IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 20-25
www.iosrjournals.org

DWT based Image Watermarking for Information Security

Subhashree Khatua[1], Debaraj Rana[2]
[1]*M.Tech Scholar, Dept. of ECE, Centurion University of Technology &Management, Odisha, INDIA*
[2]*Asst. Professor, Dept. of ECE, Centurion University of Technology &Management, Odisha, INDIA*

Abstract: *The growth of the Internet along with the increasing availability of multimedia applications has spawned a number of copyright issues. One of the areas that this growth has fueled is that of digital watermarking. Digital watermarking is the general technique of embedding a blob of information in the original file, such that an altered file is obtained. The blob of information, thus included, serves one of different uses, such as, identifying piracy, sensing tampering, or reassuring integrity. We proposed a method which includes the benefit of wavelet transform during watermarking. In this paper, we have worked on some of the watermarking algorithms for digital images, simulated the algorithm in MATLAB environment and analyzed its performance for various images.*

Keywords- *Watermark, Arnold Transform, DWT, Security*

I. Introduction

In the present day of scenario where the digital system has been evolved more which help more in the field of multimedia. Multimedia includes the transmission of image, video and audio. It is very important to keep the privacy as well as the authentication during transmission of such information. The security of multimedia information becomes more challenging [1-2]. Researchers have developed many techniques to protect the data. Watermarking in one of the technique, which is used for authentication . Watermarking techniques can broadly be classified based on their inherent characteristics: visible and invisible [3].

1.1 Visible watermarks

Visible alteration of the digital image by appending a "stamp" on the image is called a visible watermark. This technique directly maps to that of the pre-digital era where a watermark was imprinted on the document of choice to impose authenticity.

1.2 Invisible watermarks

By contrast, an invisible watermark, as the name suggests that this is invisible for the most part and is used with a different motive.

While the obviousness of visible watermarking makes distinguishing legitimate and illegitimate versions easy, its conspicuousness makes it less suitable for all applications. Invisible watermarking revolves around such suitable factors that include recognizing authentic recipients, identifying the true source and non-repudiation.

So watermarking is the process where a watermark or the confidential information embedded into a host data, which carry the water mark information. At the receiver part it needs to extract the watermark to be an authorized one. For watermarking, it can be either done with frequency domain or spatial domain. In frequency domain technique it can be done through discrete cosine transform (DCT) or discrete wavelet Transform (DWT), where as in case spatial domain watermarking we need to perform the operation into the pixels itself, which make the system simple and less complexity[4-8]

II. Discrete Wavelet Transform

Wavelets have many advantages over other mathematical transforms such as the DFT or DCT. Functions with discontinuities and functions with sharp spikes usually take substantially fewer wavelet basis functions than sine-cosine functions to achieve a comparable approximation. Wavelets ability to provide spatial and frequency representations of the image simultaneously motivates its use for feature extraction The Haar wavelet transform is a widely used technique that has an established name as a simple and powerful technique for the multi-resolution decomposition of time series. An original image of size N x N is first of all pass through a filter horizontally and vertically as shown in figure 1.

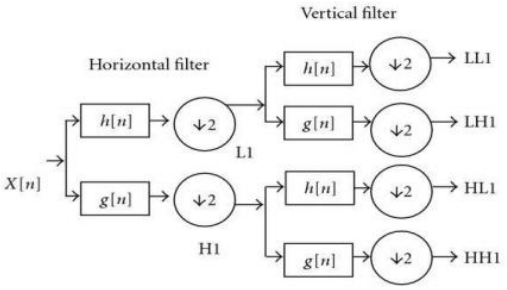

Fig. 1 wavelet Transform

The low pass filtering in horizontal direction and high pass filtering in vertical direction gives rise to LH component, likewise filtering gives rise to four components LL, LH, HL and HH during first level of decomposition [9, 10]. The LL component which represents the approximate coefficients of the decomposition is used to produce next level of decomposition. The sub band HL represents major facial expression features. The sub band LH, the vertical features of outline and nose are clearer than its horizontal features, depicts face pose features. [11]

Fig.2 single Level Decomposition using down sampling

The sub band HH is the unstable band in all sub bands because it is easily disturbed by noises, expressions and poses. And the sub band LL will be the most stable sub band. Here an image and its detail and approximate coefficients are shown in figure 2.

III. Proposed Algorithm

Generally, the procedure of watermarking includes watermark generation, watermark embedding and watermark extracting. Here, we choose 64 × 64 binary image as watermark W, and 24-bits true color standard image with size of 1024 × 1024 as host image H. The detailed algorithm is described below

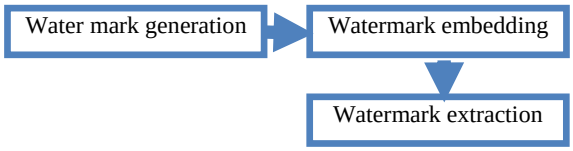

Fig. 3 The Watermarking Process

The watermarking process comprises of the following stages:

- Embedding stage
- Extraction phase
- Decision stage

Embedding stage: In this stage, the image to be watermarked is preprocessed to prime it for embedding. This involves converting the image to the desired transform. This includes the discrete cosine transform (DCT), the discrete Fourier transform (DFT) and the wavelet domains. The watermark to be embedded may be a binary image, a bit stream or a pseudo-random number that adheres to, say, a Gaussian distribution. The watermark is then appended to the desired coefficients (low frequency or intermediate frequency) of the transform, as recommended by Human Visual System (HVS) research. The watermarked image is the output of this process and is obtained by performing an inverse transform on the altered transform coefficients [12].

For enhancing the security of the proposed method, the original watermark is permuted by Arnold transform based on the secret key K1 in the stage of watermark generation [13-14]. After Arnold transform, the original watermark image is rearranged to W.

(a) (b)

Fig. 4. The Arnold transform of the original watermark (a) original watermark (b) transformed watermark

3.1. Embedding

The detailed procedure of watermark embedding is described as follows.

1) Initially convert the RGB host image H to YCbCr color space and obtain the Luminance Y component.

2) Then divide the luminance component into 16x16 non overlapping block.

3) Compute the single level DWT of each block and find the average approximate coefficient Di,j(0,0) of each block, where i and j represent the row and column indexes of each block, respectively.

4) According to the watermark information w(i, j) to decide the modifying magnitudes T1 and T2.

$$\text{if} \quad w(i,j)=1, \begin{cases} T_1 = 0.5\Delta \\ T_2 = -1.5\Delta \end{cases}$$

$$\text{if} \quad w(i,j)=0, \quad \begin{cases} T_1 = -0.5\Delta \\ T_2 = 1.5\Delta \end{cases} \qquad (1)$$

5) The possible quantization results D1and D2can be computed by the modifying magnitudes T1and T2.

$$D1 = 2k\Delta + T1$$

$$D2 = 2k\Delta + T2 \qquad (2)$$

6) Calculate the value D'i,j(0, 0)for embedding watermark in Di,j(0, 0).

$$D^{\wedge\prime}\, ij(0,0) = D2 \; if \; abs(Dij(0,0) - D2) < abs(Dij(0,0) - D1$$

$$D1 \; else \qquad (3)$$

7) Calculating the modified value MDi,jof the DWT coefficient by

$$MDi,j = D'\_i,j(0,0) - Di,j(0,0) \qquad (4)$$

8)Add Di,j/16 to all pixels in the block, that is ,embed one watermark bit into this block in the spatial domain. Repeating (3)–(8) until all blocks are performed to obtain the watermarked Y luminance. Water marked image from the YCbCr color space to RGB color space by Eq. (22), and obtaining the watermarked image H'

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1.000 & 0.000 & 1.402 \\ 1.000 & -0.344 & -0.714 \\ 1.000 & 1.732 & 0.000 \end{bmatrix} \times \begin{bmatrix} Y \\ C_b - 128 \\ C_r - 128 \end{bmatrix}$$

3.2. Extraction Stage

In this stage, an attempt is made to regain the watermark or signature from the distributed watermarked image. This stage may need a private key or a shared public key, in combination with the original image, or just the watermarked image [12].

The procedure of watermark extraction is to extract the embedded watermark from the watermarked image, in which may require the original image or the original watermark.

In the proposed algorithm, we can extract the watermark without the requirement for the original image or the watermark image. That is, the proposed algorithm is a blind watermarking.1) Converting the watermarked image H' from the YCrCb color sys-tem into the RGB color system.2) Obtaining the luminance Y of the YCrCb, and dividing it into non-overlapped 16 × 16 blocks.3) By Eq. (3), Obtain the DWT average approximate coefficient Di,j(0, 0).4) Using the quantification step Δ based on the secret key K2 to compute the watermark w'(i, j)

$$w'(i,j) = \mathrm{mod}\left(ceil\left(\frac{Dij(0,0)}{\Delta} \right), 2 \right) \qquad (5)$$

Utilizing the secret key k1 to perform the Arnold inverse trans-form on w'(i, j) and obtaining the extracted watermark imageW'.

3.3. Decision Stage

In this stage, the extracted watermark is compared with the original watermark to test for any discrepancies that might have set in during distribution. A common way of doing this is by computing the Hamming distance [15] .

$$HD = \frac{(Wmod \cdot W)}{\|Wmod\|.\|W\|}$$

where both the numerator and denominator are dot products.
HD obtained above is compared to a threshold, T, to determine how close Wmod is to W.

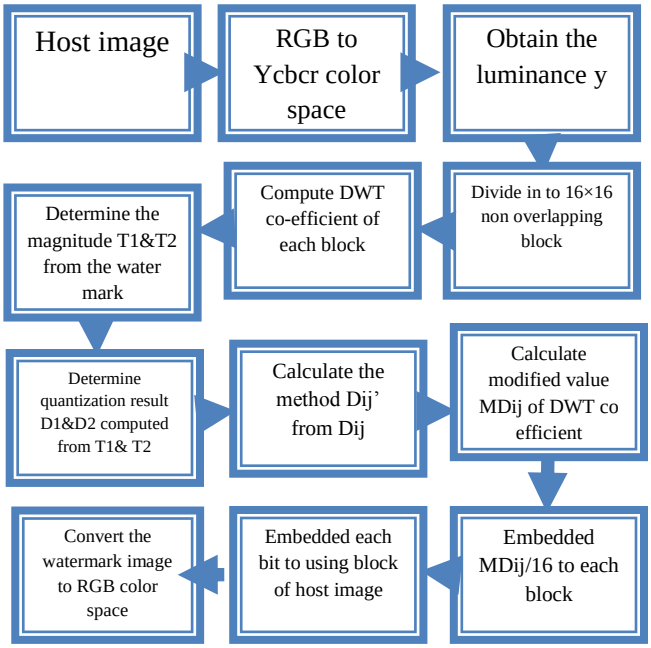

Fig 5 Overall Block Diagram

IV. Results Analysis

The proposed method is based on DWT coefficient to hide information which termed as water marking. In this technique we have folded our work into three category, one is generating the watermark followed by embedding the water mark inside a host image, and lastly extracting the water mark at the receiverend.Theoverallprocessisimplementedandsimlate in MATLAB 7.8 (R2009a) with system configuration of Intel I3 at 2.93 GHz clock frequency. In the proposed method we have considered watermark image of size 64x64 which are of binary image, if not then we need to convert it into binary form. The host images through which the watermark will be hidden are taken of dimension 1024x1024.

Initially we need to consider a host image which are generally in RGB form, it need to convert to YCbCr domain before used to hide the information. The RGB host image given below in figure 7.1.

Fig 6 Original Host Image

Out of the YCbCr domain our requirement is the luminance component which has to be divided into 8x8 non overlap block. The YCbCr domain image and its luminance component has shown below.

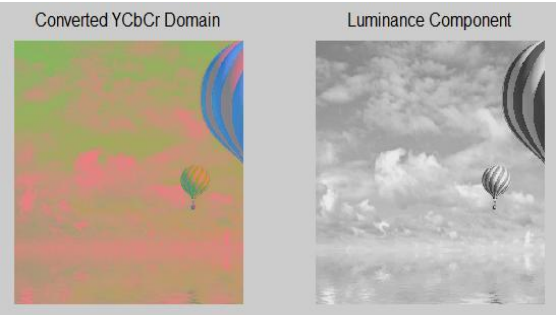

Fig 7 YCBCr and Luminance Component

The luminance component is then divided into 8x8 non overlapping block which has shown below.

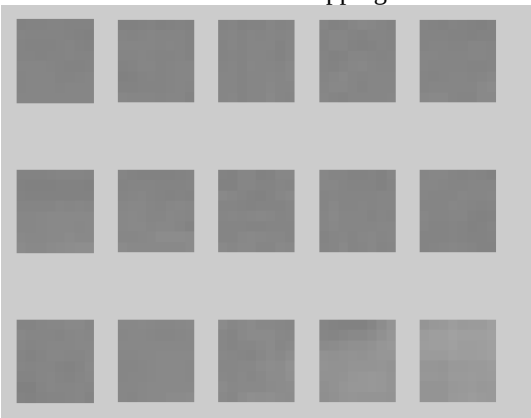

Fig 8 Non Overlap 16x16 block for host image

After extracting the 16x16 non overlapping block, each block has to be performed the single level DWT operation and find the approximate coefficient. Then find the average approximate coefficient of each block. .

The information to be hidden has to term as the watermark image. In general the water mark image is of binary image with dimension 64x64. The water mark image first passed through a transform technique called Arnold transform. The Arnold Transform will randomize the bit pattern in to a uniform pattern. The Original water mark image and the Arnold transform image has shown below.

Fig 9 The Watermark image and its Arnold Transform

During division of host image to 16x16 non overlapping, the DWT coefficient are calculated and modified using a key called K1. The modified coefficient samples are shown below.

After Arnold transform, the watermark bit is then embedded into the non overlapping block, after embedded the YCbCr color space to RGB Color space. For extraction of embedded watermark, it has to convert RGB to YCbCr domain and extract the Y component and again divide it into 8x8 non overlap blocks, then obtain the DC coefficient each block and extract the hidden watermark bit. The water mark bit bare extracted and perform the inverse Arnold transform to recover the water mark image. The recovered water mark image has been shown below.

Fig 10 Inverse Arnold Transform

V. Conclusion

Watermarking is a vast field and a lot of research is going on in this area. There are commercial players who are vying for dominance in this field. Though a clear-cut winner has not been declared yet, a combination of other cryptographic techniques (such as encryption) and watermarking together will definitely provide copyright protection for images. Depending on the intended requirements and the level of security required, an appropriate watermarking algorithm can be chosen. The proposed method efficiently hiding the information in terms of water mark image. The water mark image embedded into a host image through the process of DWT coefficient. And to generate the water mark image we are following a transform called Arnold Transform, at the other end we are extracting the watermark image by the process of inverse Arnold transform. The proposed method shows the efficient watermarking through wavelet domain.

References

[1] Su, Q., Niu, Y., Wang, Q., & Sheng, G. (2013). A blind color image watermarking based on DC component in the spatial domain. Optik-International Journal for Light and Electron Optics, 124(23), 6255-6260.

[2] H. Luo, F. Yu, Z.L. Huang, Z.M. Lu, Blind image watermarking based ondiscrete fractional random transform and subsampling, Optik 122 (2011)311–316.

[3] D.C. Lou, H.K. Tso, J.L. Liu, A copyright protection scheme for digital imagesusing visual cryptography technique, Comput. Stand. Interfaces 29 (2007)125–131.

[4] E. Vahedi, R.A. Zoroofi, M. Shiva, Toward a new wavelet-based watermarkingapproach for color images using bio-inspired optimization principles, Digit.Signal Process. 22 (2012) 153–162.

[5] X.D. He, C.Q. Zhu, Q.S. Wang, The blind watermarking model of the vectorgeospatial data based on DFT of QIM, Proceedings of the 2009 IEEE Interna-tional Conference on Network Infrastructure and Digital Content, 2009, pp.1039–1044.

[6] X.J. Qi, J. Qi, A robust content-based digital image watermarking scheme, SignalProcess. 87 (6) (2007) 1264–1280.

[7] I. Usman, A. Khan, BCH coding and intelligent watermark embedding: employ-ing both frequency and strength selection, Appl. Soft Comput. 10 (1) (2010)332–343.

[8] S.D. Lin, S.C. Shie, J.Y. Guo, Improving the robustness of DCT-based image water-marking against JPEG compression, Comput. Stand. Interfaces 32 (2010) 54–60.

[9] B. Sami, K. Lala, A. Thawar, Z. Shaaban, Watermarking of digital images infrequency domain, Int. J. Automat. Comput. 7 (1) (2010) 17–22.

[10] L.S. Liu, R.H. Li, Q. Gao, A new watermarking method based on DWT green component of color image, Proceedings of 2004 International Conference onMachine Learning and Cybernetics, 2004, pp. 3949–3954.

[11] Q. Su, X. Liu, W. Yang, A watermarking algorithm for color image based on YIQcolor space and integer wavelet transform, Proceedings of 2009 International Conference on Image Analysis and Signal Processing, 2009, pp. 70–73.

[12] K.C. Liu, Wavelet-based watermarking for color images through visual masking,AEU Int. J. Electron. Commun. 64 (2) (2010) 112–124

[13] C.K. Chan, L.M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recogn. 37 (3) (2004) 469–474.

[14] I. Nasir, Y. Weng, J.M. Jiang, S. Ipson, Multiple spatial watermarking technique in color images, Signal Image Video Process. 4 (2) (2010) 145–154.

[15] F.Y. Shih, S.Y.T. Wu, Combinational image watermarking in the spatial andfrequency domains, Pattern Recogn. 36 (4) (2003) 969–975.