[RACE: March 2017]
ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A NOVEL METHOD FOR PROTECTING RIGHTFUL OWNERSHIP OF MULTISPECTRAL IMAGES: A REVIEW

Ashly Sankar.S.J[*1] & Mrs. Safoora.O.K.[2]

[*1]Mtech scholar, Department of ECE, College of Engineering, Thalassery

[2]Assistant Professor, Department of ECE, College of Engineering Thalassery

ABSTRACT

This paper provides a review of copyright protection of remote sensing images by combining encryption and watermarking. Necessary design tradeoffs for algorithm development are highlighted for multicast communication environments. Integration of encryption and watermarking by embedding mark simultaneously with the decrypting. The future of spatial scrambling in only disordering the arrangement of protected data, which wouldn't cause disturb for watermark but modifying data. The comprehensive security protection of remote sensing image by providing uses combination of encryption and watermarking. A novel architecture for encryption and watermarking that holds promise for a better compromise between practicality and security for emerging digital rights management applications.

Keywords- *Joint fingerprinting and decryption, Selective content encryption, Digital fingerprint, Commutative Encryption and Watermarking (CEW), Watermarking*

I. INTRODUCTION

There are tons of data that is distributed over the internet. This data are stored and transmitted in a digital format and can easily be copied without loss of quality and efficiently distributed. That's why protection has become increasingly important. The security of remote sensing image contains two aspects the storage security and the usage security. Encryption and watermarking are corresponding key technologies for these two aspects. There are plenty of literatures about remote sensing image security in encryption or watermarking. However, to the authors' knowledge, no one has satisfied the two security aspects in the same time. In order to provide a comprehensive protection for remote sensing image, encryption and watermarking should be combined.

Therefore, people introduce encryption and watermarking into remote sensing image security protection. Encryption converts the protected data into illegible words by some special irreversible transforms, which can actively prevent information leakage during the storage or transmission, but after legal users' decryption, the encryption protection would become inoperative. Watermarking embeds some special information into the protected data by some marking technologies, which can carry out copyright protection or integrity authentication after finding illegally usage, but watermarking does not ensure the confidentiality of protected data.

Only combining encryption with fingerprinting together can provide comprehensive content security protection for visual media. Joint fingerprinting and decryption (JFD) framework solves encryption and fingerprinting simultaneously and has high efficiency, but several problems still remain to be tackled in JFD, including poor encryption security, severe fingerprinted image distortion, etc. An improved JFD scheme is a new encryption strategy based on selective content encryption is put forward to enhance security, and a new method for choosing fingerprint embedding area by structural distortion is proposed to reduce fingerprint's influence to image quality [1]. The easiest way to combine encryption with watermarking is superposition, but simple superposition may case many problems. Therefore, it is necessary to consider how to achieve the combination of encryption and watermarking with orthogonal operation and integrating data [2]. Commutative Encryption and Watermarking (CEW) is such a technology which can integrate encryption and watermarking to provide comprehensive protection for multimedia. For the comprehensive security protection of remote sensing image, an identical operand CEW scheme is used. In virtue of scrambling just modifying data arrangement, the proposed CEW achieves mutual independence of

encryption and watermarking by non-interference in mechanism. For encryption and watermarking being applied to the same data field, which avoids the exposing of watermarking operand, the proposed CEW possesses higher security.

Integrate encryption and watermarking based on the orthogonal decomposition for the comprehensive security protection of remote sensing image [3]. Encryption and watermarking can achieve the operation independence and the content mergence; moreover, there is not special requirement in selecting special encryption and watermarking algorithms. It makes up the shortage of recent integration method based on spatial scrambling in application and possesses higher security.

II. AN IMPROVED JFD SCHEME

Aiming at JFD's problems, we will present an improved JFD scheme which inherits JFD scheme's high efficiency and overcomes its shortcomings by two ways. That is, a new encryption/decryption strategy based on selective content encryption is proposed to enhance encryption security and solve the contradictory relationship between encryption security and fingerprinted image quality in JFD; a new structural distortion method as the measurement for choosing fingerprint embedding area is proposed to reduce partial decryption's influence on image quality. By these ways, JFD's problems can be solved in order to enable it suits for the content security protection of visual media.

A. Encryption/Decryption Strategy Based On Selective Content Encryption

There is a compromise between encryption's security and the fingerprinted image quality in JFD framework. The trouble will be allayed from two aspects. At first, selective content encryption method is used to ensure encryption security, and a partial decryption strategy is put forward to decrease the influence to image quality. Secondly, fingerprint embedding areas are chosen to make an utmost reduction of the partial decryption's influence to image quality.

Considering fingerprinted image quality, DCT coefficients are only sign scrambled during encryption in JFD scheme, which is a lightweight encryption method and clearly has low security. In order to ensure encryption effect, we present a new encryption scheme, which encrypts all perceptually significant DCT coefficients by selective content encryption method. Selective content encryption has become the mainstream way in visual media's encryption, and its security has been proved widely. In order to reduce partial decryption's influence to image quality, we design a strategy where DC coefficients are decrypted entirely, and AC coefficients which affect image quality less are partially decrypted for the purpose of ensuring encryption security as well as fingerprinted image quality.

B. Selection Of Fingerprint Embedding Area

Because of image's particular structural feature, different regions have different influences to image quality, and it will cause image distortion if encrypted image is decrypted partially without differential. Especially when the parts left encrypted are becoming large, it will result in remarkable increasing of image distortion. Taking account of image pixels' structural change in encrypted image, we propose a new way to choose fingerprint embedding area using visual security assessment based on structural distortion, by which the influence of fingerprint embedding to image quality is greatly decreased.

The visual security assessment to visual media's ciphertext is usually used to evaluate its unintelligible degree, the greater the unintelligible degree, the higher security. According to this feature, a new method for choosing fingerprint embedding area is proposed in our scheme, where sub-image blocks having higher visual confidentiality are decrypted completely, and more intelligible parts in perception are decrypted partially and embedded fingerprints to reduce the image distortion.

The research of visual security can be classified into two types, that is, subjective assessment and objective assessment. The subjective one can be influenced by the measuring environment and subjective sensation, the single

ISSN 2348 – 8034
Impact Factor- 4.022

use of it is not effective in practical application. A video quality assessment with peak signal noise ratio (PSNR) is considered as an effective objective evaluation of visual security, where PSNR values of cipher-images is used to judge the cipher-images' unintelligible degree. In this method, the differences between image's pixels are only considered and the pixel is regarded as the independent point, while the correlation between adjacent pixels and the structural feature of image are ignored, therefore the PSNR value curve of cipher-images is not consistent with the conclusions of user's subjective judgments in some cases.

C. The Construction And Distribution Of Decryption Key

In this paper, users get fingerprinted image through partial decryption, thus the decryption key plays an important role in the formation of fingerprint. A key generation and distribution method is presented in this section, where decryption key matrix is constructed according to encryption key, binary random sequence, and the location information of sub-image blocks, then the matrix is distributed securely. The steps are given as follows:

- Step1: Partition the image into several sub-image blocks, where X1, X2,…X_M, where M is the total number of blocks. Generate encryption key of each block randomly, and get an encryption key matrix $K_E=|K_1 K_2 \dots K_M|$
- Step2: Generate binary random sequence w_j^i for each user, $1 \le j \le L, 1 \le i \le N$ and L is the length, N is the number of users. Construct a binary location matrix I through the location information of sub-image blocks and the value of the random sequence codeword, let $I = |I_1 I_2 \dots I_j \dots I_M|$, suppose the fingerprint embedding area is H_1, other area is H_2, if I_J lies in H_1, then it's value is w_j , if I_j lies in H_2, then it's value is 1.
- Step3: Calculate decryption key matrix by K_{D_i} by $K_{D_i} = K_E \times I$, and use CDMA's (Code Division Multiple Access) theory to distribute it securely through public channel.

III. SCRAMBLING BASED COMMUTATIVE ENCRYPTION AND WATERMARKING

The encryption for remote sensing image, nowadays, has two main methods: the block encryption and the scrambling. The former carries out protection by complex calculation to modify original data and certainly disturbs the watermarking which provides protection also by modifying data to embed protection information. Whereas, the later carries out security protection by disordering data's arrangement or layout and wouldn't cause essential disturbance for watermarking. Therefore, the identical operand CEW can be achieved based on scrambling.

The common way to recover watermark extracted from scrambling ciphertext may be reverse scrambling. But a charming way is using the property of scrambling, such as periodicity, to embed or extract watermark. Consequently, based on scrambling, this paper gives a scheme of identical operand CEW whose diagram is shown in Figure 1. Firstly, under the control of scrambling key K_s and embedding key K_e, the original watermark w will be embedded into ciphertext Xs to get the encrypted-watermarked carrier X_{sw}. During the encrypting and embedding process, the embedding algorithm and the scrambling operation should be adjusted mutually to avoid interfering. When X_{sw} needs watermark verification, people can use K_e to extract original watermark w from X_{sw} directly. It's worth noting that watermark is still inside the plaintext X_w after reverse scrambling of X_{sw}, but exists as ciphertext w'. Only through the recovering operation of reverse scrambling can we get the original watermark w from w'. For the sake of convenient operation, the proposed CEW scheme carries out watermark embedding after scrambling. Of course, it also can embed watermark into original data firstly and then scramble the processed data to get encrypted-watermarked carrier. Under this condition, for the security of watermark and the achievement of CEW, original watermark must be encrypted one more time coordinating with the later scrambling before being embedded. But these extra operations can certainly be avoided by embedding original watermark into ciphertext as the proposed CEW scheme has done.

ISSN 2348 – 8034
Impact Factor- 4.022

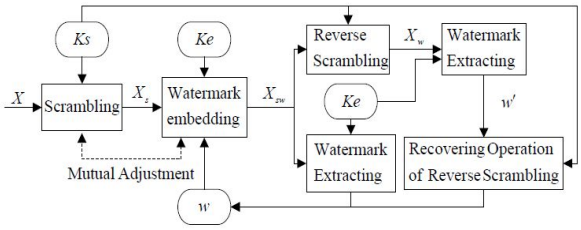

Fig 1: The identical operand CEW scheme based on scrambling

A. Practical Algorithm Based On Scrambling

If there are the right scrambling encryption and watermarking algorithm, the proposed CEW scheme can be used to protect many types of media such as audios, images, videos, etc. Given the need for remote sensing image compression, we will achieve the remote sensing image CEW algorithm based on the common JPEG compression standard.

1. Encryption

There are many kinds of spatial scrambling for remote sensing image. The most common way of combining watermarking with these scrambling is extracting the watermark ciphertext from decrypted image and then only decoding the watermark ciphertext according to the scrambling operation. But, more specially, some special properties of scrambling can be used to embed or extract watermark conveniently. Periodicity is such a special property. Assuming the period of chosen scrambling is N. Then the original watermark is embedded into the image ciphertext which has been scrambled by n1 times. After the same scrambling operation by n_2 times, where $n_1+n_2=aN$ and a is an integer, the carrier image will be recovered to plaintext because of the periodicity. But for the embedded watermark, it will exist in the image plaintext as the ciphertext by n_2 times' scrambling. Similarly, because of the periodicity, the extracted watermark ciphertext can be decrypted through n_3 times' the same scrambling operation if $n_2+n_3=bN$ where b is an integer. Considering the convenient of periodical scrambling in finding the recovering operation of reverse scrambling, in other words, periodical scrambling meets the encryption constrain, we choose periodic scrambling to realize the proposed CEW for remote sensing image.

Arnold transform, also known as chaotic cat maps transformation, is the most common periodical spatial scrambling [4]. For Arnold transform is only used to scramble 2-dimension equilateral image, then we can resort to the more general non-equilateral scrambling.

ISSN 2348 – 8034
Impact Factor- 4.022

2. *Watermarking:*

Embedding algorithm is one of the most key problems in watermarking. There are three main categories of watermark embedding algorithm according to the different domain-based: time space domain, transform domain and compressed domain. Considering the JPEG compression and the Watermarking Constrain, the embedding algorithm of dithered modulation based on block DCT is chosen to realize image CEW.

Dithered modulation modulates the quantizing interval according to the embedding information. The object of DCT dithered modulation is the amplitude or phase of DCT coefficients. This paper consults the embedding algorithm of DCT coefficients' bipolar quantization.

3. *Algorithm processes*

In consideration of JPEG compression and the proposed CEW scheme's adjustment constrain, scrambling is in units of image's 8×8 macroblock and only 1 bit watermark is embedded into one 8×8 macroblock. For an M×N gray image X (the luminance component when carrier is a color image), the watermark is an M'×N' binary information sequence w, where M'=M/8 and N'=N/8. If M or N isn't multiple of 8, then, just as JPEG suggested, repeat the last row or the far right column of image data to achieve. In order to keep the invisibility and robustness of watermark, the low-medium frequency AC coefficients is chosen to operate.
Under the proposed CEW, encryption and watermark embedding can be carried out in the same time. Remote sensing image is encrypted and watermarked before being distributed. The concrete steps of the remote sensing image CEW algorithm, which is based on scrambling and block DCT dithered modulation, are listed as follow.

- Selecting scrambling key K_s. According to the actual requirements, select scrambling parameters, such as scrambling time, initial drift pixel, transfer matrix, etc. All these parameter settings are saved as scrambling key K_s.
- Encryption. The original remote sensing image X will be scrambled in units of 8×8 macroblock by n1 times under the control of K_s. The operation result is ciphertext X_s.
- DCT transform. X_s is manipulated by 8×8 block-DCT and the result is denoted as $X_{sw'}$.
- Watermark embedding. Under the control of embedding key K_e, an odd number of low-medium frequency AC coefficients are randomly selected from each 8×8 macroblock to repeatedly embed the corresponding watermark information wi by DCT dithered modulation. After all wi being embedded, watermarked ciphertext in DCT domain $X_{sw'}$ would be got.
- DCT inverse transform. X_{sw} becomes the encrypted-watermarked image X_{sw} after DCT inverse transform. Note that, during the processes of watermark embedding, for the sake of robustness and security, the quantization step is up to the selected JPEG quantization table and the watermark w should be randomized before embedding.

For the proposed CEW integrating scrambling and watermarking, which are independence in mechanism, to realize the operation noninterference, the decryption and watermark extracting can be done separately. The same with the normal processes, the decryption of Periodical Scrambling is: under the control of K_s, X_{sw} will be scrambled in units of 8×8 macroblock by n_2 times to get decrypted watermarked remote sensing image X_w, where $n_1+n_2=aN$ .No matter encrypted or not, the proposed CEW can extract watermark from watermarked remote sensing image. The steps of watermark extracting are given as follow:

- DCT transform. The watermarked remote sensing image X_w or X_{sw} is manipulated by 8×8 block-DCT. The result is denoted as $X_{w'}$ or $X_{sw'}$.
- Watermark extracting. Under the control of Ke, all embedded ACs of each 8×8 macroblock are found out to extract watermark information according to the DCT dithered modulation. It must be pointed out that: watermark extracted from Xw is ciphertext and it must be scrambled in units of bits by n3 times.

ISSN 2348 – 8034
Impact Factor- 4.022

IV. INTEGRATION OF ENCRYPTION AND WATERMARKING BASED ON ORTHOGONAL DECOMPOSITION

Proposed Work

Both encryption and watermarking carry out security protection by modifying data, and then direct superposition will certainly cause interference with each other: watermarking the encrypted data, the ciphertext error introduced by watermarking may cause the decryption failure; encrypting the watermarked data, watermark extraction is carried out in plaintext which still has the problem of data reveal. Therefore, how to avoid the mutual interference between encryption and watermarking becomes the key problem of integrating encryption and watermarking. Orthogonal decomposition is the linear expression of one vector with a set of orthogonal unit vectors. It has two characteristics: the change of any decomposition coefficient dose not affects other decomposition coefficients; the change of resultant vector may affect all decomposition coefficients. In other words, the decomposition coefficients are independent of each other, and in the same time, integrate into the resultant vector. Based on these, this paper integrates encryption and watermarking based on orthogonal decomposition and achieves the operation independence and operand mixture of encryption and watermarking.

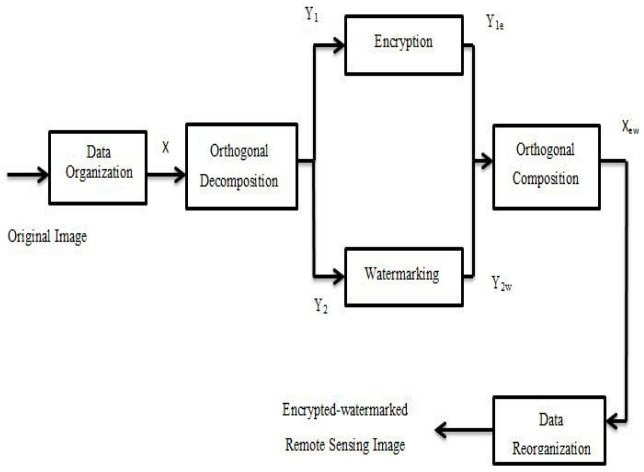

Fig 2: Diagram of the integration of encryption and watermarking based on orthogonal decomposition

The proposed method firstly organizes the original remote sensing image as a vector X; and then X is orthogonal decomposed under the control of orthogonal transformation matrix B to get the orthogonal decomposition coefficient vector Y as $Y = B^T . X$; in the following, Y is divided into two disjoint subsets $Y = (Y_1,Y_2)^T$ f for encryption and watermarking separately; in the end, the encrypted watermarked orthogonal decomposition coefficient vector $Y_{ew}=(Y_{1e},Y_{2e})^T$ is composed under the control of B to gain the encrypted-watermarked remote sensing image vector $X_{ew}= B \bullet Y_{ew}$. The hold process is shown in Figure 2.

According to the mentioned above, the operation objects of encryption and watermarking under the proposed method are not original remote sensing image data but its orthogonal decomposition coefficients. Then, based on the mutual independence of orthogonal decomposition coefficients, the operation order of encryption and watermark embedding does not affect the operation results: no mater encrypting first or watermark embedding first, there is the same encrypted-watermarked carrier; no matter decrypting or not, watermark can be extracted from the carrier. Based on the integrity of resultant vector, the operands of encryption and watermarking are mixed and inseparable in the user data domain: the remote sensing image is protected by encryption and watermarking. And, it is worth noting that, there is not any special requirement in selecting encryption and watermarking algorithms by the proposed method, which may enhance the applicability of the proposed scheme.

V.COCLUSION

This paper, in part, provides an overview of the many issues that must be addressed for security protection for sensitive multispectral images. In all existing systems, complete security analysis as well as watermark robustness analysis is not done. However, none of them have considered security aspect of watermarked multispectral images at dissemination.

This paper focuses on complete security protection for sensitive multispectral images by combining robust wavelet-based watermarking and encryption based on simple and efficient cipher. The proposed work depicts a crypto-watermarking scheme by combining watermarking and encryption to protect copyright of multispectral images and to provide security to the watermarked image at dissemination level. We have proposed wavelet-based watermarking and multiplicative-transposition-based cipher for encryption. The proposed watermarking system satisfies all multispectral image watermarking requirements. This approach is suitable for secure dissemination and protection of large size multispectral images by ensuring security as well as the robustness of the whole crypto-watermarking technique.

REFERENCES

[1] *Y. Xu, Z. Xu, and Y. Zhang, "Content security protection for remote sensing images integrating selective content encryption and digital fingerprint,"J. Appl. Remote Sens., vol. 6, no. 1, p. 063505, 2012.*

[2] *L. Jiang and Z. Xu, "Commutative encryption and watermarking for remote sensing image," Int. J. Digital Content Technol. Appl., vol. 6,no. 4, pp. 197–205, 2012.*

[3] *L. Jiang, Z. Xu, and Y. Xu, "A new comprehensive security protection for remote sensing image based on the integration of encryption and watermarking," in Proc. IEEE Int. Geosci. Remote Sens. Symp., 2013,pp. 2577–2580.*

[4] *Yongkui Li, Qiaosheng Feng, Fen Zhou, Qiang Li, "2-D Arnold transformation and nonequilateral image scrambling transformation,"Computer Engineering and Design, vol. 30, no. 13, pp. 3133-3135,2009.*