International Scholarly Research Network
ISRN Signal Processing
Volume 2012, Article ID 781940, 11 pages
doi:10.5402/2012/781940

Research Article

DCT Watermarking Approach for Security Enhancement of Multimodal System

Mita Paunwala[1] **and S. Patnaik**[2]

[1] *C. K. Pithawala College Of Engineering and Technology, Pithawala Educational Complex, Near Malvan Mandir, Via Magdalla Port, Dumas Road, Surat, Gujarat, India*
[2] *Sardar Vallabhbhai National Institute of Technology, SVNIT, Ichchhanath Road, Piplod, Surat, Gujarat, India*

Correspondence should be addressed to Mita Paunwala, mpaunwala@yahoo.co.in

Received 1 November 2012; Accepted 24 November 2012

Academic Editors: C.-M. Kuo and P.-Y. Yin

We have addressed a novel watermarking algorithm to support the capacity demanded by the multimodal biometric templates. Proposed technique embeds watermark in low frequency AC coefficients of selected 8×8 DCT blocks. Selection of blocks accomplishes perceptual transparency by exploiting the masking effects of human visual system (HVS). Embedding is done by modulating the coefficient magnitude as a function of its estimated value. Neighborhood estimation is used for the weighted DC coefficients from eight neighboring DCT blocks. The weights of the DC coefficients are calculated from local image intrinsic property. For our experimentation we have used iris and finger prints as the two templates which are watermarked into standard test images. The robustness of the proposed algorithm is compared with the few state-of-the-art literature when watermarked image is subjected to common channel attacks.

1. Introduction

With the current advances in information communication, world-wide-web connectivity, the security and privacy issues for authentication have increased by many folds. Applications such as electronic banking, e-commerce, m-commerce, ATM, smart cards, and so forth require high attention of data security, either while data is stored in the database/token, or transmitted over the network. This makes implementation of automatic, robust, and secure person identification a hot research topic. Biometric recognition offers a consistent solution for the user authentication to identity management systems. One of the reasons for popularity of this biometric system is its ability to differentiate between authorized person and forger who might illegally attempt to access the privilege of authorized person [1].

System accuracy depends on how efficiently it accepts genuine user and decline imposter user. Acceptance or denial of the user is confirmed based on matching between live and template database. However, a single physical characteristic or behavioral trait of an individual sometimes fails to stand as sufficient for user identification/verification. For this reason systems with integration of two or more different biometrics are currently have derived attention for being designed and made inter-operative. This recent development can provide an acceptable performance to increase the reliability of decisions as well as increases robustness with regard to fraudulent technologies when used by even more than one billion of users. Further it also helps to reduce failure to enroll rate (FER) or failure to capture rate (FCR) [2].

In [3] authors point out that a biometrics based verification system works properly only if the verifier system gives guarantee that the biometric data came from the genuine person at the time of enrollment and protected from various attacks while transmitted from client to server (between the database center and matcher). Though a biometric system can sustain security, it is also susceptible to various types of threats [4, 5]. In [6] author produces a generic biometric system with eight possible hierarchical positions of threats. These threats can be from fake biometric (fake finger, a face mask, etc.), an old recorded signal (old copy of fingerprint, recorded audio signal of a speaker, etc.), a feature extractor could be forced to produce feature generated value chosen by attacker than that of the actual one, synthetic feature set, artificially match score, manipulated template due to a non-secure communication channel between stored template and matcher.

One of the approaches to address the problem of non-secure communication channel and template manipulation is to embed biometric features as invisible structure to innocuous cover image. This technique is known as watermarking which prevents an eavesdropper from accessing sensitive template information and reduces manipulation rate.

A number of watermarking techniques have been proposed to secure information in an image. These can be mainly classified as spatial domain techniques and transformed domain techniques. Recent watermarking techniques are used in conjunction with biometric [7–17] to enhance the security of biometric. Ratha et al. [12] proposed a blind data hiding method, which is applicable to fingerprint images compressed with WSQ (Wavelet-packet Scalar Quantization) standard. The watermark message is assumed to be very small compared to the fingerprint image. The quantizer integer indices are randomly selected and each watermark bit replaces the LSB of the selected coefficient. At the decoder, the LSB's of these coefficients are collected in the same random order to construct the watermark. Jain et al. [13] used the facial information as watermark to authenticate the fingerprint image. A bit stream of eigen face coefficients are embedded into selected fingerprint image pixels using a randomly generated secret key. The embedding process is in spatial domain and does not require the original image for extracting the watermark. Noore et al. [14] proposed multiple watermarking algorithm, in texture regions of fingerprint image using Discrete Wavelet Transform (DWT). They used face and text information as watermark. Their approach is resilient to common attacks such as compression, filtering and noise. Komninos and Dimitriou [15] combined lattice and block-wise image watermarking technique to maintain image quality along with cryptographic technique to embed fingerprint templates into facial images. Al-Assam et al. [16] proposed a lightweight approach for securing biometric template, based on a simple efficient and stable procedure to generate random projections which meets the revocability property. Nagar et al. [17] proposed bio-hashing and cancelable fingerprint template transformation techniques based on six metrics to protect biometric trait, facilitates the security evaluation and vulnerable to linkage attacks.

The problems of biometric template security raise concerns with the wide spread explosion and deployment of biometric systems both commercially and in government applications. So by keeping security and secrecy issues in concern for the template security enhancement, in this paper, we present a novel biometric watermarking algorithm to support the capacity demanded by the multimodal templates. Section 2 describes the approach of biometric feature extraction and matching algorithms in brief. Sections 3 and 4 explains the proposed watermarking technique and fusion model respectively. The results obtained are illustrated in Section 5. We verify the matching ability of different biometrics without watermarking and with watermarking technique and study the resilience to various attacks during transmission and processing of host signal.

2. Biometric Feature Extraction and Matching Approach

Fingerprints and iris are selected as biometric as they are easily acquired, socially accepted and more or less invariant to individual aspects like culture, sex, education level, orientation, and so forth. This section briefly explains fingerprint minutiae (features) extraction, iris feature extraction, and matching technique.

2.1. Fingerprint Feature Extraction and Matching. To employ fingerprint minutiae extraction step, sensed print undergoes few necessary steps. In this work the raw finger print image has been routed through steps like (a) pre-processing: to extract fingerprint area, to remove the boundary, morphological opening operation requires to remove peaks introduced by background noise and closing operation to eliminate small cavities generated by improper pressure of fingerprint, (b) thinning: required to remove erroneous pixels which destroy the integrity of spurious bridges and spurs, exchange the type of minutiae points and miss detect true bifurcations, (c) false minutiae removal: required to remove false ridge breaks and ridge cross-connections which are generated due to insufficient amount of ink and over inking respectively.

After extracting minutia points special feature vector F_k is generated corresponding to single minutia point M_k which is rotation invariant. Feature vector F_k is generated by defining surface geometry consisting of N radial grids ($d_1 - d_N$), with origin at the minutia point and grid separation angle $360/N$ as shown in Figure 1. Grid d_1 is oriented along the orientation of kth minutia (ϕ_k). Grid nodes (points on grid) are marked along each grid at an interval of τ starting with the minutia point M_k as the origin. Larger the value of N and smaller the value of τ makes the size of feature vector large. This will give better accuracy at the cost of increased computational complexity. By defining the orientation of grid nodes as, $\phi^k_{i,m}$ ($1 \leq m \leq N$), we calculate the relative orientation between minutia M_k and node ridges as

$$\Psi^k_{i,m} = \left(\phi_k - \phi^k_{i,m}\right) \tag{1}$$

which is free from the rotation and translation of the fingerprint. $\phi^k_{i,m}$ represents the orientation of the ridge, that passes through the ith node, of mth grid, and for the kth minutia. If a node falls at furrows, then $\phi^k_{i,m}$ is assigned as 0. The final feature vector F_k of a minutia M_k that describes local structural characteristic, is then given as

$$F_k = \left\{ \left\{ \psi^k_{i,dm} \right\}^P_{i=1} \right\}^N_{m=1}, \tag{2}$$

where P gives number of grid nodes along the direction metric d_m corresponding to kth minutiae.

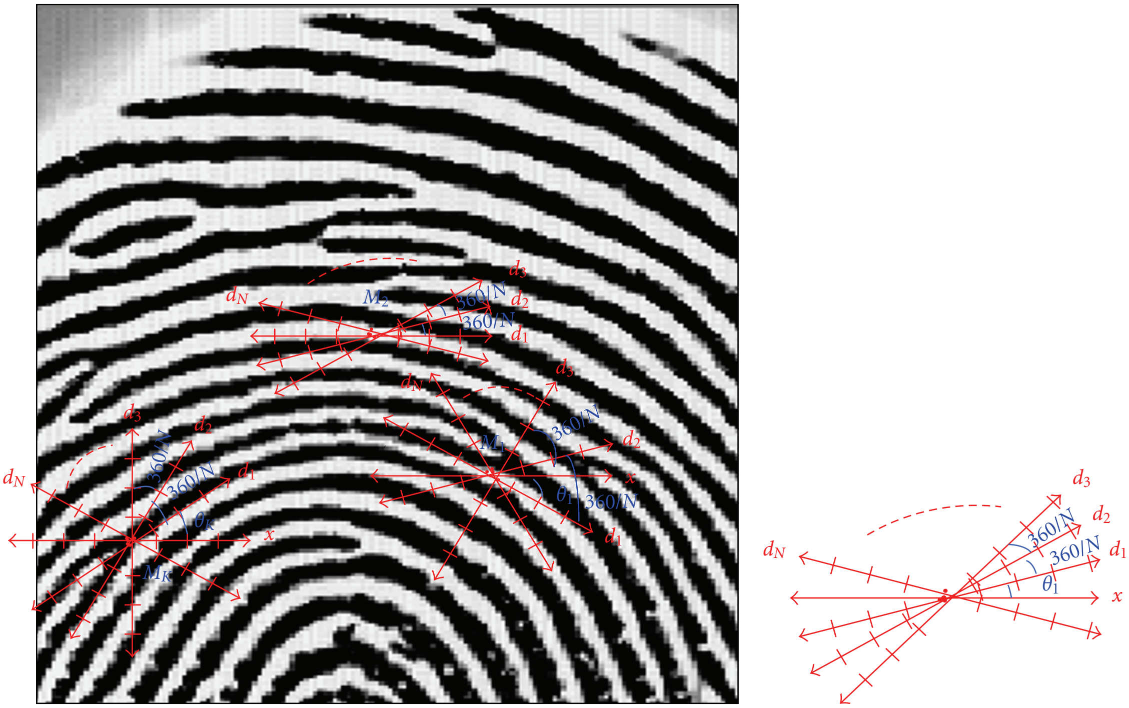


FIGURE 1: (a) N lines around a minutia detail (b) Grid nodes organized on radial grids.

Considering three grids and five nodes per each grid, specified feature vector will be of size 1×15 for each minutiae point. These feature vectors are converted into binary stream denoted as W'_f. Each relative orientation is represented with four bit, one for sign and three for orientation. Individual minutiae data sets contained between 20 to 30 minutiae points, with an average of 25 minutiae points. Thus the size of W'_f is $15 \times 4 \times 25 = 1500$ bit for single fingerprint template.

A distortion-tolerant matching algorithm [18] is used here that defines a novel feature vector for each fingerprint minutia based on the global orientation field. These features are used to identify corresponding minutiae between two fingerprint impressions by computing the similarity between feature vectors that gives high verification accuracy. Suppose F_i and F_j are the structure feature vectors of minutia i from input fingerprint and minutia j from retrieved features of fingerprint respectively, then a similarity level is defined as

$$S(i,j) = \begin{cases} 1 - \dfrac{\left|F_i - F_j\right|}{T} & \text{if } \left|F_i - F_j\right| < T, \\ 0 & \text{otherwise,} \end{cases} \qquad (3)$$

where $|F_i - F_j|$ is the Euclidean distance between feature vectors F_i and F_j and T is the predefined threshold. Here, the selection of the value of T is trade-off between False Acceptance Rate (FAR) and False Rejection Rate (FRR), high value of T increases FAR and opposite is true for FRR. Here, the similarity level describes a matching assurance level of a structure pair.

2.2. Iris Feature Extraction and Matching. The general iris recognition system consists of four important steps: (1) iris segmentation which extracts iris portion from the localized eye image, (2) iris normalization which converts the iris portion into rectangular strip of fixed dimensions to compensate for the deformation of pupil due to change in environmental conditions, (3) iris feature extraction deals with extraction of core iris features from the iris texture patterns and generate bitwise biometric template, and (4) iris template matching compares the stored template with the query template and gives the decision of authentication of a person based on some predefined threshold [19]. Among these steps the iris segmentation plays very important role in the whole system as it has to deal with eyelids and eyelashes occlusions, specular highlights. If iris portion is not properly segmented, then it may lead to poor recognition rates.

Iris segmentation is done using pupil circle region growing technique which uses binary integrated edge intensity curve approach to avoid eyelids and eyelashes. After locating the iris inner and outer boundaries, which contains eyelids and eyelashes, we grow the circle of the pupil gradually and generate its edge image using Sobel horizontal edge detector. As eyelids are horizontally aligned, horizontal biased Sobel operator gives prominent horizontal eyelid edges. This approach is specially used to detect the upper and lower eyelid regions and to restrict the Region of Interest (ROI). When the computed horizontal edge intensity curve is below threshold value $T1$, it indicates that the eyelids portion has not started as shown in Figure 2. The radius is required to

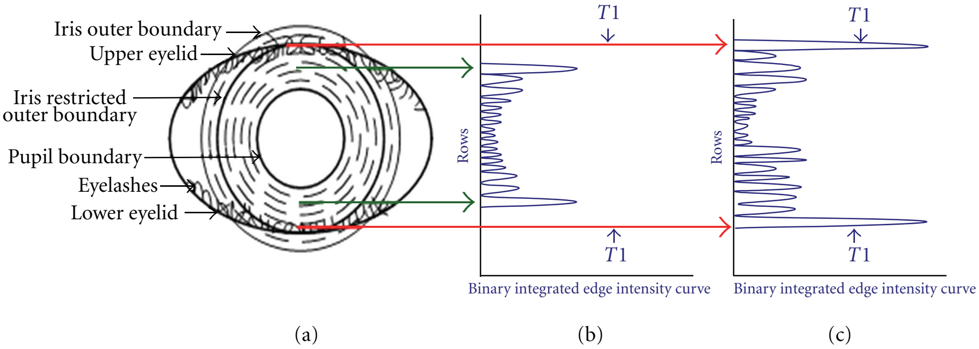

Iris outer boundary
Upper eyelid
Iris restricted outer boundary
Pupil boundary
Eyelashes
Lower eyelid
T1
T1
Rows
Binary integrated edge intensity curve
T1
T1
Rows
Binary integrated edge intensity curve
(a)
(b)
(c)

Figure 2: (a) Diagram of pupil circle region growing (b) edge intensity curve before threshold (c) edge intensity curve at threshold.

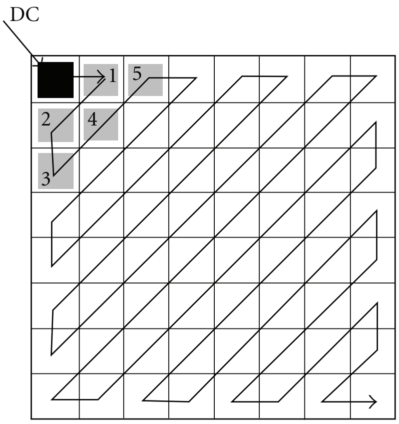


Figure 3: Signal energy distribution of 8 × 8 DCT block.

DC1	DC2	DC3
DC4	DC5	DC6
DC7	DC8	DC9

Figure 4: 3 × 3 Neighborhood of DCT blocks.

be grown until it covers eyelids. When the horizontal edge intensity curve exceeds threshold value $T1$, then it indicates that either upper or lower eyelid region has started appearing in the ROI. Here the growth of pupil circle is stopped. Thus the pupil circle is grown gradually to achieve a new outer iris boundary such that the area between the pupil boundary and new outer boundary does not contain eyelids or eyelashes.

The partial iris region between iris inner and restricted outer boundary is converted into rectangular strip of fixed dimensions 60 × 450 ($r \times \theta$) by Daugman's Rubber Sheet model [20]. Core feature of rectangular strip are extracted as suggested in [21]. The size of iris core feature W_i is 348 bits which is used as watermark. The matching between input iris feature and retrieved iris feature is done by standard Hamming Distance (HD).

3. Proposed Watermarking Approach

We have proposed a Discrete Cosine Transform (DCT) based blind watermarking technique. In the proposed approach original image X of arbitrary size $M \times N$ is divided into non-overlapping 8 × 8 blocks. Let x_{ij} be a pixel values from the block, where $1 \leq i, j \leq 8$. Each block is transformed into a two dimensional DCT block and categorized into smoother block, texture block, and edge block by measuring local block variance and local block projection of gradient. The key issues in watermarking are capacity, robustness and invisibility. These requirements are mutually viable and cannot be optimized simultaneously. For situation demanding immense amount of bit embedding, tradeoff between invisibility and robustness is necessary therefore reasonable compromise is always inevitability [22].

For biometric watermarking robustness is very important as biometric information (fingerprint feature vector and iris feature) is embedded where even a change in one bit can decrease the authenticity. Most of the signal energy of the block DCT is dense in the DC component and the remaining energy always has a spreading diminishingly in the AC components in zigzag scan order as shown in Figure 3. In that block with black shade represents DC component of 8 × 8 DCT block while blocks with gray and white shade indicate low frequency and high frequency AC component respectively.

Hiding of watermark bit in DC co-efficient gives more robustness but perception of watermark is then a major issue. Vice versa is true for high frequency AC coefficients. As a tradeoff, proposed technique embeds watermark in low frequency AC coefficients of the selected 8 × 8 DCT blocks. Embedding of watermark bit is done by modulating low frequency AC coefficients of 8 × 8 DCT block based on their estimated values. Estimated value of an AC coefficient is computed using the DC coefficients from eight neighboring DCT blocks as shown in Figure 4. In which DCj, $1 \leq j \leq 9$ are DC coefficients of neighborhood 8 × 8 blocks.

By considering such 3×3 overlapping neighborhood DCT blocks, AC_i, where $1 \leq i \leq 5$ coefficients of center DCT block are estimated by using

$$\begin{aligned}
\mathrm{AC}_1 &= k_1 * \mathrm{DC4} + k_2 * \mathrm{DC6},\\
\mathrm{AC}_2 &= k_3 * \mathrm{DC2} + k_4 * \mathrm{DC8},\\
\mathrm{AC}_3 &= k_5 * \mathrm{DC2} + k_6 * \mathrm{DC5} + k_7 * \mathrm{DC8},\\
\mathrm{AC}_4 &= k_8 * \mathrm{DC1} + k_9 * \mathrm{DC3} + k_{10} * \mathrm{DC7} + k_{11} * \mathrm{DC9},\\
\mathrm{AC}_5 &= k_{12} * \mathrm{DC4} + k_{13} * \mathrm{DC5} + k_{14} * \mathrm{DC6}.
\end{aligned} \tag{4}$$

The notions behind the selection of $\mathrm{DC}j$, $1 \leq j \leq 9$ coefficients to estimate particular AC_i coefficient in (4) are as follows.

(1) Horizontal variations in each 8×8 DCT block are characterized by AC components AC_1 and AC_5. Hence, DC values of horizontal neighborhood blocks (DC4, DC5 and DC6) are considered in the objective function for estimating AC_1 and AC_5.

(2) Vertical variations in each 8×8 DCT block are characterized by AC components AC_2 and AC_3. Hence, DC values of vertical neighborhood blocks (DC2, DC5 and DC8) are considered for estimating AC components AC_2 and AC_3.

(3) AC_4 represents the diagonal variations. Hence, DC1, DC3, DC7 and DC9 are considered for estimating AC components AC_4.

Linear Programming based optimization technique [23] is considered to calculate optimal weights (K_1 to K_{14}) based on image content. In this method known AC_i coefficients of benchmark images are used. All weights calculated for a particular AC_i coefficient are stored in different matrices and histogram for matrix elements is computed. The histogram of this matrix with weights as elements is a discrete function

$$h(K_i) = n_i, \tag{5}$$

where K_i is the ith weight and n_i is the number of weights in the matrix having ith value. From this set of weights, a weight whose frequency of occurrence obtained maximum is taken and accordingly multiplied with corresponding $\mathrm{DC}j$ coefficient for the AC coefficient estimation. The edge blocks are neither considered for estimation nor for watermark embedding because it leads to artifact in resultant watermarked image. Figure 5(a) shows artifact when considering edge blocks along with smooth blocks for embedding watermark.

The proposed method considers the local block features like variance and projection of gradient to identify the edge block in order to remove them from bit embedding processing. Statistical parameter variance is very sensitive to uncertainties so that it is used as a decisive parameter to find the smoother and edge block but it cannot discriminate between texture and edge blocks. However maxima of 1st order difference of projection of gradient image can differentiate the edge block from texture block. Uniform distribution of edges in the texture block will keep the difference at low value and for random presence of edge either or both vertical or horizontal projection difference will have significant values. If local variance is less than predefined threshold then block is marked as smoother block. If local maxima, of differential projection is significantly larger than that of global image then the block is marked as edge block.

In this approach low frequency AC_i co-efficient of each smoother and texture blocks are selected for hiding watermark (fingerprint and iris features). Iris feature W_i and fingerprint features W_f are sequentially embedded by modifying the amplitude of transform domain AC_i coefficients of selected DCT block. Modification is done based on comparison between original AC_i value and its estimated value $\overset{\Lambda}{\mathrm{AC}}_i$ as in (6). Where, η is a positive fraction which controls tradeoff between robustness and perceptibility. "w" in (6) represents watermark logo vector obtained from cascading of fingerprint feature "W_f" and iris feature "W_i":

$$\begin{aligned}
&\text{For } w(k) = 1\\
&\quad \text{if } \mathrm{AC}_i > \overset{\Lambda}{\mathrm{AC}}_i\\
&\qquad \text{then } \mathrm{AC}_i = (1+\eta)\mathrm{AC}_i\\
&\quad \text{else}\\
&\qquad\quad \mathrm{AC}_i = \overset{\Lambda}{\mathrm{AC}}_i + \eta \mathrm{AC}_i\\
&\text{for } w(k) = 0\\
&\quad \text{if } \mathrm{AC}_i < \overset{\Lambda}{\mathrm{AC}}_i\\
&\qquad \text{then } \mathrm{AC}_i = (1-\eta)\mathrm{AC}_i\\
&\quad \text{else}\\
&\qquad\quad \mathrm{AC}_i = \overset{\Lambda}{\mathrm{AC}}_i - \eta \mathrm{AC}_i.
\end{aligned} \tag{6}$$

Decoding of watermark bit requires estimated value $\overset{\Lambda}{\mathrm{AC}}_i$ of coefficient and original value AC_i to extract watermark bit. If $\mathrm{AC}_i > \overset{\Lambda}{\mathrm{AC}}_i$ then extracted bit is "1", otherwise extracted bit is "0".

4. Fusion Model

During the verification process feature vector (live template) $V_l = [F_l, I_l]$, where F_l is fingerprint feature vector and I_l is iris feature vector, is compared with extracted feature vectors. But extracted fingerprint features are in the form of binary numbers W_f', so it has to be first converted into numeric form F_t. Let the corresponding extracted iris feature be I_t. If similarity score for fingerprint system $S(F_l, F_t) > \theta_1$ and Euclidian distance for iris system $d(I_l, I_t) < \theta_2$ is satisfied than user is verified as genuine. The threshold values θ_1 and θ_2 are determined during the system validation process.

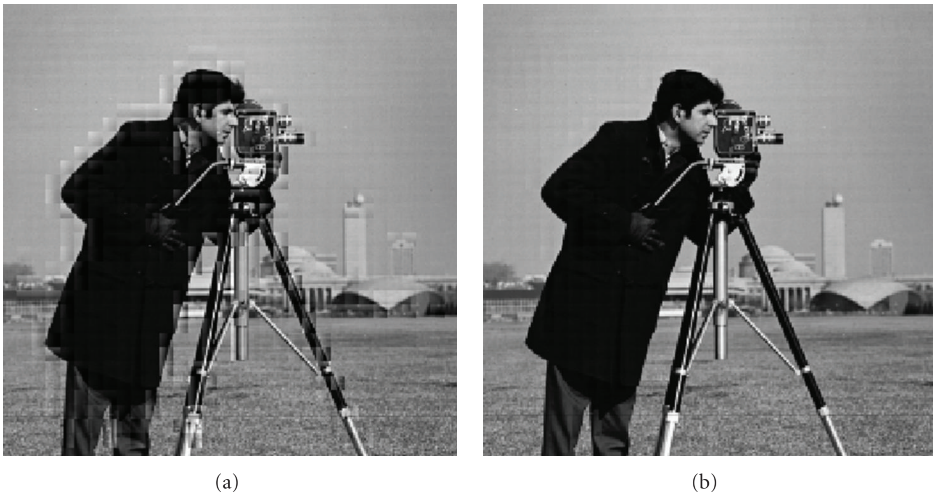


Figure 5: Watermarked Image (a) Considering all DCT blocks for embedding watermark. (b) Discarding edge blocks for embedding watermark.

Empirically it has been found that user is registered in database only if both systems have accepted the user.

For the security system generally low FAR is preferred. Fingerprint and Iris based system provides considerably low FAR. The fusion in our system is performed at decision level to further reduce the FAR. Simple Conjunction ("AND") rule can be used to combine the two systems F (fingerprint) and I (iris), that means a False Accept can only occur if both system F and I produce a False Accept. Let $P_F(\mathrm{FA})$ and $P_I(\mathrm{FA})$ is probability of False Accept using fingerprint and iris respectively and $P_F(\mathrm{FR})$ and $P_I(\mathrm{FR})$ is probability of False Reject using fingerprint and iris respectively. Thus the combined probability of a False Accept $P_C(\mathrm{FA})$ is the product of its two probabilities for the individual systems:

$$P_C(\mathrm{FA}) = P_F(\mathrm{FA})P_I(\mathrm{FA}). \tag{7}$$

But combined probability of a False Reject $P_C(\mathrm{FR})$ can be expressed as the complement of the probability that neither system F nor I produce a False Reject, which is higher than it is for either system alone:

$$\begin{aligned} P_C(\mathrm{FR}) &= \left(P_F(\mathrm{FR})' P_1(\mathrm{FR})'\right)' \\ &= 1 - [1 - P_F(\mathrm{FR})][1 - P_1(\mathrm{FR})] \\ &= P_F(\mathrm{FR}) + P_1(\mathrm{FR}) - P_F(\mathrm{FR})P_1(\mathrm{FR}). \end{aligned} \tag{8}$$

Equations (7) and (8) state that joint probability of false acceptance decreases (satisfies aim of security system) and joint probability of false rejection increases with simple conjunction rule. To improve FRR, proposed fusion technique aims to modify a decision threshold of weaker (fingerprint) system. This can be achieved by limiting the threshold of the fingerprint (weaker) system to a maximum value, obtained by projecting 50% of the cross-over error rate (point at which both error rate are equal) on to the FRR curve of the stronger (iris) system. This is achieved at the cost of degradation in combined FAR. Figure 6(b) is the magnified version of Figure 6(a). It shows the performance of individual as well as combined model in which point (1), (2), (3), and (4) indicate cross-over point of fingerprint system, iris system, after combining both systems with simple conjunction rule and with modified approach, respectively. Simple conjunction rule improves FAR but at the same time increases FRR than the individual systems. Cross-over point of fingerprint systems, iris system, with simple conjunction rule and with modified approach are 6.2%, 3.2%, 5.5%, and 1.2%, respectively.

FRR and FAR of modified approach are better for threshold range tagged by line segment (5)-(6) than the individual systems.

5. Experimental Evaluation

An ideal template protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system. This section extends the experimental results of DCT watermarking by computing the verification performance of fingerprint, iris, and multimodal biometrics for different attacks on the watermarked cover image. This experiment is performed to verify the integrity and robustness of the proposed biometric watermarking algorithm. Since the proposed watermarking algorithm uses fingerprint and iris, we use a decision level biometrics fusion algorithm. The multimodal biometric verification performance is computed using proposed conjunction rule based fusion algorithm. In order to explore the performance of the proposed watermarking algorithm, number of experiment are performed on different images of size 512 × 512, namely Texture, Cameraman, India logo and Bank logo (shown in Figure 7(a)).

To calculate the optimal weights, all objective functions in (4) are simplified by using above four images based on image content and repeated weights are selected to estimate

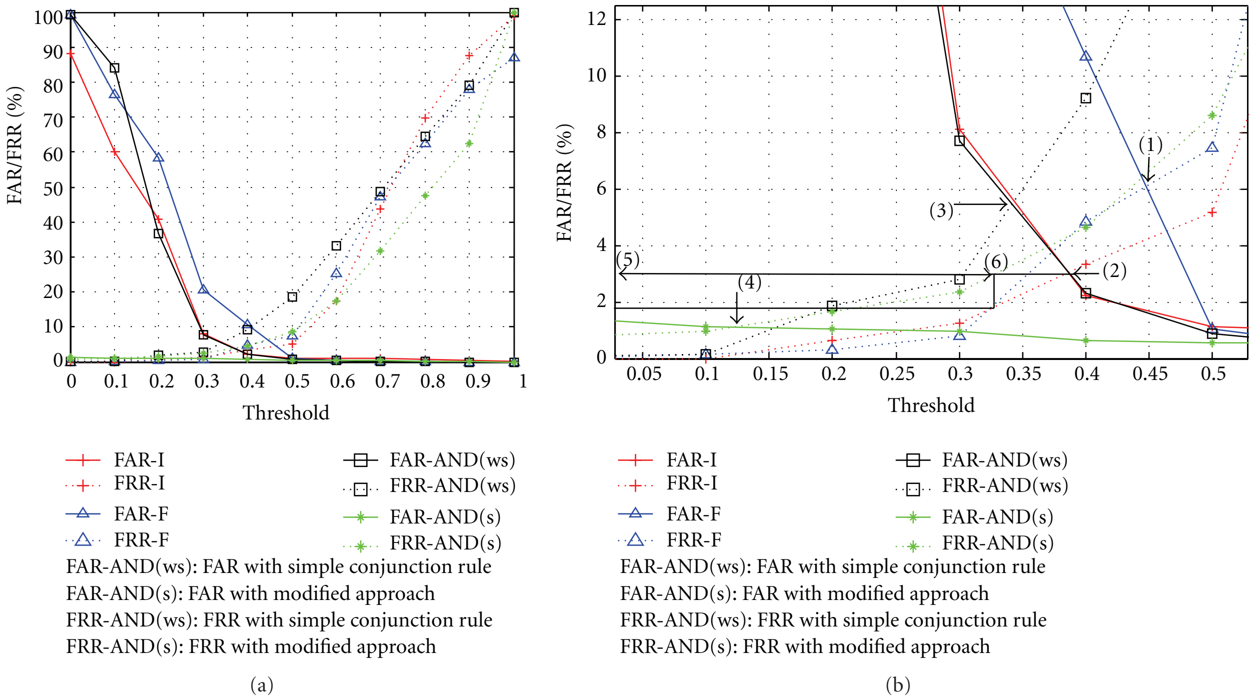
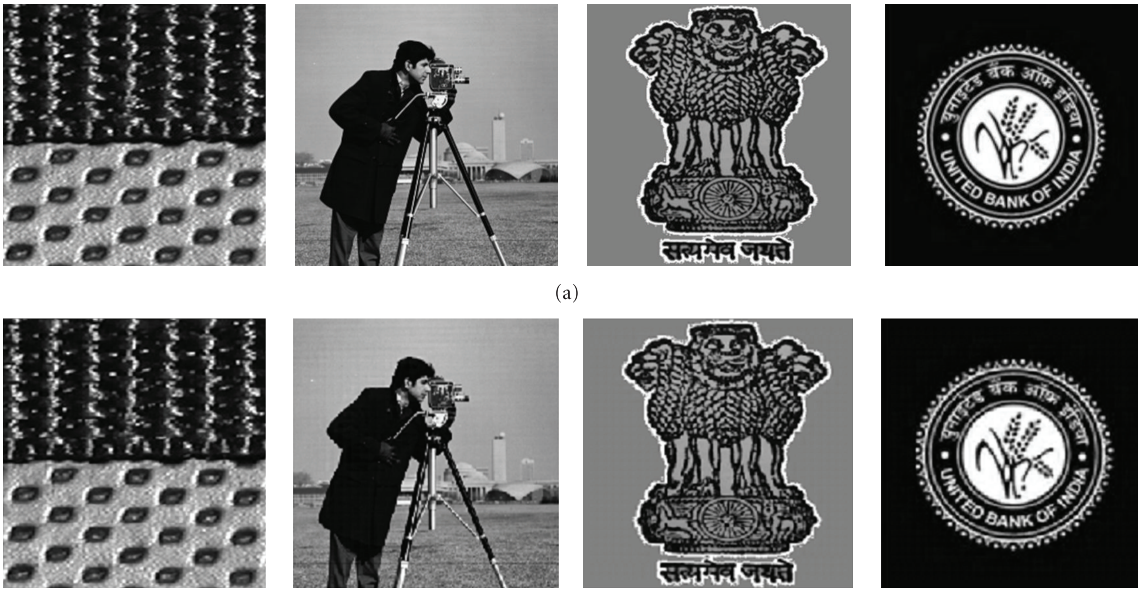


FIGURE 6: (a) Performance of individual and modified approach. (b) Magnified portion of part (a).


(a)

(b)

FIGURE 7: (a) Original test images. (b) Watermarked images.

TABLE 1: Optimal weights.

K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}
0.20	−0.20	0.19	−0.19	0.09	−0.18	0.09	0.03	0.03	−0.03	−0.03	0.06	−0.12	0.06

Table 2: Payload capacity for different benchmark images.

Images	Size (512 × 512) 3844 blocks Proposed method (Capacity = Blocks available after discarding Edge blocks ∗ bits per block)	Method in [26]	Method in [27]
Cameraman	13945 = 2789 ∗ 5	2205	441
Texture	12115 = 2423 ∗ 5	2205	441
India logo	10120 = 2024 ∗ 5	2205	441
Bank logo	9225 = 1845 ∗ 5	2205	441

the AC_i values. Table 1 shows the weights derived from the experiment.

In order to check the performance of fingerprint and iris system, DB3 database in FVC2004 [24] and CASIA database version-1 [25] is used, respectively. DB3 database comprises of 800 fingerprint images of size 300 × 480 pixels captured at a resolution of 512 dpi, from 100 fingers (eight impressions per finger). Individual minutiae data sets contained between 20 to 30 minutiae points, with an average of 25 minutiae points. CASIA database version-1 contains 756 gray scale eye images of 108 users with resolution of 320 × 280. Each user has 7 images captured in two sessions. Each image is represented by 348 bit after feature extraction. We have chosen 100 users from CASIA database and randomly correlate it with fingerprint data base to check improvement due to fusion approach.

It is found that a standalone fingerprint and iris system gives equal error rate (EER) at threshold values $\theta_1 = 0.45$ and $\theta_2 = 0.39$ respectively, as shown in Figure 6(b). In order to take advantage of fusion model, threshold point of fingerprint system is shifted between threshold ranges 0 to 0.32, indicated by line segment (5)-(6) in Figure 6(b). After combining both systems with $\theta_1 = 0.12$ and $\theta_2 = 0.39$ for fingerprint and iris system respectively, EER obtained is 1.2% (point (4) in Figure 6(b)).

The main advantage of biometric watermarking is that the fingerprint and iris image of the individual need not be stored in separate databases. Digital watermarking allows all related data to be stored and retrieved at the same time. The retrieval of the fingerprint and the iris feature helps in verification of an individual.

It is well known that blind watermarking extraction is more difficult than the watermark recovery with the aid of a reference image. Hence results should only compare within same group. We tried to compare the robustness of our proposed biometric watermarking method with the method suggested in [26, 27]. The algorithms have been reimplemented, closely following the description in Section 3 of this paper (five bits are embedded in each 8 × 8 block).

Pay load capacity is one of the comparative parameter. Pay load capacity of proposed approach for the size of 512 × 512 images is shown in Table 2.

Imperceptibility of watermark is measure by calculating Peak Signal to Noise Ratio (PSNR) value as in

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{255}{\mathrm{MSE}}\right), \text{ where}$$
$$\mathrm{MSE} = \left\{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[I(i,j) - I'(i,j)\right]^2\right\}. \tag{9}$$

Here, $I(i,j)$ and $I'(i,j)$ are the pixel values in original host image and watermarked image, respectively, and $M \times N$ is the size of an image. The PSNR value of proposed method is observed higher than the method in [26, 27] as stated in Table 3. In [26] watermark is embedded in low frequency AC_i coefficients of center block of all 3 × 3 non overlapping neighborhood blocks without discarding edge block in image. While in [27] watermark is embedded into DC coefficient, which decides the block average. So, even a small variation in DC coefficients only effects intensity of all the pixels within the block and hence results in low PSNR value.

The electronic transmission of cover image over the communication channel introduces degradations in the image data. For example, images are compressed when transmitting large image files over low bandwidth channel; a median filter is used to smooth the image; and during transmission some noise is introduced. These effects on the watermarked image are studied by using various image processing attacks such as JPEG compression, median filtering with 3 × 3 filter mask, and the addition of Gaussian noise. To check the robustness against Image compression, the watermarked image is tested with JPEG compression attack with different quality factors and results are as shown in Table 3. In proposed algorithm, watermark extraction Bit Error Rate (BER) is calculated as

$$\mathrm{BER} = \frac{\text{number of error bits}}{\text{total number of embedded bits}}. \tag{10}$$

It can be clearly seen that larger Q brings robustness, and higher extraction accuracy of bits can guarantee recognition performance to a greater extent. Table 4 shows the extraction error rate for median filtering attacked watermarked image with mask size of 3 × 3.

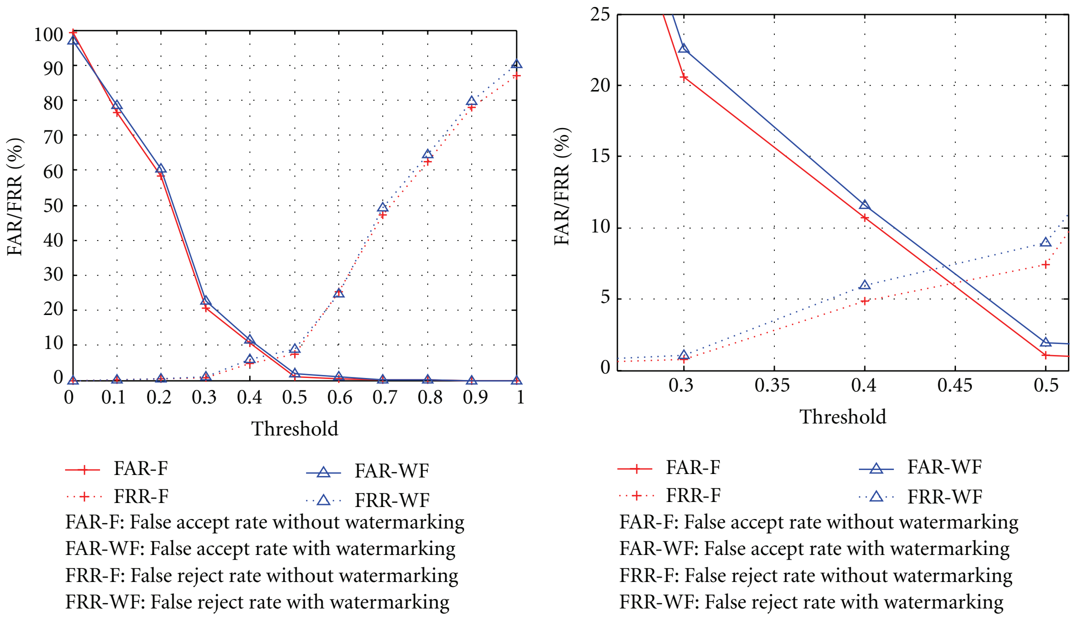
Table 5 shows results for Gaussian filtering attacks. In all cases our method appears better than the methods in [26, 27]. Proposed technique is also robust against various signal processing operations like enhancement (gamma = 0.7) and rescaling (512-256-512). For both mentioned operation results are shown in Table 6.

Receiver Operating Characteristic (ROC) curve of standalone systems are shown in Figures 8 and 9, in which Equal Error Rate (EER) obtained for fingerprint system is 6.2% and for iris system 3.2%. It is clearly seen from ROC curve that FAR and FRR of the systems without watermarking is almost same as that with watermarking.

Table 6 shows the EER of fingerprint and iris system for different clauses. Results illustrate that proposed watermarking algorithm is robust against various template manipulation causes (intentional, unintentional). Small variation in retrieved template is survived by strong matching algorithm.

Table 3: Watermark Extraction Bit Error Rate due to JPEG Compression.

Image	Imperceptibility measurement PSNR			Quality Factor	Comp-ression	Watermark extraction BER (%)		
	Proposed method	Method in [26]	Method in [27]	(Q)	(BPP)	Propose method	Method in [26]	Method in [27]
Texture	37.2025	36.7493	35.7245	90	2.8527	0	0.39	0.93
				80	2.1015	0	0.39	0.93
				75	1.8981	0	0.39	0.93
Cameraman	38.2340	38.3245	34.8972	90	2.1323	0	0.56	2.47
				80	1.4608	0	0.56	2.47
				75	1.2816	0.1	0.56	2.47
India logo	48.7235	46.2068	36.8863	90	2.5463	0	0.39	0.93
				80	1.8955	0	0.39	0.93
				75	1.7143	0	0.39	0.93
Bank logo	42.0910	41.8456	39.6230	90	1.9196	0	0.73	1.35
				80	1.4365	0	0.73	1.35
				75	1.3010	0.5	0.73	1.35



(a)

(b)

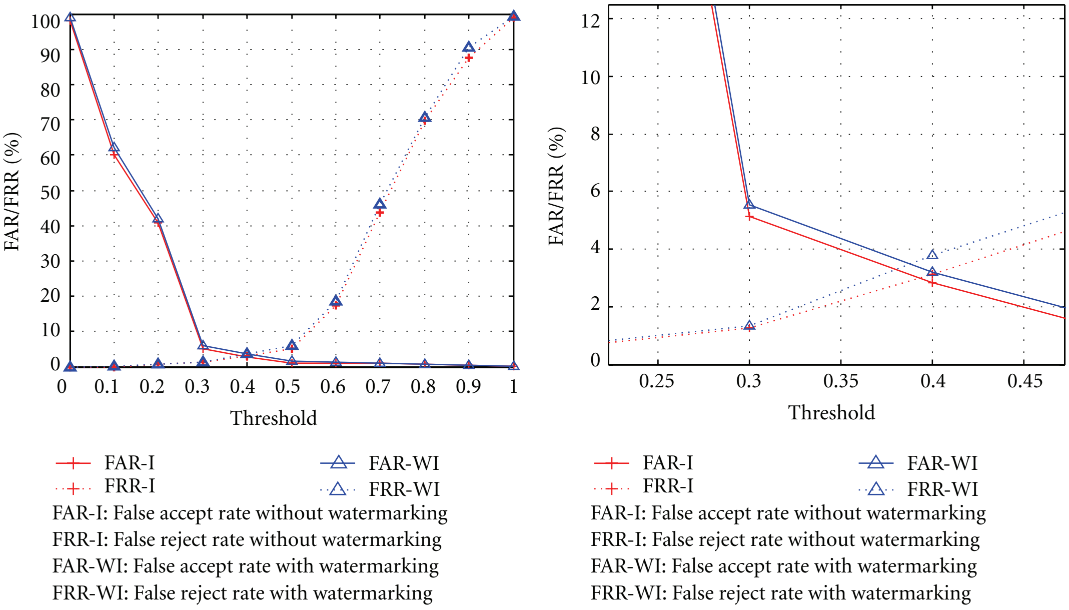
Figure 8: (a) ROC of fingerprint system and (b) magnified area of (a) indicating EER point with and without watermarking.

Table 4: Watermark Extraction Bit Error Rate due to median filtering (3 × 3).

Image	Watermark extraction BER (%)		
	Proposed method	Method in [26]	Method in [27]
Texture	0	0.48	1.33
cameraman	0.02	0.57	2.25
India logo	0.08	0.53	1.45
Bank logo	0.01	0.61	3.97

Table 5: Watermark Extraction Error Rate due to Gaussian filtering (7 × 7) attack.

Image	Watermark extraction BER (%)		
	Proposed method	Method in [26]	Method in [27]
Texture	0.16	Destroyed	Destroyed
cameraman	0.12	Destroyed	Destroyed
India logo	0.14	Destroyed	Destroyed
Bank logo	0.13	Destroyed	Destroyed



(a)

(b)

Figure 9: (a) ROC of iris system (b) magnified area of (a) indicating EER point with and without watermarking.

Table 6: EER of combine model in different clauses.

Clauses	EER (%)	
	Fingerprint	Iris
Without watermarking	6.20	3.2
With watermarking		
Without attacks	6.40	3.6
Host image attacked by compression (50%)	6.49	3.6
Median filtering (3 × 3)	6.45	3.64
Gaussian filtering (7 × 7)	6.69	3.70
Contrast adjustment (Gamma = 0.7)	6.4	3.61
Scaling (512-256-512)	6.4	3.6

6. Conclusion

Challenge of the public system like e-Voting, e-Passport, and e-commerce endorsed with biometrically authentication includes massive number of users, demands high discrimination ability and secured transmission under varying channel conditions. In order to achieve first demand we propose multi-biometric system with fusion of decision using conjunction rule. Overall FRR of the combined model is improved by conditionally limiting the threshold of the fingerprint system to a maximum value, obtained by projecting 50% of the cross-over error rate on to the FRR curve of the iris system. This is achieved at the cost of degradation in combined FAR. Furthermore, to achieve secured transmission, biometric feature embedded inside any host image by blind watermarking algorithm is essential. We proposed spatial and spectral feature based block discrimination and coefficient estimation approach. The payload capacity we obtained is far better than state of art algorithms and robust against various signal processing and channel attacks.

References

[1] A. Jain, S. Pankanti, and R. Bolle, *BIOMETRICS: Personal Identification in Networked Society*, Kluwer, New York, NY, USA, 1999.

[2] S. Ribaric, D. Ribaric, and N. Pavesic, “Multimodal biometric user-identification system for network-based applications,” *IEE Proceedings on Vision, Image & Signal Processing*, vol. 150, no. 6, pp. 409–416, 2003.

[3] B. Schneier, “The uses and abuses of biometrics,” *Communications of the ACM*, vol. 42, no. 8, p. 136, 1999.

[4] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2003.

[5] U. Uludag and A. K. Jain, “Attacks on biometric systems: a case study in fingerprints,” in *Proceedings of the Security, Seganography and Watermarking of Multimedia Contents VI*, vol. 5306 of *Proceedings SPIE*, pp. 622–633, San Jose, Calif, USA, January 2004.

[6] N. K. Ratha, J. H. Connell, and R. M. Bolle:, “An analysis of minutiae matching strength,” in *Proceedings of the 3rd International Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 223–228, June 2001.

[7] V. Claus and S. Ralf, “Approaches to biometric watermarks for owner authentication,” in *Proceedings of the Security and Watermarking of Multimedia Contents III*, vol. 43 of *Proceedings of SPIE*, no. 14, pp. 209–219, January 2001.

[8] A. K. Jain and U. Uludag, “Hiding fingerprint minutiae in images,” in *Proceedings of 3rd Workshop on Automatic Identification Advanced Technologies (AutoID ’02)*, pp. 97–102, 2002.

[9] A. K. Jain and U. Uludag, “Hiding biometric data,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 11, pp. 1494–1498, 2003.

[10] M. Vatsa, R. Singh, and A. Noore, “Improving biometric recognition accuracy and robustness using DWT and SVM watermarking,” *IEICE Electronics Express*, vol. 2, no. 12, pp. 362–367, 2005.

[11] M. Vatsa, R. Singh, A. Noore, M. M. Houck, and K. Morris, “Robust biometric image watermarking for fingerprint and face template protection,” *IEICE Electronics Express*, vol. 3, no. 2, pp. 23–28, 2006.

[12] N. K. Ratha, J. H. Connell, and R. M. Bolle, “Secure data hiding in wavelet compressed fingerprint images,” in *International Multimedia Conference*, Proceedings of the ACM Workshop on Multimedia, pp. 127–130, 2000.

[13] A. K. Jain, U. Uludag, and R. L. Hsu, “Hiding a face in a fingerprint image,” *Proceedings of International Conference on Pattern Recognition*, vol. 3, pp. 756–759, 2002.

[14] A. Noore, R. Singh, M. Vatsa, and M. M. Houck, “Enhancing security of fingerprints through contextual biometric watermarking,” *Forensic Science International*, vol. 169, no. 2-3, pp. 188–194, 2007.

[15] N. Komninos and T. Dimitriou, “Protecting biometric templates with image watermarking technique,” in *International Conference on Biometrics*, vol. 4642 of *Lecture Notes in Computer Science*, pp. 114–123, 2007.

[16] H. Al-Assam, H. Sellahewa, and S. Jassim, “A lightweight approach for biometric template protection,” in *Proceedings of the Mobile Multimedia/Image Processing, Security, and Applications*, vol. 7351 of *Proceedings of SPIE*, April 2009.

[17] A. Nagar, K. Nandakumar, and A. K. Jain, “Biometric template transformation: a security analysis,” in *The International Society for Optical Engineering*, vol. 7541 of *Proceedings of SPIE*, January 2010.

[18] M. Paunwala and S. Patnaik, “Robust biometric watermarking using image intrinsic local property for e-database applications,” in *IASTED International Conference on Computer Vision*, pp. 240–247, Vancouver, Canada, June 2011.

[19] H. M. Patel, C. K. Modi, M. Paunwala, and S. Patnaik, “Human identification by partial iris segmentation using pupil circle growing based on binary Integrated edge intensity curve,” in *Proceedings of the IEEE International Conference on Communication Systems and Network Technologies (CSNT ’11)*, pp. 333–338, June 2011.

[20] J. G. Daugman, “High confidence visual recognition of persons by a test of statistical independence,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148–1161, 1993.

[21] T. W. Ng, T. L. Tay, and S. W. Khor, “Iris recognition using rapid Haar wavelet decomposition,” in *Proceedings of the 2nd International Conference on Signal Processing Systems (ICSPS ’10)*, pp. V1820–V1823, July 2010.

[22] J. Fridric, “Applications of data hiding in digital images,” in *Tutorial for the International Symposium on Signal Processing and Its Applications (IPACS ’98)*, Melbourne, Australia, November 1998.

[23] Hiller and Lieberman, *Introduction To Operations Research*, Tata McGraw-Hill, 7th edition, 2001.

[24] http://bias.csr.unibo.it/fvc2004/download.asp.

[25] http://biometrics.idealtest.org/findTotalDbByMode.do?mode=Iris.

[26] Y. Wang and A. Pearmain, “Blind image data hiding based on self reference,” *Pattern Recognition Letters*, vol. 25, no. 15, pp. 1681–1689, 2004.

[27] Y. Choi and I. Aizawa, “Digital watermarking using inter block correlation,” in *Proceedings of the International Conference on Image Processing*, vol. 2, pp. 216–220, October 1999.

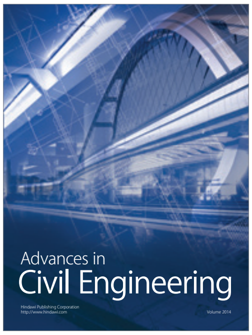
Journal of
Engineering

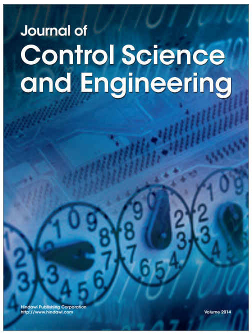
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

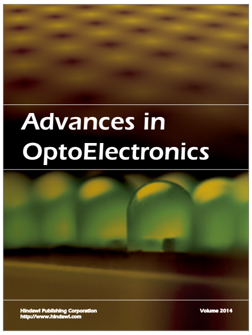
International Journal of
Distributed
Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

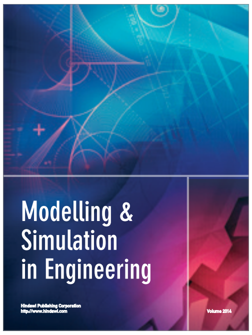
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

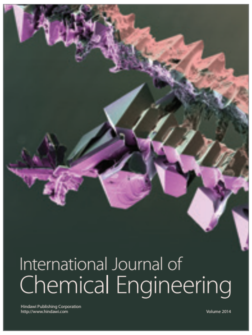

Advances in
OptoElectronics

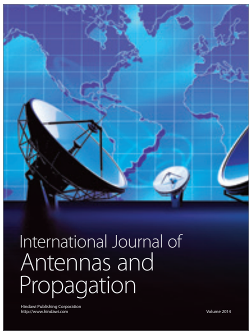
VLSI Design

International Journal of
Navigation and
Observation

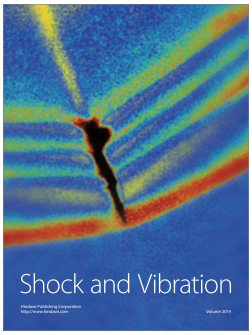

Modelling &
Simulation
in Engineering

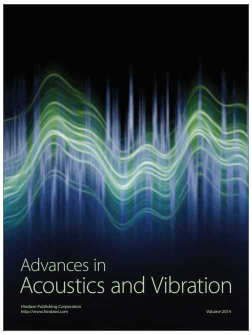
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration