WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 3, Number 1, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v3n1.27
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Research on the Development of Chaotic Image Encryption

Chao Huang, Mingqiang Gao *, Haoyuan Ma

University of Science and Technology Liaoning, Anshan, China
*Corresponding Author: 18823496@qq.com

ABSTRACT

With the development of the information age, the use of images for information expression has become very common. In view of the security of images, more and more scholars begin to study image encryption. In this paper, we briefly describe the development of chaotic image encryption field, describe the concept of chaos theory, chaotic characteristics and discriminant criteria, common typical chaotic systems, security analysis methods and development summary.

KEYWORDS

Cryptography; Image encryption; Chaotic system; Encryption algorithm

1. INTRODUCTION

Due to the characteristics of multimedia information, such as strong intuitiveness, large amount of information, coupled with the maturity of related technologies, the use of image, sound and video multimedia forms for information expression has been very common. Digital image contains more information than sound and forms the basis of video, so it plays an important role in multimedia information. Pictures are one of the easiest ways to leak personal information, and if the information on the photos is obtained by criminals, the consequences will be very serious. Therefore, in different fields, we need to pay more attention to the management and protection of image files, so that it can play a greater role. In addition, in national security, technology, military and other fields, there is a large amount of image information worthy of attention, so the research on image security is of great significance to both the country and individuals. Building a cryptosystem requires many of the characteristics of chaotic mapping, such as pseudo-randomness and initial value sensitivity. Therefore, chaotic encryption technology has been more and more applied to image encryption.

2. CHAOTIC ENCRYPTION

2.1. Chaos Theory

Chaos is a kind of deterministic seemingly irregular motion appearing in nonlinear dynamic systems. It can also have random behavior without any additional random factors, that is, there is inherent randomness. This kind of motion is neither periodic nor convergent, and has an extremely sensitive dependence on the initial value. In the article "Deterministic Nonperiodic Flow" by Lorenz, an American meteorologist, a strange effect of atmospheric turbulence is pointed out that there is a link between the failure of the climate to repeat itself precisely and the inability of long-term weather forecasters to do anything about it, that is, between aperiodic and unpredictability [1]. Lorenz's research focuses on a fundamental property of chaos: sensitivity to initial conditions. This is the famous "butterfly effect", which also laid a solid foundation for future chaos theory research.

2.2. Chaotic Characteristics and Discriminant Criteria

2.2.1. Chaotic characteristic

Chaos is an unstable and finite constant motion phenomenon, and its steady state is not the standard deterministic motion of quasi-periodic motion, periodic motion and static three common states. The characteristics of chaotic system mainly include seven aspects.

Extreme sensitivity to the initial value: When there is any small change in the initial value, the continuous iteration of the chaotic system can produce a very large difference.

Long-term unpredictability: Because the initial conditions are only limited to a certain limited precision, the chaotic system is extremely sensitive to the initial conditions. Therefore, it is impossible to predict the dynamic behavior of a chaotic system at some point in the future.

Internal randomness: The original completely determined system produces randomness, and the source of these randomness can only come from the system itself. This randomness arises spontaneously in chaotic systems.

Continuous power spectrum: Power spectrum is usually used when people analyze time series and signals, which is used to describe the distribution of amplitude after Fourier transform. The power spectrum of chaotic signals has the characteristics of continuous power spectrum similar to that of random signals.

Boundedness: It means to the chaotic attraction domain. It shows that chaos is bounded, and its motion path is always confined to a definite region.

Universality: It refers to some common characteristics of different systems when they tend to be chaotic, which does not change with the change of specific system equations or parameters, and is a manifestation of the inherent regularity of chaotic systems.

Ergodicity: Indicates that the chaotic orbit passes through every state point in the chaotic attraction domain, but it will never linger at a certain state point.

2.2.2. Chaotic system discriminant method

Judging whether a system has chaotic motion is an important topic in the study of chaos science. The commonly used methods include Lyapunov exponent, measure entropy and power spectrum method.

Lyapunov exponent is used to describe the speed of contact and separation of attractor orbits, and to describe the statistical properties of their motion. One-dimensional discrete system: $X_{n+1} = F\left(X_n\right)$, its Lyapunov calculation formula is shown in Equation (1).

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{dF}{dx_i} \right| \tag{1}$$

Power spectrum analysis is of great value in the field of chaos and vibration analysis. Because all periodic motion *x(t)* can be extended into Fourier series, the relationship between the frequency coefficients and the corresponding spectrum is a discrete spectrum, and the aperiodic motion frequency is a continuous spectrum. The random signal *x(t)* has the following power spectral density parameters.

$$S_y(\theta) = \int_{-\infty}^{\infty} R_y(\sigma) e^{-j\theta\sigma} d\tau \tag{2}$$

Where: $y(\sigma)$ is the autocorrelation function of $R_y(\sigma)$, σ is the sampling time interval. If the calculated power spectrum is a continuous spectrum similar to broadband noise, then it shows that the system has chaotic characteristics. Because when the power spectrum has a single peak or several peaks, it corresponds to a periodic or quasi-periodic sequence, and when the power spectrum has no obvious peak or the peak is connected into a piece, it corresponds to a chaotic sequence. According to these characteristics of the work spectrum, people can identify whether the motion is periodic, quasi-periodic or chaotic.

Phase diagram method is a very classical graphical analysis method, which is suitable for the drawing and analysis of phase trajectories of first-order and second-order systems. However, the phase trajectory of the third-order system is in three-dimensional space, so it is not suitable for phase diagram analysis, but for Lyapunov method and other methods. Then, the phase diagram of chaotic motion refers to the projection of the solution curve of the system in the phase space in a nonlinear dynamic system, and the projection curve is called the phase trajectory. With computer simulation calculation, we can get the phase trajectory pattern quickly and accurately, which is convenient for the analysis and design of the system.

2.3. Common Typical Chaotic Systems

2.3.1. One-dimensional chaotic system

Logistic map, also known as worm model [2], is a simple but very important nonlinear iterative equation. The Logistic mapping equation is shown in Equation (3).

$$x_{n+1} = \mu x_n (1 - x_n) \quad x \in [0,1] \tag{3}$$

where the parameter 3.5699456<x<=4.Logistic map appears chaotic,as shown in Figure 1.

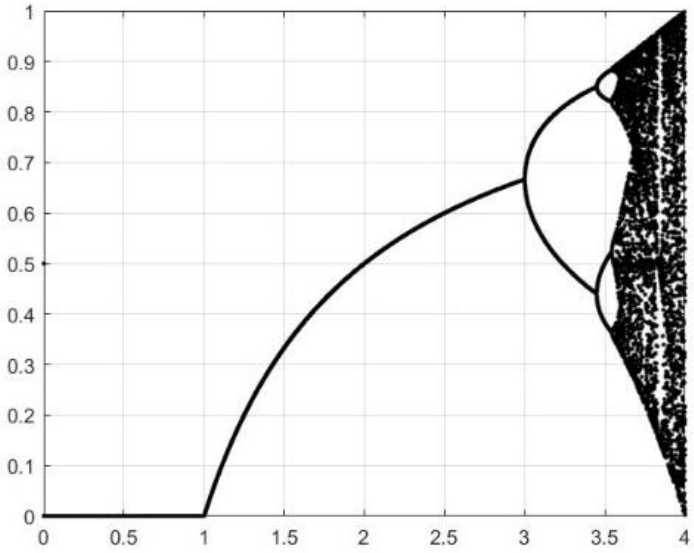

Figure 1. Logistic map bifurcation diagram

2.3.2. Two-dimensional chaotic system

In 1976, astronomer Henon proposed a two-dimensional chaotic map, often referred to as the Henon map [3].The equation is shown in Equation (4).

$$\begin{cases} x_{m+1} = -ax_m^2 + y_m + 1 \\ y_{m+1} = bx_m \end{cases} \tag{4}$$

Where a=1.4, b=0.3, the system can produce chaos.

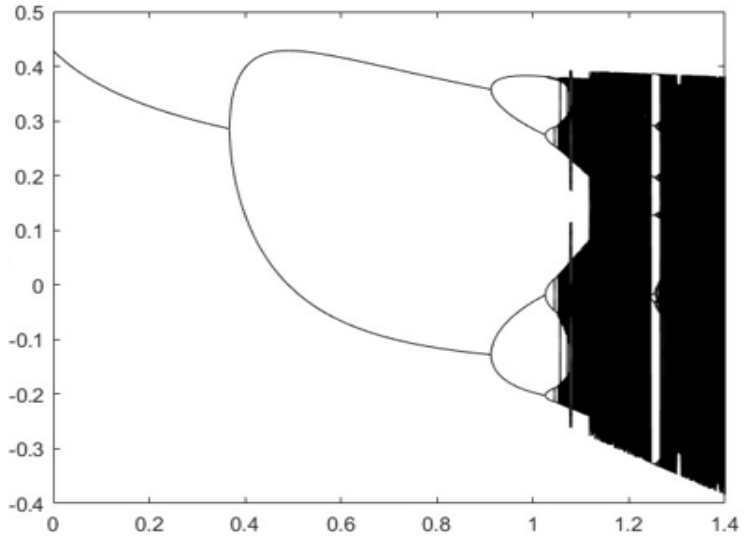

Figure 2. Henon map bifurcation diagram

2.3.3. Three-dimensional chaotic system

Take Lorenz system as an example [4], as shown in Equation (5).

$$\begin{cases} \dfrac{dx}{dt} = -\alpha(x - y) \\ \dfrac{dy}{dt} = \beta x - zx - y \\ \dfrac{dz}{dt} = xy - bz \end{cases} \tag{5}$$

Where the parameter $\alpha = 10$, $\beta = 28$, $b = \dfrac{8}{3}$, the system is in a chaotic state.

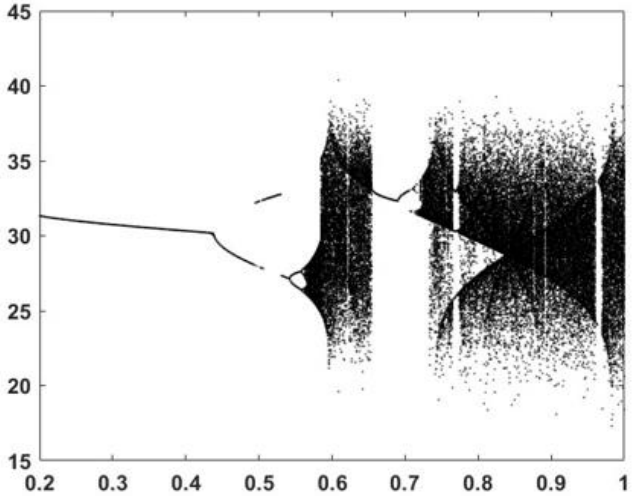

Figure 3. Lorenz bifurcation diagram

3. SECURITY ANALYSIS METHOD

3.1. Key Space Analysis

The key space of a good encryption algorithm should be large enough to resist exhaustion attacks. The key space should not be smaller than $2^{100} \approx 1.27 \times 10^{30}$[5].

3.2. Sensitivity Analysis

In security analysis, the cryptosystem is required to have a very high key sensitivity, and a small change in the key can lead to a large change in the encrypted image. If a small change in the key can cause the original image to be unable to be correctly decrypted, the encryption algorithm can be considered sensitive to the key. Image pixel value can be set as the initial condition or control parameter of chaotic system and used as the key, so it can not only be sensitive to the key but also resist the known plaintext attack and chosen-plaintext attack.

3.3. Statistical Characteristic Analysis

Statistical analysis usually includes histogram analysis and correlation analysis of adjacent pixels.

Histogram: histogram is a function of gray level, describing the number of pixels of the gray level in the image, mainly used for statistics of the frequency of each pixel value, as a frequency distribution table. It can be seen that the histogram of the image reflects the statistical characteristics of the image. Then a standard to measure the encryption effect is to make the histogram distribution of the ciphertext image as uniform as possible.

The correlation of adjacent pixels reflects the correlation degree of pixel values in adjacent positions of the image. Image encryption.

The second goal is to reduce the correlation between adjacent pixels, mainly including horizontal pixels, vertical pixels and diagonal pixels between three aspects.

3.4. Attack Resistance

In practice, an absolutely secure encryption system does not exist, and if the cost of deciphering the algorithm is greater than the cost of encrypting the information, then the algorithm can be considered secure. Therefore, we need to verify the anti-attack performance of the designed system by using existing password attack methods as much as possible, such as statistical attack, differential attack, selective plaintext attack, selective ciphertext attack and exhaustive attack [6].

4. SUMMARY

Because of some characteristics of chaotic system, it is being used by more and more researchers in image encryption research. However, there are still some shortcomings in the current research, but its research prospect is broad. With the further development of the research, the application of chaos in the direction of image encryption is bound to receive more and more attention.

REFERENCES

[1] Devaney R L. (1989). An introduction to chaotic dynamical systems. New York, Westview Press. https://doi.org/10.4324/9780429502309

[2] May R M. (1976). Simple mathematical models with very complicated dynamics. Nature 261(5560),459-467. https://doi.org/10.1038/261459a0

[3] Hénon M. (1976). A two-dimensional mapping with a strange attractor. Communications in Mathematical Physics 50(1),69-77. https://doi.org/10.1007/BF01608556

[4] Lorenz E N. (1963). Deterministic Nonperiodic Flow. Journal of the Atmospheric Sciences, 20(2),130-141. https://doi.org/10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2

[5] Wu Z, Pan P, Sun C. et al. (2021). Plaintext-Related Dynamic Key Chaotic Image Encryption Algorithm. Entropy (Basel) 23(9),1159. https://doi.org/10.3390/e23091159

[6] Lee Y-S, Lee Y-J, Han D-G. et al. (2012). Performance Improvement of Power Analysis Attacks on AES with Encryption-Related Signals. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E95.A(6),1091-1094. https://doi.org/10.1587/transfun.E95.A.1091