PROTECTION OF MULTISPECTRAL IMAGES USING WATERMARKING AND ENCRYPTION

HARSHA PUSHPAN[1], PRACHOD P PILLAI[2]

[1]PG SCHOLAR, Dept. of Computer Science & Engineering, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala
[2]Associate Professor, Dept. of Computer Science & Engineering, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala

---

Abstract – *The key problem in spatial information service is the copyright protection of multispectral images. This paper defines a scheme that combines watermarking and encryption for the protection of multispectral images. This paper proposes wavelet based watermarking and a secured multiplicative-transposition-based cipher for encryption. Experimental results show that the proposed algorithm provides good robustness against encryption attacks ,transparency, strength, large data hiding capacity, correct extraction of watermark, and strong robustness against JPEG lossy compression, filtering, and noise.*

***Key Words*: Multispectral image, Watermarking, Wavelet based watermarking, Encryption, Multiplicative and Transposition based cipher.**

1. INTRODUCTION

Digitising texts, images, videos are very easy in this era due to the advancement of technology. Digital data can be easily accessed and shared with the help of Internet. But this leads to misuse of digital data. The unauthorized acquisition of multispectral images and its preprocessing are cost- and manpower-intensive tasks. Hence, it is important to protect the ownership rights of the data owner and data processing . Digital watermarking serves as a good and efficient solution for the above said problem. Multispectral images are used in various applications including defense, which are related to national security, so need high level of confidentiality. This makes multispectral images highly sensitive and its confidentiality needs urgent attention. Therefore, certain precautions have to be adopted in handling the sharing of such sensitive and confidential images over the Internet.

Although standard and asymmetric encryption algorithms like AES, DES, and RSA are available, they cannot be implemented for multispectral images as the data volume is high and nature of multispectral images. A single key cannot be used for encrypting multispectral images. For multiple keys, key storage and implementation for such a high-volume data is impractical. Moreover, these algorithms are time consuming for encryption as well as decryption. The combination of encryption and watermarking could be the best solution to provide security and confidentiality for multispectral images.

2. LITERATURE SURVEY

The paper "Content security protection for remote sensing images integrating selective content encryption and digital fingerprint" by Y. Xu, Z. Xu, and Y. Zhang ,proposed a method by combining watermarking and encryption. They tried to embed watermark at decryption. This scheme does not provide total security and confidentiality as the encrypted image does not carry watermark.

L. Jiang and Z. Xu proposed "Commutative encryption and watermarking for remote sensing image" that implement commutative encryption and watermarking solution for remote sensing images. They used spatial scrambling based on Arnold scrambling for encryption using a symmetric scheme for whole remote sensing image. If the key is compromised, the whole encryption procedure would fail.

L. Jiang, Z. Xu, and Y. Xu proposed "A new comprehensive security protection for remote sensing image based on the integration of encryption and watermarking" to integrate encryption and watermarking using orthogonal decomposition of remote sensing images. This method has important effects on edges of remote sensing images and need to perform some preprocessing at watermarking to retainand recover edge information.

3. DISCRETE WAVELET TRANSFORM

The wavelet transform is based on function representing wavelets. Wavelets are mathematical function that represents both the scaled and translated copies of a finite-length waveform i.e, mother wavelet. It helps to calculate different frequency components of the given multispectral image at different resolution levels. Discrete wavelet transform (DWT) is a multi resolution description of an image that represents the mathematical function. DWT separates the signal into high- and low-frequency coefficients.

The high-frequency coefficients contain information about the edge components, while the low-frequency coefficient is

split again into high- and low-frequency coefficients. The 2-D wavelet transform decomposes an image into lower resolution approximation coefficients (LL) and detail coefficients such as horizontal (HL), vertical (LH), and diagonal (HH) coeffi- cients. Watermark embedding in low frequency (LL) increases robustness against compression, Gaussian noise, scaling, and cropping while watermarking in high frequency (HH) is robust to histogram equalization and intensity adjustments.

4. PROPOSED METHOD

Multispectral image mostly includes satellite images and aerial photographs. The demand for these data has increased dramatically due to the large number of applications capable to use them. Digital watermarking and encryption are used to achieve copyright protection and security of multispectral images at dissemination level. A wavelet-based algorithm is developed for copyright protection. Simple and strongly secure encryption based on multiplicative and two-stage transposition cipher is used to provide security at the transmission level.

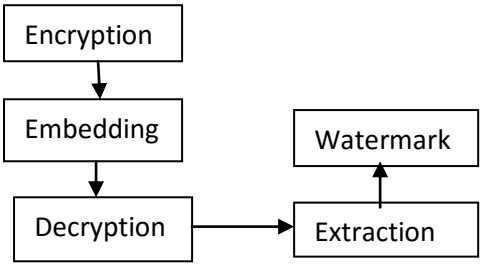

Fig 1 : Proposed System

4.1 Discrete Wavelet Transform

Wavelets are a special kind of mathematical functions, in DWT (Discrete Wavelet Transform) there is a need to deal with two sets of functions scaling functions and wavelet functions . Most of the scaling and wavelet functions are fractal. The commonly used wavelet functions are 'Haar, Daubechies, Symlets, Coiflets, Biorthogonal, Discrete Meyer etc. Filter cofficients of these wavelet functions are discrete.

The steps in watermark preprocessing are:

1) Watermark preprocessing: To enhance the robustness and security of the watermarking scheme, it is always desirable to apply basic transformation on watermark before embedding it into host data. Matrix interleaving is used in this method.

2) Watermark Embedding:

The embedding algorithm uses a binary image as watermark and color multispectral image as a host image. Host multispectral image is decomposed up to third level for the process of watermark embedding.

Algorithm 1. Watermark Embedding

Input: Host image (R), Binary Watermark (W), Matrix interleaved position (M)

Process:

(1) Scramble the watermark (length = N) using M

(2) Apply 2-D DWT on each channel of host multispec-tral image up to 3 levels (LL_3, HL_3, LH_3, and HH_3). Select $LL3$ and HH_3 coefficients for watermark embedding.

(3) At third level, calculate watermark strength (alpha) as a function of wavelet coefficients.

$$alpha = mean\ mean\ C_k^{ch}(i, j)$$

$$where\ i, j = 1, .., n\ ch = R, G, B\ k = LL_3, HH_3$$

(4) Watermark is embedded in selected wavelet coefficients as:

$$\mathrm{Ck}(i, j) + alpha \times W(l, m)$$

$$C_k\ \ (i, j) = C_k$$

$$where\quad i, j = 1..n\ l, m = 1 \ldots N \qquad ch = R, G, B$$

$$\mathrm{k} = LL_3, HH_3$$

(5) Apply inverse DWT to obtain watermarked multispectral image.

~

Output: Watermarked image (R)

Watermark Extraction

~

Input: Watermarked image (R), Host image (R), Arnold Key (A_k)

Process:

1) Using 2-D DWT, perform a third level decomposition of the watermarked host image.

2) Calculate alpha from selected coefficients (LL_3, HH_3) of each band of host multispectral image (R).

3) Extract the watermarks from LL_3 and HH_3 coefficients and perform averaging to get scrambled watermark.

4) Obtain the binary watermark (W) by applying inverse of matrix interleaving.

Multiplicative and Transposition Cipher-Based Encryption

For encryption and decryption of multispectral images, we are proposing multiplicative and transposition cipher (MTC) based on symmetric key multiplicative affine cipher and two-stage transposition cipher. Individually, they are vulnerable to brute force, statistical, and cipher text-only attacks. However, combination and proper cascading of these ciphers provide more secure and strong cipher than the individual.

We are applying MTC on multispectral image (red, green, and blue channel) of size $M \times N$ and gray levels G. Even and odd row elements are multiplied by EK_{ER} and EK_{OR}. Each row and column are shifted by EK_{SR} and EK_{SC} . Even and odd column elements are multiplied by EK_{EC} and EK_{OC}. Multiplier parameters EK_{ER}, EK_{OR}, EK_{EC}, and EK_{OC} are relatively prime to G, whereas $0 < EK_{SR} < M$ and $0 < EK_{SC} < N$.

For RGB multispectral image, we have $(3 \times 6)!$ options for key arrangement. At decoder side, both the correct sequence of operations and correct keys should be available to get the correct decryption; otherwise decoder cannot recover the original image.

5. ANALYSIS

We have tested the performance of the proposed system on

different multispectral images of varying sizes on MATLAB on 2.27 GHz Core Duo Processor.

The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. Because many signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale.

Entropy converts any class other than logical to uint8 for the histogram count calculation so that the pixel values are discrete and directly correspond to a bin value.

Rough entropy measures calculation of the cluster centers which is based on lower and upper approximation generated by assignment of data objects to the cluster centers. Roughness of the cluster center is calculated from lower and upper approximations of each cluster center. In the next step, rough entropy is calculated as the sum of all entropies of cluster center roughness values.

A good encryption algorithm should robust against all kinds of brute force, cryptanalytic, and statistical attacks. The histogram of encrypted image should be uniform to avoid statistical attacks. Similarly, key space must be large enough to avoid brute force attacks. In this section, the robustness of the proposed encryption algorithm is presented. It has been observed that the proposed algorithm is robust against all the mentioned attacks.

Key Sensitivity Analysis: In MTC, correct encryption and decryption are highly sensitive to the utilized key space. Secure image cryptosystems need high key sensitivity so that the image cannot be decrypted correctly even if there is a very small change in correct keys. Key used in multiplicative cipher are more sensitive as inverse of these keys only exists if it is relatively prime to gray levels of an image. Original image cannot be obtained even if a very small change occurs in these keys. The sequence of operations in MTC is also sensitive, as a small sequence change can result into an incorrect decrypted multispectral image.

Histogram Analysis: The encryption algorithm is strong if it possesses good confusion and diffusion properties. Histogram analysis is used to demonstrate confusion and diffusion of the proposed scheme. The color variations in RGB channels of the original and encrypted image are represented in terms of histogram. It is observed that the histogram of the encrypted image is nearly uniformly distributed, and significantly different from the respective histograms of the original image. So the encrypted image does not provide clues to employ any statistical attack on the proposed scheme.

Table 1 : Entropy Analysis

Images	Original	Watermarked	Encrypted	Decrypted
Sat_image1	6.4189	6.4315	7.9980	6.4315
Sat_image2	7.4447	7.4448	7.9938	7.4447
Sat_image3	7.4549	7.4552	7.9910	7.4543
Sat_image4	7.3949	7.3951	7.9968	7.3945
Sat_image5	7.6163	7.6265	7.9960	7.6162
Sat_image6	7.8015	7.9222	7.9809	7.8000

6. CONCLUSION

It is important to protect the ownership rights of the data owner. Digital watermarking serves as a solution over the above said problem. Multispectral images are used in various applications including defense, which are related to national security. This makes multispectral images highly sensitive and its security needs urgent attention. In this paper crypto watermarking, a combination of watermarking and encryption to provide copyright protection form

multispectral images and secure delivery of copy righted multispectral images is proposed. During transmission, encryption can be used to prevent information leakage and protocol attacks.

Ownership can be proved later as invisible water mark is retained in the multispectral image. Ownership cannot be proved until and unless the original multispectral image is made available. It is observed that the proposed crypto-watermarking approach satisfies the security of encryption, the invisibility, robustness, and classification accuracy retention of watermarking. Moreover, this algorithm survives all the attacks having low-frequency as well as high-frequency characteristics as we have utilized both low- and high-frequency bands for watermarking. The same algorithm can further be used for hyperspectral images security at storage as well as the dissemination.

REFERENCES

[1] T. Hemalatha, V. Joevivek, K. Sukumar, and K. Soman, "Robust water- marking of remote sensing images without the loss of spatial infor- mation," in Proc. 10th ESRI India User Conf., 2009, vol. 1, no. 2, pp. 1–8.

[2] B. Kumari and V. Rallabandi, "Modified patchwork-based watermarking scheme for satellite imagery," Signal Process., vol. 88, no. 4, pp. 891– 904, 2008.

[3] P. Zhu and C. Chen, "A copyright protection watermarking algorithm for remote sensing image based on binary image watermark," Int. J. Light Electron Opt., vol. 124, no. 20, pp. 4177–4181, 2013.

[4] 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.

[5] 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.

[6] 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.

[7] S. Mallat, "The theory for multiresolution signal decomposition: The wavelet representation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 11, no. 7, pp. 654–693, 1989.