ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 3, March 2016

Protection And Self Recovery Using Dual Watermark And Source Channel Coding Approach

W. Annie Felcia, X.M. Binisha

***Abstract*— Advancement in digital technologies has led to the increase in usage of digital images. When a change is made on the image, it is very difficult to identify the original image. The number of software used to alter the image has increased and hence the integrity of the image has become a question. These things led to the cause of increase in security of the image. Image tampering detection and localization are used in many applications including forensics. Watermarking is mainly used to check the security and authenticity of the image. In dual watermarking and source channel coding project, dual watermark is designed in such a way to detect and locate the tampering and restore the image. Tampering detection is done by using check bits and information is carried throughout the image by reference bit. Dual watermark is embedded and extracted on the receiver side to get the information hidden in it. Block decomposition is done to detect the tampering. SPIHT is used to partition the classification tree and error checking is done by Reed Solomon code. By comparing it with the real image, lost pixels can be recovered.**

Keywords— Self recovery, Tampering detection, Tampering localization, Watermarking.

I. INTRODUCTION

Light which passed through the surface led to the creation of first photographic image. Digital image has been used more often after its discovery. Its processing is easy and it requires less memory for storage than other methods like analog. The Digital image is obtained by taking a photo shot of an object. The image pixel are sampled and mapped accordingly as zeroes or ones. The pixels are converted into mathematical representation by storing the image and compressing it. The bits are interrupted by computer to display analog version. Photographs cannot be altered easily, hence they are considered as an unchangeable form. Medical, military, forensics, research, crime detection are some of the applications being used. By using digital image processing, the image can be altered. Some of the softwares used are Photoshop, cropping, editing, splicing, thickening etc. Due to this reason we cannot say if the image is original or not [12]. Tampered images can lead to illegal causes like the patients can change the image accordingly so that they can claim insurance and another example is that in case of crime scene if the image is tampered the criminal might become free of charges. The tampered image gives false information in the education field and students will also tamper images according to their own benefit which is illegal [4]. Watermarking is a process of hiding the digital information on the image [15]. It is used to prove authenticity and can be done by two methods embedding and extraction. The watermark is embedded in the image the information is extracted from the watermark. It is categorized into visible and invisible watermarking. Visible watermarking means the watermark appears visible to the eyes and provides authenticity. It does not affect the original image and can be used for advertisement purpose.

In Invisible watermarking unlike visible watermarking it does not appear to human eyes but it provides authenticity [6]. Based on the robustness it is divided into fragile, semi-fragile and robust watermarking. Fragile watermarking cannot tolerate all attacks hence tampering can be detected. In Robust watermarking it withstands all malicious attacks. Semi-fragile watermarking is a type of watermarking which is between fragile and robust watermarking [3]. Block wise and pixel wise are two tampering detection techniques. In block- wise technique the image is divided into large number of blocks and then processed. In pixel-wise technique the image is processed based on pixels. Previous method like hashing has the disadvantage that the same channel has to be reused.

Section II describes the structure of proposed work, section III describes about the dual watermarking method, section IV deals with encryption and decryption, section V deals with SPIHT and RS code, section VI deals with tampering detection and self recovery, section VII experimental results and analysis, section VIII deals with conclusion.

II. STRUCTURE OF PROPOSED WORK

Real image is given as input. Dual watermark is embedded on the image. Watermarking is mainly used to hide information on the image. In dual watermarking, visible and invisible watermarking is used. Image is encrypted by using hash algorithm for security purpose. The image is transferred. In the receiver side the dual water embedded is extracted from the image. The encrypted image is also decrypted on the receiver side. The real image is taken as 8 bits 5 MSB and 3 LSB. Dual watermarking is embedded on

Manuscript received Mar, 2016.

***W.Annie Felcia**, ECE, Pet Engineering College, Vallioor, India.*
***X.M. Binisha**, ECE, Pet Engineering College, Vallioor, India.*

All Rights Reserved © 2016 IJARECE

the 3 LSB. Check bits is used for tampering detection and reference bits to carry check bits. Check bits is used to determine the tampering detection. Hash is used as the encryption method. Decryption is the reverse process of Encryption. Only the authorized user

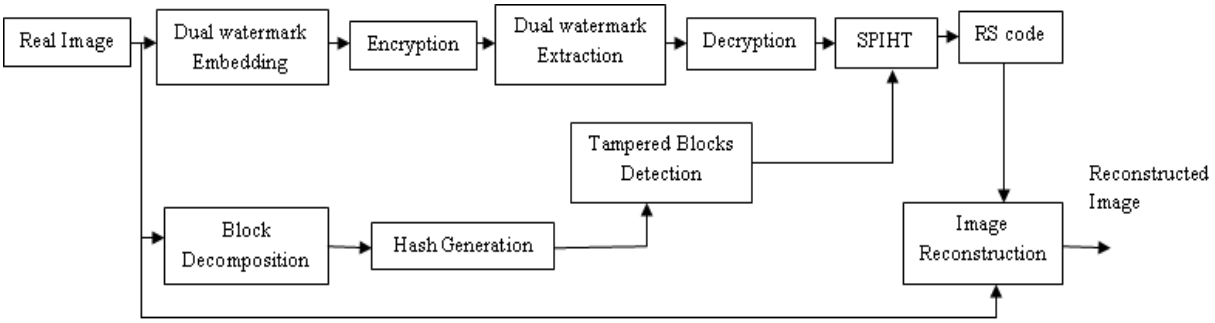

Fig 1.Block diagram

information. Random binary bits are ex-ored with hash bits to generate check bits which is transmitted along with dual watermarking. In the receiver side the image is divided into blocks respectively. The hash bit is ex-ored with check bits to obtain the binary bits. If it is equal it means no tampering present otherwise tampering is present. The block diagram is shown in Fig 1.SPIHT is applied to the image. It compresses the image by selecting the self similarities. Thus the storage is reduced. By using the Reed Solomon code the error can be detected and corrected. By using the reference data in 5 MSB the lost pixes can be recovered.

III. Dual Watermarking

Watermarking is the process of embedding information in the digital image. The requirements of watermarking are imperceptibility, Robustness and Security. In dual watermarking, two watermarks are used. They are visible and invisible watermarking. Visible watermarking means the watermark is visible and invisible watermarking means the watermark embedded is invisible. Dual watermarking is a combination of both visible and invisible watermarking. In the original image visible watermarking is embedded. The invisible watermarking is embedded on that image. If there is any problem with the primary watermark, the secondary watermark becomes active. Hence the security of the system is maintained.

The signal to noise ratio is found by using the formula

$$\text{SNR}= 10 \log_{10} \left(\sigma_i/\sigma_e\right). \longrightarrow \quad (1)$$

Where σ_i is the variance of the input image and σ_e is the variance of the difference between the input and output image respectively. The dual watermark is embedded in the transmitter side and information is extracted from the receiver side.

IV. Encryption and Decryption

Encryption is the process of encrypting the image in such a way that only authorized user can access it. The dual watermark embedded image is encrypted and transferred. Random binary bits are Ex-ored with hash bits to generate watermark which is embedded is extracted from the receiver side and is decrypted. Check bit is ex-ored with hash bit to generate binary bit.

V. SPIHT and RS code

SPIHT is Set Partitioning in Hierarchical Transform. It is one of the embedded compression algorithm. If more output rates are exploited the quality of reconstruction will be better. To obtain this it uses multi-resolution wavelet transform coefficients. The order in which it is sorted should be available to the decoder so that the reconstruction is easy. It finds the self-similarities by using the tree method.

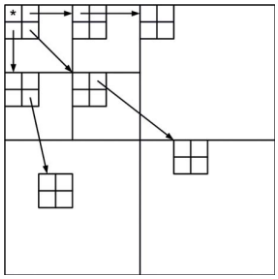

Fig 2.Tree Classification

The tree diag is shown in Fig 2. It has adaptive output rate hence applicable for applications with different compression rate. The PSNR value is calculated by

$$PSNR(n_w) = 10\log_{10}\left(\frac{255^2}{MSE(n_w)}\right) \longrightarrow \quad (2)$$

n_w is the watermark insertion. Reed Solomon code is used for error detection and correction. For large codewords it acts effectively such that it converts large words into single symbol thus reducing the number of words affected by tampering. RS(n, k) where R=k/n= n_s/n_c. The tolerable tampering rate is given by

$$TTR(n_s, n_c) = 1 - \frac{n_s}{n_c}$$

All Rights Reserved © 2016 IJARECE

→ (3)

n_s - source code bits, n_p - channel code parity

$$n_c = n_s + n_p$$

VI. TAMPERING DETECTION AND SELF RECOVERY

The image is divided into 8 bits. The image is divided into blocks accordingly. Check bit is embedded inside which is obtained by ex-oring the random binary bits and hash bits. In the receiver side the check bit is ex-ored with hash bits to obtain random binary bit. If it is same as that of the transmitter then it means no tampering is present otherwise tampering is present. 8 bits is divided into 5 MSB and 3 LSB. Dual watermarking is embedded in the 3 LSB. The 5 MSB consists of check bits and reference bits. Output from the RS code is examined with the 5 MSB to see if the image has any loss or is present without any loss if any pixel is lost it can be obtained from the reference data present in the MSB.

VII. EXPERIMENTAL RESULTS AND ANALYSIS

8 bit image is given as input. The original image is given in Fig 3. The cover image is given in Fig 4. Dual watermarking is embedded on the original image. In Previous methods some data might be lost. By using dual watermarking even if one watermarking is affected we can use secondary watermarking. Hence it is efficient. The dual watermarked image is shown in Fig 5.

Fig 3.Original image

Fig 4.Cover image

Fig 5.Dual watermarked image

Random binary keys are needed to be ex-ored with hash to generate check bits which is used to detect if tampering is present or not. Encryption process is used so that only the authorized user can access the image. Hash technique method is used here for encryption. The encrypted image is given by discrete wavelet transform. The lower plane and higher plane are taken respectively. Encrypted image is shown n Fig 6.

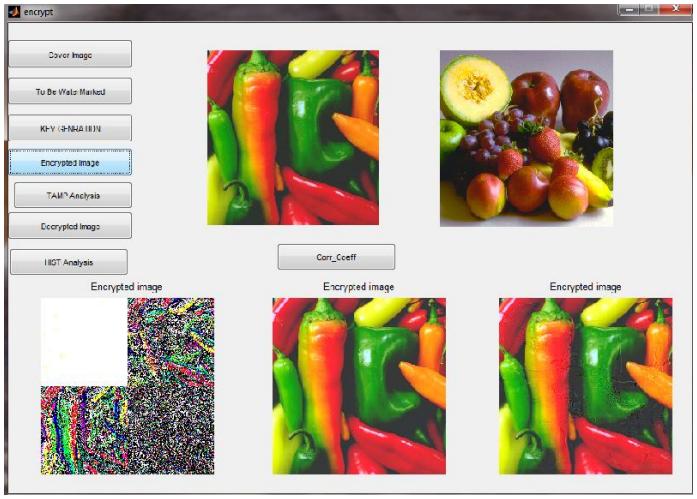

Fig 6.Encrypted image

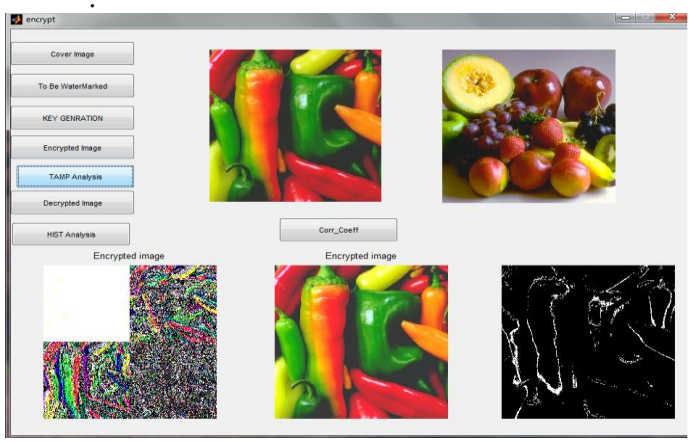

Fig 7. Tampering detection

Tampering is detected by ex-oring the hash code and check bits in the receiver side. If the binary number equals the random binary on the transmitted side it means no tampering is present. If there is change in the binary bit it means tampering is present. Self similarities are obtained by SPIHT code. It compresses the image hence storage is reduced. Reed Solomon code detects and corrects the error. If any data is lost it can be compared to the reference data which contains the details of the image. Thus the original image can be obtained.

VIII. CONCLUSION

Thus the tampering has been detected and localized by using dual watermarking and source channel coding approach. Image transmission was secured by using encryption and decryption and the tampering detection and localization was obtained using check bits and reference bits.. Binary key was Ex-ored with hash bit to produce the check bits. The comparison of binary key in sender and receiver led to detection of tampering, self-similarities will

All Rights Reserved © 2016 IJARECE

be obtained using SPIHT method. Error will be detected and corrected using Reed Solomon code and Self Recovery is obtained by comparing the result obtained from Reed Solomon and the 5 MSB bits.

Annie Felcia has done the B.Tech degree in Electronics and Communication Engineering in 2014 from Kalasalingam University and is pursuing M.e Communication Systems in Pet Engineering College.

X. M. Binisha is working as an assistant professor in Electronics and Communication Department, Pet Engineering College. She completed her B.e in 2008 from CSI Institute of Technology and M.e in 2012 from Pet Engineering College. Her area of interest includes Embedded and signal

REFERENCES

[1] S. Bravo-Solorio, C.-T. Li, A. K. Nandi, "Watermarking Method with Exact Self-Propagating Restoration Capabilities", WIFS 2012.
[2] Chao-Ming Wu, Yan-Shuo Shih, "A Simple Image Tamper Detection and Recovery Based on Fragile Watermark with One Parity Section and Two Restoration Sections", Optics and Photonics Journal, 2013, 3, 103-107**.**
[3] Chunlin Song, Sud Sudirman, Madjid Merabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images", ISBN 2009.
[4] Deepika Sharma, Pawanesh Abrol, "Digital Image Tampering – A Threat to Security Management", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2013.
[5] J. Fridrich, "Image watermarking for tamper detection," in Proc. Int. Conf. Image Process.(ICIP), vol. 2. Oct. 1998, pp. 404–408.
[6] Gurpreet Kaur, Kamaljeet Kaur, "Digital Watermarking and Other Data Hiding Techniques", IJITEE ISSN: 2278-3075, Volume-2, Issue-5, April 2013.
[7] Huijuan Yang and Alex C. Kot, "Binary Image Authentication With Tampering Localization by Embedding Cryptographic Signature and Block Identifier", IEEE Signal Processing Letters, Vol. 13, No. 12, December 2006.
[8] X. B. Kang and S. M. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Proc. Int. Conf. Comput. Sci. Softw. Eng., vol. 3. Dec. 2008, pp. 926–930.
[9] P. Korus and A. Dziech, "Efficient method for content reconstruction with self-embedding," IEEE Trans. Image Process., vol. 22, no. 3, pp. 1134–1147, Mar. 2013.
[10] Marco Tagliasacchi, G. Valenzise, and S. Tubaro, "Hash-based identification of sparse image tampering," IEEE Trans. Image Process., vol. 18, no. 11, pp. 2491–2504, Nov. 2009. [4] M. Wu and B. Liu, "Watermarking for image authentication," in Proc. Int. Conf. Image Process. (ICIP), vol. 2. 1998, pp. 437–441.
[11] Mehmet Utku Celik, Gaurav Sharma, Eli Saber, Ahmet Murat Tekalp, "Hierarchical Watermarking for Secure Image Authentication With Localization", IEEE Transactions On Image Processing, Vol. 11, No. 6, June 2002.
[12] Minati Mishra, Flt. Lt. Dr. M. C. Adhikary, "Digital Image Tamper Detection Techniques - A Comprehensive Study", International Journal of Computer Science and Business Informatics, Vol. 2, No. 1. June 2013, ISSN: 1694-2108.
[13] Saeed Sarreshtedari, Mohammad Ali Akhaee, "A Source-Channel Coding Approach to Digital Image Protection and Self-Recovery", IEEE Transactions On Image Processing, Vol. 24, No. 7, July 2015.

All Rights Reserved © 2016 IJARECE