Available online at www.sciencedirect.com
ScienceDirect

Chaos, Solitons and Fractals 35 (2008) 408–419

CHAOS
SOLITONS & FRACTALS

www.elsevier.com/locate/chaos

A novel algorithm for image encryption based on mixture of chaotic maps

S. Behnia [a,*], A. Akhshani [a], H. Mahmodi [a], A. Akhavan [b]

[a] *Department of Physics, IAU, Urmia, Iran*
[b] *Department of Engineering, IAU, Urmia, Iran*

Accepted 14 May 2006

Communicated by Prof. M.S. El Naschie

Abstract

Chaos-based encryption appeared recently in the early 1990s as an original application of nonlinear dynamics in the chaotic regime. In this paper, an implementation of digital image encryption scheme based on the mixture of chaotic systems is reported. The chaotic cryptography technique used in this paper is a symmetric key cryptography. In this algorithm, a typical coupled map was mixed with a one-dimensional chaotic map and used for high degree security image encryption while its speed is acceptable. The proposed algorithm is described in detail, along with its security analysis and implementation. The experimental results based on mixture of chaotic maps approves the effectiveness of the proposed method and the implementation of the algorithm. This mixture application of chaotic maps shows advantages of large key space and high-level security. The ciphertext generated by this method is the same size as the plaintext and is suitable for practical use in the secure transmission of confidential information over the Internet.

1. Introduction

Chaos theory has been established since 1970s by many different research areas, such as physics, mathematics, engineering, and biology, etc. [1]. Since 1990s, many researchers have noticed that there exists the close relationship between chaos and cryptography [2,3]; many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems. Chaotic systems have several significant features favorable to secure communications, such as ergodicity, sensitivity to initial condition, control parameters and random like behaviour, which can be connected with some conventional cryptographic properties of good ciphers, such as confusion/diffusion. With all these advantages scientists expected to introduce new and powerful tools of chaotic cryptography. Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptosystems are divided between those that are symmetric (secret-key) and those that are asymmetric (public-key). The chaotic cryptography technique which we are going to use in this

[*] Corresponding author.
E-mail address: s.behnia@iaurmia.ac.ir (S. Behnia).

0960-0779/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.chaos.2006.05.011

paper belongs to symmetric key cryptography. There is a further division of symmetric cryptosystems into block ciphers and stream ciphers. Two main approaches to the application scenario of chaotic systems in designing cryptographic systems can be found in the literatures: analog and digital. Most analog chaos-based cryptosystems based on the concept of chaotic synchronization, first shown by Pecora and Carrol [4]. Also many different chaotic modulations have been proposed. These techniques may be classified into the following main families:chaotic switching or chaos shift keying (CSK), differential CSK (DCSK), and chaotic masking. Some of these methods are overviewed in [5–9].

This paper chiefly focuses on the chaotic digital encryption techniques.In the digital world nowadays, the security of digital images becomes more important since the communications of digital products over network occur more and more frequently. Thus, to protect the content of digital images, some specific encryption systems are needed. Encryption of images is different from that of texts due to some intrinsic features of image, such as bulk data capacity and high correlation among pixels, traditional cryptographic techniques such as DES, IDEA and RSA are not suitable for practical image encryption, especially under the scenario of on-line communications.

The ideas of using digital chaotic systems to construct cryptosystems have also been proposed [10–17]. Undoubtedly, security has been a topic of increasing importance in communications as the Internet and personal communications systems are being made accessible worldwide.

However, the recent development of chaotic cryptosystem is rather disappointing. On the other hand, various cryptanalysis have exposed some inherent drawbacks of chaotic cryptosystems [18–21]. Here we enumerate some of them; weakness in security even with chaotic dynamics completely hidden, slow performance speed due to analytical floating-point computation and small key space, which make it difficult to promote the chaotic digital encryption into practical service.

In this paper, a new design of a class of chaotic cryptosystems is suggested to overcome the aforementioned drawbacks by using one dimensional chaotic map and their coupling for obtaining high level security [22,23].

The motivation to investigate coupled chaotic map along with a chaotic map as a cryptosystem using coupling parameter was to achieve some computational goal, and also using coupling parameter as connection between coupled map and third map. An approach to further enhance the security is to use high-dimensional chaotic systems such as a coupled map. A coupled dynamical network can be regarded as a high-dimensional dynamical system. On the other hand, we use high-dimensional chaos as the basic structure of the cryptography, which leads to the following significant advantages: due to the high-dimensionality and chaoticity, the output ciphertext has high complexity, long periodicity of computer realization of chaos, and effective byte confusion and diffusion in many directions in the variable space. All these properties are favorable to achieve high practical security. In this paper a general framework for chaos-based cryptography has been developed. By applying the proposed technique, it is possible to design cryptosystems based on introduced hierarchy of chaotic maps [22,23].

This paper will be arranged as follows. In Section 2 a brief description of chaotic coupled map is presented. The encryption algorithms are described in Section 3 and in Section 4 the results are devoted. Security analysis and conclusion will be discussed in Sections 5 and 6, respectively.

2. Applied coupled map model

Simulation of the natural phenomena is one of the most important research fields and coupled map lattices are a paradigm for studying fundamental questions in spatially extended dynamical systems.

We can divide them into two categories: internal and external coupled map lattice [24]. Globally coupled map is one of the most well-known examples of the external coupling, with different number of elements [25]. Coupling relations such as the week coupling [26], noisy coupling [27], and functional coupling [28] used to make the new coupled map. In order to create the new encryption model based on the internal coupling, in this section we introduce coupled map model of two chaotic system, where they are coupled according their control parameter in order to increase the security of encrypted massage and decrease the encryption time.

2.1. One-dimensional map

The modeling of the physical system may be most appropriate in terms of a discrete time. Some examples of one-dimensional maps are Lorenz map, tent map, and logistic map.

We generalize Logistic maps to a Hierarchy of one parameter families of maps with invariant measure, where the Logistic map is topologically conjugate to the first map of this hierarchy [22].

These one-parameter families of chaotic maps of the interval $[0,1]$ with an invariant measure can be defined as the ratio of polynomials of degree N:

$$x_N(n+1) = \frac{\alpha^2 (T_N(\sqrt{x(n)}))^2}{1 + (\alpha^2 - 1)(T_N(\sqrt{x(n)})^2)}, \tag{1}$$

where T_N are Chebyshev polynomials of type I, α control parameter, n presents the time and N is an integer greater than one. $x_N(n+1)$ is $(N-1)$-model map, that is it has $(N-1)$ critical points in unit interval $[0,1]$. By studying Shwarzian derivative one can show that, the maps $x_N(n+1)$ have at most $N+1$ attracting periodic orbits [22,29]. These maps have only one single period one stable fixed points or they are ergodic.

Maps do not have any kind of n-cycle or periodic orbits for $\frac{1}{N} < \alpha < N$, actually they are ergodic for this interval of parameter. Hence all n-cycles except for possible period one fixed points $x = 0$ and $x = 1$ are unstable, where for $\alpha \in \left[0, \frac{1}{N}\right]$, the fixed point $x = 0$ is stable in maps $x_N(n+1)$ (for odd integer values of N), while for $\alpha \in [N, \infty)$ the $x = 1$ is stable fixed point in the maps. We used their conjugate or isomorphic maps. Conjugacy means that the invertible map $h(x) = \frac{1-x}{x}$, maps $I = [0,1]$ into $[0,\infty)$ and transform maps $x_N(n+1)$ into $\tilde{x}_N(n+1)$ defined as:

$$\tilde{x}_N(n+1) = h \circ x_N(n+1) \circ h^{-1} = \frac{1}{\alpha^2} \tan^2(N \arctan \sqrt{x(n)}). \tag{2}$$

In this paper we used the hierarchy of chaotic map where we increase their domain to $[0,\infty)$ in order to improve the security by increasing the control parameter domain and freedom in choosing the initial conditions.

We have derived analytically their invariant measure for arbitrary values of the parameter α and every integer values of N [22]

$$\mu(x,\beta) = \frac{1}{\pi} \frac{\sqrt{\beta}}{\sqrt{x(1-x)}(\beta + (1-\beta)x)}, \quad \beta > 0. \tag{3}$$

We choose the parameter α in $x_N(n+1)$ in the following form:

$$\alpha = \frac{\sum_{k=0}^{\left[\frac{(N-1)}{2}\right]} C_{2k+1}^{N} \beta^{-k}}{\sum_{k=0}^{\left[\frac{N}{2}\right]} C_{2k}^{N} \beta^{-k}}, \tag{4}$$

where the symbol [] means the greatest integer part. By considering the invariant measure, we have analytically calculated the Kolmogorov–Sinai (KS) entropy of these maps (see for more details [22]):

$$h_{ks}(\mu, x_N) = \int \mu(x)\,\mathrm{d}x \ln\left|\frac{\mathrm{d}}{\mathrm{d}x} x_N\right| = \ln\left(\frac{N(1+\beta+2\sqrt{\beta})^{N-1}}{\left(\sum_{k=0}^{\left[\frac{N}{2}\right]} C_{2k}^{N} \beta^{k}\right)\left(\sum_{k=0}^{\left[\frac{N-1}{2}\right]} C_{2k+1}^{N} \beta^{k}\right)}\right). \tag{5}$$

2.2. *Two-dimensional coupled map*

We could create the internal coupled map by using the hierarchy of families of one-parameter chaotic maps (2) as follows:

$$\Phi_{N_1,N_2}(\tilde{x}_1, \tilde{x}_2) = \begin{cases} \tilde{x}_1(n+1) = \frac{1}{\alpha_1^2(x_2(n))} \tan^2(N_1 \arctan \sqrt{x_1(n)}), \\ \tilde{x}_2(n+1) = \frac{1}{\alpha_2^2} \tan^2(N_2 \arctan \sqrt{x_2(n)}), \end{cases} \tag{6}$$

where they was coupled through salve map control parameter α:

$$\alpha_N(\tilde{x}(n)) = \frac{B_N\left(\frac{1}{\beta(\tilde{x}(n))}\right)}{A_N\left(\frac{1}{\beta(\tilde{x}(n))}\right)} \sqrt{\frac{\beta(\tilde{x}(n+1))}{\beta(\tilde{x}(n))}}, \quad \beta(\tilde{x}(n)) = (\sqrt{\beta_0} + \epsilon \tilde{x}(n))^2. \tag{7}$$

Now with respect to N one could expand β_0 and control parameter of slave map in respect to the control parameter of master map (for more detail refer to [22,23]). As an illustration we give:

$$\Phi_{2,2}(\tilde{x}_1, \tilde{x}_2) = \begin{cases} \tilde{x}_1(n+1) = \frac{1}{\alpha_1^2(x_2(n))} \tan^2(2 \arctan \sqrt{x_1(n)}), \\ \tilde{x}_2(n+1) = \frac{1}{\alpha_2^2} \tan^2(2 \arctan \sqrt{x_2(n)}) \end{cases} \tag{8}$$

with

$$\alpha_1(x_2(n)) = \frac{2\beta(x_2(n))}{1+\beta(x_2)(n)}\sqrt{\frac{\beta(x_2(n+1))}{\beta(x_2(n))}}, \quad \beta(x(n)) = \left(\sqrt{\frac{\alpha_1}{2-\alpha_1}} + \epsilon x(n)\right)^2.$$

As it is proved [23] the invariant measure $\mu_{\Phi_{N_1,N_2}}(x_1,\ x_2)$ has the following form:

$$\frac{1}{\pi}\frac{\sqrt{\beta_2}}{\sqrt{x_2(1-x_2)}(\beta_2+(1-\beta_2)x_2)} \times \frac{1}{\pi}\frac{\sqrt{\beta_1(x_2)}}{\sqrt{x_1(1-x_1)}(\beta_1(x_2)+(1-\beta_1(x_2))x_1)} \tag{9}$$

with $\beta_2 > 0$ and $\beta_1(x) > 0$ given in (4).

KS-entropy for heirarchy of introduced coupled map in respect to invariant measure calculated and the result presented in our previous paper [23].

3. Proposed algorithm based on coupled map

In this section, a chaotic cryptosystem is presented. The proposed cryptosystem is a symmetric key block cipher algorithm in which chaotic Coupled maps are used along with a single chaotic map. A positive way to describe the key space might be in term of positive Lyapunov exponents. Since it was proved that the introduced map has invariant measure according the Bikhof ergodic theorem one could use the equally the KS-entropy and Lyapunov exponents [30]. Now refereing to analytically calculated KS-entropy, we select a suitable control parameters domain at chaotic maps for the key space (see Figs. 1(a) and (b)). Fig. 2 shows the block diagram of the chaotic encryption algorithm. The system consists of a chaotic coupled map and a single chaotic map. First, image $I_{m\times n}$ is transformed into matrix $M_{(m\times n)\times 1}$ and then this matrix is encrypted using results of iteration of chaotic coupled map and the third map. Using the initial condition and control parameters of the coupled map, the coupled map is iterated and then using a function of new $\tilde{x}_1(n+1)$ and $\tilde{x}_2(n+1)$ initial condition for the third map is made. Then the third map is iterated once and C_i is generated using.

$$C_i = M_i XOR(\tilde{x}_3(n+1) \times 10^{14} \bmod 256).$$

Then initial condition of $\tilde{x}_2(n+1)$ and coupling parameter (ϵ) are generated using a function of C_i and $\tilde{x}_3(n+1)$. This process continues up to $M_{m\times n}$. Then $M_{m\times n}$ is set equal to $C_{m\times n}$ and the whole process is repeated for the new M from the last element to the first one and new matrix C is the output as the ciphertext. The decryption procedure is similar to that of encryption process illustrated above with reverse of cipher text as input instead of plain text in the encryption procedure. Since both decryption and encryption procedures have similar structure, they have essentially the same algorithmic complexity and time consumption.

In this scheme the coupling parameter of the coupled map and initial condition of the third map are changed in each round and also they are sensitive to plaintext, so that the change of a pixel in the plaintext causes a completely different cipher text. In every step control parameters change in the $\tilde{x}_1(n+1)$. If we assume that attacker can find control parameters of $\tilde{x}_2(n+1)$ then parameters of $\tilde{x}_1(n+1)$ may be detected too. To solve this problem the coupling parameter was related to the third map. As example in this paper we select the following maps from the hierarchy of chaotic maps.

$$\Phi_{2,3}(\tilde{x}_1,\tilde{x}_2) = \begin{cases} \tilde{x}_1(n+1) = \frac{1}{\alpha_1^2(x_2(n))}\tan^2(2\arctan\sqrt{x_1(n)}), \\ \tilde{x}_2(n+1) = \frac{1}{\alpha_2^2}\tan^2(3\arctan\sqrt{x_2(n)}) \end{cases} \tag{10}$$

with

$$\alpha_1(x_2(n)) = \frac{2\beta(x_2(n))}{1+\beta(x_2)(n)}\sqrt{\frac{\beta(x_2(n+1))}{\beta(x_2(n))}},$$

$$\beta(x(n)) = \left(\sqrt{\frac{\alpha_1}{2-\alpha_1}} + \epsilon x(n)\right)^2. \tag{11}$$

The last part of encryption follows by:

$$\tilde{x}_3(n+1) = \frac{1}{\alpha_3^2}\tan^2(10\arctan\sqrt{x_3(n)}). \tag{12}$$

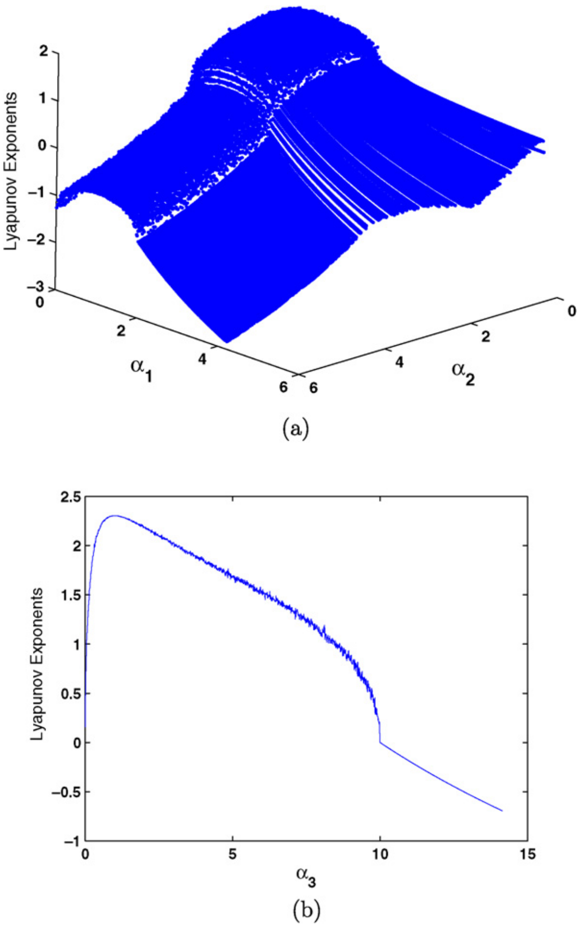


Fig. 1. Lyapunov exponents: (a) $\Phi_{2,3}(\tilde{x}_1, \tilde{x}_2)$ vs. α_1 and α_2, (b) $\tilde{x_3}(n+1)$ vs. α_3.

4. Experimental results

In this section, some experiments have been done to evaluate the performance of the proposed algorithm. Experimental analysis of the new algorithm presented in this paper has been done with "Barbara" image. Fig. 3(a) is the 256 grey-scale Barbara plain-image of size 256 × 256. Fig. 3(b) is it's encrypted image with the encryption key. For example encryption keys are chosen as follows, first we choose $\alpha_2 = 1.5$ and substitute $\alpha_1 = 1.2$ in Eq. (11) and the encryption process continues by choosing $\alpha_3 = 3$. It should be mentioned that the initial conditions are $\tilde{x}_1(0) = 2$, $\tilde{x}_2(0) = 33$.

The performed experiments were done on a 2.4 GHz Intel celeron Pentium(IV), 256 Mb memory and 80 Gb hard-disk capacities. Another important feature, we observe that decryption/encryption processes duration is less than 0.2 s.

As regard the obtained results, it can be seen that the decrypted image is clear and correct without any distortion. So it can be concluded that the chaotic encryption algorithm is sensitive to the key, it should be pointed out that a small change of the key would generate a completely different decryption result. For the proposed scheme, the corresponding ciphertext is the same size as the plaintext.

With a statistical analysis of 'Barbara' image and its encrypted image, their grey-scale histograms are given in Figs. 4(a) and (b). Fig. 4(b) shows uniformity in distribution of grey-scale of the encrypted image.

5. Security analysis

The crucial measure for the quality of a cryptosystem is its capability to withstand the attempts of an unauthorized participant-an opponent-to gain knowledge about the unencrypted information. This measure is called security. The

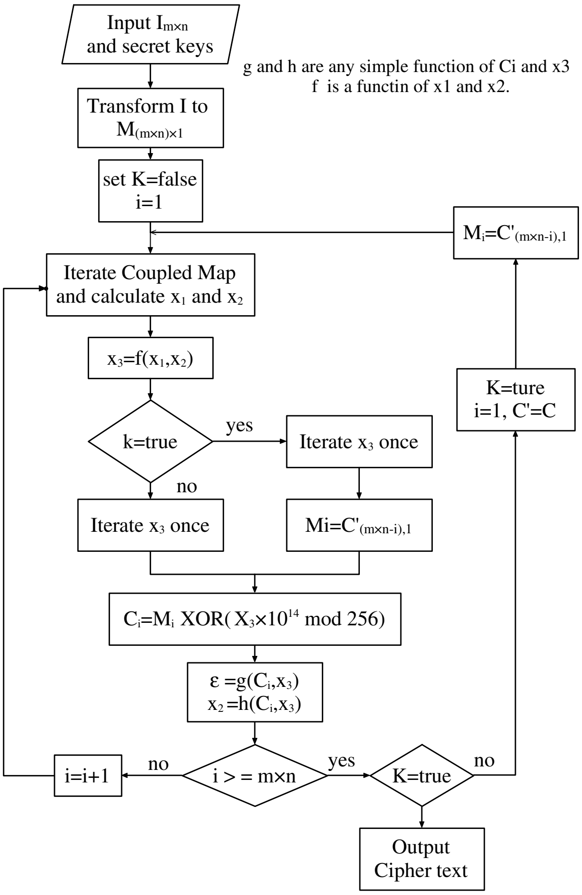
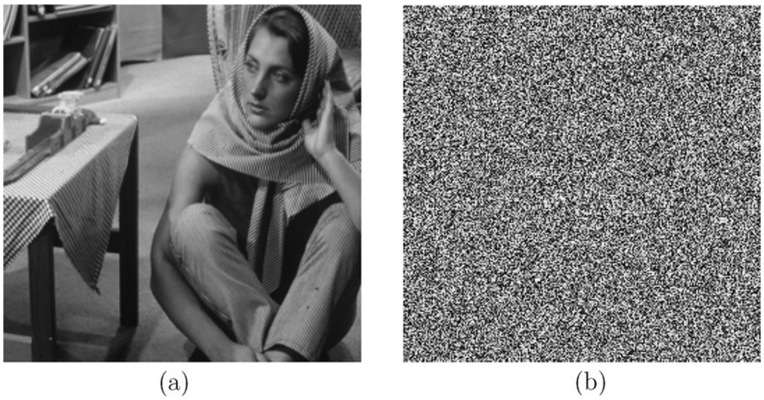


Fig. 2. Block diagram.


(a)

(b)

Fig. 3. (a) Plain-image. (b) Ciphered image.

discussion of the security for discrete-value cryptosystems is based on a model which was first introduced by Shannon [31] and was extended later by others. In this section the security analysis as follows: Key space analysis, Information entropy, Correlation analysis of two adjacent pixels and Differential attack.

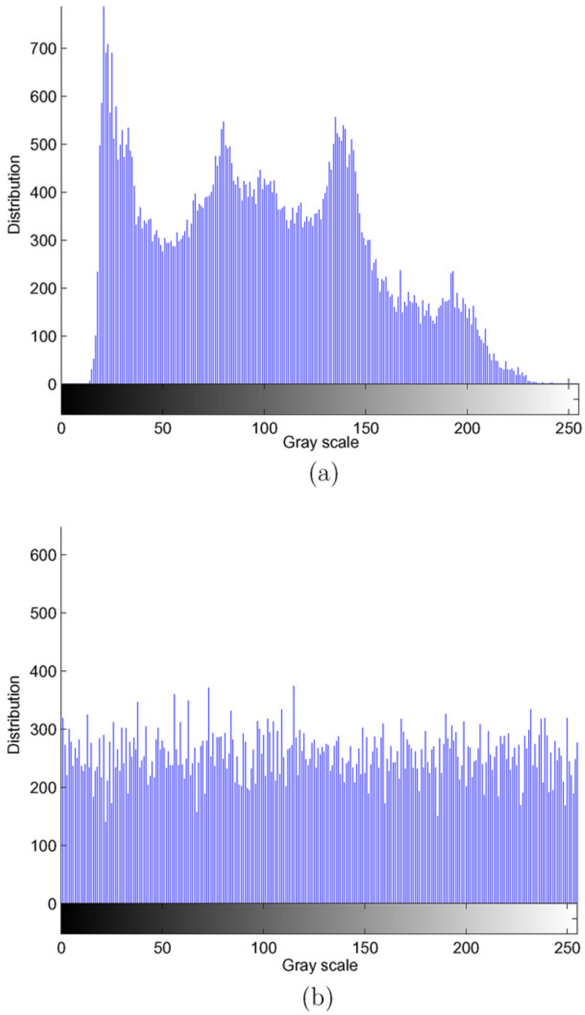


Fig. 4. (a) Histogram of plain-image. (b) Histogram of ciphered-image.

5.1. Key space analysis

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. If the precision is 10^{-14}, the key space size for initial conditions and control parameters is over than 2^{260}. Apparently, the key space is large enough to resist all kinds of brute-force attacks.

5.2. Information entropy

Information theory is the mathematical theory of data communication and storage founded in 1949 by Claude E. Shannon [32]. Modern information theory is concerned with error-correction, data compression, cryptography, communications systems, and related topics.

To calculate the entropy $H(m)$ of a source m, we have:

$$H(m) = \sum_{i=0}^{2N-1} P(m_i)\log_2 \frac{1}{P(m_i)}, \tag{13}$$

where $p(m_i)$ represents the probability of symbol mi and the entropy is expressed in bits. Let us suppose that the source emits 2^8 symbols with equal probability, i.e., $m = \{m_1, m_2, \ldots, m_{2^8}\}$. After evaluating Eq. (13), we obtain its entropy

$H(m) = 8$, corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

Let us consider the ciphertext of image encryption using the proposed algorithm, the number of occurrence of each ciphertext block is recorded and the probability of occurrence is computed. The entropy is as follows:

$$H(m) = \sum_{i=0}^{255} P(m_i) \log_2 \frac{1}{P(m_i)} = 7.9968 \approx 8.$$

The value obtained is very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the encryption system is secure upon the entropy attack.

5.3. Correlation analysis of two adjacent pixels

The superior confusion and diffusion properties are shown by a test on the correlations of adjacent pixels in the ciphered image [17]. To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels, respectively, in a ciphered image, the following procedure was carried out. 1000 pairs of two adjacent (in vertical, horizontal, and diagonal direction) pixels from plain-image and ciphered image were randomly selected and the correlation coefficients were calculated by using the following two formulas:

$$\mathrm{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \tag{14}$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{15}$$

where x and y represent grey-scale values of two adjacent pixels in the image. In numerical computation, the following discrete formulas were used:

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i, \tag{16}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2. \tag{17}$$

Fig. 5 shows the correlation distribution of the two horizontally adjacent pixels in the plain-image and in the cipher image: the correlation coefficients are 0.9574 and 0.0038, respectively, which are far apart. Similar results for diagonal and vertical directions were obtained, which are shown in Table 1.

5.4. Differential attack

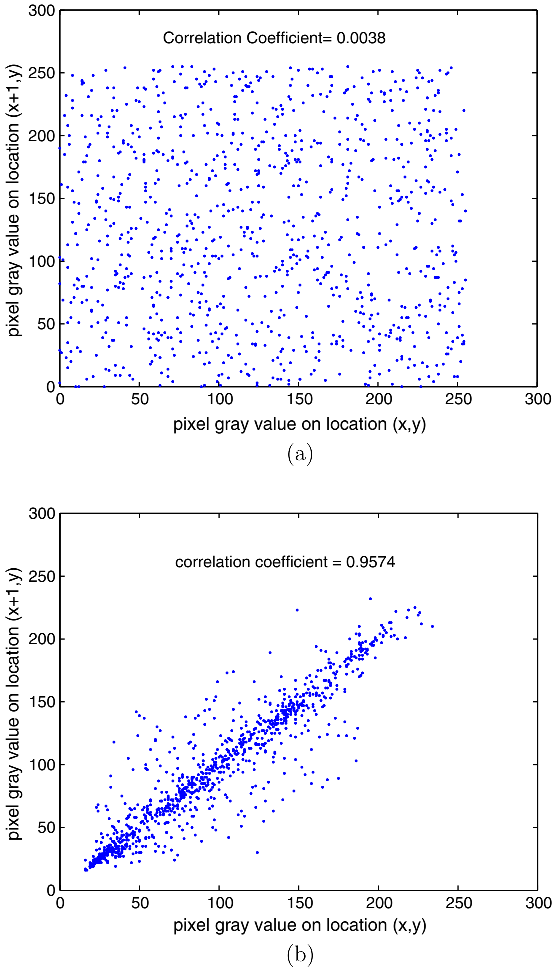
To test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, two common measures were used: NPCR and UACI [17]. NPCR means the change rate of the number of pixels of ciphered image while one pixel of plain-image is changed. UACI which is the unified average changing intensity, measures the average intensity of the differences between the plain-image and ciphered image.

Denote two cipher-images, whose corresponding plain-images have only one-pixel difference, by C_1 and C_2, respectively. Label the grey-scale values of the pixels at grid (i,j) of C_1 and C_2 by $C_1(i,j)$ and $C_2(i,j)$, respectively. Define a bipolar array, D, with the same size as image C_1 or C_2. Then, $D(i,j)$ is determined by $C_1(i,j)$ and $C_2(i,j)$, namely, if $C_1(i,j) = C_2(i,j)$ then $D(i,j) = 1$; otherwise, $D(i,j) = 0$.

NPCR and UACl are defined by the following formulas:

$$\mathrm{NPCR} = \frac{\sum_{ij} D(i,j)}{W \times H} \times 100\%, \tag{18}$$

$$\mathrm{UACI} = \frac{1}{W \times H} \left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\%, \tag{19}$$



(a)

(b)

Fig. 5. Correlations of two horizontally adjacent pixels in the plain-image and in the cipher-image: (a) Correlation analysis of plain-image. (b) Correlation analysis of cipher-image.

Table 1
Correlation coefficients of two adjacent pixels in two images

	Plain image	Ciphered image
Horizontal	0.9574	0.0038
Vertical	0.9399	0.0023
Diagonal	0.9183	0.0004

where W and H are the width and height of C_1 or C_2. Tests have been performed on the proposed scheme, about the one-pixel change influence on a 256 grey-scale image of size 256×256. We obtained $\mathrm{NPCR} = 0.41962\%$ and $\mathrm{UCAI} = 0.3325\%$. The results show that a swiftly change in the original image will result in a significant change in the ciphered image, so the algorithm proposed has a good ability to anti differential attack.

6. Summary and conclusion

In this paper, a way of improving the security of chaos-based cryptosystem is proposed, using a hierarchy of one dimensional chaotic maps and their coupling, which can be viewed as a high dimensional dynamical system, which it belongs to interval $[0,\infty)$ [22,23]. These maps, which are defined as ratios of polynomials of degree N, have interesting features such as invariant measure, ergodicity, capability of calculation KS-entropy and variable control parameters in the two interval: $\left[\frac{1}{N},N\right]$ for odd N and $[0,N]$ for even N [23].

The general concept proposed in this paper appears quite robust. One of the main motivations for using coupled chaotic map along with a chaotic map as a cryptosystem used coupling parameter (ϵ) is to achieve some computational goal. Beside coupling parameter was used as connection between coupled map and third map. A complete description of the algorithm, security properties, performance and implementation aspects were given before. We introduce the mixture mechanism of chaotic maps, which enhance the key space and security of algorithm. In regard to the tight relationship between cryptography and chaos theory and two general principles which leads to the design of good cryptosystems, diffusion and confusion [32], and with respect to partitioning of the state space which turns the deterministic chaotic system into an ergodic information source that can be analyzed in terms of information theory. The source tends to become stationary for mixing maps, in this case every initial measure, leads to the ergodic invariant measure. Therefore, mixing maps are good candidates for encryption algorithms because both diffusion and confusion are their immanent properties. The proposed algorithm presented several interesting features, such as a high level of security, large enough key space, pixel distributing uniformity and an acceptable encryption speed. Besides the fast encryption speed, production of the ciphertext has same size as its corresponding plaintext. The algorithm has been successfully applied to and tested for the image encryption. Although the algorithm presented in this paper has focused on image encryption, it is not just limited to this area and can be widely applied in the secure transmission of confidential information over the Internet. It can be seen from the results that the proposed system offers a higher complexity. The high complexity of such chaotic dynamics indicates that they could be advantageously used in chaotic cryptographic techniques with enhanced security. According to the results obtained using our cryptosystem, encryption with this algorithm seems to be more efficient than other methods, as it develops security of such systems. Hence it seems that they could be helpful to reduce or even overcome cryptographical weaknesses of chaotic cryptosystems. As a conclusion, we have used in the present algorithm only two prototype of the hierarchy of one-dimensional chaotic maps (one dimensional chaotic map and their coupling). Apparently, it can be easily used for any mixing of 1D chaotic maps with 2D coupled chaotic maps. It seems that, the triple of such one dimensional maps may increase the security of cryptosystem in compared to the proposed cryptosysytem. Also this algorithm is suggested in serious applications that requires a high level of security.

Appendix A. Derivation of entropy of coupled chaotic maps

The KS-entropy of $\Phi_{2,2}$ given in (8) can be written as

$$h(\tilde{\mu},\tilde{\Phi}_{2,2}) = \int_0^\infty \tilde{\mu}(x_1)\,\mathrm{d}x_1 \int_0^\infty \tilde{\mu}(x_2)\,\mathrm{d}x_2 \left(\ln\left|\frac{\partial\tilde{x}_1(n+1)}{\partial x_1(n)}\right| + \ln\left|\frac{\partial\tilde{x}_2(n+1)}{\partial x_2(n)}\right|\right) \tag{A.1}$$

or

$$\begin{aligned} h(\tilde{\mu},\tilde{\Phi}_{2,2}) &= \int_0^\infty \tilde{\mu}(x_1)\,\mathrm{d}x_1 \int_0^\infty \tilde{\mu}(x_2)\,\mathrm{d}x_2,\\ \ln&\left|\frac{\partial}{\partial x_1}\left(\frac{1}{\alpha_1^2(x_2(n))}\tan^2(2\arctan\sqrt{x_1(n)})\right)\right| + \ln\left|\frac{\partial}{\partial x_1}\left(\frac{1}{\alpha_2^2}\tan^2(2\arctan\sqrt{x_2(n)})\right)\right|, \end{aligned}$$

where the measure $\tilde{\mu}$ related to the measure μ to the following relation:

$$\tilde{\mu}(x) = \frac{1}{(1+x)^2}\mu\left(\frac{1}{1+x}\right).$$

The first integral by substituting $\alpha_1(x_2(n))$ and $\beta(x(n))$ and change of variable $x=\frac{1}{\beta}\tan^2(\theta)$ reduces to:

$$\begin{aligned} &= \frac{2}{\pi}\int_0^{\frac{\pi}{2}} \mathrm{d}\theta \left(\ln\left(\frac{\alpha_2(2\alpha_1+1)}{(\alpha_1+1)(\alpha_2+1)}+\epsilon\right) + \left(\frac{\alpha_2(2\alpha_1+1)}{(\alpha_1+1)(\alpha_2+1)}+\epsilon\right)\cos\theta)\right)\\ &\quad\times\ln\left(\frac{\alpha_2}{\alpha_2+1}+\frac{\alpha_2}{\alpha_2+1}\cos\theta\right) + \ln\left(\frac{3}{4}+\cos\theta+\frac{1}{4}\cos 2\theta\right) + \ln(A+B\cos\theta+C\cos 2\theta)\Bigg), \end{aligned}$$

which

$$\begin{cases} A = \frac{1}{8}(3(\frac{2\alpha_1+1}{\alpha_1+1}) + \frac{2\epsilon(\alpha_2+1)}{\alpha_2}\sqrt{\frac{\alpha_1}{\alpha_1+1}} + 3\left(\frac{\epsilon(\alpha_2+1)}{\alpha_2}\right)^2), \\ B = \frac{1}{2}\left(1 + \frac{\alpha_1}{\alpha_1+1} - \left(\frac{\epsilon(\alpha_2+1)}{\alpha_2}\right)^2\right), \\ C = \frac{1}{8}\left(\frac{2\alpha_1+1}{\alpha_1+1} + \frac{2\epsilon(\alpha_2+1)}{\alpha_2}\sqrt{\frac{\alpha_1}{\alpha_1+1}} + \left(\frac{\epsilon(\alpha_2+1)}{\alpha_2}\right)^2\right). \end{cases}$$

The above expression can be calculated by using the following integral:

$$\frac{1}{\pi}\int_0^{2\pi} \mathrm{d}\theta \ln(A + B\cos\theta + C\cos 2\theta) = 2\ln\Delta,$$

$$\Delta = \frac{1}{\pi}\left(\frac{\sqrt{A - 3C + \sqrt{(A+C)^2 - B^2}}}{2} + \frac{\sqrt{A+B+C} - \sqrt{A-B+C}}{2}\right).$$

where the above integral has been evaluated by using the well known mean values theorem of analytic function

$$\frac{1}{\pi}\int_0^{2\pi} \mathrm{d}\theta \ln|f(z_0 + R\mathrm{e}^{\mathrm{i}\theta})| = |f(z_0)|$$

by choosing $f(z) = \alpha + \beta\mathrm{e}^{\mathrm{i}\theta} + \gamma\mathrm{e}^{2\mathrm{i}\theta}$. Now the first part of integral (A.1) reads:

$$= \int_0^\infty \tilde{\mu}(x_1(n))\mathrm{d}x_1(n)\int_0^\infty \tilde{\mu}(x_2(n))\mathrm{d}x_2(n)\ln\left(\left|\frac{2}{\alpha_2^2}\cdot\frac{1}{\sqrt{x_2(n)}(1+x_2(n))}\cdot\frac{\sin 2(\arctan\sqrt{x_2(n)})}{\cos^3 2(\arctan\sqrt{x_2(n)})}\right|\right)$$

with the same change of variable in second part integral (A.1) and by considering:

$$\frac{1}{\pi}\int_0^{\pi} \ln|a + b\cos\theta| = \begin{cases} \ln\left|\frac{a+\sqrt{a^2-b^2}}{2}\right|, & |a| > |b|, \\ \ln\left|\frac{b}{2}\right|, & |a| \leqslant |b|. \end{cases}$$

This part of integrals is taken:

$$\ln\left(\frac{1 + \frac{\alpha_2}{\alpha_2+1} + 2\frac{\alpha_1}{\alpha_2+1}}{1 + \frac{\alpha_2}{\alpha_2+1}}\right).$$

Now, combining it's results:

$$\ln\left(\frac{1 + \frac{\alpha_2}{\alpha_2+1} + 2\frac{\alpha_1}{\alpha_2+1}}{1 + \frac{\alpha_2}{\alpha_2+1}}\right) + \ln\frac{\left(\sqrt{1 + \sqrt{\frac{\alpha_1}{\alpha_1+1}}} + \sqrt{\frac{\epsilon}{\frac{\alpha_2}{\alpha_2+1}}}\right)^4}{\left(\sqrt{1 + \frac{\alpha_1}{\alpha_1+1}} + \frac{\epsilon}{\frac{\alpha_2}{\alpha_2+1}} + \sqrt{\frac{2\epsilon\sqrt{\frac{\alpha_1}{\alpha_1+1}}}{\frac{\alpha_2}{\alpha_2+1}} + \frac{2\epsilon}{\frac{\alpha_2}{\alpha_2+1}}\sqrt{1 + \frac{\alpha_1}{\alpha_1+1}}}\right)^2}.$$

References

[1] Hao B. Starting with parabolas: an introduction to chaotic dynamics. Shanghai China: Shanghai Scientific and Technological Education Publishing House; 1993.

[2] Brown R, Chua LO. Clarifying chaos: examples and counterexamples. Int J Bifurcat Chaos 1996;6(2):219–42.

[3] Fridrich J. Symmetric ciphirs based on two-dimensional chaotic maps. Int J Bifurcat Chaos 1998;8(6):1259–84.

[4] Pecora LM, Carroll TL. Synchronization in chaotic systems. Phys Rev Lett 1990;64:821–4.

[5] Feki M. An adaptive chaos synchronization scheme applied to secure communication. Chaos, Solitons & Fractals 2003;18:141–8.

[6] Parlitz U, Chua LO, Kocarev L, Halle KS, Shang A. Transmission of digital signals by chaotic synchronization. Int J Bifurcat Chaos 1992;2:973–7.

[7] Morgul O, Feki M. A chaotic masking scheme by using synchronized chaotic systems. Phys Lett A 1999;251:169–76.

[8] Cuomo KM, Openheim AV. Circuit implementation of synchronized chaos with applications to communications. Phys Rev Lett 1993;71:65–8.

[9] Chen JY, Wong KW, Cheng LM, Shuai JW. A secure communication scheme based on the phase synchronization of chaotic systems. Chaos 2003;13:508–14.

[10] Xiao D, Liao X, Wong K. An efficient entire chaos-based scheme for deniable authentication. Chaos, Solitons & Fractals 2005;23:1327–31.

[11] Tang G, Liao X, Chen Y. A novel method for designing S-boxes based on chaotic maps. Chaos, Solitons & Fractals 2005;23:413–9.

[12] Xiang T, Liao X, Tang G, Chen Y, Wong KW. A novel block cryptosystem based on iterating a chaotic map. Phys Lett A 2006;349:109–15.

[13] Lü H, Wang S, Li X, Tang G, Kuang J, Ye W, et al. A new spatiotemporally chaotic cryptosystem and its security and performance analyses. Chaos 2004;14:617–29.

[14] Huang F, Guan ZH. Cryptosystem using chaotic keys. Chaos, Solitons & Fractals 2005;23:851–5.

[15] Lee PH, Pei SC, Chen YY. Generating chaotic stream ciphers using chaotic systems. Chin J Phys 2003;41:559–81.

[16] Baptista MS. Cryptography with chaos. Phys Lett A 1998;240:50–4.

[17] Chen G, Mao Y, Chui C. A symmetric image encryption scheme based on 3d chaotic cat maps. Chaos, Solitons & Fractals 2004;21:749–61.

[18] Kocarev L. Chaos-based cryptography: a brief overview. IEEE Circ Syst 2001;1:6–21.

[19] Parker AT, Short KM. Reconstructing the keystream from a chaotic encryption scheme. IEEE Trans Circuits Syst I 2001;48(5):104–12.

[20] Zhou ChS, Lai CH. Extracting messages masked by chaotic signals of time-delay systems. Phys Rev E 1999;60:320–3.

[21] Dachselt F, Schwarz W. Chaos and cryptography. IEEE Trans Circuits Syst 2001;48(12):1498–509.

[22] Jafarizadeh MA, Behnia S, Khorram S, Nagshara H. Hierarchy of chaotic maps with an invariant measure. J Stat Phys 2001;104(516):1013–28.

[23] Jafarizadeh MA, Behnia S. Hierarchy of chaotic maps with an invariant and their coupling. Physica D 2001;159:1–21.

[24] Li Wentian. Phenomenology of non-local cellular automata. J Stat Phys 1992;68:829.

[25] Cosenza MG, Parravano A. Dynamics of coupling functions in globally coupled maps: Size, periodicity, and stability of clusters. Phys Rev E 2001;64:036224.

[26] dos Santosa AM, Vianaa RL, Lopesa SR, Pintob SE de S, Batista AM. Chaos synchronization in a lattice of piecewise linear maps with regular and random couplings. Physica A 2005.

[27] Monteb S, Dovidioc F, Chate H, Mosekildea E. Effects of microscopic disorder on the collective dynamics of globally coupled maps. Physica D 2005;205:25–40.

[28] Coca D, Billings SA. Analysis and reconstruction of stochastic coupled map lattice models. Phys Lett A 2003;315:61–75.

[29] Devancy RL. An introduction to chaotic dynamical systems. Addison Wesley; 1982.

[30] Keller G. Equilibrium states in a ergodic theory. Cambridge University Press; 1998. p. 23–30.

[31] Shannon CE. A mathematical theory of communication. Bell Syst Tech J 1948;27(3):379–423, 623–56.

[32] Shannon CE. Communication theory of secrecy systems. Bell Syst Tech J 1949;28:656–715.