Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105
Volume **9**, Number **2**, May **2024**

New Media Short Video File Encryption Algorithm Based on Improved Chaotic Sequence

Yang Liu

College of Humanities,
Hubei University, Zhixing College, Wuhan 430011, P. R. China
zxedu_cl@yeah.net

Lv Chen*

College of Computer and Information Engineering,
Hubei University, Zhixing College, Wuhan 430011, P. R. China
hanneiyang@126.com

Viktor Gruev

School of Education,
Grenfell Campus, Memorial University of Newfoundland, Corner Brook A2H 5G4, Canada
fz9082@163.com

*Corresponding author: Lv Chen
Received July 26, 2023, revised September 20, 2023, accepted November 18, 2023.

Abstract. *With the popularity of new media short videos and the acceleration of information dissemination on the Internet, the security problem of short video files has become increasingly prominent. The study of new media short video encryption technology can explore safer and more reliable data protection methods and improve the overall security of short video platform. Chaotic sequence cipher has the characteristics of complex structure and large key space, which can effectively meet the characteristics of multimedia encryption, so the application of chaotic sequence in multimedia encryption has a better application prospect. Aiming at the above problems, this work designs an improved chaotic sequence generator using a two-dimensional generalised Logistic equation and spatio-temporal two-dimensional discrete mapping. Various pseudo-random properties of the generated chaotic sequences are detected using the single-bit frequency detection method and the correlation detection method, and the simulation experiments illustrate that the pseudo-random properties are excellent and have the advantage of better pseudo-randomness compared with the existing common chaotic sequence generation methods. In addition, the proposed new chaotic sequence generator is used to encrypt AVI video files, which are commonly used in multimedia, using direct encryption. Matlab simulation experiments demonstrate the excellent encryption effect of the proposed method. Compared with the traditional direct encryption algorithm, the proposed method has the advantage of better encryption speed.*
Keywords: Chaotic sequences; Video encryption; Discrete-time systems; Logistic equations; Pseudo-randomness

1. **Introduction.** With the popularity of new media short videos and the acceleration of information dissemination on the Internet, the security problem of short video files has become increasingly prominent. The study of new media short video encryption technology can explore safer and more reliable data protection methods and improve the overall security of short video platforms [1,2].

With the continuous development of society and the continuous progress of information technology, people's spiritual and cultural life is also more and more rich, a variety of new media, new entertainment endless. The development of these emerging media industries are inseparable from the application of multimedia information technology, such as youtube, volcano video, etc. [3,4]. In multimedia information technology, image data files are mostly in the format of BMP, TIFF, etc., and video data files are in the format of WAV, AVI, JPRG, etc., and the multimedia files in the above formats have been deeply penetrated into all aspects of people's daily life. However, video data files are likely to be invaded or even interfered by illegal hackers during network transmission, such as stealing video surveillance information [5,6], or maliciously tampering with the data, and so on. These illegal behaviours can cause great harm to people's privacy and security, and require particularly high communication security due to the security, commercial and military domains. In these fields, especially in the military field [7,8], once the data invasion, theft or tampering in the process of communication transmission, it will cause unanticipated impact on our country, and the importance of the security of multimedia information becomes very important. Therefore, multimedia video file encryption algorithm has been a hot research direction in the field of information security.

A large amount of high-quality original content and unique creativity emerge from short video platforms, and the protection of intellectual property rights of these contents is an important part to protect the rights and interests of creators. The research of encryption technology can prevent infringement behaviours such as theft, tampering and copying, and promote the development of creative industries [9,10]. New media short video platforms store a large amount of user data and video content, which become the target of hacker attacks and data leakage. Research on encryption technology can increase the protection of data against unauthorised access and misuse and improve user data security [11,12]. Short videos may contain sensitive details such as users' personal information and location information. Research on encryption technology can protect user privacy and prevent unauthorised access and exploitation. The research and application of encryption technology can improve the credibility and security of short video platforms, increase users' trust in the platform, and facilitate the development and growth of the short video industry.

In summary, the study of new media short video file encryption technology has important practical significance and application value, and plays a positive role in promoting the sustainable development of short video industry by safeguarding intellectual property rights, data security and user privacy.

In order to solve the problem of information security and protection of such body multimedia, researchers and scholars at home and abroad have proposed many kinds of solutions [13]. Among them, the most mainstream method is cryptography. The origin of cryptography is relatively early, through the long-term evolution and development, up to now, there have been a number of mature and secure encryption algorithms, such as DES, RC2, RSA and other encryption algorithms. Although the above algorithms have high security, they can only handle the encryption and decryption of simple data streams, such as text data. When encrypting large amounts of data, such as multimedia video files, they cannot effectively solve the problem of large correlation between data. In addition, the efficiency of encryption must be taken into account during network transmission [14,15]. In other words, traditional encryption algorithms cannot solve the real-time and correlation requirements of multimedia video file encryption.

As an important branch of cryptography, chaotic sequence cipher shows the advantages of strong initial value sensitivity, unusually complex structure and good pseudo-randomness, which is more in line with the needs of multimedia encryption. Therefore,

in this paper, an improved chaotic cryptography algorithm is proposed, which can generate a new pseudo-random key stream sequence according to the initial secret key. each frame extracted from AVI video file is heterodyne operated with the new pseudo-random sequence, and the encrypted file is obtained. Network transmission encryption experiments of video files are carried out through Matlab simulation to verify the reliability and advancement of the proposed encryption algorithm.

1.1. **Related Work.** Currently, research on multimedia video encryption algorithms focuses on the following directions:

(1) Encryption algorithm based on watermarking technique. Watermarking technology plays an important role in video encryption. By embedding the watermark information into the video, functions such as authentication, copyright protection and tracking of the video can be achieved. Currently, some researches focus on how to design more covert and robust video watermarking algorithms to resist various attack methods.

(2) Encryption Algorithm based on Chaos Theory: Chaos encryption algorithm uses the chaotic properties to generate the key to encrypt the video data. This algorithm has better randomness and unpredictability and can provide high security. Currently, some researches focus on methods to improve the chaotic mapping algorithm, chaotic disruption and chaotic diffusion to enhance the encryption strength and processing speed.

In the past five years, multimedia video encryption algorithm based on chaos theory is an important research direction in the field of video encryption. Wang et al. [16] proposed an image encryption method based on composite chaotic sequence and quantum chaotic encryption. By introducing two chaotic mappings and combining the traditional quantum chaotic encryption technique, the secure encryption of image data is achieved. Experimental results show that the method has high security and encryption effect. Gayathri and Subashini [17] proposed a video encryption algorithm based on spatio-temporal chaos and block disambiguation. By introducing spatio-temporal chaotic mapping and block disambiguation techniques, the spatial and temporal information of the video is obfuscated and rearranged to achieve the protection of video data. Experimental results show that the algorithm can effectively prevent unauthorised access and analysis of the video. Li et al. [18] proposed a video encryption algorithm based on three-dimensional discrete chaotic system and DNA coding. By considering the video data as three-dimensional data and using the chaotic sequences generated by the discrete chaotic system for disruption and encryption, DNA coding is also used for key management and protection. Experimental results show that the algorithm has high security and encryption effect. Elkamchouchi et al. [19] proposed a fast video encryption scheme based on chaotic compression. The method achieves fast encryption of video data by converting the video data into chaotic sequences using chaotic compression and adopting an encryption model based on the disruption-diffusion structure. Experimental results show that the scheme has high encryption speed and confidentiality.

In general, multimedia video encryption algorithms based on chaos theory in recent years are mainly devoted to improve the encryption effect, encryption speed and security. These methods achieve the security protection of video data through technical means such as chaotic mapping, disorder operation and quantum encryption. However, more in-depth research is still needed to address the security (pseudo-randomness) and practicality of the algorithms.

Multimedia video encryption based on direct encryption algorithms is a research direction in the field of multimedia security. Direct encryption algorithms achieve fast and effective encryption of video by performing operations such as replacement, substitution

and mapping of video frames, combined with random, chaotic or block disruption techniques. Hosny et al. [20] proposed a fast video encryption method based on pixel chaotic mapping and block disruption. The encryption protection of video data is achieved by mapping video pixels to chaotic sequences and rearranging video frames using block disarrangement technique. The experimental results show that the method has high encryption effect and encryption speed.

1.2. **Motivation and contribution.** Through the above analyses, it can be seen that the direct encryption algorithm provides a certain degree of security and practicality while maintaining the video quality. However, for the direct encryption algorithm, the real-time nature of the encryption and decryption process and the ability to resist attacks still need to be improved.

Therefore, in order to improve the security and encryption speed of encryption and decryption of networked multimedia video files, this work designs an improved chaotic sequence generator using two-dimensional generalised Logistic equations and spatio-temporal two-dimensional discrete mappings.

The main innovations and contributions of this work include:

(1) Based on the one-dimensional Logistic chaotic equation [21], we propose a model of generalised Logistic equation, and design a two-dimensional generalised Logistic equation with a primary coupling term. Compared with the classical Logistic equation, the chaotic sequence generated by the two-dimensional generalised Logistic equation has better pseudo-randomness, which is more conducive to video encryption.

(2) The way of generating chaotic sequences from two-dimensional generalised Logistic equations is improved by using spatio-temporal two-dimensional discrete mapping, so that a new sequence of pseudo-random keystreams is generated based on the initial secret key, which improves the encryption speed of the encryption algorithm.

(3) Direct encryption is used to encrypt the commonly used multimedia AVI video files, and the frames extracted from the AVI video files are heteroscedastic using a new pseudo-random sequence to obtain the encrypted files. Matlab simulation is used to conduct network transmission encryption experiments to verify the feasibility of the proposed encryption algorithm. Compared with the traditional chaotic encryption algorithm, the proposed encryption algorithm has high speed and good diffusion performance.

2. Foundations of chaos theory.

2.1. **Chaos theory and cryptography.** The characteristics of chaotic system make it not conform to the principle of probability statistics in terms of numerical distribution and do not get a stable probability distribution characteristic.

Traditional cryptosystems are not suitable for video encryption due to the large computational overhead. Currently, many researchers have carried out research on multimedia message encryption based on chaotic system. Compared with the DCT coefficient permutation, the chaotic-based multimedia message encryption scheme overcomes the limitation of the encrypted data size and reduces the probability of being attacked by the outside world. The chaotic pseudo-random number generator can be used to encrypt the key stream of H.264/AVC video files.

The principle of chaotic encryption and decryption [22] is represented in Figure 1, where P denotes the message to be encrypted, C denotes the encrypted message, and F denotes a suitable operation process which serves to generate the encrypted message by performing a suitable processing on the message to be encrypted, P, and the key, K'. This process can be understood as an encryption algorithm, such as DES algorithm, RSA algorithm, etc. In chaotic encryption, the process is also capable of choosing simple

functions, such as mod operations. The most critical part in chaotic encryption is $\Sigma(K')$, the keystream generator. It can be considered as a chaotic system model [23], which generates unpredictable sequences. Since chaotic systems are very sensitive to their initial values, their initial values are usually chosen as the key, i.e., the key for the chaotic system $\Sigma(K')$ is $\Sigma(0)$.

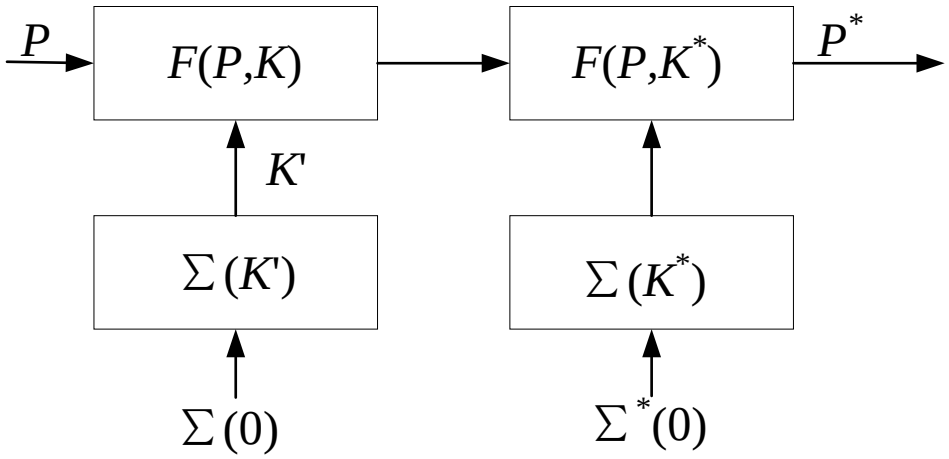


Figure 1. Chaotic encryption/decryption schematic

The encryption method and decryption method based on the principle of chaos are shown in Figure 2.

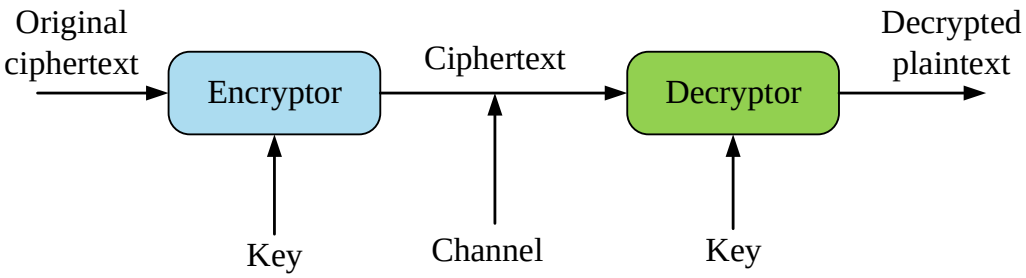


Figure 2. Encryption and decryption based on the chaos principle

The encryption process based on chaotic sequence cipher is as follows [24]: Initialisation: the appropriate initial state (seed) and chaotic system parameters are selected and set.

Generating chaotic sequences: a series of chaotic sequences are generated by iterative operations on chaotic systems. The chaotic system can be a one-dimensional, two-dimensional or higher dimensional mapping or flow, etc.

Key Generator: selects a specific number of bits from the generated chaotic sequence as a key. These key bits can be selected according to certain rules, such as skip picking, cross picking, extended picking, etc.

Plaintext Transformation: Converting the original data to be encrypted (plaintext) into a form that can be processed by a computer, e.g. converting text into binary code or vectorising video data.

Data encryption: The use of generated keys to perform anomalous operations or other obfuscation on plaintext data. The encryption process can be performed for each data bit or block.

The decryption process based on chaotic sequence cipher is opposite, so the principle of video encryption and decryption based on chaotic sequence cipher is shown in Figure 3.

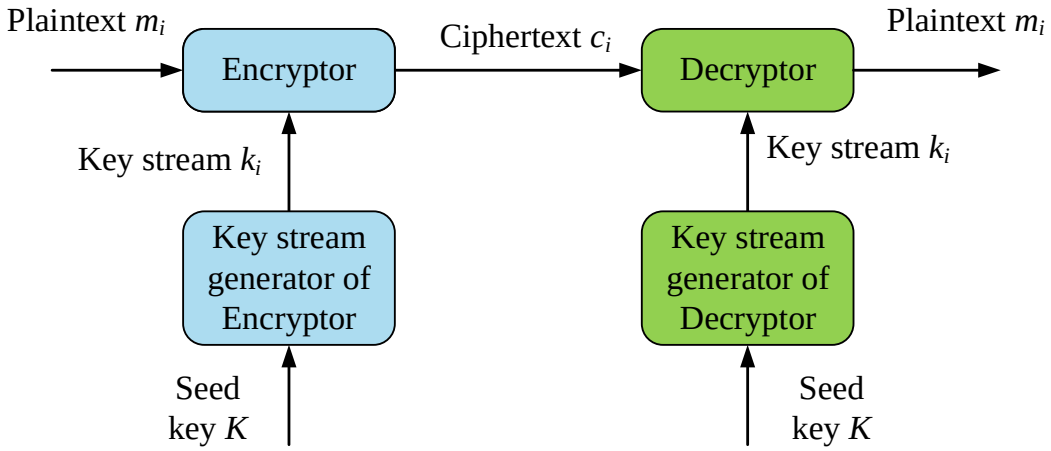


Figure 3. Principles of video encryption and decryption based on chaotic sequence codes

Logistic chaotic equations have a wide range of applications in the fields of chaotic cryptography and pseudo-random number generation. By adjusting the values of parameters and initial states, different chaotic sequences can be generated for encryption, obfuscation and other purposes. The one-dimensional Logistic chaotic equation is a common nonlinear discrete mapping, which is mathematically represented as:

$$X_n + 1 \ = \ \delta \cdot X_n \cdot (1 \ - \ X_n) \tag{1}$$

where X_n is the chaotic value at the current moment, X_{n+1} is the chaotic value at the next moment, and δ is a control parameter that specifies the behaviour of the chaotic system.

In a one-dimensional Logistic Chaos Equation, X_n usually takes values in the interval $[0, 1]$. When the parameter δ takes different values, the logistic chaos equation exhibits different dynamic behaviours, including stable periodic orbits, complex periodic orbits, and chaotic behaviours.

2.2. **Discrete space-time systems.** Discrete spacetime systems are the hotspot of chaos research in the last decade [25], and have very important application prospects in theories such as confidential communication and stochastic simulation. The spatio-temporal two-dimensional discrete mapping in discrete-space-time system can contain more initial parameters, compared with the low-dimensional chaotic system, the key space of the spatio-temporal two-dimensional discrete mapping is much larger, so the application of the spatio-temporal discrete mapping in multimedia encryption has an important research value and significance.

There are two common types of discrete space-time systems: one-dimensional discrete space-time mappings and two-dimensional discrete space-time mappings.

The mathematical expression for a one-dimensional time-varying discrete spacetime system that strictly satisfies the conditions of the Devaney chaos definition [26] can be expressed as:

$$x_{m+1,n} = f(m, x_{m,n}, x_{m,n+1}, \ldots, x_{m,n+k}) \tag{2}$$

where m denotes the time variable and n denotes the spatial location variable. The mathematical expression for spatio-temporal two-dimensional discrete mapping is shown as follow:

$$\begin{cases} x_{m+1,n} = f(m, y_{m,n}, x_{m,n}, x_{m,n+1}) \\ y_{m+1,n} = g(m, x_{m,n}, y_{m,n}, y_{m,n+1}) \end{cases} \tag{3}$$

The comparison reveals that two-dimensional time-varying discrete spacetime systems have a more complex structure and a larger key space.

3. **Improved chaotic sequence generator.**

3.1. **2D Generalised Logistic Equation.**

Logistic equation is a simple nonlinear equation [27]. With different control parameters for iterative calculation, the whole system will show different characteristics. After many iterations of computation, a completely different sequence of real numbers will be obtained [28]. Logistic equation can generate a sequence of random numbers through iterative computation, and these random numbers can be used in various encryption algorithms. Encryption is a means of security, although the Logistic equation has certain advantages, but there are some security risks, such as the existence of some blank windows in the chaotic region, and these blank windows are not related to the initial value.

In order to design a more superior chaotic equation, researchers study the generalised logistic equation based on the classical logistic equation.

$$x_{i+1} = f(x_i) = kx_i^m(1 - x_i)^n \tag{4}$$

The range of variation of k is:

$$\begin{cases} 1 \le k \le \frac{(1+n)^{n+1}}{n^n}, m = 1 \\ \frac{(m+n-1)}{(m-1)^{m-1}n^n} \le k \le \frac{(m+n)^{m+n}}{m^m n^n}, m > 1 \end{cases} \tag{5}$$

Based on the generalised logistic equation, a two-dimensional generalised logistic chaos equation with a primary coupling term is proposed in this work.

$$\begin{cases} x_{n+1} = u_1 x_n (1 - x_n) + r_1 y_n \\ y_{n+1} = u_2 {y^2}_n (1 - y_n)^2 + r_2 x_n \end{cases} \tag{6}$$

where u_1, u_2, r_1, and r_2 denote the coupled dynamics parameters. By selecting different combinations of control parameters, the dynamical behaviour of the system is comprehensively investigated.

The iterative plot of the two-dimensional generalised Logistic equation is shown in Figure 4. Where the vertical coordinates indicate the range of the output sequence distribution, and the horizontal coordinates indicate the range of values of the control parameters. From the overall point of the iterative diagram obtained for the two-dimensional generalised Logistic equation is very similar to the structure of the Logistic equation, and has the properties that the classical Logistic equation should have. From a local point of view, the chaotic interval of the 2D generalised Logistic equation has changed greatly, such as the range of values of the control parameters has changed greatly, and the 2D generalised Logistic equation is more superior than the classical Logistic equation. What's more, the chaotic density of the chaotic zone of the 2D generalised Logistic equation is higher and the gap distance is reduced.

Segmented linear mapping is a kind of one-dimensional mapping, in this work, by improving the general segmented linear mapping effectively, the segmented cosine function

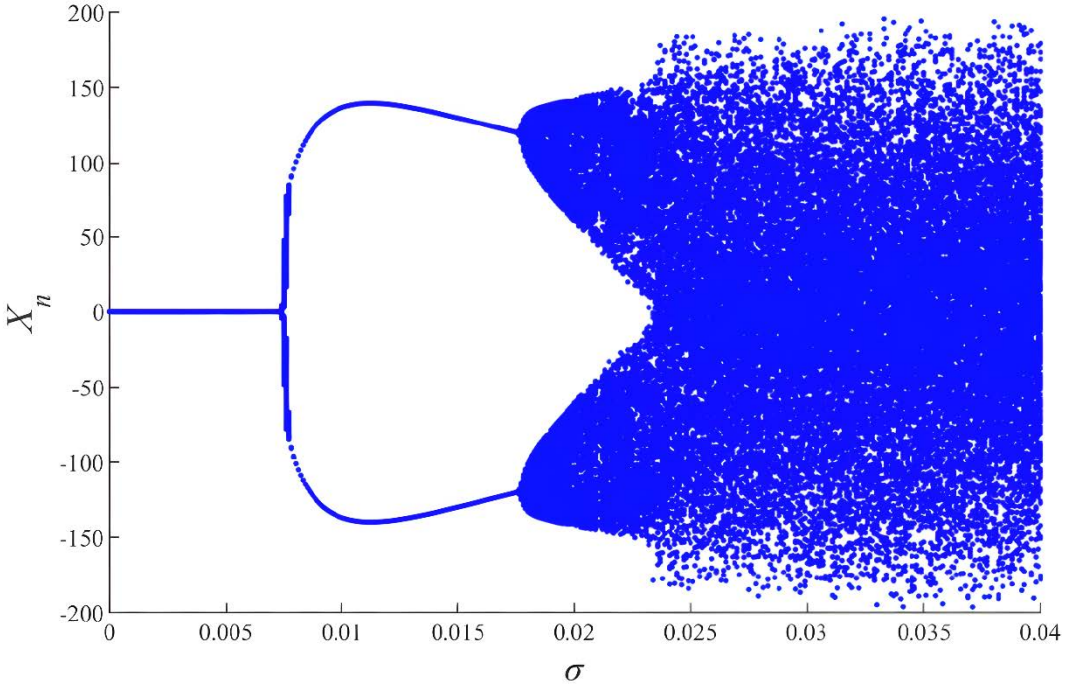


Figure 4. Iteration diagrams for two-dimensional generalised logistic equations

is obtained as follow:

$$y_{n+1} = \begin{cases} \cos[y_n/t], y_n \in (0,t) \\ \cos[(y_n - t)/(0.5 - t)], y_n \in [t, 0.5) \\ \cos[(1 - y_n - p)/(0.5 - t)], y_n \in [0.5, 1 - t) \\ \cos[(1 - y_n)/t], y_n \in [1 - t, 1) \end{cases} \tag{7}$$

where J_n is the sequence value of the initial chaos, t is the control parameter of the system, and $t \in (0, 0.5)$. The improved segmented cosine mapping has good chaotic properties and complex dynamical behaviour.

3.2. **Logistic mapping chaotic sequences based on Spatio-temporal two-dimensional discrete mapping.** In this paper, spatio-temporal two-dimensional discrete mapping is used to improve the way the two-dimensional generalised Logistic equation generates chaotic sequences, so that a new sequence of pseudo-random keystreams is generated based on the initial secret key. Therefore, a specific 2D time-varying discrete spacetime system is used in this work with the following expression:

$$\begin{cases} x_{m+1,n} = a_m y_{m,n} + b_m x_{m,n} + c_m x_{m,n+1} \mod (N) \\ y_{m+1,n} = r_m x_{m,n} + s_m y_{m,n} + t_m y_{m,n+1} \mod (N) \end{cases} \tag{8}$$

$$a_m = b_m = (1 + (-1)^m)/2 \tag{9}$$

$$a_m = b_m = (1 + (-1)^m)/2, c_m = t_m = 1 \tag{10}$$

$$\begin{cases} r_m = s_m = 0, m = 3i \\ r_m = s_m = 1, \text{others} \end{cases} \tag{11}$$

where N is a positive integer, the value of N selected in this paper is taken as 256.

The Devaney chaos maps of the two-dimensional time-varying discrete spacetime system are shown in Figure 5 and Figure 6. It can be seen that this system strictly satisfies the Devaney chaos definition conditions.

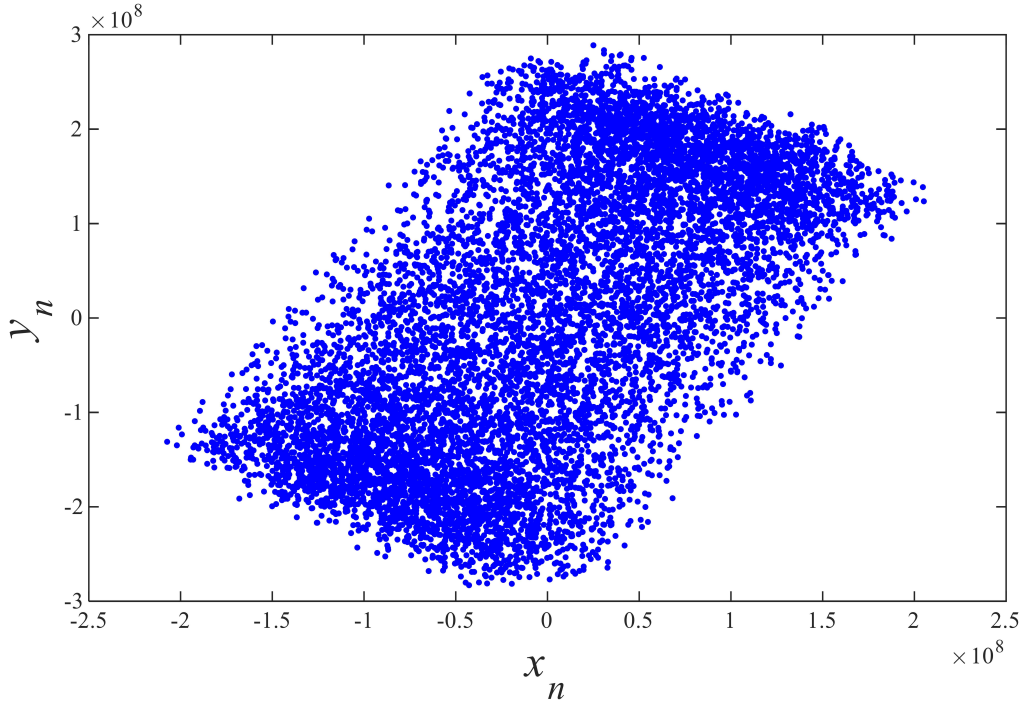


Figure 5. Devaney Chaotic Diagram (X-Y)

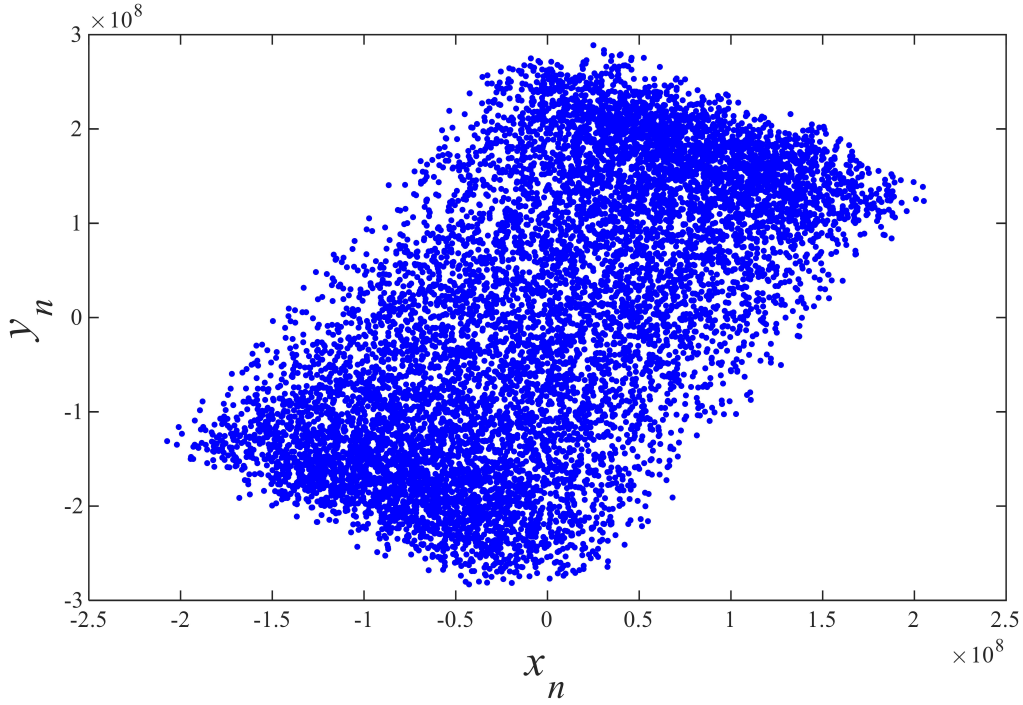


Figure 6. Devaney Chaotic Diagram (X-Z)

At this point,x_k and y_k are taken as the initial values of the two-dimensional time-varying discrete spatio-temporal system and substituted into Equation (8), and the resulting pseudo-random sequence is taken as the initial sequence.

4. **Multimedia video encryption based on improved chaotic sequences.** In this work, the commonly used multimedia AVI video files are encrypted using direct encryption

[29].The individual frames extracted from the AVI video files are subjected to a heterodyne operation using a new pseudo-random sequence to obtain the encrypted file.

Firstly, the key data and the encrypted video data are read, such as the number of frames of the encrypted video, the length and width of the frames. A new pseudo-random keystream sequence is obtained after the initial sequence is de-duplicated by 256 pairs. Read the video data, present each frame of the video and save it. Perform a different-or operation on each pixel in the frame one by one to encrypt the entire video frame.

Extract the (R, G, B) components of each image frame, take the odd part of each row of its component matrix (R_1, G_1, B_1) and encrypt each pixel in the frame one by one, thus encrypting the entire video frame.

$$\begin{cases} R_{1'} = R_1 \oplus x1(i) \oplus x2(i) \\ G_{1'} = G_1 \oplus x1(i) \oplus x2(i) \\ B_{1'} = B_1 \oplus x1(i) \oplus x2(i) \end{cases} \tag{12}$$

where i denotes the i-th set of matrices, and when i is greater than 5, recalculate from 1 again. Similarly, we also encrypt the even parts (R_2, G_2, B_2) of the (R, G, B) components of each original image frame. The even part of each component matrix of the encrypted image is obtained using dissimilarity.

$$\begin{cases} R_{2'} = R_2 \oplus R_{1'} \\ G_{2'} = G_2 \oplus G_{1'} \\ B_{2'} = B_2 \oplus B_{1'} \end{cases} \tag{13}$$

Finally, the above steps are repeated for each frame in the video, thus completing the encryption of the entire video.

The decryption process is similar to the encryption process and is the inverse of the encryption process.

5. **Experimental results and analyses.**

5.1. **Pseudo-randomness of chaotic sequences.**

Firstly, the performance of the chaotic sequence is analysed quantitatively using the mutual correlation function of the sequence. The smaller the value of the cross-correlation function, the better the pseudo-randomness of the sequence under test. The mutual correlation function is defined as:

$$R_{XY}(j) = (\sum_{i=1}^{p} x_i y_{i+j})/p \tag{14}$$

where x_k and y_k are 2 chaotic sequences of length p.

Using the Logistic equation for iterative computation, two chaotic sequences with 1,000 iteration values are generated, and the two sequences are tested for mutual correlation, and the test results are visually represented in the form of an image, and the results are shown in Figure 7. The chaos generated by the classical Logistic chaos equation has a small mutual correlation, and its correlation coefficient is around 0.35, so the chaos generated by classical Logistic chaos equation has good pseudo-randomness. Therefore, the chaotic sequence generated by the classical logistic equation has good pseudo-randomness.

Then, two chaotic sequences with 1000 iteration values are generated by iterative computation using the 2D generalised Logistic equation, and the inter-correlation of these two sequences is tested experimentally, which is used to quantitatively analyse the nature of the 2D generalised Logistic equation, and the results of the experimental simulation are shown in Figure 8. The correlation coefficients of the two sequences generated by the 2D generalised Logistic chaos equation are around 0.22, so the chaotic sequences generated

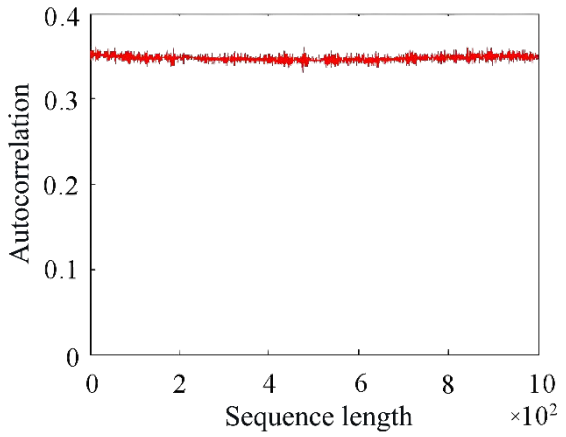


Figure 7. Reciprocal correlation of Logistic equations

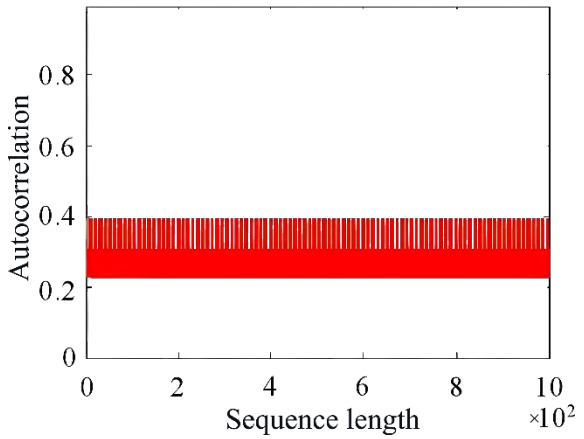


Figure 8. Reciprocal correlation of two-dimensional generalised Logistic equations

by the 2D generalised Logistic equation have higher pseudo-randomness than that of the classical Logistic equation.

Secondly, the performance of chaotic sequences was tested using frequency counting detection. Frequency count detection mainly detects whether the numbers of 0 and 1 in a binary sequence are close to each other, and in this way, it can judge whether the sequence has a good balance of 0 and 1. The 0's and 1's in the sequence to be tested are converted to -1 and 1 respectively to obtain the sequence to be tested X_i .

$$V = \frac{|S_n|}{\sqrt{n}}, S_n = \sum_{i=1}^{n} X_i \tag{15}$$

After calculating the *p_value*, if the resulting *p_value* is greater than 0.01, it means that the pseudo-random sequence to be detected can pass the frequency detection.

$$p\_value = erfc(\frac{V}{\sqrt{2}}) \tag{16}$$

where *erfc* is the residual error function.

The detection results are shown in Table 1. It can be seen that in the case of sequence lengths of 1024,4096 and 16384, although the chaotic sequences generated by the classical Logistic equation and the chaotic sequences generated by the two-dimensional generalised

Logistic equation both pass the frequency detection, i.e., the p_value is greater than 0.01, the p_value of the classical Logistic equation has a lower value, which indicates that the two-dimensional generalised Logistic equation generates chaotic sequences with better pseudo-randomness.

Table 1. Comparison of Frequency Detection Results

Sequence length	**Classical logistic equation**	**Two-dimensional generalised logistic equation**
16384	0.4627	0.6171
4096	0.4918	0.8513
1024	0.0801	0.4918

5.2. **Video encryption results analysis.** In order to analyse and verify the encryption method proposed in this paper, a multimedia video file is selected for specific experiments. The experimental hardware environment is: Intel Core i5 2.2GHz processor, 6GB memory, 400GB hard drive, GTX1060 independent graphics card. The experimental software environment is: Windows 7 operating system, Matlab 2012 (R2012a) simulation software. Logistic chaotic mapping of the initial parameters $x_0 = 0.1$, $\delta = 0.4$.

The 25-th frame of the original AVI video to be encrypted is shown in Figure 9(a), and the corresponding encrypted image frame after encryption is shown in Figure 9(b).

(a) Original frame (b) Encrypted frame

Figure 9. Video encryption simulation results

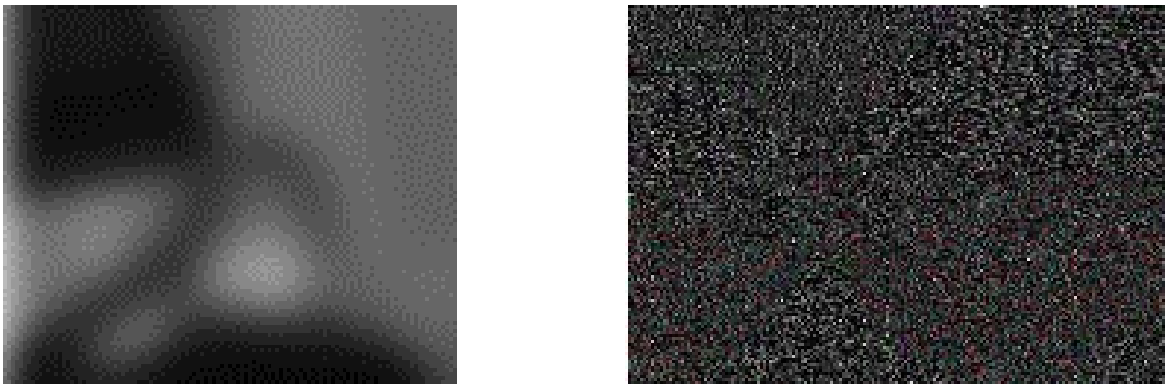
In order to validate the security of the proposed algorithm, the correlation between neighbouring frames in the video is examined and is calculated as follows:

$$p = A(i, j) - B(x, j) \tag{17}$$

Where A and B are the grey value matrices of two adjacent frames respectively, and p denotes the correlation coefficient.

The correlation results of two adjacent frames before encryption are shown in Figure 10(a), and the correlation results of two adjacent frames after encryption are shown in Figure 10(b).

As can be seen from Figure 9 and Figure 10, the encryption method based on the improved chaotic sequence generator can effectively complete the video file encryption. In



(a) Before encryption (b) After encryption

Figure 10. Correlation analysis simulation results

addition, the better encryption security is reflected in the lower correlation of neighbouring frames after encryption, that is to say, the better diffusion performance is maintained. Under the same experimental conditions, the time performance comparison of video encryption/decryption with chaotic pseudo-random number generator is shown in Table 2, which shows that the method in this paper has better encryption speed.

Table 2. Acceleration / decryption time comparison.

	Total encryption time/min	**Total decryption time/min**
Chaotic pseudo-random number generator	28.2	28.3
Improved chaotic sequence generator	23.5	23.6

5.3. **Pixel variation and diffusivity analysis.** In video encryption attack resistance analysis, information entropy (entropy) is often used to measure the security and attack resistance of encryption algorithms [32]. Information entropy is a measure of the randomness or uncertainty of data and is often used to assess the level of randomness of the ciphertext generated by an encryption algorithm. In this work, the information entropy of two multimedia videos before and after encryption is calculated, as shown in Table 3. The results show that the information entropy of the improved chaotic sequence generator both reaches 6.8747, and the encryption effect is better.

NPCR (Normalised Pixel Change Rate) [33] and UACI (Unified Average Changing Intensity) [34] are two metrics commonly used to evaluate the performance of image encryption algorithms. In this work, the computation of these two metrics, NPCR and UACI, can evaluate the performance of image encryption algorithms in terms of pixel change and diffusivity, providing a quantitative basis for performance evaluation.

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\%, D(i,j) = \begin{cases} 1, C_1(i,j) = C_2(i,j) \\ 0, C_1(i,j) \neq C_2(i,j) \end{cases} \tag{18}$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |C1(i,j) - C2(i,j)|}{255 \times M \times N} \times 100\% \tag{19}$$

Table 3. Entropy before and after encryption.

Frame rate	Video A		Video B	
	Original	Encrypted	Original	Encrypted
1	2.7505	6.8747	2.443	6.8744
2	2.8572	6.8747	2.453	6.8744
3	2.8483	6.8745	2.4499	6.8751
4	2.9364	6.8749	2.4542	6.8749
5	2.939	6.8745	2.4662	6.8748
6	2.9078	6.8746	2.4771	6.8743
7	2.9038	6.8747	2.5053	6.8744
8	2.897	6.8745	2.5421	6.8742
9	2.8555	6.8749	2.5819	6.8745
10	2.8507	6.8745	2.608	6.8741
11	2.8292	6.8744	2.6225	6.8746
12	2.8327	6.8749	2.6711	6.8745

where $C_1(i,j)$ and $C_2(i,j)$ are the pixel values in row i and column j of different encrypted video frames, respectively.

Taking video B as an example, the average NPCR (Number of Pixels Change Rate) and average UACI (Unified Average Changing Intensity) after multimedia video encryption are shown in Table 4. It can be seen that compared to other video encryption algorithms, the multimedia video encryption method based on improved chaotic sequences has a higher NPCR and UACI, which indicates that it is more capable in terms of pixel variation and diffusivity.

Table 4. NPCR & UACI of video frames.

Encryption algorithm	NPCR	UACI
Encryption based on improved chaotic sequences	99.5061	33.3601
[30]	99.5214	33.3512
[31]	99.0545	33.1071

6. **Conclusion.** In order to improve the security and encryption speed of encrypting and decrypting multimedia video files on the network, this work designs an improved chaotic sequence generator by using a two-dimensional generalised Logistic equation and spatio-temporal two-dimensional discrete mapping. Firstly, the model of the generalised Logistic equation is proposed on the basis of the one-dimensional Logistic chaos equation, and a two-dimensional generalised Logistic equation with a primary coupling term is designed. Then, a time-varying discrete space-time system is used to improve the way of generating chaotic sequences for the two-dimensional generalised Logistic equation, which improves the encryption speed of the encryption algorithm. Finally, a commonly used multimedia AVI video file is encrypted by direct encryption, and the Matlab simulation results show that the chaotic sequences generated by the 2D generalised logistic equation have better pseudo-randomness compared with the classical logistic equation, which is more conducive to the encryption of the video file. Compared with other chaotic encryption algorithms, the proposed encryption algorithm has higher encryption speed and good diffusion performance. Because the proposed encryption algorithm is the most secure full encryption

algorithm, the encryption of the sound in the video is not well handled. Further research will be carried out to address this issue.

REFERENCES

[1] D. T. S. Kumar, "A novel method for HDR video encoding, compression and quality evaluation," *Journal of Innovative Image Processing*, vol. 1, no. 2, pp. 71-80, 2019.

[2] C.-M. Chen, Y. Hao, and T.-Y. Wu, "Discussion of "Ultra Super Fast Authentication Protocol for Electric Vehicle Charging Using Extended Chaotic Maps,"" *IEEE Transactions on Industry Applications*, vol. 59, no. 2, pp. 2091-2092, Mar. 2023.

[3] C.-M. Chen, L. L. Xu, K.-H. Wang, S. Liu, and T.-Y. Wu, "Cryptanalysis and Improvements on Three-party-authenticated Key Agreement Protocols Based on Chaotic Maps," *Journal of Internet Technology*, vol. 19, no. 3, pp. 679-687, 2018.

[4] C.-M. Chen, W.-C. Fang, S. Liu, T.-Y. Wu, J.-S. Pan, and K.-H. Wang, "Improvement on a Chaotic Map-based Mutual Anonymous Authentication Protocol," *Journal of Information Science and Engineering*, vol. 34, no. 2, pp. 371-390, 2018.

[5] T.-Y. Wu, X.-N. F, K.-H. Wang, J.-S. Pan, and C.-M. Chen, "Security analysis and improvement on an image encryption algorithm using Chebyshev generator," *Journal of Internet Technology*, vol. 20, no. 1, pp. 13-23, 2019.

[6] T.-Y. Wu, X.-N. F, K.-H. Wang, J.-S. Pan, C.-M. Chen, and J. M.-T. Wu, "Security Analysis and Improvement of an Image Encryption Scheme Based on Chaotic Tent Map," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 9, no. 4, pp. 1050-1057, 2018.

[7] F. Zhang, T.-Y. Wu, and G. Zheng, "Video salient region detection model based on wavelet transform and feature comparison," *EURASIP Journal on Image and Video Processing*, vol. 2019, 58, 2019.

[8] M. Asgari-Chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," *Signal Processing*, vol. 157, pp. 1-13, 2019.

[9] Z. Tu, H. Li, D. Zhang, J. Dauwels, B. Li, and J. Yuan, "Action-stage emphasized spatiotemporal VLAD for video action recognition," *IEEE Transactions on Image Processing*, vol. 28, no. 6, pp. 2799-2812, 2019.

[10] J. S. Teh, M. Alawida, and Y. C. Sii, "Implementation and practical problems of chaos-based cryptography revisited," *Journal of Information Security and Applications*, vol. 50, 102421, 2020.

[11] A. Yaqoob, T. Bi, and G.-M. Muntean, "A survey on adaptive 360 video streaming: Solutions, challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2801-2838, 2020.

[12] D. Lee and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree," *Multimedia Tools and Applications*, vol. 80, pp. 34517-34534, 2021.

[13] Y. Zhou, L. Tian, C. Zhu, X. Jin, and Y. Sun, "Video coding optimization for virtual reality 360-degree source," *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 1, pp. 118-129, 2019.

[14] M. Orduna, C. Díaz, L. Muñoz, P. Pérez, I. Benito, and N. García, "Video multimethod assessment fusion (VMAF) on 360VR contents," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 1, pp. 22-31, 2019.

[15] Y. Yang, Z. Li, W. Xie, and Z. Zhang, "High capacity and multilevel information hiding algorithm based on pu partition modes for HEVC videos," *Multimedia Tools and Applications*, vol. 78, pp. 8423-8446, 2019.

[16] X. Y. Wang, J. J. Zhang, and G. H. Gao, "An image encryption algorithm based on ZigZag transform and LL compound chaotic system," *Optics & Laser Technology*, vol. 119, 105581, 2019.

[17] J. Gayathri and S. Subashini, "An efficient spatiotemporal chaotic image cipher with an improved scrambling algorithm driven by dynamic diffusion phase," *Information Sciences*, vol. 489, pp. 227-254, 2019.

[18] X. Li, H. Yu, H. Zhang, X. Jin, H. Sun, and J. Liu, "Video encryption based on hyperchaotic system," *Multimedia Tools and Applications*, vol. 79, pp. 23995-24011, 2020.

[19] H. Elkamchouchi, W. M. Salama, and Y. Abouelseoud, "New video encryption schemes based on chaotic maps," *IET Image Processing*, vol. 14, no. 2, pp. 397-406, 2020.

[20] K. M. Hosny, M. A. Zaki, H. M. Hamza, M. M. Fouda, and N. A. Lashin, "Privacy Protection in Surveillance Videos Using Block Scrambling-Based Encryption and DCNN-Based Face Detection," *IEEE Access*, vol. 10, pp. 106750-106769, 2022.

[21] R. Senkerik, I. Zelinka, D. Davendra, and Z. Oplatkova, "Utilization of SOMA and differential evolution for robust stabilization of chaotic Logistic equation," *Computers & Mathematics with Applications*, vol. 60, no. 4, pp. 1026-1037, 2010.

[22] Z. Zhang, Y. Luo, C. Zhang, X. Liang, M. Cui, and K. Qiu, "Constellation shaping chaotic encryption scheme with controllable statistical distribution for OFDM-PON," *Journal of Lightwave Technology*, vol. 40, no. 1, pp. 14-23, 2021.

[23] U. A. Bhatti, Z. Yu, J. Li, S. A. Nawaz, A. Mehmood, K. Zhang, and L. Yuan, "Hybrid watermarking algorithm using Clifford algebra with Arnold scrambling and chaotic encryption," *IEEE Access*, vol. 8, pp. 76386-76398, 2020.

[24] P. Rashmi, M. Supriya, and Q. Hua, "Enhanced lorenz-chaotic encryption method for partial medical image encryption and data hiding in big data healthcare," *Security and Communication Networks*, vol. 2022, pp. 1-9, 2022.

[25] S. Mortajez, M. Tahmasbi, J. Zarei, and A. Jamshidnezhad, "A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images," *Informatics in Medicine Unlocked*, vol. 20, pp. 100396, 2020.

[26] C. Liang, Q. Zhang, J. Ma, and K. Li, "Research on neural network chaotic encryption algorithm in wireless network security communication," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, pp. 1-10, 2019.

[27] B. Zhu, F. Wang, and J. Yu, "A chaotic encryption scheme in DMT for IM/DD intra-datacenter interconnects," *IEEE Photonics Technology Letters*, vol. 33, no. 8, pp. 383-386, 2021.

[28] A. Adeel, J. Ahmad, H. Larijani, and A. Hussain, "A novel real-time, lightweight chaotic-encryption scheme for next-generation audio-visual hearing aids," *Cognitive Computation*, vol. 12, pp. 589-601, 2020.

[29] S. Thakur, A. Singh, B. Kumar, and S. Ghrera, "Improved DWT-SVD-based medical image watermarking through hamming code and chaotic encryption," pp. 897-905.

[30] S. Fan, K. Li, Y. Zhang, H. Tan, Q. Fang, K. Han, and J. Wang, "A hybrid chaotic encryption scheme for wireless body area networks," *IEEE Access*, vol. 8, pp. 183411-183429, 2020.

[31] A. Alghafis, N. Munir, M. Khan, and I. Hussain, "An encryption scheme based on discrete quantum map and continuous chaotic system," *International Journal of Theoretical Physics*, vol. 59, pp. 1227-1240, 2020.

[32] H. Xiong, M. Yang, T. Yao, J. Chen, and S. Kumari, "Efficient Unbounded Fully Attribute Hiding Inner Product Encryption in Cloud-Aided WBANs," *IEEE Systems Journal*, vol. 16, no. 4, pp. 5424-5432, 2022.

[33] X. Huang, H. Xiong, J. Chen, and M. Yang, "Efficient Revocable Storage Attribute-based Encryption with Arithmetic Span Programs in Cloud-Assisted Internet of Things," *IEEE Transactions on Cloud Computing*, vol. 11, no. 2, pp. 1273-1285, 2023.

[34] H. Xiong, T. Yao, H. Wang, J. Feng, and S. Yu, "A Survey of Public-Key Encryption with Search Functionality for Cloud-Assisted IoT," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 401-418, 2022.