International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-4, April 2013

DWT Based Invisible Watermarking Technique for Digital Images

Pallavi Patil, D.S. Bormane

Abstract— The two most aspects of any image based steganographic system are the quality of the stego-image & the capacity of the cover image. A lossless data hiding scheme is presented based on quantized coefficients of discrete wavelet transform (DWT) in the frequency domain to embed secret message. Using the quantized DWT based method, we embed secret data into the successive zero coefficients of the medium-high frequency components in each reconstructed block for 3-level 2-D DWT of cover image. The procedures of the proposed system mainly include embedding & extracting. The original image can be recovered losslessly when the secret data had been extracted from stego-image.

Keywords— DWT, Haar Wavelet, Information Hiding, PSNR, Security,

I. INTRODUCTION

Information hiding is a technique in the field of information security presently. It hides the existence of important information into cover-object to form stego-object. A cover image is an image file into which a secret message will be embedded. A stego image is an image file which has been altered to contain a message. The Steganography is used for secret data transmission. In steganography the secret image is embedded in the cover image and transmitted in such a way that the existence of information is undetectable. The digital images, videos, sound files and other computer files can be used as carrier to embed the information. The object in which the secret information is hidden is called covert object. Stego image is referred as an image that is obtained by embedding secret image into covert image. The hidden message may be plain text, cipher text or images etc Steganography is a method of hiding secret information using cover images. Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range. One major category, perhaps the most difficult kind of steganography is text steganography or linguistic steganography because due to the lack of redundant information in a text compared to an image or audio.

Data hiding methods for images can be categorized into two categories. They are spatial-domain and frequency-domain ones. In the spatial domain, the secret messages are embedded in the image pixels directly. The most common methods are histogram-based and least-significant bit (LSB) techniques in the spatial domain. Steganographic model is proposed that is based on variable-six LSB insertion to maximize the embedding capacity while maintaining image fidelity.

Manuscript published on 30 April 2013.
***** Correspondence Author (s)
Dr. D. S. Bormane is working as Principal and Professor in JSPM˝s RSCOE, Pune, India.

In the frequency domain, the common well-known methods for data hiding are discrete cosine transformation (DCT)-based, discrete wavelet transformation (DWT) based on similar mechanisms. Joint photographic expert-group (JPEG) is a famous file for images.DCT is a widely used tool for frequency transformation. JPEG images are routinely used in Steganographic algorithms due to the most popular lossy image compression method. JPEG domain to embed the secret message into the medium-frequency coefficients of the DCT-transformed cover image.

The paper is structured as follows. Introduction is given Section I. A review of related work is in Section II. Section III presents the proposed method. Experimental Result is discussed in Section IV. Section V describes the Conclusion of the paper.

II. RELATED WORK

The least-significant bit (LSB) [11] insertion method is the most common and easiest method for embedding messages in an image. An image steganographic model is proposed that is based on variable-six LSB insertion to maximize the embedding capacity while maintaining image fidelity. For each pixel of a grey-scale image, at least four bits can be used for message embedding. Three components arc provided to achieve the goal. First, according to contrast and luminance characteristics, the capacity evaluation is provided to estimate the maximum embedding capacity of each pixel.

Cui-ling JIANG et al., [2] have presents the cover image is divided into non-overlapping blocks of 16×16 pixels instead of traditional dividing cover-image into 8×8 blocks and the DCT is used to transform each block. The DCT coefficients are quantized and embedded the secret messages. The method has the larger steganography capacity and better stego-image quality than the other methods. Hui-Yu Huang [1] proposes a technique lossless data-hiding method for a DWT. Using the quantization factors for DWT, our proposed approach can offer high hiding capacity and preserve the image quality of stego-images. The original image can be recovered losslessly when the secret data had been extracted from stego-images.

Guorong Xuan et al., [10] have presents a novel lossless data hiding method for digital images using integer wavelet transform and threshold embedding technique is proposed. Data are embedded into the least significant bit-plane (LSB) of high frequency CDF integer wavelet coefficients whose magnitudes are smaller than a certain predefined threshold. Histogram modification is applied as a preprocessing to prevent Overflow/underflow. Experimental results show that this scheme outperforms the prior arts in terms of a larger payload (at the same PSNR) or a higher PSNR (at the same payload).

Abdelwahab and Hassan [5] propose a data hiding technique in the DWT domain. Both secret and cover images are decomposed using DWT (1st level). Each of which is divided into disjoint 4x4 blocks. Blocks of the secret image fit into the cover blocks to determine the best match. Afterwards, error blocks are generated and embedded into coefficients of the best matched blocks in the HL of the cover image. Two keys must be communicated; one holds the indices to the matched blocks in the CLL (cover approximation) and another for the matched blocks in the CHL of the cover. Note that the extracted payload is not totally identical to the embedded version as the only embedded and extracted bits belong to the secret image approximation while setting all the data in other sub images to zeros during the reconstruction process. From literature review digital data hiding in cover image using wavelet gives the good results as compared to other methods

III. PROPOSED METHOD

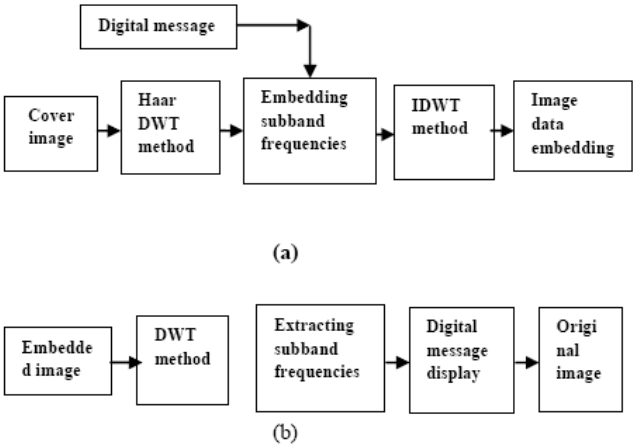

Fig.1 The proposed watermarking technique (a) Embedding process (b) Extracting process

The proposed watermarking technique is shown in fig.1 the proposed method embeds secret message into DWT coefficients in medium high frequency components and restores the original image coefficients after the secret messages have been extracted. Wavelet transform is used to converts an image from time or spatial domain to frequency domain. Decomposition of digital image will be pair of waveform with high frequency corresponds to detailed parts of an image & low frequency to smooth parts of image. The digital message will be embedding in medium-high frequency components & the image will be reconstructed to get cover image with digital message hidden. Embedded image decomposed into inverse discrete wavelet transform. Inverse wavelet transform is used to convert frequency domain to spatial domain. Hence it is frequency-time representation. Embedded image will be extracted in to sub-band frequencies using dwt method. The digital data will be taken from the medium high frequency components & the extracted digital data will be compared with original message. This system includes the procedures of embedding &extraction.

A. *Embedding Algorithm*

1. Set the secret key& size of image block for Embedding.
2. Read & display cover image.
3. Determine row & column size of cover image.
4. Read & display message image.
5. Determine row & column size of message image & reshape it into vector.
6. Cover image decomposed into 1st level decomposition using haar dwt & display image.
7. Add block size to Horizontal (H2), vertical (V2) &(D2) sub bands when message is 0 & 1.
8. Message is embedding in H2, V2 & D2 display the image .
9. Apply IDWT to the embedded image.
10. Watermarked image convert into unsigned 8-bit integer.
11. Write watermarked image to file.
12. Show the watermarked image.

B. *Extracting Algorithm*

1. Set the threshold wavelet coefficients of two details sub graphs.
2. Read & display watermark image.
3. Determine row & column size of watermarked image.
4. Read & display message image.
5. Determine row & column size of message image.
6. Watermarked image decomposed into 1st level decomposition using haar dwt & display image.
7. Add block size to Horizontal (H2) , vertical (V2) &diagonal (D2) sub bands when message is 0 & 1.
8. Reshape the message vector and display extracted watermark.
9. Watermarked image convert into unsigned 8-bit integer.
10. Write watermarked image to file.
11. Show the original cover image.

Fig. 2 Cover Images

Fig. 3 Cover Images

IV. RESULTS

The four gray-level test images with 384*384 pixels are shown in fig.2 & fig.3. The various keys used for testing were A=4;B=1;b=0.318.we use a 60*24binary message. The proposed method is tested using MATLAB. For performance evaluation, the visual quality of watermarked image is measured using the Peak Signal to Noise Ratio, which is defined in Equation (1).

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$$PSNR = 10\log(\frac{255^2}{MSE}) \quad (1)$$

Where MSE is mean square error defined in Equation (2)

$$MSE = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \frac{[OI(i,j) - DI(i,j)]^2}{M \times N} \quad (2)$$

Where OI and DI denote the gray-level values between original and watermarked image; M and N are the height and width of the image, respectively. The PSNR value of watermarked image is 38.5221& MSE is 8.6240, which indicates that there is very little deterioration in the quality of the image.

Table1- PSNR (db) & MSE of watermarked images under different attacks

Cover images	Attacks	Pepper & salt noise (nd=0.02)	Gaussian low pass (window3*3)	Median filter (window2*2)
Lena	PSNR	38.5221	38.6764	38.7450
	MSE	8.6240	7.8123	7.7909
Camera	PSNR	35.2198	36.3707	35.0257
	MSE	26.1667	19.1154	27.6007
Circles	PSNR	28.4534	32.9610	44.0769
	MSE	2.2928	0.7896	0.8337
Bird	PSNR	38.3772	38.3510	38.3771
	MSE	11.2413	10.7991	11.3846

The robustness of the proposed watermarking scheme is evaluated against several attacks including adding salt & pepper noise, median filter, Gaussian low pass filter, scaling, cropping, rotation & JPEG2000 compression. Table 1 shows PSNR & MSE of distorted watermarked images under above distortions.

We evaluate the robustness by adding salt & pepper noise to the watermarked image. In this test density of additive noise was 0.02. fig. 4(a1)shows adding salt & pepper. Extracted watermark is showed in fig. 4(b1) with high MSE value 8.6240.

We investigate the robustness by smoothing the watermarked image with median filter whose window size is 2*2pixel & Gaussian low pass filter whose window size is 3*3showed in fig. 4(a2) & (a3).

(a1)

(a2)

(a3)

(b1)

Figure 4.(a1), (a2) & (a3) watermarked image is degraded respectively through adding salt & pepper noise ,median filtering & Gaussian low pass noise (b1) the corresponding extracted watermarks.

V. CONCLUSION

We proposed a new robust watermarking scheme, which provides a complete algorithm that embeds & extracts the watermark information effectively. It has been confirmed that the proposed watermarking method is able to extract the embedded message watermark from the watermarked images that have degraded through pepper & salt noise median & Gaussian filtering. Lossless data embedding using a DWT to improve data hiding capacity & retain good stego image quality. Cover image within (text) message Embedded into Horizontal (H1) & vertical (V1) sub bands using Haar DWT & finally we get the stegoangraphic image and the hidden message is invisible.

REFERENCES

[1] Hui-Yu Huang & Shih-Hsu Chang "A lossless data hiding based on discrete Haar wavelet transform",10th IEEE International Conference on Computer and Information Technology, 2010

[2] Cui-ling JIANG"A Steganographic Method based on the JPEG Digital images" Institute of Information, East China University of Science and Technology,2011

[3] Anjali A. Shejul & Prof. U.L Kulkarni "A DWT based Approach for Steganography Using Biometrics", International Conference on Data Storage and Data Engineering, 2010

[4] Souvik Bhattacharyya and Gautam Sanyal "Data Hiding in Images in Discrete Wavelet Domain Using PMM", World Academy of Science, Engineering and Technology, 2010.

[5] Mohammad Reza Soheili "A Robust Digital image Watermarking Scheme Based on DWT" Journal of Advances in Computer Research, m2(2010) 75-82.1

[6] Adel Almohammad "High Capacity Steganographic Method Based Upon JPEG" The Third International Conference on Availability Reliability and Security, 2008.Y. K. Lee and L.-H. Chen, "High capacity image steganographic model", Vision, Image and Signal Processing, IEEE Proceedings, 2000

[7] Qingzhong Li, Chen Yu and Dongsheng Chu "A Robust Image Hiding Method Based on Sign Embedding and Fuzzy Classification", Proceedings of the 6th World Congress on Intelligent Control and Automation, 2006

[8] Mohammad Shirali-Shahreza "A New Method for Real-Time steanography" ICSP,2006 Proceedings

[9] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", IEEE International Journal of Applied Science and Engineering,2006

[10] Guorong Xuan, Yun Q. Shi & Chengyun Yang "Lossless Data Hiding Using Integer Wavelet Transform and Threshold Embedding Technique" 0-7803-9332-5/05/$20.00 ©2005 IEEE

[11] Y. K. Lee and L.-H. Chen, "High capacity image steganographic model", Vision, Image and Signal Processing, IEEE Proceedings, 2000

Ms. Pallavi Patil have done B.E (Electronic & Telecommunication) from North Maharashtra University, also pursuing M.E (Digital System) from JSPM's RSCOE, Pune University. Have published one paper in IEEE National Conference.

Dr. D. S. Bormane is working as Principal and Professor in JSPM's RSCOE, Pune ,Have done PhD in Engineering (EC & CSE) from S.R.T.M.U., Nanded in 2003 in area of 'Noise Filtering From Images Using Wavelet Based Techniques. Have published15 papers in International Journals,10 papers in IEEE Computer society, 24 in International conferences and 14 in National conferences. Area of interests are Digital Signal Processing Image & Speech Processing, Have memberships and achievements like – LMISTE,ISCEE,FMIETE etc.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)