A Blind DCT Domain Digital Watermarking for Biometric Authentication

Ameya K. Naik
S.G.G.S. Institute of Engg. and Tech.
Vishnupuri, Nanded
Maharashtra, India 431606

Raghunath S. Holambe
S.G.G.S. Institute of Engg. and Tech.
Vishnupuri, Nanded
Maharashtra, India 431606

ABSTRACT
In this paper, an efficient blind digital image watermarking algorithm using mapping technique is presented. The algorithm can embed or hide an entire image or pattern (logo) directly into the original image. The embedding process is based on changing the selected DCT coefficients of the host image to odd or even values depending on the binary bit value of watermark DCT coefficients. The algorithm is tested for fingerprint image embedded with a face watermark. It is demonstrated that the watermarking algorithm offers a significant advantage of providing biometric image compression and authentication without introducing any significant degradation in the image quality. Moreover the watermarking scheme is blind and does not require any additional data for logo extraction.

Categories and Subject Descriptors
I.4.2 [**Computing Methodologies**]: Image Processing and Computer Vision – *Compression (Coding), Approximate methods.*

General Terms
Algorithms, Performance, Experimentation, Security, Verification.

Keywords
Blind Watermarking, DCT, Face, Fingerprint, Data hiding.

1. INTRODUCTION
Biometrics based authentication systems are becoming increasingly popular as they offer enhanced security and user convenience as compared to traditional token-based (I.D. card) and knowledge based (password) systems. With the increasing usage of biometric systems the problem of storing the sensor data has become an important issue. Also in most of the cases the sensor data has to be transferred via a communication channel with low bandwidth and high latency. Therefore minimization of the amount of data is highly desirable which is achieved by compressing [1] the data before transmission.

During the last decade several algorithms and standards for compressing biometric image data have been evolved. The recent ISO/IEC 19794 standard specifies that fingerprint and face image data be stored in lossy manner in JPEG [2] (Joint Photographic Experts Group), WSQ (Wavelet Scalar Quantization) and JPEG 2000 format.

Another important issue related to biometric system is the security and integrity of the stored templates. Existing literature [6] focuses on encryption and watermarking techniques to address this problem. Encryption techniques do not provide security once the data is decrypted. As against this watermarking involves embedding information into host data itself, thus providing security even after decryption. Recently a watermarking technique was proposed that embeds facial information of a user in his/her fingerprint images.

During the last decade considerable work and research has been done in the area of digital watermarking. However most of the algorithms used for watermarking were incomplete (non-blind), i.e. they require the original image to extract the watermark.

In this paper, an efficient blind watermarking technique[5] is presented. In this technique the face image is embedded into a fingerprint host image. The fifteen DCT (Discrete Cosine Transform) [3][4] coefficients of the logo (face image) are converted into binary bits using mapping technique. These binary bits embedded into ten low frequency band coefficients of the DCT sub-blocks. It is seen that the algorithm provides excellent compression without degrading the image quality.

2. THE MAPPING TECHNIQUE
The mapping technique[9] is based on the principle of converting the transform coefficients to a range of decimal values less than unity. The number of bits used to represent each mapped values can be selected by the user considering the amount of compression required and the quality of reconstructed image. Similar to the JPEG in this technique, the image is first divided into blocks of size 8 x 8 pixels and discrete cosine transform is calculated for each block. We have used DCT since DCT gives excellent energy compaction only in small number of coefficients. We then map the transform coefficients to a new scale. The new range depends on the number of bits used to represent each transform coefficient. Since the performance of this technique also depends on the range of the transformed pixel coefficients, we perform the mapping operation by grouping the transform coefficients into fixed sized blocks

The watermark logo (face image) is first converted into the binary form $\{w(z)\}$ using the mapping technique (figure 1). The parameters used for logo binary conversion are as follows

(i) Size of the sub-block (ns) = 8

(ii) Number of coefficients considered for each block (nc) = 15

(iii) Number of bits used for binary representation of transform coefficients (n) = 8

(iv) Number of bits used for binary representation of offset and range = 14

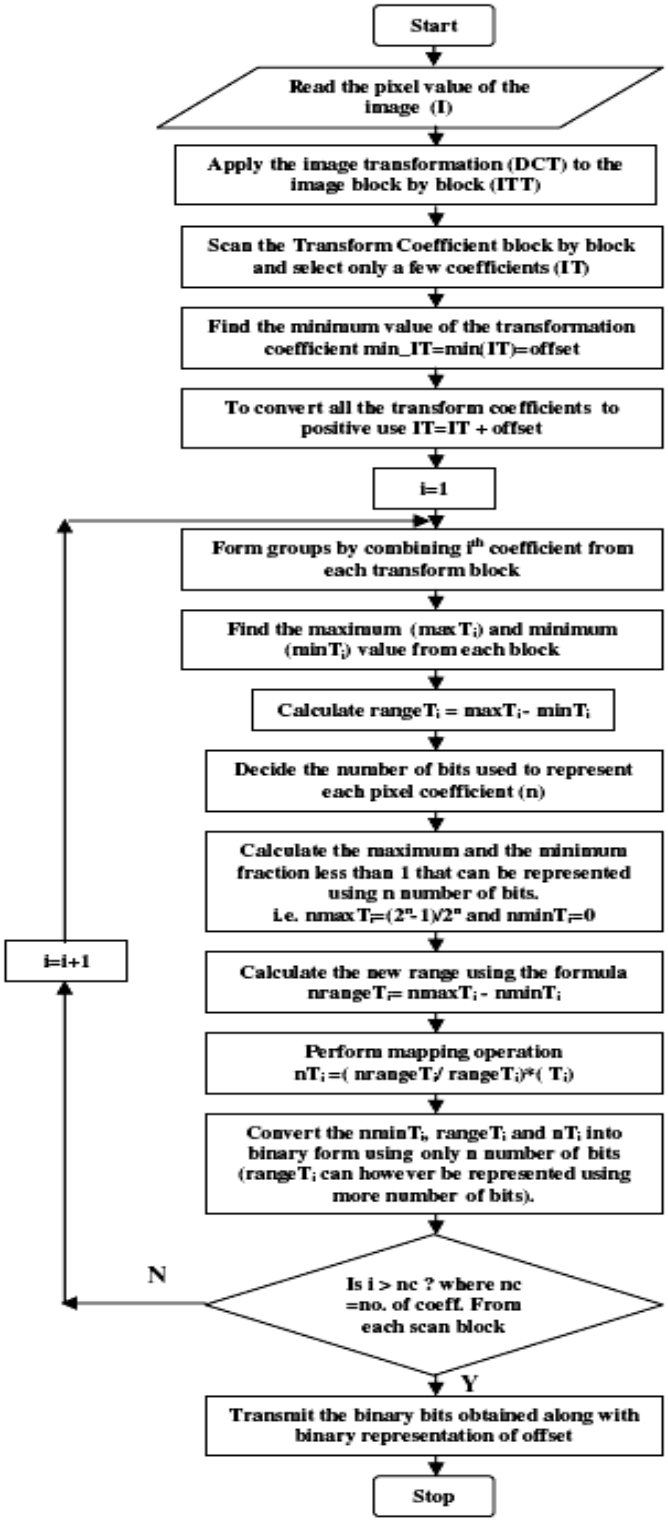


Figure 1. The Mapping Technique.

3. THE EMBEDDING ALGORITHM

The watermark embedding algorithm is described in the following steps.

Step 1: The host image (fingerprint) is divided into N, 8x8 sub-blocks which are DCT transformed as shown

$$F_k(u,v) = DCT\{f_k(i,j)\} \quad u \le 8, v \le 8, 1 \le k \le N$$

where k = block number

f_k = pixel intensities in the k^{th} block

F_k = DCT coefficients in the k^{th} block . (1)

Inside every 8 x 8 sub-block , ten DCT coefficients are identified. Each block of DCT coefficient is subjected to a process of zigzag scan. The first ten low frequency coefficients including the DC coefficients are selected. The coefficients from each block are arranged according to the scheme as shown in figure 2.

DC1	DC2	….	DC 10	AC 1,1	AC 1,2	…	AC 1,10	AC 2,1	…..	AC N,10

Figure 2. The ordering of DCT coefficients

Step 2: The binary bits w(z) obtained from the logo after mapping are embedded into the 10N DCT coefficients of the host image. The bit embedding equation [5] is defined as

If $w(z) = 1$ then

$$F'_k(u,v) = \begin{cases} \Delta Q_e\left(\dfrac{F^c{}_k(u,v)}{\Delta}\right) \\ F^c{}_k(u,v) \end{cases} 1 \le k \le N$$

$$1 \le k \le N$$

If $w(z) = 0$ then (2)

$$F'_k(u,v) = \begin{cases} \Delta Q_o\left(\dfrac{F^c{}_k(u,v)}{\Delta}\right) \\ F^c{}_k(u,v) \end{cases} 1 \le k \le N$$

$$1 \le k \le N$$

where Δ is a scaling quantity, Q_e is the quantization to the nearest even number, Q_o is the quantization to the nearest odd number and $F^c{}_k$ is the nearest integer greater than or equal to F_k

Step 3: The watermarked host image is obtained using the inverse DCT of all $F_k(u,v), 1 \le k \le N$.

4. THE RECONSTRUCTION ALGORITHM

The merged watermarks information $w(z)$ can be extracted by the following steps.

Step 1: Perform 8x8 DCT transform for the watermarked fingerprint image.

Step 2: Perform zigzag scan on the coefficients and select ten coefficients from each sub-block. The coefficients from each block are arranged according to the scheme as shown in figure 2.

Step 3: Extract the watermark bits. The extraction formulae are as shown

If $Q_o\left(\frac{F'_k(u,v)}{\Delta}\right)$ is odd then $w(z) = 0$

If $Q_o\left(\frac{F'_k(u,v)}{\Delta}\right)$ is even then $w(z) = 1$ (3)

Step 4: Perform inverse mapping on the bits obtained. The inverse mapping procedure is exactly the reverse of the mapping procedure. Finally, the transform coefficients and hence the reconstructed image (logo) is obtained.

5. PERFORMANCE METRICS

The original host image (fingerprint) and the original logo (face) are compared with the watermarked image and the extracted logo respectively. The performance metric used is the peak signal to noise ratio ($PSNR$)[3]. Higher $PSNR$ values imply closer resemblance between reconstructed and original image.

If the pixels of the original image are denoted by P_i and the pixels of the reconstructed image as Q_i (where $1 \le i \le n$), we first define the mean square error (MSE) between n pixels of the two images as

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(P_i - Q_i\right)^2 \quad (4)$$

The root mean square error ($RMSE$) is defined as the square root of the MSE , and the $PSNR$ is defined as

$$PSNR = 20\log_{10}\frac{\max_i |P_i|}{RMSE} \quad (5)$$

The amount of compression achieved by the algorithm is given by

$$Compression\ Ratio = \frac{Size\ of\ input\ stream - Size\ of\ output\ stream}{Size\ of\ input\ stream} X100 \quad (6)$$

6. EXPERIMENTAL RESULTS

In this section we present simulation results to depict the performance of the watermarking algorithm for biometric images. The performance is evaluated in terms of $PSNR$ for different combination of host and logo images. For simulation the following parameters are considered.

(i) The original host image (fingerprint)(figure 3)is a 512 x 512 pixel gray scale with intensity levels ranging from 0 to 255.

(ii) The original logo (face)(figure 4)is a 128 x 128 pixel gray scale with intensity levels ranging from 0 to 255.

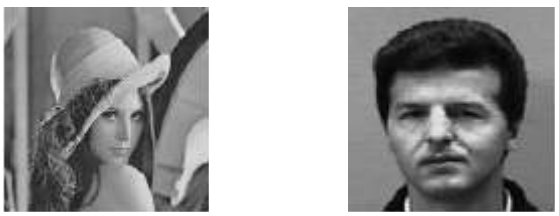
(iii) The transform block and the scanning block used for both fingerprint and face images is 8 x 8. For face image after scanning only 15 coefficients are considered for mapping to binary bits whereas for fingerprint image after scanning only 10 coefficients are considered for watermark embedding.

(iv) The scaling factor Δ is considered to be unity.

Results are presented for two sets of fingerprint and watermark images. Figure 5 shows the output obtained for the watermark algorithm based on mapping technique. As a first case we embed the first logo image (figure 4a) in the first host fingerprint image (figure 3a). It is seen that there is no noticeable difference between the watermarked ($PSNR$ =36.66dB) and extracted logo images ($PSNR$ =33.88dB). Similarly different combinations of host and watermark images are tested for watermark algorithm. The $PSNR$ values are tabulated in Table 1. Results (figure 5a-5d) show that the $PSNR$ values obtained in all the cases are greater than 30dB thus offering a satisfactory resemblance between original and reconstructed images.

(a) **(b)**

Figure 3. Fingerprint host images (Size 512 x 512).



(a) **(b)**

Figure 4. Watermark Face images (Size 128 x 128).

The *PSNR* values also depict that a better image quality can be obtained if higher number of coefficients (nc=15 for host and 21 for logo) are considered while mapping. However the improved performance is obtained at the cost of increase in the data bits.

(a)

(b)

(c)

(d)

Figure 5. Watermarked image and Extracted Logo.

The actual storage space required using the mapping and the well known JPEG [7] techniques is presented in Table 2.

Table 1. *PSNR* **values obtained for different host and watermark images.**

Host Fingerprint image	**Logo Face image**	*PSNR* in dB			
		nc=10 for host nc=15 for logo		**nc=15 for host nc=21 for logo**	
		HOST	LOGO	HOST	LOGO
Figure 3a	Figure 4a	36.66	33.88	41.19	34.82
Figure 3b	Figure 4b	33.87	37.21	37.52	39.37
Figure 3a	Figure 4b	36.65	37.21	41.20	39.37
Figure 3b	Figure 4a	33.87	33.88	37.53	34.82

Table 2. Size of the stored images in KB in bitmap format, JPEG format and using Mapping technique

Bitmap format (Host+Logo) (KB)	**JPEG format (Host+Logo) (KB)**	**Mapping Technique (KB)**	
		nc=10 for host nc=15 for logo	**nc=15 for host nc=21 for logo**
274	49.87	47.00	67.00
274	49.76	47.00	67.00
274	49.06	47.00	67.00

274	50.57	47.00	67.00

The observed values demonstrate that the performance of Mapping technique is better than JPEG and bitmap formats if lesser coefficients are considered. More ever the watermarked image obtained using mapping technique provides authentication[8] of the host image since the face image is hidden in the fingerprint image itself.

7. CONCLUSION

This paper discusses the mapping technique to be used for watermarking of the biometric images. The image quality obtained using this scheme can be changed by varying the number of coefficients considered. Moreover in this technique the face image itself can be retrieved from the watermarked fingerprint image. Thus authentication of the fingerprint data is achieved along with compression.

8. REFERENCES

[1] B. D. Tseng and W. C. Miller. On computing the discrete cosine transform, IEEE Trans. Computing, vol. C-27: July 1976, 966-968.

[2] C. Wang, Z. Hou, and A. Yang. An Improved JPEG Compression Algorithm Based on Sloped-facet Model of Image Segmentation In Proceedings. IEEE International Conference on Wireless Communications, Networking and Mobile Computing, Sept. 2007, 2893-2896.

[3] David Salomon. Data Compression - The Complete Reference 3rd Edition, Springer, 2004

[4] N. Ahmed, T. Natarajan, and K. R. Rao, Discrete cosine transform, IEEE Trans. Comput., vol. C-23, Jan. 1974, 90-93.

[5] Al-Gindy, A.N. Tawfik, A. Al Ahmad, H. Qahwaji, R.A, A New Blind Image Watermarking Technique for Dual Watermarks Using Low-Frequency Band DCT Coefficients, In Proceedings , 14th IEEE International Conference on Electronics Circuits and Systems 2007, 11-14 December 2007, 538-541.

[6] Anil K. Jain and Umut Uludag, Hiding Biometric Data, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 25, No. 11, Nov 2003, 1494-1498.

[7] K. Delac, M. Grigic and S. Grigic, Effects of JPEG and JPEG 2000 compression on face recognition, In Proceedings of ICAPR 2005, LNCS 3687, Springer-Verlag, 2005, 136-145.

[8] Umut Uludag, Sharath Pankanti, Salil Prabhakar and Anil K. Jain, Biometric Cryptosystems Issues and Challenges, In Proceedings of IEEE, vol. 92, no. 6, June 2004, 948-960.

[9] Shivali D. Kulkarni, Ameya K. Naik, and Nitin S. Nagori, "A Comparison of Real Valued Transforms for Image Compression", Fifth International Conference on Signal and Image Processing World Academy of Science Engineering and Technology, WCSET 2008 Congress Heidelberg, Germany, September 24-26, 2008, 504-508.