Comparative analysis of image encryption models based on chaos

Zhonglin Yang[1], Yanhua Cao[1], Qinyu Zhu[1], Mengyang Wang[1], Shanghui Zhou[1], Hang Chen[1,2*]

[1]School of Space Information, Space Engineering University, Beijing, 101416, China

[2]Universitéde Lorraine, CNRS, CRAN UMR 7039, Nancy, 54000, France

[*]Corresponding author: hitchenhang@foxmail.com

Keywords: chaotic model, Logistic mapping, Arnold model, Ushiki mapping, Chirikov model

Abstract: This paper first introduces the characteristics of chaotic model and explains the advantages of chaotic model in image encryption. Then the link between chaos theory and cryptography is briefly summarized to provide theoretical support for image encryption. Then, several commonly used chaos models are introduced in detail, and their advantages and disadvantages in application are summarized.

1. Introduction

Chaos refers to the seemingly random irregular movement in deterministic system, which is a universal phenomenon in nature. In 1972, Professor Lorenz of Massachusetts Institute of Technology published a paper titled "Butterfly Effect" at the American Association for the Advancement of Science conference, which officially opened the prelude of chaos theory research. The study of chaos only stayed at the theoretical level at first, and it took several decades from theory to practice. In the late 1980s, The Object of key stream generator was named Logistic mapping by Matthews, a British mathematician. Chaos was first introduced into cryptography, which also triggered a boom in cryptography chaos research. In 1998, Fridrich used two-dimensional chaotic mapping to construct a scrambling - diffusion scheme in image encryption[1]. The proposal of this scheme attracted many scholars at home and abroad to study chaotic image encryption scheme[2-9].

The research of image encryption has been continuing, and chaos model has gradually become the mainstream method. Chaos models include Logistic mapping[10], Chebyshev mapping[11], Tent mapping[12], Henon mapping[13], Duffing mapping[14], Tinkerbell mapping[15], Lozi mapping system[16], Arnold transform[17], 3D Arnold transform[18] and hyperchaos[19]. In order to analyze their advantages and disadvantages and select a transformation with the most balanced performance, this paper expounds and compares several commonly used chaos models.

The rest of this paper is organized as follows. In section 2, the cryptographic advantage of chaos model and its relation to cryptography are introduced in detail. Introduction and comparative analysis of commonly used chaos models are given in section 3. Finally, the concluding remarks are summarized in the last section.

2. Basic knowledge of chaos mapping

2.1 The advantage of chaotic model in encryption

Chaos is often used in image encryption because of its good encryption properties. As shown in Table.1, the characteristics and manifestations of chaos are introduced in detail.

DOI: 10.25236/iwmecs.2022.009

Table.1 The characteristics and manifestations of chaos

characteristics	Specific forms of expression
Extreme sensitivity to initial values and parameters	Even small changes in initial values or system parameters can produce completely different results, also known as the "butterfly effect"
Unpredictability	Because the orbit of chaotic system is extremely unstable and highly sensitive to parameters, it is difficult to predict the future orbit state of chaotic system accurately
Intrinsic randomness	The generation of chaos is a spontaneous randomness within the system, which has nothing to do with the outside world. It also indicates the local instability of chaotic motion (the above two characteristics of chaos jointly lead to its internal randomness).
Ergodic	The chaotic attraction domain is not fixed in a certain state, and the intrinsic randomness and local instability of chaotic systems lead to ergodic trajectories in the attraction domain
Self-similarity	The phase diagram of chaotic system trajectory is formed by infinite self-similar nesting
Boundedness	The phase space of a chaotic system is clearly defined within a fixed region

2.2 The relationship between chaos theory and cryptography

Chaos theory and cryptography have the following similarities and differences, as shown in Table 2.

Because there are many similarities with the cryptographic system, so the application of chaos in image encryption has a great advantage, and the difference between the cryptographic system and the difference is the place that needs to pay attention to in the application process.

Table.2 The relationship between chaos theory and cryptography

name	cryptography	chaos
Similarity	Encryption round number	The number of iterations
	Controlled by and sensitive to a key	Controlled by parameters and initial conditions and is extremely sensitive to them
	Chang statistical characteristics through obfuscation and substitution	Change statistical properties by scrambling and diffusion
Difference	Mapping on a finite set of integers	Mapping on the set of real numbers
	There are more complete evaluation and performance indicators	There are no comprehensive evaluation and performance indicators

3. Introduction and comparison of commonly used chaos models

3.1 Logistic mapping

The chaotic mapping is a one-dimensional discrete chaotic system, also known as a bug model. This model is simple in structure, simple and efficient in implementation, and is often used in pixel scrambling of image encryption system to enhance the security of algorithm. The expression is as follows

$$x_{n+1}=\mu x_n(1-x_n) \tag{1}$$

Where n = 1, 2, 3, 4... , x_n and x_{n+1} are the values before and after the transformation. Fig.1 is the bifurcation diagram of Logistic mapping, from which it can be known that when U reaches a certain value, the mapping reaches chaos state.

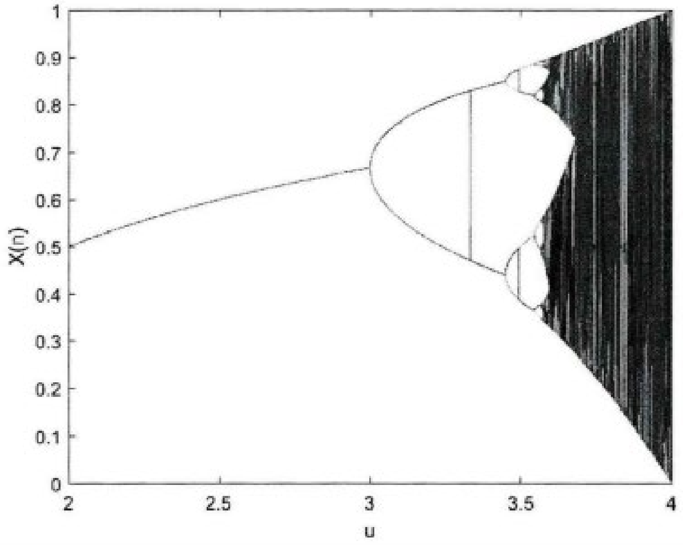

Fig.1 The bifurcation diagram Logistic chaotic mapping

3.2 Arnold model and 3D Arnold

Arnold transform is a transformation proposed by V.J. Arnold in the study of ergodic theory. It is originally referred to as cat Mapping, commonly known as cat face transform. Arnold transform is an important two-dimensional nonlinear discrete system, which is widely used to generate preliminary scrambling graphs. Similar to some other nonlinear systems, small changes in equation parameters and initial values may lead to large differences in qualitative structure of orbits. In fact, this property can be used to improve the sensitivity of keys in encryption algorithms. The mathematical definition of a two-dimensional Arnold map can be written as follows

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod}\, L) \tag{2}$$

where p and q are control parameters of the chaotic system, and L is size of the image; the system is the classic Arnold transform when p=q=1. (x_n, y_n) and (x_{n+1}, y_{n+1}) are the position coordinates of pixels before and after the transformation. The pixel value of the image changes with position.

The principle of Arnold transformation is to change the x-axis direction first, and then the y-axis direction. The final mode operation is equivalent to the cutting and backfill operation. The schematic diagram of the transformation is shown in Fig.2.

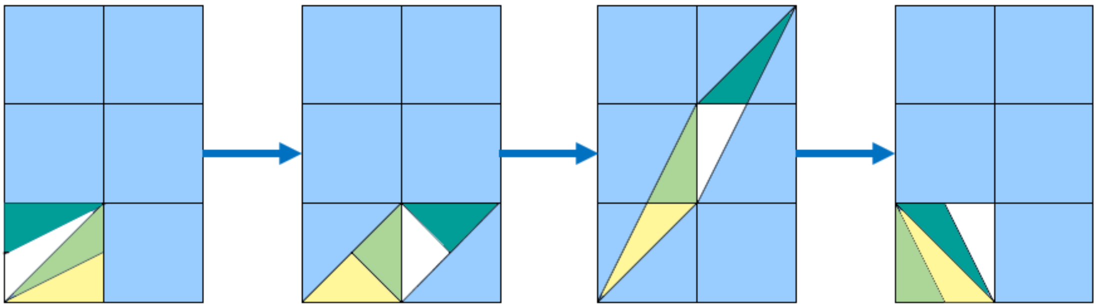

Fig.2 The diagram of Arnold transformation

Some scholars obtained three-dimensional Arnold by transforming the form of two-dimensional Arnold as follows:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ h_{n+1} \end{pmatrix} = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 5 \\ 2 & 1 & 4 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ h_n \end{bmatrix} (\bmod L) \tag{3}$$

This transform is often used to encrypt hyperspectral images, but the encryption object is usually a cube image. Where, $[x_n, y_n, h_n]^t$ and $[x_{n+1}, y_{n+1}, h_{n+1}]^t$ represent the three-dimensional position coordinates of the input and output. For hyperspectral images, its parameters $[x_n, y_n, h_n]^t$ can be interpreted as the image pixels in the h-band (x_n, y_n) of hyperspectral images.

3.3 Ushiki mapping

Ushiki is an important two-dimensional nonlinear discrete system, which is often used as a generator of chaotic sequences. The mathematical expression is as follows

$$\begin{cases} x_{n+1} = (a - x_n - by_n)x_n \\ y_{n+1} = (a - cx_n - y_n)y_n \end{cases} \tag{4}$$

Where, *a*, *b* and *c* are the control parameters of the chaotic system, and the necessary and sufficient condition for Ushiki to display the chaotic state is $b = 0.1$, $c = 0.2$ and $a \in [2.5, 3.8]$. Then, $Y = \{y_1, y_2, ..., y_n\}$ and $X = \{x_1, x_2, ..., x_n\}$ are the two chaotic sequences generated by Ushiki. When $x_1 = y_1 = 0.32$ and $a = 3.7$, Fig.3 shows the *(x-y)* of Ushiki.

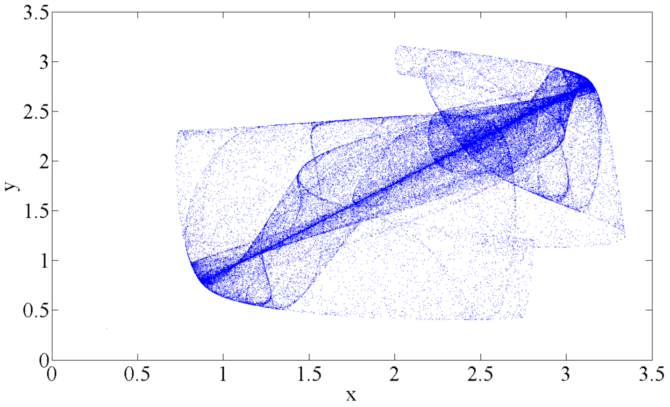

Fig.3 The diagram (x-y) of Ushiki chaotic mapping

3.4 Modified Chirikov model

The mathematical definition of Chirikov's model is as follows:

$$\begin{cases} x' = (k \bullet \sin y + x) \bmod 2\pi \\ y' = (y + x') \bmod 2\pi \end{cases} \tag{5}$$

Where K is a positive integer control parameter, and the variables (x, y) and $(x`, y`)$ are pixel positions before and after transformation. Some scholars designed an improved Chirikov mapping on the basis of (5), whose mathematical representation method can be described as follows:

$$\begin{cases} x' = (k \bullet \sin y + x) \bmod 2\pi \\ y' = (h \bullet y + x') \bmod 2\pi \end{cases} \tag{6}$$

Where *h* is a new control parameter, also a positive integer.

3.5 Classification analysis and comparison

Compared with traditional text information, image information has the characteristics of intuitive, vivid and large amount of information, large amount of data, high redundancy and strong correlation of pixels. The use of traditional encryption methods such as data Encryption Standard (DES), Advanced Encryption Standard (AES) and RSA encryption algorithm to encrypt images has high time cost and poor encryption effect. It shows that the encryption methods designed for traditional text data can not meet the requirements of image encryption.

However, the research of chaos in encryption algorithm has not stopped, but its theory is not mature yet. The chaotic system adopted by scholars is more natural chaotic system, and its defect lies in that these systems do not have strict confidentiality in the sense of cryptography. How to make better use of chaotic system for encryption and decryption is still attracting a large number of scholars to further study. Chaos models can be classified according to dimensions, as shown in Table 3.

Table.3 The relationship between chaos theory and cryptography

name	**dimension**	**classification**
chaos	One	Logistic mapping, Chebyshev mapping, Tent mapping
	Two	Henon mapping, Duffing mapping, Tinkerbell mapping, Lozi mapping, Arnold transformation
	Three	3D Arnold transform, hyperchaos

Arnold, as the most classic chaotic transformation, has advantages that other transformations do not:

(1) Dimensional variability. Arnold can be divided into two dimensions and three dimensions. By changing the number of columns and columns of the matrix, the purpose of dimensional transformation can be achieved. The operation is simple and the programming is easy to achieve.

(2) Directly acting on the image. Chaotic transformation generally generates a series of pseudorandom numbers and then processes these pseudorandom numbers before they can be used for image encryption. Arnold transform can directly act on the image, simplify the operation process and save the pretreatment time.

However, the Arnold transform also has the common disadvantages of chaos transform:

(1) The key space is insufficient. Arnold chaotic system is widely used in the construction of chaotic cryptosystems because of its simple structure and high operation efficiency. However, due to the limitation of the number of state variables, it faces the problems of small key space and insufficient anti-exhaustive attack in practical application.

(2) The periodicity of chaotic mapping. In image scrambling operations, area-preserving reversible chaotic mappings represented by Arnold transformation, Baker mapping and Standard mapping have been widely used. However, after the discretization of continuous chaotic system, its aperiodic characteristics will be degraded, and the periodic behavior will appear, which seriously affects the safety. For 256*256 size images, if scrambled using Arnold transform, the original text will be restored automatically after 192 rounds, regardless of the Arnold transform parameter.

(3) Applicability of high-dimensional chaos. The dimensional characteristics of 3D Arnold mapping correspond to the band of hyperspectral image, but in practical application, the processing object must be cube formation, namely A * A * A, which limits the application scope of 3D mapping.

4. Conclusion

In image encryption, chaos has incomparable advantages. Among various chaos models, Arnold is widely used because of dimensional variability and its direct effect on images. However, Arnold also has some disadvantages in practical use, which need further study to overcome

References

[1] Fridrich J. Image watermarking for tamper detection[C]// Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on. 1998.

[2] Birx D L, Pipenberg S J. Chaotic oscillators and complex mapping feed forward networks (CMFFNs) for signal detection in noisy environments[C]// International Joint Conference on Neural Networks. IEEE, 2002.

[3] Musheer A, Alam M S. A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping[J]. International Journal on Computer Science & Engineering, 2010, 2(1):46-50.

[4] Salleh M, Ibrahim S, Isnin I F. Image encryption algorithm based on chaotic mapping[J]. Jurnal Teknologi, 2003, 39(1).

[5] Liu Z, Yu Z, Wei L, et al. Optical color image hiding scheme based on chaotic mapping and Hartley transform[J]. Optics and Lasers in Engineering, 2013, 51(8):967–972.

[6] Marotto F R. Chaotic behavior in the Hénon mapping[J]. Communications in Mathematical Physics, 1979, 68(2):187-194.

[7] Zhu L, Li W, Liao L, et al. A Novel Algorithm for Scrambling Digital Image Based on Cat Chaotic Mapping[C]// International Conference on Intelligent Information Hiding & Multimedia. IEEE, 2006.

[8] Cheng H, Liu C Z. Mixed Fruit Fly Optimization Algorithm Based on Chaotic Mapping[J]. Computer Engineering, 2013, 39(5):218-221.

[9] Tian-Yu Y E, Niu X X, Yang Y X. Fragile Authentication Watermark Based on Singular Value Decomposition and Chaotic Mapping[J]. Opto-Electronic Engineering, 2008.

[10] Sethi N, D Sharma. A novel method of image encryption using logistic mapping. 2012.

[11] Lei L H, Guan-Yi M A, Cai X J, et al. Study of Chaotic Sequence Based on Chebyshev Mapping[J]. Computer Engineering, 2009, 35(24):4-6.

[12] Zhang X, Wen S, Li H, et al. A Chaotic Particle Swarm Optimization Algorithm Based on Tent Mapping[J]. Journal of Taiyuan University of Science and Technology, 2011, 19(17):2108-2112.

[13] Tresser C, Coullet P, Arneodo A. TOPOLOGICAL HORSESHOE AND NUMERICALLY OBSERVED CHAOTIC BEHAVIOR IN THE HENON MAPPING[J]. Journal of Physics A General Physics, 2017, 13(5):L123.

[14] Hayashi C, Ueda Y, Kawakami H . Solution of Duffing's equation using mapping concepts. , 1968.

[15] Lozi R. Shaping topologies of complex networks of chaotic mappings using mathematical circuits[C]// 2014 IEEE International Workshop on COMPLEX SYSTEMS and NETWORKS. IEEE, 2014.

[16] Liu Z, Xie H, Zhu Z, et al. The Strange Attractor of the Lozi Mapping[J]. International Journal of Bifurcation & Chaos, 1992, 2(4):-.

[17] Chen W, Quan C, Tay C J. Optical color image encryption based on Arnold transform and interference method[J]. Optics Communications, 2009, 282(18):3680-3685.

[18] Deng X, Zhao D. Color component 3D Arnold transform for polychromatic pattern recognition[J]. Optics Communications, 2011, 284(24):5623-5629.

[19] Rossler O E. An Equation for Hyperchaos[J]. Physics Letters A, 1979, 71(2-3):155-157.