International Journal of
Science and Engineering Investigations vol. 1, issue 2, March 2012

An Improved Watermarking Algorithm for Hiding Biometric Data

Saeid Fazli [1], Maryam Zolfaghari-Nejad [2]
[1,2] Electrical Dept., Eng. Faculty, Zanjan University, Zanjan, Iran
([1]fazli@znu.ac.ir, [2]maryam_zolfaghari@znu.ac.ir)

Abstract- This paper presents a novel watermarking algorithm for authentication based on fusion strategy of faces and fingerprint biometrics. The Discrete Wavelet Transform is used for embedding the minutiae data in face image of the same individual. The performance of the watermarking algorithm is experimentally validated and the results show that the extracting the minutiae data with no error is possible. Experimentation has been done using six different attacks. The results of the method reveal better resistance in comparison to the existence methods.

Keywords- Watermarking, Biometrics, discrete wavelet transform, minutiae data.

I. Introduction

Biometric authentication systems have inherent advantage over traditional personal identification techniques. Utilizing biometrics for personal authentication is becoming more accurate than current methods (such as the utilization of passwords or Personal Identification Number-PINs) and more convenient (nothing to carry or remember). Thus, Biometrics is not just about security, it’s also about convenience [7].

However, the security of biometric data is of paramount importance and must be protected from external attacks and tempering. It is therefore required to protect the biometric templates of individuals at all times [1]. In biometric watermarking, a certain amount of information referred to as watermark, is embedded into the original cover image using a secret key, such that the contents of the cover image are not altered [2].

The problem is which watermarking algorithm is suitable for this work. Reference [8]’’ focused on information hiding in the spatial domain. Recently, efforts are mostly based on frequency-domain techniques [9]. Generally, DCT (Discrete Cosine Transform), DFT (Discrete Fourier Transform) and DWT (Discrete Wavelet Transform) are transformed in the frequency-domain. In these methods, the watermark is distributed over entire domain of original data.

Given the suitability of Discrete Wavelet Transform to model the Human Visual System [10-11] behaviour and its multi-resolution properties, the DWT has gained interest among watermarking researchers, as it is witnessed by the number algorithms following this approach that have been proposed over the last few years [12-15].

In this study, ICAO standards (International Civil Aviation Organization) for fingerprint and face images in done experiments is considered. In this standard, the extracted minutiae of fingerprint image (and not fingerprint image) are stored in travel documents. Because the aim of this paper is to follow the instructions of this standard about biometrics, we must extract minutiae of the fingerprint image and watermark it in the face image of the same individual.

According to ICAO, standard face image should be colourful or grey and with 240 x 320 size, So the used face image is captured by Sony Cyber Shot DSC-Tc and is in ICAO standard size. The inserted data is 25 extracted minutiae from a 200 x 200 fingerprint image. (ICAO standard is accepted about 20 to 30 minutiae for identification in travel documents. Due to this fact, for each minutiae be considered three fields(x-coordinate, y-coordinate and orientation), if we consider 9 bits for each component, watermark bits is 25 x 3 x 9=675. A 675 bits watermark is a very big watermark comparing to the face image’s size that most of the common methods lose their performance. In the next part, we’ll propose a new algorithm that can embed a large watermark with no visibility in grey-scale images.

This paper is organized as follows: in the next section, we explain the discrete wavelet transform domain in images. In section III, we propose a new biometric watermarking algorithm based on the tow-dimensional discrete wavelet transform, to securely and robustly, embed the minutiae data into the face image of the same individual. In section IV, we test the proposed watermarking algorithm against common distortions introduced by compression and geometrical attack and show considerable improvements in comparison to the corresponding wavelet based methods. Section V is conclusions.

II. Descrete Wavelet Transform Domain

Transform Domain methods hide data in significant areas of host image (face image) which makes them robust against compression, enhancement and etc. Many transform domains exist for data hiding. DCT helps separate the image into spectral sub-bands of differing importance. Some DCT steganographic algorithms have been given in [16-18].

The Discrete Wavelet Transform (DWT) of images produces a non-redundant image representation which provides better spatial and spectral localization of image formation. In case of sub-band analysis of images, we require extraction of its approximate forms in both horizontal and vertical directions, details in horizontal direction alone, details in vertical direction alone and details in both horizontal and vertical directions. This analysis of 2D signals require the use of following two-dimensional filter functions through the multiplication of separate scaling and wavelet functions in n_1 (horizontal) and n_2 (vertical) directions, as defined below:

$$\varphi(\mathrm{n}_1,\mathrm{n}_2)=\varphi(\mathrm{n}_1)\varphi(\mathrm{n}_2) \tag{1}$$

$$\psi^{\mathrm{H}}(\mathrm{n}_1,\mathrm{n}_2)=\psi(\mathrm{n}_1)\varphi(\mathrm{n}_2) \tag{2}$$

$$\psi^{\mathrm{V}}(\mathrm{n}_1,\mathrm{n}_2)=\varphi(\mathrm{n}_1)\psi(\mathrm{n}_2) \tag{3}$$

$$\psi^{\mathrm{D}}(\mathrm{n}_1,\mathrm{n}_2)=\psi(\mathrm{n}_1)\psi(\mathrm{n}_2) \tag{4}$$

In the above equations, $\varphi(\mathrm{n}_1,\mathrm{n}_2)$, $\psi^{\mathrm{H}}(\mathrm{n}_1,\mathrm{n}_2)$, $\psi^{\mathrm{V}}(\mathrm{n}_1,\mathrm{n}_2)$, and $\psi^{\mathrm{D}}(\mathrm{n}_1,\mathrm{n}_2)$ represent the approximated signal, signal with horizontal details, signal with vertical details and signals with diagonal details respectively. The 2-D analysis filter implemented through separable scaling and wavelet function is shown in fig.1.

The filtering in each direction follows sub sampling by a factor of two, so that each of the sub-bands corresponding to the filter outputs contain one-fourth of the number of samples, as compared to the original 2-D signal. The output of the analysis filter banks is the Discrete Wavelet Transformed (DWT) coefficients. The bands , $\varphi(\mathrm{n}_1,\mathrm{n}_2)$, $\psi^{\mathrm{H}}(\mathrm{n}_1,\mathrm{n}_2)$, $\psi^{\mathrm{V}}(\mathrm{n}_1,\mathrm{n}_2)$, and $\psi^{\mathrm{D}}(\mathrm{n}_1,\mathrm{n}_2)$ are also referred to as LL,LH,HL and HH respectively, where the first letter represents whether it is low-pass (L) or high-pass (H) filtered along the columns and the second letter represents whether the low-pass or high-pass filtering is applied along the rows (horizontal direction). The two-dimensional DWT of an image function $\mathrm{s}(\mathrm{n}_1,\mathrm{n}_2)$ of size $N_1 \times N_2$ may be expressed as

$$W_\varphi(j_0,k_1,k_2)=\frac{1}{\sqrt{N_1N_2}}\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2}s(n_1,n_2)\varphi_{j_0,k_1,k_2}(n_1,n_2) \tag{5}$$

$$W_\psi^i(j_0,k_1,k_2)=\frac{1}{\sqrt{N_1N_2}}\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2}s(n_1,n_2)\psi_{j_0,k_1,k_2}(n_1,n_2) \tag{6}$$

Where i={H,V,D} indicate the directional index of the wavelet function. j_0 represents any starting scale, which may be treated as $\mathrm{j}_0=0$. Given the equations (5) and (6) for two-dimensional DWT, the image function $\mathrm{s}(\mathrm{n}_1,\mathrm{n}_2)$ is obtained through the 2-D IDWT, as given below:

$$\begin{aligned}s(n_1,n_2)&=\frac{1}{\sqrt{N_1N_2}}\sum_{k_1}\sum_{k_2}W_\varphi(j_0,k_1,k_2)\varphi_{j_0,k_1,k_2}(n_1,n_2)\\&+\frac{1}{\sqrt{N_1N_2}}\sum_{i=H,V,D}\sum_{j=0}^{\infty}W_\psi^i(j,k_1,k_2)\psi^i{}_{j_0,k_1,k_2}(n_1,n_2)\end{aligned} \tag{7}$$

The 2-D scaling and wavelet functions used in equations (5) to (7) can be realized through separable, one-dimensional FIR digital filters of impulse responses $h_\varphi(-n)$ and $h_\psi(-n)$. Various forms of filters are used, Haar filters having $h_\varphi(-n)=\{1/\sqrt{2},-1/\sqrt{2}\}$ and $h_\psi(-n)=\{1/\sqrt{2},-1/\sqrt{2}\}$ }. If the 2-D analysis filter bank, with Haar filter coefficients is applied on the digital image shown in fig.1a, what results is a Discrete Wavelet Transformed (DWT) image with first level of decomposition, as shown in fig. 1b.

III. Proposed Watermarking Algorithm

In this paper, the extracted minutiae data of fingerprint image are used as watermarks and are embedded in the face image to be authenticated. The proposed embedding method consists of two parts: watermark embedding and extraction process.

A. Watermark Embedding Process

The grey-scale face image is decomposed using a 1-level two-dimensional DWT to obtain four sub-bands. Fig. 1 shows the DWT decomposition of a face image {cA, cH, cV, cD}.

In our method, we select the diagonal detail coefficients (cD) for embedding. Experimental results reveal that embedding in cD, gives better PSNR than doing so with other coefficients. During compression and filtering attacks, some of the information will be lost in high frequency bands. We overcome this loss by repeatedly embedding information in diagonal detail coefficient.

A uniformly distributed, zero mean and two-dimensional pseudorandom sequence [8, 15] of the size of sub-band matrix is generated with the secret key. This pseudorandom sequence is used to embed the watermark bits in the locations of the

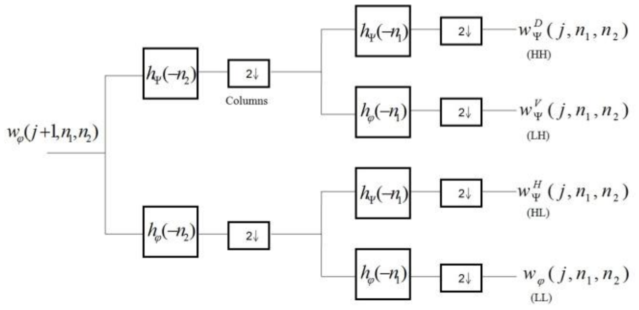

Fig. 1. 2-D analysis filtering through separable scaling and wavelet functions

selected sub-band to be watermarked. During the embedding watermark bits, a location more than once not decoded. As a result the next place checked for embedding.

The details of embedding procedure are as follows: cD is diagonal sub-band matrix and K at the first is 1.

For each watermark bit:

If the watermark bit is 0

$$cD(i,j) = \min(cD(i,j+1), cD(i,j+2), cD(i,j+3)) - k \quad (8)$$

If the watermark bit is 1

$$cD(i,j) = \max(cD(i,j+1), cD(i,j+2), cD(i,j+3)) + k \quad (9)$$

Where k is constant parameter that makes the extracting procedure more accurately be performed.

After the embedding all of watermark bits (minutiae data), we apply the inverse DWT on the transformed image. Until the primary watermarked image be produced.

B. Watermark Extraction Process

In this part, we explain the extraction procedure. We apply 1-level DWT to the watermarked image and select the diagonal sub-band into which the watermarked was embedded.

By a secret key, regenerate the same pseudorandom sequence used in the embedding procedure. So the location of watermark bits is determined.

This extraction does not require the original image and it is called as semi-blind. The extraction process is formulated as follows:

If $cD(i,j) < median(cD(i,j+1), cD(i,j+2), cD(i,j+3))$ (10)

Watermarked bit is 0.

If $cD(i,j) > median(cD(i,j+1), cD(i,j+2), cD(i,j+3))$ (11)

Watermarked bit is 1.

The extracting procedure may make wrong bits, because the decoding is based on the estimation and may lead to be wrong bits. In interested application, the correct decoding of all the bits is very important yet. Because the valuable data is inserted and even changing one bit causes reducing of capability of using data. In order to ensure the decoding without error, the encoder uses a controller block.

This block adjusts the constant parameter k, if there's a possibility of incorrect bit decoding. The proposed wavelet-based watermark embedding and extraction scheme is shown in figure 2. Figure 3 show the block diagram of watermark algorithm. For robust against difference attacks, every watermark bit is embedded at multiple locations.

Peak Signal to Noise Ratio (PSNR) is generally used to analyze quality of images in dB. PSNR calculation of two images, one original and altered image describes how far two images are equal.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (12)$$

Where MSE is Mean Squared Error between original and altered image, which defined as below:

$$MSE = \sum_{i=1}^{x}\sum_{j=1}^{y}\frac{(\left|O_{ij} - W_{ij}\right|)^2}{x \times y} \quad (13)$$

Where O is original image and W is the watermarked image and $x \times \mathrm{y}$ is the size of image.

In this paper, we used correlation coefficient to show the similarity between the original and extracted watermark. In the proposed method, correlation coefficient is defined as

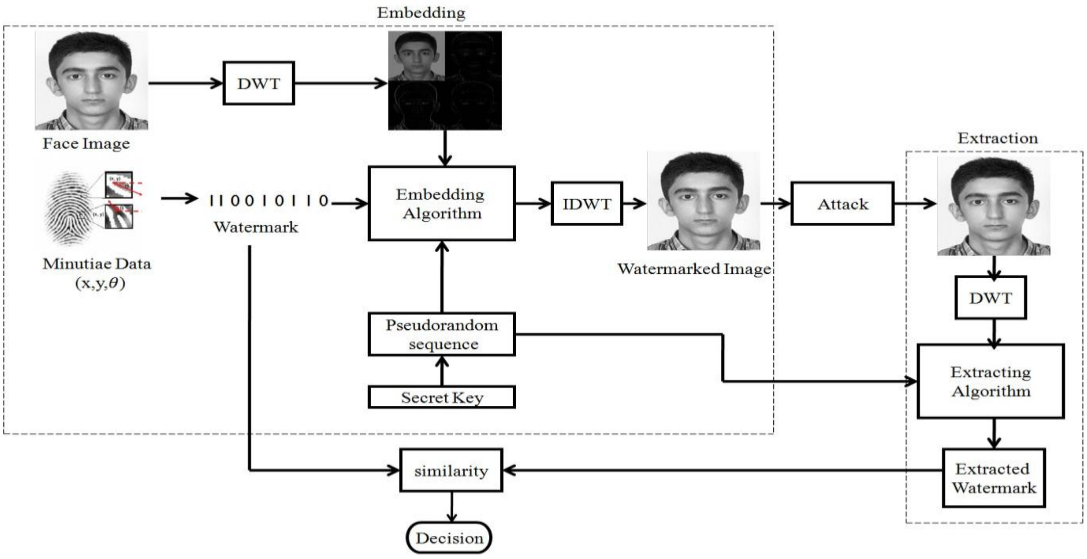

Fig. 2. The scheme of proposed biometric watermarking

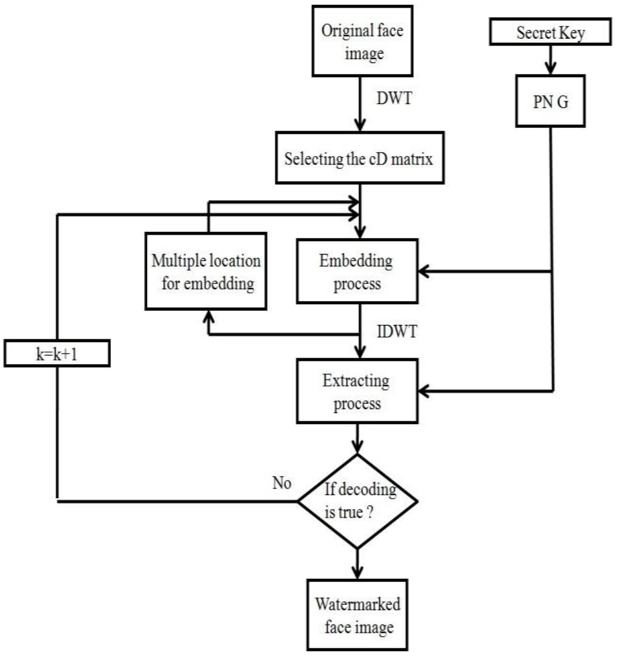

Fig. 3. Block diagram of proposed algorithm

$$\rho(w,\bar{w}) = \frac{\sum_{i=1}^{r} w(i)\bar{w}(i)}{\sqrt{\sum_{i=1}^{r}\bar{w}^{2}(i)}\sqrt{\sum_{i-=1}^{r} w^{2}(i)}} \tag{14}$$

Where w is the original watermark, and is the extracted watermark and r is the length of the watermark. , because w and lies between {1,-1}, we replace watermark bit o by -1.

IV. Exprimental Results

In order to evaluate the performance of proposed biometric watermarking algorithm, MATLAB platform is used. The proposed algorithm is validated on the database containing 100 face images and minutiae data from 100 individuals.

In figure 4, watermarked face image with proposed method and watermarked image with method in reference [1] are shown. As observed, in watermarked image, no perceptual degradation is found according to the human visual system (HVS). The quality of watermarked face image is measured with PSNR, which for all images were obtained about 49.6 dB. Robustness of proposed algorithm under the common image processing operations have been identified with help of similarity Ratio, and compared against proposed method in reference [1].

These attacks may occur during the communication and transmission of biometric. The watermarked face image is attacked by Cropping, Histogram Equalization, Gaussian and salt & pepper noises addition, Resizing, Sharpening, Contrast adjustment, JPEG2000 compression and Rotation attacks. Watermarked face image degraded by adding 15% Gaussian noise randomly and robustness against additive noise is estimated. This watermarked image compressed using JPEG2000 with compression ratio 50 and watermark is extracted from compressed watermarked image. For image cropping attack, 20% area of the watermarked image is cropped and then watermark is extracted. To check the robustness against Resizing attack, watermarked image is resized to 80% and the size of it is reduced to 210 x 295. Then back to its original size i.e. 240 x 320 for watermark extracting. These attacks are shown in figure 5. Under the same conditions, we compared the proposed algorithm in this paper with proposed algorithm in ref. [1]. The correlation coefficients and watermark data decoding performance of all extracted watermark bits after attacks are given in table 2. Experimental results show that the proposed method is more robust under the many of the attacks comparing to ref. [1].

TABLE I
PSNR of the watermarked face image

Method	PSNR (dB)
Proposed method	49.62
Method [1]	30.06

V. Conclusion

The biometric watermarking is One of the methods that prevent attacks on biometric, especially, when the biometric is transmitted via network or by a person (on ID card Smart). So, for efficiency and security, the identification systems, proposed to use of two biometric simultaneously, which is watermarked the one in the other. In this paper, we proposed a new approach in the DWT domain for embedding the minutiae data in the face image, which has more efficiency and security. This method is robust under many attacks such as Sharpening, Contrast Adjustment, Histogram Equalization

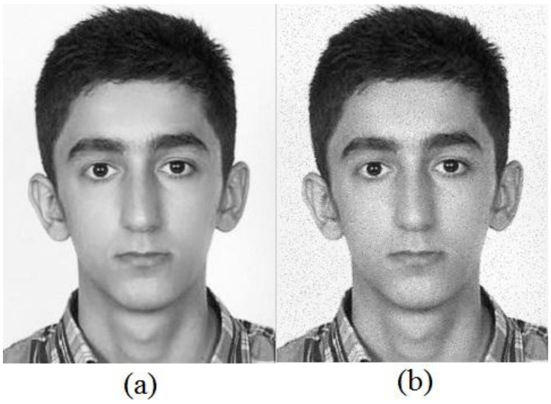
(a) (b)

Fig. 4. a) Watermarked image with proposed method b) watermarked image with method [1] and other image processing operation. As observed, in watermarked image, no perceptual degradation is found.

TABLE II
CORRELATION COEFFICIENTS AND WATERMARK DATA DECODING PERFORMANCE AFTER ATTACKS

Attacks	ρ		WP (%)	
	Prop.method	**method[1]**	**Prop.method**	**method[1]**
No Attack	1	0.95	100	97.24
Cropping	0.92	0.98	95.56	99.90
Histogram Equalization	0.93	0.8	96.29	72.43
Salt & pepper Noise	0.93	0.18	96.67	57.77
Gaussian Noise	0.90	0.73	92.59	86.48
Sharpening	1	0.98	100	99.44
Resizing	0.91	0.71	98.7	84.4
Rotation	0.71	0.76	85.56	88.33
JPEG2000 Compression	0.98	0.89	98.7	91.23
Contrast Adjustment (50% increased)	0.96	0.59	98.33	79.62
Contrast Adjustment (50% reduced)	0.98	0.80	98.88	88.92

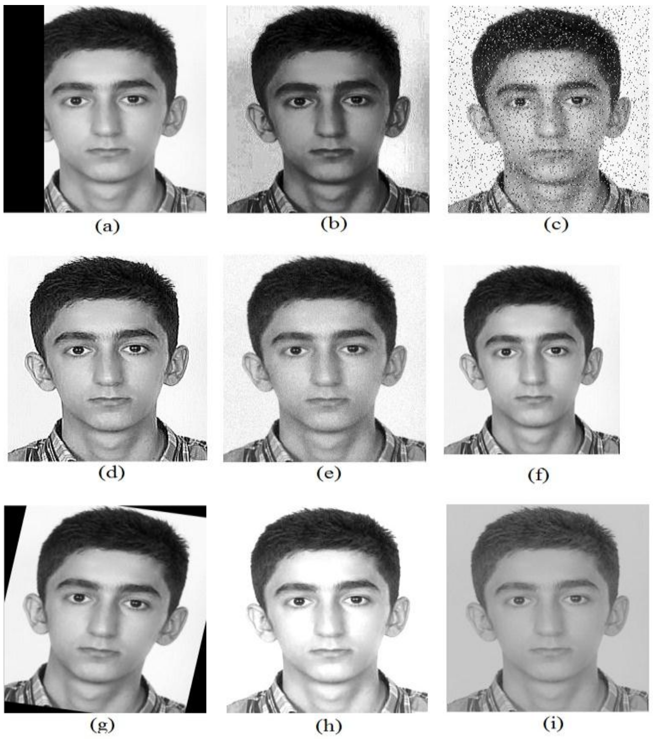

Fig. 5. Attached Watermarked face image with a) Cropping (20%) b) Histogram Equalization c) Salt & Pepper Noise Addition d) Sharpening (50%) e) Gaussian Noise Addition f) Resizing (80%) g) Rotation (10°) h) Contrast Adjustment (Increased) i) Contrast Adjustment (Reduced)

REFERENCES

[1] Jain A.K and Uludag U., "Hiding Biometric Data," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 25, NO. 11, pp. 1494-1498, November 2003.

[2] [2] Pankanti S. and Yeung M.M., "Verification Watermarks on fingerprint Recognition and Retrieval," *Proc. SPIE*, vol. 3657, pp.66-78, 1999.

[3] [3] A.K. Jain, K.Nandakumar, and A.Nager, "Biometric Template Security," *EURASIP Journal on Advances in Signal Processing,* 2008, pp. 1-17.

[4] [4] B.Gunsel, U.Uludaga and A.M. Tekalp, "Robust Watermarking of Fingerprint Images," *Pattern Recognition,* 35(12), 2002, pp. 2739-2747.

[5] [5] D. Kundur and D.Hatzinakos, "Digital Watermarking Using Multiresolution Wavelet Decomposition," *International conference on acoustic Speech and Signal Processing (ICASSP),* Seattle, May.1999, pp. 2969-2972.

[6] [6] F. Petitcolas, R. Anderson, and M. Kuhn, "Information hiding – A survey," *Proc. IEEE,* vol. 87, no. 7, pp. 1062-1078, 1999.

[7] [7] Salah M. Rahal, Hatim A. Aboalssamh, Khalid N. Muteb," Multimodal Biometric Authentication System – MBAS," 2nd *IEEE International Conf. On Communication & Technologies*, April 24-28, 2006 Damascus, Syria.

[8] [8] A.K. Jain and U. Uludag, "Hiding Fingerprint Minutiae in Images," *Proc. International Conference on Pattern Recognition,* 3(3), 2002, pp. 756-759.

[9] [9] A. Abu-EErrub, A. Al-Haj, "Optimized DWT Based Image Watermarking," *IEEE*, 2008

[10] [10] J. Delaigle, C. De Vleeschouwer, B. Macq, "Psychovisual Approach to Digital Picture Watermarking," *Journal of Electronic Imaging*, vol. 7, no. 3, pp. 628-640, 1998.

[11] [11] R.C. Gonzalez, R.E. Woods, *Digital Image Processing,* New Jersey: Prentice Hall, Upper Saddle River, 2002.

[12] [12] C. V. Serdean, M. Tomlinson, J. Wade, A.M. Ambroze, "Protecting Intellectual Rights: Digital Watermarking in the wavelet domain," *IEEE Int. Workshop Trends and Recent Achievements in IT,* pp. 16-18, 2002.

[13] [13] R.safarbakhsh, S.zzaboli, A. Tabibiazar, "Digital Watermarking on Still Images Using Wavelet Transform," *in Proc. International Conference on Information Technology: Coding and Computing ITCC'04,IEEE,* 2004.

[14] [14] A. Graphs, "An Introduction to Wavelets," *IEEE Computational Science and Engineering,* vol. 2, no. 2, pp.50-61, 1995.

[15] [15] B.Furht, D. Kirovski, "Encryption and Authentications: Techniques and Applications," USA: Auerbach, 2006

[16] [16] R. K Chhotaray. K.B Shiva Kumar, K. B Raja and Sabyasachi Pattanaik, "Bit length replacement steganography based on dct coefficients," *International Journal of Engineering Science and Technology,* 2:3561-3570, 2010.

[17] [17] Chia-chen Lin, "High capacity data hiding scheme for dct-based images," *Journal of Information Hiding and Multimeda Signal Processing,* 2010.

[18] [18] Ajit Danti and Preethi Acharya, "Randomized embedding scheme based on dct coefficients for image steganography," *IJCA Special Issue on Recent Trends in Image Processing and Pattern Recognition,* 2010.