Secure Transmission Mechanism of Space Data Based on Information Attribute

MA Heng-tai, LIU Xiao-xia, WANG Xue−fei
Sc. and Tech. on Integrated Information System Laboratory
Institute of Software, Chinese Academy of Sciences
Beijing, China
hengtai@iscas.ac.cn, xiaoxia@iscas.ac.cn

YI Xiao-wei
State Key Laboratory of Information Security
institute of information engineering, CAS
Beijing, China
yixiaowei@iie.ac.cn

***Abstract*—An optimal secure transmission scheme of space data is designed by optimizing the secure distribution of the space observation data in view of the change of source-channel condition. Various source-channel models are built based on the optimization objective of data quality, and then the data protection strategy and approach based on joint source-channel and secure coding are proposed. A quality evaluation and distribution model of space observation data is established, and the secure distribution of space observation data under separated source-channel coding and the encryption-authentication distribution of space observation data under joint source-channel coding are optimized and evaluated. The algorithms are analyzed and simulated. The data protection strategy and approach are validated in robustness, scalability and reliability.**

Keywords—information technology;information security; space data; information attribute; security mechanism

I. INTRODUCTION

With the rapid development of the aerospace and information technology, the spatial information advantage has become the key to succeed in the modern information war. Faced with the ever-changing war environment, information superiority is the safeguards of rapid command decision. In modern wars, mutil-arms combat units require a secure, reliable, fast and accurate spatial information support to work together, and a safe and efficient spatial data secure transmission capability will enhance combat effectiveness and flexibility.

In the future's multi-arms combat units corordinating scenes, space information support is needed, and each combat unit are dependent on telematics support obtained from communications satellites. As an important backbone nodes, communication satellites can give full play to its broadcasting capacity, applying information support for mutil-arms combat units. To support the secure transmission of data information in war environment, we need to consider the characteristics of satellite channel broadcasting, the channel bandwidth of satellite communication systems which is limited by time and space, and characters by limited data cache space and data processing capabilities, channel packet loss rate, delay jitter and so on [1]. Therefore, building a safe and efficient spatial data transmission optimization mechanism to improve the utilization of space communications resources and enhance the ability of information technology has important significance.

As for the secure transmition mechianism of space data, the exist schedume is simple, and not consider the special nature of spatial data attributes, so it can not take full advantage of communications coverage and broadcast properties of the space nodes, and can not meet the case of multi-source and channel parameters change, resulting in limitatation in nature and reliability.

In this paper, we take optical remote sensing image data as an example. For the information needs of war environment remote space support, we will view the data quality as the optimize core and base on information attribute to explore solutions to the security problems of non-equilibrium robust spatial data. Finally, build the spatial data quality assessment and security-aware transport model based on information attributes. For spatial channel errors and packet loss issue, we propose the algorithm which combined the source and channel coding of spatial data encryption with authentication, then establish the optimization strategies at the core of data quality, and finally establish the spatial data secure transmission optimization method based on source-channel coding.

II. RELATED WORK

The Consultative Committee for Space Data Systems (CCSDS) is mainly responsible for the development and adoption of suitable space communications and digital processing systems of various communication protocols and data handling specifications. According to the characteristics of spaceborne equipment and spatial mage data itself, CCSDS issued the a 122.0-B-1 recommendation letter in November 2005, proposing an image data source coding standard which is based on wavelet transform [2] [3]. When doing lossless data compression, the compression ratio is between 1.5 to 3. Although the compression ratio is not very high, the algorithm is simple, has low demand on hardware conditions, and is also to be improbed in the further. It has a good prospects [4]. Afer that, the CCSDS releases the 131.1-O-2 Technical Report in September 2007[5], which optimize the parameters of LDPC channel coding in space communications conditions and give the experimental results.

As early as the late 1990s, in order to solve the data security problem of space communications, CCSDS has made the secure communication protocol (SCPS-SP)[6] targeted on the end-to-end system of cyber network. SCPS-SP protocol is

a network layer protocol that uses a fixed packet data encryption and authentication algorithms. The protoco does not consider the link environmental changes and other factors, so it has poor adaptability in error resilience and loss of tolerance to variable channel environment. In terms of data security space, CCSDS has also issued safety guidelines [7] [8], and is completing the formulating for space sata systems standards[9]. CCSDS will then publish the space data link security protocol criteria [10].

The research on the data protection of source coding is mainly focused on secure coding research combined with image source coding[11]. The article [12] proposed Huffman code table based scrambling encryption algorithm. For CCSDS image encryption standard, article [13] proposed a rear-mounted encryption scheme based stream ciphers. The program can support intermediate node doing bit rate conversion directly on ciphertext. The article [14] proposed a hybrid encryption method of remote sensing image domain and [15] designed a suitable CCSDS image compression algorithm which is a scalable encryption scheme.

In the aspect of certification for the image data, [16] proposed an image authentication algorithm (hash chaining) based on a hash chain. In aspect of content-related image authentication algorithm research, according to the feature JPGE2000 image compression algorithm, the literature [17] designs a image authentication algorithm suitable for JPEG2000 compression coding. The article[18] gives the optimizaton of the algorithm. Perceptual hash is a new image authentication technology in recent years [19]. Using hash chain and hash tree structure, article[20] proposed a verification scalable image streams authentication algorithm and article[21] proposed a end-to-end authentication method which is based on the quality optimization mechanism using the codec dependent.

III. Secure Transmission Mechanism of Space Data Based on Information Attribute

A. *Data distribution modeling based on information attribute perception.*

End-to-end data security distribution system based on the quality of content is a complex data transmission control system. The secure data distribution control need to consider many conflictiong factors, like their own property characteristics, the uncertainty, security policies and security mechanisms in transmission. Therefore, design a safety data distribution scheme with optimized performance is very complicated. In this paper, we use the method of controlling a variable constraint to analysis the issue. Firstly, classify all the factors that affecting the data distribution control according to different properties, then analyze the constraint relationship between the property value in the same property class, and finally analyze the ones between the property value in different property class. We can use the relationship between each attribute class to guide the design a safe and efficient distribution control strategies and mechanism.

For a end-to-end data secure distribution system, the control factors can be classified into three property categories: security attributes, information attributions and process attributions. We will illustrate the specific attribute values in each attribute class below.

1) Security attributes.

Security attributes include confidentiality, integrity, authenticity, availability and non-repudiation.

Confidentiality refers to prevent unauthorized reading of information body, that is to say, unauthorized users can not gain access to sensitive information.

Integrity is to prevent information from unauthorized tampering. It is to protect the information to keep the original state, so that making the information integrated.

Authenticity refers to the accuracy and consistency of the original information. It ensures that the received information is derived from the authentic sender and ensure the accuracy of the information.

Availability refers to the ability to receive timely services when the authorized ones have requirement. It is the new requirements proposed in information security stage, as well as an information security requirement in the networked space.

Non-repudiation refers to the behavior that the exchanged parties should not deny the process to send or reveive information in the network environment.

In addition to the five above-mentioned aspects, there are also information auditability, identifiability and controllability. Information security's auditability refers to the person in information system can not deny their information processing behavior. The visible identification of information refers to that the recipient of information should identity of the sender. And controllable means of monitoring implementation of safety management for the information and information systems to prevent illegal use of information and information systems.

2) Information Attributes

Information attributes refers to the inherent nature of the physical characteristics and features or characteristics of the data content, such as data quality, data rate, field characteristics and geometry.

Data quality is a measure of accuracy, rationality, integrity and timelyness of information.For example, image data quality can be evaluated by subjective and objective criteria. For high quality image data, more effective details can be getted. In the safety data distribution control process, the authenticity of data quality should be primary guaranteed, and then consider the availability of data.

Data rate refers to the amount of data in a given size of data quality conditions. Typically for the same data object, the higher the data rate is, the higher quality can be obtained.

Domain feature refers to the distribution pattern or ralated characteristics of the content data information in some domain of information. Domain features for image data mainly include spatial feature, frequency domain feature and compression domain feature. Spatial feature of two-dimensional image data is as follows: the amount of data is large, for a eight grayscale

image data of 10240 × 10240 is 100M bytes; data redundancy is large, snd usually there is a space pixel image data redundancy, mental visual redundancy and coding redundancy. The frequency domain features of two-dimensional image data is mainly shown for uneven in spatial energy distribution. The low-frequency part of the data focus most of the energy, thus playing a very important role in enhancing the quality of the image reconstructed. While the high frequency data is important for the details of the image content. The compression domain of two-dimensional image data exhibit characteristics of hierarchical structure, while the structures of compressing domain data generated from different compression coding have different characteristics.

Geometric features refers to the space structure of the content data. Geometric features of the image data mainly refers to multi-resolution display.

3) Process Attributes

Process attributes refer to factors that affect data distribution process, including real-time and channel change characteristics.

Real-time data characteristics means that the delay end-to-end distribution time of content data is within the specified range. For example, the time that the image content data transmit from request to appearance should be maintained at the nanosecond level or less.

The channel change characteristics refer to the changing pattern of channel environment variation with time, such as the channel errors and packet errors caused by the channel loss.

We will take the distribution cooperative multitasking scenario of content data as an example, and give qualitative analysis for the relationship between the property values of the same property class and property values of different classes.

a) The relationship of different property values in the same property class

The security attributes demand of data exhibite grade level feature. Assumed that the security property is set to be high, medium and low level. The onboard terminals, airborne terminals and vehicle mount terminals have different requirements for confidentiality, integrity and authenticity, which is shown in Table 1. Even the same terminal have different level of security requirements for different tasks.

Table 1 the level of security requirements for terminals with different tasks

	confidentiality	integrity	authenticity
onboard terminal	low	low	high
airborne terminals	low	medium	high
vehicle mount terminals	medium	high	high

For information attribution class, data quality is positive correlation with data rate, and we usually use a higher data rate for gaining higher data quality. Taking fully use of information domain features can enhance the data source coding efficiency. Geometric features have practical applications in different terminals.

For process attribution class, real-time characteristics are affected by the change channel. When the channel condition is better and stable, real-time data transmission can be more effectively protected.

b) Relationship of property values in different attributes classes

Typically the relationship of property values in different attributes classes has a greater contact with task characteristics. Take the image content data secure distribution as an example to qualitative analysis the restrict relationship between attribution classes. With the enhancement of the quality of the image data (when data quality level increase, the amount of data increase), data confidentiality enhances, authentication decreases, and the end-to-end delay increases, shown in figure 1.

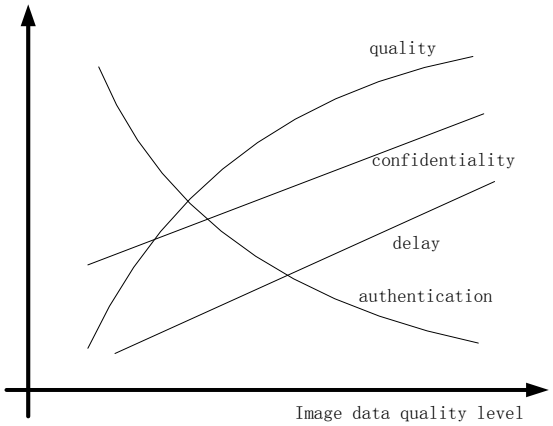

Fig. 1. the relationship of property values in different attributes classes

With the large redundancy, complex and highly asymmetric feature of spatial data, the traditional data evaluation model based on the limitations of subjective quality have some limitations. In this paper, we will combine the traditional peak signal to noise ratio (PSNR) model with the quality evaluation model based on the data content, and then analysis the hierarchy of observational data, content features and the spatial distribution of information interest, and finally construct quality models targeted on different types the space observation data.

B. The security distribution mechanism based on data quality-driven

We will introduce keys dependent mechanism in different stages of the source coding process. Figure 2 shows the situation of using the Advisory Committee for Space Data Systems image data compression (CCSDS IDC) coding standards. According to the spatial characteristics of the observed image sources, establish a joint optimization model which is of data quality, compression, security, and the coding efficiency, and then further construct the secure source coding method for pace observation missions. The secure source coding method should not destroy the compression encoding flow characteristics, like original source coding syntax structure, and has little or no effective on some important

statistical characteristics of the sourcing, finally increase the availability of the cipher text stream.

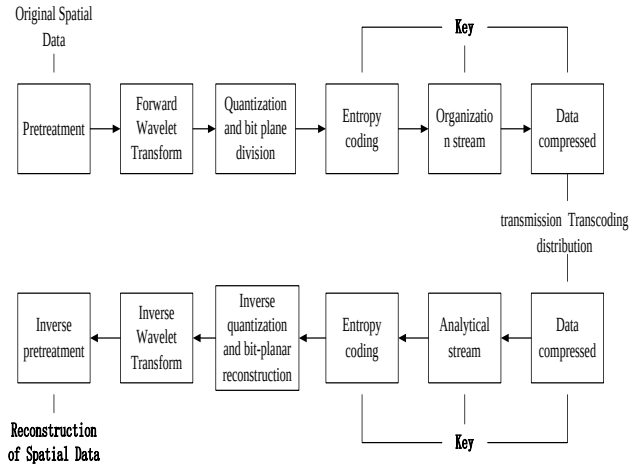

Fig. 2. the secure coding method combined with CCSDS image source coding

In raditional communication schemes, error correction and encryption are independent in the communication networks. However, channel coding and passwords have a lot of mathematical relationships. In this paper, we combine LDPC coding in space communications with the packet encryption algorithm, and then design a secure channel coding method suitable for space-based observations. The method uses the wide trail strategy, so that it can effectively against differential cryptanalysis and linear cryptanalysis attacks. Meanwhile, for the LDPC generator matrix has better diffusion properties, the method can have substantially equal security level as AES coding algorithm when counting anti-linear, differential attacks in fewer rounds. LDPC coding generates two vectors: the parity bit vector and vector information bits. Connect a interleaver to a LDPC error correction code encoder to upset location information, which can further enhance the ability to resist cryptanalysis attacks. Compared with the traditional design of separate error correction and encryption, the method can effectively avoid the error caused by the proliferation of encryption and increasing packet loss rate.

Different with the existing secure communication frameworks, in this paper, we will take an security optimization framework for data quality. The optimization framework constructs the optimization model at the core of establishment of spatial data quality assessment, and use the data source coding features. It can achieved on a non-equal security for data quality, ensuring reducing data communication cost less at the condition of make sure the optimum quality of the data from end to end. To make sure the security authentication for space observation data from end to end (including data origin authentication and data integrity authentication), the sender generates hash, digital signature and authenticatio of original data auxiliarily. The method is represented by a directed acyclic graph (DAG) $\langle V, E \rangle$, in which V represents a collection of nodes, and E represents the set of the edges. Each element (node) in the collection V represents a data packet or a signature package. Usually authentication scheme makes signature only once for the data once, so that V contains only one signature node. The edge from the node P_i to the P_j represents a hash value connection from P_i to P_j, namely calling P_i and P_j as the source node and the destination node respectively, and calling $e(i, j)$ as the hash value connection from P_i to P_j. The redundant of node P_i represent the number of directional drawn edges from P_i. In particular, redundancy of signature nodes is equal to zero. Since the communication process is affected by channel noise and other factors, the packets may be lost during transmission. So when reconstructing certification image, the recipient needs to remove the nodes missing data packets in certification graph. For recepient, a packet P_i can be verified in the certifacation graph will be describe as a path from node P_i to the signature node.

In order to formally describe the certification optimization problem of the rate-distortion model (RDM), we define the quantitative element $\pi = [\pi_0, \pi_1, ..., \pi_m, ..., \pi_{M-1}]$, in which π_m represents the destination nodes set whose source node is P_m, and the redundancy of node P_m is $|\pi_m|$ ($|\pi_m| \geq 1, m = 1, 2, ..., M-1$). When given a set of nodes V, the certification graph is uniquely determined by the vector diagram π. The overall rate is recorded as R (including letter source rate, channel bit rate and certification rate) and total pre-distortion as D, and our goal is to solve an optimal π^* on a given condition $\lambda > 0$, to make Lagrange minimum number in (1) least. The Lagrange multipliers is measured by R and D. For example, when λ is reducing, the optimal strategy will decrease D and increase R corresponding, and vice versa.

$$\pi^* = \arg \min_{\pi} (D + \lambda R) \tag{1}$$

In formulas(1), $D = D_s + D_c + D_a$, $R = R_s + R_c + R_a$, and assuming distortion D and bit rate R have the linear additive feature. Open source letter rate R_s and distortion D_s represent rate and distortion after data compression respectively. Similarly, the channel bit rate R_c and channel distortion D_c represent data bit rate and distortion through the channel encoded respectively. Certification rate R_a indicates the size of the authentication auxiliary data (including data packet hashes and digital signatures), the calculation expression is formula (2).

$$R_a(\pi) = SIZ_{\text{sig}} + \sum_{P_m} |\pi_m| \, SIZ_{\text{hash}} \tag{2}$$

SIZ_{sig} and SIZ_{hash} represent the size of the digital signature and hash values respectively.

Certified as distortion $D_a(\pi)$ is calculated by formula (3), and it is also linear distortion added.

$$D_a(\pi) = D_0 - \sum_{P_m} \Delta D_m \rho_m [1 - \varepsilon(\pi_m)] \tag{3}$$

D_0 represents of the data when no data packets are verified; ΔD_m represents the amount of reduced distortion value when packet P_m is reconstructed conrrectly; $1-\varepsilon(\pi_m)$ indicates the probability of a packet can be verified.

From (1), generally, it is computationally infeasible for solving the global optimal solution π^*, when taking the source coding, channel coding and certification into account. A more feasible approach is to first consider global resource allocation policies based on source coding, channel coding and authentication, and then optimize them independently. For example, you can ignore some items of D and R, such that (1) can be simplified, and then solve the equation (1). After that, assign some arguments according to some empirical methods. In particular, for space observation data, we can calculate the authentication without the cost of each packet, but simply all the packets into multiple categories, and the same type of data packet will have the same certification costs. Finally study how to achieve optimal performance at different spatial data, different compression formats and different channel conditions.

IV. SIMULATION EXPERIMENTS AND RESULTS

A. *Computational overhead*

Considering the cost time of transcoding, simulation experiments analyze the Lena (512×512) and Man (1024×1024), using the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) to calculate the processing encrypted time's percentage of total time respectively. Figure 3 shows the results and either AES or DES, the time-consuming proportion of encryption process is less than 2%. The results show that the additional time encryption algorithm costs is small compared with that without using it.

Considering the cost space of transcoding, simulation experiments analyze the Lena and Man, using the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) to calculate the encryption filling part's percentage of total length of the final code stream packets. Figure 4 shows the results and either AES or DES, the custom header and amount of padding data of encryption process is less than 2%. The results show that the additional space encryption algorithm costs is small compared with that without using it.

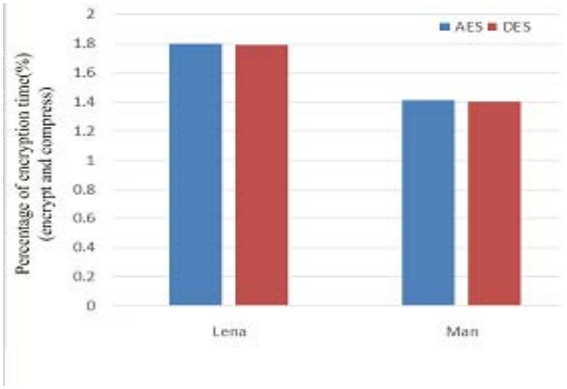

Fig. 3. The time cost caused by encryption mechanism Communication cost

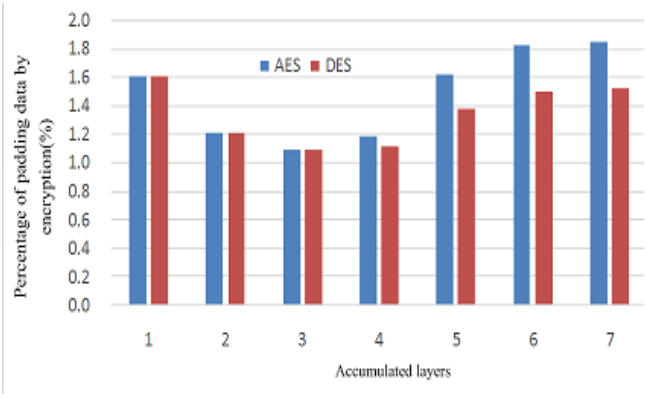

Fig. 4. The space cost caused by encryption mechanism Loss robustness of authentication mechanism

Since the introduction of the certification path takes along dependence between packages, stream authentication algorithm based on image constructed may cause that some proper transmission and correctly decoded packet can not be certified, when using in network with packet loss. This feature of authentication algorithm can be exhibited by the peak signal of noise ratio(PSNR) and packet loss rate. The higher the peak signal of noise ratio is in the same loss rate, the better the algorithm performs. PSNR will not add up to more than source stream of the uncertification scheme.

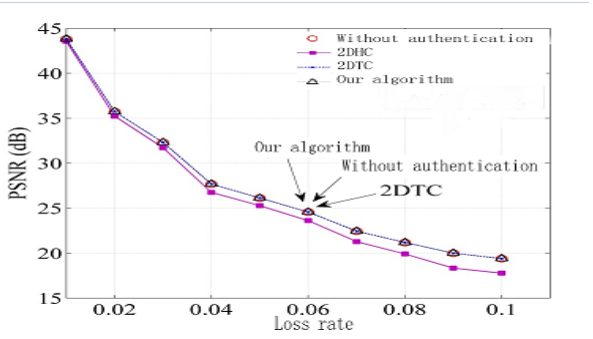

Fig. 5. Loss robustness of authentication mechanism (PSNR——the peak signal of noise ratio)

As shown in figure 5, the curve by our method coincide with the curves of 2DTC and source streams, and higher than

2DHC curve. This shows that in unreliable networks, this authentication method does not reduce availability of the data stream, and has better packet loss robustness than 2DHC. The reason is that the algorthem is on the base of certification path, ensuring the consistency of the dependence relationship in each packet and that in various parts in code when codecing.

V. CONCLUSION

In this paper, we firstly analyze the spatial data's characteristics in the distribution process, and then study the constraint patterns between attributions of spatial data internal and with the security attributes, finally establish a reasonable and feasible spatial data quality assessment model and data security distribution mechanism, exploring the optimization distribution method for security distribution demands. In experiments, we verify the robustness, scalability, and reliability from theoretical analysis and simulation, certifying the availablility in security transport policies and methods. Our method has effectively solve the limitaions in the scalability and reliability when using existing spatial data secure transmission scheme, and provide theory and technical support for the secure distribution of spatial data protection which is faced with data quality.

Acknowledgment

This work was supported by the NSFC under 61202218 and the Innovation Fund of CAS under Y4YC876922.

References

[1] LIU Yong, DONG Yong, LI Ze-hui. Discussion of Data Security About Space-Earth All-in-One Networking and Analysis of CCSDS SCPS [J]. Chinese Space Science and Technology, 2002, 24(1): 31-36.(in Chinese).

[2] CCSDS. CCSDS 122.0-B-1 Cor. 2 Image data compression [S]. USA:CCSDS, 2008.

[3] CCSDS. CCSDS 120.1-G-1 Image data compression [S]. USA:CCSDS, 2007.

[4] Yeh P S, Armbruster P, Kiely A, et al. The new CCSDS image compression recommendation [C]// IEEE Aerospace Conference. Big Sky, MT, USA: IEEE, 2005: 4138-4145.

[5] CCSDS. CCSDS 131.1-O-2 Low Density Parity Check Codes for Use in Near-Earth and Deep Space [S]. USA:CCSDS, 2007.

[6] CCSDS. CCSDS 713.5-B-1 Cor. 1 Space Communications Protocol Standards (SCPS) - Security Protocol (SCPS-SP) [S]. USA:CCSDS, 2010.

[7] CCSDS. CCSDS 350.0-G-2 The Application of CCSDS Protocols to Secure Systems [S]. USA:CCSDS,2006.

[8] CCSDS. CCSDS 350.7-G-1 Security Guide for Mission Planners [S]. USA:CCSDS, 2011.

[9] CCSDS. CCSDS 351.0-R-1 Security Architecture for Space Data Systems [S]. USA:CCSDS,2011.

[10] CCSDS. CCSDS 355.0-R-2 Space Data Link Security Protocol [S]. USA:CCSDS,2012.

[11] Mao Y, Wu M. A joint signal processing and cryptographic approach to multimedia encryption [J]. IEEE Trans on Image Processing, 2006, 15(7): 2061-2075.

[12] Shi C, Bhargava B. A fast MPEG video encryption algorithm [C]//The 6th ACM International Multimedia Conference. Bristol, UK: ACM, 1998: 81-88.

[13] Li M, Yi X, Ma H. A scalable encryption scheme for CCSDS image data compression standard [C]// 2010 IEEE International Conference on Information Theory and Information Security. Beijing, China: IEEE,2010: 464-469.

[14] Zhang X Q, Zhu G L, Ma S L. Remote-sensing image encryption in hybrid domains [J]. Optics Communications, 2012, 285: 1736-1743.

[15] Li M, Yi X, Hu X, et al. Scalable streaming for CCSDS IDC standard with encryption and authentication [C]// IEEE International Conference on Pervasive Computing, Signal Processing and Applications (PCSPA). Harbin,China: IEEE, 2011.

[16] Gennaro R, Rohatgi P. How to sign digital streams [C]// Proceedings of Advances in Cryptology (CRYPTO'97). Lecture Notes in Computer Science, held in Santa Barbara, California, USA, in August 1997 under the sponsorship of the International Association for Cryptologic Research (IACR), 1294:180–197.

[17] Zhang Z, Sun Q, Wee S, et al. An optimized content-aware authentication scheme for streaming JPEG-2000 images over lossy networks [C]// 2006 IEEE International Conference on Acoustics, Speech, and Signal Processing. Toulouse, France: IEEE, 2006: 293–296.

[18] Gao F, Leman K. Improved optimized content-aware authentication scheme for secure scalable streaming and transcoding with JPEG-2000 images [C]// Proceedings of the 2009 IEEE International Conference on Multimedia & Expo. NJ, USA: 2009: 1086-1089.

[19] NIU Xia-mu, JIAO Yu-hua. An overview of perceptual hashing [J]. ACTA Electronica Sinica, 2008, 36 (7): 1405-1411. (in Chinese).

[20] Yi X, Li M, Ma H. Optimized graph-based authentication for image streams delivery over wireless networks[C]//Proceedings of the 2011 IEEE International Conference on Intelligent Computing and Intelligent Systems. Guangzhou, China: 2011, II:640-646.

[21] Yi X, Li M, Zheng G, Zheng C. Quality-optimized authentication of scalable media streams with flexible transcoding over wireless networks [C]//Proceedings of The 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC). Washington,DC, USA:IEEE Computer Society, 2012:148-153.