Digital Watermarking using DWT and DES

Nirupma Tiwari
Department of Computer Science
Suresh Gyanvihar University,
Jaipur, India
girishniru@gmail.com

Manoj Kumar Ramaiya
Department of Computer Engineering
Suresh Gyanvihar University,
Jaipur, India
manojramaiya@gmail.com

Monika Sharma
Department of Comp. Sci. & Engg.
ShriRam College of Engg & Mgmt.,
Gwalior, India
monika.mini222@gmail.com

***Abstract*—The digital data are transmitted using the Internet. So digital data must be secure, copyright protected, and authenticated at the same time. This paper proposes an algorithm to protect digital data by embedding watermark that is encrypted by DES algorithm. Two level discrete wavelet transformation (DWT) is applied to the original image. This ensure robustness of the proposed scheme. DES encryption to the watermark with a key and iterating operations ensure security of the watermark information. Encryption and decryption key is same for both the process. If we want to extract the watermark image, we must obtain the secret key. The experimental result shows that the watermark is robust against various attacks.**

***Keywords*— Grey image, DES, DWT**

I. INTRODUCTION

The efficiency of digital watermarking algorithm is based on robustness of embedded watermark against various attacks. With the use of Internet technology, it is easy to copy the digital products such as text, digital audio, image, video. Therefore digital product must be secured . Many methods are available for protecting digital data. A method is used to improve the ownership over image by placing low level signal directly into image; this signal is called as watermark. A digital watermarking method is also available to solve the tamper proofing and authentication [1].

II. RELATED WORKS.

Kuo-Cheng Liu proposed HSV based watermarking scheme for color images in order to achieve robustness and transparency. A new just noticeable distortion (JND) estimator for color images is first designed in the wavelet domain and used in image coding for grey scale images [2]. Discrete wavelet transform convert image space to frequency. It is used to remove problem in DCT domain [3]. DES is most popular method, it is mostly used 64bit key to encrypt or decrypt data blocks. This method used in varies fields, such as electronic business , financial data[4] [5]. The key in DES is short and required iterative cipher. Des for image encryption is researched [6].

DES evolves from the Lucifer algorithm developed by IBM. It takes adequately advantage of permutation, substation, iteration and many common cipher operational methods [7]. It is widely used in information security and secure communication.it based on initial values, small changes in it affect the output.

III. WATERMARKING WITH ENCRYPTED WATERMARK

This algorithm starts with choosing original image and the watermark image. The block diagram of this method is shown in Fig. 1.

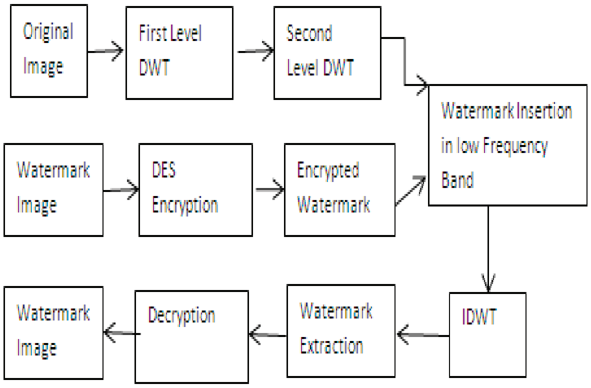


Fig. 1. Block Diagram of Watermarking Algorithm

DWT domain:-There are many frequency domain methods. DWT is one of them that analyse signal at multiple resolution or level.

A two dimensional image is transformed into single DWT, image is decomposed into four parts, one part is a low frequency of original image, the one bottom left is vertical details of the original image, the top right contains horizontal detail of the image , the bottom right block contains high frequency of original image, Again compute second level

978-1-4673-4529-3/12/$31.00 ©2012 IEEE

DWT of the image. The transform move grade by grade and model DWT decomposing is shown in Fig. 2.

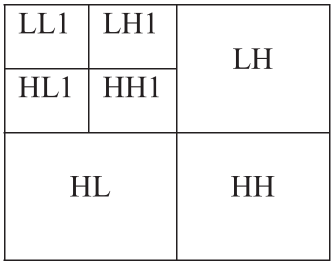


Fig. 2. DWT Decomposition

The low frequency coefficient contains most information of the original image, so it is more robust to embed watermark in this position. Watermark must be robust against compression so it is necessary to choose the low frequency of DWT to embed watermark. A digital binary image is used for the watermark. This digital image is divided into blocks of size 8×8. DES is applied on all these 64 bit blocks of binary watermark image with a same key. DES encrypted blocks are assembled to generate the watermark. The block diagram of DES is shown in Fig.3.

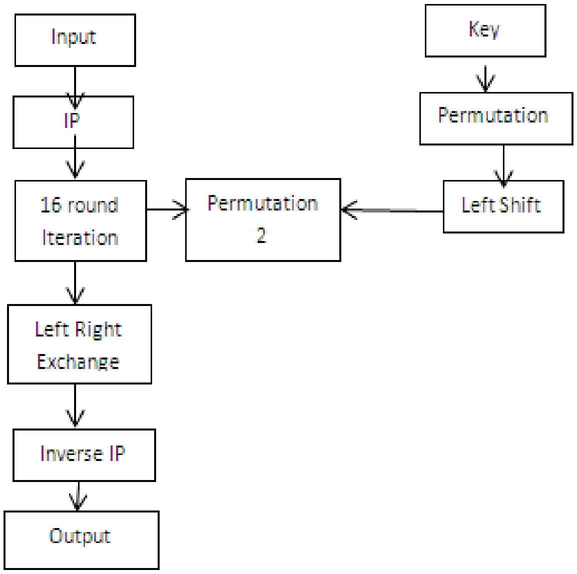


Fig. 3. Block diagram of DES

A. Watermark embedding process

In the proposed scheme DES is used to assure security to the watermark image. Block wise DES encryption ensures the effectiveness of the encryption method. Here 64 bit binary key is used. Same key has to be used for encryption and decryption. If we want to extract the watermark image, we must obtain the secret Key. Embedding coefficient also plays an important role to extract the watermark of satisfying visual quality. During the extraction process one should have knowledge of embedding coefficient.

The step of watermarking is as follows:

1) Decompose the original image I (N×N) by two level discrete wavelet transform (DWT).
2) Generate random key K of 64 bits.
3) Divide the binary watermark image of size ((N×N)/4) in blocks of size 8×8. Encrypt the image blocks with DES using key K.
4) Append all the encrypted image block to generate complete encrypted image W.
5) W is the encrypted watermarking information.

Choose the low level coefficient of two levels DWT let L to embed the encrypted watermark.

B. Watermarking extraction process

There are so two types of watermark extraction process such as blind and non-blind, we use non-blind watermark extracting, so we 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. Let the embedding coefficient is a and w* is extracted watermark.

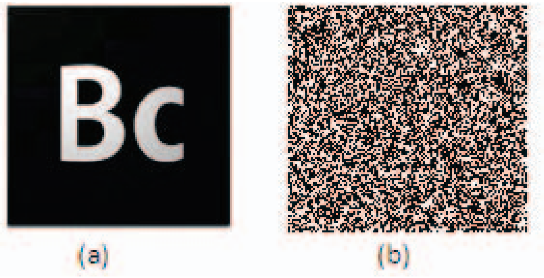
$$\mathrm{W}^{*}= \frac{1}{a}\,[\,W - L\,]$$

3) Divide the encrypted image W^{*} in blocks of size 8×8. Decrypt the image blocks with DES using key K.

4) Append all the decrypted image blocks to generate the watermark image.

IV. SIMULATION RESULT

MATLAB 6.5 is used to simulate the proposed scheme. Figure 4 (a) shows the binary watermark image of size 128×128, (b) is the encrypted watermark image, (c) is the correctly decrypted image and (d) is the wrong decrypted image.



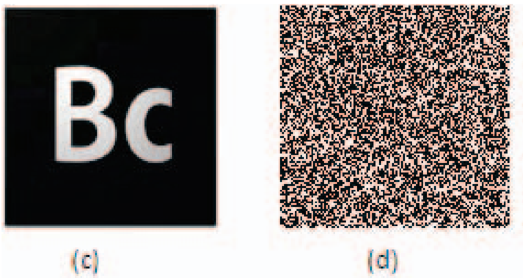


Fig. 4. Image simulation

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) DES encrypted watermark image, (d) is watermarked image with embedding coefficient 0.14, (e) is the extracted watermark image and (F) is DES decrypted image using same key used in Encryption.

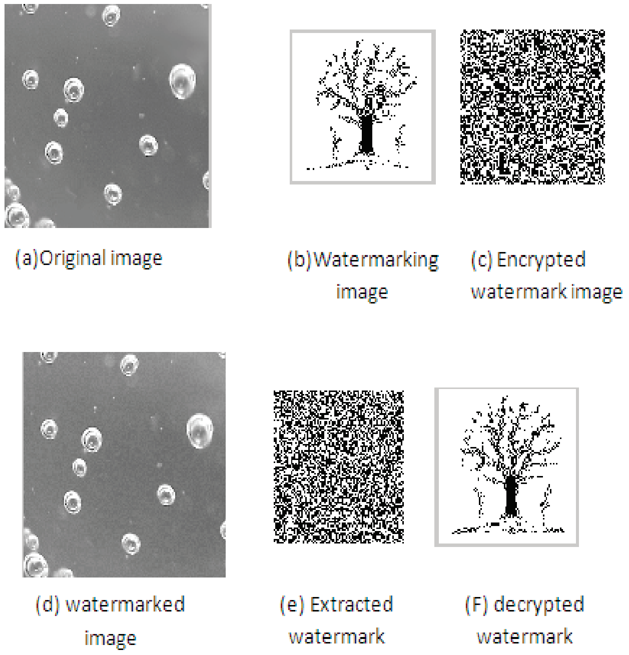


Fig. 5. Image simulation results

TABLE I Correlation coefficient between the decrypted watermark image and original watermark image with different quality factors.

Quality factor	100	90	70	50
Correlation coefficient	0.9201	0.9082	0.7620	0.7483

Table 1 and Fig. 5 shows some experimental results to demonstrate the success of our technique for embedding and extraction of watermark in DWT domain.

We applied correlation function to measure the similarity between decrypted watermark image and original watermark image and also calculated robustness against compression with varying quality factor.

A is original watermark image and B is decrypted watermark image. Correlation coefficient for A and B is calculated as:

$$\text{Corr\_coff} = \frac{\sum_{M}\sum_{N}(A(M,N)-\overline{A})(B(M,N)-\overline{B})}{\sqrt{(\sum_{M}\sum_{N}(A(M,N)-\overline{A})\text{^}2)(\sum_{M}\sum_{N}B(M,N)-\overline{B})\text{^}2)}}$$

Where $\overline{A}$ is mean of A(M,N), $\overline{B}$ is mean of B(M,N).

V. CONCLUSION RESULT

Proposed model, a new color image watermarking algorithm based on the self- embedding techniques. The main contribution of this paper is to assure that it is quite efficient and easy to embed the content of image in itself as a watermark. We used cubic interpolation to scale the watermark information. 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] Kundar D,hotzinakos Digital watermarking fot telltale proofing and authentication."procession IEEEspecial issue 1999.

[2] Kuo-Cheng Liu,"Human Visual System based watermarking for color image"IEEE 2009.

[3] Guangmin Sun,Yao Yu, "Dwt based Watermarking algorithm of color image"IEEE2007.

[4[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.

[5] Rush M David, "The encryption standards in perspective". Communication Mazine. IEEE vol.16,pp.5-9,nov1998.

[6] Maldonab J. A, Heenandez J.A., "Chaso theory applied to communicatior Mazine,.IEEE vol.16,pp.50-552007".

[7] L.Li. "The des encryption algorithm in information security," Modern Electronic Technique. Vol.9, pp. 118-120, Jan 2005.

[8] Guangmin Sun,Yao Yu, "Dwt based Watermarking algorithm of color image"IEEE 2007.