Journal of Network Intelligence
Taiwan Ubiquitous Information

Volume **8**, Number **3**, August **2023**

Chaotic Sequence-based Video Encryption Algorithm for Network Surveillance

Jie He*

Department of Electronic Information Engineering
ChongQing Technology and Business Institute
ChongQing, 401520, China
76231249@qq.com

*Corresponding author: Jie He
Received February 21, 2022, revised March 24, 2022, accepted May 20, 2022.

Abstract. *Network surveillance video information has the characteristics of large data volume and continuity, and requires a fixed playback format, so the network surveillance video encryption technology must have good real-time performance. Discrete-time chaotic systems are more suitable for the field of confidential video communication. Therefore, this work combines network video surveillance and chaotic cryptographic algorithms, and designs a chaotic sequence-based network surveillance video encryption algorithm. Firstly, the overall architecture of the video surveillance encryption system is given. Secondly, a three-dimensional discrete chaotic dynamical system is designed and based on it, the three-dimensional sine-modulated self-synchronous chaotic stream cipher (3-D SM-SCSC) algorithm is designed. Uses a low 8-bit XOR operation to mask plaintext information. In which, the sine function is used as a non-linear step of the cipher, which effectively improves the security of the cipher. Finally, the feasibility of the proposed video encryption algorithm is verified by simulation. The simulation results show that the proposed 3-D SM-SCSC algorithm has better encryption effect than the traditional 3-D SCSC algorithm and other video encryption algorithms. 3-D SM-SCSC algorithm is less time consuming for encrypting video images and is resistant to statistical and differential attacks with high security.*
Keywords: Network surveillance, Video encryption, Chaotic systems, Stream cipher, Sine function

1. **Introduction.** With the rapid development of communication technology, security issues are receiving more and more attention. As an important part of security issues, video surveillance is widely used in the military, intelligent transportation, home security and many other fields. Traditional video surveillance technology is developing in the direction of digitalisation and networking. Information security technology is an inevitable and important topic in the development of science and technology [1,2,3,4]. In some sensitive places such as banks, homes and the military, encryption of surveillance information is required as the surveillance information is only available to designated authorised users. It is quite possible for data leaks to occur during the transmission of network video surveillance information. Video information can also be tampered with to the extent that false information is generated. In the early days, we mainly authenticated the identity of the visitors. However, the authentication was only permission controlled and there was no encryption of the video information itself. Unencrypted video messages could easily be intercepted by others during transmission. Therefore, it is clear that the security of video data transmission cannot be truly ensured simply by permission control [5,6,7,8]. It is of

great importance to strengthen the research on video surveillance encryption systems.
Network surveillance video encryption is the original video in the image under the control of the key through the encryption algorithm into a haphazard screen, so as to achieve the purpose of protecting the video image information. Network surveillance video information has the characteristics of large data volume and continuity, and requires a fixed playback format, so network surveillance video encryption technology must have good real-time performance [9,10]. Traditional cryptography contains two main categories [11,12,13,14]: the first category is symmetric cryptosystems and the second category is asymmetric cryptosystems. Symmetric cryptographic algorithms can be subdivided into group ciphers and sequence ciphers. Grouped cryptographic algorithms are complex and time-consuming. Sequential cryptographic algorithms have the advantage of being fast. Sequential cipher algorithms can achieve higher real-time performance with guaranteed security. Sequential cryptographic algorithms are gradually replacing traditional cryptographic algorithms in video data encryption research. Chaotic cipher algorithm, as an emerging sequence cipher algorithm, is gradually attracting attention by virtue of its extreme parameter sensitivity and high real-time performance.
Chaos is a seemingly random dynamical behaviour generated by a deterministic system. Chaos has properties such as being very sensitive to initial conditions, non-periodic and non-linear [15]. These characteristics coincide with those of traditional cryptosystems. Unlike traditional cryptographic algorithms, chaotic cryptographic algorithms are able to generate pseudo-random sequences in real time and can meet the need for fast and secure encryption. Currently, research on chaotic secure communications has focused on discrete-time chaotic systems, mainly because they are easier to implement in microprocessors. In addition, the design of higher dimensional discrete-time chaotic systems will have the advantages of greater randomness and a larger key space, which will ensure the confidentiality and communication efficiency of the encryption system. Therefore, discrete-time chaotic systems are more suitable for the field of confidential video communication.
Therefore, in the context of the above application, this study combines network video surveillance and chaotic cryptographic algorithms to design a chaotic sequence-based video encryption algorithm for network surveillance. This study applies the chaotic cipher algorithm to video surveillance, which effectively improves the security of surveillance information.

1.1. **Related Work.** Video information is characterised by a large volume of data and high real-time requirements. The development process of video encryption technology can be divided into three stages
In the first stage, the structure of the video stream is scrambled to disrupt the statistical properties of the data and achieve the goal of information masking. However, the scrambling process destroys the inter-pixel correlation and causes difficulties in the later compression coding process. At the same time, the algorithm has low complexity and is not very secure. The scrambling algorithm is therefore only suitable for encrypting video images that do not require compression processing. With the development of multimedia compression technology in the second phase, many video coding and compression techniques have emerged, such as JPEG, MPEG, etc. The advent of video compression algorithms has made it possible for video information to no longer exist in the form of raw data. The compressed video has no significant loss in clarity but the amount of data is significantly reduced, improving the efficiency of information storage. Encryption algorithms for compressed video data have become the focus of research in this field. Many researchers have proposed to first compress and encode the video data, and then encrypt

it using cryptographic algorithms such as DES and RSA [16,17,18]. However, the complexity of the traditional cryptographic algorithms leads to a reduction in the real-time performance of the video. For example, the RSA algorithm performs encryption operations mainly through modulo-power and modulo-multiplication operations. Algorithms such as DES, IEDA and AES rely on multiple disruption and diffusion operations (high computational complexity) to achieve high security, which also suffers from computational inefficiency.

It has been discovered that critical information in video is only present in some of the frames, hence the rise in the use of partial encryption algorithms for video data encryption. By reducing the amount of data computed to ensure real-time video, the speed requirements of the hardware are reduced. However, due to the use of partial encryption, the information in the encrypted frames can be deduced from the unencrypted frames, making the security of the information a potential concern. Therefore, partial encryption algorithms cannot be used in scenarios with high security requirements.

With the rapid development of sequence cipher algorithms in the third phase, sequence ciphers have been widely used in the field of voice and video encryption for their advantages such as high security and high real-time performance. Chaotic phenomena are seemingly random movements arising in deterministic systems.

Chaotic systems have properties such as sensitivity to initial conditions and unpredictability. Chaotic cryptography is an emerging discipline that studies pseudo-random key flows [19,20]. Chaotic systems generate chaotic sequences that satisfy the characteristics of traditional ciphers, while generating secret keys faster. Therefore, it is advantageous to use chaotic cryptographic algorithms for encryption of video information with high real-time and large data volume. Al-Nuaimy et al. [21] used chaotic encryption algorithms in images and effectively dislocated image pixels. Zhao et al. [22] applied chaotic encryption algorithms to video information encryption, which improved both real-time and security of video information. Based on the chaotic inverse control principle, Lin et al. [23] designed two 8-dimensional discrete-time chaotic systems and used the chaotic random sequences generated by the systems to encrypt RGB video data. Wei et al. [24] used a multi-stage chaotic encryption scheme to perform multiple rounds of chaotic encryption operations on compressed digital audio signals. Asiain and Garrido [25] introduced the chaotic inverse control design process in the non-linear nominal matrix to enhance the security of chaotic stream ciphers and use an improved chaotic system to generate pseudo-random sequences, thus encrypting compressed video data. The practical application of chaotic cryptographic algorithms in the security field has proven the effectiveness and usefulness of chaotic ciphers. However, chaotic cipher algorithms still have security vulnerabilities. Bai et al. [26] effectively deciphered part of the key of a traditional chaotic system using statistical and differential attacks respectively.

1.2. **Motivation and contribution.** In response to the above problems, this paper conducts an in-depth study of network video surveillance encryption systems and designs a chaotic sequence-based video encryption algorithm for network surveillance on this basis. By applying the chaotic cryptographic algorithm to video information encryption, the security of video information is improved. Firstly, the overall architecture of the video surveillance encryption system is given. Secondly, the cryptographic fundamentals, chaos theory and chaotic sequence cipher are highlighted. Then, a three-dimensional discrete chaotic dynamical system is designed. Finally, the feasibility of the proposed video encryption algorithm is specifically verified.

The main contributions and novelties of this work can be summarized as follows:

(1) A three-dimensional discrete-time chaotic dynamical system is designed. The chaotic system is obtained from the inverse control of an asymptotically stable system. The dimension of the asymptotically stable linear system used in this work is 3, taking into account the limitations of the ARM processor.

(2) Based on the above three-dimensional discrete-time chaotic dynamical system, a three-dimensional sine modulated self-synchronous chaotic stream cipher (3-D SM-SCSC) algorithm is designed. After performing a series of sine, multiplication and rounding operations on a single state variable of a chaotic system, the plaintext information is masked using a low 8-bit heterodyne operation. In this case, the sine function is used as a non-linear step in the cipher, which effectively enhances the security of the cipher. The ciphertext needs to be fed back into the chaotic system after generation, both to form a closed-loop encryption and improve the relevance of the cipher, and as a driver to achieve self-synchronisation.

The rest of the paper is organized as follows: Section 2 introduces the overall architecture of network surveillance encryption system. Section 4 presents the desgin of three-dimensional sine modulation self-synchronizing chaotic stream cipher algorithm. Section 5 presents the experimental results and test analysis. Section 6 concludes the paper.

2. **The overall architecture of the network video surveillance encryption system.** The network video surveillance encryption system in this paper is based on the secondary development of a Hikvision network camera. Firstly, the network camera captures the picture and obtains the video stream. The stream is then encrypted by a network video encryption machine and forwarded to the network, and the stream is decrypted by the encryption machine before it can be previewed and played on the PC side. The topology of the network video surveillance encryption system is shown in Figure 1.

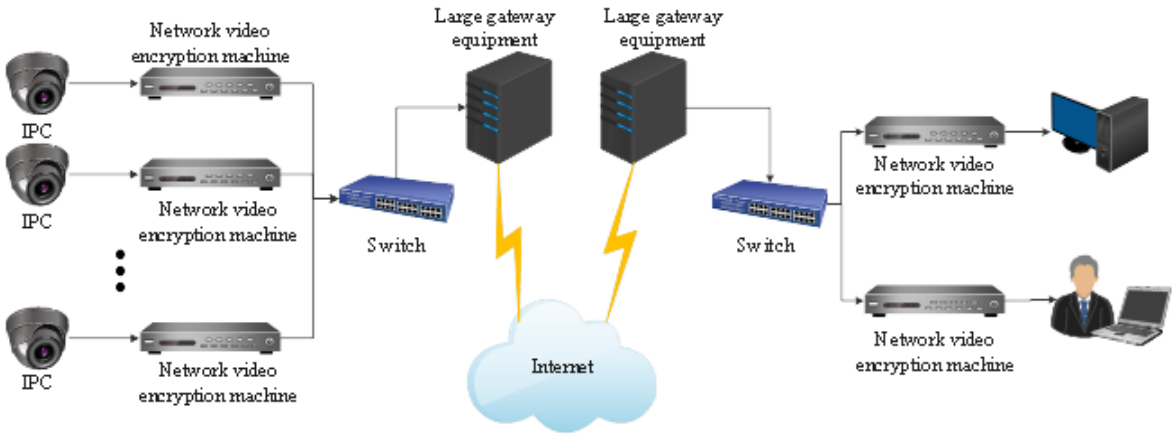


Figure 1. Topology of the network video surveillance encryption system.

The network video encryptors is implemented by a SoC processing unit, which mainly consists of an ARM processor. The network encryptor uses the design idea of a core board. The core board is an ARM embedded minimal system. According to the interfaces provided by ARM and the actual application requirements, the peripheral backplane circuit of the network video encryption machine is designed, including modules such as DM9000, dip switches and serial ports as well as JTAG debugging.

A network camera is a combination of a network coding module and an analogue camera, referred to as an IPC. In order to connect the IPC to switches and routers, the analogue video signal captured by the analogue camera needs to be converted into a digital signal. The IPC not only captures images, but also has a built-in digital compression controller

and an embedded operating system; the IPC not only compresses the video data, but also transmits it to the terminal via a wired or wireless network; the IPC can be directly connected to a digital network based on TCP/IP and its main function is to transmit video over a local area network.

3. **Fundamentals of cryptography and chaotic ciphers.**

3.1. **Basic concepts of cryptography.**

Cryptography is the study of the design and decipherment of cryptographic algorithms for securing information systems. The two main components are coding and analysis. Cryptography focuses on the process of encryption implementation and the design of suitable cryptographic algorithms for information masking. Cryptanalysis is the study of the objective laws of encrypted messages. The essence of cryptanalysis is to find ways to break a cipher without knowing the key.

The basic application of cryptography is to hide the meaning of a message. The classical model of cryptographic communication is shown in Figure 2.

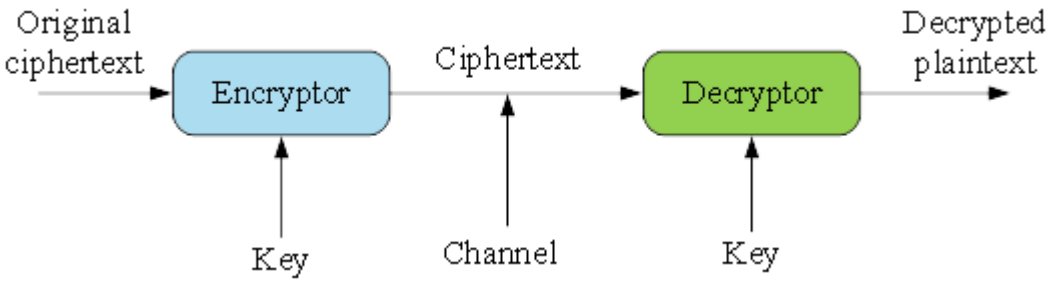


Figure 2. Encrypted communication model.

There are five basic elements in this cryptographic system:

(1) Plain text: Messages that are not encrypted are called plain text and are denoted by p. The plain text space is denoted by P. Plain text can be text, bitmaps, digitised voice or video streams, etc.

(2) Cipher text: The encrypted message is called cipher text and is denoted by c. The cipher text space is denoted by C.

3) Key: The key is a secret parameter used in the encryption and decryption algorithm, usually owned only by the communicator and denoted by k. The key space is denoted by K. Both encryption and decryption are carried out under the control of the key.

(4) Encryption Algorithm: The mechanism used to transform plaintext into ciphertext, also known as the encoding process. It is denoted by $E(c = Ek(p))$.

(5) Decryption Algorithm: The inverse of the encryption algorithm, the mechanism used to transform the cipher text into plain text. It is also called the decoding process and is denoted by $D(p = D_k(c))$.

In a secret communication, the selection of the key is the key to ensure the quality of confidentiality. After the source has selected the appropriate key k, the plaintext p is converted to ciphertext c by the encryption algorithm E with the participation of the key k. This process can be expressed as $E{:}P\times K\rightarrow C$. The decryption process is the inverse of the encryption process, where the ciphertext obtained with the encryption algorithm can always be recovered from the original plaintext by the corresponding decryption algorithm, a process that depends on the key.

3.2. **Foundations of Chaos Theory.** Before the 1960s, scientists generally believed that the behaviour of deterministic systems was perfectly certain and predictable. Subsequent research has shown that many deterministic systems are subject to unpredictable, random behaviour. The complex random behaviour in deterministic systems was referred to as chaos. Today chaos theory has developed into an important theory for the study of nonlinear systems in several fields.

Chaos is a complex nonlinear dynamical property that manifests itself in deterministic systems and is an important branch of nonlinear science. We give a definition of chaos in terms of interval mapping.

Definition 1 Suppose that $f{:}A \to A$ is a self-map. For $x \in A$, if there exists a positive integer n satisfying the following condition.

$$f^n(x) = f\left(f\left(\cdots f(x)\cdots\right)\right) = x \tag{1}$$

Also, there exists any positive integer $k < n$ that satisfies the following condition.

$$f^k(x) \neq x \tag{2}$$

Then x is said to be a periodic point of $f.n$ is called the period.

Definition 2A continuous self-map $f(x)$ on a closed interval I is said to be chaotic on the interval I if the following conditions are satisfied.

(1) There is no upper bound on the frequency of cycles of occurrence of f.

(2) There exists a subset S interval on I satisfying the following condition.

$$\lim_{x\to\infty} \sup \left|f^n(x) - f^n(y)\right| > 0 \tag{3}$$

Where $x, y \in S$. A continuous system is in a chaotic state if there is a periodic point on the closed interval I and the span of that periodic point is 3.

The simplest chaotic system is the Logistic function.

$$y = \lambda x\left(1 - x\right), x \in [0, 1], \lambda \in [0, 4] \tag{4}$$

Where λ is called the system parameter. When $\lambda \in [3.57, 4]$, the logistic mapping enters a chaotic state and exhibits many complex dynamical properties.

3.3. **Chaotic sequence ciphers.** In cryptography, Diffusion and Confusion are the basic principles to be observed in cryptographic design; Diffusion means that the statistical properties of a plaintext or key are randomly dispersed into multiple output ciphertexts so that the plaintext information is masked. The performance of the system against attacks is improved by scrambling the relationship between plaintext and ciphertext, reducing their correlation. Chaos theory corresponds well to these two principles of cryptographic design. The local disorder and overall orderliness of chaotic orbits is consistent with the Diffusion property of cryptography [27]. The random-like nature of chaotic systems and the sensitivity to the parameters and initial values of the system are consistent with the Confusion property of cryptography.

Sequence ciphers are an important part of cryptography. Sequence cipher algorithms are independent of how the data is composed. Sequence cipher algorithms do not perform statistical analysis processing during encryption, but treat the data to be encrypted as an undifferentiated sequence stream and run the encryption algorithm directly. If the sequence generator has good randomness, it has high security performance. The encryption and decryption process of a sequence cipher is shown in Figure 3. When communicating with data, keys need to be transmitted securely. This is difficult to achieve in practice due to the high security requirements of the transmission. Most sequence ciphers use a method called "seed keys" to construct pseudo-random sequences. The key to a chaotic sequence cipher algorithm is a chaotic sequence generator, the prototype of which relies

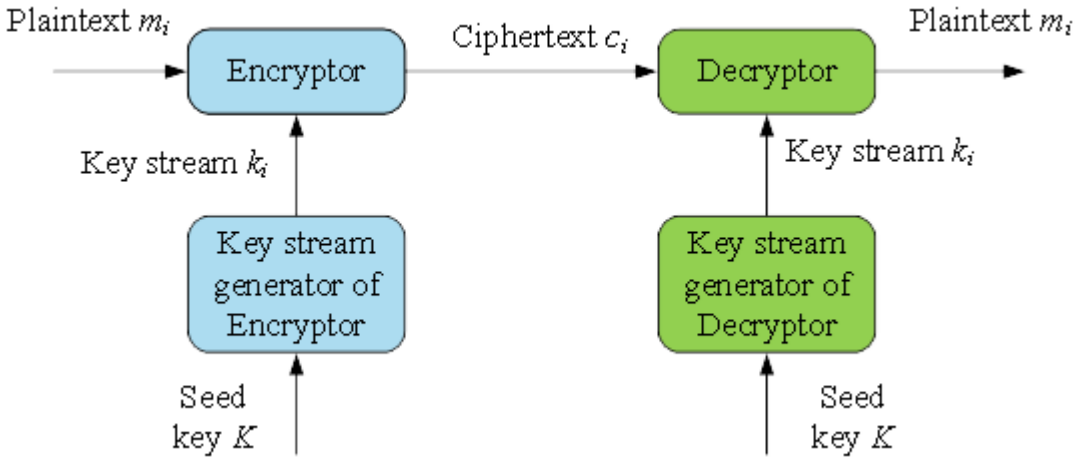


Figure 3. Encryption and decryption process of a sequence password.

on a chaotic system. The security of the sequence cipher depends on the random performance of the sequence generator used. The most important feature of a chaotic system is its sensitivity to small perturbations. Any small perturbation will cause an unpredictable change in the trajectory of the chaotic system. Chaotic sequences generated by chaotic pseudo-random sequence generators usually have a high degree of randomness.
The use of these sequences in data encryption can make the cipher difficult to break, thus increasing the security of the information being encrypted. At the same time, chaotic sequence cipher algorithms are fast and have low hardware requirements.

4. Three-dimensional sinusoidally modulated self-synchronous chaotic flow cipher algorithm.

4.1. Design of three-dimensional discrete-time chaotic dynamical systems.

When designing chaotic systems, higher dimensionality implies better chaotic properties and can also improve the overall security of chaotic encryption. However, in practice, the number of multipliers and adders required for higher dimensions increases accordingly, so an appropriate number of dimensions should be chosen. Given the limitations of the ARM processor, the dimensionality of the asymptotically stable linear system used in this design is 3. The definition of a 3-dimensional asymptotically stable linear system is shown below.

$$\begin{bmatrix} x_{1,k+1} \\ x_{2,k+1} \\ x_{3,k+1} \end{bmatrix} = A_{3\times 3} \begin{bmatrix} x_{1,k} \\ x_{2,k} \\ x_{3,k} \end{bmatrix} \tag{5}$$

$$A_{3\times 3} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = \begin{bmatrix} 0.205 & -0.595 & 0.265 \\ -0.265 & -0.125 & 0.595 \\ 0.33 & -0.33 & 0.47 \end{bmatrix} \tag{6}$$

The eigenvalues of the matrix $A_{3\times 3}$ are all less than 1. This design uses a sinusoidal function to implement a bounded feedback controller.

$$u(k) = \begin{bmatrix} 0 \\ 0 \\ \varepsilon \sin(\sigma x_{1,k}) \end{bmatrix} \tag{7}$$

Where ε and σ are the parameters of the controller. When $\varepsilon \neq 0$ and σ satisfies the following relation

$$\begin{cases} \sigma > \max\left\{\frac{\pi}{2\varepsilon}, \frac{3\pi}{2\varepsilon}, \frac{2\phi+3\pi}{2\varepsilon\sin(\phi)}, \frac{1+\|A_{3\times3}\|_\infty}{\varepsilon\cos(\phi)}\right\} \\ 0 < \phi < \frac{\pi}{2} \end{cases} \tag{8}$$

We can consider this controlled system as a chaotic system [28]. The resulting 3-dimensional discrete-time chaotic system was designed in the following form.

$$\begin{cases} x_1(k+1) = a_{11}x_1(k) + a_{12}x_2(k) + a_{13}x_3(k) \\ x_2(k+1) = a_{21}x_1(k) + a_{22}x_2(k) + a_{23}x_3(k) \\ x_3(k+1) = a_{31}x_1(k) + a_{32}x_2(k) + a_{33}x_3(k) + \varepsilon\sin(\sigma x_1(k)) \end{cases} \tag{9}$$

Where the bounded controller u(k) has parameter $\varepsilon = 3.3 \times 10^8$ and parameter $\sigma = 2.5 \times 10^5$.In this case, the poles of the controlled system are configured outside the unit circle. The Lyapunov Exponents of the controlled system are shown separately as follows:

$$LE_1^+ = 15.0236, LE_2^+ = 14.9957, LE_3^+ = 0.19093 \tag{10}$$

The chaotic phase diagram of the controlled system under the above parameter conditions is shown in Figure 4 and Figure 5.

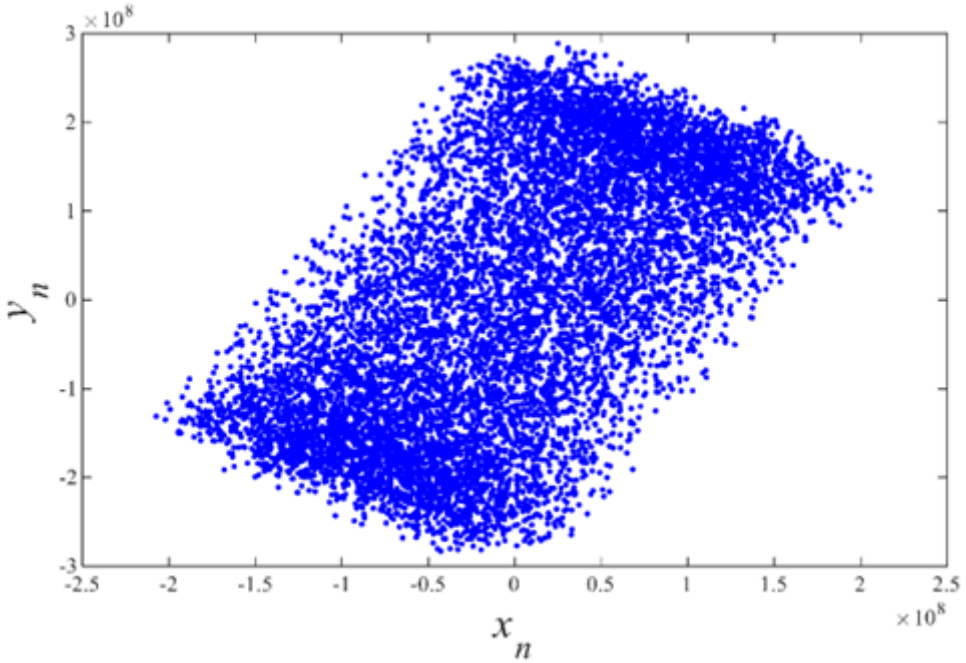


Figure 4. Chaotic Phase Diagram (X-Y)

4.2. **Self-synchronization mechanisms for chaotic flow ciphers.** Ciphertext transmission over the real channel is not completely immune to errors or loss, which is fatal for stream ciphers without a synchronisation mechanism, and results in a mismatch between the decryption key stream and the ciphertext stream. The mismatch would lead to a failed decryption and no recovery. The introduction of synchronisation is therefore key to the practicalisation of chaotic stream ciphers.

As early as 1990 Pecora and Carroll proposed a synchronisation method for two homogeneous systems. In this synchronisation method, the two systems are used as a drive system and a response system. The drive system and the response system are connected by a single or a common set of signals. Under certain conditions, the response system

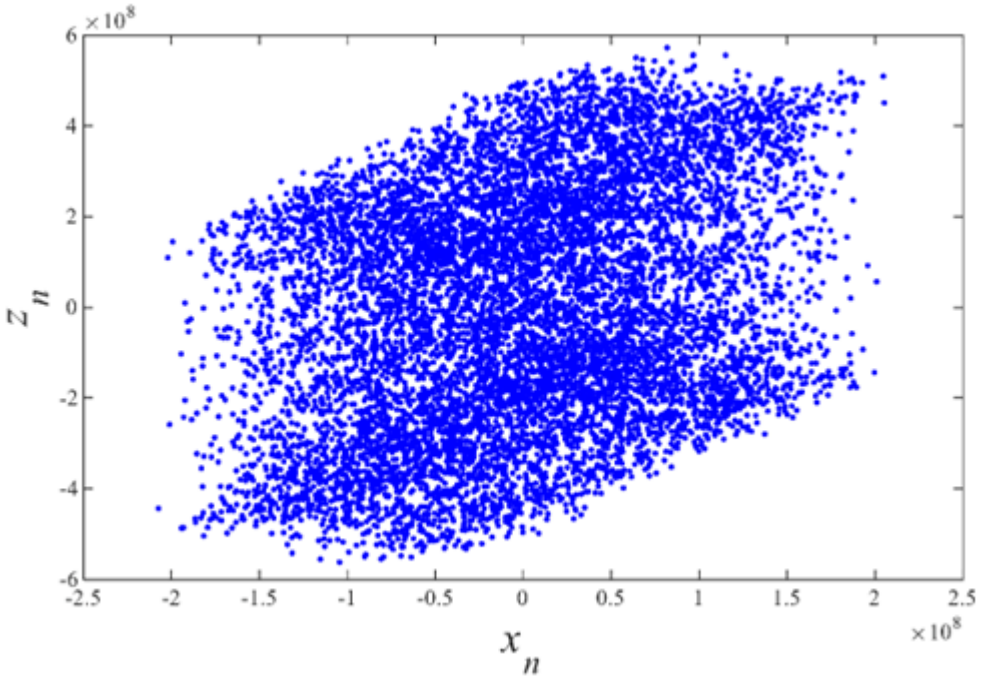


Figure 5. Chaotic Phase Diagram (X-Z)

is able to follow the drive system steadily from an arbitrary initial state, thus achieving synchronisation of the two systems [29].

With the help of the above synchronisation theory, this paper uses the above three-dimensional discrete-time chaotic dynamical system to construct self-synchronisation. We treat the encryptor as the driving system and the decryptor as the responding system. The ciphertext is the common link between the two systems. The specific form of the drive system and response system is shown below.

$$\begin{cases} x_1^{(d)}(k+1) = a_{11}^{(d)} x_1^{(d)}(k) + a_{12}^{(d)} x_2^{(d)}(k) + a_{13}^{(d)} x_3^{(d)}(k) \\ x_2^{(d)}(k+1) = a_{21}^{(d)} c(k) + a_{22}^{(d)} x_2^{(d)}(k) + a_{23}^{(d)} x_3^{(d)}(k) \\ x_3^{(d)}(k+1) = a_{31}^{(d)} c(k) + a_{32}^{(d)} x_2^{(d)}(k) + a_{33}^{(d)} x_3^{(d)}(k) + \varepsilon^{(d)} \sin\left(\sigma^{(d)} c(k)\right) \end{cases} \tag{11}$$

$$\begin{cases} x_1^{(r)}(k+1) = a_{11}^{(r)} x_1^{(r)}(k) + a_{12}^{(r)} x_2^{(r)}(k) + a_{13}^{(r)} x_3^{(r)}(k) \\ x_2^{(r)}(k+1) = a_{21}^{(r)} c(k) + a_{22}^{(r)} x_2^{(r)}(k) + a_{23}^{(r)} x_3^{(r)}(k) \\ x_3^{(r)}(k+1) = a_{31}^{(r)} c(k) + a_{32}^{(r)} x_2^{(r)}(k) + a_{33}^{(r)} x_3^{(r)}(k) + \varepsilon^{(r)} \sin\left(\sigma^{(r)} c(k)\right) \end{cases} \tag{12}$$

Where c(k) is the ciphertext, responsible for connecting the driving system and the responding system. When the two systems are isomorphic and have identical parameters, a new equation can be obtained by the subtraction operation.

$$\begin{cases} \Delta x_1(k+1) = a_{11}\Delta x_1(k) + a_{12}\Delta x_2(k) + a_{13}\Delta x_3(k) \\ \Delta x_2(k+1) = a_{22}\Delta x_2(k) + a_{23}\Delta x_3(k) \\ \Delta x_3(k+1) = a_{32}\Delta x_2(k) + a_{33}\Delta x_3(k) \end{cases} \tag{13}$$

Name the submatrix of $A_{3\times3}$ as $B_{2\times2}$.

$$B_{2\times2} = \begin{bmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{bmatrix} \tag{14}$$

$$\begin{bmatrix} \Delta x_2(k) \\ \Delta x_3(k) \end{bmatrix} = (B_{2\times2})^k \begin{bmatrix} \Delta x_2(0) \\ \Delta x_3(0) \end{bmatrix} \tag{15}$$

Where $\Delta_{x2}(0)$ and $\Delta_{x3}(0)$ are the difference between the initial values of the two systems respectively. Take the 2 norm to both sides of this equation.

$$\left\| \begin{bmatrix} \Delta x_2(k) \\ \Delta x_3(k) \end{bmatrix} \right\| \leq \|B_{2\times 2}\| \left\| \begin{bmatrix} \Delta x_2(0) \\ \Delta x_3(0) \end{bmatrix} \right\| \tag{16}$$

Take the limit for k in the above equation.

$$\lim_{k\to\infty} \|\Delta x_2(k)\| = \lim_{k\to\infty} \sqrt{(\Delta x_2(k))^2 + (\Delta x_3(k))^2} = 0 \tag{17}$$

Since $||a_{11}|| < 1$, the above equation, after simplifying the operations, we can get:

$$\lim_{k\to\infty} \Delta x_1(k) = 0 \tag{18}$$

It can be seen that as the number of generations tends to infinity, the error in each state variable between the drive and response systems will tend to zero, thus proving that the two systems are self-synchronising.

In order to verify the effectiveness of the self-synchronization, the self-synchronization system designed in this paper was built in MATLAB simulation software, and the ciphertext c(k) was directly replaced by a pseudo-random number. Of course, the ciphertext transmitted to the responding system should be the same as that of the driving system. Under the condition of the same ciphertext, the state variables of the two systems are differenced separately, and a set of data with decreasing error values with the number of selected generations is obtained, as shown in Figure 6. It can be seen that the errors

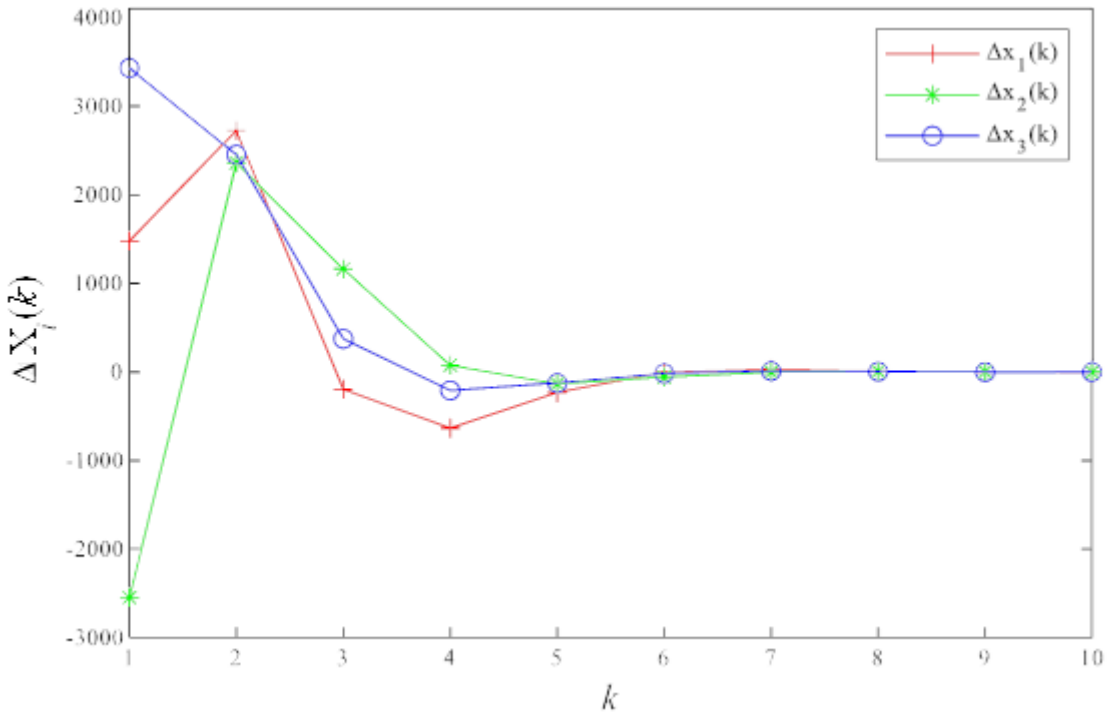


Figure 6. Self Synchronization Diagram

of the state variables in the 3 dimensions are close to 0 within 10 steps of the chosen generation, and the two systems reach full synchronisation at approximately $k = 30$ (the state variables are expressed as double precision floating point data).

4.3. **Sinusoidally modulated self-synchronous chaotic flow cipher.** The expression for the ciphertext c(k) in the 3-dimensional discrete-time chaotic system proposed in this work is shown below.

$$c(k) = \mod\left(\lfloor x_1(k) \times \xi \rfloor, 2^8\right) \oplus p(k) \tag{19}$$

Where the symbol $\oplus$ is the XOR operation, mod(,28) denotes the lower 8 bits of the intercept result, and p(k) is the plaintext. The constant ξ amplifies the chaotic sequence to the integer part and takes values in the general range of $105 < \xi < 104$. The larger the value of ξ, the more sensitive the key is.
However, encryption and decryption methods using both a single state variable and the multiplication of two state variables are not effective against statistical attacks. In addition, an attacker can use a differential attack to decipher a partial key. To address this problem, this work introduces sinusoidal modulation, which effectively isolates the state variables from the ciphertext, making it impossible to compromise the key in the form of a modal operation by selecting the initial state. The improved ciphertext is shown below.

$$c(k) = \mod\left(\lfloor \sin\left(x_1(k)\right) \times \xi \rfloor, 2^8\right) \oplus p(k) \tag{20}$$

The improved cipher is known as the 3-D sine modulated self-synchronous chaotic stream cipher (3-D SM-SCSC). 3-D SM-SCSC's encryption and decryption flow and channel transmission structure are shown in Figure 7. 3-D SM-SCSC belongs to the symmet-

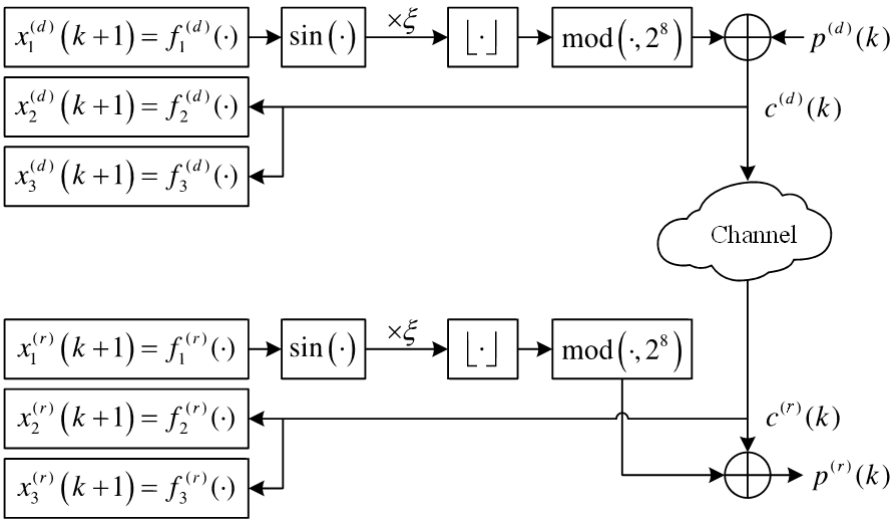


Figure 7. The Block Diagram of 3-D SM-SCSC

ric stream cipher, and the same keys are used for encryption and decryption, including ε, σ and A_{33}. The cipher chooses the state variable $x_1(k)$ in the above 3-dimensional discrete-time chaotic system. After sine mapping, multiplication, rounding and modulo operations, the corresponding key stream is obtained. The ciphertext stream is obtained from the keystream and the plaintext stream using a simple by-bit XOR operation. Thus, the decryption and encryption operations can be identical, which allows the encryptor and decryptor to be multiplexed in key logic to reduce resource usage.

5. **Experimental simulation and safety analysis.**

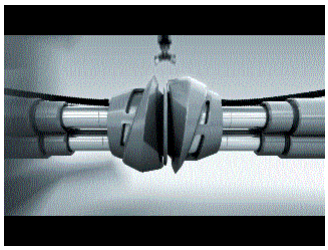
5.1. **Assessment of statistical stochastic properties.** Currently, the most authoritative test method for the performance of chaotic sequence ciphers is the series of statistical test suites offered by the National Institute of Standards and Technology (NIST). This test suite has 15 performance metrics. The test results use both the PROPORTION and P-VALUE metrics. If the PROPORTION of the test results falls within the confidence interval, it indicates that the 3-D SM-SCSC algorithm has a high degree of randomness. Conversely, it indicates that the 3-D SM-SCSC algorithm has low randomness. In general, a P-VALUE greater than 0.001 indicates good randomness of the input sequence. Various tests were performed on the 3-D SM-SCSC and the results are shown in Table 1.

Table 1. Result of NIST Statistical Test.

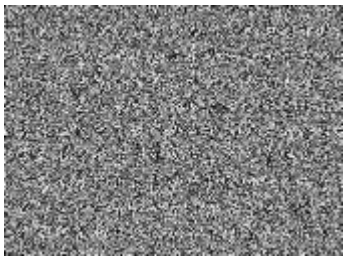
Statistical Tests	**P-VALUE**	**PROPORTION**
Frequency	0.829047	0.976
Block Frequency	0.000198	0.987
Cumulative Sums	0.653773	0.972
Runs	0.410055	0.99
Longest Run	0.574903	0.986
Rank	0.657933	0.987
Fft	0.002373	0.999
NonOverlapping Template	0.001173	0.999
OverlappingTemplate	0.881662	0.99
Universal	0.516113	0.989
ApproximateEntropy	0.000156	0.985
RandomExcursions	0.84253	0.9937
RandomExcursions Variant	0.989002	0.9952
Serial	0.420827	0.995
LinearComplexity	0.33611	0.995

It can be seen that all tested PROPORTIONs are within the confidence interval and the P-VALUE is greater than 0.001, which indicates that the 3-D SM-SCSC algorithm produces sequences with high random performance.

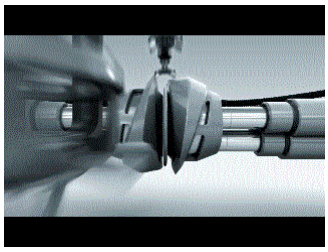
5.2. **Subjective tests.** In the subjective test, two HEVC video sequences (frames 1-12) were encrypted to verify the feasibility of the solution, with a resolution of 352×288 and 60fps transmission frame rate. The adopted video coding software is HM 16.9, and the quantization parameter is set to 10. The plaintext images and encrypted images of frames 6 and 12 are shown in Figure 8 and Figure 9, respectively. It can be seen that no visual information can be seen on the chaotic encrypted video frames, indicating that the 3-D SM-SCSC algorithm has good confidentiality.



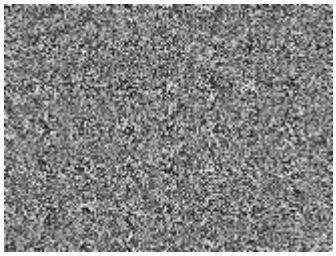
(a) Frame 6 of the original video



(b) Frame 6 of the encrypted video



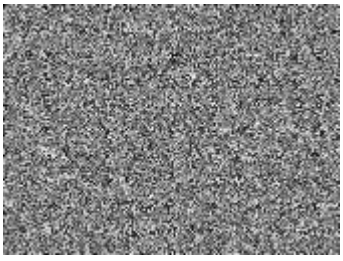
(c) Frame 12 of the original video



(d) Frame 12 of the encrypted video

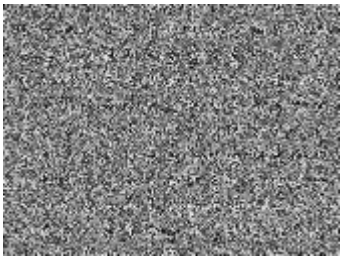
Figure 8. Encryption results for part of frames in video A

(a) Frame 6 of the original video



(b) Frame 6 of the encrypted video

(c) Frame 12 of the original video



(d) Frame 12 of the encrypted video

Figure 9. Encryption results for part of frames in video B

5.3. **Objective tests.** Firstly, information entropy is usually used to measure the uncertainty and randomness of information. A higher entropy value of the encrypted video frame indicates a higher randomness of the entire image pixel distribution, and at the same time can reflect a lower amount of information contained in the video frame. Therefore, this scheme uses information entropy to verify the encryption effect of the 3-D SM-SCSC algorithm and to compare it with other video encryption algorithms [30,31,42,33,34]. The closer the information entropy is to 8, the better the encryption performance is. In this paper, the information entropy of each frame of Video A and Video B was calculated before and after encryption, as shown in Table 2. The results show that the information

entropy of both video frames reached 7.997 after encryption, which is a good encryption effect.

Table 2. Entropy of video frames before and after encryption

Frames	Video A		Video B	
	Original video	Encrypted video	Original video	Encrypted video
1	3.8736	7.9978	3.5661	7.9975
2	3.9803	7.9978	3.5731	7.9975
3	3.9714	7.9976	3.573	7.9981
4	4.0595	7.998	3.5771	7.998
5	4.0621	7.9976	3.5893	7.9979
6	4.0309	7.9977	3.6002	7.9974
7	4.0269	7.9978	3.6284	7.9975
8	4.0201	7.9976	3.6652	7.9973
9	3.9786	7.998	3.705	7.9976
10	3.9738	7.9976	3.7311	7.9971
11	3.9523	7.9975	3.7456	7.9977
12	3.9558	7.998	3.7942	7.9976

The average information entropy per frame after video A encryption is shown in Table 3. It can be seen that the information entropy of the 3-D SM-SCSC algorithm is at a high level compared to other encryption algorithms, and is higher than that obtained by the traditional 3-D SCSC algorithm.

Table 3. Entropy of video frames before and after encryption

Algorithms	Original video	Encrypted video
3-D SM-SCSC	3.9904	7.9978
3-D SCSC	3.9904	7.9977
[30]	7.4532	7.9897
[31]	7.4532	7.9978
[32]	7.5697	7.9975
[33]	7.4532	7.9992
[34]	7.6927	7.9969

Secondly, NPCR and UACI are two metrics that test whether an encryption algorithm can resist differential attacks; the expected value of NPCR is 99.6094% and the expected value of UACI is 33.4635%. When the values of NPCR and UACI are close to the expected value, the better the encryption performance.

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \quad D(i,j) = \begin{cases} 1, C_1(i,j) = C_2(i,j) \\ 0, C_1(i,j) \neq C_2(i,j) \end{cases} \tag{21}$$

$$\mathrm{UACI} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |C1(i,j) - C2(i,j)|}{255 \times M \times N} \times 100\% \tag{22}$$

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. The average NPCR and average UACI of video A after encryption is shown in Table 4. It can be seen that the NPCR and UACI of the 3-D SM-SCSC algorithm are closer to the expected values compared to other video encryption algorithms, which indicates a better resistance to differential attacks.

Table 4. NPCR & UACI of video frames

Algorithms	NPCR	UACI
3-D SM-SCSC	99.6063	33.4603
3-D SCSC	99.6010	33.4537
[30]	99.5956	33.3937
[31]	99.6136	33.4512
[32]	99.6212	31.3851
[33]	99.6216	33.4502
[34]	99.1547	33.2072

6. **Conclusion.** In this paper, an in-depth study of network video surveillance encryption system is conducted, and a chaotic sequence-based network surveillance video encryption algorithm is designed on this basis. Firstly, the overall architecture of the video surveillance encryption system is given. Secondly, the cryptographic fundamentals, chaos theory and chaotic sequence cipher are highlighted. Then, a three-dimensional discrete chaotic dynamical system is designed. Based on the above three-dimensional discrete-time chaotic dynamical system, the 3-D SM-SCSC algorithm is designed. After performing a series of sine, multiplication and rounding operations on a single state variable of the chaotic system, a low 8-bit XOR operation is used to mask the plaintext information. In this case, the sine function is used as a non-linear step of the cipher, which effectively improves the security of the cipher. Finally, the feasibility of the 3-D SM-SCSC algorithm is specifically verified. Subjective and objective experiments are analysed on the encrypted video. The experimental results verify the effectiveness of the 3-D SM-SCSC algorithm, and the encrypted video can effectively resist existing attacks.

Data Availability. The data used to support the findings of this study are included within the article.

Conflicts of Interest. The author declares that there is no conflict of interest regarding the publication of this paper.

Funding Statement. This work is supported by project of Chongqing Natural Science Foundation Project (CSTB2022NSCQ-MSX1510).

REFERENCES

[1] K. Talvitie-Lamberg, "Video Streaming and Internalized Surveillance," *Surveillance & Society*, vol. 16, no. 2, pp. 238-257, 2018.

[2] T.-Y. Wu, C.-M. Chen, X. Sun, S. Liu, and J. C.-W. Lin, "A Countermeasure to SQL Injection Attack for Cloud Environment," *Wireless Personal Communications*, vol. 96, no. 4, pp. 5279-5293, 2017.

[3] T.-Y. Wu, X. Guo, Y.-C. Chen, S. Kumari, and C.-M. Chen, "SGXAP: SGX-Based Authentication Protocol in IoV-Enabled Fog Computing," *Symmetry*, vol. 14, no. 7, 1393, 2022.

[4] T.-Y. Wu, Q. Meng, S. Kumari, P. Zhang, "Rotating behind Security: A lightweight authentication protocol based on IoT-enabled cloud computing environments," *Sensors*, vol. 22, no. 10, 3858, 2022.

[5] T.-Y. Wu, Q. Meng, L. Yang, X.-L. Guo, S. Kumari, "A provably secure lightweight authentication protocol in mobile edge computing environments," *The Journal of Supercomputing*, vol. 78, pp. 13893-13914, 2022.

[6] L.-L. Kang, R.-S. Chen, Y. –C. Chen, C.-C. Wang, X.-G. Li, and T.-Y. Wu, "Using Cache Optimization Method to Reduce Network Traffic in Communication Systems Based on Cloud Computing," *IEEE Access*, vol. 7, pp. 124397-124409, 2019.

[7] T.-Y. Wu, X.-L. Guo, Y.-C. Chen, S. Kumari, and C.-M. Chen, "Amassing the Security: An Enhanced Authentication Protocol for Drone Communications over 5G Networks," *Drones*, vol. 6, no. 1, 10, 2021.
[8] J.-Q. Gao, H.-Y. Zou, F.-Q. Zhang, and T. Y. Wu, "An intelligent stage light-based actor identification and positioning system," *International Journal of Information and Computer Security*, vol. 18, no. 1/2, pp. 204-218, 2022.
[9] T.-Y. Wu, X.-N. Fan, K.-H. Wang, J.-S. Pan, 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.
[10] S. Kumar, A. Damaraju, A. Kumar, S. Kumari, and C. –M. Chen, "LSTM Network for Transportation Mode Detection," *Journal of Internet Technology*, vol. 22 (4), 891-902, 2021.
[11] X.-J. Tong and M.-G. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator," *Signal Processing*, vol. 89, no. 4, pp. 480-491, 2009.
[12] K. B. Sudeepa, G. Aithal, V. Rajinikanth, and S. C. Satapathy, "Genetic algorithm based key sequence generation for cipher system," *Pattern Recognition Letters*, vol. 133, no. 12, pp. 341-348, 2020.
[13] Z.-X. Wang, X.-Y. Wang, and T. Tian, "Constructing de Bruijn Sequences Based on a New Necessary Condition," *International Journal of Foundations of Computer Science*, vol. 31, no. 3, pp. 301-312, 2020.
[14] S. Maitra, B. Mandal, T. Martinsen, D. Roy, and P. Stanica, "Analysis on Boolean Function in a Restricted (Biased) Domain," *IEEE Transactions on Information Theory*, vol. 66, no. 2, pp. 1219-1231, 2020.
[15] X. Zhang, Z. Zhou, and Y. Niu, "An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding," *IEEE Photonics Journal*, vol. 10, no. 4, pp. 1-14, 2018.
[16] C.-M. Chen, L.-L. Xu, K.-H. Wang, S. Liu, 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.
[17] C.-M Chen, W.-C Fang, S. Liu, T.-Y. Wu, J.-S. Pan, K.-H. Wang, "Improvement on a Chaotic Map-based Mutual Anonymous Authentication Protocol," *Journal of Information Science & Engineering*, vol. 34, no.3, 2018.
[18] C.-T. Li, T.-Y. Wu, and C.-M. Chen, "A Provably Secure Group Key Agreement Scheme with Privacy Preservation for Online Social Networks Using Extended Chaotic Maps," *IEEE Access*, vol. 6, pp. 66742-66753, 2018.
[19] S. Lian, J. Sun, J. Wang, and Z. Wang, "A chaotic stream cipher and the usage in video protection," *Chaos, Solitons & Fractals*, vol. 34, no. 3, pp. 851-859, 2007.
[20] A.-V. Diaconu and K. Loukhaoukha, "An Improved Secure Image Encryption Algorithm Based on Rubik's Cube Principle and Digital Chaotic Cipher," *Mathematical Problems in Engineering*, vol. 2013, no. 6, pp. 1-10, 2013.
[21] W. Al-Nuaimy, M. A. M. El-Bendary, A. Shafik, and F. Shawki, "An SVD audio watermarking approach using chaotic encrypted images," *Digital Signal Processing*, vol. 21, no. 6, pp. 764-779, 2011.
[22] Y. Zhao, X. Zou, Z. Lu, and Z. Liu, "Chaotic Encrypted Polar Coding Scheme for General Wiretap Channel," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 12, pp. 3331-3340, 2017.
[23] Y. Lin, Q. Din, M. Rafaqat, A. A. Elsadany, and Y. Zeng, "Dynamics and Chaos Control for a Discrete-Time Lotka-Volterra Model," *IEEE Access*, vol. 8, pp. 126760-126775, 2020.
[24] H. Wei, C. Zhang, T. Wu, H. Huang, and K. Qiu, "Chaotic Multilevel Separated Encryption for Security Enhancement of OFDM-PON," *IEEE Access*, vol. 7, pp. 124452-124460, 2019.
[25] E. Asiain and R. Garrido, "Anti-Chaos control of a servo system using nonlinear model reference adaptive control," *Chaos, Solitons & Fractals*, vol. 143, p. 110581, 2021.
[26] X. Bai, Q. Li, and M. Xu, "Nonlinear Dynamics and Control of Time-Delay Supercavitating Vehicle," *International Journal of Bifurcation and Chaos*, vol. 32, no. 02, 2022.
[27] K. SundaraKrishnan and J. B, "A Symmetric Key Multiple Color Image Cipher Based on Cellular Automata, Chaos Theory and Image Mixing," *Information Technology and Control*, vol. 50, no. 1, pp. 55-75, 2021.
[28] K. K. Bhardwaj, S. Banyal, and D. K. Sharma, "Probabilistic routing protocol with firefly particle swarm optimisation for delay tolerant networks enhanced with chaos theory," *International Journal of Innovative Computing and Applications*, vol. 12, no. 2/3, 123, 2021.

[29] S. Rusu-Anghel, S. S. Mezinescu, and I. C. Lihaciu, "Experimental stand and researches on pantograph-catenary contact force control using chaos theory," *Journal of Physics: Conference Series*, vol. 1781, no. 1, 012029, 2021.

[30] D. Chen, S. Shi, X. Gu, and B. Shim, "Weak Signal Frequency Detection Using Chaos Theory: A Comprehensive Analysis," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 8950-8963, 2021.

[31] F. Sufi, F. Han, I. Khalil, and J. Hu, "A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications," *Security and Communication Networks*, vol. 4, no. 5, pp. 515-524, 2010.

[32] Y. Bai, B. Liu, J. Ren, and Y. Mao, "Highly Secure and Reliable 7-Core Fiber Optical OFDM Access System Based on Chaos Encryption Inside Polar Code," *IEEE Photonics Journal*, vol. 14, no. 1, pp. 1-6, 2022.

[33] M. Maazouz, A. Toubal, B. Bengherbia, O. Houhou, and N. Batel, "FPGA implementation of a chaos-based image encryption algorithm," *Journal of King Saud University - Computer and Information Sciences*, vol. 11, no. 2, 2022.

[34] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, no. 2, pp. 943-961, 2018.