

IMPERCEPTIBLE IMAGE WATERMARKING TECHNIQUE USING 3-LEVEL DISCRETE WAVELET TRANSFORM (DWT)

¹RITA CHOUDHARY, ²GIRISH PARMAR

^{1,2}Deptt. Of Electronics, Rajasthan Technical University, Kota (Rajasthan.), India

Abstract— The rapidly use of digital data in the present era over the internet requires the effective watermarking techniques. Watermarking is a technique which provides security to digital data i.e. image, audio, and video. In general, the host image is embedded with watermark image where watermark image is in binary or gray scale. In this paper, 3-level Discrete Wavelet Transform (DWT) based digital image watermarking is proposed. In this technique, a multi-bit watermark is inserted into the low-frequency component of a cover image by using variable visibility factor. In this paper, 3-level DWT-based image watermarking is compared with the 2-level DWT- based image watermarking methods after applying attacks on both the levels. The simulated results indicate that the watermarks generated with the proposed method are invisible and robust. Normalized cross-correlation and peak signal to noise ratio are the different fidelity parameters used for evaluating performance, Parameters are compared for various noises like Gaussian noise, Salt and Pepper noise etc.

Index Terms— Image watermarking, 3-level DWT, wavelet Transform, PSNR, NCC.

1. INTRODUCTION

In this digital world, the multimedia data is distributed over internet and users enjoy the advantages that the network provided. Presently the challenge is to protect the owner's data that allows to full usage of the internet resources. Cryptography and steganography are the data hiding techniques but these are not so effective because there is the possibility of data is lost [1].

Data hiding is a very important topic of research in the field of communication over the internet. Today every person depends on the computer for communication, banking and for many other various areas. So security is a very important to protect the multimedia data and it is very big question for researchers to secure the owner's data. Digital watermarking is the best solution to preserve the owner's data and more secure with fast access to resources over the internet [2-3]. Digital watermarking is the process of hiding digital data into digital multimedia content without degradation, such that this watermark can resist any external operation or noise attacks. Digital Image Watermarking is basically a phenomenon by which we can easily encrypt and decrypt a data in digital format so that it can be used by authorized users and unauthorized users will not be able to decrypt the data. The watermark can be visible or invisible; invisible watermarks are the most commonly employed [4]. Copyright protection, data payload, stability, security and imperceptibility are the basic characteristics of any watermarking schemes can be used by authorized users and unauthorized users will not be able to decrypt the data. The strength of the watermark against duplication is that it is stable to linear and nonlinear filtering, lossy compression, cropping and scaling. Invisibility is the measure of perceptual resemblance between the host and watermarked signals. The watermark can be made imperceptible under untailed observation by embedding the

watermark in a discreet, self-effacing manner. The capability of the watermark to oppose antagonistic attacks is known as Security. Attacks are not restricted to elimination of the watermark content, but they also comprise watermark falsification or estimation, collusion, and uncertainty attacks.

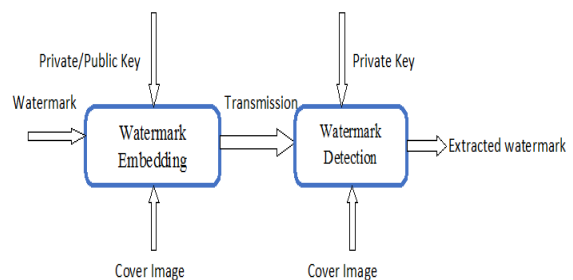


Fig.1 General Processes involved in a watermarking system

Existing digital image watermarking techniques in which the watermark is embedded can be classified into two main groups: spatial domain techniques and transform domain techniques, these are two domains in which image watermarking can be done more efficiently [6]. In the spatial domain, the pixel values embedded on the watermark directly, whereas in the transform domain, after modulating the magnitude of the transformed coefficients and these coefficients embedded with data. Transform domain approaches are preferred because they allow more information to be embedded and provide greater robustness against attacks [5]. There are mainly 4 types of transforms used in the frequency domain:

- Discrete Wavelet Transform (DWT),
- Discrete Cosine Transform (DCT),
- Discrete Fourier Transform (DFT) and
- Discrete Hartley Transform (DHT)

Each of these transforms has its own characteristics and represents the image in different ways.

Watermarks can be embedded within images by modifying these values, i.e. the transform domain coefficients. Further performance of image watermarking using DWT can be improved by increasing the levels of DWT.

II. DISCRETE WAVELET TRANSFORMS (DWT)

Wavelet Transform is a modern decomposing technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves called wavelet, of varying frequency and limited duration. A wavelet series is a representation of a square-integrable function by a certain orthonormal series generated by a wavelet. The basic idea of discrete wavelet transform(DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district Furthermore, the properties of wavelet could decompose the original signal into wavelet transform coefficients which contain the position information. The original signal can be completely reconstructed by performing Inverse Wavelet Transformation on these coefficients. Watermarking in the wavelet transform domain is generally a problem of embedding watermark in the different subbands of the cover image.

There are four subbands created at the end of each level of image wavelet transformation: they are Low-Low pass sub-band (LL), High-Low (horizontal) sub-band (HL), Low-High (vertical) sub-band (LH) and High-High (diagonal) pass sub-band (HH). Subsequent level of wavelet transformation is applied to the LL sub-band of the previous one. The sub-band LL1 for the coarse-scale DWT coefficient while the other sub-bands are the fine scale of DWT coefficient. Further, 3-level DWT is applied on LL1 sub-bands. Due to this multi-resolution, the DWT technique is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In general, most of the image energy is concentrated at the lower frequency sub-bands LLx and therefore embedding watermarks in these sub-bands may degrade the image significantly but increases the robustness.

The DWT decomposition for image analysis is done through first row wise decomposition and then column wise. In 3-level DWT, the first level of decomposition of image, divide the image into four parts. Each of them has a quarter size of the original image. They are called approximation coefficients (LL), horizontal (LH), vertical (HL) and detail coefficient (HH). Approximation coefficients obtained in the first level can be used for the next decomposition level.

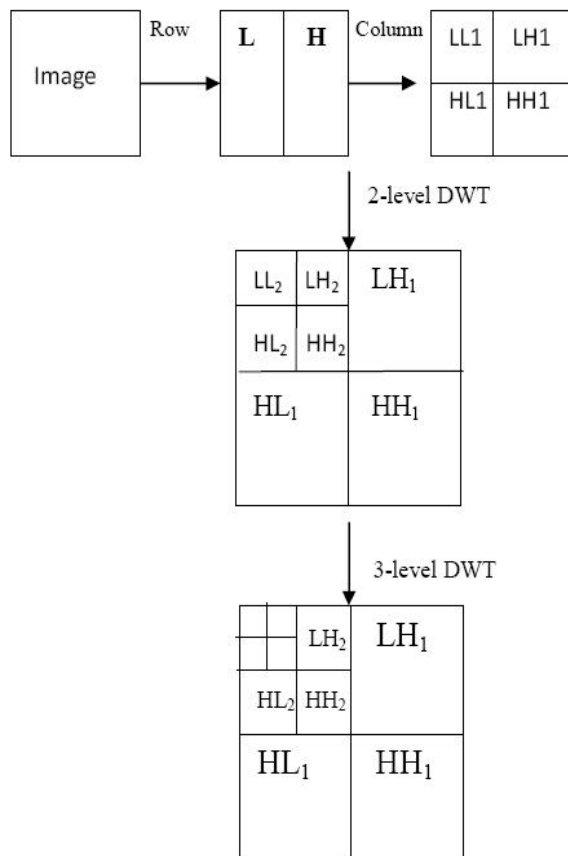


Fig.2 Show DWT decomposition of image at level-3

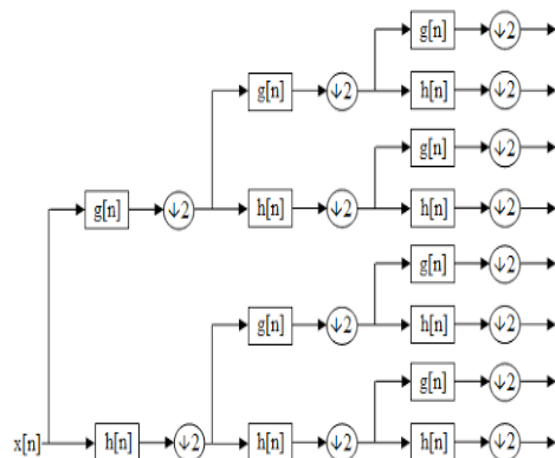


Fig. 3 Represents the 3-level DWT decomposition of data

There are many types of filters that we are used in transformation. The most commonly used filters for watermarking technique are:-Haar Wavelet Filter, Daubechies Orthogonal Filters, Daubechies Bi-Orthogonal Filters, Symlet wavelets. These filters decompose image into low and high frequency components. Single level decomposition gives four frequency representations of the images.

III. PROPOSED TECHNIQUE

Here, we propose a stable image watermarking technique using 3-level Discrete Wavelet Transform (DWT) and applied attacks on it. The proposed

algorithm is divided into two parts, watermark embedding and watermark extraction.

A. Watermark Embedding

The watermark embedding process is described as below and shown in Fig. 3.

Step 1:- Initialize the cover image and watermark image as I_c and I_w .

Step 2:- Decomposed both the images into $LLc1$, $LHc1$, $HLc1$, $HHc1$ and $LLw1$, $LHw1$, $HLw1$, $HHw1$ sub-bands using DWT for cover and watermark images, respectively.

Step 3:- Again decomposed LL band of both the images into $LLc2$, $LHc2$, $HLc2$ and $HHc2$ and $LLw2$, $LHw2$, $HLw2$ and $HHw2$ respectively.

Step 4:- Again decomposed LL band of both the images into $LLc3$, $LHc3$, $HLc3$ and $HHc3$ and $LLw3$, $LHw3$, $HLw3$ and $HHw3$ respectively.

Step5:- Compute new matrix $WMLL3$ using fusion of $LLc3$ and $LLw3$ matrixes. It is defined by

$$WMLL3 = LLc3 + k * LLw3; \quad (1)$$

k = visibility factors for the host image and watermark image.

Step 6:- Therefore, watermarked image obtained using inverse DWT based on $WMLL3$ band and remaining $LHc3$, $HLc3$, $HHc3$ band. It is defined as:

$$I_{wd} = \text{inverse dwt} [WMLL3, LHc3, HLc3, HHc3]$$

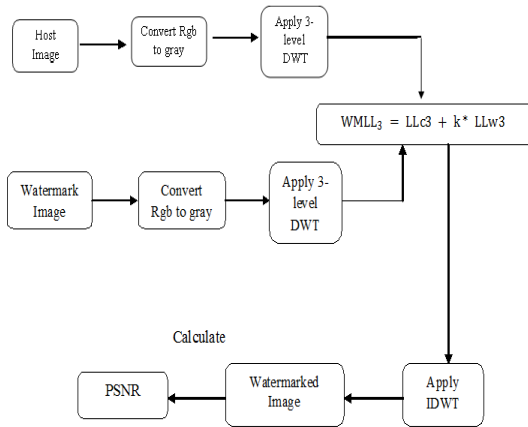


Fig.4:- Block Diagram of watermark embedding algorithm

B. Watermark Extraction

The watermark embedding process is described as below and shown in Fig. 3.

Step 1:- Initialize the watermarked image and cover image.

Step 2:- Decomposed both the images into $LLc1$, $LHc1$, $HLc1$, $HHc1$ and $LLwm1$, $LHwm1$, $HLwm1$, $HHwm1$ sub-bands using DWT for cover and watermarked images, respectively.

Step 3:- Again decomposed LL band of both the images into $LLc2$, $LHc2$, $HLc2$ and $HHc2$ and $LLwm2$, $LHwm2$, $HLwm2$ and $HHwm2$ respectively.

Step 4:- Again decomposed LL band of both the images into $LLc3$, $LHc3$, $HLc3$ and $HHc3$ and $LLwm3$, $LHwm3$, $HLwm3$ and $HHwm3$ respectively.

Step5:- Compute new matrix RW using fusion of $LLc3$ and $LLwm3$ matrixes. It is defined by

$$RW = (WMLL3 - LLc3) / k; \quad (2)$$

k = visibility factors for the host image and watermark image.

Step 6:- Therefore, extracted watermark image obtained using inverse DWT based on RW band and remaining LHw , HLw , HHw band. Its define as,

$$I_{ew} = \text{inverseswt} [RW, LHc3, HLc3, HHc3]$$

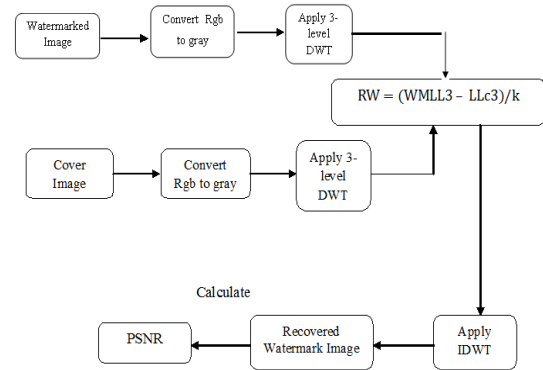


Fig.5:- Block diagram of watermark extraction algorithm

IV. EXPERIMENTAL RESULTS

Here, an experimental performance analysis of proposed technique has been presented. These experiments illustrate the efficiency of proposed watermarking technique

4.1 Materials and Methods

Here, host (cameraman) and watermark image (text) with the 512X512 pixels has been taken in this experiment. Analysis and compare 3-level DWT and 2-level DWT with considering fidelity parameters.

4.2. Evaluation Fidelity Parameters

Generally, visual performance of watermarked images is analysis by using two important fidelity parameters i.e., peak signal-to-noise ratio (PSNR) and Normalized Correlation which are historically adopted in image processing in order to evaluate the performance of the output results as shown in tables. The parameter Peak signal to noise ratio is defined by:-

$$MSE = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M (f(i, j) - g(i, j))^2$$

$$PSNR = 10 \log_{10} \frac{L^2}{MSE} \quad (3)$$

Here, L defines the range of pixels of images. As MSE is inversely proportional to PSNR, thus the small mean square error tends to high signal to noise ratio. The quality measurement for the image is directly measured from the pixel values. For better image quality the PSNR must be high. The quality of

the image is measured using normalized cross correlation (NCC) and is obtained by using eq. (2)

$$NCC = \frac{\sum_{i=1}^N \sum_{j=1}^M g(i, j) * g'(i, j)}{\sqrt{\sum_{i=1}^N \sum_{j=1}^M (g(i, j))^2} \sqrt{\sum_{i=1}^N \sum_{j=1}^M (g'(i, j))^2}} \quad (4)$$

Here, PSNR considered for good efficiency is close to 35 dB to avoid having a visible watermark but at the same time including the watermark with a large energy to be resistant to attacks.

4.3. Simulated Experimental Results



Figure 6(a): Cameraman, size (512x512).

Sample of watermark image



Text image

Figure 6(b): watermark image

Fig. 6(a) shows the original image and Fig. 6(b) shows the watermark image for embedding of watermark in the original image

Table I show the PSNR value for different levels using proposed method (cameraman (as cover image) & text (as watermark image))

| Visibility Factor | PSNR | |
|-------------------|--------------|--------------|
| | 3-level DWT | 2-level DWT |
| K | | |
| 0.04 | 31.45 | 31.39 |
| 0.03 | 33.58 | 33.42 |
| 0.025 | 35.81 | 35.77 |
| 0.02 | 37.46 | 37.37 |
| 0.01 | 42.41 | 42.12 |

Table II show the NCC value of recovered watermark image by 3-level DWT using proposed method (cameraman (as cover image) and text (as watermark image))

| Visibility Factor | Normalized Cross Correlation NCC | |
|-------------------|----------------------------------|---------------|
| | 3-level DWT | 2-level DWT |
| K | | |
| 0.04 | 0.9985 | 0.9965 |
| 0.03 | 0.9978 | 0.9957 |
| 0.025 | 0.9923 | 0.9895 |
| 0.02 | 0.9947 | 0.9870 |
| 0.01 | 0.9813 | 0.9620 |

In table II, we evaluated that the performance of 3-level DWT is better than 2-level DWT. Now, analysis the performance of 3-level DWT of watermarked image by applying attacks (salt & pepper noise, rotation, Gaussian noise) on it and calculated the Normalized cross correlation of recovered watermark image.

Table III show the NCC value of recovered watermark image after applying attacks on watermarked image

| Visibility Factor | Normalized Cross correlation (NCC) | | |
|-------------------|------------------------------------|----------|----------------|
| | Salt & pepper noise | Rotation | Gaussian noise |
| K | | | |
| 0.04 | 0.9985 | 0.9985 | 0.9985 |
| 0.03 | 0.9978 | 0.9978 | 0.9978 |
| 0.025 | 0.9952 | 0.9952 | 0.9952 |
| 0.02 | 0.9947 | 0.9947 | 0.9947 |
| 0.01 | 0.9813 | 0.9813 | 0.9813 |

As seen in simulated results, we compared proposed 3-level DWT to the 2-level DWT technique. For above technique, we have used images cameraman as the original image and the text image as the watermark. Both the images are of equal size of 512X512. The value of visibility factor k is varied from 0.04 to 0.005 and we see that the value of PSNR increases but at the same time the value of CC decreases as we decrease the value of visibility factor. We see that the value of NCC is not changed after applied the attacks on 3-level watermarked image and best result seen at k=0.025.



Watermarked image & recovered watermark image at 0.025 3-Level DWT

Fig.7 shows the watermarked image and recovered watermark image at 0.025

CONCLUSION

In this paper, 3-level DWT based an image watermarking techniques has been introduced and also implemented. Experiment results show that the quality of the watermarked image and the recovered watermark are dependent only on the visibility factors and also indicate that the 3-level DWT provide better performance than 2-level and attacks does not affect 3-level based image watermarking techniques.

REFERENCE

- [1] P. H. W. Wong, O. C. Au and G. Y. M. Yeung, "A Novel Blind Multiple Watermarking Technique for Images," accepted by IEEE Transactions on Circuits and Systems for

- Video Technology: Special Issue on Authentication, Copyright Protection and Information Hiding, Sept. 2003.
- [2] P V Nagarjuna and K. Ranjeet, 'Robust Blind Digital Image Watermarking Scheme Based on Stationary Wavelet Transform', IEEE IC3, 8-10 Aug. 2013.
- [3] Samira Lagzian, Mohsen Soryani, Mahmood Fathy, 'A New Robust Watermarking Scheme Based on RDWT-SVD' International Journal of Intelligent Information Processing, Vol. 2, Number 1, 2011, Doi:10.4156/ijiiip.vol2.issue1.3
- [4] Ezz El-Din Hemdan et al. "Hybrid Digital Image Watermarking Technique for Data Hiding" IEEE 30th national radio science conference 2013, pp220-227, April 2013
- [5] Cheng Mingzhi, Li Yan*, Zhou Yajian and Lei Min, "A Combined DWT and DCT Watermarking Scheme Optimized Using Genetic Algorithm" Journal of Multimedia, volume 8, paper 3, June 2013
- [6] Shahin Shaikh1, Manjusha Deshmukh "Digital Image Watermarking In DCT Domain" ISSN 2250-2459, ISO 9001:2008 Certified Journal, International Journal of Emerging Technology and Advanced Engineering Volume 3, Issue 4, April 2013
- [7] Mr. Gaurav N Mehta, Mr. Yash Kshirsagar, Mr. Amish Tankariya, " Digital Image Watermarking: A Review", International Journal of Scientific Engineering and Technology (ISSN : 2277-1581) www.ijset.com, Volume No.1, Issue No.2 pg:169-174 01 April 2012
- [8] Ansu Anna Ponnachen, Lidiya Xavier, "Dwt Based Watermarking For Lifting Based Compression And Symmetric Encryption Of Jpeg Images", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 www.ijert.org Vol. 2 Issue 6, June - 2013
- [9] Ghazali Bin Sulong, Harith Hasan(Corresponding author) , Ali Selamat, Mohammed Ibrahim and Saparudin, "A New Color Image Watermarking Technique Using Hybrid Domain", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 1, November 2012
- [10] L. Hu, F. Wan, 'Analysis on wavelet coefficient for image watermarking', Int. Conf. MINES'10, pp. 630-634, 2010
- [11] Singh A. P., Mishra A., Wavelet Based Watermarking on Digital Image, Indian Journal of computer Science and Engineering 2011.
- [12] Akhil Pratap Singh," Wavelet Based Watermarking On Digital Image " ,Indian Journal of Computer Science and Engineering Vol 1 No 2, 86-91:
- [13] X. G. Xia, C. G. Boncelet and G. R. Arce, "A Multiresolution Watermark for Digital Images," in Proc. of IEEE Int. Conf. Image Processing, vol. 1, pp. 548-511, Oct. 1997.
- [14] E. T. Lin and E. J. Delp, "A Review of Data Hiding in Digital Images," in Proc. of the Image Processing, Image Quality, Image Capture Systems Conf. (PICS' 99), pp. 274-278, Apr. 1999.
