A Semi-Fragile Multiple Authentication Technique for Authentication and Restoration in Digital Images

S Abhirami
M.Tech 4th sem Student
Dept of CSE,MSEC

Malatesh S H
HOD Dept of CSE,MSEC

Abstract—In this paper, a multimedia authentication and restoration scheme is proposed with the security of AES-128 ciphered watermarking and correlated watermarking. An encrypted or ciphered image embedding is done by modified version of Closest Point Transform (CPT) in a digital photograph. We perform several security attacks e.g. noise attack, compression attack, and cropping attack on multiple watermarked photographs and evaluated the proposed watermarking technique to examine the system robustness. Image Authentication is done by locating the tempered areas and restoration is performed by correlated watermark on the tempered region of watermarked photograph. The PSNR values are checked to evaluate the proposed watermarking technique. The results of PSNR, MSE, and SSIM show that the imperceptibility of our scheme is high compared to existing methods.

Keywords—Multimedia authentication, image restoration, multimedia security, digital photography, noise attacks, cropping attack, compression attack, Advance Encryption Standard

I INTRODUCTION

To secure the multimedia content various techniques are used e.g. cryptography, steganography, and watermarking. Each technique is used for its purpose. Cryptographic techniques are used to change the meaning of the documents. Steganographic techniques are used to conceal the existence of the important content. Watermarking schemes are used for protection and or authentication of multimedia content. In this paper, we have used semi-fragile watermarking technique for digital photographs. This is an era of advanced communication and modern technologies.With the evolution of digital and hand-held devices it is easy to make the digital contents. Multimedia content e.g. video, voice, and images are also saved in digital form. These contents are shared over online public community websites for various purposes with the aspiration of copyright protection and authorization Its real time application is that the photographers want to share their art and also want the copyright protection.The photograph should be secure and also the embedded watermark should not degrade the quality of the photographs. The degradation of quality of photographs limits the amount of data being embedded. For security purposes, the watermark should be robust and perceptually invisible so it could not be removed from the photographs. Watermark must survive the malicious attacks too. We hereby deal with the mentioned criterions, problems and methods for watermarking the digital photographs. The authentication of the photographs can be achieved by locating the parts of the photographs that are changed. If some areas in the photograph are changed or removed to change the meaning of the picture, so restoration of these malicious parts is done to solve the problem. In short, the watermarking authentication and restoration process of digital photographs is a new and an important area of modem research. Many researchers have put their efforts in the area of watermarking. Their contributions include content authentication, content verification , tampering localization,content restoration etc. However, robust watermarking techniques are insensitive to malicious attacks and thus it is difficult to detect the distortions or alterations performed in the watermarked content. Verification techniques are also proposed in literature which can detect that the content has undergone some distortions but they cannot locate the tamper locations. Content tampers localization techniques are available and they can localize the tampered areas but they fail to recover the tampered region. For authentication and additional ability of recovering the distorted image, multiple watermarking technique is required.Previous work in this area has been related to self-restoration techniques which are capable of restoring tampered regions once the regions localizations is done . In this paper we use the security of AES-128 and embed multiple watermarks: encrypted watermark and correlated watermark images. We encrypt the first watermark by AES, and correlate the second watermark with original

S Abhirami. Student [1] is with Dept. of CS&E, M S Engineering College, Bengaluru-562110, Karnataka. India. (E-mail: abhi1991132@gmail.com)
Malatesh.S.H HOD[2] Dept. of CS&E,M S Engineering College,Bengaluru-562110,Karnataka,India

IJERT

photograph. The first watermark embedding is done in the original photographs by our modified CPT algorithm. The second watermark is embedded in the wavelet sub-bands. First watermark is used for authentication purposes and second watermark is used for recovering the estimation of original photograph. By combining the restored version and the tampered one, we recover the photograph with a good quality.

II EXISTING SYSTEM

To secure multimedia content like images and videos, various techniques are used e.g. cryptography, steganography, and watermarking. Each technique is used for its purpose, watermarking mainly used for protection and or authentication of multimedia content. There are three categories of watermarking techniques developed for specific goals, robust watermarking, fragile watermarking and semi-fragile watermarking. Robust watermarks can stand up to malicious attacks and are difficult to remove from multimedia content, thus used for copy-right protection purposes. Fragile watermarks are easy to break and to remove from the multimedia contents, thus their existence or absence leads us to the conclusion of authentication. Semi-fragile watermarking techniques are used for both authentication and protection of data. In order to secure data in the images as well as recover the data, there is no single algorithm that works for both cases.

III PROPOSED SYSTEM

We propose a system which authentication and restoration of images is achieved by a series of watermarking techniques. Most existing systems only look at solving one problem at a time. Here we attempt to build image authentication system along with the additional aim of image restoration in case of an attack. This can be treated as a multi-stage process that addresses two important problems at one go. The authentication of the photographs can be achieved by locating the parts of the photographs that are changed. If some areas in the photograph are changed or removed to change the meaning of the picture, so restoration of these malicious parts is done to solve the problem. In short, the watermarking authentication and restoration process of digital photographs is a new and an important area of modem research. The proposed method uses the security of AES-128 and embeds multiple watermarks: encrypted watermark correlated watermark images. The first watermark is encrypted by AES. The second watermark is correlated with original photograph. The first watermark embedding is done in the original photographs by a modified CPT algorithm. The second watermark is embedded in the wavelet sub-bands. First watermark is used for authentication purposes and second watermark is used for recovering the estimation of original photograph. By combining the restored version and the tampered one, the system recovers the photograph with a good quality.

Encrypted watermark with AES 128

The method uses an AES 128 algorithm to encrypt the first watermark image as block by block approach by dividing the image into 4 blocks each of 128x 128 bits. First 128 bits in the first row of block# 1 are input to AES-128 module. The full block of 128 x 128 size is then converted to 4 x 4 square matrix of bytes. The cipher consists of N-rounds. The number of rounds depends on the key length. We used the key length of 128 bits and thus total rounds become 10. So we get the encrypted watermark, We in total 10 rounds. These rounds are taken to avoid the brute force attack.

Correlated watermark

The second stage involves correlated watermark generation. The second watermark image is created through correlation of the original photograph I(x,y) by using the equation given below.

where $I'(x,y)$ is the inverse of the photograph and the result is the correlated watermark image.

$$W_h = \frac{\sum_{x=1}^{X}\sum_{y=1}^{Y} I'(x,y) \times I(x,y)}{\sum_{x=1}^{X}\sum_{y=1}^{Y} I'(x,y)^2} \quad \ldots$$

Embedding watermarks into the image

The encrypted watermark W_e and correlated watermark W_h are embedded into the cover image respectively. The first watermark is embedded through extended version of CPT algorithm. In this CPT algorithm, only 2 bits/block are changed in the first bit plane and remaining bits in the present block are untouched. The remaining bits can be used to increase the embeddable payload size in Kb's. Teh embedding is performed in important locations per block by extracting the features from digital photographs. The features include saturation, intensity, and normalized contrast. Based on these features, the region of interest points per block is selected, and the encrypted watermark is embedded in the first bit plane, i.e. the decided threshold values of the features within each block decides the usage of certain points for embedding watermark. The second watermark W_h is used for the recovery of the tampered areas. For embedding in the cover image, the wavelet coefficient of W_h is used and embedded in the second level wavelet sub-band {HH2} and in third level wavelet subband {VV3}.

Retrieval and Decryption of watermark

It is the inverse process of embedding and encrypting the watermark. First watermark is obtained by first bit plane of the feature points from every block of cover image. Inverse AES is applied by the authorized key (128 bits) for each 4 blocks. Second watermark is retrieved from the wavelet sub-bands {HH2} and {VV3}.

IJERT

Block diagram with input and output

The basic block diagram for the watermarking system is shown in the diagram below.

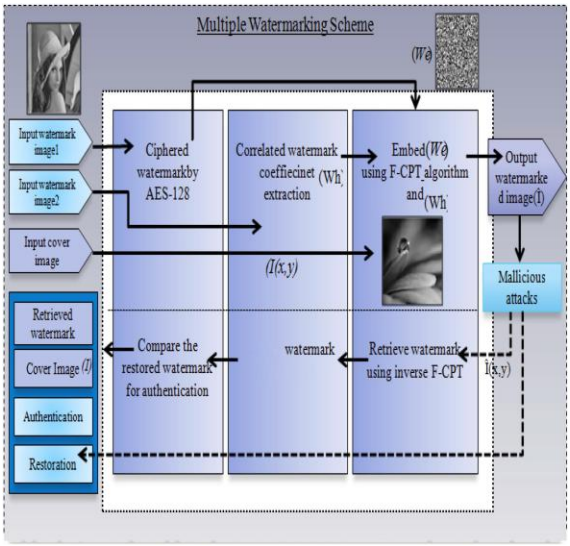
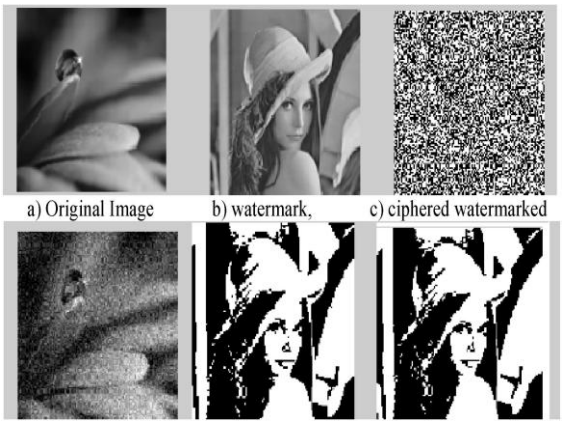


Fig3.1 Block Diagram

IV RESULTS



The results of embedding the watermark with AES-128 ciphering and recovering the watermark after noise.

V CONCLUSIONS

In this paper, a multiple watermarking scheme is proposed for digital photographs authentication and restoration. We used the security of AES-128 to make a ciphered watermark and embedded it in the cover image by F -CPT algorithm for content authentication. Image restoration is achieved by correlated watermark embedding in wavelet sub-bands. Several malicious attacks are performed i.e. noise attack, compression attack, and cropping attack etc. The results of PSNR, MSE and SS[M show that the imperceptibility of our system is high and the technique is highly robust.

VI REFERENCES

[I] G.-B. Shelly, M.-E. Vermaat, 1.-1. Quasney, S.-L. Sebok, 1. Jeffrey,"Multimedia and content sharing," in Discovering Computers 2009, Boston, USA: Cengage Learning, 2008.

[2] c. Paar, 1. Pelzl, "Introduction to cryptography and data security," in Understanding Cryptography: A Textbook for Students and Practitioners, reprint, Germarny: Springer, 2010.

[3] Z. Duric, M. Jacobs and S. Jajodia, "Information hiding: steganography and steganalysis," in Handbook of Statistics: Data Mining and Data Visualization, USA: Elsevier, 2005.

[4] B. Furht, D. Kirovski, "Protection of multimedia content in distribution networks," in Multimedia Watermarking Techniques and Applications, USA: CRC Press, Taylor and Francis Groups, 2006.

[5] E.-T. Lin, C.-I. Podilchuk, E.-1. Delp, "Detection of image alterations using semi-fragile watermarks," in Proc.SPlE 3971, 2000, p. 721-722.

[6] H.-T. Sencar, M. Ramkumar, A-N. Akansu, "Communication with side information and data hiding," in Data Hiding Fundamentals and Applications: Content Security in Digital Media, London, UK: ELSEVIER Academic Press, 2004.

[7] W. Huang, "Watermarking-based content authentication of motionJPEG sequences," in Proc. VIE, 2008, p. 813-818.

[8] R.-S. Alomari, A AI-Jaber, "A Fragile watermarking algorithm for content authentication," in IEEE Trans. JCIS, vol. 2, No. 1, April, 2004.

[9] S. Dadkhah, A-A Mana(S. Sadeghi, "EtlIcient digital image authentication and tamper localization techniques using 3Lsb watermarking," in T.TCSI, Internation Journal of Computer Science, vol. 9, issue. I, no. 2, January, 2012.

[10] X. Zhang, S. Wang, "Fragile watermarking with error-free restoration capability," in IEEE Trans. on Multimedia, vol. 10, no. 8, December, 2008.

IJERT