] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis S. Tsekeridou, I. Pitas, Markov chaotic sequences for correlation based watermarking schemes, chaos, solitons and fractals 17 (2003) 567-573.

[4] B. Schneier, Applied cryptography protocols, algorithms, and source code , New York: John Wiley & Sons, (1996).

[5] C.M. Gonza leza, H.A. Larrondoa, O.A. Rosso, Intensive statistical complexity measure of pseudorandom number generators, Physica A 354 (2005) 133-138.

[6] C. Peng, S. Prakash, H. J. Herrmann, H. E. Stanley, Randomness versus deterministic chaos : Effect on invasion percolation clusters, Phys. Rev. A. 42 (1990) 4537-4542.

[7] D. Ruelle, Chaotic Evolution and Strange Attractors Part II, Cambridge University Press, Cambridge, (1989).

[8] E. Ott, Chaos in dynamical system, Cambridge university pess, Canada, (1993).

[9] G. Voyatzis, I. Pitas, Digital image watermarking using mixing systems, Computers & Graphics 22 (1998) 405-416.

[10] J. P. Eckmann, D. Ruelle, Ergodic theory of chaos and strange attractors , Rev. Mod. Phys. 57 (1985) 1115-1115.

[11] J.R.Dorfman, An Introduction to Chaos in Nonequilibrium Statistical Mechanics, Cambridge, (1999).

[12] M.A. Jafarizadeh, S. Behnia, S. Khorram, H.Nagshara, Hierarchy of Chaotic Maps with An Invariant Measure, J. Stat. Phys. 516 (2001) 1013-1028.

[13] M. Barni, F. Bartolini, A. Piva, Improved wavelet based watermarking through pixel-wise masking, IEEE Trans Image Process 10 (2001) 783-791.

[14] M. Falcioni, L. Palatella, S. Pigolotti, Properties making a chaotic system a good pseudo random number generator, Phys. Rev. E 72 (2005) 016220-10.

[15] P. Lee, Yi Chenb, S. Pei, Y. Chena, Reply to the comment Keystream cryptanalysis of a chaotic cryptographic method, Computer Physics Communications 160 (2004) 208.

[16] R. M. Ďsouza, Y. Bar-Yam, M. Kardar, Sensitivity of ballistic deposition to pseudorandom number generators, Phys. Rev. E 57 (1998) 5044-5052.

[17] R. Ursulean, Reconsidering the Generalized Logistic Map as a Pseudo Random Bit Generator, Elektronika IR Electrotechnika, 56 (2004) 10-13.

[18] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps, Physics Letters A 366 (2007) 391-396.

[19] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, Cryptography based on chaotic random maps with position dependent weighting probabilities Chaos, Solitons & Fractals 35, (2008) 408.

[20] S. Nikolaidis, I. Pitas, Comparison of different chaotic maps with application to image watermarking, In: Proceedings of IEEE international symposium on circuits and systems, Geneva, (2002) 509-512.

[21] S. Tsekeridou, V. Solachidis, N. Nikolaidis, A. Nikolaidis, A. Tefas, I. Pitas, Theoretic Investigation of the Use of Watermark Signals Derived from Bernoulli Chaotic, In: Proceedings of IEEE international conference on acoustics, speech and signal processing, (2001) 1989-1997.

[22] Y. Shu, A. Zhang, B. Tang, Switching among three different kinds of synchronization for delay chaotic systems, Chaos, Solitons & Fractals 23 (2005) 563-571.

[23] Z. Peng, W. Liu, Color image authentication based on spatiotemporal chaos and SVD, Chaos, Solitons & Fractals, 36 (2008) 946-952.

Table B.1
Simulation results of PSNR and BER under different attacks.

Attacks	PSNR (dB)	BER (%)
JPEG compression	63.41	11.94
Salt & Pepper noise 10%	60.79	4.96
Gaussian Noise (0,0.1)	67.59	23.17
Histogram Equalization	56.46	5.00
Median Filtering $[3 \times 3]$	66.77	45.29
Low pass filter $[5 \times 5]$	62.21	18.97
Gamma Correction 0.6	56.46	53.17
Motion Blur 45°	67.45	40.26
Rotation 2°	64.55	27.88
One quarter Cropped	66.48	3.42
Sharpening	67.19	15.75
Complement	69.08	100.00

Fig. 1. Lyapunov exponents at synchronized state: (a)$Eq.(10)$ while N=2 and $\epsilon = 0.1$ vs. α_1 and α_2 , (b) $Eq.(11)$ vs. α.

Fig. 2: flowchart.

Fig. 3 (a) Original "MADINEH" image, (b) Watermark logo "FATIMA", (c) Watermarked image, (d) Extracted watermark logo.

Fig. 4 The watermarked "MADINEH" image under different attacks. (a) JPEG compression, (b) Salt & pepper noise 10%, (c) Gaussian noise $(0, 0.01)$, (d)Histogram Equalization; (e) Median filter $[3 \times 3]$, (f) low-pass filter $[5 \times 5]$, (g) Gamma correction 0.6, (h) motion blur (45°), (i) Rotation (2°), (j) Cropping (25%), (k) sharpening, (l) complement.

Fig. 5 Extracted watermarks under different attacks. (a) JPEG compression, (b) Salt & pepper noise 10%, (c) Gaussian noise $(0, 0.01)$, (d)Histogram Equalization, (e) Median filter $[3\times3]$, (f) low-pass filter $[5\times5]$, (g) Gamma correction 0.6, (h) motion blur (45°), (i) Rotation (2°), (j) Cropping (25%), (k) sharpening,(l) complement.