Research on Multimedia Data Information Security Algorithm Based on Chaos Theory

*Jie Zhao[1]
[1]College of Electronic Information Science, Fujian Jiangxia University, Fuzhou, Fujian, 350108, China.
E-mail: jiezhao3202@gmail.com
*Corresponding author

Keywords: chaos theory, multimedia, security, cryptography, algorithm

Received: January 10, 2023

Chaos theory is a fast, parallel, and globally retrievable modern intelligent optimization algorithm. At present, it has been widely used in the field of computer technology and intelligent control. Based on the complete analysis of chaos theory, this paper constructs a multimedia data information security algorithm, which can analyze the data analysis model and model convergence in detail. Finally, the experimental results show that the proposed algorithm has good performance and can effectively enhance the security and protection of multimedia data information.

Povzetek: V tem članku je na podlagi celovite analize teorije kaosa predstavljen algoritem za varnost multimedijskih podatkov, ki zagotavlja izboljšano varnost in zaščito informacij, kar potrjujejo tudi rezultati eksperimentov.

1 Introduction

With the continuous improvement of scientific and technological levels and the continuous development of Internet technology, it has been widely used in many fields. The transmission of large-scale data information on the Internet network [1-2] needs to play a more critical role in increasing its security and data protection [3]. However, multimedia data information system has their vulnerability because there is much hardware in data information protection system, and the shortcomings of software or data information security methods will lead to significant security risks [4-5]. If these vulnerabilities are used illegally, multimedia data security will be significantly threatened [6]. Therefore, the research on multimedia data information network security has attracted the focus of research at home and abroad [7-8]. In general, it is difficult to obtain satisfactory results by using previous data methods to solve the problems of data encryption and multimedia data information security. With the use of the bionic intelligent algorithm in classical problems [9], it has better global performance in application.

Based on chaos theory, this paper constructs an algorithm that can effectively solve the security of multimedia data information. Through the in-depth analysis of chaos theory and the practical comparative analysis of convergence, the performance is tested and analyzed by simulation software to highlight the scientificity and effectiveness of this algorithm.

2 Related work

Now more than ever, people worry about keeping their multimedia files safe while they are being transferred and stored. Since multimedia data comprise a considerable amount of redundant data, a vast size, and a strong correlation of data elements, conventional encryption algorithms such as DES, AES, 3-DES, and RSA cannot be used for multimedia data encryption. Dynamic multimedia data encryption can be achieved with chaos-based methods. The term "chaos" describes a set of characteristics in dynamical systems, including non-convergence, non-periodicity, and unpredictability. In cryptography and information security, the ability to generate randomness using only predictable systems is an attractive feature. Numerous significant developments have occurred in chaotic cryptography since its inception in the early 1990s. Multiple significant scientific advances have been made during this period. An introduction to chaos-based cryptography and its recent developments is provided in this paper by Al-Hazaimeh et al. (2022).

It is only possible to imagine current encryption with the contribution of chaotic maps. Most experts agree that algorithms built with chaotic maps are the most efficient and safe option. In this paper, we offer a new method for image encryption that uses a 3D mixed chaotic map. The authors propose this method to ensure that the conditions for safe image transmission are met by using a 3D mixed chaotic map to modify pixel position. They performed a cryptanalysis on the suggested scheme using previously developed techniques and compared their findings to other algorithms already published in the literature. Yasir

Ref no& Year	Methodology	Advantage	Disadvantage
[16] 2022	Chaos-based multimedia data encryption technique	Increase security	For limited applications
[17] 2019	3D mixed chaotic map	Provides secure image transmission	Resistive for limited attacks only
[20]2020	Multi-dimensional chaos, hyper and composite chaos in image encryption	Highly Secure	Need to focus on real time applications
[21]2022	Multi-stage chaos-based image encryption algorithm	Higher security and is light weigh	Need to focus on audio and video content encryption
[22]2022	Advanced Encryption Standard (AES), Data Encryption Standard (DES) and chaotic systems by using the Tent map	Less execution time	Need to focus on security issues
[23]2022	IoT-related multimedia security and privacy protection	Multimedia data protection in the IoT	Need to focus on security and attacks

Table 1: Summary of literature work

To protect data transmitted over wireless networks, many different types of encryption algorithms play critical roles. Data privacy and security are two primary applications of cryptography. As a result, an unauthorized user cannot compromise the original data. More security is added to programs by employing encryption methods and many beneficial algorithms. The widely recognized technique of chaotic algorithm is utilized in this paper by Priyanka Tiwari et al. (2014). Secure real-time picture transmission methods employ a chaotic algorithm. This algorithm is often used as an effective means of encryption and decryption in academic studies. There play a crucial role in integrating chaos theory and cryptography in Information Security. This message proposes a novel chaotic map-based image encryption technique for grayscale 2D images. This suggested approach begins with the raw or original image, which has MXN dimensions. Then Pixels can be redistributed pair-wise, with only the verified owner knowing the relocation criteria. This method involves iteratively scrambling all of the image's pixels to maximize energy scattering.

Cryptography relies on several subfields, one of which is the production of keys and associated sequences. Stream cipher previously utilized pseudo-random number generators for the key sequence. After their evolution, the properties of chaotic systems were superior to those of pseudo-random number generators. In this study, Naseer et al. (2019) offers a method superior to previous algorithms in safe picture transmission; their results from security analysis, statistical analysis, and differential analysis back up this claim.

The safety of digital and multimedia transmissions through wireless networks is crucial. When it comes Sheela S. et al. (2017) attempted to investigate chaotic systems' theoretical foundations, classifications, and characteristics. In addition to discussing chaotic systems, we go over how to generate sequences with chaotic systems and how to use sequences in different kinds of image encryption. At last, an appropriate method for generating key sequences utilizing a chaotic system is provided.

There has been a rise in the development and deployment of trustworthy picture encryption techniques in response to the growing importance of secure digital communication and the proliferation of digital technologies. In their publication, "Chaos Theory and Its Application in Image Encryption Schemes," Arshad et al. (2020) provide a comprehensive overview of this topic. The advantages of chaos-based picture encryption algorithms over more conventional encryption methods stem from their ergodicity and initial key sensitivity. The study focuses on one of chaos theory's most important application areas, picture encryption. Images can be encrypted using a variety of chaotic maps, including one-dimensional chaos, multi-dimensional chaos, hyper-chaos, and composite chaos.

Additionally, the article covers state of the art in chaotic image encryption as well as the future directions of the field. This work lays the groundwork for future studies and helps newcomers get up to speed quickly. A chaos-based cryptosystem has been the subject of several suggestions for enhancement.

The multi-stage chaos-based picture encryption technique is the basis for the image encryption scheme presented in this paper by Fadia Ali Khan et al. (2022). Confusion and diffusion are crucial to the method's efficacy. Compared to the current methods, the proposed one, which incorporates confusion and

diffusion modules, is much more secure and efficient. At the outset, an image is split into three equal parts (RGB), each divided into blocks of the same size. Tinkerbell Chaotic Map (TBCM) is applied to each block individually to generate random-ordered blocks and pixels. Composite Fractal Function (CFF) modifies the pixel values of each color channel (layer) to generate a chaotic pattern. Three layers of a simple image are encrypted using the resulting random sequence.

Table 1 shows summary of related works. Finally, XORing Brownian Particles (BP) provides additional protection with each encrypted layer. A battery of statistical and experimental tests verified the security of the proposed approach. According to the data presented in the research, the suggested strategy is more secure and less resource intensive than existing methods in the field.

In order to determine how to secure two different encryption algorithms when applied to text, Ismehene Chaouch et al. (2022) conducted an analysis study. The first is the tried-and-true methods of encryption, known as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), respectively (DES). A second source is research into chaotic systems utilizing the Tent diagram. The examination of experimental findings demonstrates that the chaotic encryption algorithm is superior to traditional methods in terms of security and efficiency. Furthermore, the chaotic system has a high rate of encryption.

Due to this sector's swift development, massive amounts of multimedia data are being produced and transferred across numerous IoT devices, systems, and applications. However, the security and privacy of multimedia data have surfaced as important problems that may hinder the widespread adoption of IoT devices in data-sensitive settings. W. Yang et al. (2022) perform an extensive literature review on multimedia data security and privacy protection in the IoT. They start by categorizing multimedia files into distinct groups and degrees of protection based on their intended use. They then evaluate and debate the IoT's multimedia data protection mechanisms, such as cryptography, watermarking, and various newer technologies like blockchain and federated learning. They aim to advance the study in the relevant fields and help researchers gain a deeper understanding of state of the art on multimedia data protection in the IoT by providing a detailed analysis of the research development of IoT-related multimedia security and privacy protection, pointing out some open challenges, and providing future research directions.

This work develops an algorithm based on chaos theory that may successfully address the security of multimedia data by taking into account the shortcomings of current techniques. To demonstrate the science and effectiveness of this algorithm that can successfully address the security of multimedia data information, the performance is tested and analysed by simulation software using the in-depth analysis of chaos theory and the practical comparative analysis of convergence. Simulation software is used to test and assess the performance, highlighting the objectivity and efficacy of this algorithm via a thorough examination of chaos theory and a realistic comparison study of convergence.

3 Chaos theory

Chaos refers to a deterministic system, which may occur under nonlinear interaction. It is a very sensitive and irregular complex motion to the initial value. It is the unity of the contradiction between local instability and global stability. So far, the specificity and complexity of a chaotic system have yet to be fully understood, and chaos has not been strictly defined [10]. Chaos is not a simple disorder but an ordered structure without a clear period, symmetry, and rich internal layers. It is a new form of existence in nonlinear systems.

A straightforward and widely studied chaotic power system is logistic mapping, which is defined as follows:

$$x_{i+1} = \mu x_i \left(1 - x_i\right), i = 1, 2, \cdots \tag{1}$$

The double period branching diagram of the logistic map is shown in Figure 1, which defines the whole process of the logistic map branching into chaos according to the double period.

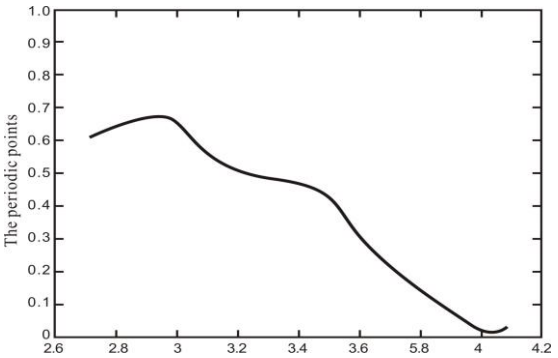

Figure 1: period-doubling bifurcation diagram of the logistic map.

The probability distribution density function of chaotic sequence is

$$\rho\left(x\right) = \frac{1}{\pi\sqrt{1-x^2}}, -1 < x < 1 \tag{2}$$

Some interesting statistical properties of $\rho\left(x\right)$ chaotic sequences generated by Logistic mapping are easily obtained. The average value of trajectory points of the chaotic sequence is X

$$\bar{x} = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} x_i = \int_0^1 x\rho\left(x\right) dx = 0.5 \tag{3}$$

The cross-correlation function of two initial x_0 y_0 sequences can be selected independently for the correlation function.

$$c(l)=\lim_{N\to\infty}\left\{(1/N)\sum_{i=0}^{N-1}\left(x_i-\bar{x}\right)\left(y_{i+1}-\bar{y}\right)\right\} \quad (4)$$
$$=\int_0^1\int_0^1\rho(x,y)\left(\vec{x}-x\right)\left(\tau^l(y)-\bar{y}\right)dxdy=0$$

Since the encryption method of multimedia data information is a digital quantity, it mainly maps $\{X_i\}$ to all pseudo-random number sequences according to the sequence composed of real numbers. It encrypts the data information simultaneously [11-12]. The commonly used mapping method uses the significant digits after the decimal places to form an integer. Therefore, according to the Logistic chaotic map shown in Figure 2, the encryption/decoding model is adopted. This paper designs and completes a data information encryption algorithm, as shown in Figure 3.

X_i The decoding process is essentially the reverse process of encryption. Taking the initial values x_0 μ as variable parameters in the logistic Equation, it is mainly calculated from repeated m, and the other parts are mainly taken as 255. Finally, the data information in the data information is different or the obtained encrypted ciphertext [13-14]. After the data information is replaced, the data in the generated sequence is the same as each value of the encrypted data information, which is conducive to enhancing the resistance to attack.

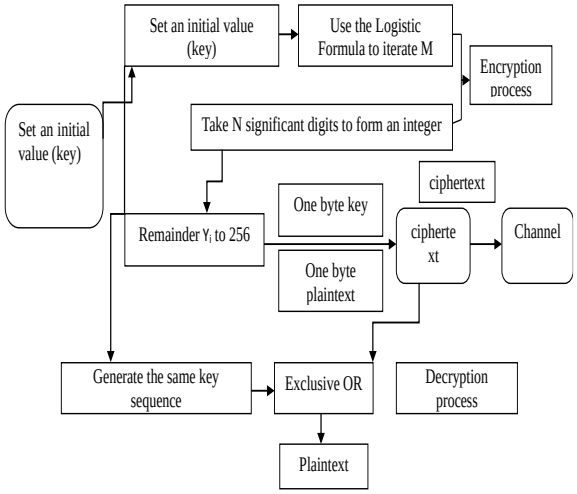

Figure 2: Encryption/decryption model.

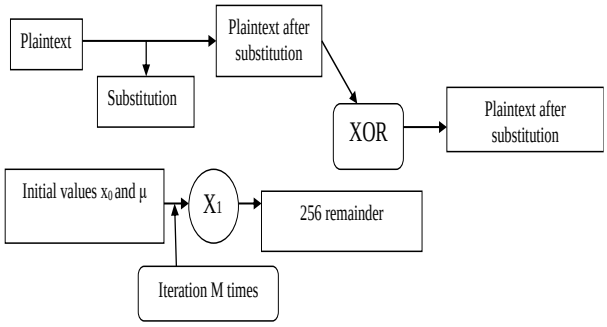

Figure 3: Encryption algorithm.

Improving the adaptability to the selected data information attack is to process the X_i row data,

Making the relationship between X_i X_{i+1} and complex, to avoid the attacker solving the μ value through simple operation [15]. If a number is separated between X_i and X_{i+1}, the relationship between X_i and X_{i+1} becomes:

$$x_{i+1}=\mu\left(\mu x_i\left(1-x_i\right)\right)\left(1-\mu x_i\left(1-x_i\right)\right) \quad (5)$$

3.1 Multimedia data information security algorithm

Initial population selection

Research summary: The initial population performance seriously affects the convergence performance of all algorithms [7]. Traditional chaos theory uses random methods to generate the initial population and inevitably increases the amount of extra computation. When the initial population N value is small, the operation speed can be improved, but the diversity of the population will be reduced, which can easily cause premature convergence. If N is large, the algorithm is going to be less efficient.

In order to improve the nature of the initial group, it is necessary to improve the convergence speed and effect to some extent to insert some individuals with superior performance into the initial group. In this paper, the generation of the initial group is almost random, and a few parts are generated by prior knowledge, and the method combining the two is adopted. Experimental results show that this strategy can better combine the prior information of a particular problem, reduce the time complexity of the calculation without affecting the convergence effect, and find a better and optimal solution.

Selection of turbidity function

1) In chaos theory, the choice of turbidity function is critical, directly affecting the convergence rate of chaos theory and whether the best solution is found. Generally speaking, the design of the turbidity

function should satisfy some critical conditions. 2) Can reflect the reasonable and consistent, that is, the advantages and disadvantages of the corresponding solution. 3) Small computation, that is, short time and space complexity. 4) Generality.

In order to design a good algorithm, this paper considers several design standards of the algorithm simultaneously so that the designed box can reach a globally optimal solution in multiple encryption features. The two most effective attacks against group ciphers are linear and differential attacks. At the same time, based on the design principle of the algorithm, this paper considers the encryption nonlinear, difference uniformity, orthogonality, avalanche effect characteristics of the algorithm, and the essential encryption characteristics of the algorithm are designed.

The selection of adaptation function in this paper is shown in Equation (6) :

$$f(S)=a_s f_s(N_s)+a_d f_d(\delta_S)+a_B f_B(B_S) \quad (6)$$

In order to describe the avalanche effect quantitatively, the definition of "avalanche degree" is given. In this paper, let

$$S(x)=(f_1(x), f_2(x),\cdots, f_m(x)): F_2^n \to F_2^m$$

be a multi-output function, and call B_S the avalanche degree of S(x), where B_S is expressed by Equation (7) :

$$B_S=\frac{1}{2^n}\sum_{a\in F_2^n}\sum_{d_H(a,\beta)=1}\left(\frac{m}{2}-d_H(S(a),S(\beta))\right) \quad (7)$$

Select operation

The usual selection operations in chaos theory are; calculates the The roulette & selection method first fitness value of each column in a generation group and then calculates the proportion of the fitness value of the whole group. That is the probability that the individual will be selected during the selection process. In this paper, for the algorithm population $S=\{s_1, s_2,\cdots, s_j,\cdots, s_n\}$ with a given size of n, the adaptation value of the individual s_j is $f(s_j)$, and the selection probability is

$$P(s_j)$$

$$P(s_j)=\frac{f(s_j)}{\sum_{j=1}^{n} f(s_j)}=\frac{f_j}{\sum_{j=1}^{n} f_j}=\frac{f_j}{n\overline{f}} \quad (8)$$

Formula (8) $\overline{f}$ is the mean of the adaptive value of the algorithm group.

In order to reduce the difference of each selection probability, the selective pressure drop method is used to adjust the turbine's function in the early stage of evolution, and the Formula is used in the linear matching value scale transformation.

$$f'=af+b \quad (9)$$

In the Formula, f is the original adaptive function value, f&; Set the optimal individual adaptation value after conversion as the value of the adaptive function after conversion.

$$f'_{\max}=c\overline{f} \quad (10)$$

In the Formula, c=1.5 is the empirical value. The average turbidity before and after the transformation should remain unchanged, i.e., $\overline{f'}=\overline{f}$ the equation group is obtained.

$$\begin{cases} f'_{\max}=af_{\max}+b \\ \overline{f}=af+b \end{cases} \quad (11)$$

The solution of (5) and (6) can be obtained as follows:

$$\begin{cases} a=(c-1)\overline{f}/(f_{\max}-\overline{f}) \\ b=(f_{\max}-c\overline{f})\overline{f}/(f_{\max}-\overline{f}) \end{cases} \quad (12)$$

After the change, the selection probability p'_j of the individual is:

$$p'_j=\frac{f'_j}{\sum_{j=1}^{n} f'_j}=\frac{af_j+b}{a\sum_{j=1}^{n} f_j+nb}=\frac{af_i+b}{n(a\overline{f}+b)}=ap_j+\frac{b}{n\overline{f}} \quad (13)$$

In late evolution, the group maintains a relatively stable diversity. This paper introduces a mechanism for both parents and children to participate in the selection to speed up the search and save the time and complexity of computing.

Crossover operation and mutation operation

The selection of crossover probability (P_c) and mutation probability (P_m) is an essential factor in the chaos concept's result, and the computation convergence is fast. The cross operation is typically carried out from three angles (1) good genetic factors have the chance of inheritance and inheritance to the next generation. (2) Can have excellent gene results for the results of cross-operation. (3) The crossover scheme has a great relationship with the coding of the

problem, and it needs to be combined with the scheme design of coding bit string effectively.

The crossover operation method in this paper is the first operation process. There are two joint genetic opportunities, and the design criterion of the crossover operation in the calculation is satisfied. The selection of the crossover probability can determine the frequency of the crossover operation. At the same time, when the frequency is high, the convergence effect can reach its best. If the value is too large, the collective value result will be affected; if the value converges too early, the later operation result will be affected. If there are many, the birth rate of new individuals will be slowed. To solve this problem, the operation method in this paper is modified dynamically. That is, the crossover probability is changed with iteration algebra. Figure 4(a) shows the relationship between the crossover probability P_c and the advanced algebra T. The previous operation that P_c obtains the maximum value P_{cM} $3/5P_{cM}$ is taken at the end of evolution, and the middle part shows a linear downward trend. Experimental results show that the crossing rules can improve search efficiency and speed up the algorithm's convergence to some extent.

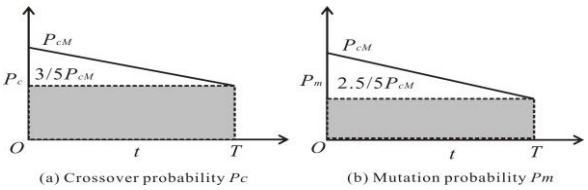

Figure 4: The relationship between crossover P_c, mutation probability P_m, and evolutionary algebra T.

4 Simulation verification

Two experiments were conducted to prove the above chaotic conclusion and the design box's feasibility and efficiency.

(1) The initial population of the algorithm is entirely randomly generated, and the crossover probability and mutation probability are fixed $P_c = 0.65$ $P_m = 0.5$,

(2) The initial population of the algorithm is added into 8 boxes of DES (Data Encryption Standard) [15], and the crossover probability (P_c) and mutation probability (P_m) are respectively modified by the above dynamic linear method.

In the first experiment, the population value was N=1024, and the evolutionary value was T=1200. The password values calculated by evolution are shown in Figure 5. It can be seen from Table 2 (is the nonlinearity, is the difference uniformity, and the corresponding data value calculation is the calculation method value). It can be seen from the results that both the nonlinearity of the calculation method and the difference uniformity degree have been improved, nearly 61.43% on the whole (is the 4 elements in the lower right corner of Table 2, (110+126+104+289) /1024) is concentrated in the nonlinear and high difference position, which proves that the calculation method of chaos concept has a good effect on the optimization of cryptography, and the calculation method is perfect.

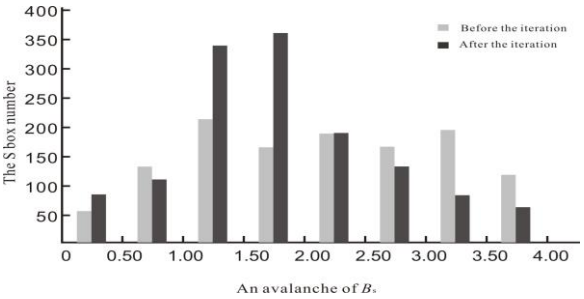

Figure 5: Distribution curve of avalanche degree before and after the first experimental iteration.

Figure 5 shows the B_S distribution curve of avalanches before and after the first set of experimental repeats. After chaos theory optimization of the initial population, the avalanche degree of the whole population is also improved, and most of the avalanche degree is concentrated around 1.5. According to the avalanche degree calculation, about 40 individuals meet the strict avalanche effect.

In the second set of experiments, the parameters were set as N = 1024, $P_c = 0.65$ T=800 and the method of dynamic linear correction was used to optimize the encryption performance of the algorithm, as shown in Table 3 and Figure 6. P_c P_m can see from Table 3 that by optimizing the algorithm, the nonlinear and difference uniformity of the algorithm is better \By comparing the avalanche degree distribution curves after repeated experiments of the two groups (FIG. 3 and FIG. 4), the average avalanche degree and the individuals meeting the strict avalanche effect obtained in the second group of experiments are significantly improved compared with those obtained in the

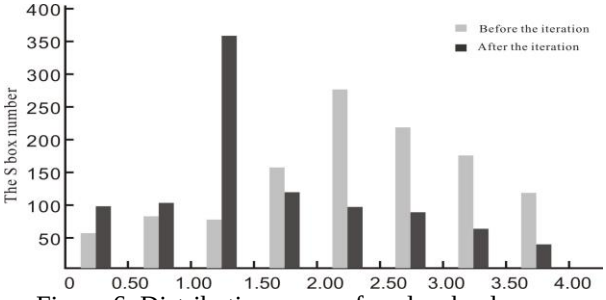

Figure 6: Distribution curve of avalanche degree before and after the second experimental iteration.

The experimental results of the two groups are shown in Figure 7. The average turbid evolution value represents the convergence rate and the effect diagram of two sets of experimental results of each expected value between the convergence result and the chaos value. The figure assumes that the crossover probability value and the different probability values are fixed. It is known from the experimental data of the first group that convergence occurs when the repetition is over 1100 years old. The average value is 18.5, which is lower than the experimental data of the improved and is close to 71.19% in the whole group. In terms of difference uniformity, Figure 6 shows the avalanche distribution curve before and after the experimental iteration of the second group. After the algorithm in this paper optimizes the initial group, the overall avalanche degree is greatly improved, with most avalanches concentrated around 0.75. According to the avalanche calculation, about 90 individuals have achieved the strict avalanche effect. The second set of experiments is better improved than the first, and the optimization algorithm is.

Proposed in this paper is sufficient to improve algorithm encryption's characteristics effectively.

The reason is that the initial population data in the first group of the experimental calculation method is not random, indicating that the results of the initial population will lead to the convergence data of the whole calculation method. In the second group of experiments, the calculation method generated before prior knowledge is added to change the data's crossover probability and difference probability dynamically. The average turbidity value is as high as about 20.5. When the convergence value is about 8000, it can reach more than 350, about 33% of the calculation method containing encryption.

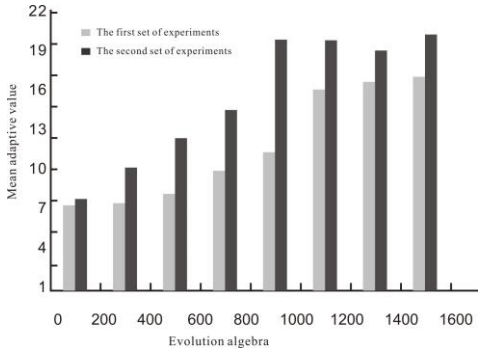

Figure 7: Mean turbidity - evolutionary algebraic curve.

Table 2: Distribution of δ_S N_S and before and after iteration.

δ_S	Before the iteration N_S					After the iteration N_S				
	17	18	19	20	21	17	18	19	20	21
20	18	25	28	26	27	9	8	7	3	4
19	15	43	51	65	37	10	19	9	15	16
18	23	47	95	89	38	17	19	24	38	34
17	15	51	66	84	50	20	55	33	111	127
16	12	17	45	47	20	6	34	23	104	289

Table 3: Distribution of the sum of algorithms before and after iteration.

δ_S	Before the iteration N_S					After the iteration N_S				
	17	18	19	20	21	17	18	19	20	21
20	19	27	30	30	28	7	9	5	4	2
19	15	43	54	69	38	6	17	9	8	6
18	21	48	93	86	39	14	20	31	35	25
17	15	53	61	86	46	10	19	37	123	148
16	13	18	47	48	22	9	18	25	135	327

5 Conclusion

This paper proposes a multimedia data information security algorithm based on an effective combination of chaos theory. The algorithm can save the operation time of the algorithm effectively and obtain the optimal solution in a short time without affecting the convergence of the chaos algorithm. Finally, the experimental results show that the algorithm has a good convergence effect and nonlinearity compared with the traditional algorithm, has better data information security, and has a specific application value.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest

Funding Statement

Educational research projects of young and middle-aged teachers in Fujian Province sponsor this research study. The name of the project is Research on Chinese character cryptography algorithm based on NTRU and ancient philosophy. The project number is JT180592. The paper is published for the conclusion of the project. Thank the project for supporting this article!

References

[1] Wang, S., Li, Y., Xu, R., Wei, Y., & Shao, S. . (2016). Research on characteristics of first-order sea clutter for hf sky-surface wave radar. IET Microwaves Antennas & Propagation, 10(10), 1124-1134. DOI: 10.1049/iet-map.2014.0771

[2] Xiaoming, Fu, Dirk, Kutscher, Satyajayant, & Misra, et al. (2018). Information-centric networking security. IEEE Communications Magazine,6(8), 43-47. DOI: 10.1109/MCOM.2018.8539022

[3] Francia G A , Ming Y , Trifas M . Applied image processing to multimedia information security[C]// International Conference on ImageAnalysis & Signal Processing. IEEE, 2009.

[4] Bera, A., Kumar, A., Rakshit, D., Prabhu, R., & Sen, U. (2015). Information complementarity in multipartite quantum states and security in cryptography. Physical Review A, 93(3), 166-168. DOI: https://doi.org/10.1103/PhysRevA.93.032338

[5] Alam, M., and M. U. Bokhari. "Information Security Policy Architecture." International Conference on Computational Intelligence & Multimedia Applications IEEE Computer Society, 2007. DOI:10.1109/ICCIMA.2007.275

[6] Hausken, K. , & He, F. . (2016). On the effectiveness of security countermeasures for critical infrastructures. Risk Analysis, 36(4), 711-726. DOI: 10.1111/risa.12318

[7] Ji, W. , Li, Z. , Poor, H. V. , Timmerer, C. , & Zhu, W. . (2019). Guest editorial multimedia economics for future networks: theory, methods, and applications. IEEE Journal on Selected Areas in Communications, 37(7), 1473-1477. DOI: 10.1109/JSAC.2019.2918962

[8] Canovas, A. , Jimenez, J. M. , Romero, O. , & Lloret, J. . (2018). Multimedia data flow traffic classification using intelligent models based on traffic patterns. IEEE Network, 32(6), 100-107. DOI: 10.1109/MNET.2018.1800121

[9] Britto, P. X. , & Selvan, S. . (2019). A hybrid soft computing: sgp clustering methodology for enhancing network lifetime in wireless multimedia sensor networks. Soft Computing., 59(6.), 117-125. https://doi.org/10.1007/s00500-018-03716-3

[10] Pan, Zhou, Yingxue, Zhou, Dapeng, & Wu, et al. (2016). Differentially private online learning for cloud-based video recommendation with multimedia big data in social networks. IEEE Transactions on Multimedia, 13(8), 2709-2714. DOI: 10.1109/TMM.2016.2537216.

[11] Canovas, A. , Jimenez, J. M. , Romero, O. , & Lloret, J. . (2018). Multimedia data flow traffic classification using intelligent models based on traffic patterns. IEEE Network.12(4), 46-58. DOI: 10.1109/MNET.2018.1800121

[12] Cho, K. , Courville, A. , & Bengio, Y. . (2015). Describing multimedia content using attention-based encoder-decoder networks. IEEE Transactions on Multimedia, 17(11), 1875-1886. https://doi.org/10.1109/TMM.2015.2477044

[13] Khattak, S. , Jan, S. , Ahmad, I. , Wadud, Z. , & Khan, F. Q. . (2020). An effective security assessment approach for internet banking services via deep analysis of multimedia data. Multimedia Systems, 27(4), 733-751. https://doi.org/10.1007/s00530-020-00680-7

[14] Ghadi, M. , Laouamer, L. , & Moulahi, T. . (2016). Securing data exchange in wireless multimedia sensor networks: perspectives and challenges. Multimedia Tools and Applications, 75(6), 3425-3451. https://doi.org/10.1007/s11042-014-2443-y

[15] Verdoliva, & Luisa. (2016). Handbook of digital forensics of multimedia data and devices [book reviews]. Signal Processing Magazine IEEE, 33(1), 164-165.

[16] Al-Hazaimeh, Obaida & Abu-Ein, Ashraf & Al-N'awashi, Malek & Gharaibeh, Nasr. (2022). Chaotic based multimedia encryption: a survey for network and internet security. Bulletin of

Electrical Engineering and Informatics. 11. 2151-2159. 10.11591/eei.v11i4.3520.

[17] Yasir Naseer et al., “A novel approach to improve multimedia security utilizing 3D mixed chaotic map,” Microprocessors and Microsystems, Volume 65, 2019, Pages 1-6. https://doi.org/10.1016/j.micpro.2018.12.003

[18] Priyanka Tiwari et al., "Chaos Based Information Security in Multimedia Communication" International Journal of Current Engineering and Technology, Vol.4,No.3 (June- 2014) https://doi.org/10.3390/e22111253

[19] Sheela S. & S. V. Sathyanarayana “Application of chaos theory in data security-a survey” ACCENTS , Transactions on Information Security, Vol 2(5) ISSN (Online): 2455-7196, http://dx.doi.org/10.19101/TIS.2017.25001

[20] Arshad, Shaukat, S, Ali, A, Eleyan, A, Shah, S & Jawad, A 2020, 'Chaos Theory and its Application: An Essential Framework for Image Encryption', Chaos Theory and its Applications, vol. 2, pp. 17-22.

[21] Fadia Ali Khan et al., “A Secure and Lightweight Chaos Based Image Encryption Scheme” Computers, Materials & Continua, 2022, vol.73, no.1. http://dx.doi.org/10.32604/cmc.2022.028789

[22] Ismehene Chaouch, Anis Naanaa, Sadok ElAsmi et al. A New Chaos-based Text Encryption/Decryption to Secure Cloud Computing, 26 September 2022, PREPRINT (Version 2) available at Research Square. DOI: https://doi.org/10.21203/rs.3.rs-1999341/v2

[23] Wencheng Yang et al., “Multimedia security and privacy protection in the internet of things: research developments and challenges,” Int. J. Multimedia Intelligence and Security, Vol. 4, No. 1, 2022. DOI:10.1504/IJMIS.2022.10044461