Research Significance of Reversible Data Hiding in Encrypted Domain under Cloud Technology

Yong-jun Kong[1,a], Min-Qing Zhang[1,b*], Si-yuan Huang[1,c], and Guang-sheng Tu[2,d]

[a] fighting_kyj@163.com, [b] api_zmq@126.com, [c] 1013581648@qq.com, [d] 1542855584@qq.com

[1]Key Laboratory of Network and Information Security under Chinese People Armed Police Force (PAP), Engineering University of PAP, Xi'an 710086, China

[2]Command College of Chinese People Armed Police Force(PAP), Hang'zhou, Chinese People, Armed Police Force

Abstract: Reversible data hiding in encrypted domain, which combines encryption technology and data hiding technology, can not only realize privacy protection of data content on open channel, but also realize reversible embedding of information, which is of great significance to meet the increasingly complex application requirements in the cloud era. This paper mainly discusses the research significance of reversible data hiding in encrypted domain from four application scenarios: encrypted data management, covert communication of intelligence, military cooperative operation, and technology fusion innovation.

Keywords: Information security; Reversible data hiding; Cloud environment; Image processing; Encrypted Domain

1 INTRODUCTION

With the continuous development of cloud computing, machine learning, data mining and multimedia technologies, the popularity of cloud technology[1] provides users with convenient services such as network storage and network computing. More and more users choose to upload data to the cloud storage or rely on the cloud to complete specific tasks, thus saving local storage costs or improving computing power. However, while enjoying the convenience brought by cloud technology, the frequent occurrence of privacy data leakage[2][3] within the framework of this technology cannot be ignored. In view of the threat of privacy disclosure, more and more cloud applications require encryption technology[4] to protect sensitive data in all aspects of transmission, storage and calculation. In combination with actual needs in the cloud space environment, how to make more efficient use of encrypted data has become a focus of network security research in recent years[5]-[7].

Reversible Data Hiding in Encrypted Domain (RDH-ED)[8] refers to the process in which encrypted data is used as the carrier to be embedded and secret information is embedded in the basis of protecting data content for lossless transmission. For the carrying secret text embedded with secret information, it can not only ensure the accurate extraction of secret information, but also realize the lossless recovery of original data after decryption. Combined with the application environment of explosive growth of encrypted data in cloud space, it has

ICIDC 2023, June 02-04, Nanchang, People's Republic of China

DOI 10.4108/eai.2-6-2023.2334672

great application potential in the field of secure communication. For example, data annotation, traceability tracking, integrity verification, access control, content distribution, etc. In particular, this technology has important application prospect and research value for military operations, telemedicine, judicial forensics and other fields that require high accuracy of carrier content[9]-[11]

2 RESEARCH SIGNIFICANCE

Reversible data hiding in encrypted domain, as a fusion and cross technology of encrypted signal processing and reversible data hiding technology,combined with the characteristics of distributed data storage and multi-user processing on the cloud, secret message transmission using encrypted images as the carrier can further realize a series of functions such as heterogeneous data interaction in the network space, data disaster protection, separable content access control, and sub-threshold message transmission, which is of great significance to meet the increasingly complex application requirements in the cloud era. In view of the technical characteristics of reversible data hiding in encrypted domain, the research significance is mainly reflected in the following four aspects: encrypted data management, intelligence covert communication, military cooperative operations, technology integration and innovation.

2.1 Encrypted Data Management

With the improvement of privacy protection awareness, commercial and civil encryption technology is popularized. Encryption technology and numerous cryptographic schemes are widely used in content privacy protection, system authority authentication, network protocol design and other fields. With the increasing proportion of encrypted data in cyberspace, how to implement security management on noisy encrypted data while taking into account content protection of encrypted data, so as to realize integrity authentication, traceability and tracking of encrypted data and other derivative functions has become an important issue to be solved urgently [12]. The traditional management method based on ciphertext retrieval has some disadvantages, such as high computational complexity, single function and easy tailoring of information. RDH-ED technology, by embedding a series of management annotation information such as time stamp, classification information, authentication information and traceability information in ciphertext, can not only carry out real-time embedding while encrypting operation to save data storage cost, but also implement control access management of encrypted data by using the personalized application characteristics of embedded information. While realizing efficient management of encrypted data, the reversibility of RDH-ED technology can ensure that authorized users can recover the carried secret text without distortion, and the separable performance can enable cloud service providers to realize ciphertext management without decryption to ensure the privacy of the original data.

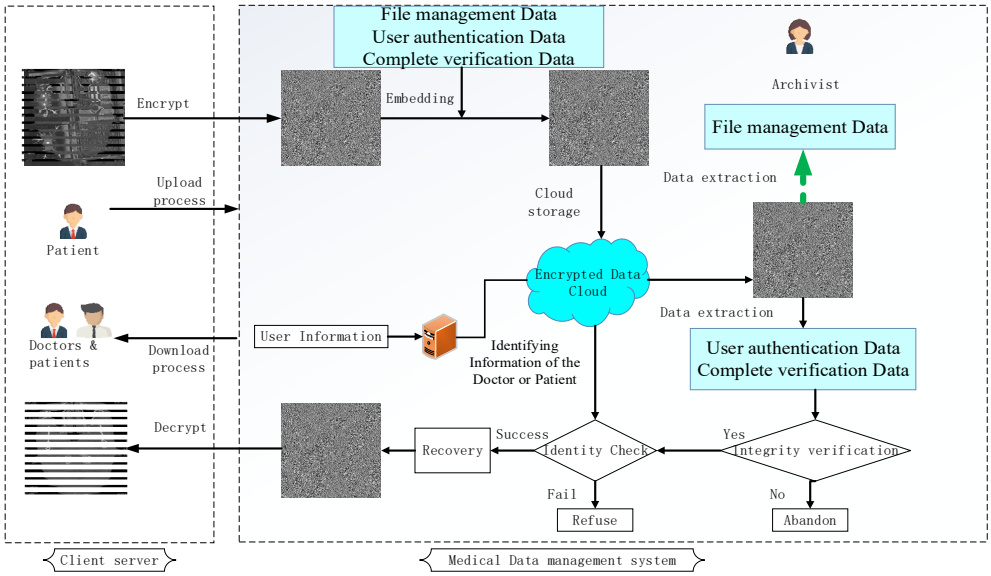

Figure 1. Example of medical encrypted data management application

Figure 1 shows the schematic flow chart of RDH-ED's application of medical confidential data management: In order to prevent personal information disclosure, patients encrypt medical images containing private content and then upload them to the cloud data management system. In order to assist the realization of a series of data functions such as file management, access control and integrity verification of confidential data, the server uses RDH-ED to embed information (such as patient identity information, medical record retrieval information, medical diagnosis results, integrity verification code, etc.) in the ciphertext to obtain the carrying ciphertext and save it to the cloud server. Archivists can realize the secret data management according to the extracted file management information without reading the contents of the carrying secret text. Medical information such as medical image is sensitive to data distortion, so carrying secret text not only supports extraction of additional information, but also supports decryption and non-destructive recovery of medical image. In the process of ciphertext transmission, RDH-ED is used to extract the complete check code from the carrying dense text, which can be used for data tracing or integrity verification without decryption. Meanwhile, according to the user information provided by patients and doctors, the access control mechanism can be combined to realize the controllable decryption and reading of medical images.

2.2 Intelligence Covert Communication

With the development of information technology, the types of communication carriers are constantly updated. In the process of implementing secure communication, intelligence security departments have special requirements for the security and concealment of communication. The traditional covert communication technology with plaintext multimedia data as the carrier is difficult to achieve provable security, while the subthreshold channel technology uses network communication protocol as the cover to transmit information.

Although it has provable security, the information transmission rate is low. The data hiding feature of RDH-ED technology is that the secret message is hidden in the encrypted image. Second, the behavior of communication is hidden in the normal process of information transmission; Third, the two sides of the communication are hidden in a large number of information contacts; Fourth, the transmission channel is hidden in the mass information transmission process[13]. Using these features, RDH-ED based ciphertext steganography can realize hidden communication under new media under the cover of common encrypted data exchange platform, and has unique advantages in achieving provable security and improving transmission rate. The application of cryptography technology in RDH-ED makes the carrying secret data transmitted in the form of meaningless noise in the open channel. For illegal third parties, the biggest interest in attack lies in the decryption and recovery of information while ignoring the transmission of secret information, which reduces the possibility of covert communication being detected and then analyzed. At the same time, the reversible recovery of original data can conceal the existence of data hiding and disguise the covert communication based on encrypted data as data encryption transmission behavior.

2.3 Coordinated Military Operations

The concept of "combat cloud" proposed by the US Air Force relies on distributed cloud computing to solve the problem of incompatibility of information transmission and ineffective coordination among different combat platforms [14]. If our army wants to carry out the guiding concept of joint operations and realize the comprehensive perception of battlefield situation, it must also have the corresponding technical means to obtain the powerful "information sharing ability" to ensure the cross-domain integration of battlefield information. For example, a series of military information such as combat images and cooperative instructions need to be encrypted at the source end before subsequent operations are performed due to its strategic importance. At the same time, the difficulty of obtaining military regional information and the far-reaching influence of military tasks determine that military information cannot tolerate the slightest deviation, so it is highly sensitive to the damage and loss of original data. RDH-ED technology, which effectively takes into account the transmission of secret information and the lossless recovery of original data, has important research significance for disaster recovery sharing of combat data and collaborative processing of encrypted instructions in cloud environment.

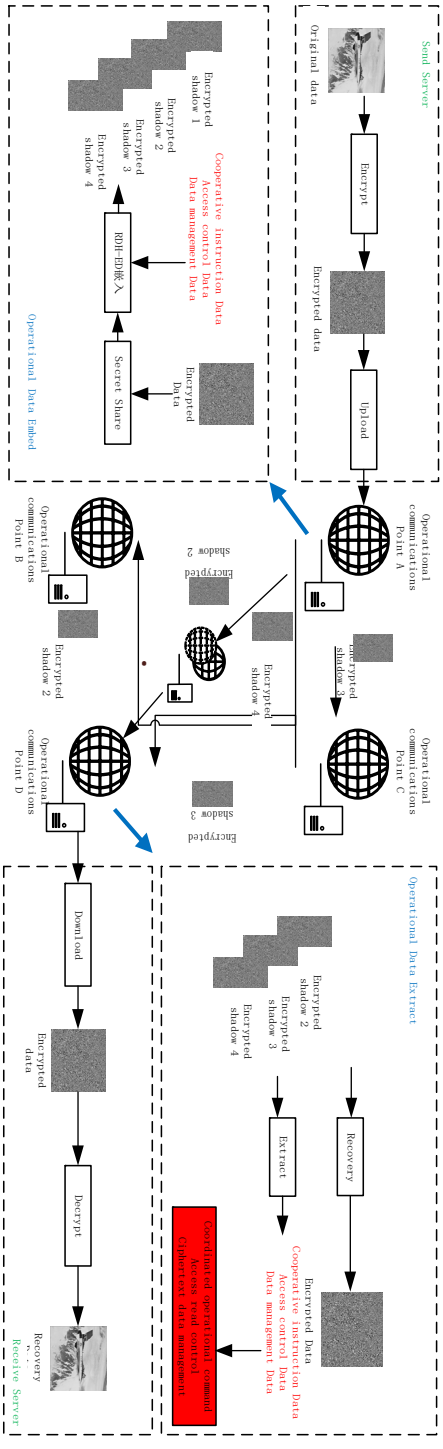

Figure. 2 Example of military cooperative operations

Figure. 2 shows the schematic flow diagram of the application of RDH-ED to military cooperative operations: For the military combat imaging obtained by reconnaissance troops, in order to protect the content security of the imaging in the open channel transmission, it is encrypted and uploaded to the combat communication site A in the cooperative operations network. After obtaining encrypted data, combat communication site A divides the encrypted data into multiple secret shares and shares them with multiple combat communication sites for distributed storage to improve the disaster recovery capability of the data store. Using specific RDH-ED technology, secret information of operational significance can be embedded in the process of secret share segmentation to achieve better collaborative command operations in the later period, such as collaborative command information, access control information, data management information, etc. For any combat communication site, by establishing a reasonable negotiation mechanism, once the threshold of secret recovery is met, the lossless recovery of original data and real-time acquisition of instructions can be realized. For a few combat communication stations, the loss and damage of carrying secrets due to the impact of the operational environment are acceptable for the RDH-ED military cooperative combat application based on secret sharing, which still does not affect the overall combat instruction and data recovery. At the same time, combined with the design of access control mechanism and data management, it can further realize the enrichment of tactical level of combat command.

2.4 Technology Integration Innovation

The trusted architecture of cyberspace security needs to be integrated and supplemented by new technologies. With the rapid rise of computing resources in cyberspace in recent years, emerging information technologies with revolutionary significance, such as big data [15], cloud computing [16] and deep learning [17], have gradually become the mainstream of information development. RDH-ED, as a cross technology between encryption technology and data hiding technology, can provide reliable and safe technical guarantee for promoting the integration and development of emerging technologies by means of multi-technology integration. For example, the fusion of RDH-ED cloud storage technology can facilitate cloud administrators to make better use of index information and statistical data embedded in dense cloud data for statistical analysis; The deployment of RDH-ED big data management technology can ensure the privacy and security of massive data by encryption processing, and realize the feature analysis without exposing the data content by data tag embedding combined with deep learning network. With the continuous development of research and technology maturation, RDH-ED can play an important role in the planning and design of broader security architecture in the future. Therefore, the research results of this paper not only enrich the theoretical system in the field of reversible data hiding, but also provide technical support for the integrated innovation and development of emerging technologies.

3 CONCLUSIONS

With the continuous innovation of network communication technology and the continuous improvement of privacy protection requirements, data needs to be transmitted, processed and stored in the cloud space in the encrypted state to meet the needs of more complex and diverse applications. Then, encrypted data brings many difficulties for cloud labeling, management

and retrieval. How to efficiently manage encrypted data has become an important issue urgently to be solved in this field. Reversible data hiding in encrypted domain, as a cross-fusion technology of encryption technology and data hiding technology, takes a large number of encrypted data existing in cloud space as the carrier for data hiding, and combines its technical characteristics with cloud technology, which has important research value for the four aspects of intelligence covert communication, military cooperative operations, technology integration and innovation.

ACKNOWLEDGEMENTS: This work was supported by Natural Science Foundation of China under Grant No.61872384 and Grant No.U1603261 and National Key R&D Program of China under Grant No.2017YFB0802000. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers.

REFERENCES

[1] Mao Y, You C, Zhang J, Huang K, et al. A Survey on Mobile Edge Computing:The Communication Perspective[J]. IEEE Communications Surveys & Tutorials, 2017,19(4):2322-2358.

[2] Yan K, Luo G, Zheng X, et al. A Comprehensive Location-Privacy-Awareness Task Selection Mechanism in Mobile Crowd-Sensing[J]. IEEE Access, 2019, 7:77541-77554.

[3] Wu D, Si S, Wu S, et al. Dynamic Trust Relationships Aware Data Privacy Protection in Mobile Crowd-Sensing[J]. IEEE Internet of Things Journal, 2018, 5(4):2958-2970.

[4] Zhou J, Cao Z, Dong X, et al. Security and Privacy for Cloud-Based IoT:Challenges[J]. IEEE Communications Magazine, 2017, 55(1):26-33.

[5] Ge X, Yu J, Zhang H, et al. Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key Based Verification[J]. IEEE Transactions on Dependable and Secure Computing, 2019:1-11.

[6] Liang X, Yan Z, Chen X, et al. Game Theoretical Analysis on Encrypted Cloud Data Deduplication[J]. IEEE Transactions on Industrial Informatics, 2019, 15(10):5778-5789.

[7] Sun J, Xiong H, Zhang H, et al. Mobile access and flexible search over encrypted cloud data in heterogeneous systems[J]. Information Sciences, 2020, 507:1-15.

[8] Kumar, Sanjay, 等. Reversible Data Hiding:A Contemporary Survey of State-of-the-Art, Opportunities and Challenges[J]. Applied Intelligence, 2021, 1-34.

[9] Kong P , Fu D , Li X , et al. Reversible data hiding in encrypted medical DICOM image[J]. Multimedia Systems, 2021(2):1-13.

[10] Kittawi N , Al-Haj A . Reversible data hiding using bit flipping and histogram shifting[J]. Multimedia Tools and Applications, 2022, 81(9):12441-12458.

[11] Puteaux P , Ong S Y , Wong K S , et al. A Survey of Reversible Data Hiding in Encrypted Images - The First 12 Years[J]. Journal of Visual Communication and Image Representation, 2021, 77:103085.

[12] Li J, Ma R, Guan H. Tees:an efficient search scheme over encrypted data on mobile cloud[J]. IEEE Transactions on Cloud Computing, 2017, 5(1):126-139.

[13] Sun Y, Zhang X. A kind of covert channel analysis method based on trusted pipeline [C]. 2011 International Conference on Electrical and Control Engineering (ICECE), Yichang, China, 2011:5660-5663.

[14] Wang W;Wang W;Shi F.Lu L. Review on US Navy digital transformation strategy [J].Ship Science and Technology, 2021, 12: 170-175.

[15] Yan Z, Wang M, Li Y, et al. Encrypted data management with deduplication in cloud computing[J]. IEEE Cloud Computing, 2016, 3(2): 28-35.
[16] Gong X Y , Li B H , Chai X D , et al. Survey on Big Data Platform Technology[J]. Journal of System Simulation, 2014.
[17] Akhtar N , Mian A . Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey[J]. IEEE Access, 2018, 6:14410-14430.