Advances in Computer, Signals and Systems (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2023.070811
ISSN 2371-8838 Vol. 7 Num. 8

Research on Design of Chaotic Symmetrical Digital Image Encryption System

Han Chen

Shanwei Institute of Technology, Shanwei, China

Keywords: Chaos theory, symmetric encryption, digital image

Abstract: With the widespread dissemination of digital information, the security encryption of digital images has become particularly critical. This study deeply discusses the chaotic symmetric digital image encryption system based on chaos theory and symmetric encryption technology. By combining the technologies of these two fields, an efficient and safe encryption method is provided for digital images. Experimental evaluations show that the system is capable of effectively encrypting images so that they are visually distinct from the original content. At the same time, the system shows strong resistance to differential attacks, and has a high encryption speed, which is suitable for real-time applications.

1. Introduction

With the wide application of digital technology, digital images have been widely used in communication, medical treatment, entertainment and other fields. However, the digitalization and dissemination of images has brought about the problem of information security, and the secure transmission and storage of digital images has become an important research field. Traditional encryption methods may be difficult to meet the highly complex security requirements of modern digital images, especially in the exploration of encryption strategies with high efficiency and strong noise resistance [1]. Chaos theory, due to its natural unpredictability and high sensitivity, offers an interesting research direction to enhance image encryption techniques. In recent years, symmetric encryption, as a classic encryption method, has played a key role in ensuring information security. However, symmetric encryption alone may have certain limitations. Combining chaos theory and symmetric encryption, a new and more secure encryption strategy can be designed to improve the efficiency and security of digital image encryption.

2. Overview of digital image encryption technology

With the development of information technology, digital images have been widely used in various fields, such as medical, military, commercial and entertainment, etc. This wide range of applications has led to an urgent need for confidentiality and security of digital image data. Therefore, digital image encryption technology is born, which provides technical support for ensuring the integrity, confidentiality and availability of image data[2]. Digital image encryption technology is mainly concerned with converting recognizable images into unrecognizable formats

to prevent unauthorized access and tampering. Encrypted key management, encryption algorithm selection and encrypted image quality are also the core issues of digital image encryption technology. Choosing an appropriate encryption strategy and algorithm is crucial to ensure the secure transmission and storage of images.

3. Application of Chaos Theory in Symmetric Encryption

3.1 Basics of Chaos Theory

Chaos theory originates from the research of mathematics and physics, and mainly studies the seemingly disordered or random behavior of nonlinear dynamical systems under deterministic conditions. These systems are often described by a set of nonlinear differential equations, and although these equations may be structurally deterministic, their long-term behavior is unpredictable. Small changes in initial conditions can lead to large variations in system behavior. This is also known as the "butterfly effect" and means that in a chaotic system, small deviations from the initial conditions grow exponentially over time[3]. In a chaotic system, any two adjacent trajectories will separate over time. In its state space, a chaotic system has an infinite number of periodic trajectories. Chaotic attractors usually have complex, fractal structures.

3.2 The principle of symmetric encryption

Symmetric encryption, also known as private key encryption or single- key encryption, is an encryption technique in which the same key is used for encryption and decryption. This means that the sender and receiver must share a secret key and must ensure that this key is stored and transmitted securely to prevent it from being stolen by unauthorized third parties.

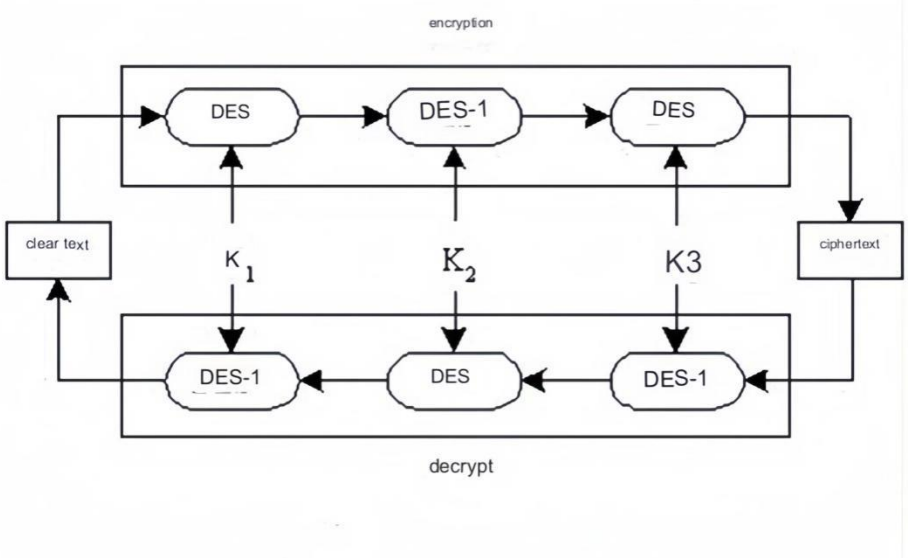

Figure 1: Principle of symmetric encryption

The working principle of symmetric encryption is shown in Figure 1. First, the sender and receiver agree and choose a shared secret key. This key can be predetermined or dynamically generated, but the key is that both parties must know this key. When senders need to send a message, they encrypt the message using a key of their choice and a symmetric encryption algorithm, resulting in a ciphertext. The encrypted ciphertext is sent to the receiver through the communication channel. The recipient uses the same key and corresponding decryption algorithm to decrypt the ciphertext, thereby recovering the original message. The receiver can verify that the

decrypted message is identical to the original message to ensure that it has not been tampered with in transit. There are many types of symmetric encryption algorithms, including stream ciphers and block ciphers. Stream ciphers operate on each bit of the original data stream when encrypting, while block ciphers divide the original data into fixed-size blocks and encrypt each block. Although symmetric encryption has advantages in efficiency, it also has certain defects, mainly the complexity of key management. Because the same key is used for both encryption and decryption, it is important to ensure that the key is stored and transmitted securely from unauthorized third parties.

3.3 Combination model of chaotic symmetric encryption and its advantages

Chaotic symmetric encryption combines the unpredictability of chaos theory with the efficiency of symmetric encryption. In this model, the dynamic behavior of a chaotic system is used to generate or adjust keys or algorithm parameters for symmetric encryption. Since chaotic systems are extremely sensitive to initial conditions, this combination ensures that small changes in keys or parameters can lead to large differences in encryption results, increasing the difficulty of countering attacks. Compared with traditional symmetric encryption, chaotic symmetric encryption has several obvious advantages. First, it provides a more complex and unpredictable key generation mechanism. Not only does this increase the size of the key space, thereby improving resistance to brute-force attacks, but it also ensures that each encryption process can be unique, even with the same original key. Second, the inherent irregularity of chaotic systems provides encryption with an additional layer of randomness. This means that attempts to reverse engineer the encryption process or to predict the ciphertext become very difficult. Finally, the model of chaotic symmetric encryption allows fine-tuning of the encryption process to make it more suitable for specific application needs.

4. Design of chaotic symmetric digital image encryption system

4.1 System Architecture

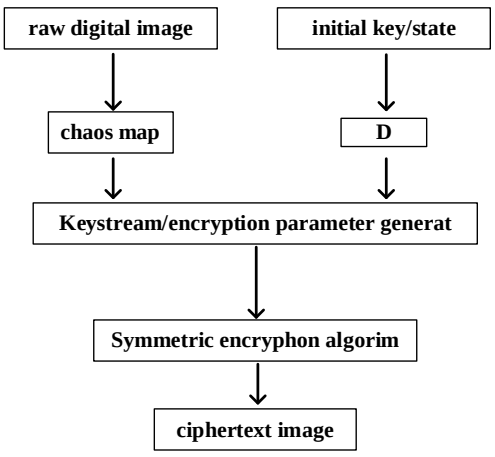

Figure 2: Architecture diagram of chaotic symmetric digital image encryption system

Chaotic symmetric digital image encryption system structure combines chaos theory and symmetric encryption technology, and provides a highly secure encryption mechanism for digital images. As shown in Figure 2, at the core of the system, the chaotic map, as a main component, is used to generate the key stream or fine-tune the encryption parameters. This key stream interacts with the digital image to be encrypted to realize the safe encryption of image data. The system first receives a raw, unencrypted digital image as input. At the same time, an initial key or initial state is

provided to the chaotic map to start the chaotic process. As a chaotic system evolves, it produces a keystream or series of encryption parameters that are combined with a symmetric encryption algorithm to form an encryption mechanism capable of operating on an input digital image. After encryption is complete, the resulting ciphertext image is provided as output, while ensuring that enough information is preserved to allow correct decryption by the receiver. The decryption process uses the same chaotic map and symmetric algorithm as encryption, but in reverse, to restore the original image.

4.2 Key technologies and their implementation

In the design of chaotic symmetric digital image encryption system, the selection and realization of key technologies are very important. First, the system uses an advanced chaotic map, specifically the Henón map, to generate the key stream. Known for their chaotic properties and high sensitivity to initial conditions, Henón maps provide an additional layer of security for encryption. This mapping is optimized in this system to produce a key stream that is difficult to predict and replicate, further strengthening its security.

4.3 Encryption process and steps

The implementation of the chaotic symmetric digital image encryption system starts with the input of the original digital image, which is firstly preprocessed by discrete wavelet transform. Subsequently, the initial keys and state associated with the preprocessed image are passed to the Henón map. At this stage, the Henón map starts and generates a keystream based on its chaotic properties. After getting the key stream, the system integrates it with the preprocessed image data into the improved AES algorithm. This algorithm is specifically designed to work with the keystream produced by the Henón map, ensuring that each block of image data is properly encrypted. Under the action of the AES algorithm, the data is converted into a secure ciphertext format, which makes it difficult for unauthorized users to decipher or tamper. Finally, the data encrypted by the AES algorithm is organized into encrypted images, ready for transmission or storage.

5. Experiment and Results

5.1 Experimental setup

In order to verify the performance and security of the chaotic symmetric digital image encryption system, a series of experiments are designed in this study. The experimental environment was built on a computer equipped with a quad-core processor and 16GB RAM, and Ubuntu 20.04 was used as the operating system. The encryption algorithm is implemented in Python language, and the OpenCV library is used for image processing. Five test images of different content with a resolution of 1920x1080 were selected to represent common usage scenarios. Regarding keys, the initial state and parameters of the Henón map are generated from a random seed, ensuring that the keystream is unique for each experiment. For the AES algorithm, a key length of 256 bits is used to provide sufficient security. The purpose of the experiment is to evaluate the system's encryption effect, speed, and adaptability to different image contents through multiple rounds of encryption and decryption operations. At the same time, its resistance to various potential attacks, such as differential attacks and statistical attacks, will also be evaluated.

5.2 Encryption effect display

After many encryption experiments, comparing the results of the original image and the encrypted image, it really shows the superiority of the chaotic symmetric digital image encryption system. The encrypted image is visually completely different from the original image without any obvious pattern or structure to follow, demonstrating the efficient encryption performance of the system. To quantify the effect of encryption, the degree of correlation between the original image and the encrypted image is calculated. Mathematically, the degree of relevance R is defined as:

$$R = \frac{\sum_{x,y}\left(I_o(x,y)-\bar{I}_o\right)\left(I_e(x,y)-\bar{I}_e\right)}{\sqrt{\sum_{x,y}\left(I_o(x,y)-\bar{I}_o\right)^2\sum_{x,y}\left(I_e(x,y)-\bar{I}_e\right)^2}}$$

Among them, I_o is the original image, $\bar{I}_o$ is its mean value, I_e is the encrypted image, and $\bar{I}_e$ is the mean value of the encrypted image.

Table 1: Results on five test images

test image number	Relevance R
1	0.0032
2	-0.0021
3	0.0017
4	-0.0015
5	0.0024

It can be seen from Table 1 that all the correlation values are close to zero, which means that the correlation between the original image and the encrypted image is extremely low. The encryption process successfully removes any identifiable characteristics of the original image, providing a strong security barrier for the data.

5.3 Safety and Performance Evaluation

In order to ensure the reliability and efficiency of the chaotic symmetric digital image encryption system in practical applications, the research further evaluates its security and performance. First, starting from the aspect of security, the system's resistance to differential attacks is evaluated. For this purpose, the difference statistic D is defined:

$$D = \frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N}\left|I_e(x,y)-I_e'(x,y)\right|$$

Among them, I_e is an encrypted image, but another encrypted version of the original image with only a small change of one pixel. I_e' Ideally, a small change of one pixel should make a large difference in the encrypted image.

The data in Table 2 shows that even when one pixel of the original image changes slightly, about 50% of the pixels in the encrypted image change, which strongly demonstrates the system's resistance to differential attacks.

In terms of performance, the encryption time of five images was measured to evaluate the efficiency of the algorithm. Timing results (unit: milliseconds) are shown in Table 3.

Table 2: Test results on five test images

test image number	Difference statistic D
1	127.5
2	128.2
3	127.8
4	126.9
5	127.3

Table 3: Encryption time of 5 images

test image number	Encryption time (ms)
1	12.5
2	13.2
3	12.8
4	12.1
5	13.0

It can be seen that the encryption time is below 13 milliseconds, which proves that the system has high efficiency in real-time encryption applications. Combining the results of security and performance, the chaotic symmetric digital image encryption system shows its outstanding potential not only in theory but also in practical application.

6. Conclusion

Based on chaos theory and symmetric encryption technology, the system provides a highly secure and effective encryption method for digital images. The experimental results clearly demonstrate that the system effectively masks the content of the original image visually, while maintaining a high encryption speed, which is suitable for real-time operation. More critically, the system is proved to be highly resistant to common differential attacks through the evaluation of differential statistics. The measurement of encryption time further highlights its superiority in terms of performance.

Acknowledgement

This work was supported by Shanwei Institute of technology research start-up funding projects：(SKQD2021Y-022); (SHYYYB-202104).

References

[1] Bai Yulong, Yang Yang, Tang Lihong. Design of a new multi- scroll chaotic system and its application in image encryption [J]. Journal of Electronics and Information Technology, 2021, 43(2): 436-444.
[2] Liang Yuting, Luo Yuling, Zhang Shunsheng. A Review of Chaotic Image Encryption Based on Compressive Sensing [J]. Journal of Guangxi Normal University-Natural Science Edition, 2022, 40(5).
[3] Wang Jiaqi, Zhang Miao, Tong Xiaoyun, et al. Image compression encryption algorithm based on fractal coding and LIC chaotic system[J]. Application Research of Computers/ Jisuanji Yingyong Yanjiu, 2022, 39(12).