EMBEDDING IMAGE IN MID FREQUENCY BAND USING DWT TECHNIQUE

Amandeep Kaur[1], Blossom Kaur[2], Navneet Singh[1], Sukhdeep Singh[3], Parneet Kaur[2]

[1]Department of Information Technology, A.I.E.T, Faridkot.
[2]Department of Computer Science, A.I.E.T, Faridkot.
[3]Department of Electronics and Communication, A.I.E.T, Faridkot.

ABSTRACT

As for the ensurement of copyright protection of the cover image and the watermark, we propose a DWT based dual watermarking technique in which blind and non-blind algorithms are used. The binary image and the mid-frequency coefficients of the cover image are used to modify the DWT coefficients of the primary watermark .As some features are embedded in the watermark, the security is increased and it ensures the protection of watermark from any copy attack. For the fulfilment of the purpose a new pseudorandom generator based on the mathematical constant π has been developed. The unpredictable nature of the embedding process has been ensured by the incorporated randomness of the existing techniques in selecting the location to embed the watermark. Since the watermarked cover image with the signed-logo is subjected to various attacks like, rotation, noising etc, so the results show that it is very robust and has good invisibility.

KEYWORDS

Dual Watermark; Discrete Wavelet Transform (DWT), Signed-Logo.

1. INTRODUCTION

Watermarking is the technique of embedding data or a signal into a multimedia content such as image, audio or video. The embedded data can later be extracted from host data for security purposes. A watermarking algorithm consists of host data, the watermark, an embedding algorithm and an extraction algorithm. Watermarks should be imperceptible, robust unambiguous, and have a high capacity. Imperceptibility refers to the watermark that should be perceptually invisible such that the experience of viewing the image is not affected. Robustness is the resistance of an embedded watermark against intentional attacks. Unambiguity means the recovery of the watermark should unmistakably identify the owner of the watermarked image. Capacity is the amount of data that can be represented by an embedded watermark. Watermarking is done in two domains:-spatial domain and frequency domain.

Spatial-domain technologies refer to those embedding watermarks by directly changing pixel values of host images. Compared to spatial-domain watermark, watermark in frequency domain is more robust and compatible to popular image compression standards. Possible frequency image transformations include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform. The concept of dual watermarking, wherein, two watermarks are embedded instead of one for increased protection and security has been proposed earlier in both spatial and transform domains [3][4][7][8] .In this paper, Discrete Wavelet Transform (DWT) domain is used and the watermark is embedded in the mid-frequency region, in order to achieve perceptual invisibility as well as robustness to attacks. A new concept of embedding two watermarks into the cover image by actually embedding only one is introduced here, wherein features from the host image as well as the secondary watermark are used. This can be done by calculating the DWT coefficients of the primary watermark and secondary binary image (the sign), before embedding into the cover image. The sign is virtually embedded into the cover image through the logo i.e. the signed-logo is embedded into the cover image. Besides selecting the locations for embedding the watermark in the mid frequency region of source image, watermark pixels are also chosen pseudo randomly. [2] This helps us in achieving the security by two levels. The crux of the process is that we include both blind

and non-blind methods into one watermarking scheme i.e. the sign is embedded into the logo using non-blind algorithm which creates a signed-logo which is then embedded into the cover image using blind algorithm. The concept of signing the watermark rules out any possibility of malicious use of the watermark. The original logo is available only to the authentic receivers. The standard deviation of the second level and first level mid-frequency coefficients of the cover image are used in both blind and non-blind methods respectively [5][10]. To further increase the security a pseudo random number generator (PRNG) is used at various instances in the algorithm. This reduces the chances of watermark extraction by prediction. We have developed a PRNG based on the universal constant π[1].

The rest of the paper is organized as follows. Section 2 describes the pseudo-random number generator and Section 3 describes the non-blind embedding algorithm. Section 4 discusses blind embedding algorithm. In Section 5 we explain the watermark extraction operation. In Section 6 we present the experimental results and conclude in Section 7.

2. PSEUDO RANDOM GENERATOR

A pseudo random number generator is the key to provide security to the watermark. It is based on π and used in the embedding and extraction algorithm. The value of π is known to be a series of continuous and random numbers occurring in a non-repetitive manner. This pseudo random generator is used in determining the subblock locations and also in selecting the pixel values of the watermark which are to be embedded/extracted. The random number is generated as follows:

$$x(k) = pi(M) + i$$
$$M = M + j \qquad (1)$$

Where, $x(k)$ represents the selected number, M is the key used (K1, K2, K3, K4, K5), $pi(M)$ is m^{th} position of real part of π and i & j are the variable loop parameters. [9] The selections obtained from this sequence are more random and unpredictable. This randomness proves resistant to most of the attacks.

3. NON BLIND EMBEDDING ALGORITHM

The sign (p x q binary image) is embedded into the logo (m x n gray scale image) by the following steps:

1. Original logo is divided into various subblocks and pxq subblocks are chosen pseudo randomly for embedding each bit of the sign.
2. Each subblock S_i is decomposed into single level of DWT
3. All the wavelet coefficients of LH and HL subbands are raised or lowered by values K depending on the bit sign (i).
   - 3.1. If sign(i) is 0then $Ci\,(x,y) = Ci\,(x,y) - Ki$ (2)
   - 3.2. If sign(i)=1then $Ci(x,y) = Ci(x,y) + Ki$ (3)

Where $Ci\,(x,y)$ is wavelet coefficient of Si and (x,y) corresponds to the coordinates of the wavelet coefficients of the LH and HL sub bands inSi. The image dependent parameter Ki is derived from the standard deviation of the second level mid frequency coefficients of the cover image. Ki is also suitably quantized in the range of wavelet coefficients Ci.

3.1 Blind Embedding Algorithm

1. The proposed algorithm uses the standard deviation of the sub-blocks to determine the threshold levels.
2. Encoding is done using the private keys derived from PI PRNG to determine the embedding location within each of the selected sub-blocks and using a quantization factor Q.

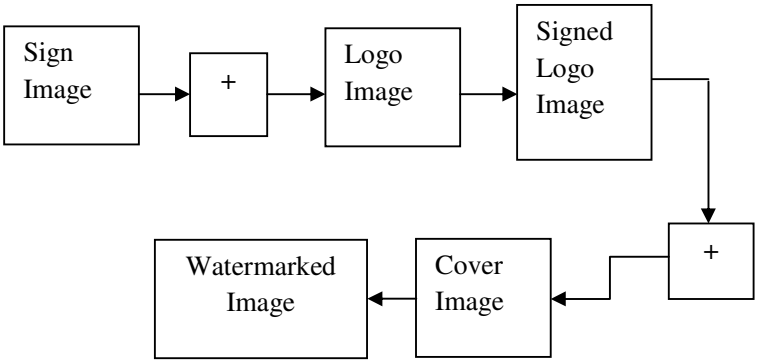

Fig 3.1 Embedding technique

The pseudo random generator is used to linearize the watermark into a $mn \; x \; 1$ pseudo-random sequence (Lw) using the keys K1, K2. The LH and HL sub bands of Im are used for embedding Wm. A total of mn sub blocks are chosen pseudo-randomly from LH and HL subbands using the key K5. Encoding is done using the keys K3, K4 to determine the embedding location (EM, a 2D array) within each of the selected subblocks. For any i^{th} sub block

$$mean(i) = \left(\frac{1}{M-1}\right) \sum_{(x,y) \in S_i} C_i(x,y) \qquad (4)$$

$$std(i) = \sqrt{\left(\frac{1}{M-1}\right) \sum_{(x,y) \in S_i} \{C_i(x,y) - mean\ i\}^2} \qquad (5)$$

Where the index i varies from 1 to pxq and indicates the subblock number; M is the total size of each sub block; Si refers to i^{th} sub block; $Ci(x,y)$ is the DWT coefficient of the location (x,y) within the i^{th} sub block. For i[th] subblock, the mean and standard deviation (std) are calculated using only (M-1) locations (i.e. excluding the embedding location $EMi(x,y)$. For finding the different threshold levels the following formula has been defined:

$$Th(j) = A * std(i) + B * j \qquad (6)$$

Where j is the running index which decides the 256 unique threshold values and A, B are secret keys. Based on the value of $Lw(i)$, a value is assigned to $EMi\,(x,y)$ depending on the value of the corresponding threshold $Th(i)$. A parameter Q is used for quantization as shown:

$$EM'i(x,y) = EMi\,(x,y)/Q \qquad (7)$$

where $EM'i\,(x,y)$ is the new value assigned to $EMi(x,y)$.

4. WATERMARK EXTRACTION

Extraction is the reverse of the embedding procedure .The extraction of binary watermark image from the watermarked image is explained in this sub-section.

4.1 Stage 1

The extraction in Blind doesn't require the original image or any of its characteristics but it requires watermarked image, size of watermark image, embedding strength. After extracting the wavelet coefficient C*i(x, y) is scaled back using the quantization factor Q.

$$Ci(x,y) = (C * i(x,y)) * Q$$
$$WM(i) = j \; if \; Ci(x,y) \in th(j) \pm const \qquad (8)$$

Finally the watermark (Wm*) is recovered from the above pseudo-random linear array (WM) using the same keys K1, K2. In some cases, the extracted coefficient may not correspond to any of the 256 thresholds calculated.

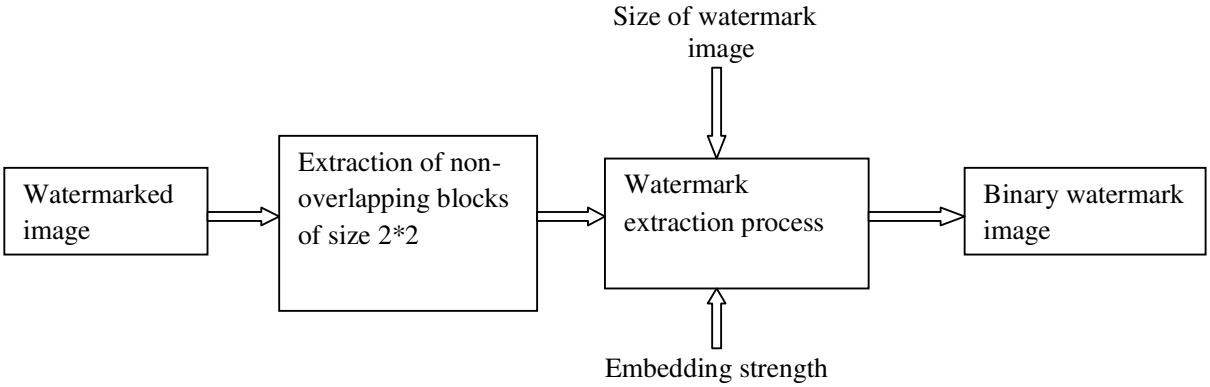

Fig 4.1.1 Block diagram of the watermark extraction process

4.2 Stage 2

From the signed logo which is obtained from stage 1 the sign is extracted using the original logo as follows: As explained in the embedding procedure, the original logo and the extracted logo are divided into sub blocks and transformation is taken. The sum of the mid-frequency coefficients of each corresponding sub block is then compared and based on their difference the sign bit is determined as follows.

If Sum (j) > Sum*(j) then the embedded bit
Sign (j) = 0
Else if Sum (j) < Sum*(j) then
Sign (j) = 1

where j refers to the sub block index and Sum and Sum* denote the sum of all the wavelet coefficients in the LH and HL sub bands of j^{th} sub block in original and signed logo respectively. During the process of watermark embedding and extracting, the initial seeds to the pseudorandom generator *(K1, K2)* <applied to Wm>, *K5* <to select different sub blocks> and *(K3, K4)* <to determine the embedding location within each sub block> are used as secret keys.

5. EXPERIMENTAL RESULTS

The cover/host image used is 512x512 grayscale 'Lena' and the logo is a 64x64 grayscale image of 'logo'. The sign is a 16x16 binary image having the letter 'm' on it. The various keys used for testing were K1=11, K2=21, K3=31, K4=41, K5=51, A=250, B=2.5 and Q=4800. The cover image which is watermarked with the signed-logo, is subjected to various types of noise. For each type of noise the results are computed for the maximum extent that can be tolerated.

Table 1: Watermarked image under Gaussian noise attack

Noise Density	**Watermarked Image (Db)**	**Watermark Signed-Logo(Db)**	**Extracted binary image-sign (dB)**
0.02	81.8867	43.4816	21.5730
0.04	76.4827	37.8410	15.8181
0.06	73.0076	35.1500	13.6340
0.08	70.4224	32.4872	12.1880
0.10	68.4146	31.9640	11.4630

Attacked Cover Image	Extracted Watermark (Signed-Logo)	Extracted Sign
		

Fig 5.1 the cover image, extracted watermark and the sign

Table 2: Watermarked image under salt and pepper noise attack

Noise Density	Watermarked Image (Db)	Watermark Signed-Logo(Db)	Extracted binary image-sign (dB)
0.02	51.5630	66.0850	46.6700
0.04	44.8889	59.6050	39.4360
0.06	40.8363	50.4966	34.7361
0.08	37.7028	49.2970	27.8042
0.10	35.6930	45.2100	22.5720

Table 3: Watermarked image under speckle noise attack

Noise Density	Watermarked Image (Db)	Watermark Signed-Logo(Db)	Extracted binary image-sign (dB)
0.02	52.1103	29.0887	8.0808
0.04	45.5115	28.9903	7.5722
0.06	41.6670	29.5545	7.2470
0.08	38.9855	29.1710	7.2470
0.10	36.9200	29.4982	6.8547

6. CONCLUSION

In this paper a new DWT based watermarking scheme is proposed which uses both blind and non-blind algorithms. The main aim of the algorithm is that besides protecting the copyright of the host image it also protects the watermark from any misuse. Since the embedding process uses data from the source image as well, the extraction of watermark by an unauthorized person is not possible. It thus serves the dual purpose of providing copyright protection to the watermark and increasing the security of the whole process. For this purpose a new pseudo random generator based on the mathematical constant p has been developed and used successfully at various stages in the algorithm. The new concept of applying pseudo randomness in selecting the watermark pixels makes the process more resistant to attacks. In the proposed technique the randomness is also incorporated in selecting

the location to embed the watermark. Results show that the method is resistant to most of the commonly occurring attacks.

7. FUTURE SCOPE

The proposed technique can be made more robust by introducing the concept of Fuzzy Logic, Adaptive Fuzzy Logic or Neural Networks. In this method, fuzzy Logic can be used instead of pseudo-random approach, in the selection of the subblocks, where the watermark pixels are to be embedded. It can be made more secure by combining it with DCT technique.

REFERENCES

[1] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, (1997) "Handbook of applied cryptography", *CRC Press LLC*, ISBN 0-8493-8523-7, pp.169-190.

[2] Dr.M.A.Dorairangaswamy," A Novel Invisible and Blind Watermarking Scheme For Copyright Protection of Digital Images", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.4, April 2009

[3] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy, (2005) "A Dual Digital-Image Watermarking Technique", *World Academy of Science, Engineering and Technology 5*, pp. 136-139.

[4] Mathias Schlauweg, Dima Pröfrock, Benedikt Zeibich and Erika Müller, (2006) "Dual Watermarking for Protection of Rightful Ownership and Secure Image Authentication", *MCPS'06*, Santa Barbara, California, USA, pp. 59-66, October.

[5] P. Meerwald and A. UhI, (2001) "A Survey of wavelet-Domain watermarking Algorithms", *Proceedings of SPlE Security and Watermarking of multimedia Content 111*, San Jose.CA,Vol.4314, pp. 505-516.

[6]. Rafael C. Gonzalez, Richard E. Woods, ―Digital Image Processing, 2nd Edition

[7] R.Dhanalakshmi, K.Thaiyalnayaki, (2010) "Dual Watermarking Scheme with Encryption", *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 7, No. 1, pp. 248-253.

[8] Saraju P.Mohanty, K.R. Ramakrishnan and Mohan Kankanhalli,(1999) "A Dual Watermarking Technique for Images", *Proceedings of the 7th ACM International Multimedia Conference*, pp. 49-51.

[9] Shikha Tripathi1, Nishanth Ramesh2, Bernito A3, Neeraj K J, "A DWT based Dual Image Watermarking Technique for Authenticity and Watermark Protection", Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010

[10]. Zhang Guannan, Wang Shuxun and Nian Guijun, (2004) "A Blind Watermarking Algorithm Based on DWT Color Image", *Intl. Symposium on Multi-Dimensional Mobile Communications*, Vol. 2,pp. 634- 638.

Authors' biography

Er. Amandeep Kaur is a student of M. Tech in information technology from A.I.E.T, Faridkot. She has done her degree of B. Tech from L.L.R.IE.T, Moga in the year 2008.

Er. Blossom Kaur is a student of M.Tech in Computer Science from B.M.S.C.E.T, Muktsar. She has completed her degree of B.Tech in CSE from A.I.E.T, Faridkot in the year 2007.

Er. Navneet Singh Randhawa is working as an Associate Professor in A.I.E.T, Faridkot

Er. Sukhdeep Singh is a student of M. Tech in Electronics &Communication from A.I.E.T, Faridkot. He has done his degree of B.Tech in Electronics &Communication from G.G.S.C.E.T.,Talwandi Saabo (Bathinda) in the year 2009.

Er. Parneet Kaur is working as a lecturer in A.I.E.T., Faridkot. She has completed her degree of B.Tech in CSE from A.I.E.T, Faridkot in the year 2007.