Data Security Protection Mechanism of Video and Image Feature Modeling Based on Domestic Crypto Algorithm

Yueqiang Tu

The Third Research Institute of the Ministry of Public Security, Shanghai, 201204, China

*Corresponding author’s e-mail: tuyueqiang@gaskmp.cn

Abstract: Video and image monitoring is increasingly appearing in our home, travel and other aspects. Through video and image analysis and comparison of video and image monitoring data, it can provide strong analysis support capabilities for social security prevention and control, traffic command, safety production and so on. Video and image feature modeling is a necessary prerequisite for video and image analysis and comparison. Video and image feature modeling forms video and image feature data. Video and image feature data reflects the most essential information of various elements such as people, vehicles and objects. However, video and image data is easy to be damaged, changed and leaked in the process of collection, aggregation, analysis, modeling and storage. Facing data security risks. This paper proposes a set of video and image feature modeling data security protection mechanism based on domestic algorithm to realize the whole process encryption protection of data acquisition, transmission and storage.

1. Introduction

With the rapid development of Internet of things, cloud computing, big data, artificial intelligence and other new generation of information technology, as well as the hardware cost reduction and network performance improvement brought by new technology breakthrough, video and image monitoring has been rapidly popularized and developed. From the "Xueliang Project" [1] and other urban monitoring and security systems to smart home products represented by smart camera door locks, video and image monitoring is deeply affecting our lives. The video and image data formed by video and image monitoring contains a lot of feature information such as personnel appearance, personnel behavior, vehicle appearance and vehicle behavior. Through the collection, aggregation, analysis and feature modeling of video and image data, the video and image feature data is formed. Video and image feature data reflects the most essential information of people, vehicles, objects and other elements. Through the comparison of video and image feature data, it can provide strong analysis support ability for social security prevention and control, traffic command, safety production and so on.

Just because video and image data or video and image feature data play such an important role on above situation, once these data are destroyed, changed and leaked, it will cause irreparable losses to personal privacy, public security, etc. And even provide opportunities for potential criminals. The security protection of video and image data or video and image feature data is particularly important.

Cryptography is the core technology to ensure information security. Cryptography can achieve confidentiality, integrity, authenticity and non-repudiation of related entities and behaviors. The core of cryptographic technology is cryptographic algorithm. Since 2012, China has released a series of national standard domestic cryptographic algorithms (SM crypto algorithm), including asymmetric cipher algorithm represented by SM2 algorithm [2], digest algorithm represented by SM3 algorithm [3],
symmetric cipher algorithm represented by SM4 algorithm [4]. These algorithms are widely used in big data security, Internet network communication, public security system, bank information system, blockchain, e-government and other fields.

Compared with other existing international algorithms, SM crypto algorithm has great advantages in encryption and decryption speed, security strength and so on. For example, in the case of the same hardware and software conditions, the encryption and decryption speed of SM4 algorithm is faster than that of AES algorithm; SM3 algorithm has higher security strength than SHA-256 algorithm; The speed of key generation and encryption and decryption of SM2 algorithm is faster than that of RSA algorithm [5]. Therefore, this paper uses SM2 algorithm, SM3 algorithm and SM4 algorithm to solve the security problem of video and image data or video and image feature data.

2. Related work

Some scholars [6] - [8] explored the security encryption and decryption of data collection, transmission, storage and other processes, and proposed the security protection methods for these links. However, these literatures did not comprehensively consider the whole life cycle security of data, and only optimized one link.

Hussain I et al. [9] proposed a scheme of data protection by RSA and DES encryption technology. Sun B Y et al. [10] proposed an AES-GCM authentication encryption (AE) method. The core of AES-GCM is to provide a counter secret (CTR) mode of block cipher and GHASH authentication and integrity protection. These methods are all international common cipher algorithms, we can improve it by SM crypto algorithm in the encryption and decryption efficiency and security intensity.

Kakkad V et al. [11] proposed a method based on biometric authentication and data encryption to obtain the specific biometrics of customers and generate two keys, public key and private key. The private key is used to encrypt plain text into ciphertext. Whenever users want to access data, they can use the public key to decrypt. This method not only has identity authentication, but also has asymmetric encryption algorithm to ensure data security. However, from the perspective of efficiency, it can simplify the encryption and decryption process in a specific scenario and improve the efficiency of encryption and decryption.

In order to effectively prevent the information leakage in the process of privacy information collection, a new hardware and software encryption structure system is designed [12]. The hardware part mainly designs the connection mode of CPU and bus; The software of the system is designed according to the hardware structure, and the software flow is designed through protocol layering, algorithm construction, code stream file construction and key setting. However, this method of privacy information collection security protection through SM crypto algorithm needs coordinated control of PCI controller, encryption chip, decryption chip and pulse transformer. It is a strongly integration of software and hardware, and unable to adapt to the elastic and scalable cloud environment.

3. Data security mechanism of video and image feature modeling

3.1. Analysis of data security requirements for video and image feature modeling

3.1.1. Data security protection in the whole process of video and image feature modeling

Design video and image data collection, aggregation, analysis, modeling process, and design data security protection methods for each link of the process. According to the characteristics of SM crypto algorithm, combined with the requirements of encryption and decryption efficiency and security protection strength, the video and image data encryption and decryption methods are comprehensively considered. The applicability of SM crypto algorithm involved in this paper is shown in Table 1.
Table 1. Applicability of SM crypto algorithm involved in this paper.

| Algorithm type     | Key length          | Algorithm application                                                                 |
|--------------------|---------------------|----------------------------------------------------------------------------------------|
| SM2 algorithm      | Asymmetric cryptographic algorithm  | Public key 64 Bytes Private key 32 Bytes                                                  |
|                    |                     | It is mainly used to generate message signature to ensure the non repudiation of data.   |
| SM3 algorithm      | Digest algorithm    | -                                                                                      |
|                    |                     | It is mainly used to calculate digest value to ensure the integrity of data.             |
| SM4 algorithm      | Symmetric cipher algorithm | 16 Bytes                                                                            |
|                    |                     | It is mainly used to encrypt and decrypt data to ensure the confidentiality of data.     |

3.1.2. Intra application encryption and decryption
For the scenario of transmission and exchange of video and image or other data between different nodes in the same application, under the premise of ensuring security, the efficiency of encryption and decryption is the primary consideration, while the demand for identity authentication in the same application is relatively low. Therefore, we can consider the encryption and decryption of video and image or other data.

3.1.3. Inter application encryption and decryption
For the scenario of transmission and exchange of video and image or other data between different applications, the encryption scheme needs to focus on identity authentication (non repudiation of data, etc.) and data integrity, because the transmission involves an external environment that may be unsafe.

3.1.4. Database data encryption and decryption
The database is the system that all the core assets such as video and image data or video and image feature data are finally gathered, and the data encryption in the database is a necessary protective measure. Database data encryption includes the encryption of structured data and unstructured data. After encryption, the data is stored in the form of ciphertext, which prevents the direct exposure of data. At the same time, the access control of encrypted data is enhanced, which greatly reduces the risk of data leakage and malicious damage.

3.2. Video and image feature modeling process and data security design

3.2.1. Data security protection in the whole process of video and image feature modeling
Camera, AR glasses, law enforcement recorder and other front-end equipment capture personnel, vehicles, objects and other video and image data, which are stored in the database through the data access, processing, organization and other processes of video and image receiving service. The database can store original video and image data, analysed structured and unstructured data, etc. The multi algorithm and multi version management service has the management function of multiple modeling engines, and also has the scheduling and management function of modeling tasks. The multi algorithm and multi version management service reads the pictures in the database, schedules the background modeling engine to model the pictures, forms the feature data after modeling, and stores the feature data in the database. The process of video and image feature modeling is shown in Figure 1.
Figure 1. Video and image feature modeling process.

In the above process, for the video and image data or video and image feature data transmission within the system (between different nodes), intra application encryption and decryption methods are adopted, such as data transmission between each application node of video and image receiving service and data transmission between each application node of multi algorithm and multi version management service; For cross system transmission of video and image data or video and image feature data, inter application encryption and decryption is adopted, such as data transmission between front-end system and video and image receiving service, data transmission between modeling engine and multi algorithm multi version management service; Video and image data or video and image feature data should also be encrypted in the process of storage and reading from the database.

3.2.2. Intra application encryption and decryption

The process of intra application data encryption and decryption includes two roles: data sender and data receiver.

The message plaintext of node 1 of application server is symmetrically encrypted by SM4 to form message ciphertext. After encryption, the same key is used to generate message digest based on SM3 algorithm, and the digest value is added at the end of the ciphertext as the output of data sender. The process of intra application data encryption is shown in Figure 2.
After receiving the data sent by the sender, node 2 of the application server first checks the data integrity, uses the same key as the sender to calculate the ciphertext with SM3 algorithm, and compares the calculated digest value with the digest value received from the sender. If it is consistent, the data integrity check is successful. If it is inconsistent, it means that the data is tampered in the transmission process. After passing the data integrity check, SM4 algorithm is used to calculate the ciphertext with the same key as the sender to get the plaintext. The process of intra application data decryption is shown in Figure 3.
3.2.3. Inter application encryption and decryption

The process of inter application encryption and decryption covers two roles: data sender and data receiver, both of which have a pair of public and private key pairs (SM2 algorithm).

The application 1 server is used as the sender to obtain the public key of the receiver, generate the session key of communication, use the session key to encrypt the message plaintext with SM4 algorithm to form the message ciphertext, and then use the public key of the receiver to encrypt the session key with SM2 algorithm. The digest value is calculated for the message ciphertext and the encrypted session key with SM3 algorithm, and then the generated digest value is signed by SM2 algorithm using the private key of the sender. The encrypted message, the encrypted session key and the signature value are sent to the receiver together. The process of inter application data encryption is shown in Figure 4.

![Figure 4. The process of inter application data encryption.](image)

After the application 2 server receives the data from the sender, it uses the sender's public key to calculate the received signature value by SM2 and decrypt it to get the digest value. At the same time, it calculates the digest of the received session key ciphertext and message ciphertext by SM3 algorithm and compares the two digest values to confirm whether the data is sent by the application 1 server and has not been tampered. After verification, the private key of the receiver is used to calculate and decrypt by SM2 to get the session key, and the decrypted session key is used to decrypt the message ciphertext by SM4 to get the message plaintext. The process of inter application data decryption is shown in Figure 5.
3.2.4. Database data encryption and decryption

SM4 algorithm is used to encrypt the database data. By configuring the database encryption strategy, the data that needs to be stored in the database is encrypted by SM4 algorithm to get the ciphertext. The granularity of the encryption strategy can be refined to the field level. When other authorized applications read the database data, they can automatically decrypt the field plaintext data, which makes the decryption of encrypted database data transparent. When unauthorized applications read the database, they can't spy and steal the plaintext data in the database. The database data encryption and decryption process is shown in Figure 6.

4. Conclusion

With the accelerated popularization of video and image monitoring, the amount of video and image monitoring data is growing explosively. The video and image features formed by video and image monitoring data modeling also expand the scope of personal privacy data protection. It is urgent to protect these important data. In this paper, a video and image feature modeling data security protection
mechanism based on domestic algorithm is proposed. Domestic algorithms such as SM2 algorithm, SM3 algorithm and SM4 algorithm are adopted. In the process of video and image data acquisition, aggregation, analysis, modeling and storage, taking into account the factors such as encryption and decryption efficiency, security and protection strength, this paper proposes the method of intra application encryption and decryption, inter application encryption and decryption, database data encryption and decryption, and realizes the whole process security protection of video and image feature modeling data. In the future, data security protection can be further extended in terms of granularity. At the same time, the optimization based on domestic cryptographic algorithms can also be applied to the video and image data security protection in this paper.

Acknowledgments
This paper is one of the phased achievements of the project "Research on Key Technologies of prison video data password security protection based on domestic cryptographic algorithm" (KYC 21366).

References
[1] Zhu Yanmin. (2021) Discussion on the construction of three-dimensional prevention and control scheme for "Xueliang Project" of video surveillance. Changjiang Information and Communication, 34 (03): 93-95.
[2] GB/T 35276-2017, (2017)Information Security Technology SM2 Cryptographic algorithm usage specification. People's Republic of China: National Standardization Management Committee.
[3] GB/T 32905-2016, (2016)Information Security Technology SM3 Cryptographic hash algorithm. People's Republic of China: National Standardization Management Committee.
[4] GB/T 32907-2016, (2016)Information Security Technology SM4 Block cipher algorithm. People's Republic of China: National Standardization Management Committee.
[5] Tang Shengyu, Zeng Shuishui, Zhao Meng, Liao Xinyuan, Lin Minxiang. (2020)Analysis of Cryptographic Algorithm at Home and Abroad. Information and communication, 2020 (02): 68-69.
[6] Mohd Tajammul,Rafat Parveen. (2020)Auto encryption algorithm for uploading data on cloud storage. International Journal of Information Technology: An Official Journal of Bharati Vidyapeeth's Institute of Computer Applications and Management,12(3).
[7] K Rani and R K Sagar, (2017) "Enhanced data storage security in cloud environment using encryption, compression and splitting technique," 2017 2nd International Conference on Telecommunication and Networks (TEL-NET),pp.1-5,doi:10.1109/TEL-NET.2017.8343557.
[8] Jasmin M, Beulah Hemalatha S. (2017)Security for industrial communication system using encryption/decryption modules. International Journal of Pure and Applied Mathematics, 116(15): 563-568.
[9] Hussain I, Negi M C, Pandey N. (2017)A secure IoT-based power plant control using RSA and DES encryption techniques in data link layer,2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS). IEEE, 464-470.
[10] Sung B Y, Kim K B, Shin K W. (2018)An AES-GCM authenticated encryption crypto-core for IoT security,2018 International Conference on Electronics, Information, and Communication (ICEIC). IEEE, 1-3.
[11] Kakkad V, Patel M, Shah M. (2019)Biometric authentication and image encryption for image security in cloud framework. Multiscale and Multidisciplinary Modeling, Experiments and Design, 2(4): 233-248.
[12] Huang Rongsheng, Zhang Qiankun, Li Guo, Huang Shiping. (2020)Privacy information collection process encryption system based on national secret algorithm. Automation and Instrumentation, 2020 (09): 212-215.