An Improved Method for Data Hiding and Secure Dissemination of Multispectral Images

Arya Divakaran
Dept. of Electronics and Communication, College of Engineering Cherthala, Alapuzha, India

Abstract
The acquisition and preprocessing of multispectral images are manpower-intensive tasks and costly. 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 Therefore, it is very important to protect the ownership rights of these images. Digital watermarking serves as a solution over the above problem. The paper proposes a novel and improved method for data hiding and secure dissemination of multispectral images using crypto-watermarking. Digital watermarking and encryption are used to achieve copyright protection and security of multispectral images at dissemination level. Haar based 2D DWT at three level 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. Arnold transformation is used to enhance the robustness and security of the watermarking scheme. PSNR and SSIM are the two parameters used to check the quality of the decrypted image and watermark image in this paper.

Keywords
Classification, crypto-watermarking, Discrete Wavelet Transform, Encryption, Multispectral Image.

I. Introduction

Remote sensing information is highly sensitive. With the development of spatial technology, information technology and communication technology, , it becomes easy to digitize text, images, videos, etc.Also digital data can be accessed and shared easily with the help of Internet. But this leads to rampant misuse of digital data.While it brings great convenience for the communication and sharing of remote sensing information, and contributes to the further application of remote sensing images, it also causes the uncontrollable duplication and spread of remote sensing images, making remote sensing images much easier to leak. The acquisition of multispectral images as well as preprocessing of multispectral images are cost- and manpower-intensive tasks. Therefore, 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. Moreover, the dissemination of such sensitive images over the publicly accessed Internet is prone to information leakage.Therefore, a content security protection method should be adopted to guarantee the security of remote sensing information during its transmission and usage so that the information's flow direction can be strictly controlled and the leakage of secret information can be prevented.

Security of multispectral images contains two aspects: security at storage and security at usage. These aspects can be very well handled by technologies like watermarking and encryption.There is plenty of literature available for watermarking of multispectral images both in spatial and frequency domain . However, none of them have considered security aspect of watermarked multispectral images at dissemination. Although standard encryption algorithms like AES, DES, and RSA are available, they cannot be utilized for multispectral images due to high-volume data and nature of multispectral images. A single key is not feasible for encryption of multispectral images. For multiple keys, key management for such a high-volume data is critical. Moreover, these algorithms take more time for encryption as well as decryption. Crypto-watermarking, a combination of encryption and watermarking can be the best solution to provide total security for multispectral images. In all existing systems, complete security analysis as well as watermark robustness analysis are not done.

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 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.

This paper is structured as follows. Section II gives brief overview of digital watermarking and discrete wavelet transform. Proposed work is presented in Section III. Section IV describes experimental results Conclusion. are discussed in Section V. Acknowledgment is drawn in Section VI.

II. A Brief Overview About

A. Digital Watermarking

Digital image watermarking is a method of embedding information in an image in such a manner that it cannot be removed. This watermark can be used for ownership protection, copy control and authentication. Any sort of copyright infringement forms a legal basis for prosecution.An effective watermarking technique for satellite images should have the following features:

1. **Imperceptible:** The watermark should be imperceptible to the naked eye.
2. **Undeletable:** The watermark must be undeletable, at least without visibly degrading the original image.
3. **Statistically Undetectable:** A pirate should not be able to detect the watermark by comparing several watermarked signals belonging to the same author.
4. **Unambiguous:** Retrieval of the watermark should unambiguously identify the owner.
5. **Easy Decodable:** The watermark should be readily detectable by the proper authorities.
6. **Selective:** The watermarking technique should not distort certain specific areas in the image.
7. **Blind:** The watermark extraction should not require the original image

The image watermarking algorithms can be classified into two categories: spatial domain techniques (spatial watermarks) and frequency domain techniques (spectral watermarks). The spatial

domain techniques directly modify the intensities or color values of some selected pixels while the frequency domain techniques modify the values of some transformed coefficients. The simplest spatial-domain image watermarking technique is to embed a watermark in the Least Significant Bits (LSB) of some randomly selected pixels. The watermark is invisible to human eyes but the watermark can be easily destroyed if the watermarked image is low-pass filtered or JPEG compressed.

B. Discrete Wavelet Transform

The wavelet transform is based on wavelets. Wavelets are mathematical function representing scaled and translated copies of a finite-length waveform called mother wavelet. It helps to analyze the given image in different frequency components at different resolution levels. Discrete Wavelet Transform (DWT) is a multiresolution description of an image.

DWT splits 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 [11]. 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) coefficients. 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.

III. Proposed Method

In this paper proposed a Crypto-Watermarking Scheme. 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 depicts the flowchart of the proposed scheme.

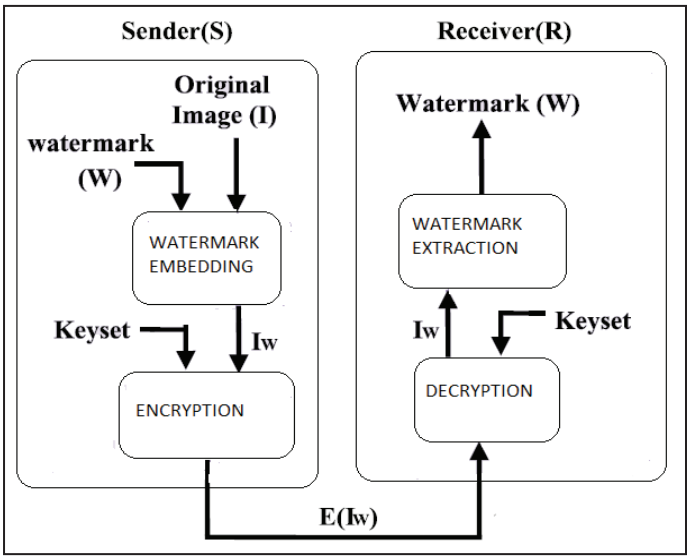

Fig. 1: Proposed Framework for Secure Dissemination and Protection of Multispectral Images

A. Wavelet-Based Watermarking

Although, general purpose image watermarking schemes can be applied to multispectral image, these schemes have to fullfill all the specific requirements for multispectral image watermarking. The requirements are:

1. The watermarking technique should not distort certain specific areas in the image
2. Less distortion
3. Good robustness against attacks
4. Invisible watermarking scheme
5. Retention of classification accuracy.

B.Watermark Preprocessing

To enhance the robustness and security of the watermarking scheme, it is always desirable to apply some transformation on watermark before embedding it into host data. Arnold transform is a simple, easy to implement, and iterative permutation method .In case of an attack on image, Arnold transform maximally disperses the damaged bits into different parts of the watermarks resulting into good robustness. Arnold transformation and its inverse for 2-D image are given by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad (1)$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod N \quad (2)$$

where N is the size of the image. When Arnold transform is applied on image, it randomizes original organization of pixels. On enough iterations (Arnold key), it generates the original image.

B. Watermark Embedding Process

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 watermark embedding. Low-frequency and high-frequency sub-bands are selected for watermark embedding to achieve acceptable performance of imperceptibility and robustness (Algorithm 1).

Algorithm 1. Watermark Embedding

Input: Host image (R), Binary Watermark (W), Arnold Key (A_k)

Process:

(1) Scramble the watermark (length $= N$) using Arnold's transformation using Arnolds key as given in equation 1.

(2) Apply 2-D DWT on each channel of host multispectral 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.

$$alpha = mean\left(mean\left(C_k^{ch}(i,j)\right)\right)$$
$$where\ i,j = 1,..,n\ \ ch = R,G,B\ k = LL_3\,, HH_3$$

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

$$\tilde{C}_k^{ch}(i,j) = C_k^{ch}(i,j) + alpha \times W(l,m)$$
$$where\ \ i,j = 1..n\ \ l,m = 1\ldots N\ \ ch = R,G,B$$
$$k = LL_3\,, HH_3$$

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

Output: Watermarked image ($\tilde{R}$)

C. Multiplicative and Transposition Cipher-Based Encryption (MTC)

For encryption and decryption of multispectral images,proposing ,MTC based on symmetric key multiplicative affine cipher and twostage 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. The final cipher generated using such cascading approach is so strong that it is very difficult to break it. The detail flowchart depicting sequence of operations and correct arrangement of keys at each operation is shown in fig. 2. We are applying MTCon multispectral image (red, green, and blue channel) of size M × N and gray levels G. Even and odd row elements are multiplied by EKER and EKOR. Each row and column are shifted by EKSR and EKSC. Even and odd column elements are multiplied by EKEC and EKOC. Multiplier parameters EKER, EKOR,EKEC, and EKOC are relatively prime to G, whereas 0 < EKSR <M and 0 < EKSC < N. Inverse MTC has keys DKEC,DKOC,DKSR,DKSC, DKER and SKOR for even columns, odd columns, shifting rows, shifting column, even rows, and odd rows, respectively, satisfying the conditions: EKER * DKER = 1(mod G); EKOR *DKOR = 1(mod G); EKEC * DKEC = 1(mod G); and EKOC * DKOC = 1(mod G). For RGB multispectral image, we have (3 × 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.

D. Watermark Extraction Process

Watermark extraction is the inverse procedure of embedding.A watermark is extracted by applying DWT on both original data and watermarked data.Low-frequency coefficients of both are compared to detect watermark W (Algorithm 2).

Algorithm 2. Watermark Extraction

Input: Watermarked image ($\tilde{R}$), Host image (R), Arnold Key (A_k)

Process:

(1) Using 2-D DWT, perform third level decomposition of the watermarked multispectral 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 Arnold's inverse transformation using equation 2 and Arnold key (A_K).

Output: Binary watermark (W)

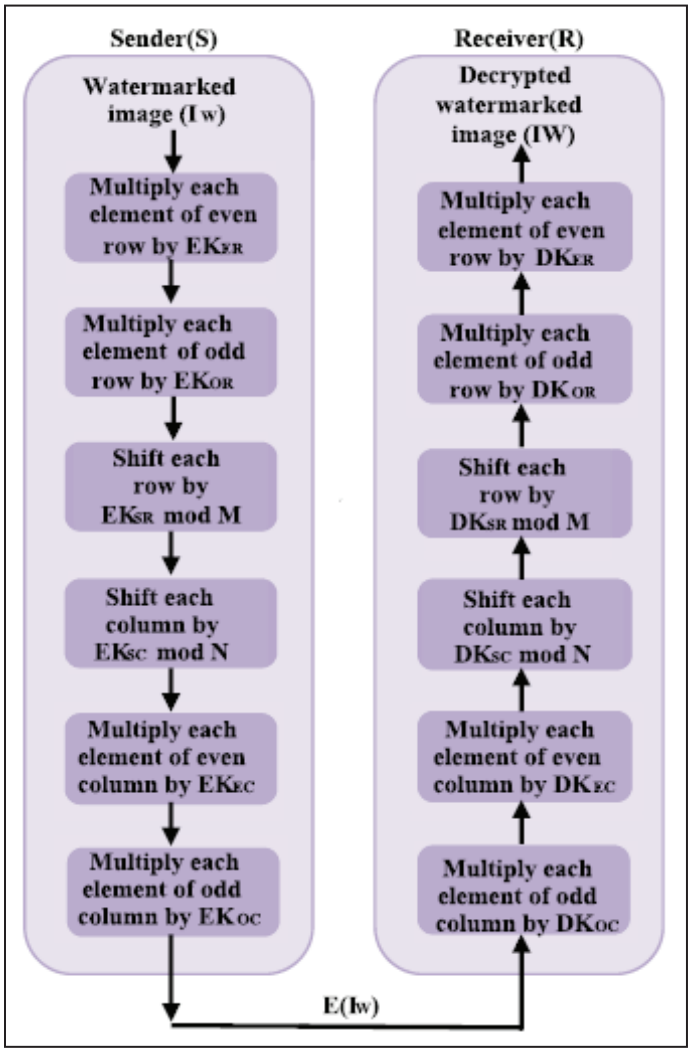

Fig. 2: MTC-based Encryption Scheme

IV. Experimental Result

Have tested the performance of the proposed system on different multispectral images of varying sizes. All the experiments are conducted on MATLAB on a machine with 2.27 GHz Core 2 Duo processor and 4 GB RAM. The watermark of size 25 × 50 pixels is used for watermarking. To improve the robustness of the watermarking scheme, original watermark is scrambled with Arnold's transformation. In the experiment, we have taken 27 as an Arnold's key for the watermark of size 25 × 50 which produces the scrambled watermark. The extracted watermark with NC = 1.We have considered "Haar" wavelet in our experiment. For encryption, MTC is proposed which combines multiplicative cipher with two-stage transposition cipher. Total 36 keys are used in encryption and decryption procedure.The result is shown in figs. 3-6.

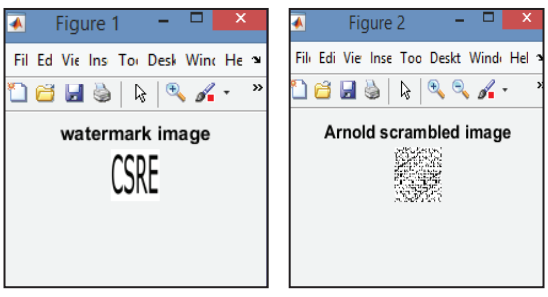

Fig. 3: Watermark Image and its Arnold scrambled Image

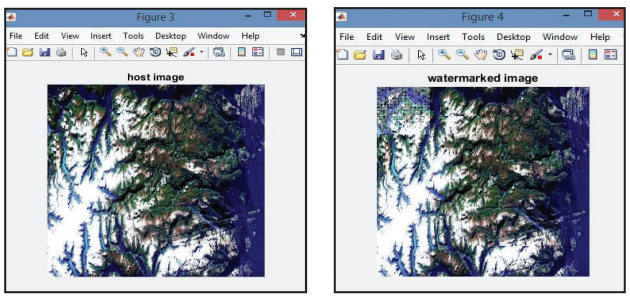

Fig. 4: Host Image and Watermarked Image

A. PSNR Result

PSNR is one of the most important objective evaluation indexes for image quality. The smaller value of PSNR means worse image quality and better perceptual security. The proposed scheme gives good encryption perceptual security as it has very less value of PSNR between original and encrypted as well as watermarked and encrypted multispectral image. The result is shown in Table 1.

Table 1: PSNR Result

Multispectral Images	Resolution	PSNR Values
Sat_Img1	1280 x 1280	68.5848
Sat_Img2	1160 x 1160	65.235
Sat_Img3	1150 x 1145	60.235
Sat_Img4	1148 x 1130	59.884

B. SSIM

SSIM is the Structural Similarity Index for measuring image quality .Using SSIM the structural similarity of input watermark and output watermark image can be analysed.Also the error analysing can be done using SSIM.The similarity between the encrypted and decrypted image can also done using this. The result is shown in Table 2.

Table 2: SSIM Result

Images	Resolution	SSIM Value
Out_Img1	40 x 40	1.00
Out_Img2	39 x 39	1.00
Out_Img3	38 x38	1.00
Out_Img4	38 x 37	1.00

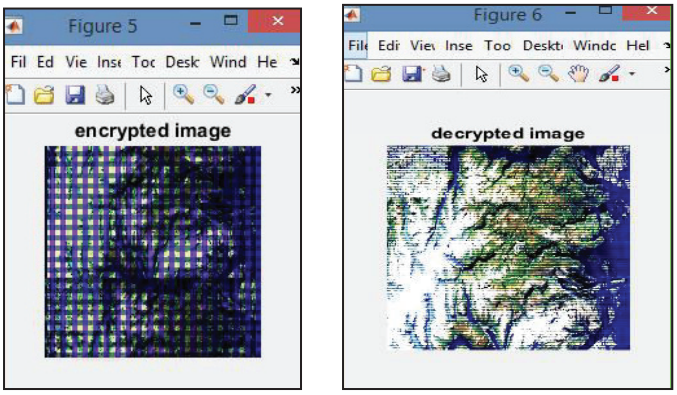

Fig. 5: Encrypted and Decrypted Image

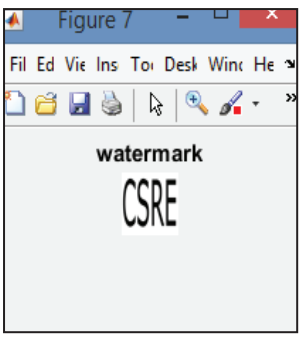

Fig. 6: Output Image

V. Conclusion

In this paper, we have proposed crypto-watermarking, a combination of watermarking and encryption to provide copyright protection for multispectral images and secure delivery of copyrighted multispectral images. During transmission, encryption can be used to prevent information leakage and protocol attacks. Ownership can be proved later as invisible watermark 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 at dissemination.

References

[1] M. Barni, F. Bartolini, V. Cappellini, E. Magli, G. Olmo, "Nearlossless digital watermarking for copyright protection of remote sensing images", In Proc. IEEE Int. Geosci. Remote Sens. Symp., pp. 1447–1449, 2002.

[2] Y. Chauhan, P. Gupta, K. Majumder,"Digital watermarking of satellite images," In Proc. 3rd India Conf. Comput. Vis. Graph. Image Process., pp. 235–240, 2002.

[3] T. Hemalatha, V. Joevivek, K. Sukumar, K. Soman, "Robust watermarking of remote sensing images without the loss of spatial information", In Proc. 10th ESRI India User Conf., Vol. 1, No. 2, pp. 1–8, 2009.

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

[5] P. Zhu, 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.

[6] B. Ziegeler, H. Tamhankar, J. Fowler, L. Bruce,"Wavelet-Based watermarking of remotely sensed imagery tailored to classification performance," In Proc. IEEE Workshop Adv. Techn. Anal. Remotely Sensed Data, pp. 259–262, 2003.

[7] Y. Xu, Z. Xu, Y. Zhang,"Content security protection for remote sensing images integrating selective content encryption and digital fingerprint," J. Appl. Remote Sens., Vol. 6, No. 1, pp. 063505, 2012.

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

[9] L. Jiang, Z. Xu, 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., pp. 2577–2580, 2013.

Arya Divakaran received her B.Tech degree in Electronics and Communication Engineering from College, College of Engineering Cherthala, Kerala, India in 2014 under CUSAT university. She completed her M.Tech degree in Signal Processing from College, College of Engineering Cherthala, Kerala, India in 2017 under KTU university.