Chaotic Encryption-Based Network Robot for Indoor Security and Remote Video Monitoring

*Man Zhang, Ning Chen
Chongqing Technology and Business Institute, Chongqing, 401520, China
E-mail: zhangman@cqtbi.edu.cn; chenning@cqtbi.edu.cn
*Corresponding author

Keywords: video encryption, video encrypted transmission, home security robot, multi-hazard information acquisition, active sniffing

Recieved: April 20, 2024

As society develops and living standards improve, people are putting forward higher and higher requirements for their living environment. To fulfill interior security requirements, fire security, and building automation, intelligent robotics has come into being. Video data under intelligent network remote monitoring is different from traditional data, as video is a kind of data with a large amount of information, highly complex coding and decoding, difficult to process, and requires real-time operation. Therefore, it is important to focus on the format characteristics of H.264 when designing the encryption scheme. Due to the heavy computational burden caused by the large amount of video data, it is not possible to encrypt all data when encrypting video data, and at the same time to ensure that the traditional encryption algorithms, such as Data Encryption Standard (DES) and Rivest-Shamir-Adleman (RSA), are no longer suitable for video encryption applications to ensure that the format specificity and good operability are not compromised. Therefore, this paper aims to design a sufficiently secure and practical video encryption scheme for the remote monitoring of network robots based on the H.264 codec standard by introducing a chaotic iterative system, and finally to design and implement an indoor security method for remote monitoring of video technology based on chaotic encryption for network robots with certain practical application value.

Povzetek:Študija predlaga razvoj varnega video enkripcijskega sistema za oddaljeno spremljanje z uporabo robotske tehnologije, temelječe na H.264 in kaotičnem iterativnem sistemu za izboljšanje notranje varnosti.

1 Introduction

With the rapid development of China's economy, people's living standards continue to improve, and people also put forward a higher level of requirements for the family living environment [1]. Indoor security system is an indispensable part of the modern residential security system, in the process of modern urban construction, a lot of homes use advanced, scientific, and technical means to carry out community management and maintenance [2-3]. However, the traditional sense of the community access control system is due to its complex functions and was built to reduce its use [4-5], in addition to many intelligent management systems although it achieves some conventional control, but cannot fully meet the people of the family living environment intelligent monitoring of this feature. The network robot remote video technology under the indoor security monitoring system, can be on people's living environment, home security, and other aspects of real-time monitoring [6-7]. It can not only achieve remote control and centralized management functions, but also send alarm signals to the security center through the alarm device when some unexpected events occur, to achieve rapid processing purposes [8], and at the same time can also upload the dangerous situation information to the dispatching room, so that the management staff can take corresponding measures in time. Therefore, it is important to explore new methods of indoor security based on chaotic encryption of the network robot remote monitoring video technology, for today's indoor security [9-10].

Table 1: Related work

Reference	**Objective**	**Method**	**Result**	**Limitations**
[11]	The paper investigated chaotic encryption as an option for security issues related to video leakages, testing the viability of the idea by establishing a working prototype system in place for real-time video communications.	A prototype system for transmitting video in real-time was created to verify the efficacy of approach, which uses tent connecting to improve a chaotic encryption algorithm for enhanced performance.	The result demonstrated the viability and efficacy of the optimized chaotic encryption method in real-time video transmission by showing that it outperforms distinct techniques and incorporates logistic and tent mapping.	The following section indicates several possible drawbacks, such as the need for more testing in various scenarios, unfixed vulnerabilities, or scalability problems with bigger datasets or in various systems.
[12]	The research focused on integrated programming features in robotics boards, the work attempts to enhance the effectiveness and safety of algorithms for recognizing face s in robotics applications.	The study suggested using a cloud server to enhance the robustness, efficiency, and speed of facial recognition processing in robotics boards and proposes a secure hybrid encryption method using bit slicing (BS) and discrete Fourier transform (DFT).	The study result shows that the suggested approach significantly outperforms the current models and encryption algorithms, such as advanced Encryption Standard (AES), BS-DFT encryption, Genetic Algorithm (GA), and deoxyribonucleic acid (DNA) algorithm.	A potential BS-DFT encryption algorithm was presented in the work, although it lacks comprehensive information on computational or resource expenses, as well as deep insights into potential limits and negative aspects.
[13]	The objective solves the issues of significant redundancy and inadequate communication safety for industrial robots' multi-channel real-time vibration sensor information.	The study suggested a compressed sensing (CS)-based approach that uses a separate cosine transform matrix, a chaotic matrix, and cross-correlation function integration for sparse decomposition evaluation, robot data integration, and effective encrypted transmission.	The research results show that the suggested approach improves encryption efficiency during transmission while also drastically reducing the quantity of data transferred. That maintains signal transmission security and efficiency without compromising useful information.	The suggested method's shortcomings are not specifically mentioned in the section. Difficulties with computing expenses, complexity of implementation, or certain situations where the approach could not work well are illustrations of possible drawbacks.

[14]	The objective of the research suggested a lightweight encryption strategy for the Internet of Robotic Things (IoT) robots, utilizing discrete-time chaotic maps like Cubic Map and Ricker's Population Model Map for effective data encryption.	The study developed a new chaotic encryption mechanism using discrete-time maps, tested it on the NVIDIA Jetson Orin evolution package, and evaluated its effectiveness using statistical tests and security evaluations.	The research demonstrated that a high rate of image encryption per second was possible due to the developed encryption mechanism's suitability for parallel processing, providing robust security for Internet of Things (IOT) applications, particularly when encrypting large files.	The paper suggested an encryption method, but acknowledges its limitations, such as scalability and suitability for various IoRT scenarios, and calls for further analysis to assess its resilience and suitability for real-world implementation.
[15]	The objective of the research was to solve security issues with portrait data by setting the proposed identity security technology platform for remote sensing (RS) images provided by Unmanned aerial vehicles (UAVs).	The suggested approach makes use of dynamic chain Deoxyribonucleic Acid (DNA) encoding, phase-change discontinuous propagation, lightweight bit-level disorientation hash eigenvalue extraction, edge identification face detection technology, and selected matrix encryption.	The study's experimental results that chaotic pseudo-random sequence and dynamic DNA chained encrypting increase the resilience of cryptographic systems, decrease their complexity, and increase their security and efficiency.	Though efficient and secure, the suggested system lacks information regarding possible drawbacks such as processing complexity or particular situations, and further research has been done to determine how well it works in a variety of UAV and RS communication contexts.
[16]	The objective of the investigation was to examine security concerns related to IoT-based smart home systems (SHSs) and present a thorough synopsis of previous studies conducted in the domain.	The methodology tackles two security issues by analyzing SHSs, proposing precise definitions, analyzing design, extracting features, and discussing cyber-attack methods, defenses, security frameworks, assessment methods, technology scenarios, and real-world research.	The study explored security concerns in SHS through analysis of architecture, cyberattack techniques, defenses, structures, and combination scenarios.	The study makes the argument that resolving security problems can prove difficult due to the quickly growing and complicated nature of SHSs and that the emphasis on study cannot adequately account for real-world constraints.
[17]	The primary objective of the	The research proposed encryption protocols for	Comparing the modified AES algorithm to the	The section does not mention

	study propose and evaluate the lightweight crypto-encryption protocols and content-based video encryption standards for real-time video surveillance, focusing on object tracking enhancement and data security in video surveillance (VS) technologies.	object tracking and video data protection, including weight average background reduction, an entropy adaptable object learning model, and a modified Advanced Encryption Standard (AES) method for multi-object tracking.	current encryption standards, it demonstrates virtually NCPR value and quickest time. Weight average background removal techniques help the entropy adaptive object learning model conserve memory and enhance multi-object tracking performance.	specific limitations, but potential drawbacks include integration difficulties, additional validation requirements, and balancing security and computing performance.
[18]	The study investigated enhancing the safety features of a multi-chaotic systems-based color image encrypting technique by addressing defects such as poor statistical characteristics and vulnerability to known-plaintext and chosen-plaintext attacks.	The approach involves altering the pixel-chaotic-shuffle method of image encoding, establishing a new pixel-chaotic-diffusion structure, extracting keys from chaotic configurations, and adjusting shuffling time based on plain images.	The modified cryptosystem has greater statistical properties and more resilient to known and specific plaintext attacks, according to the study findings.	The suggested approach can be impacted by possible drawbacks such as higher computing complexity, speed trade-offs for security, and difficulties incorporating modifications in current systems.
[19]	The study explored the challenge of preventing unauthorized access to sensitive image information using a new privacy-preserving method combining a chaotic dynamical system, Arnold transformation (AT), and the code for DNA sequencing.	The proposed privacy-preserving method utilizes an Arnold transformation, DNA sequencing code, and a chaotic dynamical system to create an initial S-box. Various techniques, such as the National Institute of Standards and Technology, histogram analysis, nonlinearity analysis, and strict avalanche criterion (NIST, HA, NL, SAC) , are used in tests to validate the randomness and security of the S-box.	The effectiveness of suggested system was demonstrated by its strong security measures and resilience to different types of assaults, which havebeen evaluated and comparedwith current approaches.	The suggested privacy-preserving scheme can have drawbacks in real-world implementation and scalability, and its efficiency in practical scenarios can require further evaluation.

[20]	The study examined the security issues in SHS through consideration of cyberattack tactics, defenses, architecture, structures, and combination situations.	The methodology used involves analyzing several SHS-related factors, including their architecture, cyberattack tactics used, defense systems in place, structural weaknesses, and possible situations in which numerous attack vectors are merged.	The study of the results indicates possible weak points, attack routes, and defense systems for SHS, offering insights into the difficulties and dangers involved in protecting against cyberattacks.	The analysis provides insightful information on SHS security issues, but it could be affected by the study's breadth, the accuracy of data, the evolution of cyber threats, and the efficacy of suggested defenses.

There are issues with the suggested BS-DFT encryption algorithms scalability, weaknesses, and computational complexity. Chaotic encryption is suggested as a solution, providing increased efficiency and security. To guarantee its resilience in IoRT and SHS settings, more investigation is required.

2 Video encryption algorithm based on chaos principle

2.1 Analysis of STC principle

Here the author uses one of the most widely used models in the study of spatio-temporal chaotic systems, i.e. the coupled image lattice to analyse the spatio-temporal chaotic behaviour. For the reaction-diffusion process.

$$\partial_t \mu = F(\mu) + \delta \nabla^2 u \tag{1}$$

Here it is divided into two processes, one of which is the local chaotic reaction process; the local reaction process can be formulated as a parallel non-linear image in one dimension, and its constraints are as follows.

$$x(i) -> x'(i) = f(x(i)) \tag{2}$$

where x is the state of the current process, i are the coordinates of the lattice and L is the number of lattices of the system in the current STC. The second process is the overall diffusion process. For the diffusion process, we assume that each lattice is only associated with the lattice nearest to it, and here the Labrador operator discretization is used to calculate the final connected image lattice model in one dimension was found to be

$$X_{n+1}(i) = (1-\varepsilon) f\big(X_n(i)\big) + \varepsilon/2[f\big(X_n(i+1)\big) + f\big(X_n(i-1)\big) \tag{3}$$

It is shown that the coupled image lattice system is considered a discretized dynamical system, both from the temporal and spatial perspectives.

2.2 H.264 STC-based video encryption algorithm

The residual data is encoded in the basic grade specified in the H.264 standard using the CAVLC encoding mode, which comes after the intra-frame inter-frame predicted method. This study presents a method that uses two modules: the space-time chaos encryption module and the encryption selection management module, to encrypt a tiny quantity of data with great security. Two chaotic sequence systems provide two pseudo-random sequences that are used to encrypt the data and regulate the encryption preference, respectively. The primary video stream proceeds to the encoder for compressing coding. Here, the pattern data following intra-frame forecasting pattern choosing and inter-frame chunking sequence selection is chosen and protected by the encryption choosing manage module. The remaining coded residual data proceeds to the CAVLC for the entropy coding manipulation, where the pertinent coding parameters in the coder process are additionally chosen and secured by the encryption preference control section utilizing the pseudo-random sequence flow produced by the STC system [21]. Through incorporating randomness into encryption algorithms and strengthening their resistance to brute-force assaults, chaotic encryption improves indoor security. This strategy strengthens security measures against unauthorized access and possible compromises by protecting sensitive data in indoor locations and guaranteeing the integrity and security of the data transferred.

2.2.1 Selective encryption control algorithm design

The DCT transformation procedure can provide a high-security encryption impact when the data is encrypted, it is simple to lose the video data's original compression properties, this method decides to encrypt the data, which has a significant influence on the decrypted video's ratio of compression intra-frame inter-frame prediction mode and the scanning sequence of the residual data and related parameters in the CAVLC encoding process.

H.264 uses context-based coding in both the entropy coding process, i.e. during the coding process, instead of coding the current data singularly, it refers to the situation of the data already coded before and after, while there are multiple code tables used for coding in the coding process, the coding only needs to select the corresponding data in the code table dynamically according to the coding value, ensuring high efficiency of coding by.

- The number of trailing coefficients and the sum of non-zero coefficients are first encoded in the residual coefficients.
- Encoding the sign bits of trailing coefficients in the range (0 - 3).
- Encode the magnitude of the other non-zero coefficients excluding the trailing coefficients.
- Next, the total number of zeros preceding the last non-zero coefficient in the residual coefficient block is encoded.
- Finally, the number of zeros preceding each non-zero coefficient in the residual block is encoded.

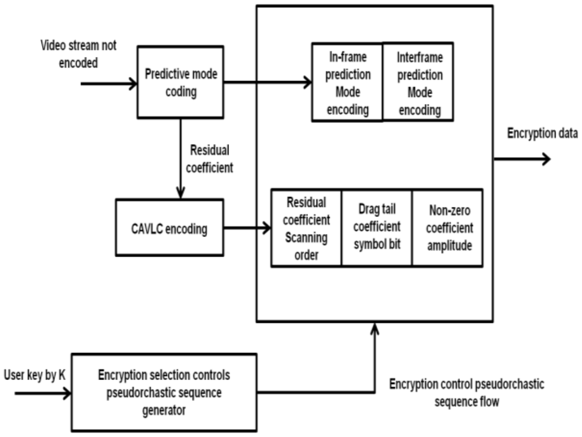
Video stream not encoded
Predictive mode coding
In-frame prediction Mode encoding
Interframe prediction Mode encoding
Residual coefficient
CAVLC encoding
Residual coefficient Scanning order
Drag tail coefficient symbol bit
Non-zero coefficient amplitude
Encryption data
User key by K
Encryption selection controls pseudorchastic sequence generator
Encryption control pseudorchastic sequence flow

Figure 1: Encryption selection control module design

Except for (1) and (4) where the modification of the encoding control parameters will result in changing the coefficient control parameters of the original message format, the encoding parameters in the other three processes without compromising the functionality of the original file format, certain factors, such as the sign bits of the following parameters, the amplitude for the non-zero coefficients, and the number of zeros preceding each non-zero coefficient, can be utilized as encryption options; To improve the encryption speed, some schemes only select the trailing coefficient symbol bits for encryption operation, which can achieve fast encryption but also sacrifice part of the security. To solve the above problems, the encryption algorithm in this paper is designed as a selective encryption control module, that produces a pseudo-random pattern of streaming key using the more widely utilized logistic equation $[i]$. These sites are encrypted using a pseudo-random sequence that is utilized to make a decision. Data encryption and when the key value should be used are determined by the parity of the pseudo-random sequence $[i]$. Figure 1, if the read is 1, the relevant data is encrypted at that moment; if it is 0, no encryption is chosen.

The encryption selection control pseudo-random sequence generator adopts equation (4) as the generation equation of the pseudo-random sequence, and uses the mean threshold method to generate the sequence according to equation (5) as follows.

$$x_{\mathrm{i}} = \mu x_{\mathrm{i-1}}(1 - x_{\mathrm{i-1}}) \tag{4}$$

$$\begin{cases} \quad aver = \sum_{i=0}^{n} x_i / n \\ key[i] = 0; \quad if x_i < aver; \\ \\ key[i] = 1; \quad if x_i > aver; \end{cases} \tag{5}$$

where n is the overall number length of the unique floating-point sequence and aver is an average value of the randomly generated original floating-point sequences. A binary sequence considers key[i] equal to 0 when the current sequence considers x_i is smaller than ever, and 1 when x_i is larger than ever. The security control is selected using the final produced binary pseudo-random sequence key. The location to be encrypted includes intra-frame prediction pattern parameters, inter-frame chunking pattern parameters, CAVLC pre-encoding zigzag rearrangement residual data, encoding trailing coefficient sign bits, and non-zero coefficient amplitude in five parts. encryption module, the scheme becomes dynamic encryption, and the encrypted data and the encryption effect of each encryption sub-process are different. This makes the encryption algorithm more secure and can achieve better encryption results.

2.2.2 STC model design

This work presents the design of an STC encryption module depending on the STC system, based on the encryption management module design. The module is designed to generate a pseudo-random sequence stream of 512 bits in length for encryption through the initial value acquisition, data truncation, and transformation of the STC box by the user inputting the key and feeding the key into the STC system. According to the analysis in the previous section, the coupled image lattice as an STC model is the most common, which has the characteristics of high computational efficiency, high degree of parallelism, compatibility with traditional theories, easy analysis, etc. Here we namely choose the neighboring STC model (Equation 6), and the algorithm is chosen as Equation (7).

$$X_{\mathrm{n}+1}(i) = (1-\varepsilon)f\big(X_{\mathrm{n}}(i)\big) + \varepsilon/2\big[f\big(X_{\mathrm{n}}(i+1)\big) + f\big(X_{\mathrm{n}}(i-1)\big)\big] \qquad (6)$$

$$X_{i+1} = 8^{*}X_i^4 - 8^{*}X_i^2 + 1 \qquad (7)$$

as the local chaos equation, with x taking values in the range (1,1).

Table 2: An estimated table of entropy indices and Lyapunov coefficients

Local mapping	Logistic	$X_{,+1}=8*X_4-8*X^2+1$
Lyapunov exponent	0.6501	1.3871
Local mapping	Logistic	$X_{,+1}=8*X_4-8*X^2+1$
approximate entropy	0.6567	1.2904
Chaotic equation	Logistic	Formula (7)
Lyapunov exponent	0.6503	1.2816
Local mapping	Logistic	$X_{,+1}=8*X_4-8*X^2+1$
Lyapunov exponent	0.6136	1.2816

By testing the data associated with the local chaos mapping (Eq. 7) in this STC, Table 2 shows the Lyapunov exponent and the approximate entropy index.

It can be seen that the performance associated with the local chaotic mapping (7) is better than that of the Logistic equation. Compared to ordinary chaotic systems, STC has extended the chaotic properties to space, ensuring that it is more complex and the resulting pseudo-random chaotic sequences for encryption are more difficult for an attacker to break. Additionally, based on the attributes of the connected image lattice model, lattices are quite closely related to each other, and the one-way robustness ensures that it is very difficult to break through by a reverse attack, greatly increasing the difficulty of attackers to break through and increasing the security of the encryption system.

3 Encoding encryption algorithm design

3.1 Predictive pattern dislocation encryption

The intra-frame chunking patterns and the inter-frame predictive structure cause a fixed pattern categorization in the encrypted information. The 4x4 intra-frame forecast component, for instance, has nine prediction options. Therefore, the encryption cannot be scrambled directly, otherwise, the encoding pattern will be illegal and cannot be decoded properly. In this paper, a pseudo-random sequence is generated by the STC system to scramble the prediction patterns of the INTRA_4x4 block. The STC system repeatedly generates the pseudo-random sequences, which improves the security of the encryption. The encryption process is as follows.

$$uRandSeq = Spa^{-}Chaos^{-}Generator(k'3)\ ;$$

$$Encrp\_Mode = Mode \oplus uRandSeq;$$

As previously examined, the inter-frame chunking manner predicts that the chunking mode inside the frame could be split into seven variable-sized block modes 16x8, 8x16, 16x16, 4x4, 8x4, and 8x8. There is a protected motion vector for each of these modes, and the total amount of motion vector values varies between blocks. To prevent the decoding errors caused by the scrambling of the block patterns, this paper does not directly encrypt the inter-frame block patterns, but adopts a scrambling swap method, by creating a 1-bit pseudo-random pattern containing zero, we may decide whether to jumble the two blocks patterns that have the same motion vector. Using an encryption control selection module, the method in this study selects to jumble the pseudo-random sequence produced by the STC system during the CAVLC encoding phase, while ensuring that the amount of data encrypted is as small as possible and the security of the encryption is as high as possible, without destroying the original encoding format. The security of the encryption is improved as much as possible while ensuring that the amount of data encrypted is as small as possible.

3.2 Residual data zigzag scanning sequence encryption

After the DCT transformation and quantization of the H.264 data encoding process, the energy of the residual data is mainly concentrated in the low-frequency and DC regions. After quantization, the coefficients of the low-frequency and DC components are mostly zero except for a small number of larger values. Therefore, to encode more efficiently, before entropy encoding, the residual coefficients can be zigzag scanned according to the statistical characteristics from high to low, to achieve better encoding efficiency.

In this paper, the zigzag scan of the residual data is scrambled to prevent the cryptographic scrambling from seriously damaging the characteristics of the DCT after coding, resulting in a significant reduction in the efficiency of entropy coding and compression. As shown in Figure 2, we choose to scramble the scanning direction of each diagonal line in the zigzag scanning process. The parity of the 1-bit frequency of the pseudo-random sequence produced by the spatio-temporal chaotic pseudo-random sequence generator is used to determine the read direction of each diagonal, thereby encrypting the zigzag scan sequence. Figure 3 shows the encryption method is illustrated.

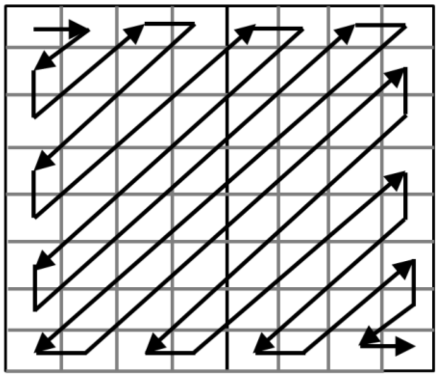

Figure 2: Zigzag saw tooth scan rule

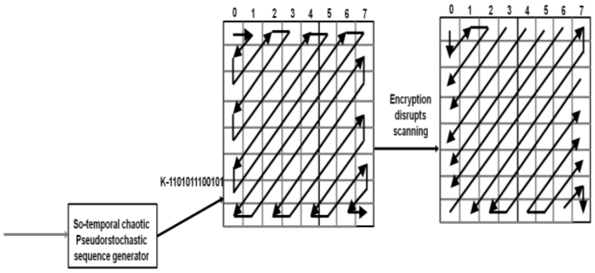
0
1
2
3
4
5
6
7
K-1101011100101
So-temporal chaotic Pseudorstochastic sequence generator
Encryption disrupts scanning
0
1
2
3
4
5
6
7

Figure 3: Zigzag data scanning scrambling process

In Figure 3, the 8x8 data block scan is used as an example. The scanning order of each diagonal data is determined by the parity of the sequence value of each 1bit, and when the read sequence value is 1, the scanning order of the corresponding diagonal data block is inverted to obtain the scrambled scanning order of the residual data. This ensures that the overall data scanning order is still from top-left to bottom-right, but disrupts the specific scanning order, and achieves encryption of the residual data with fewer operations and less impact on the compression efficiency.

3.3 CAVLC encoding process encryption

The several straggling coefficients in the CAVLC encoding process are between 0 and 3, so encryption of trailing coefficients requires at most 3 bits of pseudo-random sequence to heterodyning with the T1_Signs. The non-zero coefficients other than the trailing coefficients are divided into prefixes and suffixes, and the encoding process starts with the conversion of $levelCode = (level << 1) - 2 \ if \ \ level > 0$;

$levelCode = -(level << 1) - 1 \ if \ \ level < 0$;

$level\_prefix = levelCode/(1 << sufixLength)$

$level\_suffix = levelCode\%(1 << suffixLength)$;

If the level Code value is encrypted, the compression efficiency of the encoding may be seriously affected, and on the other hand, the encrypted data may not be legal and cannot be decrypted. Therefore, in this paper, the encryption operation is carried out for level _ prefix. Since the encoding is not directly encoding the amplitude value but encoding the value in the corresponding code table through the level _ prefix lookup table, the encryption of the non-zero coefficient amplitude value is achieved indirectly by scrambling the level _ prefix here, and the encryption process is as follows

$uRandSeq = Spa\_Chaos\_Generator(k, 4)$;

$Encrp\_level\_prefix = \ level\_prefix \oplus uRandSeq$;

4 A new approach to indoor security design and implementation of a networked robot remote monitoring system under chaotic algorithm

4.1 Overall design and functional design

The system is capable of implementing basic video data playback, video encryption, and decryption functions, video encoding and decoding functions, as well as video encapsulation and encryption-related performance testing functions in several parts.

4.1.1 Encryption security level selection module

If a video encryption system only provides a single encryption scheme, then the system may not be able to cope with the encryption needs of users with different needs. Some users do not want their video data to be encrypted too well, instead, they want to be able to encrypt only part of the effect, or even be able to see part of the original video information from the encrypted video data, for example, commercial video applications, businessmen in attracting users to buy For example, in commercial video applications, merchants want to entice users to buy video services by allowing them to see some of the information but not all of it, so that they can pay for it. Some users, on the other hand, do not care about the time and expense of encryption but want their video data encrypted as effectively and securely as possible, such as military, government, confidential commercial video conference data, etc. Consequently, to satisfy the various customers' expectations for video encryption, as a video encryption system is bound to provide a variety of security encryption schemes for users to choose from, the system designed in this paper provides three levels of encryption schemes according to the different levels of encryption security, namely primary, intermediate and advanced.

The primary encryption scheme uses an STC model with fixed local equations, which only encrypts the magnitude of non-zero coefficients of the residual coefficients and the sign bits of the trailing coefficients. This is generally suitable for video data with small motion information and low requirements for encryption effect; the intermediate encryption scheme uses the space-time chaotic model with fixed local equations and adopts a selective encryption control module. Based on the primary one, the scanning order of the residual coefficients is encrypted and the prediction pattern between frames is encrypted. It is generally suitable for video data with a large amount of motion information and also with certain requirements for encryption security. The advanced encryption scheme selects the STC model with dynamically changing local equations, introduces motion vector directional values and sign bit encryption based on the intermediate level, encrypts the sign bits of non-zero coefficients, and does dynamic encryption frame by frame. It is generally applicable to video data with very high-security requirements.

4.1.2 Key matching symmetric module

As the video encryption and decryption scheme in this paper is based on the H.264 encoding and decoding process, how to ensure the synchronization of the encrypted and decrypted data is a crucial point of the whole encryption scheme, if the decryption process cannot be synchronized with the encryption process, the correct decryption cannot be carried out. Since the H.264, the encoder has many time-spending calculation functions in the encoding process, these functions also perform encoding operations during the encoding process, but their main function is to budget the encoding overhead and does not perform encoding operations on the encoded data, while there are no such functions on the decoding side, so if the encryption is directly targeted at the encoding process, the decryption will not correspond to the encryption, so it is necessary to, Therefore, each encryption operation must be operated separately, i.e. the encryption process is only implemented in the real encoding operation on the encoding side, while the function for predicting the encoding overhead is left unchanged, to assure the encoded and decoded sides' encryption and decryption synchronization. The integration of advanced encryption and decryption techniques is achieved in indoor security through the use of chaotic encryption network robotic remote monitoring video technology. To protect video data both during transmission and preservation, the system uses chaotic encryption techniques. Increasing data security, these algorithms produce inconsistent patterns.

More computing resources may be needed for both encryption and decryption of stronger encryption techniques, which are generally weighed against computational complexity when determining effective security encryption. Selected encryption methods must balance resilience and controllable computing complexity in order to provide the greatest possible security. Users can observe real-time video feeds from their computers or smartphones by using remote monitoring. Interior conditions are well protected against potential security concerns by encryption, which makes sure that unauthorized persons cannot access or interfere with the video data. In the H.264 codec, the functions for the intra-frame prediction mode coding operation are

Write Syntax

*Element_Intra4x4Prediction Mode (Syntax Element*se, Data Partition *this_data Parr).*

Under normal circumstances, the function is called as shown in Figure 4. We can see from the diagram that three of the four calls are to functions with RDCOST, i.e. they all act as budget encoding overheads and do not involve specific encoding, so for the operation of intra-frame predictive mode encryption, these three calls need to be avoided, i.e. as shown in Figure 5.

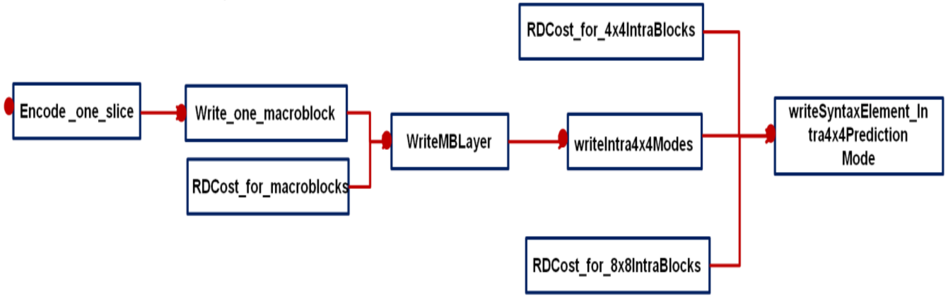
Encode_one_slice
Write_one_macroblock
RDCost_for_macroblocks
WriteMBLayer
RDCost_for_4x4IntraBlocks
writeIntra4x4Modes
RDCost_for_8x8IntraBlocks
writeSyntaxElement_Intra4x4Prediction Mode

Figure 4: The in-frame prediction mode encoding function is called

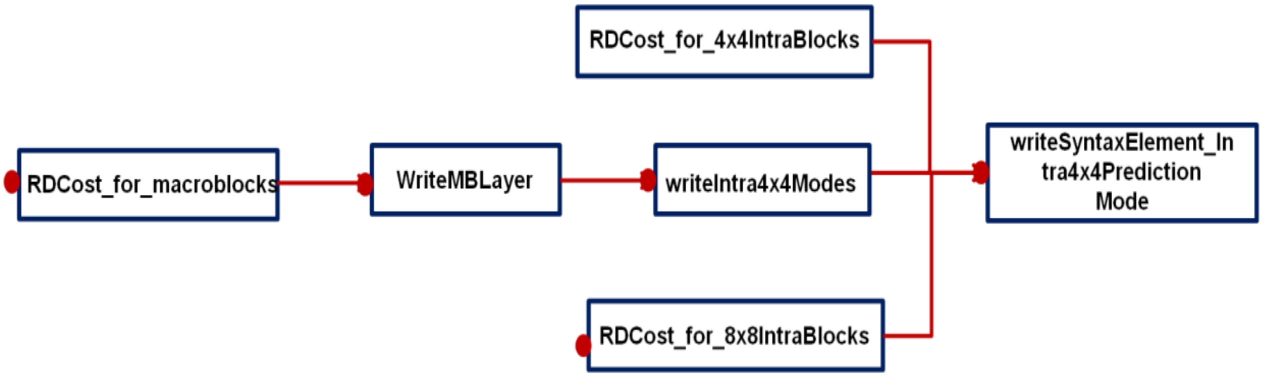
RDCost_for_4x4IntraBlocks
RDCost_for_macroblocks
WriteMBLayer
writeIntra4x4Modes
writeSyntaxElement_Intra4x4Prediction Mode
RDCost_for_8x8IntraBlocks

Figure 5: Budget coding attrition process calls the in-frame predictive mode coding process

4.2 Video encoding and encryption module design

First, the intra-frame prediction and motion vector difference dislocation encryption operation. In the scrambling process, since the performance of inter-frame chunking mode encryption is relatively not very high, so I discarded the operation of inter-frame chunking mode in the previous paper and only encrypted the intra-frame prediction mode in the prediction mode information encryption, meanwhile, to ensure the scrambling of inter-frame motion information, I chose to introduce motion vector values for encryption here.

In the inter-frame prediction mode, each chunk will have an MV to be encoded, assuming that the current chunking mode is 4x4, then 16 MVs are needed for encoding, and each MV contains both horizontal and vertical values, so it would take a lot of space to encode the MVs directly, so the H.264 encoding process makes use of the fact that the MVs between adjacent chunks have contextual relationships to the current chunk's Here, the actual MV values is deducted from its closest neighbouring block's MV value, and the remaining amount is seized, i.e. the motion vector difference value is encoded. Therefore, this chapter generates a 1-bit pseudo-random sequence to determine whether the horizontal and vertical components of the motion vector difference are to be encrypted interchangeably, as shown in the following equation.

```
uRandSeq = Spa_Chaos_Generator(k,1);
 if(uRandSeq)
{
temp=MVD-x;
MVD-x=MVD;
 MVD-y=temp;
}
```

where uRandSeq is the generated pseudo-random sequence; Spa _Chaos _ Generator is the spatio-temporal chaotic pseudo-random sequence generation system, k is the user key, and 1 represents the generation of a 1-bit length pseudo-random sequence.

temp is the temporary storage value, and MVD-x and MVD-y are the horizontal and vertical values of the motion vector difference, respectively. By encrypting the directional values of the motion vectors, the motion information appearing in the encrypted video is severely scrambled, which plays a very good encryption effect and security performance.

Secondly, encrypting the motion vector difference sign bits. In the previous section, this scheme encrypts the directional value of the motion vector difference, and to better disrupt the motion information in the encrypted video, the motion vector difference symbolic bit encryption operation is continued here. In the H.264 encoding process, the motion vector difference is used as a signed value for signed exponential Columbus encoding, in which a signed bit encryption operation can be performed for the write stream process, as shown in the following equation.

```
uRandSeq = Spa_Chaos_Generator(k,1);
Encrp_MVD_sign = MVD_sign uRandSeq;
```

where uRandSeq is the generated pseudo-random sequence; Spa _Chaos _ Generator is the spatio-temporal chaotic pseudo-random sequence generation system, k is the user key, and 1 represents the generation of a 1-bit length pseudo-random sequence. Encrp _ MVD _ sign is the sign bit of the current motion vector difference MVD after encryption, and MVD _ sign is the sign bit of the motion vector difference MVD before encryption. By encrypting the sign bits of the motion vector difference, the improved scheme has a more confusing encryption effect for motion information.

Thirdly, the CAVLC entropy coding encryption operation. The leftover block data's zigzag scanned sequence before to encoding remains mixed in the CAVLC entropy decoding procedure, and the sign bits of the trailing coefficients in the CAVLC process are also encrypted. This improvement improves the efficiency of the encryption scheme without reducing the quality of the encryption.

4.3 Implementation of the video surveillance module of the robotic encryption system with chaotic algorithms

Video surveillance assumes a very important responsibility in home security. The cost and risk of crime increase with video surveillance, which can theoretically lead to a reduction in the crime rate, and although it does not directly prevent criminal activity, it can provide a strong line of defense to deter crime and provide strong evidence. Moreover, even when traveling on business or on the way to work, you can inspect everything at home remotely at any time. The video surveillance module in this article consists of a gimbal and a motion camera. The gimbal uses a three-axis brushless head for aerial photography, which is stable and shake-proof, with a wide range of angle adjustments.

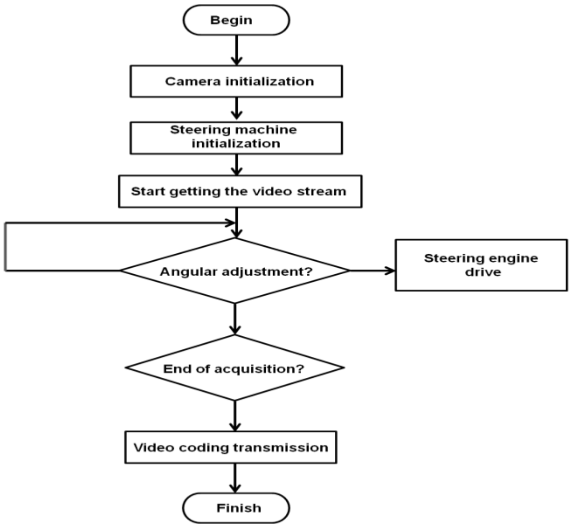

Figure 6: Video monitoring software flow chart

The sports camera has a high-resolution wide-angle lens with high resolution and a US2.0 direct plug interface for the output. The designed video surveillance program, when the video surveillance task is ready, first initialize the camera and rudder, after confirming that the camera and rudder are normal, start acquiring the video stream, during which the direction and angle of the video surveillance can be controlled by the rudder driver after the video acquisition task is finished, carry out video encoding transmission to complete the video surveillance task. The flow of the video monitoring software is shown in Figure 6.

4.4 Encryption algorithms

This investigation offers a chaotic encryption-based DES-improved security solution for interconnected robots in remote monitoring systems. The method provides strong data protection by combining chaotic encryption with DES. This strategy improves security dependability and security while providing an efficient and secure of remote environment monitoring. Chaotic encryption provides unpredictability to the network, increasing security, whereas RSA encryption is used for secure transmission of information in interior domains. This combination encryption strategy is used by robots that are outfitted with remote monitoring video technology to protect critical data and guarantee the integrity of video updates, therefore strengthening protections against any intrusions. Figure 7 shows the outcome of the RSA and DES.

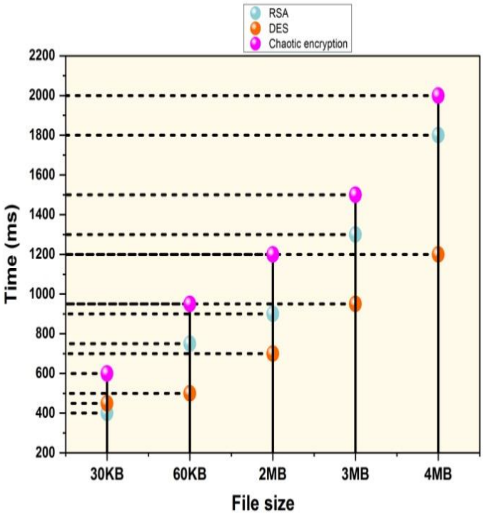

Figure 7: Outcome of the RSA and DES

4.5 Sensitivity

Sensitive information is protected by security encryption, which encrypts it to thwart illegal access or interception. This protective mechanism maintains the security and privacy of sensitive data in a variety of situations by preventing from possible dangers, such as hackers, unauthorized users, or hostile entities. AlexNet [22] scored 0.64 %, VggNet [22] scored 0.79%, and GoogLeNet [22] scored 0.24%, the proposed approach Chaotic encryption has the greatest sensitivity level of 0.92%. Figure 8 shows the outcome of sensitivity.

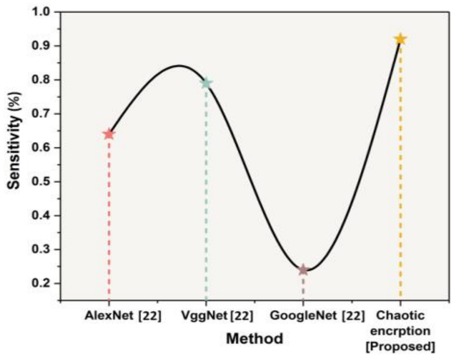

Figure 8: Outcome of sensitivity

4.6 Discussion

The comparatively small 56-bit key length of the DES is one of its drawbacks. This key length is susceptible to brute force assaults in the modern computer environment, in which an attacker continuously tries every potential key before the right one is discovered. These kinds of assaults are doable in a fair amount of time given the capabilities of current processors. Furthermore, improved algorithms for encryption such as providing longer key lengths and greater cryptographic features, have eclipsed DES. For this reason, in settings where higher encryption requirements are necessary, DES is seen as being less appropriate for protecting sensitive data. The processing complexity of RSA encryption is one of its drawbacks, especially when using large key sizes. Since RSA depends on intricate mathematical processes such as modular exponentiation, it can be resource-intensive, particularly on appliances with minimal computing power or in situations where encryption and decryption are required instantly. Performance and usability can be negatively impacted by difficult key handling, especially with greater key sizes. Moreover, perfect forward secrecy is not provided by RSA, which means that previous communications can be decrypted if a private key is compromised. Consequently, while using RSA, trade-offs between performance, security, and key management must be carefully considered. Sensitivity analysis has a few disadvantages, including the potential for conclusions to be unclear due to their dependence on assumptions. Furthermore, inadequate or false insights into the robustness of a model or selection can result from sensitivity analysis's inability to appropriately capture all plausible sources of variability or interactions among variables. A suggested technique that makes use of chaotic encryption can improve security by overcoming the shortcomings of conventional encryption techniques like DES and RSA. By introducing unpredictability through chaotic systems, chaotic encryption reduces the viability of brute force assaults. This technique overcomes the drawbacks of conventional encryption algorithms and increases security against contemporary threats while increasing encryption efficiency.

5 Conclusion

In summary, based on the previous work, this paper designs a complex STC model to construct a pseudo-random sequence suitable for video encryption, thereby improving the resistance to attack of this random sequence and thus the resistance to attack of the whole video encryption algorithm. Based on the encryption algorithm of H.264 codec standard, the encryption scheme is designed under the requirement of ensuring the encryption efficiency and real-time performance, and the encrypted data and location with better encryption effect and less impact on the compression performance and higher real-time performance are selected through multiple sets of experiments, to improve the real-time performance and operability of the encryption algorithm as much as possible while ensuring high enough security and less impact on the compression performance. The encryption algorithm is designed to ensure high enough security while maximizing the encryption algorithms operability and real-time performance, with the least amount of influence on compression efficiency. Using the H.264 codec standards as a foundation, a more workable video encryption system is created. Based on the above, the scheme is implemented in the codec platform, and provides different encryption options with different security levels and different encryption performance according to the different encryption requirements, to better provide different encryption methods for different scenarios.

Data availability

The data used to support the findings of this study are included in the article.

Conflicts of interest

The authors declare no conflicts of interest.

Funding statement

This research study is sponsored by the Chongqing Natural Science Foundation Project. The name of the project is Research on Chaos-Based Video Encryption Technology for Remote Surveillance. The project number is CSTB2022NSCQ-MSX1510. Thank the project for supporting this article!

References

[1] Fotovvat, Amir. Selective Encryption of Video Data for IoT Environments. PhD diss., University of Saskatchewan, 2021.

[2] Noura, Mohamad. Efficient and secure cryptographic solutions for medical data. PhD diss., Université Bourgogne Franche-Comté, 2019.

[3] Tolba, Zakaria. Cryptanalysis and improvement of multimodal data encryption by the machine-learning-based system. arXiv preprint arXiv, 2024, 2402.15779.

[4] Ahmad, Rami, Raniyah Wazirali, and Tarik Abu-Ain. 2022, Machine learning for wireless sensor networks security: An overview of challenges and issues. Sensors, 22, no. 13: 4730. https://doi.org/10.3390/s22134730

[5] Williams Phillip, Indira Kaylan Dutta, Hisham Daoud, and Magdy Bayoumi. 2022, A survey on security in the Internet of Things with a focus on the impact of emerging technologies. Internet of Things, 19: 100564. https://doi.org/10.1016/j.iot.2022.100564

[6] Quinga-Socasi, Francisco, Luis Zhinin-Vera, and Oscar Chang. A deep learning approach for symmetric-key cryptography system. In Proceedings of the Future Technologies Conference, 2020, pp. 539-552. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-63128-4_41

[7] Radwan, Ahmed Salem. Security of IoT Systems: AES and Cellular Automata, 2022.

[8] Banerjee, Jyoti Sekhar, Siddhartha Bhattacharyya, Ahmed J. Obaid, and Wei-Chang Yeh, eds. 2022, Intelligent Cyber-Physical Systems Security for Industry 4.0: Applications, Challenges and Management, CRC Press. https://doi.org/10.1201/9781003241348

[9] Ramya, P. Sai, and Durgesh Nandan. Analysis of security issues and possible solutions in the Internet of things for home automation system. In Soft Computing: Theories and Applications: Proceedings of SoCTA, 2019, pp. 825-836. Springer Singapore. https://doi.org/10.1007/978-981-15-4032-5_74

[10] Fkirin, Alaa, Gamal Attiya, and Ayman El-Sayed. 2021. Two-level security approach combining watermarking and encryption for securing critical colored images. Optical and Quantum Electronics, 53, no. 6: 285. https://doi.org/10.1007/s11082-021-02875-2

[11] Liu, Beisheng, Xiaodong Li, Haoyang Yu, and Jianwen Lv. A light chaotic encryption algorithm for real-time video encryption. In 4th EAI International Conference on Robotic Sensor Networks, 2022, pp. 111-118. Springer International Publishing. https://doi.org/10.1007/978-3-030-70451-3_10

[12] Antonijevic, Milos, Ivana Strumberger, Sasa Lazarevic, Nebojsa Bacanin, Djordje Mladenovic, and Dijana Jovanovic. 2022, Robust encrypted face recognition robot based on bit slicing and Fourier transform for cloud environments. Journal of Electronic Imaging, 31, no. 6: 061808-061808. https://doi.org/10.1117/1.jei.31.6.061808

[13] Yu, Xiaojie, Qiao Hu, Dan Xu, Xingju Xie, and Yaohui Liu. 2021, multi-channel monitoring data compression method for industrial robot based on compressed sensing. Measurement Science and Technology, 33, no. 1: 014007. https://doi.org/10.1088/1361-6501/ac329c

[14] Kiran, Harun Emre, Akif Akgul, Oktay Yildiz, and Emre Deniz. 2023, Lightweight encryption mechanism with discrete-time chaotic maps for Internet of Robotic Things. Integration, 93: 102047. https://doi.org/10.1016/j.vlsi.2023.06.001

[15] Wen, Heping, Zhiyu Xie, Zhuxi Wu, Yiting Lin, and Wei Feng. 2024, Exploring the future application of UAVs: face image privacy protection scheme based on chaos and DNA cryptography. Journal of King Saud University-Computer and Information Sciences, 36, no. 1: 101871. https://doi.org/10.1016/j.jksuci.2023.101871

[16] Yang, Jian, and Liu Sun. 2022, A Comprehensive Survey of Security Issues of Smart Home System: Spear and Shields, Theory and Practice. IEEE Access, 10: 124167-124192. https://doi.org/10.1109/access.2022.3224806

[17] Kumar, Chandan, and Shailendra Singh. 2024, Security standards for real time video surveillance and moving object tracking challenges, limitations, and future: a case study. Multimedia Tools and Applications, 83, no. 10: 30113-30144. https://doi.org/10.1007/s11042-023-16629-7

[18] Sharma, Sanjeev, Tarun Kumar, Ravi Dhaundiyal, Amit Kumar Mishra, Nitin Duklan, and Ashish Maithani. 2019, Improved method for image security based on chaotic-shuffle and chaotic-diffusion algorithms. International Journal of Electrical & Computer Engineering, (2088-8708) 9, no. 1. https://doi.org/10.11591/ijece.v9i1.pp273-280

[19] Masood, Fawad, Junaid Masood, Lejun Zhang, Sajjad Shaukat Jamal, Wadii Boulila, Sadaqat Ur Rehman, Fadia Ali Khan, and Jawad Ahmad. 2022, A new color image encryption technique using DNA computing and Chaos-based substitution box. Soft Computing,1-17.

[20] Radhi, Batool M., and Mohammed A. Hussain. 2023, Smart Building Security using ESP32 based AES One Bio-key and Owner's Biometrics Encryption Technology. J. Basrah Res. (Sci.), 49, no. 2: 30-47. https://doi.org/10.56714/bjrs.49.2.4

[21] Kunhoth, Jayakanth, Nandhini Subramanian, Somaya Al-Maadeed, and Ahmed Bouridane., 2023. Video steganography: recent advances and challenges. Multimedia Tools and Applications, , 82, no. 27: 41943-41985. https://doi.org/10.1007/s11042-023-14844-w

[22] Lee, Min-Fan Ricky, and Zhih-Shun Shih. 2022, Autonomous surveillance for an indoor security robot. Processes, 10, no. 11: 2175.https://doi.org/10.3390/pr10112175