A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps

S. Behnia a,⁎, A. Akhshani a, S. Ahadpour b,c, H. Mahmodi a, A. Akhavan d

a Department of Physics, IAU, Urmia, Iran
b Department of Theoretical Physics and Astrophysics, Tabriz University, Iran
c Department of Physics, Mohaghegh Ardabili University, Iran
d Department of Engineering, IAU, Urmia, Iran

Received 5 October 2006; received in revised form 10 January 2007; accepted 10 January 2007
Available online 21 February 2007
Communicated by C.R. Doering

Abstract

In recent years, a growing number of discrete chaotic cryptographic algorithms have been proposed. However, most of them encounter some problems such as the lack of robustness and security. In this Letter, we introduce a new image encryption algorithm based on one-dimensional piecewise nonlinear chaotic maps. The system is a measurable dynamical system with an interesting property of being either ergodic or having stable period-one fixed point. They bifurcate from a stable single periodic state to chaotic one and vice versa without having usual period-doubling or period-n-tupling scenario. Also, we present the KS-entropy of this maps with respect to control parameter. This algorithm tries to improve the problem of failure of encryption such as small key space, encryption speed and level of security.

© 2007 Elsevier B.V. All rights reserved.

PACS: 05.45.+b

Keywords: Chaos; Chaotic cryptosystems; Piecewise nonlinear chaotic maps; Image encryption; Security

1. Introduction

In recent years, extensive studies have been done in the theory of chaos in different fields of physics, engineering, biology, and economics as well [1]. Chaotic systems are characterized by ergodicity, sensitive dependent on initial conditions and random-like behaviors. These properties are of great importance in diffusion and confusion processes [2]. There are two main approaches of designing chaos-based cryptosystems; analog mode [3,4] and digital mode [5–7]. Most commonly employed encryption and security schemes are digital in nature since present communication systems are becoming entirely digital. This Letter aims to discuss digital cryptosystems. Many different chaotic systems like Logistic map and piecewise linear chaotic maps have been used to construct chaotic cryptosystems. These are in fact the simplest chaotic systems. In recent years, many algorithms based on Logistic map [8–10], piecewise linear maps [11–13] and piecewise nonlinear maps [14] have been proposed. Piecewise linear chaotic maps have perfect dynamical properties and can be realized simply in both hardware and software, so. They are widely used in digital chaotic ciphers [15,16]. Although one-dimensional chaotic system has the advantages of high-level efficiency and simplicity [17], there are fundamental drawbacks in this chaotic cryptosystem, such as small key space, slow performance speed and weak security function [18–21].

To address some of the weak points of piecewise linear chaotic maps (like Tent map), we introduce a new class of piecewise nonlinear chaotic maps. In our introduced model of piecewise nonlinear chaotic maps, in addition to the initial condition and control parameter, there is also another parameter namely probability. It seems that the inclusion of more than two parameters increases the confusion and diffusion in the encryption process resulting in a more secure cryptosystem due to the fact that more confusion in encryption makes cryptosystem more secure. Also, in order to improve the security of
cryptosystem, we change the probability parameter of nonlinear piecewise chaotic maps by attaching it to the additional trigonometric chaotic maps [22]. Moreover, the existence of two parameters of the trigonometric chaotic map, besides parameters of piecewise chaotic maps, has increased the size of key space.

2. Encryption algorithm based on piecewise nonlinear chaotic maps

We first present a brief review of one-parameter families of piecewise nonlinear chaotic maps with an invariant measure. These maps can be defined as [23]

\[ \Phi(x, \alpha) = \frac{a^2 F}{1 + (a^2 - 1) F}, \quad (1) \]

where

\[ F = \begin{cases} \frac{a}{p}, & 0 \leq x \leq p, \\ \frac{a - x}{1 - p}, & p < x \leq 1, \end{cases}, \quad p \in [0, 1]. \quad (2) \]

The corresponding invariant measure is (a similar calculation has been presented in [23])

\[ \mu(x, \alpha, p) = \frac{1}{\ln(\frac{1 - p}{a - p})} \cdot \frac{1}{(\alpha - p) + (1 - \alpha)x}, \quad \alpha > p. \quad (3) \]

One can calculate the KS-entropy by considering the invariant measure Eq. (3) which leads to [23–25]

\[ h_{KS} = \frac{1}{\ln(\frac{1 - p}{a - p})} \left[ \ln(ap) \ln \left( \frac{\alpha(1 - p)}{\alpha - p} \right) \right. \]

\[ - 2 \left[ \ln(ap) \ln(1 - p) - \ln p \ln \left( \frac{\alpha - p}{\alpha} \right) \right. \]

\[ + \frac{1}{\ln}\left( \frac{1 - p}{1 - p} - \frac{\alpha}{\alpha - p} \right) \ln(1 - p) \ln \left( \frac{1 - p}{\alpha(1 - p)} \right) \]

\[ - \left[ \ln^2(1 - p) - \ln^2(\alpha(1 - p)) \right] \right]. \]

In the proposed algorithm, two chaotic maps are employed to achieve the goal of image encryption.

To apply our proposed encryption, initially the plaintext \( M_{n \times n} \) is transformed into \( M_{n \times n} \times 1 \). Then, the probability parameter of the piecewise nonlinear chaotic maps \( p \) is generated by using the results of iteration of the trigonometric map Eqs. (4) and (5). As an example, we may consider the following equations [22,23]:

\[ \bar{x}_1(n + 1) = \frac{1}{a_1} \tan^2 \left( N \arctan \sqrt{x_1(n)} \right) \quad \text{while } N = 10, \quad (4) \]

\[ p = \begin{cases} x_1, & 0 < x_1 < 1, \\ \frac{1}{x_1}, & x_1 > 1. \end{cases} \quad (5) \]

Now, by considering Eq. (2), the piecewise maps are defined as

\[ \Phi(x_2, \alpha_2, p) = \begin{cases} \frac{a_2^2 \{ \frac{1}{\alpha_2} \}}{1 + (a_2^2 - 1) \left( \frac{1}{\alpha_2} \right)}, & 0 \leq x_2 \leq p, \\ \frac{a_2^2 \{ \frac{-a_2^2 - 1}{\alpha_2} \}}{1 + (a_2^2 - 1) \left( \frac{-a_2^2 - 1}{\alpha_2} \right)}, & p < x_2 \leq 1. \end{cases} \quad (6) \]

The generated \( M_{1 \times 1} \) matrix is then encrypted by using the introduced piecewise maps Eq. (6).

\[ C_1 = \left( \left[ x_2 \times 10^{14} \right] \mod 256 \right) \hat{\odot} M_{1 \times 1}. \]

Note that \( x_2 \) is, in fact, the result of iteration of the piecewise nonlinear chaotic maps. At the next step, the trigonometric map parameters \( x_1 \) and \( \alpha_1 \) are both modified by using simple functions \( f \) and \( g \) with parameters \( C_1 \) and \( x_2 \). The decryption process is almost the same as the encryption but with reverse steps (see Fig. 1).

The ciphertext is so sensitive to the plaintext that even a one-pixel change in the plaintext leads to a completely different ciphertext. The reason for this, is the existence of the diffusion in the cryptosystem. Diffusion refers, in fact, to rearrange or spread out the bits in the message. So, any redundancy in the plaintext is spread out over the ciphertext [26]. Some experiments are performed to study the diffusion and confusion properties [27]. In order to prove the claimed sensitivity to the plaintext, we may generate two plaintexts with just one pixel difference. Figs. 2(a) and (b) show the difference between two plaintexts and their corresponding ciphertexts. The difference between two ciphertexts, with a small change in their secret keys, is plotted in Figs. 2(c) and (d). Hence, the diffusion and confusion properties are confirmed. The parameters used are listed as follows:

(1) Difference in one of the initial conditions (Fig. 2(c)): \( x_1 = 9.8 \) changed to \( x_1 = 9.8000000000001 \).
3. Experimental results

Some experimental results are given to demonstrate the efficiency of our scheme which is based on the piecewise nonlinear chaotic maps. An indexed image of a ‘Boat’ sized 256 × 256 (see Fig. 3(a)) is used as a plain image and the encryption of this image is shown in Fig. 3(b). The encryption keys are chosen as follows. In trigonometric map, $x_1 = 9.8$, $\alpha_1 = 6.7$ and in piecewise nonlinear chaotic maps, $x_2 = 0.2$ and $\alpha_2 = 0.4$. We have used Visual C++ running program in a personal computer with a Pentium-IV 2.4 GHz Celeron, 256MB memory and 80GB hard-disk capacity. The average time used for encryption/decryption on 256 grey-scale images of size 256 × 256 is shorter than 0.05 s. Table 1 shows the test results of encryption/decryption speed on 256 grey-scale images of different sizes. It seems that the proposed algorithm is very fast compared to the other known block ciphers such as [28,29].

The ciphertext has the same size as the plaintext. The reason is that the cryptosystem maps bring about a one-to-one correspondence between plaintext and ciphertext. Moreover, the histogram of the encrypted image is nearly uniformly distrib-

### Table 1

<table>
<thead>
<tr>
<th>Image size (in pixels)</th>
<th>Proposed</th>
<th>Chen et al.</th>
</tr>
</thead>
<tbody>
<tr>
<td>256 × 256</td>
<td>0.046/0.046</td>
<td>&lt;0.4/&lt;0.4</td>
</tr>
<tr>
<td>512 × 512</td>
<td>0.23/0.23</td>
<td>1/1</td>
</tr>
<tr>
<td>1024 × 1024</td>
<td>0.953/0.953</td>
<td>3/3</td>
</tr>
<tr>
<td>2048 × 2048</td>
<td>3.89/3.89</td>
<td>14/14</td>
</tr>
</tbody>
</table>
uted, which makes statistical attacks difficult. The 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. In addition, the average pixel intensity and the intensity variance for plaintext is 135.75 and 321.99, and for ciphertext is 128.55 and 16.42, respectively.

4. Security analysis

Security is a major issue of a cryptosystem. In this section, a complete investigation is made on the security of the cryptosystem. We have tried to point out that this ciphertext is sufficiently secure against various cryptographical attacks, as shown below:

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 size of key space for initial conditions and control parameters is $2^{186}$. In addition, one attempt to describe the dynamics of the current system is by providing bifurcation diagram and determining interesting properties of it. In any case, the designer of any chaotic cryptosystem should conduct a study of chaotic regions of the parameter space from which valid keys, i.e., parameter values leading to chaotic behavior, can be chosen. Only keys chosen from the black region of bifurcation diagram are suitable enough [30,31]. In this cryptosystem, the interval of the initial condition of the trigonometric map and the piecewise nonlinear chaotic maps are respectively $[0, \infty)$ and $[0, 1]$. The bifurcation diagrams of the mentioned chaotic maps are given in Figs. 5 and 6. As we can see, within the black regions, there are not any periodic windows, so the entire black region is suitable for robust keys.

Information entropy. The entropy (such as KS-entropy, information entropy, ...) is the most outstanding feature of the randomness [33–35]. For this reason, in Section 2, the KS-entropy is presented. In this section information entropy is provided. Information theory is a mathematical theory of data communication and storage founded by Claude E. Shannon in 1949 [32]. There is a well-known formula for calculating this entropy:

$$H(S) = \sum_{i=0}^{2^n-1} P(s_i) \log \frac{1}{P(s_i)},$$

Fig. 5. Bifurcation diagram of $\tilde{x}_1(n + 1)$ while $N = 2$.

Fig. 6. Bifurcation diagram of $\Phi(x_2, \alpha_2, p)$ while $p = 0.1$. 

Fig. 4. (a) Histogram of plain image; (b) Histogram of ciphered image.
where $P(s_i)$ represents the probability of symbol $s_i$ and the entropy is expressed in bits. Actually, given that a real information source seldom transmits random messages, in general, the entropy value of the source is smaller than the ideal one. However, when these messages are encrypted, their ideal entropy should be 8. If the output of such a cipher emits symbols with an entropy of less than 8, then, there would be a possibility of predictability which threatens its security. The value obtained is very close to the theoretical value 8. This means that information leakage in the encryption process is negligible and the encryption system is secure against the entropy attack. Using the above-mentioned formula, we have got the entropy $H(S) = 7.9972$, for the source $S = 256$.

**Correlation of two adjacent pixels.** Statistical analysis has been performed on the proposed image encryption algorithm. This is shown by a test of the correlation between two adjacent pixels in plain image and ciphered image. We randomly select 1000 pairs of two-adjacent pixels (in vertical, horizontal, and diagonal direction) from plain images and ciphered images, and calculate the correlation coefficients [28], respectively by using the following two formulas (see Table 2 and Fig. 7(a) and (b)):

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

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

where

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

Here, $E(x)$ is the estimation of mathematical expectations of $x$, $D(x)$ is the estimation of variance of $x$, and $cov(x,y)$ is the estimation of covariance between $x$ and $y$, where $x$ and $y$ are grey-scale values of two adjacent pixels in the image.

**Differential attack.** Two common measures, NPCR and UACI, are used to test the influence of one-pixel change on the whole image encrypted by the proposed algorithm. NPCR stands for the number of pixels change rate while, one-pixel of plain image is changed. The unified average changing intensity (UACI) measures the average intensity of differences between the plain image and ciphered image. For calculation of NPCR and UACI, let us assume two ciphered images ($C_1$ and $C_2$) whose corresponding plain images have only one-pixel difference [36,37]. The grey-scale values of the pixels of the ciphered image $C_1$ and $C_2$ at grid $(i,j)$ are labeled as $C_1(i,j)$ and $C_2(i,j)$, respectively. Take 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 $C_2(i,j)$. So, if $C_1(i,j) = C_2(i,j)$ then $D(i,j) = 1$; otherwise, $D(i,j) = 0$.

NPCR and UACI are defined through the following formulas:

$$
\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%,
$$

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

where $W$ and $H$ are the width and height of $C_1$ or $C_2$. We have done some tests on the proposed scheme (256 grey-scale image of size $256 \times 256$) to find out the extent of change produced by one-pixel change in the plain image. We have obtained NPCR $= 0.46\%$ and UACI $= 0.39\%$. The results show that the proposed algorithm can survive differential attack.
5. Conclusion

In this Letter, a new scheme for image encryption based on piecewise nonlinear chaotic maps has been presented. These maps have advantages such as invariant measure, ergodicity and the possibility of KS-entropy calculation. In this scheme, we have investigated the potential use of both trigonometric chaotic maps and piecewise nonlinear chaotic maps as a reliable, secure, and a rapid encryption tool in cryptography. Note that chaotic cryptosystems are usually much slower than commercialized ones that do not depend on chaos. Both theoretical analysis and experimental results show that the proposed cryptosystem has a high security level. The aim of the proposed scheme is to obtain a higher security and a faster encryption speed. The obtained results have confirmed our proposed cryptosystem. Consequently, the light of the encouraging results of our experiments, we suggest that this encryption scheme is suitable for applications like Internet image encryption and secure transmission of confidential information in the Internet.

Acknowledgement

The authors would like to express their heartfelt gratitude to Mr. A. Bonyadi for the nice editing of their paper—this has certainly improved its readability.

References

[33] W. Li, Complex Syst. 5 (4) (1991) 381.