Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013

ISBN: 978-981-07-6260-5

A Novel DWT based Encrypted Watermarking

Monika Sharma[1] , Nirupma Tiwari[2] , Manoj Kumar Ramaiya[3] , Naveen Hemrajani[4]
[1]Department of Comp.Sci. & Engg., ShriRam College of Engg. & Mgmt., Gwalior, India
[2,3,4]Department of Computer Engineering, Suresh Gyanvihar University, Jaipur, India

***Abstract*—Digital watermarking is emerging as effective technique to protect copyrights. The propose paper present a novel technique to protect digital data by embedding encrypted watermark. In this technique discrete wavelet transform is used to embed the watermark image. Each pixel value is encrypted by using stream cipher and the key used is same for encryption and decryption. Key security is essential to protect digital data from unauthorized access. Experimental results verify that the proposed technique performs better and it can withstand compression attack.**

***Keywords*— Grey image, DWT, Image encryption. Stream cipher, digital water marking.**

I. INTRODUCTION

The growth of internet and web technology, digital data are transmitted must be authenticated, secured and copyright protected, so various information protection methods are developing day by day. Copy of digital data is more and more easy, digital watermarking has been propose a solution to copy of multimedia data in networked environment. To provide security two techniques have been used such as encryption and watermarking. Encryption can be used to protect digital data during transmission. In watermarking secrete imperceptible signal is embedded in original data. Digital watermarking has certain characteristic; the most important is robustness, imperceptibility and invisibility.

Digital watermarking is divided into two categories special domain watermarking and frequency domain watermarking. Most watermarking schemes use frequency domain such as DFT,DWT,DCT are more robust than special domain. Zhen Li,Kim-Hui yap and Bai-Ying Lei proposed a blind watermarking scheme.In which watermark is embedded into high frequency band of SVD DCT block [1].Robust watermark is generally used for copyright protection and ownership verification [2].R.Liu T.Tan, proposed SVD based watermarking scheme which is powerful transform technique. SV's are Image are stable when some bits are added. Sv's represent intrinsic algebraic image property [3].Song Qiang used bilinear interpolation for original image then use two level DWT to embed watermark. It is thwart collage attack with satisfied visual quality of image [4]. DES is most popular method, it is mostly used 64bit key to encrypt or decrypt data blocks. DES for image encryption is researched [5]. In the present paper, a new watermarking technique is developed in which encrypted watermark is embedded into two level DWT cover image. We know that watermark should be imperceptible, robust and secure against various attack. So Encryption is applied on watermark before embedding. The paper is organised as follows. In Section 2 proposed encryption process and embedding process is described in section 2 B watermark extraction process is described, in section 3 simulation results are shown. Finally, section 5 concludes the paper.

II. PROPOSED METHOD

In present paper, we proposed a novel scheme based on DWT and encryption method. Gray image of 512×512 is used as cover image to embed watermark. The watermark is 128×128 gray image with pixel value lying into [0, 255]. Here Pixel value of gray image is represented by 8 bits. Figure1 shows the 8 bit representation of a pixel in gray image. Suppose a pixel p (i, j) where (i, j) represent the pixel location in 128×128 watermark image and bits of a pixel P (i, j) can be represented as $B_{i,j,k}$ where K=0,1,2…..,7. Pseudo random bits $R_{i,j,k}$ are calculated by an encryption key using a stream cipher. Let 8 bits representation of a pixel value is 1 0 0 1 0 0 1 0 0 and pseudo random bits are 0 0 1 0 0 0 0 1 Exclusive-or operation on these two argument will be 0 0 0 0 0 1 0 1. Exclusive-or operation result will be encrypted bits, which ca vot be decrypted without the knowledge of key. Thus

$$E_{i,j,k} = B_{i,j,k} \oplus R_{i,j,k}$$

where i & j = 1,2,----------,128 and k = 0,1,..7.

A. Watermark encryption:

For encrypting the image, the exclusive-or is performed between watermark image and pseudo random bits. These pseudo random bits are used as encryption key. Same key is needed to decrypt the watermark image. Figure 2 shows the encrypted image using random key.

Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013

ISBN: 978-981-07-6260-5

Figure 1. Watermark image

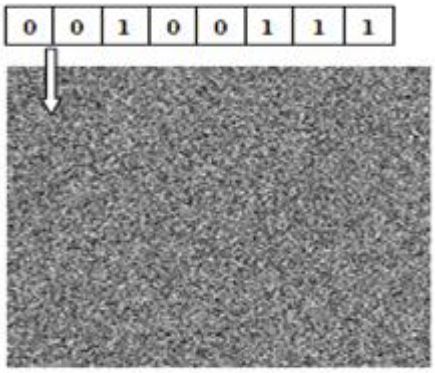

Figure 2. Encrypted watermark

For encrypting the watermark image, bits of each pixel is XORed with pseudo-random bits. Encryption of watermark image ensures the security of watermark from unauthorized attacks. Without the key information watermark cannot be decrypted.

B. Watermark embedding

For embedding encrypted watermark in cover image, 2-lavel DWT of cover image is obtained. A two dimensional cover image is transformed into the single level DWT, which decomposed image into four parts. Further decompose LL band of cover image by using DWT. Each 8 bit pixel of encrypted watermark is embedded distributively into the decomposed LL band of the cover image as shown in figure 3. First 3 bits are embedded in LL band, 2 bits in LH band, 2 bits in HL band and 1 bit in HH band of the 2- level DWT decomposed cover image. Corresponding bits of encrypted watermark will be appended into the least significant bits of 2-level decomposed cover image. DWT decomposed cover image is represented with 8 bits in which MSBs are kept intact, only least significant bits are replaced by encrypted watermark bits. Each pixel of encrypted watermark is spread in cover image in such a way that it provide more security and robustness.

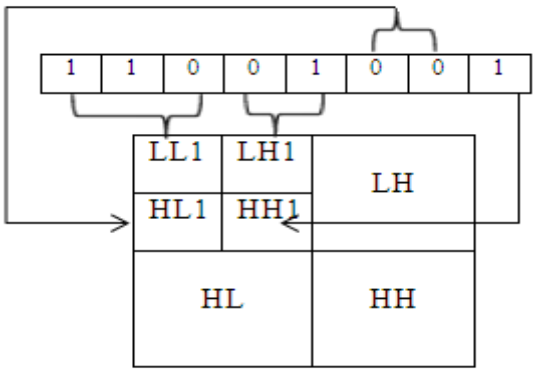

Figure 3. Block diagram of bits embedding

Each pixel of encrypted watermark is embedded into the corresponding pixels of the 2- level decomposed cover image. To ensure the robustness of proposed scheme watermark is embedded in to the low frequency coefficients of the cover image. Low frequency coefficients are chosen to provide protection against compression attack. Distribution of bits of a pixel is chosen to embed only 1 bit in HH band so that compression attack could not affect the watermark.

In the proposed scheme X-OR is used to assure security to the watermark image. Here 8 bit binary key is used to X-or with watermark image. Same key has to be used for encryption and decryption. If we want to extract the watermark image, we must obtain the secret Key.

The step of watermarking is as follows:

1) Decompose the original image I (N×N) by two level discrete wavelet transform (DWT) and represent pixel value in 8 bits.

2) Generate random key K of 8 bits.

3) X-OR each pixel of watermark image with key to encrypt the watermark.

4) Append 3 bits of encrypted watermark in LL band , 2 bit in LH, 2 bits in HL and 1 bit in HH band of 2 level DWT decomposed cover image. Bits will be appended into the LSBs of cover image.

5) This is the encrypted watermarking information.

C. Watermarking extraction process

There are so two types of watermark extraction process such as blind and non-blind, we use blind watermark

Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013

ISBN: 978-981-07-6260-5

extracting, so we do not required original image during extracting. The steps are as follows-

1) Inverse Transform to the watermarked image by two levels IDWT.

2) Choosing low frequency coefficient of two levels IDWT of watermarked image. Arrange LSBs form this band according to rule to generate encrypted watermark image.

3) Calculate the exclusive –or of the received encrypted image and key.

4) This is extracted watermark image.

III. SIMULATION RESULT

MATLAB 6.5 is used to simulate the proposed scheme. Figure 5 shows the watermarking encryption and decryption process. (a) is the original image of size (512×512), (b) is the watermark image of size (128×128), (c) encrypted watermark image, (d) is watermarked image (e) is the extracted watermark image and (F) is DES decrypted image using same key used in Encryption.

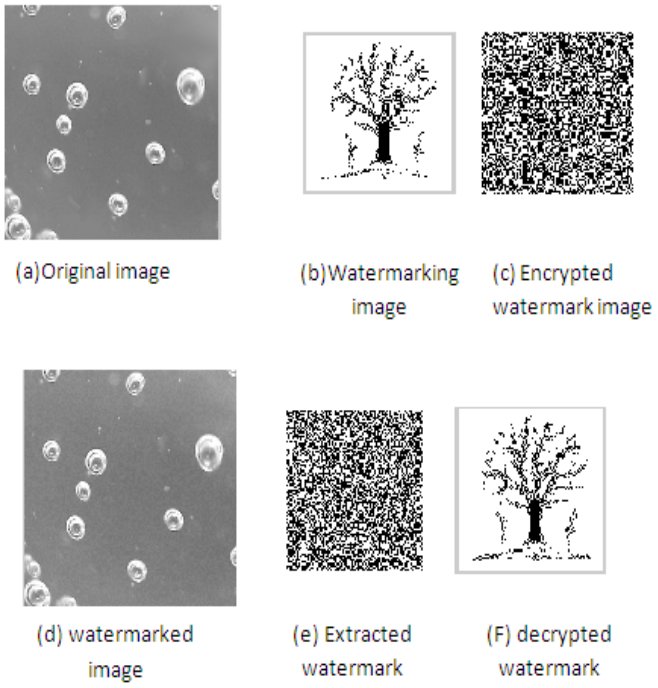

Figure 4. Image simulation results

TABLE1 PSNR between the watermarked image and original cover image.

Image Name	PSNR Value
Lena.tif	63.5744
bubble.tif	58.6624
camera man.tif	58.2467
Living_room.tif	59.1803
Mandil.tif	58.7140
Woman_dark hair.tif	58.6743
Pirate.tif	59.7569

TABLE2 PSNR between the compressed watermarked image and original cover image

Quality factor	90	80	70	50
Lena.tif	63.001	61.324	58.526	53.983

Table1 and table 2 show some experimental results to demonstrate the success of our technique for embedding and extraction of watermark in DWT domain.

For better understanding and quantitative evaluation, PSNR (Peak Signal to Noise Ratio) is introduced to evaluate the performance of proposed scheme and image quality. PSNR is defined as: The PSNR block calculates the peak signal-to-noise ratio between two images. PSNR value is often used as a quality measurement between the original and a watermarked image. The higher the PSNR, the better is the quality of the reconstructed image.

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are used to compare image quality. The MSE represents the cumulative squared error between the watermarked and the original image, whereas PSNR represents a measure of the peak error. The higher the value of MSE, the higher is the quality.

To compute the PSNR, first calculates the mean-squared error using the following equation:

$$MSE= \sum_{M,N} \frac{(I(m,n) - W(m,n))\hat{}2}{M \times N}$$

$$PSNR = 10 * \log10 \left(\frac{(255 * 255)}{MSE} \right) Db$$

The proposed scheme is experimented with different color images of size 512×512. To show the effectiveness of proposed scheme we have used images of different texture and contrast. Watermark of size 128×128 has been used for watermarking. Fig. 4 show the original images, watermarked images side by. Table 1 and Table 2 shows the effectiveness of the proposed algorithm.

IV. CONCLUSION & RESULT

Proposed model, a new color image watermarking algorithm based on the encryption and transform domain. The

ISBN: 978-981-07-6260-5

main contribution of this paper is to assure that it is quite efficient and easy to embed the encrypted watermark in dstributively. We also used DWT to embed image. Experimental results of the proposed scheme show that self–embedding method can effectively withstand attacks with satisfying adequate visual quality.

We can also use different watermark information derived from an image. Future work of this scheme is concentrating on the other scheme based on other watermark information and processing of the original image.

ACKNOWLEDGMENT

The authors' acknowledgment is due to Dr. Anil Kishore Saxena , Director, ShriRam College of Engg. & Mgmt. (SRCEM) for the all time encouragement and blessing to carry the research.

References

[1] Zhen Li,Kim Hui Yap and Bai-Ying Lei "A New Robust Image Watermarking Scheme in SVD-DCT compositeDomain"978-1-4577-1303-3/11 IEEE2011.

[2] I.J. Cox,J Kilian,F.T.Leighton,and T.Shamoon,"Secure Spread spectrum watermarking for multimedia,"IEEE Trans.Image Process.,vol 6,no. 12,pp.1673-1687,1997.

[3] R.Liu, T.Tan,"A SVD based watermarking scheme for protecting rightful ownwership",IEEE Transactions on Multimedia,vol.4,pp.121-128,2002.

[4] Song Qiang,Zhang Hongbin"Color Image Self-Embedding and Watermarking Based on DWT"978-0-7695-1/10IEEE2010.

[5] Jiang Qine-feng, Qian Gong, "A new Image Encryption Scheme Based on DES",IST 2009 – International Workshop on Imaging Systems and Technologys Shenzhen, china IEEE 2009.