Multimed Tools Appl (2017) 76:3871–3897
DOI 10.1007/s11042-016-4048-0

A multimodal biometric watermarking system for digital images in redundant discrete wavelet transform

Priyanka Singh[1] · Balasubramanian Raman[1] · Partha Pratim Roy[1]

Received: 30 April 2016 / Revised: 20 September 2016 / Accepted: 5 October 2016 /
Published online: 9 November 2016

Abstract The traditional watermarking algorithms prove the rightful ownership via embedding of independent watermarks like copyright logos, random noise sequences, text etc into the cover images. Coupling biometrics with watermarking evolved as new and secure approach as it embeds user specific biometric traits and thus, narrows down the vulnerability to impostor attacks. A multimodal biometric watermarking system has been proposed in this paper in the redundant discrete wavelet transform(RDWT). Two biometric traits of the user i.e. the iris and facial features are embedded independently into the sub-bands of the RDWT of cover image taking advantage of its translation invariant property and sufficient embedding capacity. The ownership verification accuracy of the proposed system is tested based on the individual biometric traits as well as the fused trait. The accuracy was enhanced while using the fused score for evaluation. The security of the scheme is strengthened with usage of non-linear chaotic maps, randomization via Hessenberg decomposition, Arnold scrambling and multiple secret keys. The robustness of the scheme has been tested against various attacks and the verification accuracy evaluated based on false acceptance rate, false rejection rate, area under curve and equal error rate to validate the efficacy of the proposed scheme.

Keywords Rightful ownership · Multimodal biometric systems · Redundant discrete wavelet transform(RDWT) · Impostor attacks · Non-linear chaotic maps · Hessenberg decomposition · Arnold scrambling · False acceptance rate · False rejection rate · Area under curve · Equal error rate

✉ Priyanka Singh
priyankiitr@iitr.ac.in

Balasubramanian Raman
balarfma@iitr.ac.in

Partha Pratim Roy
proy.fcs@iitr.ac.in

[1] Indian Institute of Technology Roorkee, Roorkee, India

1 Introduction

The unprecedented growth of technology has connected everbody all over the globe and allowed easy sharing of multimedia content in no restriction of time and access. However, the unlimited access has posed new threats to these multimedia data where the illegitimate individuals can intercept the data in between transmission and misuse it. Various techniques like encryption, steganography,cryptography, watermarking etc are being employed to provide authenticated systems. However, recently the biometric techniques are coupled with these aforementioned approaches to enhance the ability of distinguishing authentic users from non-authentic ones. The user specific biometric traits based on behavioral or physiological characteristics of an individual helps to build more robust systems. While designing a biometric based authentication scheme, various important factors like verification accuracy rate, security, costing, robustness against attacks, computational time and scalability of the system must be considered [14]. Some of the most efficient approaches for securing these biometric systems are encryption [9, 27, 29] or watermarking where a secret information is embedded without deteriorating the cover image [11, 14, 15, 24, 30]. Various other hybrid schemes like combining encryption with biometrics [1], cryptographic biometric systems [2], steganography or watermarking biometric trait [3, 4] have already been proposed in the literature.

The major drawback of the traditional watermarking schemes is the lack of unique watermark for the rightful owner. They use logos, images, text or random noise sequences as watermarks for embedding in the cover images. These watermarks could be easily tampered or imitated to exploit the rightful ownership or destroy the authentication results creating situation of ambiguity. Thus, user specific biometric traits based or the physical or behavioral characteristics of a person like fingerprint, iris detection, face watermark, gait etc could be used as watermarks. Embedding of such user dependent traits will definitely serve as unique watermarks for authorization and provide requisite level of security to such watermarking systems. For a person claiming as rightful owner, this watermark is extracted from the watermarked cover image and compared with the other samples kept in the database. If a match is found, then it proves the rightful ownership else he is not the legitimate owner.

Many watermarking schemes coupled with biometric information have already been proposed in the literature. Most of them mainly target embedding of one biometric trait into another biometric information, so that the rightful ownership of the biometric samples stored in the databases could be proved [5, 6]. Other schemes aim at embedding of user specific biometric traits in normal images i.e. data unrelated to the user whereby after extraction, the rightful ownership can be claimed. One such watermarking algorithm based on the hybrid domain of DWT-SVD used fingerprint as watermark data. The minutiae co-ordinates matrix was embedded after SVD decomposition into the cover image [7]. Another watermarking scheme embedded binary iris codes into the normal cover images whereby the similarity was computed between the extracted watermark and other samples of user claiming ownership to build the identity of the owner [8]. Other methods aim at exploiting the multimodality where the basic idea is to embed one biometric trait into another biometric trait [10, 12, 13].

A watermarking scheme proposed in the domain of DWT, DCT and LPC (Linear Predictive Coding) embedded multiple features of different biometric traits like face, speech signature into the cover data [10]. The similarity between each extracted trait and the other original samples kept in the database was evaluated based on correlation values. However, no fusion was done to combine the individual similarity scores of the trait. Another watermarking scheme that used fingerprint and iris features to combine into one and obtain a

fused watermark was proposed in [12]. This fused watermark was then inserted into the cover data. For verifying the ownership, the fused watermark was extracted and thereafter separated into two individual watermarks. The similarity comparisons were then performed between these individual watermarks and the other original samples stored for claiming the rightful ownership. Another watermarking scheme performed in the DCT domain modified the amplitude of the selected coefficients for embedding of two biometric traits. The fusion of the traits was done at the decision level to proceed further for the authorization purposes [13]. A multimodal biometric watermarking system has been proposed in the present paper. Based on the redundant wavelet transform, the proposed watermarking algorithm embeds two watermarks i.e. iris codes and the face features extracted from the face template into a chosen sub band which is randomized using the Hessenberg decomposition. The iris watermark is scrambled using Arnold chaotic map prior to embedding so as to enhance the security of the scheme. Further, the face features are embedded reversibly based on a secret key without deteriorating the quality of the watermarked image. The ownership verification is performed based on the fused biometric score level. Simulation studies are conducted to show the effect of watermarking on the verification accuracy of the proposed system. Also, the authentication evaluation based on the individual biometric traits as well as the fused score at the decision level are presented to assess its affect on the verification accuracy.

The rest of the paper is organized as follows: In Section 2, some preliminaries are given, Section 3 discusses the proposed multimodal biometric watermarking approach. Experimental results along with analysis are presented in Section 4 and finally, conclusions are stated in Section 5.

2 Preliminaries

A brief overview of the concepts used in the proposed approach is given as follows:

2.1 Redundant wavelet transform (RWT)

Though wavelet transform emerged as one of the very powerful tools for varied applications of image processing but it proved not vey optimal choice for other applications involving analysis of signals, filtering, detection, deconvolution etc. The reconstructed image from the altered wavelet coefficients contained many visual artifacts. This mainly arose owing to lack of the translation invariant property in wavelet transform.

The redundant wavelet transform (RWT) evolved as a discrete estimation of the continuous wavelet transform. Although, history has roots that RWT was proposed independently via different names like the overcomplete WT (OWT) [18], discrete wavelet frames (DWFs)[20], the shift-invariant WT (SIWT) [19], the undecimated WT (UWT)[17], and algorithme trous [16]. These names were given due to the fact that the downsampling was removed which resulted in shift invariance property of RWT with a fixed spatial sampling rate across the whole scale. Thus, resulting in size of the sub-bands same as the size of the input signal. Mathematically, RWT can be defined in terms of scaling $h \epsilon l^2(Z)$ and wavefilters $g \epsilon l^2(Z)$ of an underlying orthonormal wavelet transform. To maintain the multiresolution property at each scale, these filters should be adjusted accordingly. The upsampling can be defined as follows:

$$x[k] \uparrow 2 = \begin{cases} x[k/2], & \text{if } k \; is \; even \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

At scale $j+1$, the scaling and wavelet filters can be as:

$$h_{j+1}[k] = h_j[k] \uparrow 2, g_{j+1}[k] = g_j[k] \uparrow 2 \tag{2}$$

where $h_0[k] = h[k]$ and $g_0[k] = g[k]$. Recursive implementation with the filter bank operations will result in RWT of any signal $x \epsilon l^2(Z)$ as:

$$c_{j+1}[k] = h_j[-k] \times c_j[k], d_{j+1}[k] = g_j[-k] \times c_j[k] \tag{3}$$

where $c_0 = x$ and $j = 0, 1 \ldots J-1$. RWT at J scale is collection of sub bands result of filtering operations: $X^J = RWT_J[x] = [c_J d_J d_{J-1} \ldots d_1]$ such that

$$\|X^j\|^2 = \|c_J\|^2 + \sum_{j=1}^{J} \|d_j\|^2 \tag{4}$$

2.2 Singular value decomposition

Singular value decomposition is one of the efficient ways for factorization of a square or rectangular matrix to bring up the very structure of the matrix [22]. It is very popular in image processing as it has many advantages like the singular values are very stable in nature, get very less affected by the general image processing distortions and represent the algebraic properties of the image. Singular value decomposition of a real (complex) matrix X of order $m \times n$ can be represented as:

$$X = USV^T \tag{5}$$

where $S = diag(\sigma_1, \sigma_1, \ldots \sigma_r)$ and U and V are orthogonal (unitary)matrices and signify the left and right singular values. σ_i represent the singular values of the matrix and $r = min(m, n)$ is the rank of the matrix satisfying

$$\sigma_1 \geq \sigma_2 \geq \sigma_3 \ldots \geq \sigma_r \tag{6}$$

2.3 Non-linear chaotic map

To enhance the randomness and increase security aspect of the schemes, chaotic systems are often used. It possesses many useful properties like initial parameter sensitivity, non-periodicity, unpredictability etc. which make these maps as the stochastic signal generators [21]. We have employed piecewise non-linear map here to generate random sequences. Mathematically, it can be defined as follows:

$F : I \rightarrow I$ where $I = [0, 1]$

$$F(x_{k+1}) = \begin{cases} \left(\frac{1}{I_{i+1}-I_i} + a_i\right)(x_k - a_i) - \frac{a_i}{I_{i+1}-I_i}(x_k - a_i)^2 & if \;\; x_k \epsilon [I_i, I_{i+1}) \\ 0 & if \;\; x_k = 0.5 \\ F(x_k - 0.05) & if \;\; x_k \epsilon (0.5, 1] \end{cases} \tag{7}$$

Where $x_k \epsilon (0, 1]$ and I_i is the sub interval such that ,$0 = I_0 < I_1 < \ldots I_i \ldots I_{n+1} = 0.5$. The parameter $a_i \epsilon (-1, 0) \bigcup (0, 1)$ is the tune sequence in the i^{th} interval such that

$$\sum_{i=0}^{n-1} (I_{i+1} - I_i) a_i = 0 \tag{8}$$

The important properties of the above map are as follows:

- The iteration system obtained by (7) i.e. $x_{k+1} = F(x_k)$ is chaotic for all $x_k \epsilon [0, 1]$
- The sequence $(x_k)_{k=1}^{\infty}$ is Ergodic in [0,1] having the uniform probability distribution function $\rho(x) = 1$, which further shows the uniformity of the map, i.e. the probability of each value in [0,1] is equal to be selected.
- The sequence $(x_k)_{k=1}^{\infty}$ has δ-like autocorrelation function given as

$$R_F(r) = \lim_{j\to\infty} \frac{1}{j} \frac{\sum_{k=1}^{j} x_k x_{k+r}}{\sum_{k=1}^{j} x_k^2}, x \geq 0$$

2.4 Hessenberg decomposition

In Hessenberg decomposition [22], any matrix A can be factorized via orthogonal similarity transformations into the form as follows:

$$A = QHQ^T \tag{9}$$

where Q is an orthogonal matrix whereas H is an upper Hessenberg matrix, implies $H = [h_{ij} : h_{ij} = 0 \; whenever \; i > j + 1]$. This decomposition usually involves computation of Householder matrices. A Householder matrix P is the orthogonal matrix of the form:

$$P = \frac{I_n - 2uu^T}{u^T u} \tag{10}$$

where u is a non-zero vector in R_n and I_n is the $n \times n$ identity matrix.
The main reason of using these matrices is the ability of introducing zeros. For instance, suppose $x = (x_1, x_2, \ldots, x_n)$ is a non-zero vector in R_n and u is defined as:

$$u = x + sign(x_1)||x||_2 e_1 \tag{11}$$

where $sign(x_1) = \frac{x_1}{|x_1|}$ and e_1 is the first column of I_n. It then follows:

$$P_x = -sign(x_1)||x||_2 e_1 \tag{12}$$

i.e. a vector having zeros in all but its first component. There are $n - 2$ steps in the overall procedure when A is of size $n \times n$ which further proves the ability of introducing zeros. At the beginning of k^{th} step orthogonal matrices $P_1, P_2, \ldots, P_{k-1}$ have been expressed as:

$$A_{k-1} = (P_1, P_2 \ldots P_{k-1})^T A (P_1, P_2 \ldots P_{k-1}) \tag{13}$$

having the form:

$$A_{k-1} = \begin{bmatrix} H_{11}^{(k-1)} & H_{12}^{(k-1)} & H_{13}^{(k-1)} \\ 0 & b_{22}^{k-1} & H_{23}^{(k-1)} \\ 0 & H_{32}^{(k-1)} & H_{33}^{(k-1)} \end{bmatrix} \tag{14}$$

where $H_{11}^{(k1)}$ is Hessenberg matrix. Let $\tilde{P}_k = \frac{I_{n-k}-2u^k(u^k)^T}{(u^k)^T u^k}$ be a Householder matrix with the property that $\tilde{P}_k b^{k-1}$ has zeros in the last $n-j-1$ components which further follows that the matrix $P_k = diag(I_{n-k}, \tilde{P}_k)$ is orthogonal and A_k is given as:

$$A_k = P_k^T A_{k-1} P_k = (P_1 P_2 \dots P_{k-1} P_k)^T A (P_1 P_2 \dots P_{k-1} P_k) \tag{15}$$

$$A_k = \begin{bmatrix} H_{11}^{(k-1)} & H_{12}^{(k-1)} & (H_{13}^{(k-1)})^T \tilde{P}_k \\ 0 & b_{22}^{k-1} & (H_{23}^{(k-1)})^T \tilde{P}_k \\ 0 & \tilde{P}_k (H_{32}^{(k-1)})^T & \tilde{P}_k (H_{33}^{(k-1)})^T \tilde{P}_k \end{bmatrix} \tag{16}$$

where A_k is Hessenberg matrix. Since, we need $n-2$ steps in the overall procedure, the above (15) can be rewritten as:

$$H = Q^T A Q \rightarrow A = Q^T H Q \tag{17}$$

where $H = A_{n-2}$ and $Q = P_1 P_2 \dots P_{n-3} P_{n-2}$

3 The proposed methodology

The proposed scheme is based on the multimodal biometric watermarking system. It fuses the two biometric traits of iris codes and facial features into one and uses it as the decision criteria for distinguishing between genuine and impostor attempts for a claiming owner. The two watermarks i.e. iris codes and facial features are pre-processed prior to the actual embedding into the cover image. The scheme consists of four main phases: Pre-processing of biometric data before embedding, watermark embedding, watermark extraction and authentication. The details of each phase is as follows:

3.1 Pre-processing of biometric data before embedding

Two biometric watermarks: Iris as first grayscale watermark (W_1) and face features as the second binary watermark (W_2) are used in the proposed scheme. The iris images from the database are resized according to the size of the cover images and then scrambled using the arnold transformation based on a secret key to deliver it unreadable depending upon the period of the iris image. This obtained scrambled iris watermark is thus ready to be inserted. The second binary watermark is obtained from the face database images using the feature extraction algorithm as in [26]. The algorithm extracts the features based on the center symmetric local binary pattern(CSLBP) and gray level co-occurrence matrix (GLCM). The local features are captured via CSLBP and thereafter using the GLCM, the co-occurrence of the pixel intensities are encountered with. It serves as a better way of obtaining local feature descriptors for an image instead of histograms where only frequency information is captured. The feature vectors thus obtained are arranged in a matrix and operated upon by reversible XOR operation with the halftone version of the watermarked image. This halftone version is obtained via error diffusion technique and generates a secret key K_{W_2} that is used in the extraction phase.

3.2 Watermark embedding

The embedding phase involves embedding of two watermarks: grayscale and binary in hierarchial order. The embedding is done in such a way so that embedding of one watermark

doesn't disturb the other one. The detailed methodology is depicted in Fig. 1 and described in detail as follows:

1. Perform redundant wavelet transform on the cover image C upto L-level, denoted as follows: C_{Ψ}^{Γ}, where $\Psi \epsilon [1, L]$, $\Gamma \epsilon \{A, H, V, D\}$

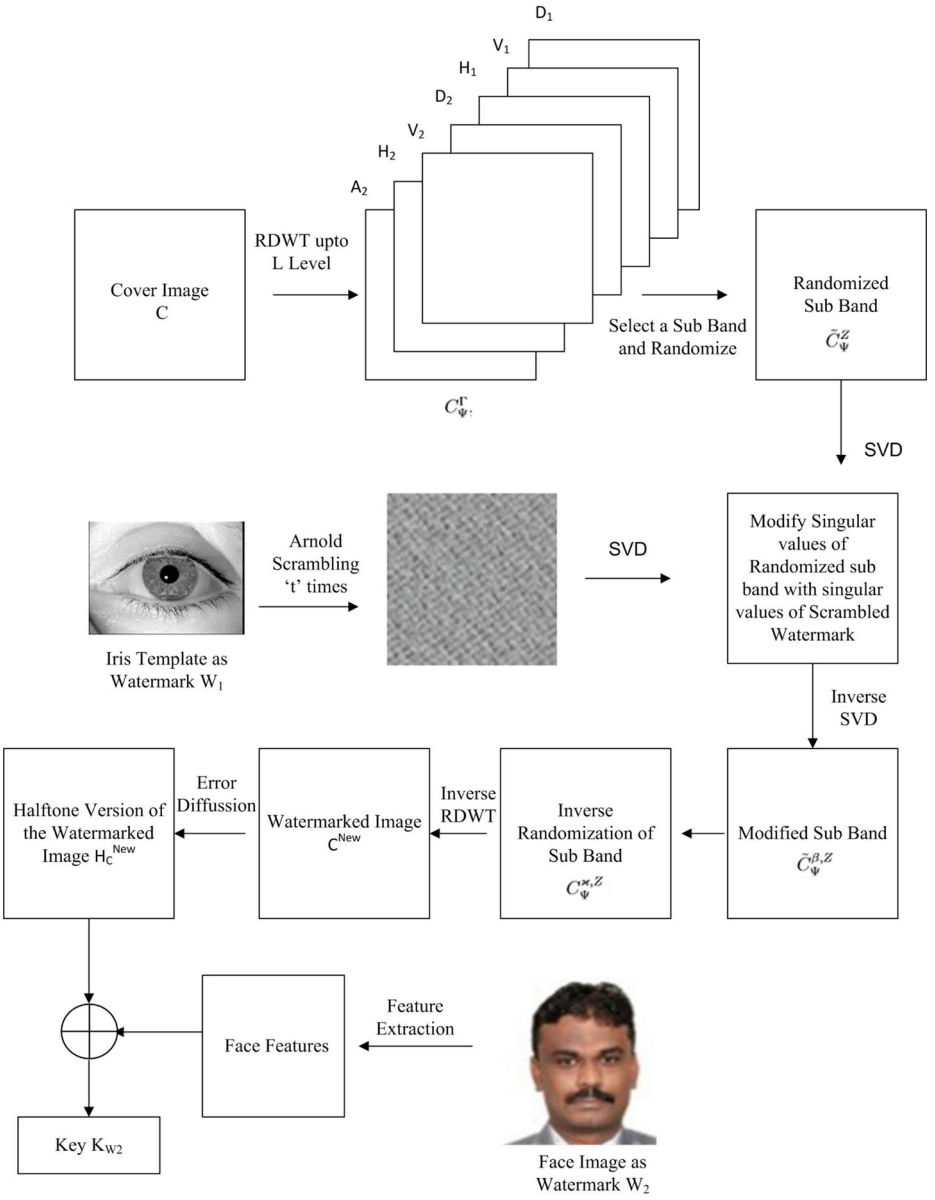


Fig. 1 Embedding process of proposed scheme

2. Selection and randomization of a sub-band: A sub band is selected from the RWT decomposition and randomized prior to actual embedding of the grayscale watermark. The details are as follows:
   (a) Obtain two random sequences via non-linear chaotic maps using secret keys k_1 and k_2 of length $M \times M$ and $N \times N$ respectively.
   (b) Rearrange the two obtained sequences to form two arrays represented by M_1 and M_2 of same length $M \times M$ and $N \times N$ respectively.
   (c) Perform Hessenberg decomposition on the arrays M_1 and M_2 to obtain two orthogonal matrices R_1 and R_2.
   (d) Select a sub band C_Ψ^Z and randomize it via R_1 and R_2 as follows:
$$\tilde{C}_\Psi^Z = R_1 C_\Psi^Z R_2 \tag{18}$$
3. The grayscale watermark W_1 is scrambled using Arnold cat map Y times to obtain W_1^s which is a secure version as it contains sensitive information of the owner.
4. Embed the scrambled watermark W_1^s as follows:
   (a) Perform SVD on both correlated watermark W_1^c and chosen sub band $\tilde{C}_\Psi^Z$ for embedding as follows:
$$\tilde{C}_\Psi^Z = U_{\tilde{C}_\Psi^Z} S_{\tilde{C}_\Psi^Z} V_{\tilde{C}_\Psi^Z}^T \tag{19}$$
$$W_1^c = U_{W_1^c} S_{W_1^c} V_{W_1^c}^T \tag{20}$$
   (b) Modify the singular values of the sub-band with the singular values of the watermark as follows:
$$S'_{\tilde{C}_\Psi^Z} = S_{\tilde{C}_\Psi^Z} + \alpha S_{W_1^c} \tag{21}$$
   where α gives the watermark strength.
   (c) Perform inverse SVD to construct modified sub-band
$$\tilde{C}_\Psi^{\beta,Z} = U_{\tilde{C}_\Psi^Z} S'_{\tilde{C}_\Psi^Z} V_{\tilde{C}_\Psi^Z}^T \tag{22}$$
5. Perform inverse randomization of the sub band as follows:
$$C_\Psi^Z = inv(R_1)\tilde{C}_\Psi^{\beta,Z} inv(R_2) \tag{23}$$
6. Inverse redundant wavelet transform upto L level is applied to obtain the watermarked image C^{New}.
7. Embedding binary watermark: The binary image W_2 is embedded as follows:
   (a) Obtain a halftone version $H_{C^{New}}$ of the watermarked image using error diffusion method.
   (b) Perform exclusive-OR operation bitwise with the halftone image $H_{C^{New}}$ and the second watermark W_2 to obtain the extraction key K_{W_2}.
$$K_{W_2} = XOR(H_{C^{New}}, W_2) \tag{24}$$

The embedding of second watermark is lossless as it doesn't alter the pixel intensities before or after the embedding.

3.3 Watermark extraction

The watermark extraction phase is depicted in Fig. 2 and detailed as follows:

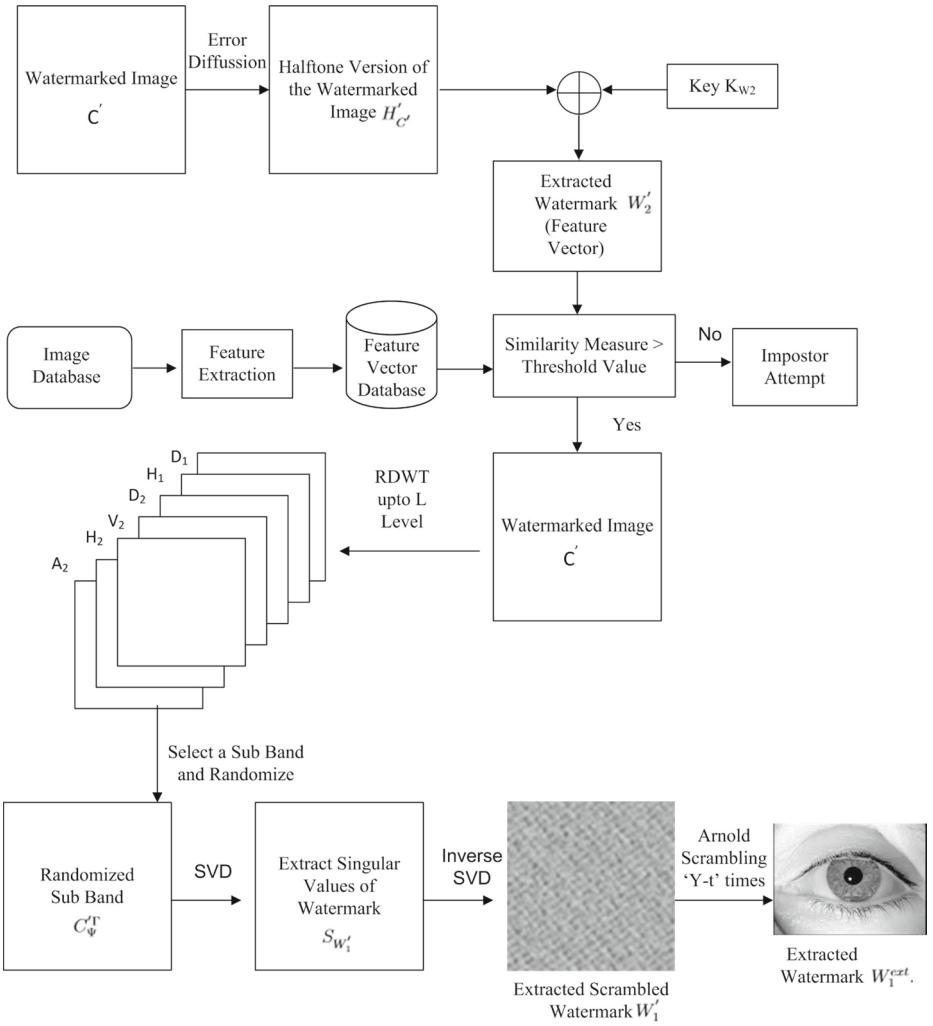


Fig. 2 Extraction process of proposed scheme

1. Obtain the halftone version $H'_{C'}$ of the suspected watermarked image C' using error diffusion method.
2. Extract the binary watermark using bitwise exclusive operation of the secret key with the obtained halftone image.

$$W'_2 = XOR\left(H'_{C'}, K_{W_2}\right) \tag{25}$$

3. Extraction of second watermark: The extracted watermark is evaluated quantitively using various similarity measures with respect to the original binary watermark. If the similarity is greater than the predefined threshold value only then the extraction of the second watermark is proceeded else it proves violation of rightful ownership. The process for extraction is detailed as follows:

(a) Perform redundant wavelet transform on the watermarked image C' upto L-level, denoted as follows: C'^{Γ}_{Ψ}, where $\Psi \epsilon [1, L]$, $\Gamma \epsilon \{A, H, V, D\}$

(b) Randomization of sub band: The selected sub band is randomized for extraction of the grayscale watermark as follows:

(i) Obtain two random sequences via non-linear chaotic maps using secret keys k_1 and k_2 of length $M \times M$ and $N \times N$ respectively.

(ii) Rearrange the two obtained sequences to form two arrays represented by M_1 and M_2 of same length $M \times M$ and $N \times N$ respectively.

(iii) Perform Hessenberg decomposition on the arrays M_1 and M_2 to obtain two orthogonal matrices R_1 and R_2.

(iv) Randomize the selected sub band C'^{Z}_{Ψ} with R_1 and R_2 as follows:

$$\tilde{C}'^{Z}_{\Psi} = R_1 C'^{Z}_{\Psi} R_2 \tag{26}$$

(v) Perform SVD on the randomized sub band $\tilde{C}'^{Z}_{\Psi}$ as follows:

$$\tilde{C}'^{Z}_{\Psi} = U_{\tilde{C}'^{Z}_{\Psi}} S_{\tilde{C}'^{Z}_{\Psi}} V^{T}_{\tilde{C}'^{Z}_{\Psi}} \tag{27}$$

(vi) Extract the singular values of the grayscale watermark as follows:

$$S_{W'_1} = \frac{S_{\tilde{C}'^{Z}_{\Psi}} - S_{\tilde{C}^{Z}_{\Psi}}}{\alpha} \tag{28}$$

(vii) Perform inverse SVD to obtain the extracted watermark.

$$W'_1 = U_{W^c_1} S_{W'_1} V^{T}_{W^c_1} \tag{29}$$

(viii) Descramble the extracted watermark $Y - t$ to obtain the actual watermark W^{ext}_1.

3.4 Authentication process

The proposed scheme performs authentication of rightful owners of digital images via extraction of both the biometric traits. The extracted watermarks are compared with the other samples provided by the users and stored in the database for this purpose. For face biometrics, feature is computed from the suspected watermarked image using the same secret key K_{W_2} as used at the time of embedding. This extracted face features serve as the second watermark and compared with the features extracted from the other samples provided by the user in the database. The similarity measure used in the algorithm is the d1 distance measure. It performs better for local pattern matching as compared to other distance measure like euclidean, manhattan,canberra,chi-square etc. If the match exceeds the threshold level, the extraction of first watermark is preceded else it is categorized as impostor attempt and halted. The iris codes are extracted from the inverse process of embedding as described in the extraction phase. Once the singular values are obtained for the iris code, inverse singular value decomposition is computed to get the grayscale scrambled iris template. The obtained iris watermark is decrambled using the secret key of the arnold scrambling depending upon its time period which finally gives the first extracted grayscale watermark. Thereafter, the feature extraction algorithm is applied on the extracted watermark to collect its features which is compared with the feature obtained from the other database samples. The decision can be based on the individual scores of each biometric trait or combined multimodal score. For instance, matching scores for feature extracted from face or iris templates or rather a fused score based on the two traits.

The $d1$ distance measure used to account for similarity between the extracted traits and the other database samples must be as minimum as possible. It must be normalized and subtracted from one prior to actual fusion of both traits using the weighted sum rule method ([25, 26]). Similarity measures must be in the same domain prior to fusing as for present case 1 indicates perfect match and 0 as perfect mismatch. Hence, fused measure becomes as follows:

$$S_{if} = w * S_{N_i} + (1 - w) * S_{N_f} \tag{30}$$

where S_{N_i} and S_{N_f} represents the normalized S_i and S_f values ranging in the interval [0, 1] with 1 as perfect match and w as weight. The fused measure S_{if} is thereafter checked and if it is greater than some threshold t, it indicates authentic user else unauthentic one.

The multimodality enhances the effectiveness of the verification stage as it reduces chances of error and provides features for convenience as it's just like a single measure comparison and no heavy computations are needed.

4 Experimental results and discussion

The performance of the proposed multimodal biometric watermarking algorithm has been tested upon SDUMLA-HMT database integrating the multiple biometric feature information into one. Whenever a ownership claim is to be resolved, the face feature vectors and iris binary templates are extracted from the suspected watermarked image and compared with the other samples of the user stored in the database. If a match is found, it is categorized as genuine claim otherwise taken as impostor attempt. The most important factor for the success of any biometric watermarking algorithm is its recognition accuracy. To validate the proposed scheme, verification based on face features, iris codes and the combined multimodal trait have been described in detail as follows:

4.1 Description of databases

For the experimental studies, biometric multimodal data of SDUMLA-HMT database has been taken. It contains data about 106 persons. We have considered only two biometric traits: face and iris images [25]. The face database contained four different kind of images varying in poses (look upward, forward, and downward), illumination conditions(normal illumination and with lamp illumination), facial expressions (smile, frown, surprise, and close eyes) and accessories (glasses and hat). The face database contains $7 \times (3 + 4 + 2 + 3) \times 106 = 8,904$ images. The size of images is 640×480 pixels with 24 bit bmp files and size of database as 8.8G. In iris images database, 10 samples (5 images per eye) for each individual was captured under infrared illumination. Hence total $1060(2 \times 5 \times 106)$ images with size as 768×576 were considered.

The performance of watermarking algorithms is generally based on evaluating imperceptibility measures like peak signal to noise ratio, mean square error or other metrics like normalized cross correlation metrics. But when it comes to a biometric watermarking system, then we need to ensure performance in terms of recognition accuracy. A watermarked biometric system should further enhance the security aspects of the biometric traits used without compromising in its quality and features. For the proposed algorithm, we have verified the performance based on face feature recognition, iris recognition and combined multimodality feature. The details are described as follows:

4.2 Performance evaluation using face verification

The images from the face database are fetched as input to the face detection algorithm which gives the face region as output of size 320 × 240 [31]. The face region is then employed with the feature extraction algorithm which computes the prominent local features based on the center symmetric local binary pattern and gray level co-occurrence matrix. The co-occurrence of pixel pairs is considered using different distances and directions in the obtained local pattern map [26]. Thereafter, these feature sets are matched using $d1$ distance measure.

4.3 Performance evaluation using iris verification

The images from iris database are resized according to the size of the cover images and thereafter, scrambled via arnold chaotic map based on secret key to render it unreadable and encrypted. It is then embedded into the sub bands of the cover image imperceptibly. For the recognition, the iris template is extracted from the watermarked image and features obtained from it are compared with the features extracted from the other samples of the user's iris templates stored in the database. Similarity based on $d1$ distance measure is computed for distinguishing the genuine and impostor attempts.

4.4 Performance evaluation using multimodal biometrics

Biometric systems based on single biometric trait often face problems of non-universality and circumvention [23]. Hence, multimodal biometric systems are preferred for biometric verification where decision is based on the combined measure of multiple biometric traits considered. In the proposed algorithm, we have employed the face and iris traits as biometric features. Hence, a fused matching score based on weighted sum of the individual similarity scores of face and iris features is considered for ownership verification based on some threshold value. For a given image, if the fused score comes out to be greater than the threshold value, it is categorized as genuine else as impostor attempt, thus proving the authenticity of the claim.

4.5 Parameters considered in the algorithm

4.5.1 Threshold determination

The security of the proposed watermarking algorithm scheme depends on various factors considered in the algorithm like the threshold value which decides the limit when the extraction of the iris codes will be proceeded. The similarity between the extracted facial features is computed with respect to the other user samples stored in the database. Only, when the authentication upto a certain limit is reached, then only the algorithm will be proceeded further. That is to say, when certainity about genunity is assured upto a limit. The threshold value is determined based on the large number of experiments where biometric templates are embedded and then matched after extracting from the other database samples. The maximum similarity reached is taken up as the threshold limit because as the threshold increases, lesser impostor attempts will be falsely classified as matches.However, more genuine attempts will be falsely classified as nonmatches. Hence, an optimum threshold value will balance security with robustness.

4.5.2 Sensitivity analysis

The sensitivity of the proposed multimodal biometric system relies on the secret keys k_1 and k_2 used as initial seed values for randomization of the cover image using non linear chaotic maps. The high sensitivity to the initial conditions enhances robustness against attacks as slight changes in the key value will totally change the results. Three cases may arise: (1) when k_1 is slightly changed, (2) when k_2 is slightly changed, and (3) when both k_1 and k_2 are slightly changed. A very slight change in the secret keys will render the extracted watermarks unrecognizable.

Also, scrambling of the iris codes using arnold map t times prior to embedding again strengthens the security as unauthentic owner will not be able to decrypt the watermark even if he obtains it. These aspects build the fact that proposed multimodal biometric scheme assures security.

4.5.3 The parameter n

The parameter n represents the level of RDWT decomposition in the proposed algorithm. As the number of levels increase, the robustness enhances against attacks. However, the time complexity increases. Besides a proper level decomposition, the verification accuracy of the multimodal biometric system doesn't get affected. The lowest frequency sub band of third level RDWT decomposition has been used for the experimental studies.

4.6 Results and discussion

To evaluate the efficacy of the proposed scheme, samples from the SDUMLA-HMT database were used.Some are shown in Fig. 3. The biometric verification was done based on the watermark data extracted from the cover images. Some sample cover images are depicted in Fig. 4. Two biometric traits that is, the iris templates and features extracted from the face image were employed as the respective watermarks. Face region was extracted using a triangle based face detection algorithm whereas iris images were resized depending on the size of the cover image. The ownership verification was done based on the fused similarity score. For the presented simulation study, 5 iris samples of right eye and 5 face images (frontal, different illumination, accessories, expressions) per subject in the dataset of 106 users were considered. To obtain the optimum value of the weight w used in the fused score, individual scores were calculated for raw biometric data from the database. The accuracy error rate was aimed to be minimized depending upon the Receiver Operator Characteristics(ROC) curves with smallest achievable values of Area Under Curve(AUC). The optimum value for the weight came out to be 0.54. The proposed system was thereafter checked for how the verification accuracy of the system gets affected by the generation, embedding and extraction of the biometric traits i.e. the iris codes and the face features into the cover images. The extracted watermarks were thereafter compared with the other biometric samples of the user kept in the database and evaluated based on the individual as well as the fused matching scores. The $d1$ distance was used as the criteria for matching of the iris templates as well as the face features extracted from the face biometric data.The total number of genuine and impostor attempts were equal to $5*4*106 = 2120$(number of intraclass comparisons) and $106*105 = 11130$(number of interclass comparisons) respectively.

The verification accuracy of the proposed system based on the individual traits, Iris templates S_i and face features S_f as well as the fused one S_{if} have been presented through

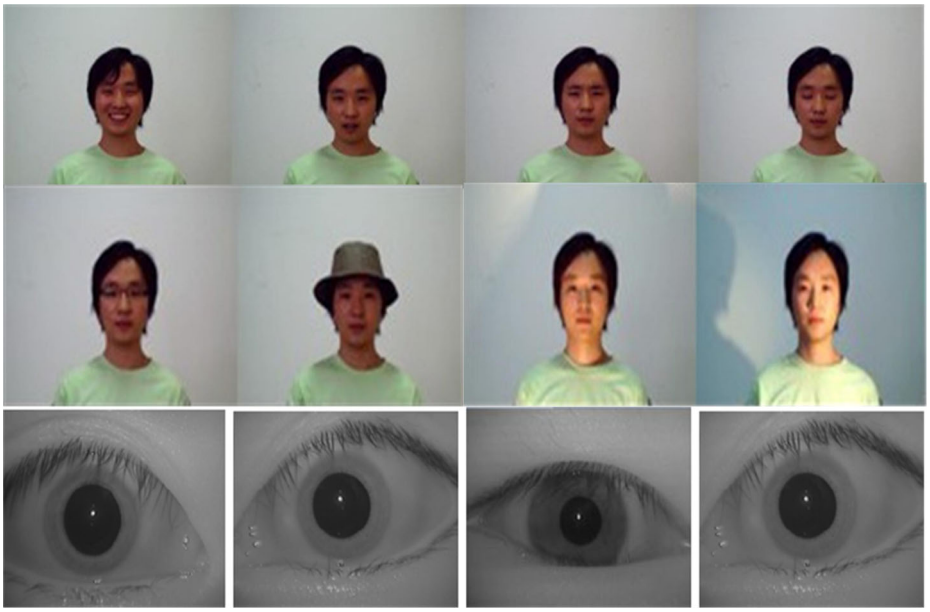


Fig. 3 Sample images of faces and Iris used as watermarks from SDUMLA-HMT database

ROC curves in Figs. 5, 6 and 21. As can be observed from the Fig. 5, the verification accuracy is almost at the same level before and after watermarking as can be inferred from the ROC curve and Equal Error Rate(EER) almost at the same level. Now, for the attacks scenario, the EER slightly increases for the histogram equalization attack, and thereafter keeps on increasing for sharpening,gaussian blur, resizing, pixilation, wrapping, salt and pepper noise and finally JPEG compression. The verification accuracy of the system keeps on deteriorating as the EER increases. Other attacks have also been tested with like horizontal flipping, contrast adjustment, row-column deletion, vertical flipping,rotation and SPIHT compression. The variation plot is depicted in Fig. 5.

For assessment of the verification accuracy based on the face features, the ROC curves are plotted in Fig. 6. The verification accuracy keeps on deteriorating as the different attacks are applied. The order of deterioration goes as for histogram equalization, sharpening,

Fig. 4 Test images used as cover images in the proposed scheme

Table 1 PSNR values of test images

Image	Lena	Pepper	Baboon	Cameraman
PSNR	36.85	35.43	34.21	36.98

gaussian blur, resizing, pixilation, wrapping, salt and pepper noise and JPEG compression. The EER increases in this order signifying the decrease in verification accuracy. The overall EER decreases for each of the attacks when the fused matching score is considered as can be observed in Fig. 21. The proposed scheme has been tested for variety of cover images. Results for some of the test images in terms of ownership verification accuracy evaluated based on PSNR, NCC, AUC and EER have been presented in Tables 1, 2, 3, 4, 5 and 6. The value of scaling factor (α) for these experimental results was taken to be 0.035. The scheme has been tested under different attack scenarios with results presented for one of the test cover images and grayscale watermark in Figs. 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 and 20. The binary watermark is in form of feature vectors extracted from the face. Hence, its quantitative evaluation is presented under aforementioned attack scenarios in Table 2 based on NCC.

In the proposed multimodal verification scheme, the redundant discrete wavelet domain is chosen for embedding the biometric traits. First of all, the reason behind choosing RDWT instead of DWT was that the size of the sub bands of RDWT remains same as size of the cover image whereas in DWT, it keeps on decreasing significantly after every decomposition. So, RDWT provides sufficient capacity for embedding of watermarks. Two biometric traits are used as watermarks and embedded in different regions of the cover image without affecting each other. The iris template used as the first watermark is rendered unreadable

Table 2 Evaluation of extracted watermarks based on NCC against various attacks

Attack	Lena image		Pepper image		Baboon image		Cameraman image	
	Iris	Face	Iris	Face	Iris	Face	Iris	Face
Histogram Eq.	0.9836	0.9334	0.9822	0.9287	0.9745	0.9136	0.9843	0.9294
Gaussian blur	0.8868	0.9426	0.8836	0.9434	0.8743	0.9352	0.8864	0.9414
Sharpen	0.8903	0.9026	0.8804	0.9018	0.8884	0.8743	0.8922	0.9022
Salt & Pepper	0.8277	0.8264	0.8264	0.8258	0.8248	0.8253	0.8238	0.8216
Resizing	0.8582	0.9498	0.8578	0.9472	0.8566	0.9448	0.8577	0.9432
JPEG	0.7688	0.9479	0.7711	0.9482	0.7602	0.9415	0.7667	0.9419
Pixelation	0.8818	0.8811	0.8808	0.8802	0.8769	0.8778	0.8823	0.8807
Wrapping	0.9081	0.9222	0.9064	0.9219	0.9267	0.9360	0.9041	0.9203
Row-col deletion	0.9193	0.8923	0.9188	0.8917	0.9042	0.8845	0.9196	0.8951
Rotation	0.7933	0.9014	0.7915	0.9008	0.7928	0.9101	0.7925	0.9022
Horizontal flipping	0.9860	0.7168	0.9855	0.7044	0.9723	0.7002	0.9823	0.7115
Vertical flipping	0.8952	0.7144	0.8923	0.7133	0.8917	0.7109	0.8922	0.7115
Contrast adjustment	0.9793	0.9413	0.9723	0.9411	0.9763	0.9401	0.9788	0.9434
SPIHT compression	0.7318	0.9609	0.7313	0.9602	0.7307	0.9588	0.7307	0.9605

Table 3 Results for Lena image based on Iris template, Face features and Fused traits for proposed approach

Attack	Iris Iemplate S_i		Face Template S_f		Fused S_{if}	
	AUC	EER	AUC	EER	AUC	EER
Without watermarking	0.0148	3.44	0.0229	5.48	0.00013	0.48
With Watermarking(No attack)	0.0163	4.24	0.0250	6.68	0.0018	0.52
Histogram equalization	0.0235	5.92	0.0460	10.45	0.0040	2.67
Gaussian Blur	0.0169	3.79	0.0280	6.89	0.0028	0.61
Sharpen	0.0230	6.09	0.0306	8.28	0.0013	0.92
Salt & Pepper noise (50 %)	0.0456	0.63	0.0302	8.19	0.0032	1.82
Resizing (512 → 256 → 512)	0.0299	7.47	0.0380	9.31	0.0013	0.92
JPEG (50:1)	0.0630	13.71	0.0380	9.31	0.0068	2.87
Pixelation	0.0230	6.09	0.237	5.86	0.0013	0.92
Wrapping	0.0299	7.47	0.0306	8.28	0.0044	2.68
Row-col deletion	0.0230	6.09	0.0306	8.28	0.0013	0.92
Rotation	0.0456	0.63	0.0302	8.19	0.0032	1.82
Horizontal flipping	0.0235	5.92	0.0460	10.45	0.0040	2.67
Vertical flipping	0.0299	7.47	0.0380	9.31	0.0013	0.92
Contrast adjustment	0.0230	6.09	0.0306	8.28	0.0013	0.92
SPIHT Compression	0.0630	13.71	0.0380	9.31	0.0068	2.87

Table 4 Results for Baboon image based on Iris template, Face features and Fused traits for proposed approach

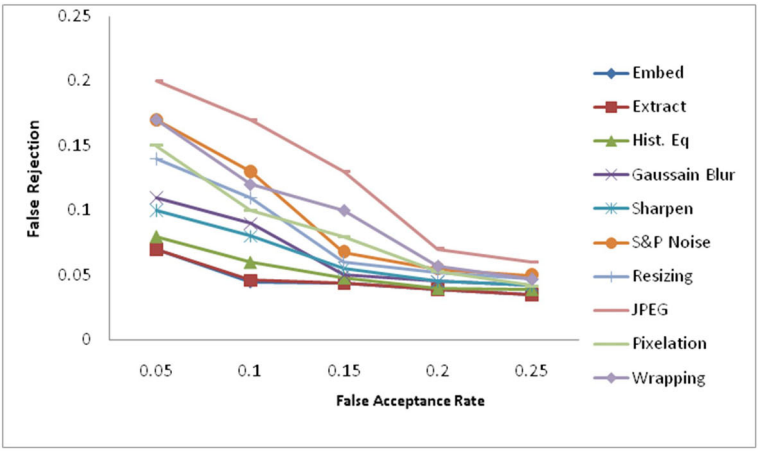
Attack	Iris iemplate S_i		Face template S_f		Fused S_{if}	
	AUC	EER	AUC	EER	AUC	EER
Without watermarking	0.0148	3.46	0.04370	8.39	0.0019	0.96
With watermarking(No Attack)	0.0153	3.78	0.04456	9.24	0.0022	1.41
Histogram equalization	0.0347	6.02	0.0560	12.45	0.0065	2.97
Gaussian blur	0.0352	6.32	0.0580	12.67	0.0085	3.02
Sharpen	0.0343	6.79	0.0372	9.02	0.0009	0.72
Salt & Pepper Noise (50 %)	0.0556	1.03	0.0365	8.80	0.0052	2.02
Resizing (512 → 256 → 512)	0.0302	8.04	0.0402	10.21	0.0083	1.43
JPEG (50:1)	0.0730	12.07	0.0480	10.53	0.0088	3.02
Pixelation	0.0233	6.78	0.245	5.98	0.0015	1.22
Wrapping	0.0302	8.35	0.0356	9.08	0.0023	1.06
Row-col deletion	0.0343	6.79	0.0372	9.02	0.0009	0.72
Rotation	0.0556	1.03	0.0365	8.80	0.0052	2.02
Horizontal flipping	0.0347	6.02	0.0560	12.45	0.0065	2.97
Vertical flipping	0.0302	8.04	0.0402	10.21	0.0083	1.43
Contrast adjustment	0.0343	6.79	0.0372	9.02	0.0009	0.72
SPIHT compression	0.0730	12.07	0.0480	10.53	0.0088	3.02

Table 5 Results for Pepper image based on Iris template, Face features and Fused traits for proposed approach

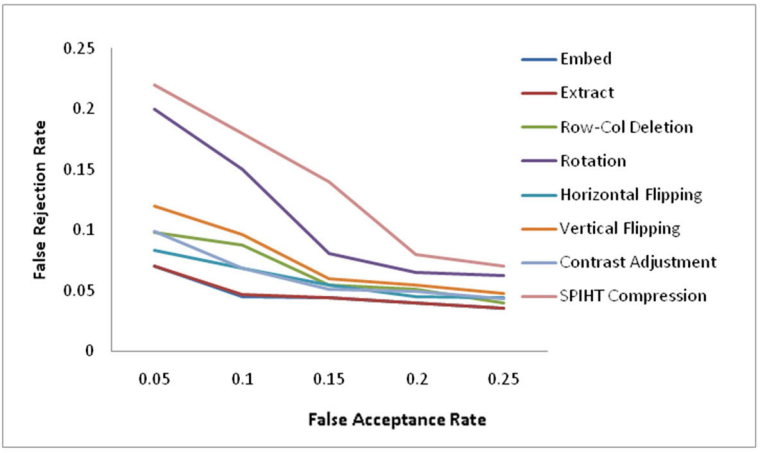
Attack	Iris Iemplate S_i		Face Template S_f		Fused S_{if}	
	AUC	EER	AUC	EER	AUC	EER
Without watermarking	0.0156	3.89	0.0254	5.86	0.0011	0.53
With Watermarking(No Attack)	0.0163	3.98	0.0263	6.33	0.0023	0.68
Histogram equalization	0.0246	6.12	0.0488	11.04	0.0052	2.92
Gaussian blur	0.0172	3.99	0.0287	6.94	0.0035	0.81
Sharpen	0.0245	6.29	0.0356	8.88	0.0009	0.78
Salt & Pepper noise (50 %)	0.0443	0.53	0.0280	7.89	0.0022	1.44
Resizing (512 → 256 → 512)	0.0302	7.24	0.0380	9.31	0.0013	0.92
JPEG (50:1)	0.0640	13.01	0.0303	8.91	0.0068	2.87
Pixelation	0.0222	5.79	0.264	6.98	0.0013	0.92
Wrapping	0.0300	7.87	0.0326	8.68	0.0043	2.57
Row-col deletion	0.0245	6.29	0.0356	8.88	0.0009	0.78
Rotation	0.0443	0.53	0.0280	7.89	0.0022	1.44
Horizontal flipping	0.0246	6.12	0.0488	11.04	0.0052	2.92
Vertical flipping	0.0302	7.24	0.0380	9.31	0.0013	0.92
Contrast adjustment	0.0245	6.29	0.0356	8.88	0.0009	0.78
SPIHT compression	0.0640	13.01	0.0303	8.91	0.0068	2.87

Table 6 Results for Cameraman image based on Iris template, Face features and Fused traits for proposed approach

Attack	Iris Iemplate S_i		Face Template S_f		Fused S_{if}	
	AUC	EER	AUC	EER	AUC	EER
Without watermarking	0.0142	3.45	0.0262	5.86	0.00011	0.57
With watermarking(No Attack)	0.0145	3.64	0.0289	6.74	0.0017	0.67
Histogram equalization	0.0255	6.24	0.0480	11.65	0.0049	2.84
Gaussian blur	0.0179	3.99	0.0290	6.99	0.0027	0.57
Sharpen	0.0240	6.29	0.0316	8.38	0.0017	1.22
Salt & Pepper noise (50 %)	0.0436	0.53	0.0322	8.59	0.0035	1.98
Resizing (512 → 256 → 512)	0.0322	8.04	0.0480	10.03	0.0017	1.20
JPEG(50:1)	0.0620	13.21	0.0340	8.71	0.0062	2.57
Pixelation	0.0222	5.79	0.247	6.06	0.0015	1.12
Wrapping	0.0269	7.17	0.0326	8.58	0.0043	2.48
Row-col deletion	0.0240	6.29	0.0316	8.38	0.0017	1.22
Rotation	0.0436	0.53	0.0322	8.59	0.0035	1.98
Horizontal flipping	0.0255	6.24	0.0480	11.65	0.0049	2.84
Vertical flipping	0.0322	8.04	0.0480	10.03	0.0017	1.20
Contrast adjustment	0.0240	6.29	0.0316	8.38	0.0017	1.22
SPIHT compression	0.0620	13.21	0.0340	8.71	0.0062	2.57



(a)

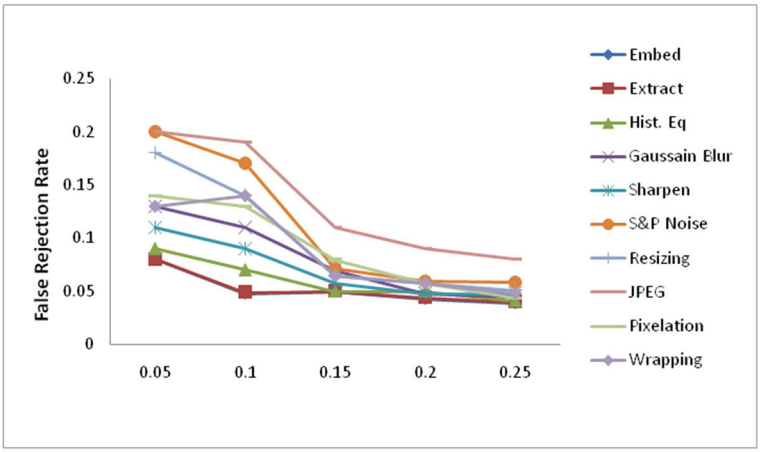


(b)

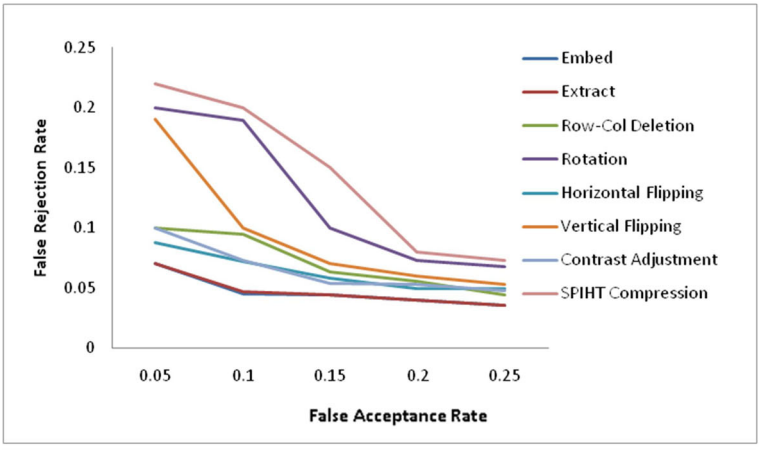
Fig. 5 ROC curve for proposed scheme based on analysis of Iris matching score S_i

before embedding based on secret key so that no one could retrieve the actual iris template without possessing the secret key. Furthermore, the randomization of a selected sub band prior to embedding based on secret keys again enhanced security. The second watermark which is extracted from the face biometric in the form of face features is embedded reversibly without affecting the watermarked image generated by the embedding of first watermark based on secret key K_{W_2}.

The comparison of the proposed scheme with the other existing state of art approaches is an integral part of the success of an approach. First of all, the proposed approach exploits the redundant wavelet transform domain for embedding of watermarks which provides enough capacity. Secondly, as compared to existing schemes [7, 8] based on single



(a)



(b)

Fig. 6 ROC curve for proposed scheme based on analysis of Face features matching score S_f

Fig. 7 Result of Histogram Equalization Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

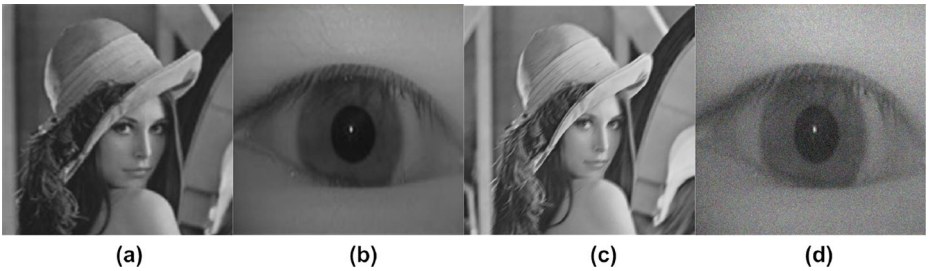


Fig. 8 Result of Gaussian Blur Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

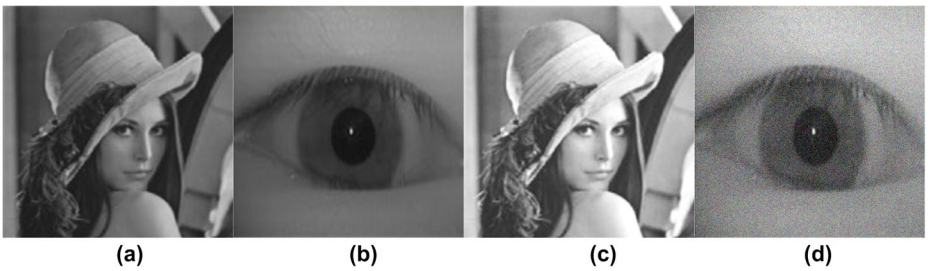


Fig. 9 Result of Sharpening Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

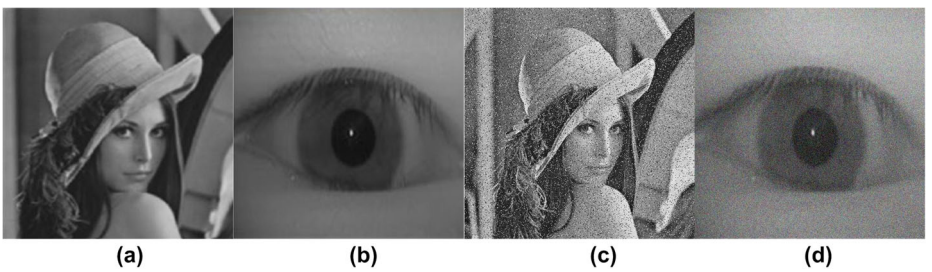


Fig. 10 Result of Salt & Pepper Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

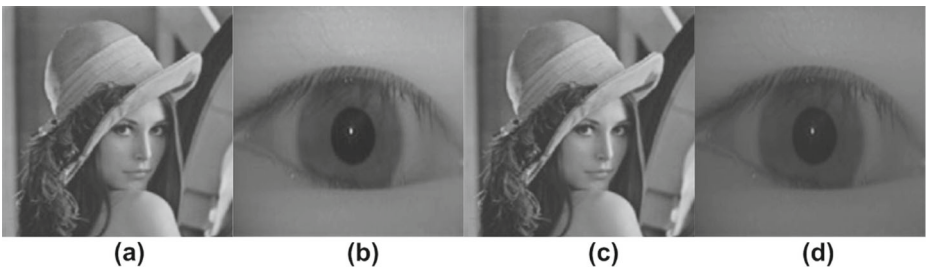


Fig. 11 Result of Resizing Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

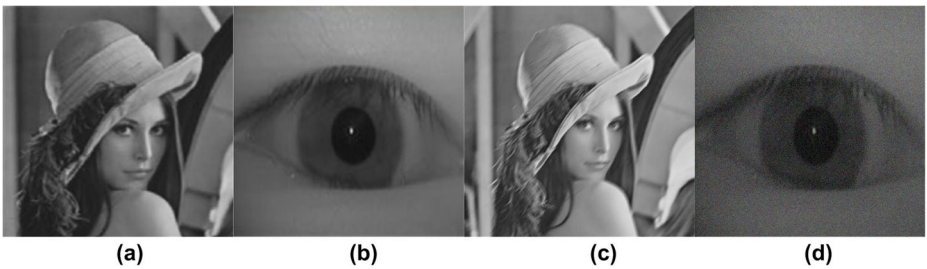


Fig. 12 Result of JPEG Compression Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

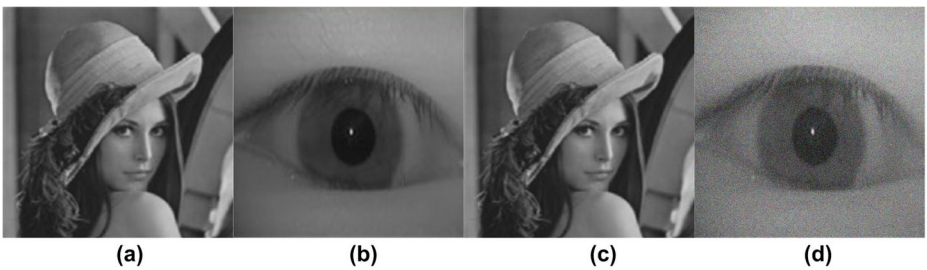


Fig. 13 Result of Pixelation Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

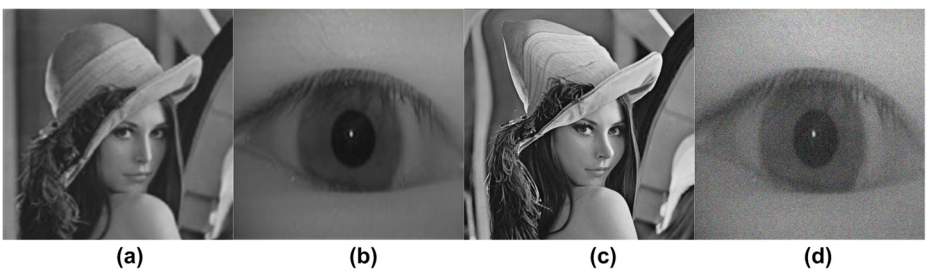


Fig. 14 Result of Wrapping Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

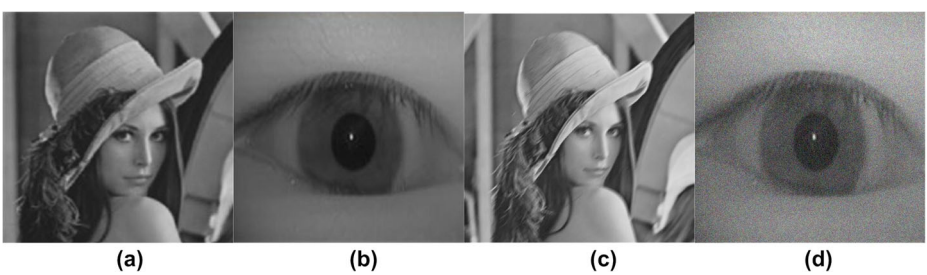


Fig. 15 Result of Row-Column Deletion Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

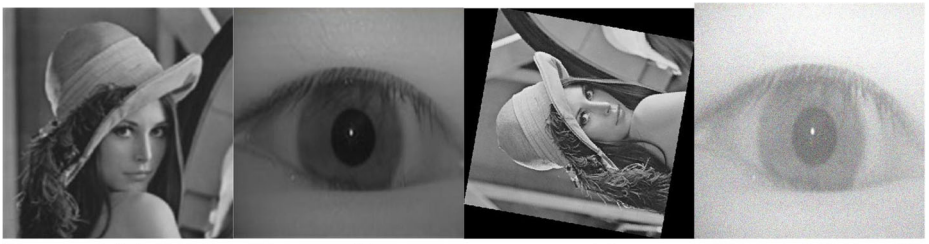


Fig. 16 Result of Rotation Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

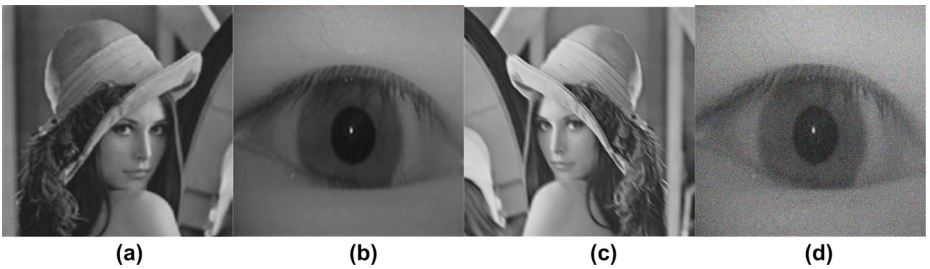


Fig. 17 Result of Horizontal Flipping Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

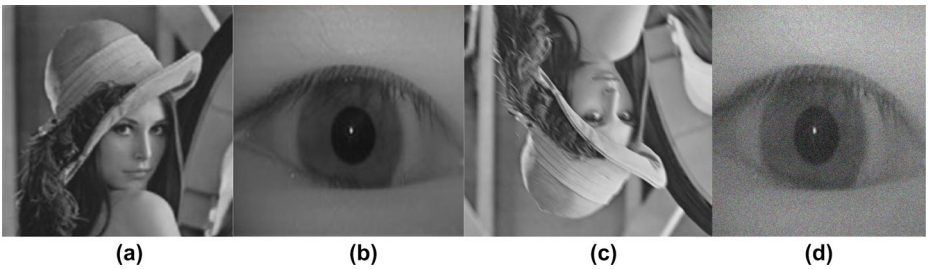


Fig. 18 Result of Vertical Flipping Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

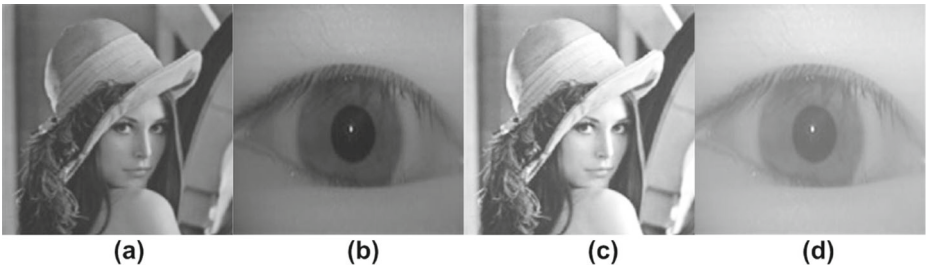
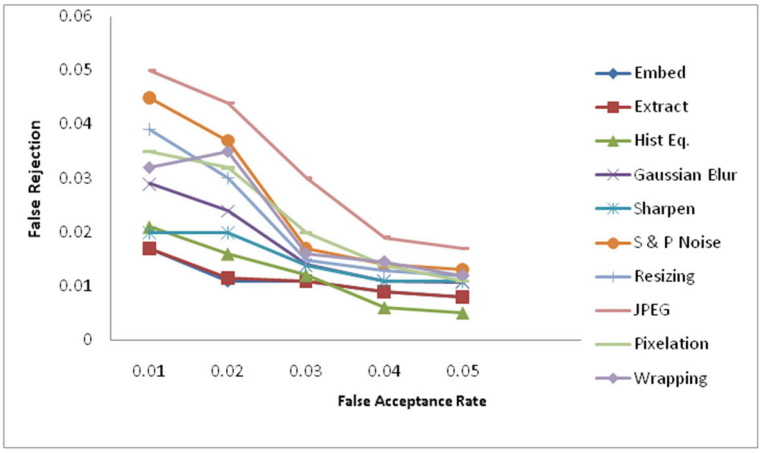


Fig. 19 Result of Contrast Adjustment Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

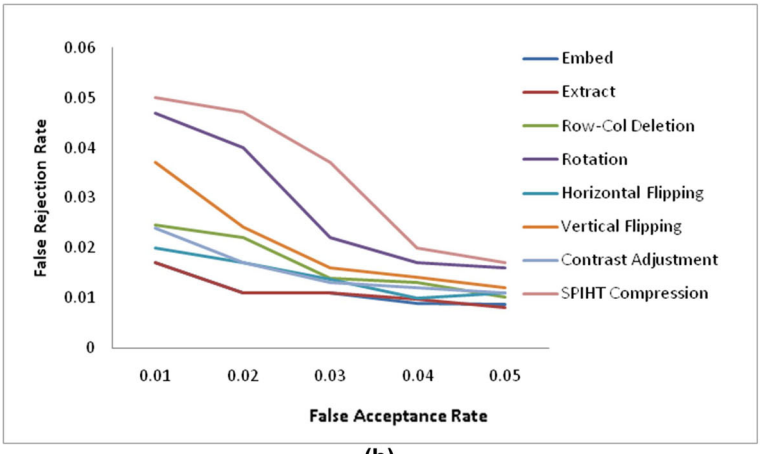
Fig. 20 Result of SPIHT Compression Attack (**a**) Original Cover Image (**b**) Gray Scale Watermark (**c**) Attacked Watermarked Image (**d**) Extracted Watermark

biometric trait, be it iris codes or face features, the proposed scheme is based on integrating multiple biometrics into one scheme. Moreover, the affect of watermarking on the verification accuracy of the proposed biometric system has been evaluated based on the extracted watermark data not just measures done in terms of imperceptibility of the watermarked images [10, 12]. Different attack scenarios and their affect on verification accuracy have been assessed. Variety of cover images independent of the biometric traits have also been tested upon for the appropriateness of the proposed authentication scheme with results tabulated in Tables 3–6 for different cover images. Multimodal biometric authentication scheme based on fingerprint and iris data has been proposed in the literature [13]. It used Daughmans model and hamming distance as the similarity evaluation techniques. The major difference between their scheme and our proposed scheme is that, first of all we used face features and iris codes as the biometric traits. Secondly, we have employed d1 distance as the evaluation criteria. Thirdly, the authentication in our scheme was based on a fused score whereas in their scheme it was at decision level. The decision level authentication required setting of two different threshold values for fingerprint and iris codes based on different conjunction rules. It will be very tough for a user with little experience and will directly affect the verification accuracy of the scheme. However, in our proposed scheme it is very convenient to use as the authentication will be based on a fused score level which will act just like using a unimodal biometric system (Figs. 5, 6 and 21).

Another work based on the fused score has been presented in [28]. However, it is based on fingerprint and iris templates used as biometric traits. They used Daughmans model and hamming distance for construction and evaluation of iris codes whereas for fingerprint, the minutiae points were extracted and matched in terms of their co-ordinates and orientations to obtain a matching score. These scores were then normalized and combined to get a fused score. The objective of the proposed scheme was to show how the verification accuracy of a biometric watermarking system increases upon usage of more than one biometric traits for recognition and the fusion of the evaluation metrics at the score level facilitates distinguishing the genuine and the impostor attempts. The accuracy of the system also depends upon the raw biometric data quality of the databases used. In our algorithm, we have used our own methods for embedding and extraction of biometric watermarks followed by subsequent evaluation by a fused score. In future, we will test it for bigger data sets and fuse more biometric metric to improve upon the verification accuracy of the system.



(a)



(b)

Fig. 21 ROC curve for proposed scheme based on analysis of fused scores of both traits S_{if}

5 Conclusion

A multimodal biometric authentication scheme has been proposed in this paper. It incorporates two watermarks: one grayscale based on iris template and the other binary based on facial features extracted via feature extraction algorithm based on center symmetric local binary pattern and gray level co-occurrence matrix.The embedding of watermarks in the redundant discrete wavelet transform provided enough capacity for embedding without deteriorating the visual quality of the watermarked images. The performance of the algorithm is evaluated from the user's verification point of view based on false acceptance rate, false rejection rate, equal error rate, area under curve and corresponding ROC curves. From the experimental results it was proved that fusion of biometric traits enhanced user's verification accuracy and increased its robustness against different attack scenarios.

References

1. Amirgholipour S, Aboosaleh S (2014) A pre-filtering method to improve watermark detection rate in DCT based watermarking. Int Arab J Inf Technol 11(2):178–185
2. Barni M, Bartolini F, Cappellini V, Piva A (1998) A dct domain system for robust image watermarking. Signal Process 66(3):357–372
3. Barni M, Bartolini F, Cappellini V, Piva A, Rigacci F (1998) A m.a.p. identification criterion for dct based watermarking. In: Proceedings European Signal Processing Conference, pp 17–20
4. Bohra A, Farooq O (2009) Izharuddin Blind self-authentication of images for robust watermarking using integer wavelet transform. Int J Electron Commun 63(8):703–707
5. Chang C, Tsai P, Lin C (2005) Svd based digital image watermarking scheme. Pattern Recogn Lett 26(10):1577–1586
6. Chu W (2003) Dct based image watermarking using subsampling. IEEE Trans Multimed 5(1):34–38
7. Consultants T (2010) Building a digital economy. The importance of saving jobs in Europes Creative Economy, Paris: International Chamber of Commerce/BASCAP. Available on line: www.ec.europa.eu/dgs/jrc/downloads/events/.../20110405budapestturlea.pdf (access 15/05/2011)
8. Cox I, Kilian J, Leighton F, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6(12):1673–1687
9. Dodis Y, Reyzin L, Smith A (2004) Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. Eurocrypt 2004(3027):523–540
10. Gangyi J, Mei Y, Shi S, Liu X, Kim Y (2002) New blind image watermarking in dct domain. In: Signal Processing, 6th International Conference, vol 2, pp 1580–1583
11. Gunsel B, Uludag U, Tekalp AM (2002) Robust watermarking of fingerprint images. Pattern Recogn 35(12):2739–2747
12. Hernandez J, Amado M, Perezgonzalez F (2000) Dct domain watermarking techniques for still images: Detector performance analysis and a new structure. IEEE Trans Image Process 9(1):5568
13. Hsu C, Wu J (1999) Hidden digital watermarks in images. Image Processing, IEEE Transactions 8(1):58–68
14. Jain AK, Uludag U (2003) Hiding biometric data. IEEE Trans Pattern Anal Mach Intell 25(11):1494–1498
15. Jain AK, Uludag U, Hsu RL (2002) Hiding a face in a fingerprint image
16. Kalantari N, Ahadi S, Vafadust M (2010) A robust image watermarking in the ridgelet domain using universally optimum decoder. IEEE Trans Circ Syst Video Technol 20(3):396–406
17. Li Z, Yap K, Lei B (2011) A new blind robust image watermarking scheme in svd dct composite domain. In: Image Processing (ICIP), 18th IEEE International Conference, pp 2757–2760
18. Lu Z, Zheng H, Huang J (2007) A digital watermarking scheme based on dct and svd. In: Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP 2007. Third International Conference, vol 1, pp 241–244
19. Maity S, Kundu M (2010) Dht domain digital watermarking with low loss in image informations. Int J Electrons Commun 64(3):243–257
20. Mohanty S, Ranganathan N, Namballa R (2003) Vlsi implementation of invisible digital watermarking algorithms towards the development of a secure jpeg encoder. In: Proceedings of the IEEE Workshop on Signal Processing Systems Based Implementation of an Invisible Robust Image Watermarking Encoder, pp 183–188
21. Morita Y, Ayeh E, Adamo O, Guturu P (2009) Hardware/software co-design approach for a dct-based watermarking algorithm. In: Circuits and Systems, 2009. MWSCAS'09. 52nd IEEE International Midwest Symposium. IEEE, pp 683–686
22. Patra J, Phua J, Bornand D (2010) A novel dct domain crt-based watermarking scheme for image authentication surviving jpeg compression. Digit Signal Process 20(6):1597–1611
23. Qi H, Zheng D, Zhao J (2008) Human visual system based adaptive digital image watermarking. Signal Process 88(1):174–188
24. Ratha NK, Connell JH, Bolle RM (2000) Secure data hiding in wavelet compressed fingerprint images. Proceedings of ACM Multimedia:127–130
25. Rawat S, Raman B (2012) A publicly veriable lossless watermarking scheme for copyright protection and ownership assertion. Int J Electron Commun 66(11):955–962
26. Sadreazami H, Amini M (2012) A robust spread spectrum based image watermarking in ridgelet domain. Int J Electron Commun 66(5):364–371
27. Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar B (1999) Biometric encryption, ICSA Guide to Cryptography, McGraw-Hill
28. Suhail M, Obaidat M (2003) Digital watermarking based dct and jpeg model. IEEE Trans Instrum Measur 52(5):1640–1647

29. Uludag U, Pankanti S, Prabhakar S, Jain AK (2004) Biometric cryptosystems: issues and challenges. Proc IEEE 92(6):948–960
30. Vatsa M, Singh R, Mitra P, Noore A (2004) Comparing robustness of watermarking algorithms on biometrics data. Proceedings of the Workshop on Biometric Challenges from Theory to Practice ICPR Workshop:5–8
31. Yang C, Hu W, Lai J (2008) Dct based watermarking by quotient-embedding algorithm. In: Innovative Computing Information and Control ICICIC'08. 3rd International Conference. IEEE, pp 20–20
32. Zhao D, Chen G, Liu W (2004) A chaos-based robust wavelet-domain watermarking algorithm. Chaos Solitons Fractals 22:47–54

Priyanka Singh received B.Tech Degree from HBTI, Kanpur, M.Tech and Ph.D. degree from NIT, Allahabad. She is currently working as a postdoctoral fellow in Department of Computer Science and Engineering, IIT Roorkee. Her areas of research include Digital Watermarking, Visual Cryptography, Image Fusion, Biometrics and Security related concepts.

Balasubramanian Raman Associate Professor in the Department of Computer Science and Engineering at Indian Institute of Technology Roorkee, obtained his B.Sc Degree in Mathematics from A.M. Jain College (University of Madras) in 1994, M.Sc degree in Mathematics from Madras Christian College (University of Madras) in 1996 and Ph.D from Indian Institute of Technology Madras in 2001. He was a Post Doctoral Fellow at University of Missouri Columbia, USA in 2001-02 and a Post Doctoral Associate at Rutgers, the State University of New Jersey, USA in 2002-03. He joined Department of Mathematics at Indian Institute of Technology Roorkee as Lecturer in 2004 and became Assistant Professor in 2006. He was a Visiting Professor and a member of Computer Vision and Sensing Systems Laboratory in the Department of Electrical and Computer Engineering at University of Windsor, CANADA during May - August 2009. His area of Research includes Vision Geometry, Digital Watermarking using Mathematical Transformations, Image Fusion, Biometrics, Secure Image Transmission over Wireless Channel, Content Based Image Retrieval and Hyperspectral Imaging. He has more than 150 research publications in reputed journals and conference proceedings.

Partha Pratim Roy received the Ph.D. degree in computer science from Universitat Autònoma de Barcelona, Spain, in 2010. He worked as postdoctoral research fellow in the Computer Science Laboratory (LI, RFAI group), France (2010–2012) and in Synchromedia Lab, Canada (2013). He has gathered industrial experience while working as an Assistant System Engineer in TATA Consultancy Services (India) from 2003 to 2005 and as Chief Engineer in Samsung, Noida from 2013 to 2014. His current research interests include pattern recognition, image processing, etc. Dr. Roy was a recipient of the Best Student Paper Award at the International Conference on Document Analysis and Recognition in 2009.