Hindawi
Mobile Information Systems
Volume 2021, Article ID 6607130, 8 pages
https://doi.org/10.1155/2021/6607130

Research Article

Information Security of New Media Art Platform of Distributed System Based on Blockchain Technology

Bozuo Zhao,[1] Rui Kong ,[1,2] and Wei Miao[3]

[1]*School of Management, Shih Chien University, Taipei 03724401, Taiwan*
[2]*School of Art, Tianjin University of Commerce, Tianjin 300222, China*
[3]*College of Foundation and Art, Shandong Vocational College of Industry, Zibo 255000, Shandong, China*

Correspondence should be addressed to Rui Kong; kongrui@tjcu.edu.cn

Received 24 May 2021; Revised 16 June 2021; Accepted 2 July 2021; Published 22 July 2021

Academic Editor: Sang-Bing Tsai

New media art is different from ready-made art, installation art, body art, and land art. New media art is a new art subject category with "optical" media and electronic media as the basic language. And, because of the continuous development of computer networks, distributed database management systems are becoming more and more popular. This article aims to study the information security control problem in the distributed new media system. Through comprehensive access control, reliable support, and many-to-many random mutual encryption, it solves the security requirements of supporting mobile computing in a distributed network environment, communication, and hierarchical grouping. Group key management and other issues have studied some key security technologies for building secure distributed information systems. This article proposes covering the behavior-based access control model ABAC (operation-based access control model), the architecture of the new Trusted Platform Module, the architecture of multithreaded crypto chips, and their service methods, as well as distributed information systems and key management solutions. Approximately obeying the chi-square distribution with 2 degrees of freedom, when the significance level is taken as 5%, the chi-square value for the skin is 5.99. Different initial values are selected for the chaotic sequence, 200 groups of chaotic sequences with a length of 2000 are selected for sequence inspection, and the pass rate is 97.5%. It can be seen that the autocorrelation and cross-correlation characteristics of the improved spatiotemporal chaotic sequence are still relatively ideal, so the usability of the platform is relatively high.

1. Introduction

1.1. Background. With the development of computer technology, network communication technology, and multimedia information and processing technology, network media are widely used in education, healthcare, news, business, management, and military fields. Compared with traditional art, new media art is a brand-new field, and the creation of new media art by artists is often realized by means of digital technology. The development and evolution of digital technology have deeply affected the overall form and content of new media art. Multimedia information adds more and more abundant digital content to people's lives. With the maturity of computer technology, this medium containing text, graphics, images, animation, audio, and video is slowly expanding. The development of information technology has promoted the progress of society and the improvement of people's living standards. As a heterogeneous, open, and distributed mobile network, the communication network system has diverse information dissemination channels, but, in terms of politics, economy, military, and so forth, sensitive multimedia information is transmitted through open channels or public domains. The database is vulnerable to the theft of sales information and data leakage. Therefore, the study of secure media encryption information becomes more and more important.

1.2. Significance. Today's science and technology are mainly based on technical elements such as electronic computers, bit rates, and the Internet. Physics, electronics, biology and genetic engineering, and various new technological concepts

have created a new art called "new media art." New media art is a discipline based on digital technology; it is the crystallization of close cooperation between science, technology, and art. No matter what, digital new media art has brought new experiences and new changes to our lives. Distributed information system is a form of information resource management in distributed communication network system. As an organic combination of digital communication technology, information technology, portable computers, and many parts of secure communication, it runs organizational structure and functions on the Internet. The optimization and reorganization of the process go beyond the separation of space and departments and can provide comprehensive, standardized, and transparent resource management services.

1.3. Related Work. Aiming at the comprehensive security protection requirements of multimedia information, Jiang proposed a new algorithm based on homomorphic encryption and watermarking. Under the proposed algorithm scheme, the plaintext watermark embedding operation is mapped to the ciphertext domain through homomorphism, and the plaintext watermark is embedded in the ciphertext domain. At the same time, the embedded plaintext watermark is also mapped to the ciphertext domain through homomorphism, realizing the embedding of the ciphertext watermark. According to the experimental results, the sequence of watermark embedding and data encryption of the proposed algorithm does not affect the generation of the same encrypted watermark data, and the algorithm has higher security [1]. However, his experimental process is not closed, leading to discrepancies in experimental results. Kim H's research shows that the sudden increase in the frequency and complexity of cyber threats has become an obstacle to the stable development of the multimedia service environment based on the Internet of Things (IoT). The current framework for understanding and analyzing cyber threats in the field of information security (IS) is the cyber kill chain model. Among these threats, specific threats that involve advanced and continuous attacks on designated targets (companies that provide multimedia services) and cause large-scale damage are called advanced persistent threats (APT). Since there may be many threat points in the IoT-based multimedia service environment, in which the networks of various heterogeneous devices are connected through multiple paths, it is important to understand the potential paths of threats. APT is usually divided into the penetration stage from the outside to the inside of the organization and the threat stage that occurs inside the organization [2]. However, due to the uncertainty of the experimental process, there are still gaps in the experimental results. Katz Y's research believes that the government's role in security information protection has been severely shaken. Unable to control the information, the incident was recorded on mobile phones and uploaded to social media, and local organizations emerged by providing information previously restricted by local authorities [3]. However, there are many influencing factors in this research process, so there are certain differences in experimental results.

1.4. Innovation. The innovation of this article is as follows: (1) the proposed multithreaded crypto chip design plan will expand the application of cryptographic algorithms. (2) A trusted platform module is proposed to solve the problems of TPM internal sensitive information preset, backup, recovery, and so forth. (3) It provides a more comprehensive introduction to the proposed behavior-based access control model, as well as the definition of management behavior and the structure of the ABAC management model.

2. New Media Information Encryption Technology

2.1. Model of Encryption System. The security system is a special communication system aimed at the security of information systems [4, 5]. Security is aimed at authorized users of the system. Unauthorized and illegal users can attack the system in two ways:

(1) Active attack, tampering, where an attacker or hacker uses false methods (e.g., adding, deleting, repeating, destroying, etc.) to insert false messages into the system, thereby actively interfering with the system [6].

(2) Passive attack, that is, an espionage attack, using cryptocurrency intercepted by an attacker for analysis. There is a typical general security communication system $S = \{M, C, (Ep, Dx)\ (Er, Dx)\}$, plaintext space Mg, ciphertext space C, encryption/decryption, as shown in Figure 1, password conversion pair (E, Dr), and anticounterfeiting (E, D) encryption/decryption conversion pair [7, 8].

2.2. Secret Key Encryption. Private keys encryption is also called symmetric key encryption. The encryption key is required to be the same as the decryption key, and the sender and receiver must agree on the private key before communicating. Security depends on the key, and the leak of the key means that anyone can encrypt and decrypt information [9].

The encryption and decryption transformation of the symmetric key can usually be expressed as

$$\begin{aligned} E_k(M) &= C, \\ D_k(C) &= M. \end{aligned} \tag{1}$$

In the above equation, M stands for plaintext, C stands for ciphertext, K stands for the secret key used in the encryption and decryption process, E stands for encryption transformation, and D stands for decryption transformation. Symmetric key algorithms can be divided into two categories: sequence ciphers and block ciphers [10, 11].

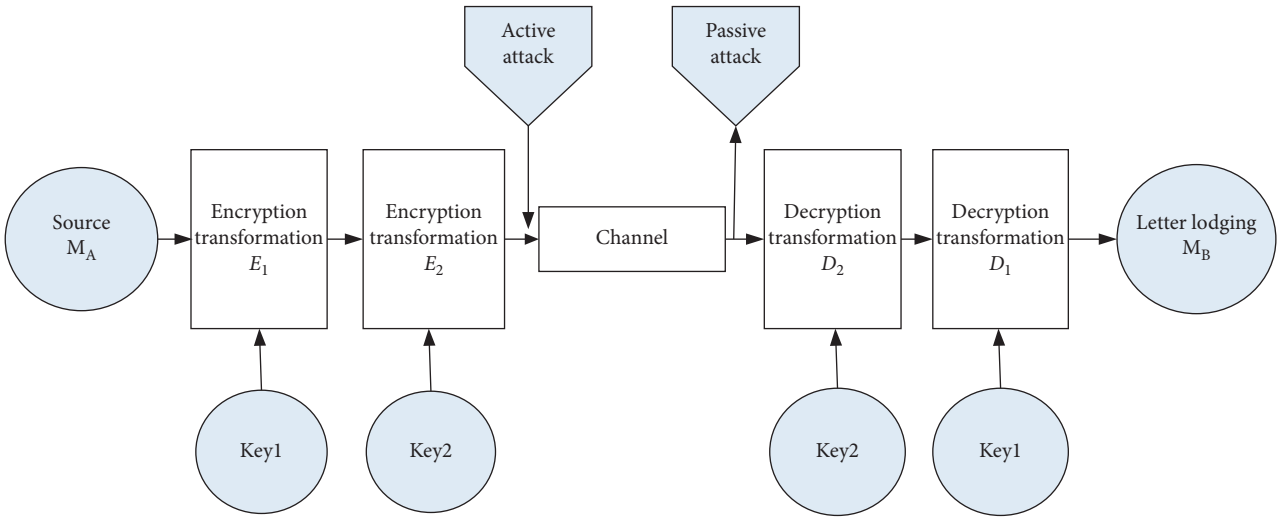

Figure 1: Generalized encryption system model.

2.2.1. Serial Password. Serial ciphers (also called stream ciphers) divide the plaintext into characters (or basic coding units, such as bits) [12, 13]. Each character is encrypted in the elementary stream, and decryption is performed by the same key stream as the encryption. A schematic diagram of the corresponding ciphertext sequence is created, which performs the exclusive OR function on the plaintext sequence and the bitwise key sequence [14, 15]. The encryption/decryption algorithm is expressed as follows:

$$\begin{aligned} c &= m \oplus k = (m_1 \oplus k_1, m_2 \oplus k_2, \ldots, m_L \oplus k_L), \\ m &= c \oplus k = (c_1 \oplus k_1, c_2 \oplus k_2, \ldots, c_L \oplus c_L). \end{aligned} \tag{2}$$

In the above equation, m represents the plaintext sequence $m = (m_1, m_2, \ldots, m_L)$, k represents the key sequence $k = (k_1, k_2, \ldots, k_L)$, and c represents the ciphertext sequence $c = (c_1, c_2, \ldots, c_L)$.

The ideal security system should use the so-called "one-time confidential" system. The communicating party must agree to an infinitely long random encryption sequence that will not be repeated (the original state is known, so that the sender and receiver can be closely synchronized) and the selected key sequence k and plaintext sequence m must be completely independent [16, 17]. However, it is difficult to create a clear random sequence encryption that meets the above requirements. Sequence encryption actually simulates the "one time one key" system, so that pure random keys are easy to create and synchronize and can manage and distribute cryptographic projects [18, 19].

2.3. Coupling Mapping Lattice. The commonly used asymmetric diffusion coupled lattice model can be written as

$$\begin{aligned} x_n(i+1) = (1-\varepsilon) f\left(x_n(i)\right) + \varepsilon\left[\alpha f\left(x_{x-1}(i)\right)\right. \\ \left. + (1-\alpha) f\left(x_{n+1}(i)\right)\right]. \end{aligned} \tag{3}$$

From the previous equation, the three following typical spatiotemporal chaotic system models are evolved [20].

One-way coupled map lattice model:

$$x_n(i+1) = (1-\varepsilon) f\left(x_n(i)\right) + \varepsilon f\left(x_{x-1}(i)\right). \tag{4}$$

Two-way coupled map lattice model:

$$x_n(i+1) = (1-\varepsilon) f\left(x_n(i)\right) + \frac{\varepsilon}{2}\left[f\left(x_{x-1}(i)\right) + f\left(x_{n+1}(i)\right)\right]. \tag{5}$$

Fully coupled map lattice model:

$$x_n(i+1) = (1-\varepsilon) f\left(x_n(i)\right) + \frac{\varepsilon}{L}\sum_{j=1}^{L} f\left(x_j(i)\right). \tag{6}$$

In equations (3)–(6), i is the discrete time coordinate, n is the discrete space coordinate, ε is the coupling coefficient, L is the length of the system, and the nonlinear image reflects the local reaction process [21]. At present, the first two models are mainly used when studying the application of spatiotemporal chaos in information encryption.

Security is another important evaluation indicator of the consensus algorithm. This section analyzes and proves the security of CRaft. CRaft guarantees the security of the algorithm through the following strategies. Introducing asymmetric encryption technology in cryptography, nodes need to carry their own public keys for identity verification when sending messages to prevent malicious nodes from forging their identities. Add the step of node verification. When voting for the Candidate node, the last log of the Candidate node needs to be verified. Only when the log verification matches will it respond; otherwise, it will refuse to respond and wait for the next vote. Therefore, the state machine security feature is established. Next, we will describe this in detail. For the setting of parameter e, we introduce the kernel density estimation function.

$$f_n(x) = \frac{1}{h}\sum_{i=1}^{h} K_n(x - x_i) = \frac{1}{nh}\sum_{i=1}^{h} K\left(\frac{x - x_i}{n}\right). \tag{7}$$

In the above equation, n represents the bandwidth, $K(x)$ represents the kernel function, and $k(x)$ satisfies the following conditions:

$$\begin{aligned} K(x) &\geq 0, \\ \int K(x)\mathrm{d}x &= 1, \\ \int xK(x) &= 0, \\ \int x^2 K(x)\mathrm{d}x &> 0. \end{aligned} \tag{8}$$

The choice of bandwidth n here will affect the results of statistics, and Mean Integrated Squared Error is usually used to optimize the value of n.

$$\begin{aligned} \mathrm{MISE}(h) &= E\int \left(f_n(x) - f(x)\right)^2 \mathrm{d}x, \\ \mathrm{AMISE}(n) &= \frac{R(K)}{nh} + \frac{1}{4}m_2 K^2 n^4 R(f), \end{aligned} \tag{9}$$

where

$$\begin{aligned} R(g) &\int g(x)^2 \mathrm{d}x, \\ m_2(K) &= \int x^2 K(x)\mathrm{d}x. \end{aligned} \tag{10}$$

In order to minimize MISE (h), it is transformed into a pole finding problem:

$$\frac{\partial}{\partial h}\mathrm{AMISE}(n) = \frac{R(K)}{nh} + m_2 K^2 n^3 R(f) = 0. \tag{11}$$

However, kernel density estimation cannot find the optimal parameters in the example, but it can estimate a reasonable parameter selection interval.

3. Sequence Randomness Test

3.1. Randomness Test. In information encryption, especially sequence cipher encryption, the pseudorandomness of spatiotemporal chaotic sequences directly affects the effect of encryption. The following is a list of methods to test the random performance of the sequence.

3.1.1. 0-1 Balance Test. The sequence has good pseudorandomness, and the quantized binary sequence also has ideal statistical characteristics and obeys a uniform distribution. The 0-1 balance test is to ensure that the numbers of 0 and 1 in the binary sequence are approximately equal. The test function can be expressed as

$$x^2 = \frac{\left(n_0 - n_1\right)^2}{n}. \tag{12}$$

In the above equation, n_0 represents the number of 0s, n_1 represents the number of 1s, and n represents the sequence length.

When the significance level is taken as 5%, the corresponding x^2 value is 3.841. If the value of the statistic is less than 3.841, it means that the sequence has passed the test. As shown in Table 1, it is an experiment on chaotic binary sequences of different lengths. As a result, it can be seen that the sequence of each length in the experiment passed the test, indicating that the binary sequence generated by the improved method has a good balance.

3.2. Sensitivity Test. In order to hide the plaintext message, Shannon proposed the concept of confusion and diffusion. The encryption system requires the full and even use of the ciphertext space. The same is true for the Hash function. For the binary representation of the Hash result, each bit has only two possibilities of 0 and 1. Therefore, the propagation effect of the ideal Hash should be plaintext, and a little change in the key will cause the probability of the Hash result to change. Figure 2 shows the construction process of the Hash function.

As can be seen from Figure 2, the transfer function of the neuron adopts the chaotic Tent mapping. The control parameters of the Tent mapping, the connection weight between the neurons, the domain value, and other parameters are all generated by the chaotic Honen mapping through multiple rounds of iteration. By combining the initial value and parameter sensitivity of chaos, the randomness of stable distribution, and the obfuscation and compression characteristics of neural networks, the obfuscation and diffusion necessary for cryptographic systems are jointly realized. This good obfuscation and diffusion effect ensures the security of the Hash function against statistical attacks. In the plaintext sensitivity experiment, the input plaintext is 1024 bits long, and the hash value is calculated, which is recorded as Hg. Change 1 bit in the input plaintext in turn, and calculate the corresponding output Hash value H.

3.3. Crash Test. The so-called collision means that different plaintext inputs produce the same Hash result; that is, multiple pair-mapping occurs. Taking the initial plaintext as 8 bits, the ASC I code range is 0~255, and the Hash result is 8 bits, which is also a number from 0 to 255, so that the plaintext space is the same as the Hash value space; remember that any-value in the Hash value space corresponds to the plaintext space. The number of original images in the center is denoted as k, and the number of points with k original images in the Hash value space is denoted as $n(k)$. Obviously, the larger $m(1)$, the smaller $n(0)$ and other items. It means that the fewer collisions, the stronger the scatter ability of the chaotic neural network. Compared with other algorithms, because the design of other algorithms is mostly related to the length of the result, the change in Hash performance is difficult to predict, and collision analysis on application scales such as 128 bits is unrealistic due to the large amount of calculation.

4. Hierarchical Group Key Management

4.1. Performance Analysis. This solution hopes to optimize the user's calculations, key storage, and key update messages. In addition, compared with other group key managements

Table 1: The balance test of the binary sequence of spatiotemporal chaos.

Sequence length	500	1000	2000	5000	10000
Number of 0s	237	521	962	2532	5023
Number of 1s	263	485	1025	2352	4962
X^2	1352	0.523	0.562	0.421	0.360

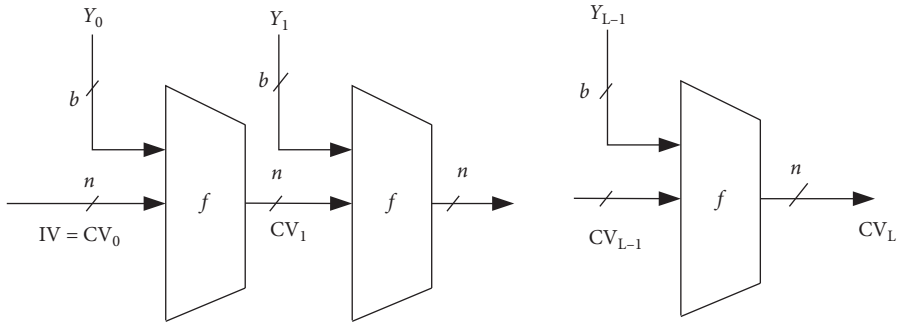

Figure 2: The construction process of the Hash function.

based on logical key hierarchy, this scheme is relatively simple and only needs to use modulo operation and multiplication operation to manage the key.

From the scheme proposed in this section, Table 2 can be obtained. It can be seen from Table 2 that the proposed scheme is relatively small in terms of computation, communication, and storage and is suitable for resource-constrained wireless networks.

4.2. Security Analysis. The rapid and effective removal of member nodes captured by attackers is of vital importance to the security of wireless networks. In this scheme, once a node is caught or an abnormality occurs, GCKS immediately executes the node withdrawal operation. The security of this scheme is based on the following assumptions: uncaught member nodes guarantee the security of their own stored keys; GCKS implants the corresponding key into the correct member node to ensure the security of the group key; all keys are randomly generated by GCKS. During the node withdrawal period, GCKS randomly generates a new group key, which is encrypted and broadcast to the group. From the above theorem's proving process, it is known that only the unrevoked nodes in the group can decrypt the new group key. Therefore, the revoked node cannot obtain its revoked group key. This scheme has forward secrecy. During the node joining phase, GCKS randomly generates a new group key and uses the current group key for encryption, so the newly joined node cannot obtain the group key before joining the group. This scheme has backward secrecy.

4.3. Load Analysis

4.3.1. Storage Load. Assuming that this scheme uses a-forked logical key tree, the total number of members in the group is denoted as N. GCKS assigns a key to each node in the logical key tree, and the total is $N-1/a-1$. From these key values, a total of (2^*-2) $(N-1)$/can be calculated $(a-1)$ An encryption key used to encrypt the group key. Each member node needs to store the key value of all nodes on the path from the corresponding leaf node to the root node. The required storage capacity is logoN, and the required storage capacity for GCKS is $N-1/a-1$.

4.3.2. Communication Load. Regardless of whether it is a member join or withdraw operation, GCKS only needs one broadcast message in this scheme, and all member nodes only need to listen to the GCKS broadcast message and extract the information they need to complete the key update. In order to measure the communication load more accurately, the number of keys in the key update message is used to measure the communication volume. Assuming that there are 1024 members in the group, each member has the same probability of being revoked due to a failure; that is, the revoked nodes are randomly distributed. Figure 3 depicts the amount of communication when the key is updated.

It can be seen from Figure 3 that the horizontal axis represents the number of revoked member nodes, and the vertical axis represents the number of keys in the key update broadcast message. It can be seen from the figure that as the number of revoked nodes increases, the communication volume gradually increases. When the revoked nodes reach a certain number, the communication volume tends to stabilize and then gradually decreases. In addition, the greater the degree of the logical key tree, the smaller the communication overhead.

4.4. Statistical Analysis of Audio Data Stream. In the MP3 audio code stream, the proportion of the scale factor data to the code stream is very small. The types of audio clips, Bass (tenor), Popm (pop song), Inst (instrument sound), Horn (trumpet), Spff (women's speech), and Spmg (men's speech), are tested and counted, and the scale factor data accounts for all The ratio of audio data is shown in Table 3.

Table 2: Performance of the proposed scheme.

Program	Encryption and decryption		Modular multiplication		Extended Euclid	Rounds	Number of keys	
	GCKS	Sensor	GCKS	Sensor	GCKS		GCKS	Sensor
System establishment	0	0	N	1	N	1	$2N-1$	$\text{Log}2N$
Secondary key	1	1	$2+N$	1	$2+N$	1		
Group key	$2\log 2N$	$\text{Log}2N$	0	0	0	1		
Leave event	$\text{Log}2N$	2	N	1	N	2		

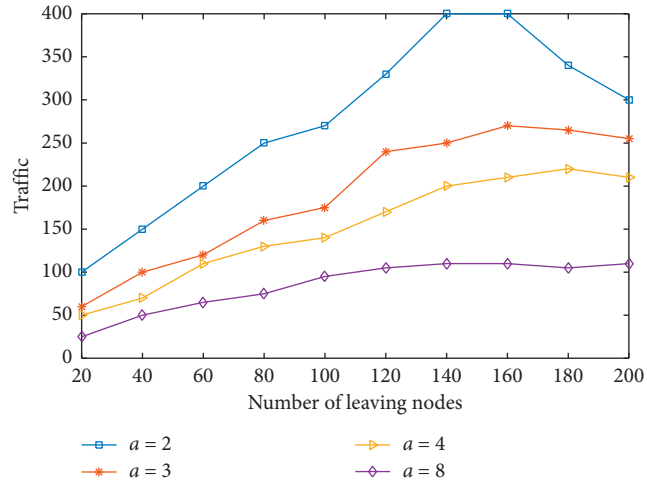

Figure 3: Communication load.

Table 3: Ratio of scale factor to audio code stream r.

Audio	Bass (%)	Popm (%)	Inst (%)	Horn (%)	Spff (%)	Spmg (%)
	4.74	5.26	6.75	4.94	6.88	6.34
r	4.86	4.64	6.24	5.24	7.15	5.94
	4.66	4.86	5.84	4.83	7.56	6.53

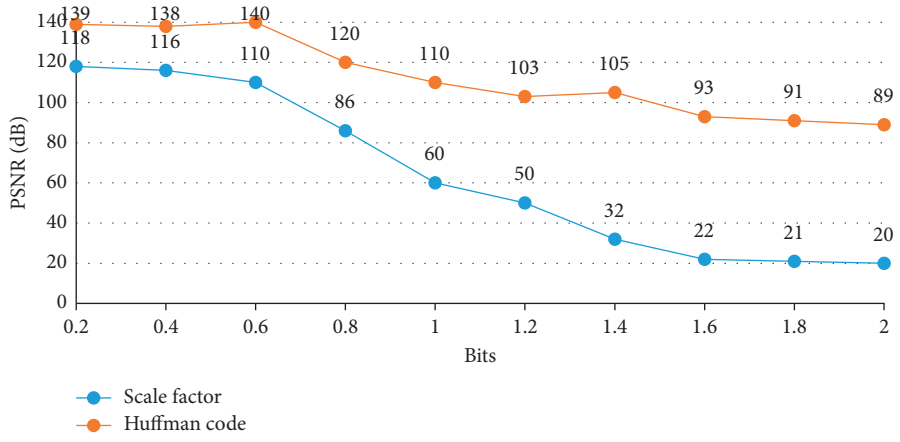

Figure 4: Comparison of sensitivity of scale factor and Huffman code to decoding.

Compared with Huffman-code data, scale-factor data has higher sensitivity to decoding. Here, the PSNR (peak signal-to-noise ratio) change of the decoded signal caused by the data error of the unit length is used to measure the sensitivity of the parameter to the decoding. From the MPEG audio coding process, it can be seen that the PSNR of the decoded signal decreases with the increase of the number of parameter errors, small. As shown in Figure 4, the PSNR average curves of the abovementioned multiple types of audio clip test results are given. It can be seen that the curve corresponding to the scale-factor data is lower than the curve corresponding to the Huffman-code data; and the slope is larger, indicating that it has a relatively high sensitivity to the decoding process.

5. Conclusions

It can be seen that the distributed multilayer application system must have a good application prospect. However, at the same time, we need to ensure that there are some problems with the structure of the distributed multitier system. For example, information system development is more complicated than traditional two-tier application systems and more difficult to design. In addition, the security measures of the application system itself are distributed, so it is also related to network security; and network security technology is constantly updated and improved. Therefore, the system security issues that need to be considered are more complicated. In addition, this article analyzes how to ensure the security of the distributed multitier application system, but since this article mainly discusses the distributed system technology of blockchain technology, in terms of chapter layout, the article first introduced the first chapter, the background, and significance and related innovations of the subject research were discussed. Then, in the second chapter, a more in-depth theoretical analysis and proof of the related theories of the chaotic system and the important conclusions covered in this paper were carried out, and several random encryptions with good performance were designed. The chaos theory and specific application key generators in the encryption of digital images and video multimedia information (block encryption and sequence encryption) will be discussed in detail later. Many existing distributed multitier application systems provide fault tolerance and load balancing capabilities. However, if you need to have the fault tolerance and load balancing capabilities of a more advanced distributed multilayer application system, you need to provide more refined load balancing algorithms and more advanced development technologies.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] L. Jiang, "The identical operands commutative encryption and watermarking based on homomorphism," *Multimedia Tools and Applications*, vol. 77, no. 23, pp. 30575–30594, 2018.

[2] H. Kim, H. Kwon, and K. K. Kim, "Modified cyber kill chain model for multimedia service environments," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3153–3170, 2019.

[3] Y. Katz, "Supremacy of social media in the hebron shooting incident," *Journalism and Mass Communication*, vol. 8, no. 3, pp. 165–173, 2018.

[4] A. Z. M. Ibrahim and J. H. Yahaya, "Information security factors in the implementation of industrial control system into cloud environment," *Advanced Science Letters*, vol. 24, no. 7, pp. 5239–5242, 2018.

[5] J.-A. Lee, "Tripartite perspective on the copyright-sharing economy in China," *Computer Law & Security Review*, vol. 35, no. 4, pp. 434–452, 2019.

[6] L. Xu, C. Jiang, J. Wang et al., "Information security in big data: privacy and data mining," *IEEE Access*, vol. 2, no. 2, pp. 1149–1176, 2017.

[7] X. Shao, Y. Ji, and H. Le, "Research and practice of cloud computing and big data in omni-directional multi-angle information security technology %. Research and practice of cloud computing and big data in omni-directional multi-angle information security technology," *Science and Technology Bulletin*, vol. 33, no. 1, pp. 76–79, 2017.

[8] Z. Trabelsi, M. Al Matrooshi, S. Al Bairaq, W. Ibrahim, and M. M. Masud, "Android based mobile apps for information security hands-on education," *Education and Information Technologies*, vol. 22, no. 1, pp. 125–144, 2017.

[9] Q. Da, J. Sun, L. Zhang et al., "A novel hybrid information security scheme for 2D vector map," *Mobile Networks and Applications*, vol. 23, no. 4, pp. 734–742, 2018.

[10] T. K. Damenu and C. Beaumont, "Analysing information security in a bank using soft systems methodology," *Information & Computer Security*, vol. 25, no. 3, pp. 240–258, 2017.

[11] A. Gasparrini, B. Armstrong, and M. G. Kenward, "DLNM: distributed lag non-linear models," *Statistics in Medicine*, vol. 29, no. 21, pp. 2224–2234, 2017.

[12] N. R. Iverson, T. S. Hooyer, and R. W. Baker, "Ring-shear studies of till deformation: coulomb-plastic behavior and distributed strain in glacier beds," *Journal of Glaciology*, vol. 44, no. 148, pp. 634–642, 2017.

[13] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[14] R. Negenborn, P. J. Overloop, T. Keviczky et al., "Distributed model predictive control of irrigation canals," *Networks and Heterogeneous Media*, vol. 4, no. 2, pp. 359–380, 2017.

[15] K. M. Chandy and L. Lamport, "Distributed snapshots: determining global states of a distributed system," *Acm Trans on Computer Systems*, vol. 3, no. 1, pp. 63–75, 2016.

[16] R. Hock and B. Holmgren, "A distributed surface energy-balance model for complex topography and its application to Storglaciären, Sweden," *Journal of Glaciology*, vol. 51, no. 172, pp. 25–36, 2017.

[17] W. Shi, X. Xie, C. C. Chu et al., "Distributed optimal energy management in microgrids," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1137–1146, 2017.

[18] H. Son and K. M. Lee, "Distributed multipole models for design and control of PM actuators and sensors," *IEEE/ASME*

Transactions on Mechatronics, vol. 13, no. 2, pp. 228–238, 2016.

[19] Z. Alymbaeva and Alimakhunov, "Threats and challenges to the information security of Kyrgyzstan," *Bulletin of Science and Practice*, vol. 7, no. 2, pp. 266–270, 2021.

[20] V. Makarchuk, "Tasks and powers of the National police of Ukraine in ensuring information security of the state," *Revista Amazonia Investiga*, vol. 10, no. 37, pp. 86–92, 2021.

[21] S. Boiko, "International information security threats as side effects of modern technologies," *International Affairs*, vol. 67, no. 2, pp. 176–186, 2021.