



# Application of CSK Encryption Algorithm in Video Synergic Command Systems

Lele Qin, School of Economics and Management, Hebei University of Science and Technology, Shijiazhuang, China

 <https://orcid.org/0000-0003-3222-6453>

Guojuan Zhang, Department of Industrial Basic Education, Hebei College of Industry and Technology, Shijiazhuang, China

Li You, Department of Economics and Trade, Hebei College of Industry and Technology, Shijiazhuang, China

 <https://orcid.org/0000-0002-7186-0142>

## ABSTRACT

Video command and dispatch systems have become essential communication safeguard measures in circumstances of emergency rescue, epidemic prevention, and control command as data security has become especially important. After meeting the requirements of voice and video dispatch, this paper proposes an end-to-end encryption method of multimedia information that introduces a multiple protection mechanism including selective encryption and selective integrity protection. The method has a network access authentication and service encryption workflow, which implants startup authentication and key distribution into the information control signaling procedure. This method constitutes a key pool with the three-dimensional Lorenz system, the four-dimensional cellular neural network (CNN) system, and the four-dimensional Chen system where the key source system and initial conditions are decided by the plaintext video frame itself. Then, this method optimizes the chaotic sequences to further enhance system security.

## KEYWORDS

Chaos Algorithm, Encryption and Decryption, Key Distribution, Synergic Commands, Video Conferencing, Video Encryption, Video Security, Video Synergic Command System, Video Systems

## 1. INTRODUCTION

As a kind of real-time communication system relying on image and voice communication, video systems enable geographically dispersed users to gather in one virtual conferencing space as the various information exchange modes through image and voice enable real and visualized exchange of cooperating members, and facilitate participant understanding of conference content (Yang et al., 2014). At present, video systems have been gradually developing in the directions of multi-network cooperation, high definition quality, development and intelligence. Video synergic command and dispatch systems can be deployed in public networks or private networks, and are broadly applied in cities' emergency responses, environmental protection, safety supervision, digital city management, public security, electric power and other industries. Particularly for public security and emergency management departments, video command and dispatch systems have become essential communication safeguard measures for large-scale security activities and emergency rescue. Especially in the prevention and control of COVID-19 outbreak in the beginning of 2020, video synergic command

DOI: 10.4018/JOEUC.20220301.oa1

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

systems played a crucial role in areas of teleconference, rescue command, video monitoring command, telemedicine and enterprise work resumption. In the application of video systems, video content may concern state secrets, military intelligence, business secrets and private information. Any leakage of such sensitive information will lead to huge safety risks. Therefore, this paper extracts cryptographic demands from typical video conferencing systems and designs a video conferencing encryption scheme using research in combination with commercial cryptographic algorithm, and by taking full advantage of chaos algorithm. This is done to guarantee the information data security, ensure the sustainable development and secure application of video conferencing. This paper proposes an end-to-end encryption scheme for multimedia information in video synergic command systems which studies, combines and designs technologies such as user authentication, end-to-end information encryption protocol, and chaotic encryption algorithm. This implements the video synergic command system and meets various personalized user demands for multimedia information encryption.

### 1.1. Research Status

Video encryption technology appeared contemporarily with the rise of the Internet, both in the 1970s, and has undergone changes from analog signal to digital signal. At the beginning of the 1990s, with the establishment of video coding standards, new video encryption algorithms were continuously proposed, but only concerning the encryption of videos without considering the relation between coding and encryption. There were two encryption methods. In the first method, original videos were processed through traditional cryptographic encryption methods before coding, i.e. substituting and disturbing the pixels of videos. The other method was also called the complete encryption algorithm, which encrypted the code stream after coding and adopted a typical encryption algorithm for its high encryption efficiency. This was deemed as having low research value because of the abnormal decoding due to the change of video format after encryption. Then these two methods, were followed by entropy coding based encryption algorithm, which fused the encryption process into the entropy coding process resulting in preferable encryption results, and high encryption and decryption efficiency (Spanos et al., 1995; Shi et al., 2006). From the beginning of the 21st century, various video encryption algorithms began to attract the attention of researchers gradually and more and more technical proposals followed. Cao brought up the video encryption algorithm using discrete cosine transform coefficient, but it had unsatisfactory encryption results because it encrypted only one type of data (Cao et al., 2005). In 1963, Antonio presented a chaotic system and applied the system in video encryption (Antonio et al., 2015). He proposed a model using the three-dimensional Lorenz Chaos to avoid the complexity in solving high-dimensional chaos (He et al., 2013). However, it was inadequate for real-time transmission when combined with coding. Tian put forward a RC4 hyperchaotic video encryption algorithm that generated four pseudorandom sequences through four-dimensional hyper chaotic mapping to work respectively as the seed keys of RC4 algorithm (Tian et al., 2015). The purpose is to realize the joint encryption of Direct Coefficient (DC), Motion Vector Difference (MVD) symbol and non-zero Alternate Coefficient (AC) symbol. This algorithm featured big key space, strong key sensitivity and high security. The above literature all sought to achieve a sound balance between the efficiency and security of video encryption. Liu et al. came up with a puzzle algorithm that first separated the code stream into blocks, scrambled the blocks and then encrypted them respectively by key streams produced through AES-CTR (Liu et al., 2015). This algorithm was applicable in multimedia P2P video conferencing systems. Traditional encryption methods are primarily mathematical methods requiring costly equipment, and don't fit the document coding structure and mass data characteristic of video information. Chaotic encryption methods are mainly physical methods utilizing the chaotic features of chaotic systems and requiring low-cost equipment. Chen discovered the Chen System in 1999 and applied the four-dimensional hyper chaotic mathematical model (Guan et al., 2015). Chua and Yang were first to establish the Cellular Neural Network (CNN), in 1988, and utilized the four-dimensional CNN hyper chaotic system (Qi et al., 2013; Duan et al., 2014). An ideal chaotic random sequence should have certain characteristics

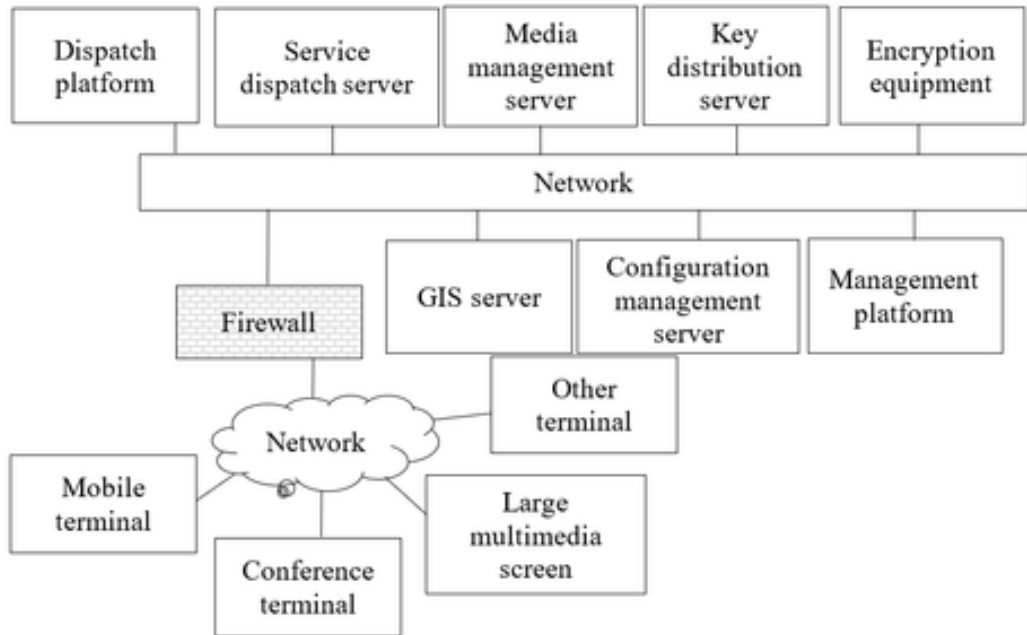
such as balanced distribution, good auto correlation, and should have the cross correlation closer to zero. Some literature mentioned encrypting and decrypting videos by adopting the one-dimensional Logistic System, the three-dimensional Lorenz System and the four-dimensional Chen System as the key source where, despite the favorable encryption result, the chaotic sequences generated were not optimized and the encryption process was not integrated into the information control instruction flow. This in turn degraded the execution efficiency(Ye et al., 2014; He et al.,2013; Chai et al., 2014; Sanpei et al., 2016). Valli et al. proposed a twelve-dimensional chaotic mapping, introduced Lkeda delay differential equation, and designed a substitution box to substitute the pixels of plain text videos(Valli et al., 2017). Such encryption scheme showed strong robustness in resisting statistical attack. Considering the increasingly growing pixel amount of monitoring videos at present, Wang et al. introduced hyper chaotic systems into the coding system, and realized the single-channel encryption of images to guarantee the video encryption efficiency and security(Wang et al., 2017). Zhu et al. designed the selection scheme for various hyper chaotic systems, optimized the chaotic sequences and increased the randomness of sequences(Zhu et al., 2016). Yang et al. applied multiple chaotic mappings and Advanced Encryption Standard (AES) algorithm to encrypt the RGB pixel value of videos respectively to enhance video information safety(Yang et al., 2016). Zhu et al. introduced keys generated from CNN to realize fast encryption of video information with high security(Zhu,2016). In spite of the numerous distinctive encryption methods and algorithms proposed so far, video command systems require not only encryption algorithms but also the combination of management theories, user authentication methods, end-to-end information encryption protocols, hyper chaotic encryption algorithms, and other technologies in order to give play to synergic video command systems. Therefore, based on synergy theories, this paper analyzes the status quo of video systems, sets forth the audio and video encryption demand and command demand of video systems. Then this paper designs a multiple defended, safely extensible and intelligent encryption scheme based on the controllable commercial cryptographic algorithm and various chaotic encryption technologies. The goal of this encryption scheme is to solve the problems in video command systems.

## 1.2. Composition of Video Synergic Command Systems

The composition and deployment of video synergic command systems are shown in Figure 1.

Video synergic command and dispatch systems are mainly composed of the command and dispatch service platform (the service dispatch server, the key distribution server, the encryption equipment, etc.) and client devices (mobile terminals, large multimedia screens, conference terminals, etc.) (Li et al., 2017; Mashamba-Thompson et al., 2020; Qin et al., 2016; Qin et al., 2018; Qian et al., 2020; SATTAR et al., 2016). The service dispatch server enables user registration, service dispatch and GIS subscription as well as track drawing and position trailing when combined with GIS server. As for the unified media server, it enables audio and video access, audio and video re-transmission, video calling, video conferencing, storage and short messages. The GIS server provides GIS service. The key distributor on this platform communicates with the service dispatch server through a network interface to enable the initialization, power-on self-test (POST), distribution, alteration, and destruction of cryptograms and online equipment management of cryptographic equipments such as the encryption equipment on the dispatch platform, terminal dongles and terminal software cryptographic modules. As a standalone equipment deployed on the command service platform, the encryption equipment communicates with the dispatch platform through the network interface to support concurrent access of multiple dispatch conditions, and to realize encryption of dispatch platform side audio and video communication service as well as the integration of chaos algorithms. Next, the configuration management server mainly enables the configuration management of the system including staff management, authority management and log management. As for the command seat operation terminal, the dispatch platform provides the command operation interface for users to conduct user management, command and dispatch, video conference initiation, GIS subscription, short message sending and other operations. Terminal dongles and terminal software cryptographic

Figure 1. Composition & Application Deployment of Video Synergic Command System



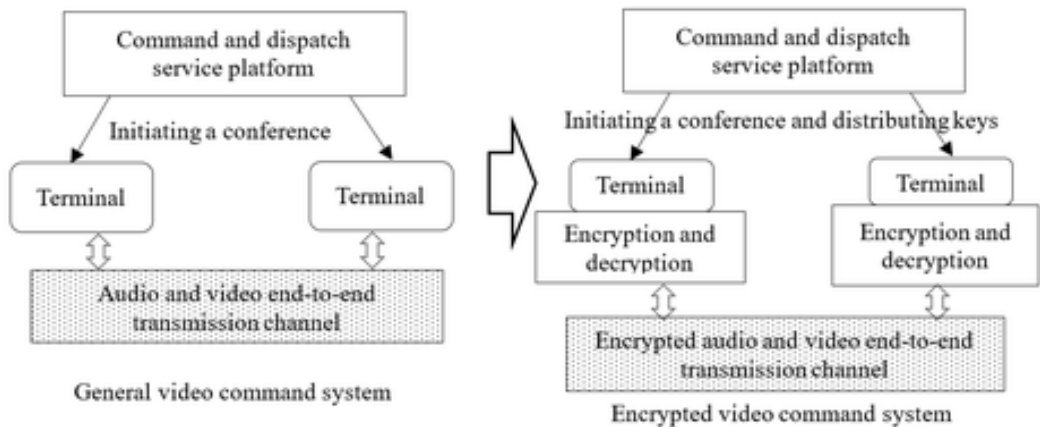
modules are deployed in mobile terminals, large multimedia screens, and conference terminals. They are invoked by mobile terminals through interfaces to enable the encryption of mobile terminal side audio and video communication service (Tian et al., 2014; Cao et al., 1999; Li et al., 2019; Hu et al., 2006; Mian et al., 2007; Yin et al., 2019; Yan et al., 2020). As public network based intelligent communication terminals, mobile terminals install dedicated video command and dispatch APP to enable video backhaul, audio and video calling, audio and video conferencing, instant short messaging, and GIS reporting functions of terminal equipment.

## 2. APPLICATION OF VIDEO ENCRYPTION TECHNOLOGY

### 2.1. Overall Framework

In traditional video conferencing or video command systems, a platform client controls the command and dispatch platform to initiate a conferencing or video request, and then the conferencing terminal gathers local audios and videos and sends them to other terminals under the dispatch of command platform. Comparatively in encrypted video command systems, the platform distributes keys to terminals simultaneously when it initiates video conferences. Each terminal encrypts locally gathered audios and videos and transmits them to equipment at the other end. Then the encrypted audios and videos are decrypted and played by the receiving end as shown in Figure 2 (Wang, 2015; Lai, 2017; Yao et al., 2020; Zhang et al., 2020). In encrypted video command systems, terminals are equipped with cryptographic management facilities such as dongles and cryptogram software modules, which cooperate with the key distribution sever and encryption equipment to enable encryption and decryption, key and certificate storage, and other security capabilities of terminals. The encryption equipment and the key distribution server deployed on the platform enable cryptogram operation, key life cycle management, certificate life cycle management, and other functions alike. Refer to Figure 1 for details.

Figure 2. Encrypted Video Command System Framework



## 2.2. Cryptographic Key Configuration Design

Video command systems adopt SM2/3/4 commercial cryptographic algorithms where SM2 algorithm is used for signature verification and symmetric key encryption protection. SM3 algorithm is used for integrity protection, and SM4 algorithm is used for encryption protection of audio and video data. The system adopts two kinds of certificates (encryption certificate and signature certificate) and three layers of keys. The key flow of encrypted video conferencing is shown in Figure 3. The cryptogram management cluster distributes conference keys to participant terminals and all participant terminals share the same conference key. The participant terminal that sends videos will generate the session key and send it to the receiving end under encryption protection of conference keys. The sending end and receiving end share the same session key, and conduct end-to-end encryption and decryption based on the session key.

## 2.3. Encryption Design

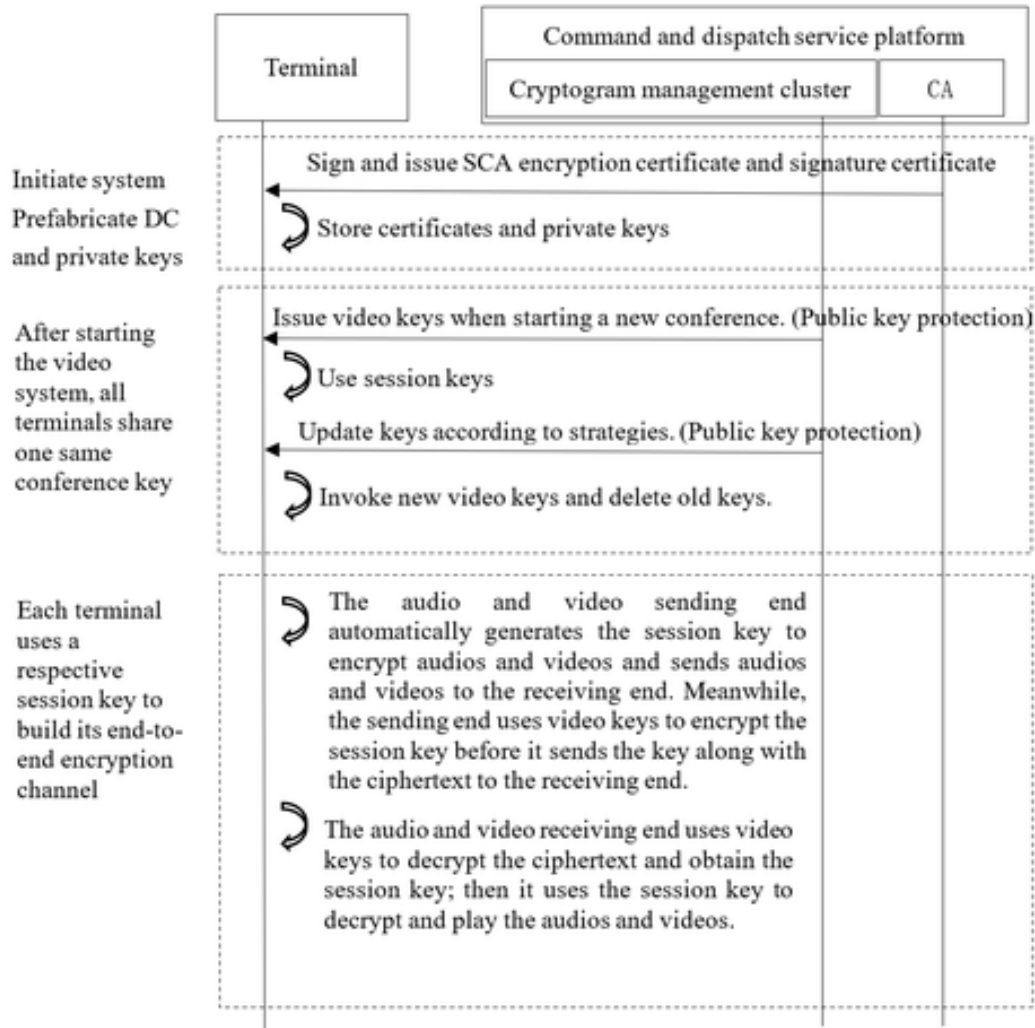
The overall framework of audio and video processing of the sending end and receiving end is shown in Figure 4, which shows that the scheme adopts three layers of protection: confusing scrambling, selective encryption and selective integrity protection. Confusing scrambling employs chaos algorithms and chooses one algorithm from the key pool. The key source and initial conditions are decided by the plaintext itself. The platform will update the key before each video transmission and distribute the key to participant terminals in order to generate more disordered code stream, and increase the difficulty in analyzing and cracking the code stream. Selective encryption provides different levels of encryption strength to protect the confidentiality of audio and video data. Selective integrity protection executes integrity protection on a portion of audios and videos as needed to prevent illegal tampering and destruction. The design of the three-layer protection greatly enhances the security of the system.

## 3. REALIZATION AND PROCESS OF ENCRYPTION TECHNOLOGY

### 3.1. Network Access Authentication after Startup and its Process

After startup, the client and the key distribution center on the platform need to conduct a two-way network access authentication to authenticate the identity, authority and cryptogram of user network access, and to download relevant parameters. The encryption equipments (including the encryption equipment and key distribution server) provide subsequent encryption service after network access

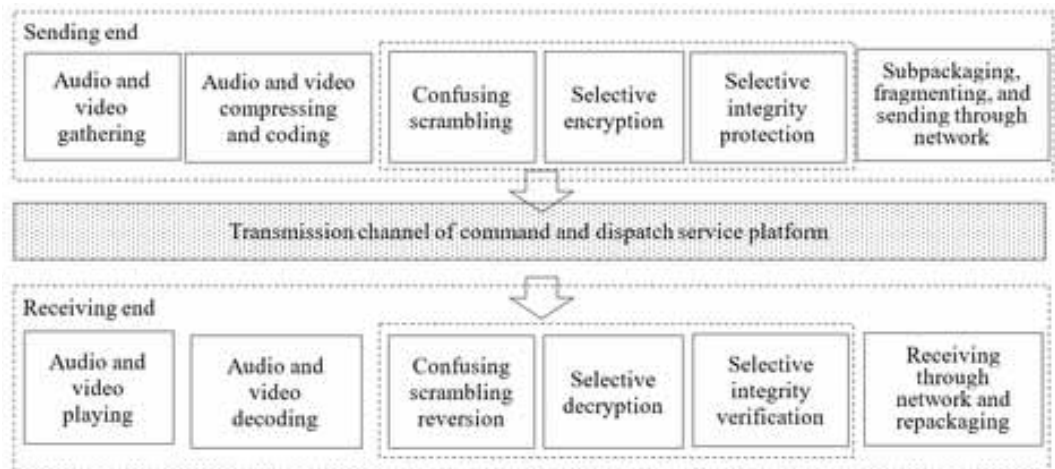
Figure 3. Key Distribution and Management Process Design



authentication. The authentication messages of the encryption equipment and the key distribution server are transmitted by the command and dispatch service platform through control plane information channel instructions, as shown in Figure 5. The process includes:

- (1) The terminal and the platform start up send log-in message and log-in application to the encryption equipment
- (2) The encryption equipment responds to the log-in, verifies user validity and sends successful log-in message through the backward terminal and the platform
- (3) The terminal and the platform send authentication processing message to the encryption equipment to confirm authority
- (4) The encryption equipment generates an authentication request, which goes through the terminal and the dispatch server before the service dispatch server retransmits it to the key distribution center for further processing

Figure 4. Overall Framework of Sending End-to-Receiving-End Encryption



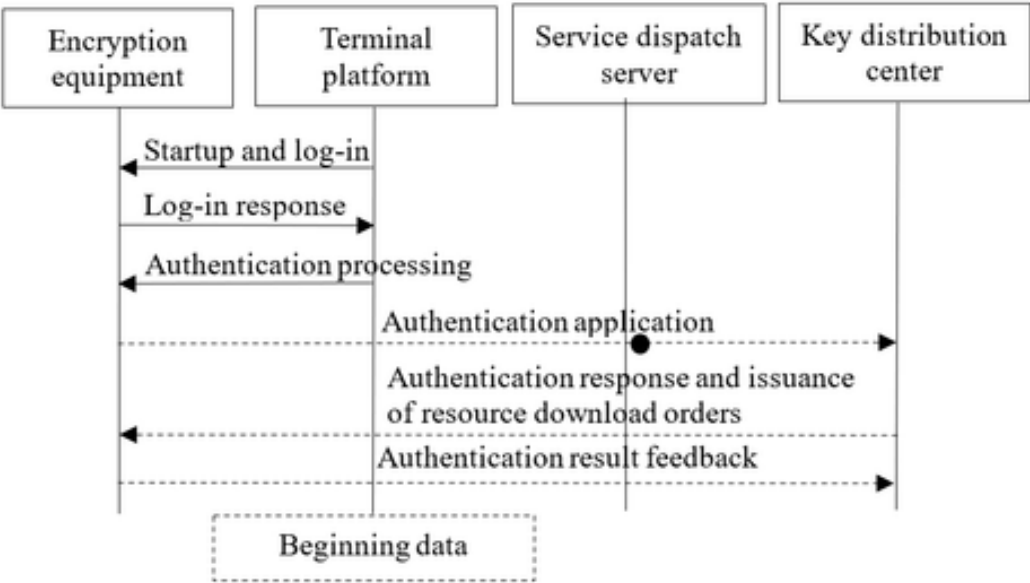
- (5) The key distribution center responds to the authentication application and issues resource download orders
- (6) The encryption equipment confirms the authentication, acquires relevant cryptographic resources and feeds it back to the key distribution center with authentication results
- (7) The terminal and the platform start data transmission

### 3.2. Realization and Process of Encrypted Video Conferencing

In video conferencing, all terminals entering the conference acquire a conference communication key through the key distribution center as shown in Figure 6. The specific process is:

- (1) The initiator initiates a video conferencing instruction, chooses and calls more than one member as the objects of the conference, and submits relevant applications to the service dispatch platform at the same time (or terminals can voluntarily enter the conference with a password)
- (2) The service dispatch platform creates the conference, and then participants get the conference communication key through the key distribution center after log-in. Keys are transmitted through dedicated communication channels
- (3) Participants feed back to the key distribution center after getting their keys
- (4) Terminal users start to gather local videos, conduct audio and video coding, then compress, encrypt, and transmit relevant data to the media server that conducts encrypted storage of audio and video data
- (5) New participants need to be authenticated, get a conference key through the key distribution center, give feedback, and then enter the conference after the service dispatch platform updates their enrollment information
- (6) New members start to gather data as in step (4)
- (7) After receiving audio and video information, video conferencing participants play audios and videos after completing decompression, decryption and decoding

Figure 5. Network Access Authentication Flow after Startup



### 3.3. Realization of Encrypted Video Calling

In video calling, both parties acquire keys online through the key distribution center as shown in Figure 7. The specific process is:

- (1) The initiator chooses a called terminal and submits video calling request to the service dispatch platform
- (2) The service dispatch platform and the called terminal receive the request at the same time
- (3) The called terminal feeds back and the service dispatch platform successfully creates a temporary video call
- (4) The key distribution center distributes keys to both parties through dedicated channels
- (5) Both parties gather audio and video data and transmit data to the media server after coding, compressing and encryption
- (6) The media server executes encrypted storage of files received from terminals and transmits data to both terminals
- (7) Both terminal parties decrypt, decode and play the audios and videos

The encryption workflow of GIS reporting is the same as above where the mobile terminal encrypts GIS information, and reports to the dispatch platform side in the form of short messages. Then the dispatch platform decrypts the information and obtains the plaintext of GIS information.

## 4. APPLICATION OF CSK ENCRYPTION ALGORITHM IN VIDEO SYNERGIC COMMAND SYSTEMS

The combined utilization of public keys and private keys basically realizes user identification and authority control; however, video data need to be encrypted to further enhance video transmission



Figure 6. Encrypted Video Conferencing Workflow

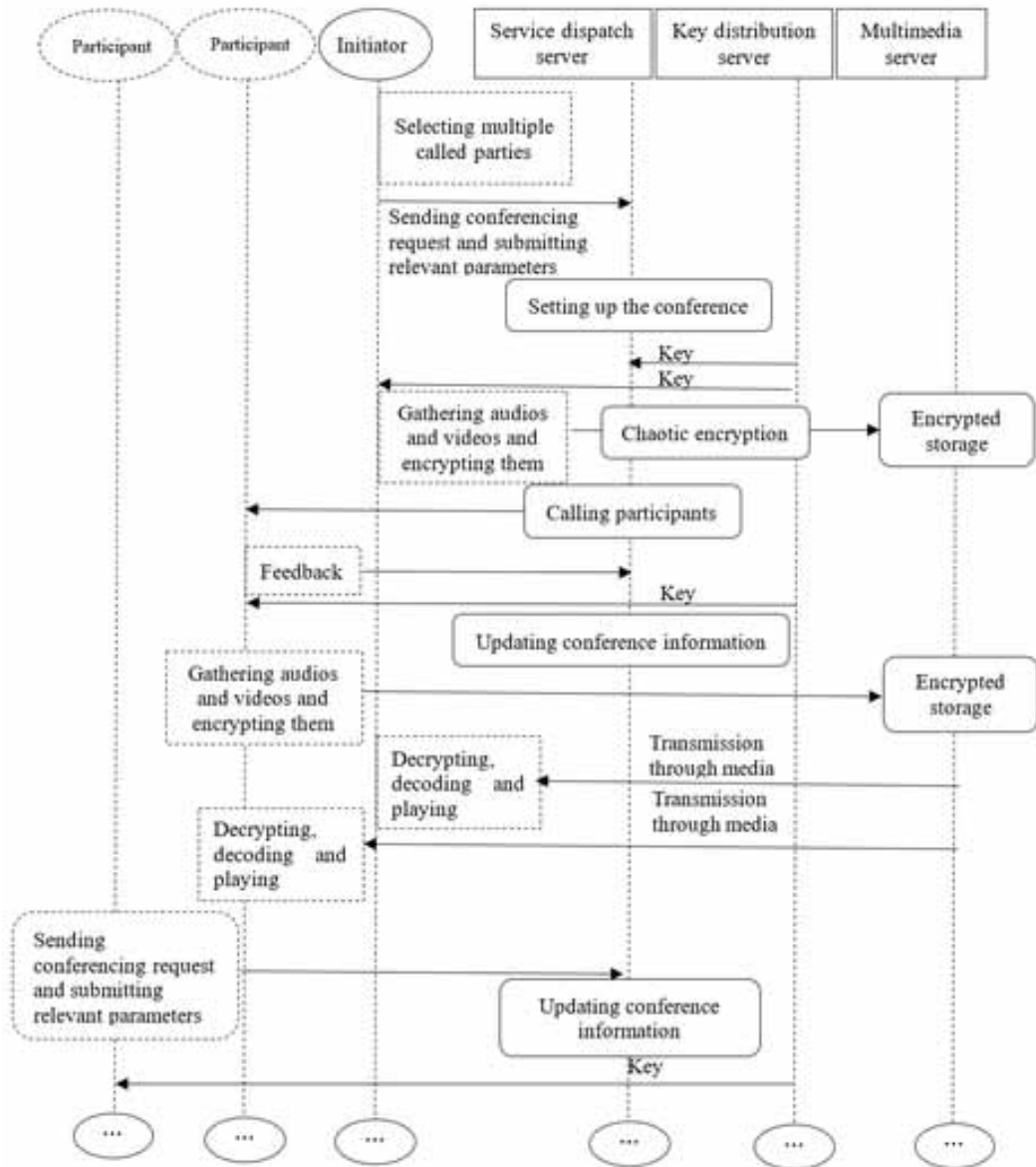
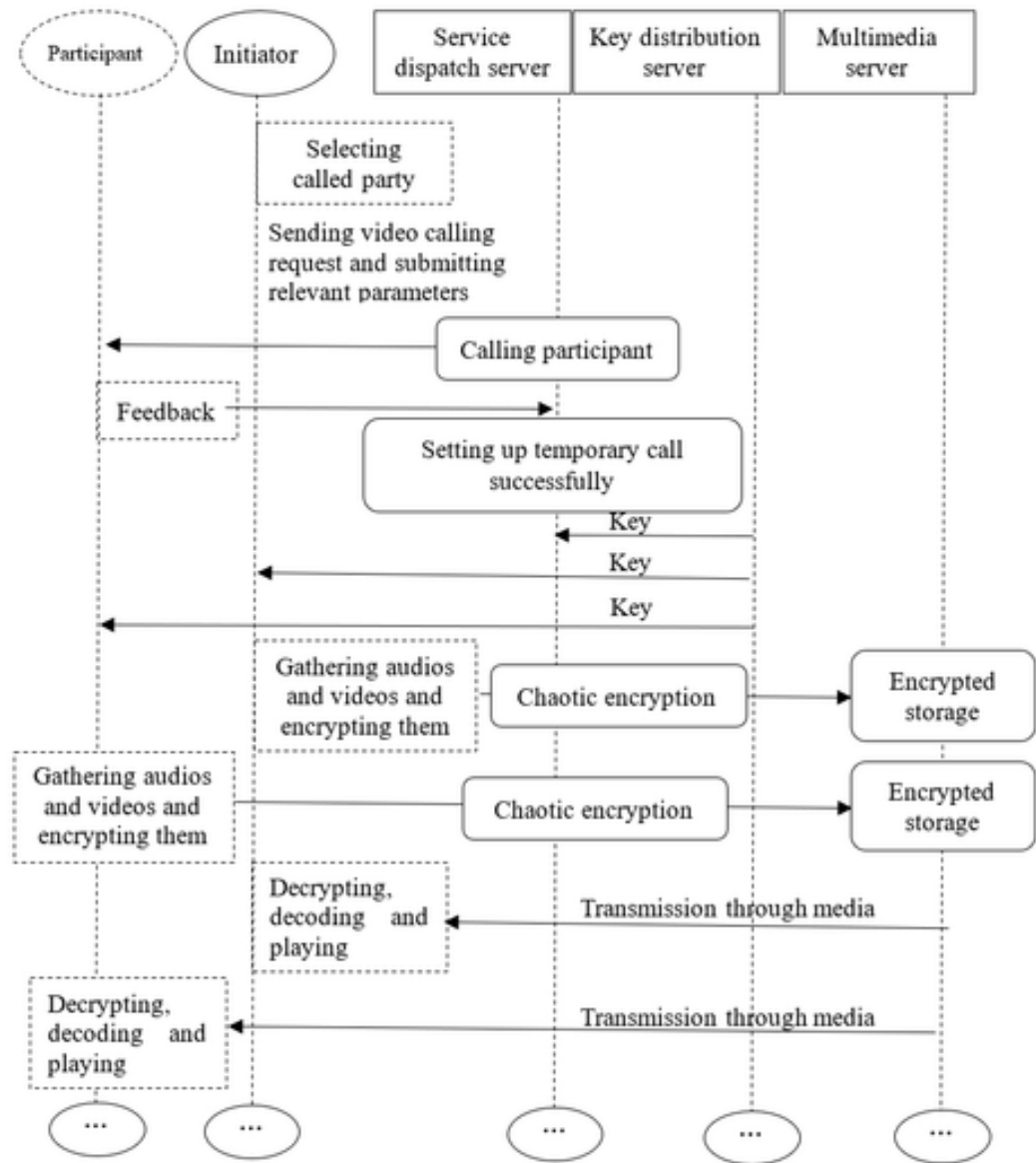


Figure 7. Encrypted Temporary Video Calling Workflow



security. Here CSK encryption algorithm is adopted with reference to the model of Zhu(Zhu et al.,2017).

The first step is to adopt the three-dimensional Lorenz System, the four-dimensional CNN System and the four-dimensional Chen System to constitute the key pool. The key source chaotic system is selected according to Formula (1) as shown below:

Table 1. System Selection Table

Source1	System Selected	$x_n$ Value
1	Lorenz	$x_1(0), x_2(0), x_3(0)$ as the original value
2	Chen	$x_1(0), x_2(0), x_3(0), x_4(0)$ as the original value
3	CNN	$x_1(0), x_2(0), x_3(0), x_4(0)$ as the original value

$$\begin{cases}
 MxWor = Red \odot Blue \odot Green \\
 Source1 = (MwXor \bmod 3) + 1 \\
 Source2 = \begin{cases} (Source1 \bmod 3) + 1 (source1 = 1) \\ (Source1 \bmod 4) + 1 (source1 \neq 1) \end{cases} \\
 Source3 = \begin{cases} Source2 \bmod 3 + 1 (source1 = 1) \\ (Source2 \bmod 4) + 1 (source1 \neq 1) \end{cases}
 \end{cases} \quad (1)$$

$\odot$ -Xor operation mod-taking remainder

where Red, Blue and Green are the respective Xor values of red component, blue component and green component of all pixels of the plaintext video frame. Formula (2) generates the original value of the key source chaotic system:

$$\begin{cases}
 x_1(0) - (m = MxWor + 1) / 255 \\
 x^2(0) = x_1(0) + p_1 \\
 x_3(0) = x_2(0) + p_2 \\
 x_4(0) = x_3(0) + p_3
 \end{cases} \quad (2)$$

In Formula (2),  $p_1, p_2, p_3 \in [0, 1]$  are adjusting parameters of the original value. Different systems are selected according to different adopted values of Source1, as shown in Table 1.

If  $q$  is the dimension number of the key source chaotic system, a  $q$ -dimensional system generates  $q$  lines of chaotic sequences. Each line generates max chaotic values where max is the maximum value of the width and height of the plaintext video frame. Source1, Source2 and Source3 chaotic sequences are chosen as the encryption keys. The chaotic sequences of the selected key source chaotic system are optimized according to Formula (3) where  $x(i, j)$  is the chaotic sequence value before optimizing,  $Y(i, j)$  is the optimized chaotic sequence value, and “round” means taking round number.

$$\begin{aligned}
 y = (i, j) = & \\
 & \left\{ \left( (10^6 x(i, j) - \text{round}(10^6(i, j))) + (10^6 x(i, j+1) - \text{round}(10^6 x(i, j+1))) \right) / 2 (j > q) \right. \\
 & \left. \left( (10^6 x(i, j) - \text{round}(10^6(i, j))) + (10^6 x(i, 1) - \text{round}(10^6 x(i, 1))) \right) / 2 (j = q) \right\} \quad (3)
 \end{aligned}$$

$i=1,2,3,\dots,\max$   
 $j=1,2,3,\dots,q$

$Y(i,j)$  - optimized chaotic sequence value

$x(i,j)$  - chaotic sequence value before optimizing

$round$  - taking round number

Optimize map chaotic sequences to the scope of [0,255] according to Formula (4):

$$z(i, j) = fix \left( \left( y(i, j) - fix(Y)(i, j) \right) \right) * 10^4 \bmod 256 \quad (4)$$

$Z(i,j)$  - chaotic sequence value after mapping

$Y(I,j)$  - optimized chaotic sequence value

$fix$  - taking the round number closer to 0.

Conduct encryption processing according to Formula (5):

$$\left\{ \begin{array}{l} FR(k) = \begin{cases} MwXor \odot R(k) \odot Z(f, source1) \odot \left( (R(m * n - 1) + R(m * n)) \bmod 255 \right), k = 1 \\ R(k) \odot Z(f, source1) \odot \left( (R(m * n) + FR(1)) \bmod 255 \right), k = 2 \\ R(k) \odot Z(f, source1) \odot \left( (FR(k - 2) + FR(k - 1)) \bmod 255 \right), k - Othervalues \end{cases} \\ FG(k) = \begin{cases} MwXor \odot G(k) \odot Z(f, source1) \odot \left( (G(m * n - 1) + G(m * n)) \bmod 255 \right), k = 1 \\ G(k) \odot Z(f, source1) \odot \left( (G(m * n) + FG(1)) \bmod 255 \right), k = 2 \\ G(k) \odot Z(f, source1) \odot \left( (FG(k - 2) + FG(k - 1)) \bmod 255 \right), k - Othervalues \end{cases} \\ FB(k) = \begin{cases} MxWor \odot B(k) \odot Z(f, source1) \odot \left( (B(m * n - 1) + B(m * n)) \bmod 255 \right), k = 1 \\ B(k) \odot Z(f, source1) \odot \left( (B(m * n) + FB(1)) \bmod 255 \right), k = 2 \\ B(k) \odot Z(f, source1) \odot \left( (FB(k - 2) + FB(k - 1)) \bmod 255 \right), k - Othervalues \end{cases} \end{array} \right. \quad (5)$$

$m$  - height of plaintext video frame

$n$  - width of plaintext video frame

where  $R(k)$ ,  $G(k)$  and  $B(k)$  are respectively the values of the red component, green component and blue component of the  $k$ th pixel of the plaintext video frame.  $FR(k)$ ,  $FG(k)$  and  $FB(k)$  are respectively the values of the red component, green component and blue component of the  $k$ th pixel of the encrypted video frame.  $Z(f, source1)$  is the encryption key where  $f = ((i * j) \bmod \max) + 1$ . The decryption process is the inverse process of the encryption process.

## 5. SYSTEM TESTING

### 5.1. Security Testing

The system adopts SM2/3/4 commercial key algorithms combined with CSK algorithm for encryption, which yields a security strength that exceeds that of international algorithms. Such encryption mode has preferable controllability and can be used in synergic video command systems. Key information of the system (e.g. strategy configuration, messy code text, key information, identity information, etc.) is transmitted on the network in the form of ciphertext to avoid destruction. As well, the leakage of any sensitive security information will not impact the security capacity of other technologies. The system especially adopts multiple chaotic encryption algorithms, which greatly increases complexity and raises the security coefficient.

Table 2. Test Table of Cryptogram Operation Capacity of a Single Conferencing Terminal in Processing One-way Code Rate

	Level I (Kbps)	Level II (Mbps)	Level III (Mbps)
SM4	0.28	1.32	2.01
SM3		0.57	1.12

## 5.2. Performance Testing

A video conference with the biggest load is adopted as the testing site. The video code rate is 2 Mbps, the frame rate is 30fps, the I/P frame rate ratio is 1:12, the size ratio is 5:1, and the audio code rate is 64 kbps. The cryptogram operation capacity of a single conferencing terminal in processing one-way code rate is tested as in Table 2. It shows that conferencing cryptogram operation speed accelerates along with the increase of security level and can entirely meet real conferencing demands.

## 5.3. Testing of Video Encryption and Decryption Condition

Cameras are used to gather video information and store the information in video files. As the chaotic value of the key source chaotic system is insensitive to initial conditions in the first dozens of seconds, the chaotic value in the first 15 seconds is removed and the original value adjusting parameters are set as  $p_1=0.1$ ,  $p_2=0.2$ ,  $p_3=0.3$ . In accordance with the above encryption scheme, the testing results of video encryption and decryption are as shown in Figure 8. It can be seen that encrypted video image differs greatly from the plaintext video image, and the characteristics of the plaintext video image cannot be identified from the encrypted video image. The subjective visual effect is favorable. Testing shows that time consumed for video encryption only increases by about 15 ms and basically has no impact on video display.

Figure 8. Testing Results of Video Encryption and Decryption

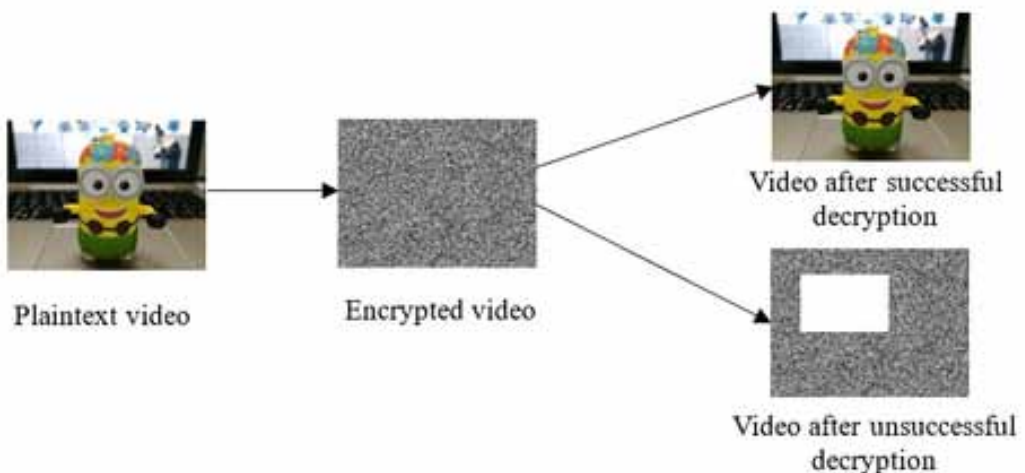
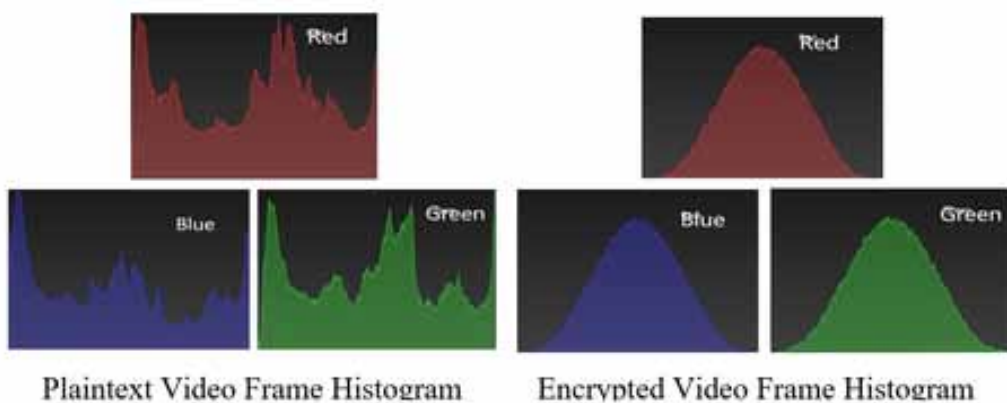


Figure 9. Video Frame Histograms before and after Encryption



## 6. SYSTEM SECURITY PERFORMANCE EVALUATION AND DISCUSSION

As videos are dynamic images, security analysis methods for static images are not applicable here. Therefore, the system can be evaluated and discussed from the perspectives of key space and statistical characteristics.

### 6.1. Evaluation and Discussion of Key Space

Key space normally refers to the value range of a key in an encryption algorithm and usually the unit is bit, i.e. to count a specific key according to its bit number. The longer the key bit is, the larger the key space is. So far, key space is cracked mainly through the method of exhaustion, which means by speculating and verifying every possible cryptogram one by one, and excluding wrong ones until the right cryptogram is identified. The encryption key adopted in this paper comes from the four variables ( $x_1$ ,  $x_2$ ,  $x_3$ ,  $x_4$ ) of the original chaotic value as well as the key controlling the starting position of chaotic sequences. The original chaotic value is computed by binary 32-bit precision floating-point number, and the pseudorandom chaotic sequence starting position key is computed by decimal number. Therefore, the encryption key in this paper is 144-bit long while the key of AES encryption algorithm that can defend numerous attacking algorithms is 128-bit long at minimum. Assuming that a cryptogram analyst uses the fastest computer in the world to search a key at 1 petaflop, it still takes more than 7,000 years to crack a 144-bit key. Therefore the key space is big enough to defend exhaustive attacks.

### 6.2. Evaluation and Discussion of Statistical Characteristics

One frame of image is cut out randomly from the video file gathered by cameras, the image is computed through Matlab. Then, the red component, green component and blue components are extracted respectively from the original color image, and encrypted color image and the statistical characteristics are analyzed respectively. In this video encryption system, the results are shown respectively in the plaintext video frame pixel histogram and encrypted video frame pixel histogram with dual encryption of both data and location. It can be seen that the pixels of plaintext image are distributed unevenly, focusing basically in the scope of 50~210, showing obvious characteristics. In comparison, the pixels of the encrypted image are distributed evenly in a way more like white noise distribution, showing no obvious statistical characteristics, which greatly reduces the correlation between plaintext and ciphertext, and increases encryption security as shown in Figure 9.

Despite the sound security performance of the system and the scientific encryption algorithm, it is undeniable that there are still problems to be settled urgently such as insufficient anti-shear ability of encryption scheme, insensitivity of chaotic value in the first few seconds, huge computing quantity of selective encryption, etc.

## **7. CONCLUSION**

In allusion to the utilization pattern and service characteristics of synergic video command systems, this paper analyzes the research achievements at the present stage, proposes an end-to-end encryption method of multimedia information that introduces a multiple protection mechanism including selective encryption and selective integrity protection, and designs a network access authentication and service encryption workflow that implants startup authentication and key distribution into the information control signaling procedure. These achievements result in reliable and stable communication, a scientific encryption algorithm, and flexible client access to and withdrawal from conferences. To enhance the encryption level of video transmission, the system integrates CSK encryption algorithm and constitutes a key pool with three different algorithms to further improve system security. The encryption design scheme proposed in this paper realizes encrypted video synergic command and dispatch, meets various personalized user demands for multimedia information encryption, and helps users to rapidly realize and deploy encrypted video synergic command systems in all walks of life.

## **FUNDING AGENCY**

This research was supported by Humanities and Social Science Research Project of Hebei Education Department (No. SD2021052), and Higher Education Teaching Reform Research and Practice Project of Hebei (2020GJJG153).

## REFERENCES

- Antonio, A., Maria, C. D., & Manuel, M. (2015). Study of the Hopf bifurcation in the Lorenz, Chen and Lv systems. *Nonlinear Dynamics*, 79(2), 885–902. doi:10.1007/s11071-014-1709-2
- Cao, P., Huang, Z., Lu, Y. L., & Chen, G. (1999). A Distributed Authentication and Key Distribution Protocol for Mobility Communication. *Journal of Huazhong University of Science and Technology*, 8, 95–97.
- Cao, Y., Zhang, R., & Liu, Z. K. (2005). Research on DCT-based Video Encryption under H. 264. *Journal of Image and Graphics*, 10(8), 1047–1051.
- Chai, X. L., & Guo, J. Y. (2014). Color image encryption on algorithm based on several rounds of proliferation. *Microelectronics & Computer*, 31(5), 62–66.
- Chen, S., & Xue, W. (2020). Image Encryption Algorithm Based on Chaotic System and Artificial Neural Network. *Computer Systems & Applications*, 29(8), 236–241.
- Duan, S. K., Hu, X. F., Wang, L. D., Gao, S., & Li, C. (2014). Hybrid memristor/ RTD structure-based cellular neural networks with applications in image processing. *Neural Computing & Applications*, 25(2), 291–296. doi:10.1007/s00521-013-1484-x
- Guan, G. R., Wu, C. M., & Jia, Q. (2015). An improved high performance Lorenz system and its application. *Wuli Xuebao*, 64(2), 020501–020501. doi:10.7498/aps.64.020501
- He, Y., Wang, L., & Xia, H. (2013). Encryption Algorithm of Color Video Image Based on Lorenz Chao. *Computer Science*, 40(6A), 365–367.
- Hu, H. P., Wu, J., & Wang, Z. X. (2006). A Security Solution Based on H.323 Video Conference System. *Journal of Huazhong University of Science and Technology*, 34(11), 55–57.
- Lai, Y. Q. (2017). Simulation Study on High Efficiency Encryption Algorithm of Multimedia Video Image. *Computer Simulation*, (11), 168–171.
- Li, L., Wang, Y. Y., & Li, M. (2019). The Key Technology of HD-Video Conferencing System. *Electronic Technology and Software Engineering*, 26(02), 26.
- Li, Y. H., & Xu, L. M. (2017). Design of Highway Command and Scheduling System Based on GIS. *Information & Communications*, (3), 112–113.
- Liu, F., & Hartmut, K. (2015). Puzzle - A Novel Video Encryption Algorithm. In *IFIP International Conference on Communications and Multimedia Security*. Springer.
- Mashamba-Thompson, T. P., & Crayton, E. D. (2020). Block chain and artificial intelligence technology for novel coronavirus disease-19 self-testing. *Diagnostics (Basel)*, 10(4), 198. doi:10.3390/diagnostics10040198 PMID:32244841
- Mian, C., Jia, J., & Lei, Y. (2007). An H. 264 video encryption algorithm based on entropy coding. In *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007)*. IEEE. doi:10.1109/IIH-MSP.2007.86
- Qi, H., Liao, X. F., & Li, C. D. (2013). Analysis of associative memories based on stability of cellular neural networks with time delay. *Neural Computing & Applications*, 23(1), 237–244. doi:10.1007/s00521-012-0826-4
- Qian, H., & Qin, L. L. (2020). The Design of Intelligent Transportation Video Processing System in Big Data Environment. *IEEE Access: Practical Innovations, Open Solutions*, (8), 13769–13780.
- Qin, L. L., & Kang, L. H. (2016). Technical framework design of safety production information management platform for chemical industrial parks based on cloud computing and the internet of things. *International Journal of Grid and Distributed Computing*, 9(6), 299–314. doi:10.14257/ijgcd.2016.9.6.28
- Qin, L. L., Yu, N. W., & Zhao, D. H. (2018). Applying the convolutional neural network deep learning technology to behavioural recognition in intelligent video. *Tehnicki Vjesnik*, 25(2), 528–535.



- Sanpei, T., Shimobaba, T., Kakue, T., Endo, Y., Hirayama, R., Hiyama, D., Hasegawa, S., Nagahama, Y., Sano, M., Oikawa, M., Sugie, T., & Ito, T. (2016). Optical encryption for largesized images. *Optics Communications*, 361, 138–142. doi:10.1016/j.optcom.2015.10.049
- Sattar, F., Cullis-Suzuki, S., & Jin, F. (2016). Acoustic analysis of big ocean data to monitor fish sounds. *Ecological Informatics*, (34), 102–107.
- Shi, T., King, B., & Salama, P. (2006). Selective encryption for H. 264/AVC video coding[C]//Security, Steganography, and Watermarking of Multimedia Contents VIII. *International Society for Optics and Photonics*, 6072, 607217.
- Spanos, G. A., & Maples, T. B. (1995). Performance study of a selective encryption scheme for the security of networked. real-time video. In *Proceedings of Fourth International Conference on Computer Communications and Networks-IC3N'95*. IEEE.
- Tian, L., Xie, S. C., & Zhang, J. Z. (2015). RC4 Video Encryption Algorithm Based on Hyper-chaos. *Video Engineering*, 39(11), 15–18.
- Tian, R. X., & Wang, F. (2014). Discussion on Data Encryption Technology in Computer Network. *Cyberspace Security*, (02), 71–73.
- Valli, D., & Ganesan, K. (2017). Chaos based video encryption using maps and Ikeda time delay system. *The European Physical Journal Plus*, 132(12), 542. doi:10.1140/epjp/i2017-11819-7
- Wang, H. W. (2015). Video optical encryption technology based on liquid crystal light valve. *Journal of Applied Optics*, 36(3), 398–402. doi:10.5768/JAO201536.0302003
- Wang, H. W., Shi, G. W., & Qin, J. (2017). Research on video optical encryption technology in single channel based on chaotic key. *Journal of Optoelectronics. Laser*, (9), 1008–1015.
- Yan, X. B., Fan, Y. M., Lee, H. H., & Qiu, R. G. (2020). Research on Personal Information Risk Assessment Model in Smart Cities. *Technical Gazette*, 27(5), 1403–1409.
- Yang, G. B., & Han, L. (2014). Survey on Video Conference System. *Application and Engineering of Video Technology*, 267(09), 60–63.
- Yang, L. J., Xie, S. C., & Zhang, J. Z. (2016). Color video stream encryption algorithm based on multi-chaotic system. *Video Engineering*, 40(12), 7–11.
- Yao, X., & Xu, X. (2020). Dual Image Cross-hybrid Encryption Algorithm Based on Chaotic System. *Software Guide*, 19(06), 248–252.
- Ye, R. S., & Tan, X. B. (2014). A multi-orbit hybrid image encryption scheme based on continuous chaotic dynamical systems. *Journal of Shantou University: Natural Science*, 29(4), 8–19.
- Yin, C., Zhang, L. Y., & Tu, M. (2019). TF-IDF Based Contextual Post-Filtering Recommendation Algorithm in Complex Interactive Situations of Online to Offline: An Empirical Study. *Technical Gazette*, 26(6), 1529–1536.
- Zhang, Y. P., & Shan, G. L. (2020). A Risk-Based Sensor Management Method for Target Detection in the Presence of Suppressive Jamming. *Technical Gazette*, 27(1), 114–124.
- Zhu, Y. P. (2016). On a New Video Encryption Algorithm Based on CNN Hyper chaos. *Journal of Southwest China Normal University*, 41(09), 113–119.
- Zhu, Y. P., & Zhao, X. L. (2017). Chaotic keying video encryption scheme research *Journal of Chongqing University of Posts and Telecommunications*, 29(1), 90–97.

*Qin Lele, male, researcher, was born in Zhangjiakou, Hebei, China on March 19, 1978. He earned a Master Degree of Engineering from Nanjing University of Science and Technology, China in 2006. His major field of study is the analysis and design of management information system. He has been in the research of management information system, and is now dean of Teaching Operation Management, Office of Teaching Affairs in Hebei University of Science and Technology. He has been teaching more than 10 courses at various levels including Management Information System, MIS Curriculum Design, and Database Principle. He has published more than 20 articles, 18 of which were indexed by EI or SCI. His research interests are the analysis and development of MIS.*

*Guojuan Zhang, female, senior experimenter, was born in 1977. In July 2007, She graduated from Hebei University of Economics and Business with bachelor's degree. She has published more than 10 articles, some of which were indexed by SCI.*

*Li You, female, associate professor, was born in July 1978. She graduated from Hebei Normal University with Bachelor of Engineering degree in Computer Science and Technology in 2002. She graduated from Hebei University of Science and Technology with master's degree. In 2008, She has published more than 10 articles, some of which were indexed by SCI. Corresponding Author, E-mail: youli\_hebei@sina.cn.*