Scholar Publishing Group
Distributed Processing System
https://doi.org/10.38007/DPS.2021.020201
ISSN 2790-0916 Vol. 2, Issue 2: 1-8

Design and Implementation of Distributed System Platform Based on Chaos Theory and Encryption Algorithm

Michele Settanni*

Univ Fed Rio Grande do Sul, Informat Inst, Av Bento Goncalves 9500, Porto Alegre, RS, Brazil

**corresponding author*

Keywords: Chaos theory, Encryption Algorithm, Distributed System, Image Encryption

Abstract: Image information is stored and transmitted more and more frequently in the public network. How to protect information security becomes particularly important. Because the image data has the characteristics of high redundancy and high correlation between adjacent pixels, the traditional encryption scheme is no longer suitable for image encryption. As a deterministic nonlinear system, chaotic system has many excellent characteristics, which makes it very suitable for image encryption. This paper designs a distributed system platform by combining encryption algorithm and chaos theory, which can solve the security problem of the platform. After testing and analyzing the system platform, the functions of the platform can run stably and the performance is normal.

1. Introduction

As the society continues to push us towards the big data era, in the process of explosive growth of information, various types of information sources, such as images, voice and video, are transmitted and stored in the public network [1]. Among them, the digital image is the main form of multimedia information. The image is visual in nature and can present the expression information intuitively and vividly. Therefore, it is widely used in the digital information system and modern communication field [2]. While digital images bring convenience to our daily life, there are also great challenges, that is, how to ensure the security of information during the transmission of digital images to prevent illegal interception and tampering of data [3].

Image information is not only related to individuals and families, but also to medical care, education, military and national economy. If it is attacked by various possible attacks in the transmission process of public network, it will cause serious information leakage [4]. Therefore, the protection of digital image security has become a research hotspot in the academic community. Because of some special properties of image data, such as high redundancy and high correlation

between adjacent pixels, the traditional encryption scheme is not suitable for image encryption. Therefore, researchers have deeply studied the image encryption system based on chaos theory, and put forward many image encryption schemes with good performance. In most cases, the ciphertext image is the same size as the original image. However, in scenarios with limited bandwidth, such as telemedicine diagnosis and field military communication, it is necessary to compress and encrypt the images at the same time to reduce the amount of data transmitted and improve the utilization of the channel on the premise of ensuring security. Compressed sensing can simultaneously compress and encrypt sparse signals, so it has a wide application prospect in the field of image encryption. Many image encryption schemes based on chaotic system and compressed sensing have emerged. Foreign scholars have proposed the compressed sensing theory, which is a new information sampling technology in the field of information processing. Subsequently, they demonstrated the theory of compressed sensing through strict mathematical derivation, which opened up a broad prospect for the simultaneous compression and encryption of plaintext images [5]. In recent years, compression sensing technology has been gradually applied to the field of image encryption. Although the algorithm improves the security of the ciphertext image and reduces the amount of data, it is less sensitive to the plaintext image and has poor ability to resist the selective plaintext attack [6].

In view of the increasingly prominent information security of image data, and the traditional encryption scheme is no longer suitable for image encryption, this paper combines the chaotic system with DNA encryption and compression sensing respectively on the basis of studying the existing algorithms, proposes two image encryption algorithms, and combines the algorithm with the distributed system design for experimental simulation and performance analysis.

2. Overview of Related Concepts

2.1. Foundations of Cryptography

Digital image encryption is developed on the basis of traditional cryptography, and many classical theoretical foundations and concepts are also applied to the field of image encryption. Therefore, in order to facilitate the understanding of image encryption, the following is a brief introduction to the relevant knowledge of cryptography [7].

A cryptosystem usually includes five parts: plaintext, ciphertext, key, encryption and decryption. They are briefly introduced below.

Plaintext: the original information before encryption, generally including: images, voice video, text, etc., expressed by the letter P.

Ciphertext: the plaintext is "camouflaged" by a certain method, and the encrypted information is represented by the letter C.

Key: variable parameter that controls or participates in cipher transformation. It can be divided into encryption key and decryption key, represented by the letter K.

Encryption: the process of converting plaintext into ciphertext, also known as encoding, which is represented by the letter E, i.e

$$C = E_k(P) \tag{1}$$

Decryption: the process of restoring ciphertext to plaintext, also known as decoding, is represented by the letter D, i.e

$$P = D_k(C) \tag{2}$$

For a secure and practical cryptosystem, it can be expressed as:

$$P = D_k(E_k(P)) \tag{3}$$

That is, the plaintext is encrypted by a specific method to hide its original information to obtain the ciphertext; And all the information of plaintext can be restored by relying on the key and ciphertext [8].

2.2. Chaos Theory

In view of the inherent random phenomenon and complexity of chaos, the definition of chaos has not been unified in a strict sense, but scholars have carried out relevant theoretical research and practical applications based on their understanding of their own research field. At present, there are many existing definitions of chaos, and there are mainly two definitions of chaos recognized by domestic and foreign scholars: Li Yorke definition and Devaney definition [9].

2.3. Chaotic Dynamics Characteristics

Chaos is not completely without laws. As a deterministic system, it can produce simple and definite behaviors. Therefore, chaos has its particularity, specifically:

(1) Extreme sensitivity to initial conditions. This property is often called "Butterfly Effect", which is also an essential characteristic that distinguishes other motion forms. As long as there is a very small difference in the initial conditions of the input, the difference between the chaotic motion trajectories can become huge.

(2) Long term unpredictability. The chaotic system is determined by the initial condition and changes with it, so the chaos is unstable locally. Therefore, it is impossible to make a long-term prediction of the chaotic motion trajectory.

(3) Boundedness. Chaotic motion should have definite infimum and infimum, which indicates that chaos has global stability and local instability. Although chaotic motion can be regarded as random like uncertain behavior, the motion of chaotic system moves in a bounded region.

(4) Non periodic. The chaotic motion is non periodic. Given the initial condition, the previous chaotic state will not be experienced repeatedly in the whole chaotic motion process [10-11].

2.4. Secure Hash Algorithm

The algorithm proposed in this paper adopts SHA-256 hash algorithm in SHA-2. In the process of transmission, the image data is likely to change, and a completely different message digest will be generated. SHA-256 algorithm has the characteristic that it is unable to recover information from the message digest and generate completely different message digest from different messages. Taking the message digest as the external key of the image encryption system, it can effectively resist exhaustive attacks and select plaintext attacks [12].

2.5. Compressed Sensing Theory [13-14]

For the non sparse signal x of length N, its sparse process can be expressed as:

$$\theta = \Psi x \tag{4}$$

Wherein, ψ N × N-size orthogonal matrix, θ Is the transform coefficient vector of the signal X. Then use an and ψ Unrelated M × Measurement matrix of n (m < n) ϕ Compress and measure the signal x, as shown in the formula:

$$y = \phi x = \phi \Psi^T \theta = A\theta \tag{5}$$

Where a is m × N-size matrix, y is the measured value. In order to ensure that the sparse signal can be reconstructed from the measured value y, the matrix A needs to meet the finite equidistant characteristic, as shown in the following formula:

$$(1-\delta_k)\|x\|_2^2 \le \|Ax\|_2^2 \le (1+\delta_k)\|x\|_2^2 \tag{6}$$

3. System Design and Implementation

3.1. Module Design and Implementation

General module refers to the module that each module needs to use in the programming process, including network programming and timer implementation.

Tcplistener is used to start TCP listening events. After each connection is completed, a new tcpconnection object will be created to identify the connection, and the socket file descriptor of the connection will be added to epoll through channel. When an event arrives, tcpconnection will be returned through channel call callback function. Epoller is a simple encapsulation of epoll, including registration, modification and deletion of FD. Channel is the encapsulation of events, thread is the simple encapsulation of Linux pthread, WorkItem is the task used to process non network events, and is encapsulated into queuechannel and added to looper. Each time looper processes events, it will put the WorkItem into the thread pool for processing [15].

In this paper, we need to use the timer function to efficiently manage the timing task by using the time wheel. The following is a time wheel implemented by using timefd. The main implementation idea of the time wheel is to use a timefd, set the corresponding trigger time interval, register the timefd into the epoll, and each time interval will trigger the read event of the epoll, and then check whether there are timed tasks in the wheel. If there are, execute, if not, skip. If there are multiple scheduled tasks on the same time scale, the linked list will be used to save the tasks and then execute them in turn. Each time an epoll read event is triggered, the scale of the time wheel will move back one grid. When it moves to the last grid, it will return to the first grid [16-17].

Service agent is an abstract concept. In this paper, there is no specific physical correspondence. Iptables rules are used to implement service agent [18].

3.2. Hardware Environment

The master node runs on the physical host with the IP address of 192.168.204.100, the worker node runs on the physical hosts 192.168.204.129 and 192.168.204.131, the two watchdog nodes run on the physical hosts 192.168.204.103 and 192.168.204.104, and the etcd cluster runs on the physical hosts 192.168.204.100, 192.168.204.129 and 192.168.204.132. Each physical host is connected through a Gigabit switch. The configuration table of each physical host is as follows

Table 1. Physical host configuration

Type	Configure
Operating system	CentOS Linux release 7.5.1804 (Core)
Processor	Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz
Memory	64G DDR3
Network card speed	1000Mb/s
Hard disk space	4T

4. System Test and Analysis

4.1. Rebound Data Test and Analysis

Data round-trip delay, CPU utilization, network card utilization, number of retroreflection generated per second, and size of sent data. The data in the following table are from the server. The initial condition is to use 20 clients to send the echo request to the echo server at the same time.

Table 2. Data of retroreflection server in the system network

Data length	Delay(ms)	10000 retroreflection / S	CPU	Network(Kb/s)
10KB	1.87	1.01	73%	115341
1KB	1.05	5.72	100%	86341
100B	0.58	6.08	100%	26548
10B	0.53	6.22	100%	15234

Table 3. Data of retroreflection server in physical host

Data length	Delay(ms)	10000 retroreflection / S	CPU	Network(Kb/s)
10KB	1.75	1.14	68%	115874
1KB	0.41	6.48	100%	75412
100B	0.22	7.35	100%	15648
10B	0.15	8.55	100%	8157

Table 4. Data of retroreflection server in flannal network

Data length	Delay(ms)	10000 retroreflection / S	CPU	Network(Kb/s)
10KB	2.03	0.98	79%	123584
1KB	1.27	5.43	100%	87412
100B	0.57	6.51	100%	23124
10B	0.51	6.55	100%	12258

It can be seen from the above three tables that the data transmission performance directly in the

physical host is significantly higher than that in the container. Because the communication across the host container needs to be forwarded by the docker0 bridge and unpacked by the vxlan protocol, and the vxlan protocol needs 50 bytes more outer data, the performance gap is more obvious in the case of small packets. In the case of small messages, the CPU occupancy rate reaches 100%, indicating that the bottleneck of this performance is CPU. Because the overlay network requires additional unpacking, the CPU has a great impact. In the case of large messages, the CPU does not reach 100%, and the network bandwidth becomes the bottleneck. Because the network cards of the testing machine are gigabit network cards, the CPU is often enough in the case of large messages. The network card bandwidth is called the bottleneck, In the case of large packets, the network delay between the overlay network and the physical machine is not much different, because the CPU has enough performance to unpack packets, so that the performance gap can be narrowed.

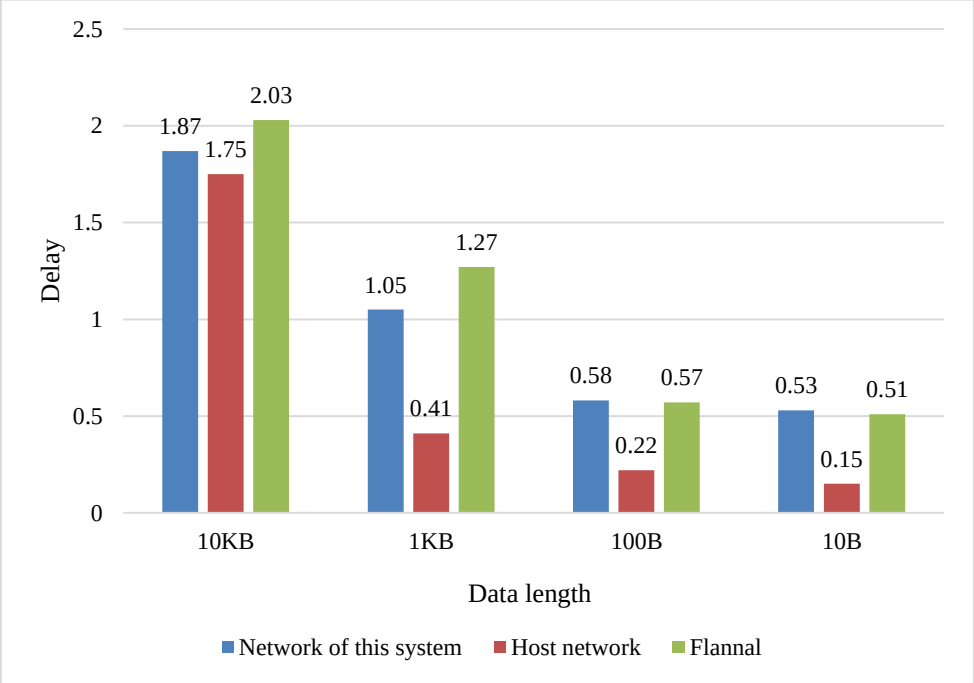

Figure 1. Packet bar graph of data packet size and delay under three network environments

The above figure more intuitively shows the performance difference between the system network, the host network and the flannal network. In the case of large messages, the performance difference between the three networks is not large, and in the case of small newspapers, the difference is more obvious. The network of this system is designed according to the original vxlan protocol, without redundant functions. Compared with the flannal network, the performance is slightly better, but the gap is not obvious. The flannal network has more complex functions, so the performance is slightly worse. According to the above data, in the case of large message transmission, the network transmission delay across the host container and the network delay directly transmitted by the real physical machine have little difference. Therefore, in this system, it is more suitable for the network scenario of message transmission.

5. Conclusion

With the rapid development of information technology, more and more information such as voice,

image and video are transmitted in daily communication. Because digital images can vividly, intuitively and vividly present and express information This paper designs and develops a platform system that combines chaos theory and encryption algorithm with distributed system, and then tests and analyzes it. It can well meet the network needs of daily use, and can also adapt to the transmission network scenarios of large-scale articles.

Funding

This article is not supported by any foundation.

Data Availability

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Conflict of Interest

The author states that this article has no conflict of interest.

References

[1] Goldstein A, Kislyakov S, Fenomenov M. Chaos Theory Methods for Contact-Center Dinamic Control. Proceedings of Telecommunication Universities, 2021, 7(2):18-23.

[2] Taylor P. How Chaos Theory is Changing Management Tech. ITNOW, 2021, 63(3):58-59.

[3] Vzhytynska K Y. Chaos Theory In The Business Space. Collection of Scientific Publications NUS, 2021(1):106-110.

[4] Bhardwaj K K, Banyal S, Sharma D K. Probabilistic routing protocol with firefly particle swarm optimisation for delay tolerant networks enhanced with chaos theory. International Journal of Innovative Computing and Applications, 2021, 12(2/3):123.

[5] Rusu-Anghel S, Mezinescu S S, Lihaciu I C. Experimental stand and researches on pantograph-catenary contact force control using chaos theory. Journal of Physics: Conference Series, 2021, 1781(1):012029-.

[6] Cha D S, Kim K I. Evaluation of the Validity of Chaos Theory Based on Systems Thinking for Non-Physicists. Open Journal of Applied Sciences, 2021, 12(5):10.

[7] Pedraza A, Deniz O, Bueno G. Approaching Adversarial Example Classification with Chaos Theory. Entropy, 2020, 22(11):1201.

[8] Postavaru O, Anton S R, Toma A. COVID-19 pandemic and chaos theory. Mathematics and Computers in Simulation, 2021, 181:138-149.

[9] Hanweck G A. Identifying House Price Booms, Bubbles and Busts: A Disequilibrium Analysis from Chaos Theory. Journal of Mathematical Finance, 2020, 10(3):448-463.

[10] Alshammari B. Cryptanalysis of a Bilateral-Diffusion image encryption algorithm based on dynamical compound chaos. Przeglad Elektrotechniczny, 2021, 1(1):130-133.

[11] Hamamreh R, Tabib E. Selective Image Compression-Encryption Algorithm Using Adaptive Huffman Coding And Aes. Journal of Theoretical and Applied Information Technology, 2021, 99(4):932-945.

[12] Hussien F, Rahma A, Wahab H. A Secure Environment Using a New Lightweight AES Encryption Algorithm for E-Commerce Websites. Security and Communication Networks, 2021,

2021(6):1-15.
[13] Sun J. 2D-SCMCI hyperchaotic map for image encryption algorithm. IEEE Access, 2021, PP(99):1-1.
[14] Elghandour A N, Salah A M, Elmasry Y A, et al. An Image Encryption Algorithm Based on Bisection Method and One-Dimensional Piecewise Chaotic Map. IEEE Access, 2021, PP(99):1-1.
[15] Rekha C, Krishnamurthy G N. An optimized encryption algorithm and F function with dynamic substitution for creating S-box and P-box entries for blowfish algorithm. Computer Science and Information Technologies, 2021, 2(1):16-25.
[16] Thomas A, Narasimhan V L. Symmetric and Asymmetric Encryption Algorithm Modeling on CPU Execution Time as Employed Over a Mobile Environment. International Journal of Natural Computing Research, 2021, 10(2):21-41.
[17] Kamal S T, Hosny K M, Elgindy T M, et al. A New Image Encryption Algorithm for Grey and Color Medical Images. IEEE Access, 2021, PP(99):1-1.
[18] Zoss B M, Mateo D, Kuan Y K, et al. Distributed system of autonomous buoys for scalable deployment and monitoring of large waterbodies. Autonomous Robots, 2018(11):1669-1689.