Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6518743, 15 pages
https://doi.org/10.1155/2021/6518743

Research Article

BSVMS: Novel Autonomous Trustworthy Scheme for Video Monitoring

Xuan Wang,[1] **Jingjing Xu**,[1] **Jiaxin Wang**,[1] **Wei Ou**,[1] **Jung Yoon Kim**,[2] **and Wenbao Han**[1]

[1] *School of Computer Science and Cyberspace Security, Hainan University, Haikou, 570228 Hainan, China*
[2] *Graduate School of Game, Gachon University, 1342 Seongnamdaero, Sujeong-gu, Seongnam, 461-701 Gyeonggi-do, Republic of Korea*

Correspondence should be addressed to Wei Ou; ouwei@hainanu.edu.cn and Jung Yoon Kim; kjyoon79@gmail.com

Received 16 June 2021; Accepted 6 August 2021; Published 26 August 2021

Academic Editor: Xiaoxian Yang

With the continuous development and application of monitoring technology, which involves increasingly more sensitive information, the global demand for video monitoring systems has surged. As a result, video monitoring technology has received widespread attention both at home and abroad. Traditional video monitoring systems experience security threats, with differing levels of severity, in terms of attack, storage, transmission, etc., which results in different degrees of damage to users' rights. Therefore, we propose a blockchain-SM-based video monitoring system called BSVMS. For the front-end device invasion risk, internal attack risk, and security storage problem of the monitoring system, we use commercial cryptography algorithms to complete the encryption processing of images through a visual change network in the imaging process, thereby ensuring the security of the video data from the source. To address the problem that the video monitoring application software and data are vulnerable to damage, we use blockchain technologies that are tamper-proof and traceable to build a trustworthy video monitoring system. In the system, no member can query the original monitoring data. To address the security issues in network transmission, we use a commercial cryptography algorithm for multilayer encryption to ensure the security of data during transmission, guarantee the confidentiality of the system, and realize domestic autonomous control. We then conduct tests and security analysis of the encryption and decryption efficiency of the SM4 algorithm used in the system, the blockchain performance, and the overall performance. The experimental results show that in this system environment, the SM4 algorithm encryption and decryption efficiency is better than other algorithms and that the blockchain used meets industry standards.

1. Introduction

With the rapid development of modern science and technology, the construction of network infrastructure is increasingly sound, and the application of network video monitoring technology is gradually increasing. Video monitoring technology is widely used, particularly in sensitive industries. In addition to the rapid development trend, the data security problem of network video monitoring systems is increasingly obvious. In particular, when monitoring technology is widely used, the monitored content may involve state secrets, military intelligence, business secrets, personal information, and other sensitive information. Once leaked, great security risks will occur, giving criminals an opportunity to harm enterprises and families through video monitoring and even threatening national and social security [1]. Therefore, the most important issue at present is to improve the security of network video monitoring systems.

The COVID-19 epidemic has promoted the development of the video monitoring industry. Thermal cameras equipped with black-body collators and facial recognition video analysis solutions are now the main solutions for screening suspected cases in public places such as railway stations, airports, hospitals, and supermarkets. Infrared thermal imaging cameras are widely used in high-temperature screening in public places [2]. The State Council has listed infrared thermal temperature measurement equipment and related products as key materials in the epidemic, which means that the production and transportation of these materials must be guaranteed and given priority. In the early stage of the epidemic, relevant news mainly focused on the latest progress and data briefing so as to meet the public's demand for authoritative information. At this stage, the public is in a state of information hunger. In special circumstances, live video monitoring without commentary, editing, or any processing has become the key to the fight against the epidemic. People's security awareness is increasing daily, and network video monitoring systems have gradually become an important way to maintain personal and social security; therefore, these systems have received extensive attention from all walks of life and have shown a rapid development trend since their inception. Intelligent video monitoring appears in the concept of distributed video monitoring [3, 4], which extends the monitoring mode to the complement of decentralized and centralized video monitoring and expands the scope of monitoring without limitations. The ubiquitous Internet and LAN are utilized to achieve plug-and-play applications within the scope of the entire network [5]. Most video monitoring systems can conduct reliable monitoring 24 hours a day and can realize unmanned monitoring modes. A large amount of electronic equipment can replace personnel and instruments to achieve the purpose of monitoring, which greatly reduces the use of human resources and financial resources and is more efficient [6, 7].

While the advent of the 5G era gives video monitoring a broader space for global development, it also brings challenges to video security technology. The current problems of video monitoring systems are as follows: (1) Front-end equipment has the risk of invasion. Front-end devices have significant advantages such as round-the-clock uninterrupted operations, strong computing power, high access bandwidth, and a large number of devices. Therefore, criminals tend to invade front-end devices. Criminals can break relatively weak passwords by force and steal high-risk sensitive data through relevant system vulnerabilities [8, 9]. (2) Application software and data are vulnerable to damage. This is an era of big data. Video monitoring focuses on application software and data mining, but it also makes application software and data the most direct targets of criminals. People use big data to obtain effective information, but at the same time, data are also vulnerable to attack and illegally exploited by criminals [10–13]. (3) In general, there are security problems in the transmission of video networks. Universal video channels have the best security, followed by VPNs, and public networks and mobile networks have the worst security [14, 15]. At present, more front-end access devices rely on the mobile Internet and public networks for transmission. Although certain security access measures will be taken, it is still difficult to avoid the intrusion of criminals, and the absolute security of the data in transmission cannot be guaranteed [16]. (4) For internal attack risk, when designing network video monitoring systems, security issues caused by internal network attacks are generally rarely considered. Therefore, most video services are in an open network environment, which makes these video services vulnerable to artificial attacks, such as data interception, information theft, data tampering, and data addition and deletion [17]. (5) For the safe storage problem, the video monitoring image data will be stored in the memory of these cameras for a considerable period of time, and traditional cameras will inevitably capture other irrelevant surrounding background information. Hackers can use the conventional cracking mode for illegal intrusion [18–22].

In order to solve the above problems, we propose a new scheme for an autonomous trustworthy video monitoring system. In view of the front-end equipment intrusion risk, internal network attack risk, and data storage security problems of video monitoring, in this paper, we modify the visual sensor directly and use a commercial cryptography algorithm to encrypt the images through the visual transformation network to realize the encryption of the images during the imaging process, which solves the root cause of the problems. In view of the vulnerability of application software and video monitoring data, we adopt blockchain technologies to manage video systems. No member is allowed to directly query the original monitoring data while all participants are allowed to query any monitoring data on the chain. Regarding the security problems during network transmissions, video data processed by key state encryption can be uploaded to the blockchain platform directly, quickly, and effectively. The blockchain network participants can use the SM4 encryption algorithm to generate a public key, which can be uploaded to the blockchain platform. In this way, we can ensure the security of the video data in the entire transmission process.

2. Background

In the development of video monitoring security, the chaotic encryption algorithm has become the mainstream method in the study of image encryption technology since Fridrich first proposed it in 1997. The chaotic encryption algorithm has developed from one-dimensional chaotic encryption to later two-dimensional and three-dimensional chaotic encryption, and even the hyperchaotic system and composite chaotic system have been proposed [23, 24]. Earlier, Microsoft used AudibleMagic's related software to extract the fingerprints of uploaded videos and protect video data by matching them with the AudibleMagic database to enable active blocking of unauthorized video distribution behavior. Kundur et al. proposed a password-based process called PICO (privacy through reversible password hiding), which applies facial recognition algorithms to images and then uses symmetric key encryption to encrypt the identified face areas. Goldstein and Osher designed a watermark-based video integrity verification method that overcomes the inability of traditional verification mechanisms such as digital signatures to distinguish between attacks and routinely modified signatures [25]. However, Kundur et al. and Goldstein and Osher still have not addressed the issues of privacy, confidentiality, and authentication in WVSNs very well.

Rahman et al. proposed a privacy-preserving mechanism that hides sensitive information from video while providing effective monitoring. This scheme is computationally efficient and suitable for real-time video transmission. However, the system is based on a chaotic encryption algorithm, which has the contradiction of achieving accuracy and confidentiality

[26]. Wang and Smith also proposed a watermarking-based framework using watermarking to embed and hide privacy information (related to the authorized person) in video with minimal perceptual changes while embedding a digital signature in the packet header to authenticate the watermarked video to address the privacy and authenticity issues in video monitoring systems [27]. Huang et al. proposed that the watermarking technique for WVSNs can be implemented using the principle of distributed source coding, which exploits the duality of data hiding and channel coding. Digital video watermarking techniques have been widely studied and implemented in various application areas [28]. However, when the watermarked video is attacked by cropping and interception, the watermark carrier is vulnerable to damage, and video security cannot be guaranteed.

In China, video monitoring security technology started late but developed rapidly. As early as the development of fingerprint technology, Youku began to try to block the spread of illegal monitoring content using fingerprint detection technology. During the COVID-19 outbreak in 2020, since people's work and studies involved video conferences, Shu-li et al. discussed the security risks associated with networking video security systems from video conferencing, video private networks, video content, and video monitoring and proposed a video protection scheme using three layers of protection: confusion scrambling, selective encryption, and selective integrity protection [29, 30].

Jia-liang et al. proposed a security audit solution for UHD video content based on visual image classification technology, target detection and recognition technology, face recognition technology, and super large-scale vector retrieval technology. However, the efficiency of the intelligent recognition and analysis of UHD video content needs to be further improved [31]. Based on the research and analysis of the private network security of public security videos, Yu-Yang et al. proposed protection methods for video private networks such as "one machine one file" docking and protocol whitelist filtering. However, these methods limit the expansion of application scenarios while ensuring data security [32]. In response to various vulnerabilities and flaws of mainstream monitoring products, Long and Haili made improvements in monitoring video transmission and storage security and proposed implementing the authentication problem of the main control side of the monitoring system with an improved RSA algorithm according to the H.265 technology framework. However, the system is not very resistant to attacks and has the problem that the application and video data are vulnerable to corruption [33]. Zheng-qiang et al. proposed a security reinforcement scheme for video monitoring system networking applications. The scheme first implements trusted operation control, access authentication, signaling reinforcement, and video data encryption in front-end devices by updating and upgrading. Second, the scheme deploys the monitoring security management platform in the central management platform to realize the security management of access devices. Finally, the scheme integrates a hardware decryption module in monitoring client computers to realize the decryption of encrypted audio and video. However, the system data are stored in a centralized manner, which requires high hardware equipment [34]. With the rapid development of 5G, Yuan-bing and Shu-li proposed a video monitoring cryptographic application framework for 5G edge computing in conjunction with domestic autonomous and controllable commercial cryptography while 5G is rapidly developing. The security of video surveillance data has been greatly improved [35]. All these results show that video monitoring security technology in China is booming, but there are still some drawbacks [36].

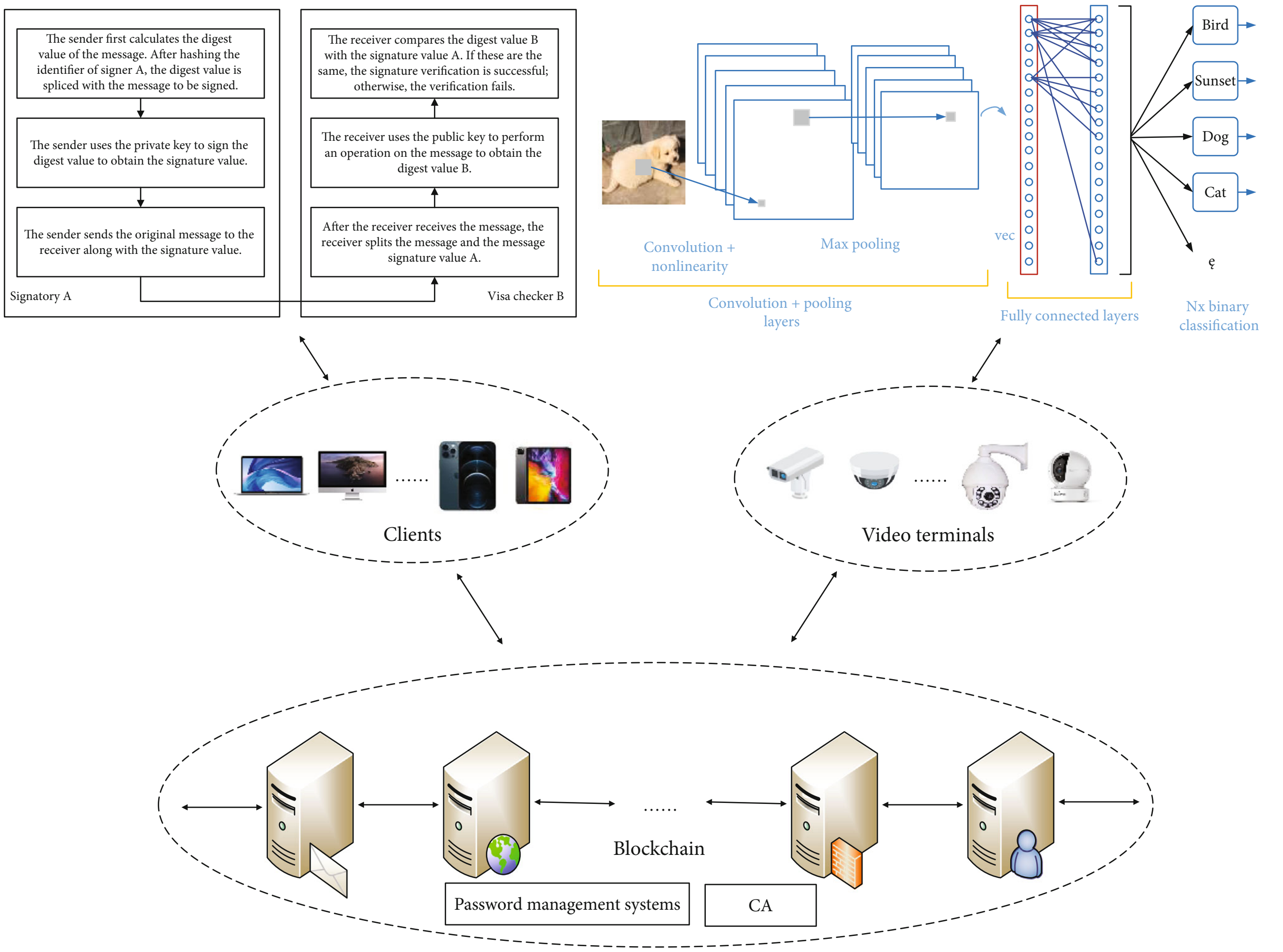
3. Autonomous Trustworthy Video Monitoring Scheme

3.1. Architecture. Our system is based on the SM4 algorithm, which can directly encrypt the visual transformation network in the network monitoring camera and upload the encrypted video data to the blockchain platform. After verification, the client can view the monitoring video data. The system is divided into video processing and blockchain management. The overall architecture of the system is shown in Figure 1.

(i) The source of the monitoring video is the network monitoring camera. The video is captured by the camera. The data processing adopts a camera with a low bit rate, low power consumption, and a high-quality image whose processor core is the mainstream embedded processor, a kernel processing ISP, audio and video codecs, and various types of interfaces. It has strong video graphic processing and intelligent analysis capabilities and can realize various types of video codecs

(ii) When the camera acquires video data, commercial cryptography encryption is performed in the monitoring front-end device firmware through the visual change network. First, we use the SM4 algorithm to generate the key, and then, the original image (x_0) is vectorized into the K-layer convolutional network $N(x) = N_k(N_{k\text{-}1}(\cdots N_1(x)))$. After encryption, the convolutional neural network becomes $N(x\,;W) = A_k W_K \cdots (A_2 W_2 A_1{}^{-1})(A_1 W_1 A_0{}^{-1})A_0 x$, which enables the front-end device to complete the encryption of video monitoring directly in the imaging process and upload it to the blockchain platform after encryption is completed

(iii) The blockchain platform distributes the key to the terminal while receiving the data, and the terminal encrypts the locally collected video and transmits it to the counterpart device, generating the key each time it receives the data and distributing it securely to the terminal. The information is encrypted by the public key or symmetric key of the receiver and then uploaded to the chain and shared, and only the receiver with the corresponding private key can decrypt the information. The transmission, storage, and update of video monitoring data are completed on the chain, and when the original data are tampered with, the responsible person can be directly identified



The sender first calculates the digest value of the message. After hashing the identifier of signer A, the digest value is spliced with the message to be signed.

The sender uses the private key to sign the digest value to obtain the signature value.

The sender sends the original message to the receiver along with the signature value.

The receiver compares the digest value B with the signature value A. If these are the same, the signature verification is successful; otherwise, the verification fails.

The receiver uses the public key to perform an operation on the message to obtain the digest value B.

After the receiver receives the message, the receiver splits the message and the message signature value A.

Figure 1: Overall structure.

(iv) The receiver needs to authenticate based on the SM2 algorithm before receiving the video sent by the counterpart device and decrypt and play the video monitoring information after receiving the ciphertext. Since the digital signature only relies on the private key of the sender, which is only owned by the sender personally, this identity authentication method is more secure

3.2. Video Preprocessing. A key net is a convolutional neural network that allows inferences regarding the collected data using specially designed sensors. When processing video monitoring using key nets, visual image classification techniques must be used.

Visual image classification technology conducts visual image classification for ultra-high-definition video content. It is mainly based on deep learning-based visual image classification technology, and the image classification architecture used is a convolutional neural network (CNN). The specific principle is as follows: based on the CNN and 3D-CNN, after the key frame extraction and short video segmentation of the video to be analyzed and identified, feature extraction is performed, the feature vector is formed, and then, the sequence is recognized and analyzed by long short-term memory (LSTM). The above process is repeatedly executed for the UHD video to be analyzed and recognized until all images and short videos are recognized so that video classification can be realized more reasonably.

We describe the SM4 algorithm that encrypts the video monitoring network through the key net. Figure 2 shows the key net.

The SM4 algorithm has a packet length of 128 bits and a key length of 128 bits. Both the encryption algorithm and the key expansion algorithm use a 32-round nonlinear iterative structure to perform encryption operations in words (32 bits), and each iteration is a round of the transformation function F.

3.2.1. Wheel Functions. The key expansion and encryption process both use the wheel function $Z = F(A, B, C, D, E)$, where $A, B, C, D,$ and E are words 4 bytes in length. Figure 3 shows the schematic structure of the wheel function.

The τ-transform is a nonlinear transformation process in the wheel function consisting of four parallel S-boxes, and the data of the S-boxes are all hexadecimal.

The L-transform is a linear transformation process in the wheel function, and for the wheel function of the encryption process, the L-transform is

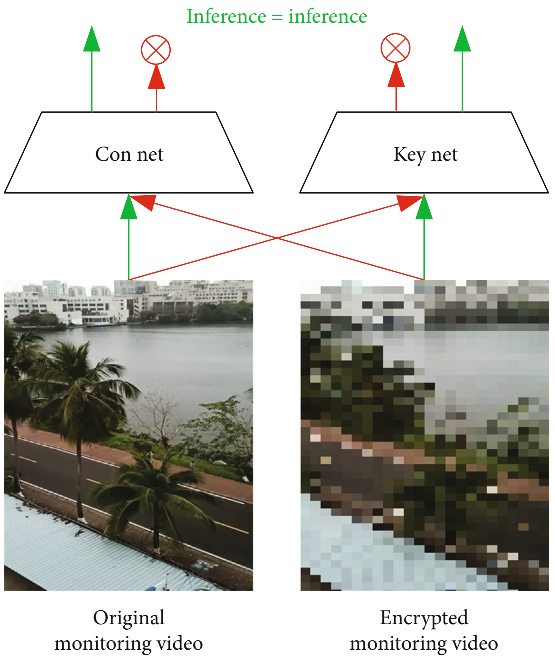


Figure 2: Key net video processing.

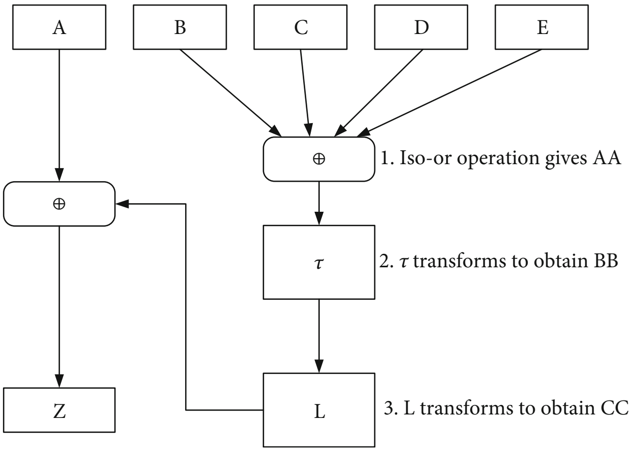

A
B
C
D
E
⊕
1. Iso-or operation gives AA
⊕
τ
2. τ transforms to obtain BB
Z
L
3. L transforms to obtain CC

Figure 3: The schematic structure of the wheel function.

$$L(BB) = BB \oplus (BB{<}{<}{<}2) \oplus (BB{<}{<}{<}10) \oplus (BB{<}{<}{<}18) \oplus (BB{<}{<}{<}24). \tag{1}$$

For the wheel function of the key expansion process, the L-transform is

$$L(BB) = BB \oplus (BB{<}{<}{<}13) \oplus (BB{<}{<}{<}23). \tag{2}$$

The overall encryption function is

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i). \tag{3}$$

T is a synthetic substitution, which consists of a τ -transform and an L-transform.

3.2.2. Key Extensions.

The values of some parameters are shown in Table 1.

rk_i is the wheel key, and the wheel key is generated from the encryption key.

First,

$$(K_0, K_1, K_2, K_3) = (MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3). \tag{4}$$

Then, for $i = 0, 1, 2, \ldots, 31$:

$$rk_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i). \tag{5}$$

Since the system parameters and the fixed parameters are known, the wheel key can be found.

3.2.3. Encryption and Decryption.

When encrypting the last round of transformations, the output is

$$(Y_0, Y_1, Y_2, Y_3) = R(X_{32}, X_{33}, X_{34}, X_{35}) = (X_{35}, X_{34}, X_{33}, X_{32}). \tag{6}$$

The decryption is simply done by reversing the order of use of the round keys.

3.3. Blockchain Management.

Blockchain management is shown in Figure 4.

(i) *Node Configuration*. When building the blockchain, it is necessary to configure the information of different nodes and CA authentication and to set the consensus algorithm, block size, and other basic parameters in the blockchain configuration file. In the future, when new nodes join Fabric, the number of nodes can be dynamically added through the node configuration, allowing nodes certified by CA to join the blockchain and build a video monitoring data protection ecology.

(ii) *Create Channel*. The channel function in Fabric can be used to isolate the data of different channels in the ledger sharing of different nodes according to their needs. In this system, it is only necessary to build one channel after the nodes are configured.

(iii) *Deployment Contract*. The smart contract in the blockchain needs to be deployed at each node in the channel to take effect, so it is necessary to write video monitoring cryptographic information on the chain into the smart contract and instantiate its deployment.

(iv) *Video Monitoring Data Information Uploading*. When the monitoring end encrypts the generated monitoring data, the monitoring end will call the video monitoring data information uploading function in the smart contract to upload the ciphertext after SM4 encryption to the blockchain and generate the block.

Table 1: Parameters and values.

Parameters	Values
Encryption key	$MK = (MK0, MK1, MK2, MK3)$
System parameters	$FK = (FK0, FK1, FK2, FK3)$
Fixed parameters	$CK = (CK0, CK1, \cdots, CK31)$

When the video platform receives the request for uploading, it will release the information to the blockchain module, and the blockchain workflow is as follows.

(i) The sending node broadcasts the new video monitoring data ciphertext upload information to the entire network

(ii) Receiving nodes examine the received data record information, such as whether the recorded information is legal, and after passing the examination, the data record will be included in a block

(iii) All receiving nodes in the entire network apply a consensus algorithm to the block

(iv) The block is formally incorporated into the blockchain for storage after passing the consensus algorithm process, and all nodes of the entire network indicate acceptance of the block. The method of indicating acceptance considers the random hash value of the block as the latest blockchain hash value, and the manufacture of the new block is extended on the basis of this blockchain

3.4. Identity Authentication. We use the SM2 algorithm and the blockchain platform for identity authentication, and the processes are shown in Figure 5. The steps are as follows.

(i) The sender first calculates the digest value of the message. After hashing the identifier of signer A, the digest value is spliced with the message to be signed

(ii) The sender uses the private key to sign the digest value to obtain the signature value

(iii) The sender sends the original message to the receiver along with the signature value

(iv) After the receiver receives the message, the receiver splits the message and the message signature value A

(v) The receiver uses the public key to perform an operation on the message to obtain the digest value B

(vi) The receiver compares the digest value B with the signature value A. If these are the same, the signature verification is successful; otherwise, the verification fails

Since the digital signature depends only on the private key of the sender, which is owned only by the individual sender, our identity authentication method is relatively secure. Furthermore, the public key of the sender is open for anyone to obtain, so this method is suitable for situations with a large number of verifiers. In addition, digital signature technology can also provide peer entities, data source identity authentication, and data integrity authentication. Therefore, the identity authentication method based on the SM2 algorithm has high security and practical feasibility.

3.5. Encryption. In the autonomous and trustworthy video monitoring system, the blockchain platform distributes the key generated by the SM4 algorithm to the terminal while initiating a monitoring request. The monitoring terminal encrypts the locally collected video and transmits it to the peer device. After receiving the video ciphertext sent by the peer device, the video is decrypted and played.

The key management system distributes conference keys to monitoring terminals, and all monitoring terminals share the same conference key. As a video uploader, the monitoring terminal uses the SM4 algorithm to generate the key, which is encrypted and protected by the conference key and sent to the video receiver. Both receiving and sending terminals share the same conference key, and end-to-end encryption and decryption are performed based on the conference key.

The key management steps are as follows.

(i) The digital certificate and private key are preset when the system is initialized. After issuing the commercial cryptography double certificate (encryption certificate and signature certificate), the certificate and private key are stored

(ii) After turning on the monitoring device, all terminals share the same conference key. When monitoring starts, the conference key is issued. Conference keys are updated, new conference keys are enabled, and old conference keys are deleted according to the policies (e.g., periodically, monitor endpoints off, and new endpoints on)

(iii) The monitoring terminals use their respective query keys for end-to-end encrypted communication. At the video sending end, the monitoring key is generated to encrypt the video on its own and send the video to the receiving end. In addition, we use the monitoring key to encrypt the query key and send the key and ciphertext together to the receiving end. As the video receiver, we use the monitoring key to decrypt the video to obtain the query key from the sender and then use the query key to decrypt and play the video

The overall flow of audio and video processing between the sending end and the receiving end is shown in Figure 6. The figure shows that the scheme adopts three layers of protection: confusion scrambling, selective encryption, and selective integrity protection. The purpose of confusion scrambling is to make the stream more confusing and increase the difficulty of stream analysis and decryption. Selective encryption provides different levels of encryption strength to protect the confidentiality of audio and video data. Selective integrity protection protects the integrity of some audio and video as required to prevent illegal tampering and destruction. The three-layer protection design greatly enhances the security of the system.

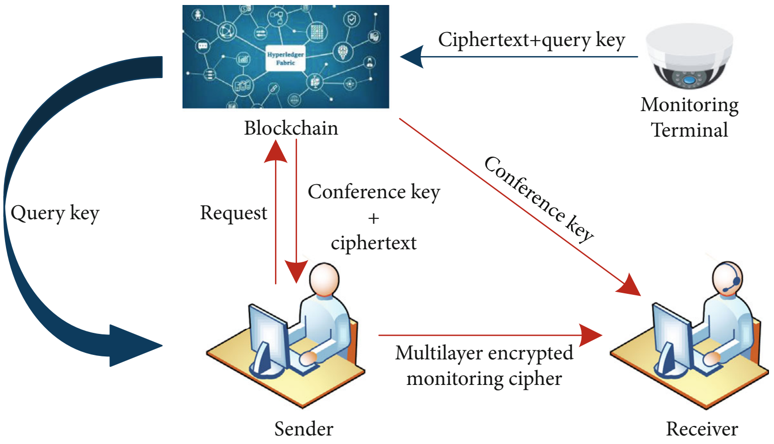


Figure 4: Blockchain management.

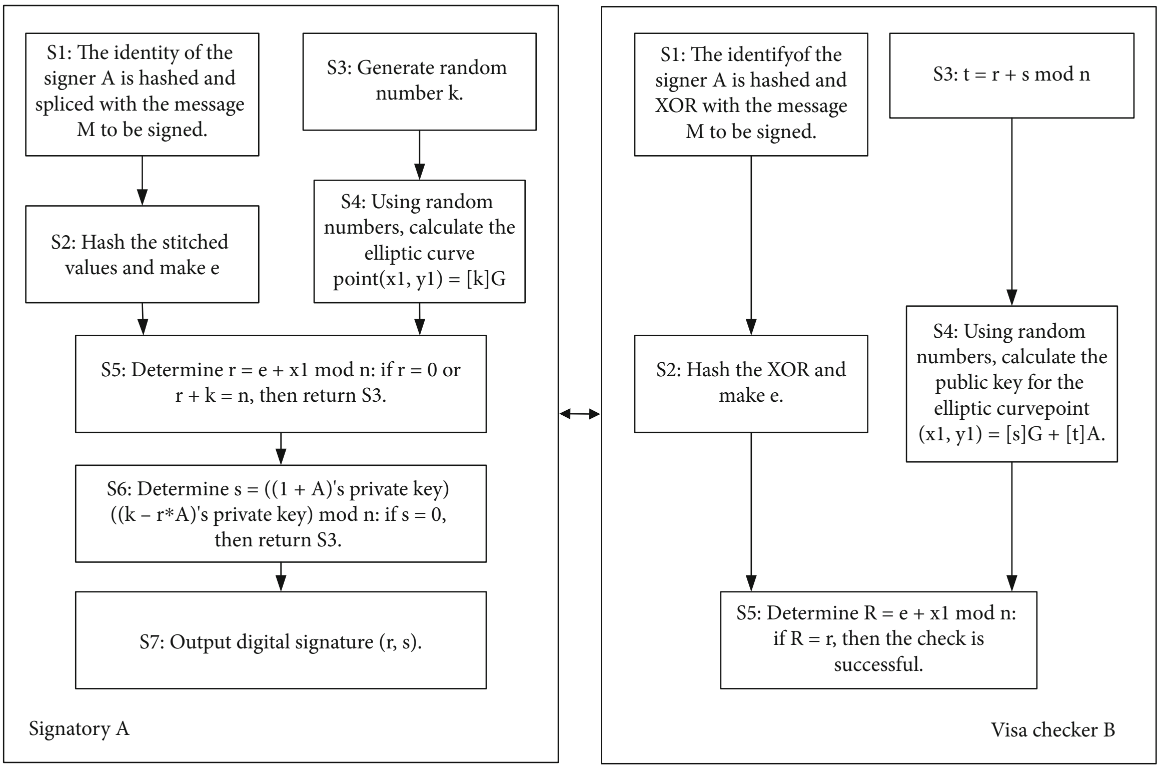

S1: The identity of the signer A is hashed and spliced with the message M to be signed.
S3: Generate random number k.
S2: Hash the stitched values and make e
S4: Using random numbers, calculate the elliptic curve point(x1, y1) = [k]G
S5: Determine r = e + x1 mod n: if r = 0 or r + k = n, then return S3.
S6: Determine s = ((1 + A)'s private key) ((k − r*A)'s private key) mod n: if s = 0, then return S3.
S7: Output digital signature (r, s).
Signatory A
S1: The identifyof the signer A is hashed and XOR with the message M to be signed.
S3: t = r + s mod n
S2: Hash the XOR and make e.
S4: Using random numbers, calculate the public key for the elliptic curvepoint (x1, y1) = [s]G + [t]A.
S5: Determine R = e + x1 mod n: if R = r, then the check is successful.
Visa checker B

Figure 5: SM2-based identity authentication process.

The key feature of confusion scrambling is the garbled codebook. The garbled codebook uses a one-for-one mechanism. The platform will generate the garbled codebook for each new conference and securely distribute it to the participating terminals. This book includes four parts: AudioRN (audio frame garbled code), IframeRNCoe (I frame garbled coefficient), PBframeRN (P/B frame garbled code), and ParaRN (parameter set garbled code). The related design and use criteria are as follows.

(i) AudioRN: AudioRN is a random number string with a length not less than the maximum length of a single audio frame. AudioRN is truncated to a string with the same length as the audio frame and then xor with the audio frame data.

(ii) IframeRNCoe: IframeRNCoe consists of a 1-kilobyte random number string A, a 64-byte incremental random number string B, and an incremental offset X. Equation (1) is used to obtain IframeRN, truncate IframeRN to a number string with the same length as the I frame, and then perform an iso-or operation with the I frame data.

(iii) PBframeRN: PBframeRN is a 64-byte random number string. Xor the first 32 bytes of the P/B frame with the first 32 bytes of PBframeRN, and xor the

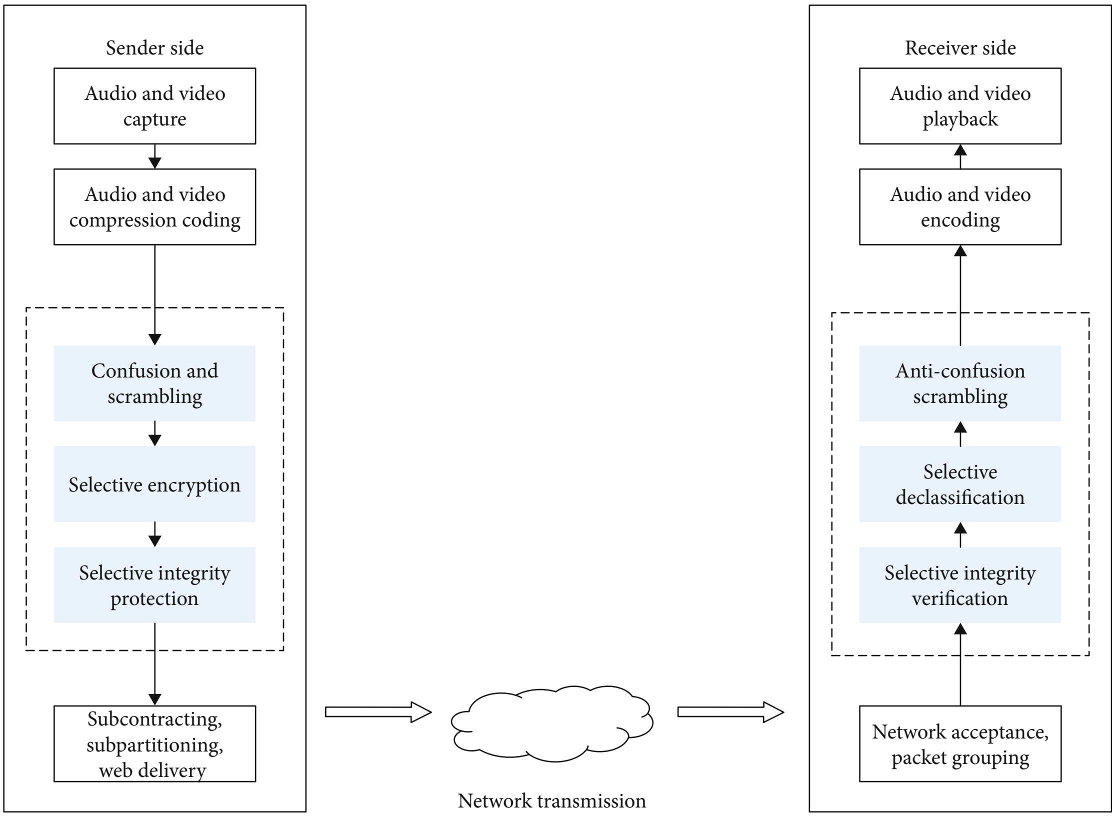

Sender side
Audio and video capture
Audio and video compression coding
Confusion and scrambling
Selective encryption
Selective integrity protection
Subcontracting, subpartitioning, web delivery
Network transmission
Receiver side
Audio and video playback
Audio and video encoding
Anti-confusion scrambling
Selective declassification
Selective integrity verification
Network acceptance, packet grouping

Figure 6: End-to-end encryption process.

last 32 bytes of the P/B frame with the last 32 bytes of PBframeRN. If the P/B frame is less than 32 bytes, PBframeRN is truncated into a number string with the same length as the P/B frame, and then, xor is performed with the P/B frame data.

(iv) ParaRN: ParaRN is a random string of 64 bytes. If the length of the parameter set is less than 64 bytes, ParaRN is truncated to the number string equal to the parameter set, and then, xor is performed with the parameter set. If the parameter set length is greater than 64 bytes, xor is performed only on the first 64 bytes of the parameter set.

Due to the large amount of I frame data, if IframeRNCoe is extended, the scrambled code IframeRN with a sufficient length can be obtained. Its implementation is as follows:

$$\text{IframeRN} = A\|(A \oplus (B<<X)\|(A \oplus (B<<(2X\text{-}1)))\|(A \oplus (B<<(3X\text{-}2)))\| \cdots , \quad (7)$$

where ‖ denotes a string splice, ⊕ denotes a bitwise iso-or, and << denotes a circular left shift.

The selective encryption algorithm of the sender is shown in Figure 7.

The flow of the algorithm in Figure 7 involves three security levels: level I (general), level II (relatively high), and level III (high). The definitions of the three security strengths are shown in Table 2.

At different intensities, different types of data will be fully encrypted or partially encrypted. Part of the encryption process is set out below. Set the data to be processed as M and the length as L, set the grouping parameter as $T(T > 4)$, and divide M into T groups of data. The length of T-1 sets of data is $\lceil L/T \rceil$, and the length of the last set of data is $L\text{-}\lceil L/T \rceil * (T\text{-}1)$. Take the first group, the $\lceil T/4 \rceil$ group, the $\lceil T/2 \rceil$ group, and the last group of data for splicing to obtain data M' of length $L\text{-}\lceil L/T \rceil * (T\text{-}4)$ and perform the SM4_OFB encryption operation on M'.

Selective integrity protection is adopted to protect the video I frame data. At level I, there is no processing. At level II, the sender calculates SM3_HMAC on the frame I data and encapsulates the HMAC value into the end of the frame I data. At level III, the sender computes the treetop summary value of frame I and its preceding $k(k > 0)$ consecutive frames and encapsulates its value into the end of the frame I data.

The diagram of the treetop summary calculation is shown in Figure 8.

The process on the receiving side is the reverse process of the sending side. We need to ensure that the receiving side shares the same policy and parameter configuration as the sending side. Concrete realization forms can be realized through platform control, negotiation between the sender and the receiver, presetting, and other ways.

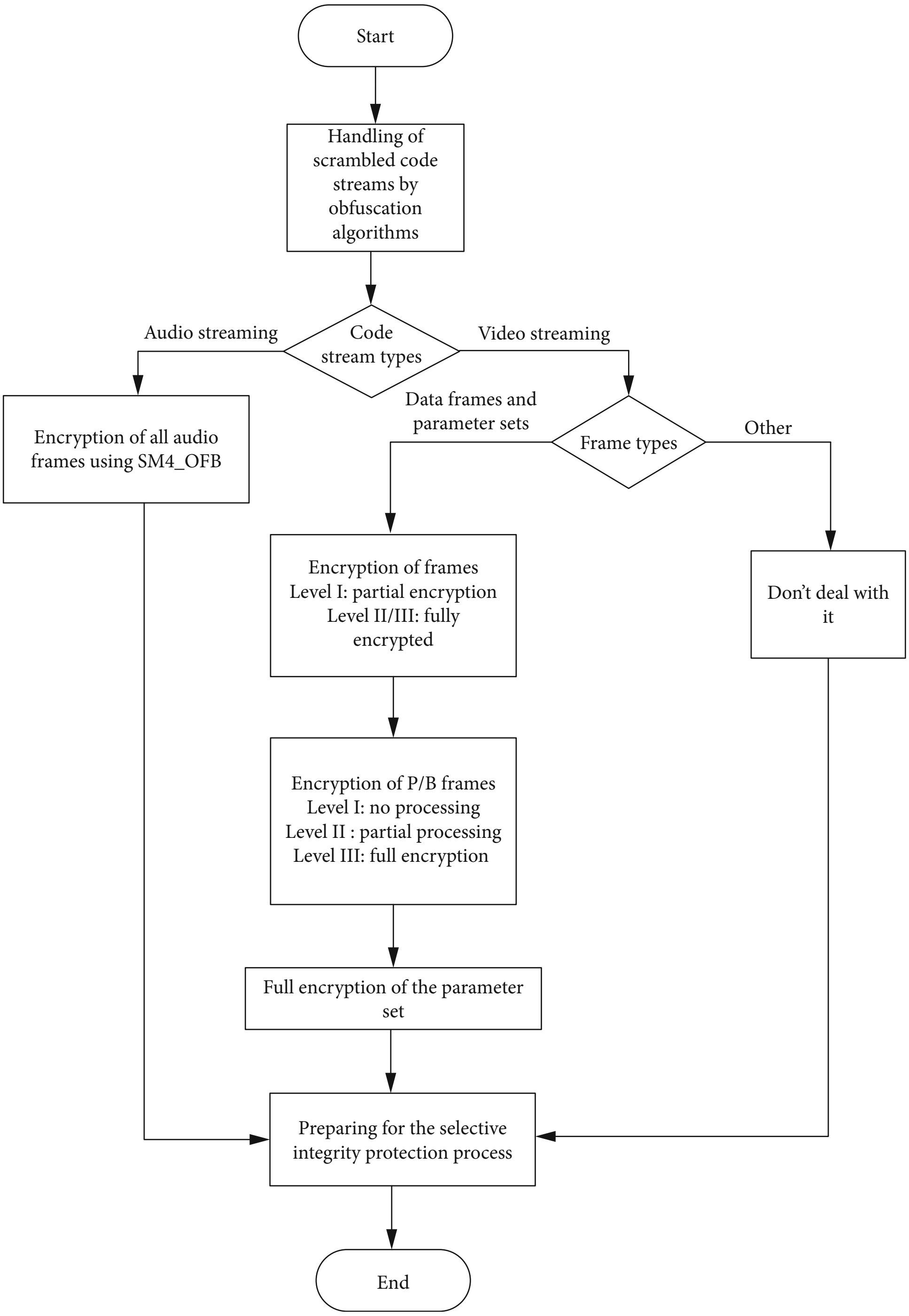

Start
Handling of scrambled code streams by obfuscation algorithms
Code stream types
Audio streaming
Video streaming
Encryption of all audio frames using SM4_OFB
Frame types
Data frames and parameter sets
Other
Encryption of frames Level I: partial encryption Level II/III: fully encrypted
Don't deal with it
Encryption of P/B frames Level I: no processing Level II : partial processing Level III: full encryption
Full encryption of the parameter set
Preparing for the selective integrity protection process
End

Figure 7: Sender side selective encryption algorithm.

4. Experiment and Analysis

4.1. Experiment. In this section, we will test the encryption and decryption time of the SM4 algorithm of the autonomous trustworthy monitoring system and other algorithms in the same environment, the encryption and decryption efficiency of the core part of data encryption, the performance of the blockchain system, and the overall performance of the system. The overall performance of the system includes the operating memory of the system, the memory occupied by the video after processing, and the response time of the system. The main purpose is to compare the overall performance of the system with the performance of the traditional system. Finally, we will analyze the experimental results and draw a conclusion. The process is as follows.

In our experiment, we use the SM4 algorithm as the core algorithm of the encryption design. In order to show that SM4 is the best algorithm of this encryption design, we compare it with AES, DES, SHA1, ECC, and RSA in encryption and decryption time in the same environment. Then, since this

Table 2: Definition of safety strength.

Level	Safety strength	Encryption range	Integrity protection range
Grade I	General	Full encryption of the parameter set, partial encryption of frame I	—
Grade II	Higher	Full encryption of frame I and parameter set, partial encryption of P/B frames	Calculation of HMAC for frame I
Grade III	Highest	Full encryption of I/P/B frames, parameter sets	Compute HMAC based on top-of-tree summary for frame I

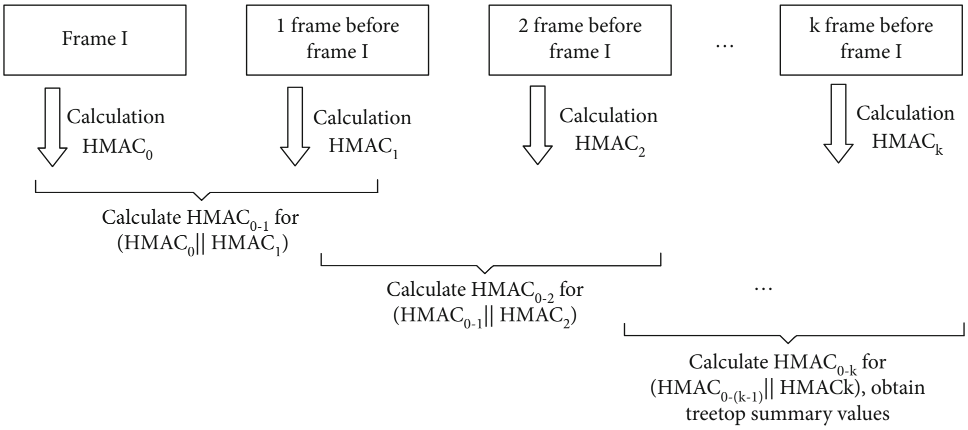

Frame I
1 frame before frame I
2 frame before frame I
…
k frame before frame I
Calculation $HMAC_0$
Calculation $HMAC_1$
Calculation $HMAC_2$
Calculation $HMAC_k$
Calculate $HMAC_{0-1}$ for ($HMAC_0$|| $HMAC_1$)
Calculate $HMAC_{0-2}$ for ($HMAC_{0-1}$|| $HMAC_2$)
…
Calculate $HMAC_{0-k}$ for ($HMAC_{0-(k-1)}$|| HMACk), obtain treetop summary values

Figure 8: Treetop summary algorithm.

system uses selective encryption, we use different encryption methods for different types of data and different security strengths. We divide the encryption strength into three levels, among which the level I security intensity is general and the level III security intensity is the highest. Because the encrypted information obtained from level I security encryption can be easily leaked, if it is used alone, it will seriously affect the security of the system. As a result, this information cannot be used alone. All things considered, we choose to compare the level III security encryption with selective encryption to analyze the execution efficiency of the encryption and decryption process. To assess blockchain performance, we adopt the caliper testing framework. First, we define the test set and then conduct performance tests against the affiliate chain we adopt. In a series of test results, we obtain the information we need to prove that the performance of the adopted blockchain meets the industry blockchain standard. Finally, we compare the overall performance of the system with that of the traditional system so as to show that our system is better than the traditional system.

For a video monitoring system, the primary goal is to ensure that the system has sufficient security, and the second goal is to achieve as high of efficiency as possible. In order to test the autonomous trustworthy video monitoring system, we use Fabric to construct our blockchain system. Fabric adopts a loosely coupled design and modularizes components such as the consensus mechanism and identity verification, which makes it easy to choose the appropriate modules according to the application scenarios during application. In addition, Fabric also adopts container technology to run Chaincode in Docker, thus enabling smart contracts to be written in almost any high-level language. We select MySQL as the offchain storage. The detailed software and hardware development environment is shown in Table 3.

A key characteristic in evaluating whether an encryption algorithm is the best for a given environment is the processing time, including both the encryption time and decryption time. Monitoring systems generally use AES, DES, RSA, SHA1, ECC, and other international cryptographic algorithms for encryption; however, SM4 is a domestic cryptographic algorithm recognized by the National Cryptography Bureau. SM4 has the advantages of a high security level and can increase the difficulty of code stream analysis and cracking; therefore, we choose to use AES, DES, RSA, SHA1, ECC, and SM4 for comparison purposes. In the first instance, we test the encryption and decryption time of the SM4, AES, DES, SHA1, ECC, and RSA algorithms in the same experimental environment.

Since the operation of the system is affected by many factors, each experiment will be conducted 5 times, and the average value is taken as the final result value. Table 4 represents the time comparison of the first 100 I frames of data (approximately 78 MB) of the same monitoring video sample with encryption and decryption.

The table shows that the encryption time is shorter than the decryption time, and the SM4 algorithm has the lowest encryption time and decryption time. Thus, it can be concluded that SM4 is the best choice among these several encryption algorithms.

Second, we test the core part of the encryption design of the system. In order to ensure the authenticity and reliability

Table 3: The experimental environment.

Name	Software and hardware environment
CPU	i7-10875H
GPU	RTX2080SMQ
Memory of a single PC	32 GB
Operating system	Ubuntu 18.04
Blockchain	Fabric 2.2
Relational database	MYSQL 5.5

Table 4: Encryption and decryption times for each algorithm.

	Encryption time (s)	Decryption time (s)
SM4	24.42	24.78
SHA1	25.69	25.96
ECC	25.45	26.10
AES	26.87	27.07
DES	24.56	24.97
RSA	25.74	26.23

of the results, we encrypt and decrypt the different-sized monitoring video data 50 times each using the SM4 algorithm with level III encryption and selective encryption and obtain the relationship between the volume of encryption and decryption data and the running time in the strength of level III encryption and selective encryption. The results are shown in Figure 9.

As shown in Figure 9, selective encryption has a short runtime, and the system performs efficiently. We can conclude that at different intensities, the full encryption or partial encryption of different types of data can not only guarantee the security of the system but also improve the performance of the system.

We then use Caliper to test the performance of our blockchain network. Caliper is a blockchain performance testing framework that tests the performance of a blockchain network with a defined test set and generates the results in a test report. Caliper supports the testing of transaction success rate, throughput (TPS), transaction latency, and resource consumption performance metrics. The data after many experiments are shown in Figure 10.

TPS is the number of transactions a system can process per second. It is calculated as TPS = number of concurrencies /average response time. It is not always the case that a higher TPS is better; instead, this should be evaluated on a case-by-case basis. Public chains have a large number of users and nodes, which require a high concurrent TPS to meet the underlying technical requirements; however, private chains and alliance chains do not need a particularly high TPS and only need to meet the industry demand. As seen in Figure 10, the throughput peaks at 5000 transactions as the number of transactions increases and then starts to decrease. The transaction latency, however, increases as the number of transactions increases, but the magnitude of the increase decreases as the number of transactions increases.

Finally, we test the main performance of the system, including the running memory, the memory occupied by the processed video, and the response time of the system; and compare the main performance of this system with the traditional system.

First, we test the running memory of the system, which refers to the memory when the system is running, the results of which are shown in Figure 11.

Figure 11 shows that, in general, the runtime memory size shows an increasing trend as the number of transactions increases. The running memory of this system is slightly smaller than that of the traditional method as it takes less memory from the user when running; therefore, the user can have more memory to run other programs at the same time.

Figure 12 is the result of the memory occupied by the video after system processing. In order to ensure the accuracy of the experiment, the system and the traditional system process the same monitoring sample.

Figure 12 shows that there is little difference between this system and the traditional system for sample processing, but the sample capacity after this system is applied is still slightly smaller; therefore, we can see that encryption has little effect on the capacity size of the sample itself.

The response times of both systems are then tested. The response time is the time it takes for a computer to respond to a user's input or request. Again using uniform variables, this system is processed on the same monitoring sample as the conventional system, but since there are many determinants of the system response time, we conduct several experiments and average the results after removing the highest and lowest values.

Figure 13 shows that the response times of both this system and the conventional system increase as the size of the monitored samples increases, but the response time of this system is shorter than that of the conventional system for the same sample size.

In summary, this system outperforms the conventional system in terms of operating memory and system response time. The system itself does not have much impact on the memory occupied by the samples.

4.2. Analysis

4.2.1. Performance. The blockchain standards we use are referenced in the Technical Reference Framework for a Trusted Blockchain, Core Requirements and Evaluation Metrics for a Trusted Blockchain, Functional Evaluation Methodology for a Trusted Blockchain, Performance Benchmarking Methodology for a Trusted Blockchain, and Blockchain Security Evaluation Metrics and Testing Methodology for a Trusted Blockchain, which are shown in Table 5.

The network test results of the system are shown in Table 6. The transaction success rate is 100%, the average transaction latency is 0.67 s (the maximum transaction latency is 2.53 s and the minimum transaction latency is 0.06 s), and the throughput is 214.8 TPS.

The experiments indicate that our blockchain performance meets industry standards.

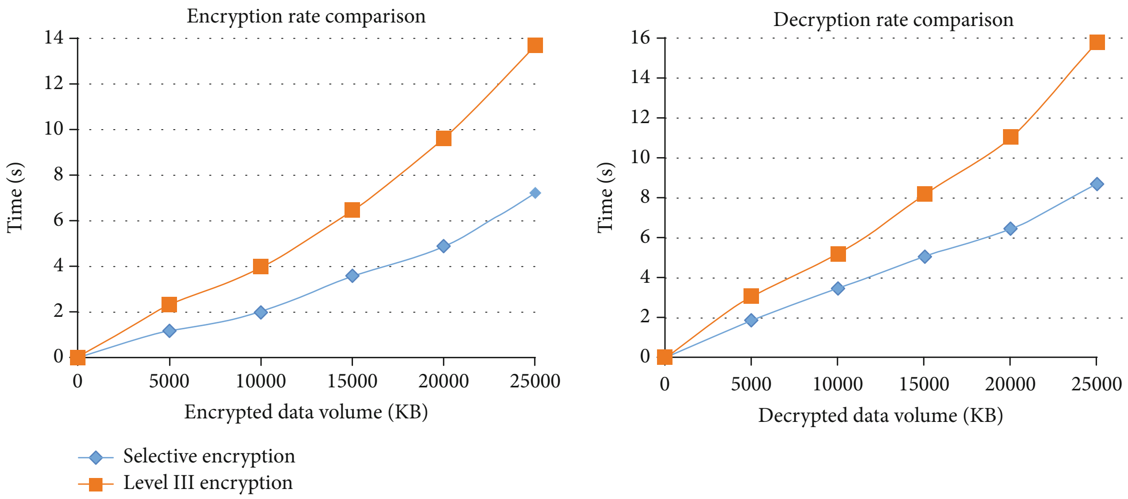


Figure 9: Encryption and decryption rate comparison.

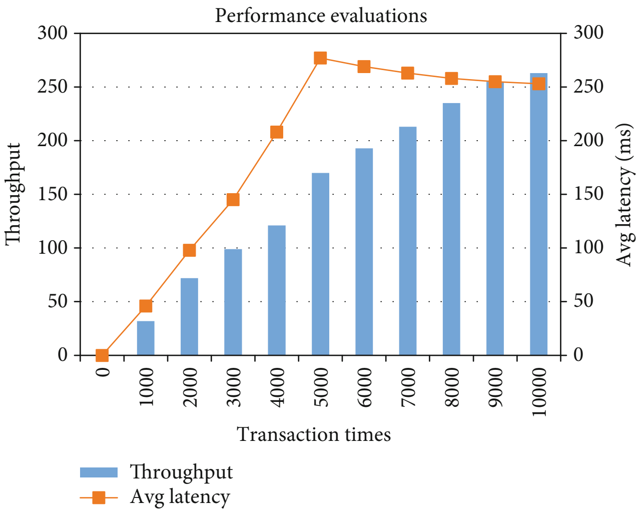


Figure 10: Performance evaluations.

4.2.2. Security

(1) Anonymity. In the video data sharing process, we protect the privacy of our users via data anonymization. Users join social groups and share video information as members of the group. Only the administrator, the users in the local cloud, and the certification center can obtain the users' private information. The blockchain management platform provides authentication functions. In addition, the authentication function can be moved forward to achieve access network authentication, or a secondary authentication system can be constructed to achieve reauthentication. For secondary authentication, according to the SM4 algorithm and the characteristics of the blockchain platform, authentication can reside in different locations such as on-chain and in business data centers to meet the actual authentication requirements in terms of performance and latency. In addition, except for the administrator and the authentication center, it is impossible to identify the users' data information through a certain video record. The ownership of video data cannot be identified by the index number. Since random numbers are added during the storage index generation process, the index of each piece of video data is different. In addition, the identity-related information is stored in a data card, thereby protecting the video data using hardware, and the information in the smart card cannot be read without authorization. For the transmission of monitoring video, similar to the sharing of data information, users use group member IDs to protect privacy during transmission.

(2) Confidentiality. In this system, the strength of the cryptographic algorithm used is high. Commonly used video encryption systems often adopt international cryptographic algorithms such as AES, RSA, and SHA1. This system uses the independently designed SM4 commercial cryptographic algorithm, which is designed to possess a high security level using a multiround cyclic operating mode, and the operating overhead is high, increasing the difficulty of analyzing and cracking the code stream, protecting the confidentiality of video data and preventing illegal tampering and destruction. The encryption design of SM4 greatly enhances the security of the system. Its security strength is no less than that of international algorithms and is independently controllable, making it suitable for deployment in government, finance, energy, and other industries. In the blockchain data sharing platform, the blockchain platform generates a key every time it receives data and distributes the key to the terminal securely. The information is encrypted by the recipient's public key or symmetric key and then chained and shared. Therefore, only the receiver with the corresponding private key can decrypt the information. Each symmetric key is different. Each symmetric key is only responsible for encrypting one piece of video information, which improves the confidentiality of video information. Regarding key distribution, it is necessary not only to protect the confidentiality of the key but also to ensure the integrity, verifiability, correctness, and controllability of the key. In special cases, the key also guarantees the nonrepudiation of both parties in

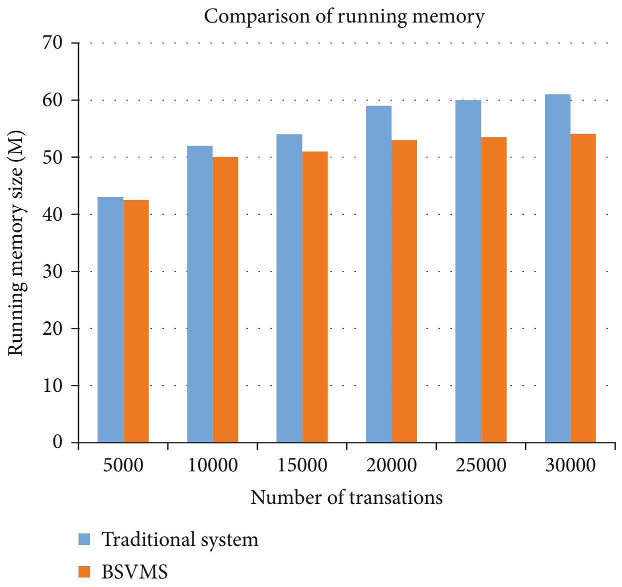


Figure 11: Running memory comparison.

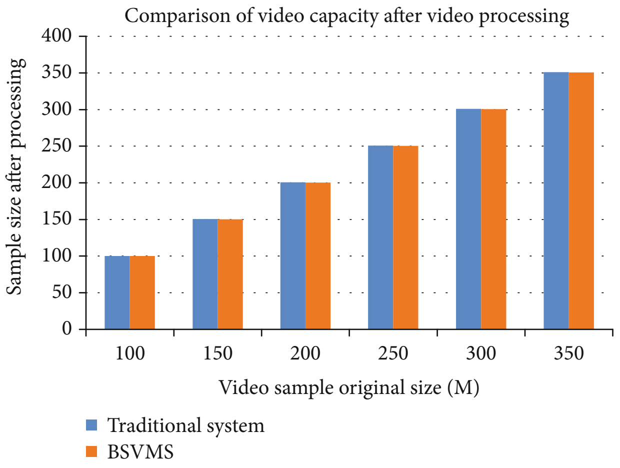


Figure 12: Video capacity comparison after video processing.

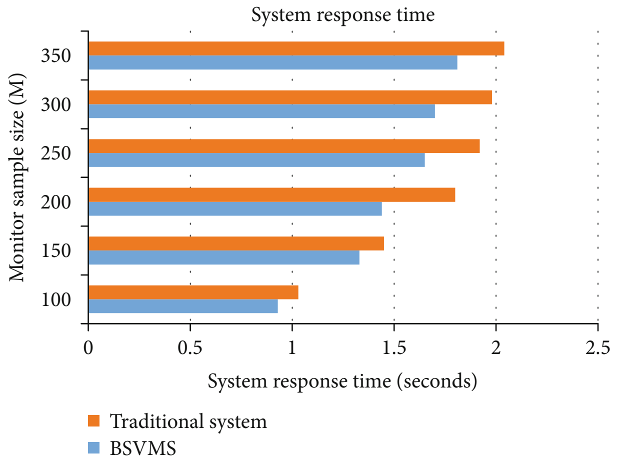


Figure 13: System response time comparison.

communication. According to the exchange method of key information, the key distribution methods are center-based key distribution and authentication-based key distribution. In terms of key storage, the key should be stored in a secret form, and the operating password should be strictly protected to ensure the confidentiality, authentication, and integrity of the key and prevent the key from being leaked and tampered with. In terms of key update and destruction, a new key must be generated after the key has reached its expiration date. The key can be updated using a batch key mode; that is, multiple keys can be injected at a time, and the update can be performed in the form of one key being effective and another key being invalid. Regarding the transmission of monitoring video, the monitoring video is encrypted by the receiver's public key, ensuring that only the corresponding receiver can read the information.

(3) Access Control. The blockchain platform provides authentication functions. In addition, the authentication function can be moved forward to achieve access authentication, or a secondary authentication system can be built to achieve reauthentication. For secondary authentication, according to the SM4 algorithm and the characteristics of the blockchain platform, the authentication can reside in different locations on the chain, in a business data center, etc., to meet the actual authentication requirements in terms of performance and delay. Through blockchain authority management, users can not only view their own monitoring information but also share monitoring information with other authorized entities. Before video information can be used, the identity of both the administrator and the user needs to be verified. Access to different entities is password-controlled and user-defined. Without the user's authorization, no entity can access the user's video monitoring information.

(4) Integrity and Authenticability. The administrator must generate a digital signature for video monitoring after verification. The user verifies the confirmation of the digital signature and the monitoring video and further generates a digital signature, i.e., a double signature. Before data transmission, users will also digitally sign their video information. Without the signer's private key, no entity can forge the entity's digital signature. Since the digital signature is only generated by a specific signer, any information with a digital signature can be authenticated. If a piece of video information is tampered with, the receiver can find it through verification.

(5) Scalable Security Levels. The traditional encryption system only encrypts audio and video without distinguishing the security level. The system fully considers the structural characteristics of audio and video data; differentiates between video data I frames, video data P/B frames, video parameter sets, and audio data frames; and integrates various security techniques such as confusion scrambling, selective encryption, and selective integrity protection to provide different levels of security protection capabilities to meet the needs of a wide range of encrypted video conferencing scenarios.

Table 5: Blockchain industry standards.

Rule requirements	Rule items	Requirements
Test scenarios	Stress test	The number of transactions received per second is basically the same as the number of uploads, and the success rate of uploads is higher than 95%
	Spike test	The number of transactions received per second is significantly higher than the number of uploads, and the success rate of uploads is higher than 75%
	Stability test	Low-load operation with no system crashes
Result items	Performance indicators	Uplink success rate (>95%) TPS (200-300) Average transaction latency (<1 s)

Table 6: Blockchain performance test results.

Name	Requirement
Success rate	100%
Average latency	0.67 s
Throughput (TPS)	214.8 TPS

5. Conclusions

In this paper, based on the commercial cryptography algorithm and blockchain technology, we modify the visual sensor and realize the encryption processing of an image during the imaging process of a camera by encrypting the visual transformation network to solve the video monitoring security problem from the root. We first elaborate on the importance and advantages of video monitoring and analyze the security threats faced in video monitoring systems and related solutions. In the second part, we introduce the current status of domestic and foreign research on video monitoring security. In the third part, we propose an autonomous trustworthy video monitoring system solution based on the commercial cryptography algorithm for the security problems faced by a video monitoring system and design a new visual sensor to replace the traditional lens imaging device to complete the encryption of an image during the imaging process. We research blockchain technologies in depth and design a complete solution for video monitoring to complete identity authentication and encryption design on the chain to realize the interaction between the key network and the blockchain part. Finally, we test the encryption and decryption efficiency of the core part of the data encryption, the performance of the blockchain system, and the overall performance of the system. We then analyze the performance of the blockchain and several aspects of the system such as its anonymity, confidentiality, access control, integrity, and authenticability to ensure that the video monitoring system is secure and trustworthy.

However, the system efficiency is not efficient enough and there are "information silos" between blockchains. The aims of further works are outlined as follows.

(i) To improve the efficiency of the encryption and decryption of video data on the side of mobile terminals using lightweight cryptography algorithms

(ii) To construct a cross-domain trustworthy monitoring system based on blockchain technologies and commercial cryptography algorithms

Data Availability

The monitoring video data used to support the findings of this study have not been made available because the data for this experiment was collected for real and involves numerous private information, such as faces and address information.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] T. Wang, "Network video monitoring system status and security issues," *Network Security Technology and Application*, no. 9, pp. 146-147, 2020.

[2] C. Jiang, "Application of thermal imaging body temperature measurement camera in epidemic prevention and control period," *Electronic production*, no. 8, pp. 31-32, 2020.

[3] H. Gao, X. Qin, R. J. Duran Barroso, W. Hussain, Y. Xu, and Y. Yin, "Collaborative learning-based industrial IoT API recommendation for software-defined devices: the implicit knowledge discovery perspective," *IEEE Transactions on Emerging Topics in Computational Intelligence (TETCI)*, pp. 1–11, 2020.

[4] Y. Huang, H. Xu, H. Gao, and W. Hussain, "SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.

[5] K. Huang, X. Chen, Y. Tang, and T. Tan, "An overview of intelligent video monitoring technology," *Journal of Computer Science*, vol. 38, no. 6, pp. 1093–1118, 2015.

[6] L. Zhang, Y. Zou, W. Wang, Z. Jin, Y. Su, and H. Chen, "Resource allocation and trust computing for blockchain-enabled edge computing system," *Computers & Security*, vol. 105, 2021.

[7] L. Zhang, Z. Zhang, W. Wang, Z. Jin, Y. Su, and H. Chen, "Research on a covert communication model realized by using smart contracts in blockchain environment," *IEEE Systems Journal*, pp. 1–12, 2021.

[8] Q. Xie, "Application and development trend of intelligent video monitoring system," *Shanxi Coal Mine*, vol. 38, no. S1, pp. 31–33, 2019.

[9] W. Gao, "The current situation and development trend of network video monitoring system," *Information and Computer (Theory Edition)*, vol. 375, no. 5, pp. 178-179, 2017.

[10] S. Li, "Analysis of the key points of the application of new technologies in the security industry in the construction of safe cities," *Information Communication*, no. 10, pp. 130-131, 2020.

[11] S. Ma, "Smart cities: connotation, dimensions, evaluation and practice," *Frontiers of Foreign Social Sciences*, no. 11, pp. 64–72+96, 2020.

[12] X. Xu and X. Liu, "A brief description of the organization and implementation plan for the construction of "snow bright" project," *China Cable TV*, no. 11, pp. 1296–1298, 2020.

[13] H. Gao, L. Kuang, Y. Yin, B. Guo, and K. Dou, "Mining consuming behaviors with temporal evolution for personalized recommendation in mobile marketing apps," *Mobile Networks and Applications (MONET)*, vol. 25, no. 4, pp. 1233–1248, 2020.

[14] C. Bo, "Research on the status and development trend of network video monitoring system," *China New Communication*, vol. 20, no. 13, p. 78, 2018.

[15] S. Zhang, "Video monitoring system development status and trends," *Electronic Paradise*, no. 9, p. 0005, 2018.

[16] Y. Duan, "The current situation and development trend of video monitoring system," *Technology Wind*, no. 29, p. 87, 2019.

[17] S. Wang, "The application and development direction of video monitoring image detection under video monitoring system," *China High-Tech*, no. 3, pp. 106–108, 2019.

[18] K. Al-Marashda, "Video security assurance framework based on efficient Joint Cryptography Compression approach," in *Electronics, Circuits, and Systems (ICECS), IEEE 20th International Conference on*, pp. 76-77, Abu Dhabi, 2013.

[19] M. Meng, "Research on network security assessment technology based on penetration testing," *Automation and Instrumentation*, no. 10, pp. 182–184, 2018.

[20] X. Wang, "Network video monitoring system status and development," *Modern Industrial Economy and Informatization*, vol. 9, no. 8, pp. 112-113, 2019.

[21] H. Gao, C. Liu, Y. Li, and X. Yang, "V2VR: reliable hybrid-network-oriented V2V data transmission and routing considering RSUs and connectivity probability," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3533–3546, 2021.

[22] H. Gao, W. Huang, and Y. Duan, "The cloud-edge based dynamic reconfiguration to service workflow for mobile ecommerce environments: a QoS prediction perspective," *ACM Transactions on Internet Technology*, vol. 21, no. 1, pp. 1–23, 2021.

[23] G. Giusseppe and M. Saverio, "Synchronizing high dimensional chaotic systems via eigenvalue placement with application to cellular neural networks," *International Journal of Bifurcation and Chaos*, vol. 9, no. 4, pp. 705–711, 1999.

[24] G. Giusseppe and M. Saverio, "Synchronization of high-dimensional chaos generators by observer design," *International Journal of Bifurcation and Chaos*, vol. 9, no. 6, pp. 1175–1180, 1999.

[25] T. Goldstein and S. Osher, "The split bregman method for L1regularized problems," *SIAM Journal on Imaging Sciences*, vol. 2, pp. 323–343, 2009.

[26] S. M. Rahman, M. A. Hossain, H. Mouftah, A. El Saddik, and E. Okamoto, "Chaos-cryptography based privacy preservation technique for video surveillance," *Multimedia Systems*, vol. 18, no. 2, pp. 145–155, 2012.

[27] J. Wang and G. L. Smith, "A cross-layer authentication design for secure video transportation in wireless sensor network," *International Journal of Security and Networks*, vol. 5, no. 1, pp. 63–76, 2010.

[28] H.-Y. Huang, C.-H. Yang, and W.-H. Hsu, "A video watermarking algorithm based on pseudo 3D DCT," in *IEEE Symposium on Computational Intelligence for Image Processing*, pp. 76–81, Nashville, TN, USA, 2009.

[29] S. Zhang, Y. Shi, X. Ren, B. Dou, M. Chao, and Z. Zhou, "Research on video conference encryption technology," *Communications Technology*, vol. 53, no. 10, pp. 2520–2527, 2020.

[30] X. Ma, H. Gao, H. Xu, and M. Bian, "An IoT-based task scheduling optimization scheme considering the deadline and cost-aware scientific workflow for cloud computing," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, 2019.

[31] J. Zhang, B. Zeng, Y. Shen, M. Zhang, and Z. Chen, "Security audit technology of ultra high definition video content," *Communications Technology*, vol. 53, no. 8, pp. 2049–2054, 2020.

[32] Y. Y. Chun, S. Guo, H. Xing, and P. Yang, "Research and analysis on security of public security video private network," *Communications Technology*, vol. 53, no. 9, pp. 2292–2296, 2020.

[33] T. Long and W. Haili, "Security risks and technical solutions of video monitoring system," *Journal of Xi'an College of Arts and Sciences (Natural Science Edition)*, vol. 23, no. 2, pp. 68–71, 2020.

[34] Z. Zhang, Z. Wu, B. Zeng, Y. Shen, and B. Li, "Security enforced solution for video monitoring system networking application," *Communications Technology*, vol. 52, no. 1, pp. 207–212, 2019.

[35] S. Yuan-bing and Z. Shu-li, "Research of cryptographic application on video monitoring based on 5G edge computing," *Communication Technology*, vol. 53, no. 5, pp. 1224–1230, 2020.

[36] X. Yang, S. Zhou, and C. Min, "An approach to alleviate the sparsity problem of hybrid collaborative filtering based recommendations: the product-attribute perspective from user reviews," *Mobile Networks & Applications*, vol. 25, no. 2, pp. 376–390, 2020.