A NOVEL BLOCK CIPHER BASED ON HIERARCHY OF ONE-DIMENSIONAL COMPOSITION CHAOTIC MAPS

A. Akhshani∗

Department of Physics
IAU
Urmia-Iran

H. Mahmodi, A. Akhavan

Department of Physics
IAU
Urmia-Iran

ABSTRACT

In the past few years, a number of image encryption algorithms based on chaotic maps have been proposed. One dimensional chaotic system with the advantages of high-level efficiency and simplicity, has been widely used. But many of them essentially encounter with problems such as small key space and weak security. To overcome these drawbacks, we introduce a new method of image encryption based on Composition of Trigonometric Maps (CTMs). The proposed scheme utilises chaotic properties for image encryption via the chaotic composition maps. Experimental results show that the new cipher has satisfactory security with a large key space. It is practicable and reliable, with high potential to be adopted for Internet image encryption, transmission applications and other information security fields.

Index Terms-Chaos, Cryptography, Security.

1. INTRODUCTION

Chaos theory is established since 1970s from many different research areas, such as physics, mathematics, biology and chemistry, etc. Chaotic systems have many important properties, such as ergodicity, sensitive dependence on initial conditions, control parameters and mixing. These properties are analogous to the confusion and diffusion properties of a good cryptosystem [1]. There exist two main approaches of designing chaos-based cryptosystems: analog mode and digital mode. This paper chiefly focuses on the digital chaotic ciphers. The ideas of using digital chaotic systems to construct cryptosystems have also been proposed [2, 3]. However, some of the researches in image encryption algorithms have been increasingly based on chaotic systems such as Logistic map has been widely used now, but the drawbacks of small key space and weak security in one-dimensional chaotic cryptosystems are obvious. Because of the advantages of high-level efficiency and simplicity of one-dimensional chaotic system [4], we emphasis on using this kind of maps.

∗afshin_akhshani@yahoo.com

To overcome these drawbacks, the purpose of this study is to introduce a new chaotic algorithm which has the advantages of high-level security and large key space. Hence we present new algorithm based on Trigonometric Maps and for improving security, we used Composition of Trigonometric Maps (CTMs) [5]. Since digital images are usually represented as two-dimensional arrays, so we applied these kind of maps in two direction of image. It is found that CTMs is particularly suitable for image encryption and transmission applications.

The remaining of the paper is organized as follows. A new chaotic algorithm is introduced briefly in section two based on CTMs. In section 3 presents the experimental analysis. In Section 4, security of the chaotic encryption algorithm is discussed. Finally, Section 5 concludes the paper.

2. A NEW ALGORITHM BASED ON CTMS

2.1. Many-Parameters Families of Chaotic Maps

Let us first consider the one-parameter families of chaotic maps of the interval \([0, \infty)\) defined as the ratio of polynomials of degree \(N\):

\[
\Phi_N^{(1)}(x, \alpha) = \frac{1}{\alpha^2} \tan^2(N \arctan \sqrt{x}),
\]

\[
\Phi_N^{(2)}(x, \alpha) = \frac{1}{\alpha^2} \cot^2(N \arctan \frac{1}{\sqrt{x}}),
\]

where \(N\) is an integer greater than one. These maps have another interesting property, that is, for even values of \(N\) the \(\Phi_N^{(1)}(\alpha, x)\) maps have only a fixed point attractor \(x = 1(x = 0)\) provided that their parameter belongs to interval \((N, \infty)(0, \frac{1}{\sqrt{N}}))\) while, at \(\alpha \geq N \ (\alpha \geq \frac{1}{\sqrt{N}})\) they bifurcate to chaotic regime without having any period doubling or period-n-tupling scenario and remain chaotic for all \(\alpha \in (0, N) \ (\alpha \in (\frac{1}{\sqrt{N}}, \infty))\) but for odd values of \(N\), these maps have only fixed point attractor \(x = 0\) for \(\alpha \in (\frac{1}{\sqrt{N}}, N)\), again they bifurcate to chaotic regime at \(\alpha \geq \frac{1}{\sqrt{N}}\), and remain chaotic for \(\alpha \in (0, \frac{1}{\sqrt{N}})\), finally they bifurcate at \(\alpha = N\) to have \(x = 1\) as fixed point attractor for all \(\alpha \in (\frac{1}{\sqrt{N}}, \infty)(see
For details and mathematical proof).
From now one, depending on the situation we will consider one of these maps. Using the above hierarchy of family of one-parameter chaotic maps we can generate new hierarchy of families of many-parameters chaotic maps with an invariant measure simply from the composition of these maps.

Hence considering the functions \( \Phi_{N_1}(x, \alpha_k), k = 1, 2, \cdots, n \) we denote their composition by: \( \Phi_{N_1,N_2,\cdots,N_n}(x) \) which can be written in terms of them in the following form:

\[
\Phi_{N_1,N_2,\cdots,N_n}(x) = \frac{1}{\alpha_1} \tan^2 \left( N_1 \arctan \left( \cdots \frac{1}{\alpha_n} \tan^2(N_n \arctan \sqrt{x}) \cdots \right) \right)
\]

(3)

one can show that the chaotic regions is:

\[
\prod_{k=1}^{n} \frac{1}{\alpha_k} < \prod_{k=1}^{n} \alpha_k < \prod_{k=1}^{n} N_k
\]

for odd integer values of \( N_1, N_2, \ldots, N_n \) and if one of the integers happens to become even, then the chaotic region in the parameter space is defined by \( \alpha_k > 0 \), for \( k = 1, 2, \ldots, n \) and \( \prod_{k=1}^{n} \alpha_k < \prod_{k=1}^{n} N_k \) if one of the integers happens to become even, respectively. Out of these regions they have only period one stable fixed points.

2.2. Lyapunov characteristic exponent

In order to investigate these maps numerically, we try to calculate Lyapunov characteristic exponent of maps \( \Phi \). In fact, Lyapunov characteristic exponent is the characteristic exponent of the rate of average magnitude of the neighborhood of an arbitrary point \( x_0 \) and it is denoted by \( \lambda_{\alpha_1,\alpha_2,\cdots,\alpha_n}(x_0) \) which is written as:

\[
\lambda := lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=0}^{n-1} \ln \left| \frac{d\Phi_{N_1,N_2,\cdots,N_n}(x_k, \alpha)}{dx} \right|,
\]

(4)

where \( x_k = \Phi_{N_1,N_2,\cdots,N_n} \circ \cdots \circ \Phi_{N_1,N_2,\cdots,N_n} \circ \Phi_{N_1,N_2,\cdots,N_n} \circ \cdots \circ \Phi_{N_1,N_2,\cdots,N_n} \circ \cdots \circ \Phi_{N_1,N_2,\cdots,N_n}(x_0) \).

For the values of parameters \( \alpha_k, k = 1, 2, \cdots, n \), where the map \( \Phi \) is measurable, Birkhoff ergodic theorem implies the equality of KS-entropy and Lyapunov characteristic exponent, that is:

\[
h(\mu, \Phi_{N_1,N_2,\cdots,N_n}) = \lambda_{\alpha_1,\alpha_2,\cdots,\alpha_n}(x_0).
\]

(5)

2.3. Encryption algorithm based on CTMs

In chaos theory, kolmogorov entropy is defined to measure the decreasing rate of the information. Since in one-dimensional chaotic maps, Kolmogorov entropy is equal to Lyapunov exponent, and also a possible way to describe the key space might be in terms of positive Lyapunov exponents so we choose a chaotic region for CTMs (see Fig (1)). Here in this paper we give a new hierarchy of many -parameter families of maps of the interval \([0, \infty)\) for encryption/decryption process. In designing this algorithm for image encryption, we substituted twice each Eq. (1), (2) in them for obtaining composition of maps. The image encryption algorithm is based on the Composition of Trigonometric Maps (CTMs) for image \( I_{m \times n} \) pixels, are presented in four steps which is based on Permutation and XOR − ing processes by using Eq. (6),(7), respectively. Following composition equations are yielded from Eq. (1),(2) where \( N_1=3 \) and \( N_2=5 \) for Eq. (1) and \( N_1=4 \) and \( N_2=8 \) for Eq. (2) and also for distinguish between control parameters in two equations, \( \beta \) is used instead of \( \alpha \) in Eq. (7).

\[
\Phi_{3,5}^{\alpha_1,\alpha_2} = \frac{1}{\alpha_2^2} \tan \left( 5 \arctan \left( \frac{\tan^2 (3 \arctan (\sqrt{x}))}{\alpha_1^2} \right) \right)^2
\]

(6)
\[
\Phi_{4,8}^{\beta_1, \beta_2} = \frac{1}{\beta_2^2} \cot \left( 8 \arctan \left( \frac{\sqrt{\beta_1^2}}{\cot^2 \left( 4 \arctan \left( \frac{1}{x} \right) \right)} \right) \right)^2
\]

Permutation and XOR-ing parameters are as follows:

**Permutation:**

\[
\begin{align*}
&m : N_x, \ x_0, \ \alpha_{1x}, \ \alpha_{2x}, \\
&n : N_y, \ y_0, \ \alpha_{1y}, \ \alpha_{2y},
\end{align*}
\]

**XOR-ing:**

\[
\begin{align*}
&m \times n : \ N, \ x_0, \ \beta_{1x}, \ \beta_{2x}
\end{align*}
\]

The encryption steps are as follows:

**Step 1:** with no loss generality, we assume that source image is a 256×256 pixels. For a smaller or larger image, we can divide it into blocks of size 256×256 or fill it up to a 256×256 pixels, respectively.

**Step 2:** Set encryption key for the plain-image, including structural parameters.

**Step 3:** using Eq. (6) to permute pixels position in both X and Y directions.

**Step 4:** Do XOR operation using the Eq. (7) output data and image gray level data. Output the calculation result to the object image.

The decryption algorithm is similar to the encryption algorithm but receiving encryption key and operating with the encrypted image. Therefore, the dynamical properties of the \((CTMs)\) yield more security than other maps.

3. RESULTS

![Fig. 2](image.png)

(a) (b)

Fig. 2. Image encryption and decryption result: (a) plain-image, (b) encrypted image

Some experimental results are given in this section to demonstrate the efficiency of our scheme which is based on the proposed \((CTMs)\). An indexed image ‘Boat’ of size 256×256 is used as a plain-image, see Fig. 2(a) and encryption of this image according to mentioned parameters is shown in Fig. 2(b). The proposed algorithm is implemented using Visual C++ running in the personal computer with 2.4 GHz Pentium IV, 256 Mb memory and 80 Gb hard-disk capacities. The average time used in encryption/decryption on 256 grey-scale images of size 256×256 is shorter than 0.5s.

From the Fig. 3(b), one can see that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image Fig. 3(a). The sensitivity to initial conditions which is the main characterization of chaos guarantees the security of our scheme. Undoubtedly, the secret keys are secure enough even a chosen plaintext/ciphertext attack is adopted.

\[
\begin{align*}
&x : \{ \alpha_1 = 2.101554, \ \alpha_2 = 3.5692, \\
&\quad x_0 = 25.687, \ N_x = 95
\end{align*}
\]

**Permutation:**

\[
\begin{align*}
&y : \{ \alpha_1 = 1.5874, \ \alpha_2 = 4.2356, \\
&\quad Y_0 = 574.46, \ N_y = 86
\end{align*}
\]

**XOR-ing:**

\[
\begin{align*}
&m \times n : \beta_1 = 61.522, \ \beta_2 = 57.26223, \\
&\quad x_0 = 79.82, \ N = 70
\end{align*}
\]

4. SECURITY ANALYSIS

Some security analysis has been performed on the proposed image encryption scheme, including the most important ones like key space analysis, information entropy and statistical analysis, which has demonstrated the satisfactory security of the new scheme, as demonstrated in the following.

The key space is large enough to resist all kinds of brute-force attacks. The experimental results also demonstrate that our scheme is very sensitive to the secret key mismatch \(10^{-14}\).
Table 1. Correlation coefficients of two adjacent pixels in two images

<table>
<thead>
<tr>
<th></th>
<th>Plain image</th>
<th>Ciphered image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizontal</td>
<td>0.9525</td>
<td>0.0015</td>
</tr>
<tr>
<td>Vertical</td>
<td>0.9441</td>
<td>-0.0079</td>
</tr>
<tr>
<td>Diagonal</td>
<td>0.9068</td>
<td>0.0061</td>
</tr>
</tbody>
</table>

4.1. Information Entropy

It is well known that the entropy $H$ of a symbol source $S$ can be calculated as (For $N=128$):

$$H(S) = \sum_{i=0}^{2^N-1} P(s_i) \log_2 \frac{1}{P(s_i)} = 7.9975 \approx 8,$$

where $P(s_i)$ represents the probability of symbol $s_i$ and $\log_2$ represents the base 2 logarithm. This means that information leakage in the encryption process is negligible and the encryption system is secure upon the entropy attack. The ciphertext entropy for a value of $s=256$ is calculated using Eq.(8).

4.2. Correlation of two adjacent pixels

To test the correlation between two adjacent pixels in plain-image and ciphered image, the following procedure was carried out [6]. Randomly select 1000 pairs of two adjacent (in vertical, horizontal, and diagonal direction) pixels from plain-images and ciphered image, and calculate the correlation coefficients, respectively (see Table 1).

4.3. Differential attack

To test the influence of one image pixel change on the whole image encrypted by the proposed algorithm, two common measures were used: number of pixels change rate (NPCR) and unified average changing intensity (UACI) [6]. We get NPCR=0.41751% , UACI=0.3314%.

5. CONCLUSION

In this paper, a new scheme for image encryption based on the hierarchy of one dimensional chaotic maps of interval $[0,\infty)$ is investigated. These maps which are defined as ratios of polynomials of degree $N$ have interesting property such as invariant measure, Ergodicity, variable control parameters in the two interval; $[\frac{1}{N}, N]$ for odd $N$ and $[N, \infty)$ for even $N$, capability of calculation KS-entropy and ability to construct composition form of maps [6]. In this algorithm, the chaotic properties such as mixing and sensitive dependence on initial conditions and control parameters are suitably utilized while the limitation and weaknesses of the chaotic encryption system are effectively overcome. This new scheme employs the chaotic map (CTMs I) to shuffle the positions of image pixels and uses another chaotic map (CTMs II) to confuse the relationship between cipher-image and plain-image, thereby significantly increasing its resistance to various attacks such as the statistical and differential attacks. We conclude inclusion of composition map increases the confusion in the encryption process and it results in a more secure cryptosystem due to the fact that more confusion in encryption makes cryptosystem more secure. The analysis indicates that the algorithm can satisfy all the performance requirements such as high level of security and large enough key space. Furthermore, the entropy measured is almost equal to the ideal value. It is practicable and reliable, with high potential to be adopted for Internet image encryption, transmission applications and other information security fields.

6. REFERENCES