Secure Pixel Transformation based Wavelet Image Watermarking System

Ankita Rastogi[1], A. K. Mohapatra[2]

[1] Department of Electronics and Communication Engineering, GGS IP University, Delhi, India
[2]Department of Electronics and Communication Engineering, GGS IP University, Delhi, India

Abstract: ***Securing the data or an image over the internet today becomes the most concerned topic. For proper utilization of bandwidth over the network, image is compressed prior to sending over the internet. To make sure that the image delivered from one end to the other end is free from intentional or unintentional attacks, we embed the watermark to the image. Watermark does not affect the size of the image, but increases the robustness of the image. This paper proposed a method to secure the wavelet based image watermarking through pixel replacement.***

Keywords: Image Compression, DWT, Watermarking, Blending Technique.

1. Introduction

Image Compression is the art of reducing the image data using compression function on to the input image to make it suitable for storage and transmission purpose. Compressed image not only occupies less storage space but also can reduce the transmission time by a factor of 2 to 10. Compression is classified in two categories: Lossy Compression (the original data cannot be retrieved back) & Lossless Compression (the original data can be retrieved back). Watermarking is a technique used to embed a hidden message within the host/cover image. It has been used extensively for various applications like proof of ownership, broadcast monitoring, copying prevention, data hiding, authentication etc. Many techniques have been proposed

Over the last few years, and many commercial products are already available.

2. Watermarking Domains

A. *Spatial Domain*

Earlier researches are based on watermarking schemes where the watermark is added by modifying pixel values of the host image. Generally, spatial domain watermarking is easy to implement from a computational point of view, but too fragile to resist numerous attacks [5].

B. *Frequency Domain*

After spatial domain, researches were directed towards watermarking in the frequency domain, where the watermark is not added to the image intensities, but to the values of its transform coefficients. Then to get the watermarked image, one should perform the transform inversely. Some of the transform based watermarking techniques used the Discrete Cosine Transform (DCT) like the one suggested in [6, 7]. Many image transforms like DCT (Discrete Cosine Transform) [2], DHT (Discrete Hartley Transform), Discrete Fouries Transform (DFT) have been considered. The lack of progressive transmission property in existing spatial- and frequency-domain watermarking algorithms limits their Internet applications. Then comes a new wavelet based watermarking techniques.

C. *Wavelet Domain*

Discrete Wavelet Transform (DWT) is most commonly used wavelet transform technique today. DWT (Discrete wavelet transforms) is the most effective and easy to implement techniques in watermarking. Due to its excellent spatial localization and multi-resolution characteristics, DWT has been used in digital image watermarking more frequently. The biggest issue in DWT-based image watermarking is how to choose the coefficients to embed the watermark. The approach includes modifying the largest DWT coefficients. This paper contributes to the implementation of 1 level DWT based image watermarking, in which the watermark which is generated by Random number generator is embedded in the DWT Coefficients of host image using the alpha blending technique.

3. DWT

DWT is a transform technique based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform DWT is the multi resolution description of an image the decoding can be processed sequentially from a low resolution to the higher resolution [8]. The DWT splits the signal into high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges. But in the proposed method, watermarking is done on the low frequency components.

The 1-level Discrete wavelet transform decomposes an image into four sub-bands-lower resolution approximation image (LL1), horizontal (HL1), vertical (LH1) and diagonal (HH1) detail components. The DWT algorithm is again applied on the approximation part LL1 which further decompose the LL1 part in four sub-bands LL2, HL2, LH2 and HH2 to compute 2 level 2D DWT.

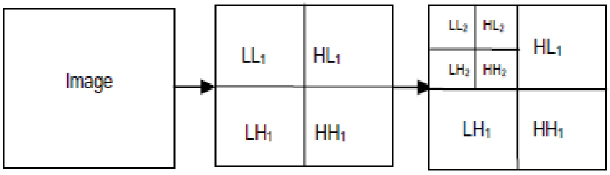


Figure1: 2 Levels DWT

4. Random Number Generator

A random number generator requires a naturally occurring source of randomness. A random number is a number generated by a process, whose outcome is unpredictable, and which cannot be sub sequentially reliably reproduced. The use of feedback shift registers permits very fast generation of binary sequences. Shift register sequences of maximum length (m-sequences) are well suited to simulate truly random binary sequences.
We have used an 8 bit linear feedback shift register with initial values [1 1 0 1 0 1 0 0] & three taps as 1, 4 & 7.

5. Proposed Method

Many researches are based on the spatial domain where the watermark is embedded into the host image by direct modification of the pixels of the original image. After that DCT, DFT and DWT came into picture which are based on the transformation of original pixels into other domains and transformation of watermark also and then applying blending technique. In this modified approach , we take DWT up to 1 level of the input original image and watermark binary random number sequence is generated using random number generator generating random values equal to the no. of bits to be modified in the original image.

Following are the steps to follow:

1. Taking 2D-DWT of the original image.

2. Locate M largest coefficients in the approximation coefficients of transformed image and their location such that
M< = W

Where W is the length of random sequence generated

3. M random numbers are generated which can be used as an encryption key through random number generator, to be considered as watermark sequence.

4. Embed the watermark to its M coefficients in the lower sub band LL1.

5. Replace the original Ri with computed Ri’.

6. Take inverse DWT with new computed Ri’ values.

7. Now, we will compute the PSNR and MSE for different
Values of alpha.

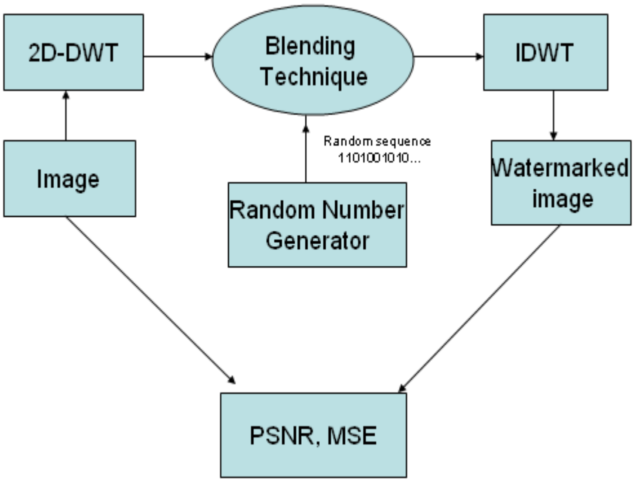


Figure 2: Proposed Method

6. Blending Phenomena

Technique used to blend a watermark on to the original image is based on the value of alpha, known as alpha blending.

Formula used to embed the watermark to the M coefficients
Of original image is

$$\mathbf{Ri' = Ri\ (1 + alpha * Wi)}$$

Where 1<i<M
Ri’= coefficient of watermarked image
Ri= coefficients of original image
Wi= random sequence number
Alpha= constant >0
Value of alpha controls the extent to which Ri’ alters Ri.

7. Experiment Results

Matlab software R2010 is used to perform the watermarking embedding and the whole experiment. Lena grayscale image with 512*512 dimensions is taken as the host image.

Fig (a): LENA 512 Gray Scale Image

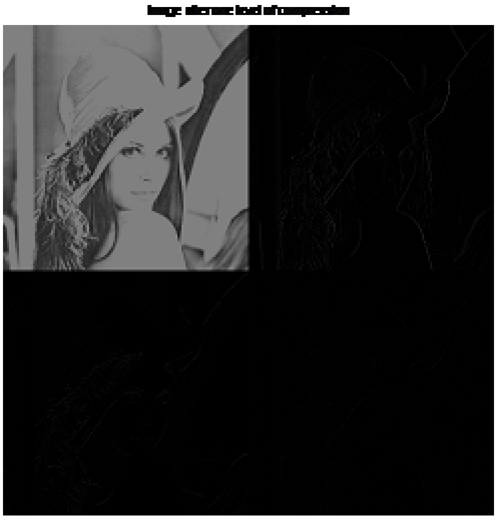


Fig (b): Lena Image after 1 Level DWT

Fig(c): Watermarked image, alp=0.1

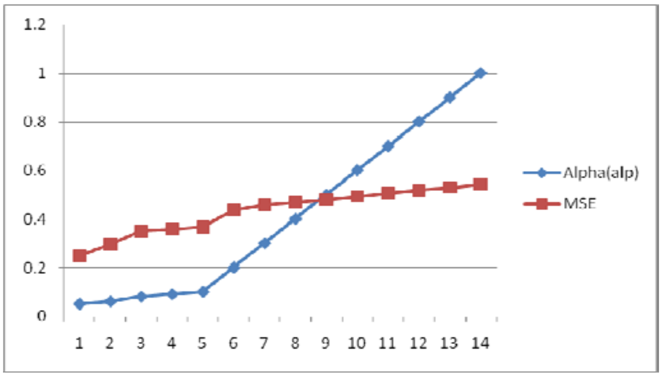
8. Observations

The watermarked image is compared with the original image on the basis of Mean Square Error (MSE) and PSNR (Peak Signal to Noise Ratio) for different values of alpha (alp).

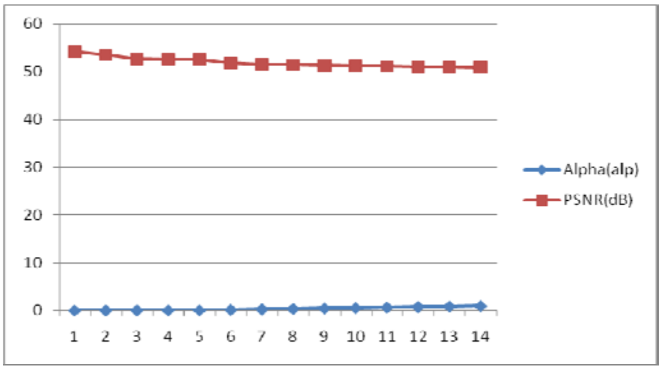
Table 1

Alpha(alp)	*MSE*	*PSNR(dB)*
0.05	0.2485	54.1779
0.06	0.2959	53.4186
0.08	0.3512	52.6752
0.09	0.3609	52.5568
0.1	0.3699	52.4497
0.2	0.4377	51.7191
0.3	0.4601	51.5025
0.4	0.4698	51.4119
0.5	0.4816	51.3060
0.6	0.4950	51.1846
0.7	0.5069	51.0813
0.8	0.5187	50.9814
0.9	0.5310	50.8795
1.0	0.5438	50.7765

As it can be observed from the table 1 and graphs that as the value of alp increases, the mean square error between the original image and watermarked image also increases whereas the PSNR decreases.



Graph 1



Graph 2

8. Conclusion

We can conclude by observing the experimental table and corresponding graphs that for best results, we should choose the value of alp such that MSE will be as small as possible and PSNR will be as large as possible. Considering alp 0.1 provides the best results. The image is securely watermarked using alpha blending technique with in differentiable visible appearance in the original and watermarked image. Here, we chose the blending technique to be applied to the values of approximation coefficients as this part contains most of the information details of host image.

References

[1] http:// www.bioinfo.in/ contents. php? Id = 33/ Advances in Computational Research, ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 4, Issue 1, 2012, pp.-42-45

[2] Cox and M. L. Miller, “A review of watermarking and the importance of perceptual modeling,” in Proc. Electronic Imaging, Feb. 1997.

[3] Evelyn Brannock, Michael Weeks, Robert Harrison, (2008) Watermarking with Wavelets simplicity leads to Robustness, IEEE.

[4] A.K. Goyal, N.Agrawal, S.Verma, (2007) Robust Watermarking in Transform domain using edge detection technique

[5] Jobin Abraham and Varghese Paul (2011) International Journal of Computer Applications, 31, 9-12.

[6] Juan R. Hernandez, Martin Amado and Fernando Perez-Gonzalez (2009) IEEE Transactions on Image Processing, 9(1), 55-68.

[7] Bo Shen, Iihwar K. Sethi and Vasudev Bhaskaran (1998)International conference on Image Processing, 1, 857-861.

[8] Asim Ali Khan, Parul Gupta. (2011) Recent Researches in Circuits, Systems, Mechanics and Transportation Systems, 168-171.

[9] http: //digital.cs.usu.edu/~xqi/ Teaching/ CS5650F03/ FinalProject/Watermarking.Barni.01.pdf

[10] http://www.ijcse.com/docs/IJCSE10-01-02-04.pdf

Authors Profile

Ankita Rastogi received the B.Sc (H). and M.Sc. degrees in Electronics from Delhi University and Barkatullah University in 2005 and 2007, respectively. She is now about to complete her M.Tech. degree in Electronics and Communication Engineering from Guru Gobind Singh Indraprastha University, Dwarka, Delhi. Her research activity is focused on Image watermarking systems, digital image processing & cryptography.

Dr. A. K. Mohapatra completed his Ph.D. in Information Technology from GGSIP University, Delhi. He is currently working as an Assistant Professor in the Department of Information Technology at Indira Gandhi Institute of Technology, Delhi. His research includes cryptography, information security and network security.