Face Features Based Biometric Watermarking of Digital Image Using Singular Value Decomposition for Fingerprinting

Vandana S Inamdar and Priti P Rege

College of Engineering, Pune, India
vhj.comp@coep.ac.in, ppr.extc@coep.ac.in

Abstract

In this paper, a semi-blind biometric watermarking scheme is proposed for fingerprinting application. Watermark is derived from face image using Principal Component Analysis. These face features are then embedded in host image using block-based watermarking scheme, which uses Singular Value Decomposition transform. This watermarking scheme works by initially dividing the original image into non-overlapping blocks, applying the SVD transform to each of them and subsequently embedding a watermark into the singular vectors. Each watermark value is embedded by modifying angles formed by the right singular vectors of each block with respect to some arbitrary plane. During embedding process the orthogonal property of the right singular vectors matrix is preserved. After extracting the features from watermarked host image it is correlated with face database features to get the approximately correct image. The robustness of this watermarking technique is tested by applying various attacks.

Keywords: *Biometric watermarking, Face features, Principal component analysis, orthogonal property, Singular Value Decomposition, robustness*

1. Introduction

Owing to the progress in information technology and growth of the internet, vast amount of data such as text, images, audio, video and graphics have been digitized for easy storage, processing and transmission over the internet. Easy availability of the content editing software, mobile and compact digital devices and the internet, make the digital lifestyle of the common man quite different from that few years ago. There is an urgent and desperate need for the protection of the intellectual property rights of digital media.

This copyright abuse is the motivating factor in developing new encryption technologies. Authentication and information hiding have also become important issues. The solution to counter the unauthorized distribution of copyrighted contents is digital watermarking. Digital watermarking refers to specific information hiding techniques whose purpose is to embed secret information inside multimedia contents, such as images, video or audio streams without affecting its perceptual quality.

1.1 Significance of Biometric Watermark

Traditionally, watermarking scheme embeds a predefined string such as name of author or logo into the host document which can be text, audio, video, image or 3D meshes. Usually these watermarks are less meaningful and intuitive for easily identifying and are also low correlative to copyright holder. The information of the holder is not inherent and may change with time. Using these as a watermark may lead to imitation, tamper and repudiation.

Traditional watermarking method does not convincingly validate the claimed identification of the person as the host might be fraudulently watermarked with a particular string pattern or logo by impersonators. Recently biometrics is adaptively merged into watermarking technology to enhance the credibility of the conventional watermarking methods.

A.K. Jain and his research team is a pioneer in suggesting biometric watermarking method. Jain and Umut [1] proposed multimedia content protection framework that is based on biometric data of the users.

If the Watermarking is combined with biometric features, then it will be more secured and confidential as biometric features are unique for each individual [2]. Biometric can be fingerprint, faces, iris, signature, finger geometry, hand geometry or voice [3].

Majority of the reported watermarking techniques use a pseudorandom sequence as a watermark and a binary decision, whether the digital media is watermarked or not is done by calculating the correlation between the watermark and media under considerations. However, watermark like PN sequence does not represent any meaningful information about authentication for ownership verification and thus serves limited application [30]. Significant motivation for using face as a watermark is that face is a modality that humans largely depend for authentication. Consequently, every human is a putative expert in face recognition from infancy and second points is that face is a modality that can be captured easily.

Most of the watermarking schemes proposed are for ownership verification or for tamper detection. These methods are source based in which owner’s information is embedded as a watermark. If out of more than one number of legal buyers of content, one starts selling the contents illegally, it may be very difficult to catch who is redistributing the contents without permission. Allowing each distributed copy to be customized for each legal recipient can solve this problem. In such scenarios destination based watermarking is required. There are some applications like finger printing where the information associated with a digital content should contain information about the end user rather than about the owner of digital content.

In this paper, we propose a novel biometric watermarking scheme based on Singular Value Decomposition (SVD) of host image which can be effectively used for fingerprinting applications. Face image database which is a biometric trait of all legal customers is maintained at the owner’s side. Each distributed copy is customized watermarked with the face feature of the legal distributor. As the face image itself contains high energy, it cannot be embedded in cover image directly because such embedding degrades the perceptual quality of image. To circumvent this problem, feature extraction technique is applied on face biometric trait.

The rest of the paper is organized as follows. Significance of SVD transform for image processing is discussed in section II. In section III some of the SVD based watermarking techniques are elaborated, while next section discusses the proposed algorithm. Section V shows experimental results. Concluding remarks are given in last section.

2. Significance of SVD in Context with Image

SVD is based on a theorem from linear algebra, which says that a rectangular matrix A of size m x n can be broken down into the product of three matrices: an orthogonal matrix U of size m x m , a diagonal matrix S of size m x n and the transpose of orthogonal matrix V of size n x n.

$$\mathrm{SVD}(\,A_{mxn}) = [U_{mxm}\ S_{mxn}\ V_{nxn}] \qquad (1)$$

By multiplying U, S and $\mathrm{V^T}$ the matrix A is obtained.

$$\mathrm{A_{mxn} = U_{mxm}\, S_{mxn}\, V_{nxn}^T} = \sum_{i=1}^{\min(m,n)} \sigma_i\, u_i v_i^T \qquad (2)$$

where $\sigma_i \in \mathcal{R}_+$, i=1…min(m ,n) are the singular values, i.e., the available diagonal elements of the matrix S sorted in descending order, u_i are the left singular vectors, i.e., the columns of U, and v_i are the right singular vectors, i.e., the rows of V^T (or columns of V). U and V are unitary matrices that means $UU^T = I_{mxm}$, $VV^T = I_{nxn}$ where I_{mxm} and I_{nxn} are the unit matrices. The eigen-vectors of AA^T make up the columns of U and the Eigen-vectors of A^TA are the columns of V. The diagonal element of S represents the square root of the Eigen values of either AA^T or A^TA.

In signal processing applications, SVD technique has been applied to image compression [6] , noise reduction and image watermarking. SVD transforms provides an elegant way for extracting algebraic features from an image. Using SVD in digital image processing has some advantages. First, the size of the matrices from SVD transformation is not fixed. It can be a square or a rectangle. Second, singular values in a digital image have very good stability, that is, when a small perturbation is added to image, it's singular values do not change significantly. Third, singular values contain intrinsic algebraic image properties. It is important to note that each singular value specifies the luminance of image while the corresponding pair of left and right singular vectors specify the geometry of the image layer [5]. Increasing the magnitude of the singular values will increase the image luminance, while lowering the magnitude will decrease the image luminance. It means that singular values are in close relation with the image luminance, while the intrinsic "geometry" of the image depends upon left and right singular vectors which are orthogonal matrices. These all characteristics of SVD make it very much desirable for watermarking.

3. SVD-based Watermarking Schemes

3.1 Classification of SVD based Watermarking Techniques

SVD based watermarking algorithms can be categorized into following four groups.

A. Watermarking techniques which cast the watermark or its singular values into the singular values of the host image.

B. Watermarking methods which embed the watermark by modifying the right/left singular vectors of the host image.

C. Watermarking algorithm based on modification of singular values as well as singular vectors.

D. Hybrid transform domain techniques, which combine SVD transform (singular vectors/values) with others transforms like DFT, DCT, DWT, Zernike Moments Transform, Haar Transform, Hadamard Transform etc.

3.2 Watermarking Techniques based on Singular Values

There are two types of pure SVD based algorithms. In some watermarking schemes, watermark is embedded into the whole cover image. In other schemes the cover image is divided into several blocks and the watermark is embedded into each block of the cover image separately. Many of the earlier algorithms, based on SVD, used to embed the watermark signal directly into the singular matrix. Liu and Tan [4] proposed an algorithm where the watermark image is embedded directly in the singular values of host image.

The major problem arising in SVD based watermarking schemes based on the singular values only, is its vulnerability to the SVs substitution attack. Zhang and Li [9] showed that watermarking algorithms which are based on modifying the singular values are fundamentally flawed and have watermark ambiguity problem.

For example two possible attack scenarios concerning SVs based watermarking schemes:

1. When two different owners cast different watermarks in two different images say A and B. Then singular matrix of A can be replaced by singular matrix of B and vice-versa, thereby changing the ownership of both images. This does not allow to solve the rightful ownership problem.
2. In the second scenario, only image B is watermarked and image A is left as it is. The substitution of its SVs of B with those of an unmarked image A causes the watermark removal from B and by consequence, a failure in proving the rightful ownership of B.

Many watermarking schemes which insert the watermark by modifying the SVs of the host image are facing these problems. This has been illustrated analytically and experimentally in various articles [9-11]. Further it is worth to mention that in case of block based watermarking techniques, to increase the payload of these schemes, the host image is split into small blocks. This fact lowers the robustness against common attacks since the stability of the SVs decreases on reducing the size of the blocks.

3.3 Watermarking Techniques based on Singular Vectors

Chang [7] proposed a watermarking scheme in which U matrix is used for watermark insertion. In the first stage entire image is divided into non-overlapping blocks. For each block SVD is applied and rank of S matrix of each block is determined to find the complexity of each block. Blocks with higher rank, i.e with higher complexity are selected for watermark embedding. In the second stage, the absolute difference between two rows of U matrix is modified according to pseudorandom sequence. In [12], the authors proposed a similar watermarking scheme except for the use of the *V* matrix in the embedding process. To improve the security, the components from the first column of the matrices *U* and *V* are randomly selected using a secret key. According to chung et al. [11] if the watermark is embedded in the columns of U matrix and rows of V matrix, the perceptibility of host image is improved, but it is not robust. This is because magnitude of U and V matrix elements are very small.

3.4 Watermarking Techniques based on Singular Values and Singular Vectors

Chandra et.al [13] proposed a method in which both S and U matrix are utilized for watermark insertion. The watermark image is partitioned into four blocks. SVD transform is applied block wise on the upper left block and watermark is embedded in the largest SV of each block by means of quantization. Again block based SVD transform is applied to bottom right image and watermark is inserted into columns of U matrix of each transform as per Chungs [11] algorithm.

3.5 Hybrid Transform Domain Techniques

SVD based watermarking schemes discussed so far are pure SVD based algorithms because in those algorithms watermark is embedded in SVD domain of the cover image.

Some algorithms have used different types of transform like DCT, DWT, Complex wavelet transform etc along with SVD domain for watermarking scheme which can be defined as hybrid SVD based algorithms.

4. Proposed Watermarking Scheme with Face Features as a Watermark

This paper proposes invisible semi blind watermarking scheme in which it first extracts the face image features using PCA. These features are then embedded using block-based watermarking scheme, which uses SVD transform of host image. Watermark embedding approach is based on singular vectors suggested by [14]. The proposed watermarking scheme works by initially splitting the original image into non-overlapping blocks, applying the SVD transform to each of the block and subsequently embedding a watermark into the singular vectors. Each watermark value is embedded by modifying a set of singular vector angles, i.e., angles formed by the right singular vectors of each block with respect to some axis in arbitrary plane. The orthogonal property of the right singular vectors matrix is preserved during embedding process. After extracting the features from watermarked host image, it is correlated with face database features to get the approximately correct face image.

4.1 Consideration for Proposed Watermarking Algorithm

Following are the parameters considered while implementing this watermarking scheme.

1) Block size: This watermarking algorithm performs a block-wise SVD transform on the original image. Block size is one of the important factors which affects the properties and behavior of the watermarking algorithm. Generally blockwise transform gives more robust features against signal processing operations than global transform. In case of SVD transform, the stability and implicitly the robustness of the singular values and vectors depends on the size of the segmentation block. Higher is the block size, better is the stability of singular values. The SVD transform produces highly stable features when performed on large blocks of image. The attacks which are very sensitive to the segmentation size are JPEG compression and addition of white Gaussian noise or salt and pepper noise. On the other hand, by splitting the cover image into small blocks, data embedding capacity increases. It is very crucial to optimize the block size. The block size is governed by following considerations:

i) Sufficiently enough block size to embed face features.

ii) High speed of computation of the SVD.

iii) Maintaining good visual quality of the watermarked image.

2) Sign ambiguity: Singular vectors are affected by a form of ambiguity called sign ambiguity that is the SVD arbitrarily assigns the sign of each singular vector [15]. Even though it makes no difference mathematically, the current arbitrariness in the sign convention has important and significant ramifications in signal processing applications. In the proposed scheme, the sign ambiguity of the singular vectors changes the sign of their components which are used in the detection process to recover the embedded watermark angle. It can modify the extracted feature set to such an extent that it becomes impossible to correctly extract the watermark. To solve this ambiguity the algorithm proposed in [15] is applied on singular vectors, which determine the sign of a singular vector by computing the sign of the inner product of this vector and individual data vectors taken from the data set, that is, in our case, the original image. With the proposed solution, good results are obtained when the inner products are not close to zero. Instead, to avoid an arbitrary sign assignment when the inner products are close to zero, the algorithm considers the combined magnitudes of both left and right singular vectors.

3) QR decomposition: The computation of SVD is based on QR decomposition. The QR decomposition performs the orthogonal-triangular decomposition of a matrix. It expresses the matrix as the product of a real orthonormal or complex unitary matrix and an upper triangular matrix.

Watermarking scheme contains following four phases:

1) Face feature extraction.
2) Feature embedding in host image to form watermarked image.
3) Feature extraction from watermarked image.
4) Recognizing face image from extracted features

4.2 Phase I (Face feature extraction)

In this phase, face features of face image are extracted using Principal Component Analysis method. Eigen space is created using PCA algorithm for a given database of face images [19].

Let FI represents the face image of size MxN and there are N_T such face images. The feature extraction process for face from a given database is as follow:

1) Form a Face Database (FD) of face images (N_T images each of size MxN) with each image representing one column of that matrix FD_{MxNxN_T}
2) Centralize the FD by subtracting the Mean Vector MV_{MxNx1} and form centralized database of face image called as CFD.

$$MV_i = \frac{1}{N_T}\sum_{j=1}^{N_T} FD_j \qquad i = \cdots (MxN) \tag{3}$$

$$CFD = FD_i - MV \qquad i = \cdots (MxN) \tag{4}$$

3) Find the Covariance Matrix CM

$$CM = CFD^T xCFD \tag{5}$$

4) Find out Eigen vectors and Eigen values of the covariance matrix CM

$$[V\ D] = eig(CM) \tag{6}$$

5) Sort and eliminate Eigen values. All Eigen values of matrix CM are sorted and Eigen vectors corresponding to Eigen values greater than one are selected.
Let EGV represents the eigenvectors of CM after eliminating.
6) Create Eigen space ES by projecting centralize the image data base CFD on Eigen vectors EGV

$$ES = CFDxEGV \tag{7}$$

Entire face database is projected on Eigen space to create Face Feature Set ‘FFS’.

Any face image whose features are to be embedded as a watermark is projected on Eigen space and feature vector generated is called Face Feature Vector ‘FFV_{NFx1}’ which is used as a watermark, where ‘NF’ is the number of features generated and is the length of watermark.

4.3 Phase II (Feature embedding in host image to form watermarked image)

In this phase, face features extracted from face image are embedded in host image H redundantly by using Block based and QR based SVD. Host image is divided into number of blocks equal to number of features. For each block one watermark feature is embedded. Watermark is added as an angle in the projection angle of selected vector with respect to some axis defined by arbitrary plane. Two vectors and plane are selected by using Key. Thus security is provided. After adding watermark to each block all blocks are collected together to form watermarked host image.

Watermark Embedding Steps are as follows:

Step 1: Let Host image is represented by $H_{P\,X\,Q}$.

Face Feature vector for watermark image is $FFV_{(NF)X\,1}$

As watermark is embedded redundantly, $FFV_{(NF)X\,1}$is replicated to get FFV_{LX1} such that its length is a square integer number.

Let L= NF1 X NF1.

Feature vector in database FFS are also set to length L.

Step 2: Divide Host image matrix $H_{P\,X\,Q}$ into L no. of blocks $B_{(\mathrm{P/NF1\;X\;Q/NF1})}$ to embed one feature in each block. Let W_b represent one component of face feature watermark which has to be embedded in one block.

Let m = P/NF1 and n = Q/NF1.

For each block B_i of size m x n, use step 3 to 10 and collect all the blocks to form watermarked host image.

Step 3: Find QR decomposition of block $(B_i)_{m\,X\,n}$ and then SVD of $R_{m\,X\,n}$ will generate 3 matrices U, S and V using svd standard function as follows:

QR Decomposition gives [17]:

$$[Q_{m\,X\,m}R_{m\,X\,n}] = QR((B_i)_{m\,X\,n}) \tag{8}$$

SVD Decomposition gives:

$$[U_{m\,Xm}S_{m\,X\,n}V_{n\,X\,n}] = \mathrm{SVD}(R_{m\,X\,n}) \tag{9}$$

Step 4: Apply sign flip function to avoid sign ambiguity problem to (QUS) and (V) [15].

Let $\mathrm{LD1} = (\mathrm{QUS})$

Step 5: Let a key KT gives 4 values i, j , k, l where V_i and V_j are vectors of V and V_k and V_l be the components on V_i and V_j used to compute the secret plane P(k, l)

$$x = V_{ki} \quad , \quad y = V_{li} \quad , \quad z = V_{kj} \quad , \quad w = V_{lj}$$

Step 6: Compute angle θ_b derived by projection vector V_i with positive axis k i.e. $\angle(\mathrm{k}, \mathrm{proj}_{\mathrm{P(k,\;l)}}\, V_i)$ defined by the components x and y using tangent inverse function:

$$\theta_b = \frac{\mathrm{atan(y/x)}}{\delta} \tag{10}$$

Scaling factor δ is used to obtain a feature angle that is in the range of–π/2 and π/2. θ_b is inserted into in the feature set as FR = $[\theta_1, \theta_2 \ldots \theta_L\ ]$

Step 7: The angle α_b is computed as follows which add W_b feature vector as angle to θ_b with strength factor β.

$$\alpha_b = \theta_b + \beta . W_b \tag{11}$$

W_b represents one component of face feature watermark which has to be embedded in one block and β is the strength of watermark varies between π/4 to π/6

Step 8: Determine the rotation angle φ_b, which is needed to rotate the vector V_i in the plane $P(V_i,\ V_j)$ so that $\alpha_b = \angle(k, \mathrm{proj}_{P(k,l)} V_i')$. To obtain this result following relation is used (see Appendix):

$$\varphi_b = \mathrm{atan}\left(\frac{x.\sin\alpha_b - y.\cos\alpha_b}{z.\sin\alpha_b - w.\cos\alpha_b}\right) \tag{12}$$

To maintain orthogonal property of matrix V, vector V_j is also rotated by same angle. Refer Figure 1 for visualization of vectors and their rotation by an angleφ_b.

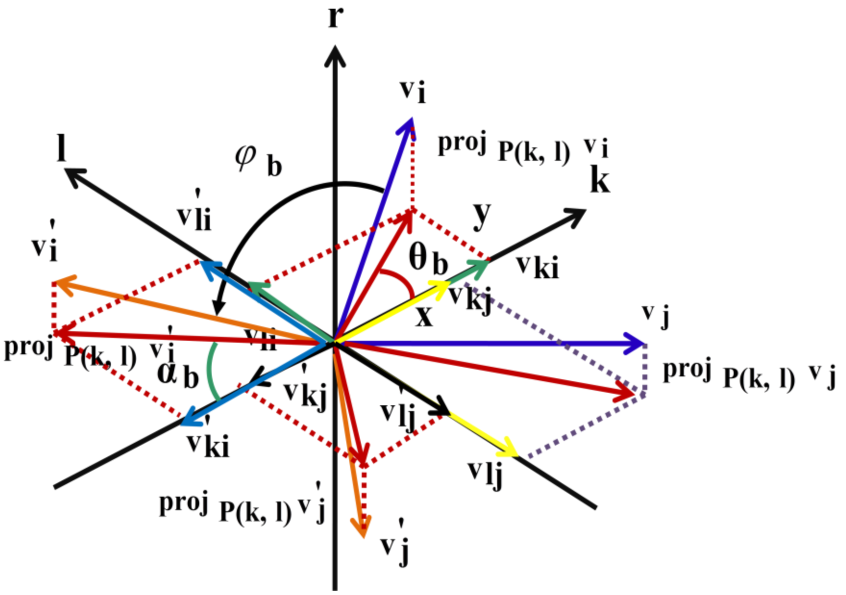


Figure 1. Pictorial representation of the vectors and their angles formed with respect to axis in arbitrary plane, involved in the watermark embedding

Step 9: Apply the transformation matrix G_b, which rotates a single pair of right singular vectors, i.e. V_i and V_j, in the plane P $(V_i\ , V_j)$, by an angle φ_b,

$$V' = (V)G_b^T \tag{13}$$

V' = modified matrix of the right singular vectors.

Step 10: Reconstruct the modified watermarked image block using V'.

$$B_i' = (LD1)\, V'^T \tag{14}$$

4.3 Phase III (Feature extraction from watermarked image)

In this phase embedded features are extracted from watermarked image H using same block based SVD algorithm as used for watermark embedding. Here the embedded angle is computed back again by using same vectors and plane given by the key. Computed angle is then used for reconstructing embedded face features.

Step1: Repeat step 2 – 5 of Phase II for watermarked image WH.

Step 2: Compute angle θ_b derived by projection vector V_i' with positive axis k i.e. $\angle(\mathrm{k}, \mathrm{proj}_{P(k,\ l)}\ V_i'\ )$ defined by the components x and y using tangent inverse function:

$$\theta_b = \mathrm{atan}\left(\frac{y}{x}\right) \tag{15}$$

θ_b is inserted into in the feature set FR1 = [θ_1, θ_2 .. θ_L]

Face feature watermark is extracted from feature set FR1 using following formula.

$$\mathrm{RF} = \frac{\mathrm{FR1} - \mathrm{FR}}{\beta} \tag{16}$$

4.4 Phase IV (Recognizing face image from extracted features)

The angles extracted from each block of the image in phase III are the embedded face features. They are correlated with each of the features of face data base. Parameters such as threshold 'TH' and quality statistic 'q' are calculated for all images in the database. These parameters are used to recognize closest face image.

Steps to recognize set of face images approximately close to embedded image from extracted features are as follows[18].

Step 1: Use retrieved features RF from Phase III and face feature Set FFS of face image data base obtained from Phase II step 1 to find threshold 'TH' and quality statistic 'q' for each face image in data base as follows.

Let L = NF1 X NF1, is the length of redundant feature vector which is extracted.

The quality statistic 'q' is given as

$$q_j = \frac{\sum_{i=1}^{L} Y_{ij}}{\mathrm{Vary_j}\sqrt{L}} = \frac{\mathrm{MeanY_j}\sqrt{L}}{\mathrm{Vary_j}} \qquad \text{for } j= 1\ldots..N_T \tag{17}$$

Where Y_{ij} is given as

$$Y_{ij} = \sum_{i=1}^{L}(FFV^{*})_i^{\,T}\left(\mathrm{FFS_{ij}}\right) \quad \text{for} \quad j = 1 \ldots N_T \tag{18}$$

$\mathrm{MeanY_j}$ and $(\mathrm{Vary_j})^2$ are the mean and variance of j^{th} feature set correlated with extracted feature.

$$\mathrm{MeanY_j} = \frac{\sum_{i=1}^{L} Y_{ij}}{L} \qquad \text{for } j = 1 \ldots N_T \tag{19}$$

$$(\mathrm{Vary_j})^2 = \frac{\sum_{i=1}^{L}(Y_{ij} - \mathrm{MeanY_j})^2}{L-1} \qquad \text{for } \quad j = 1 \ldots N_T \tag{20}$$

Intuitively we can understand that value of q_j is like a correlation between extracted features and feature set of face image data base.

Threshold (TH) is computed as follows:

$$\mathrm{YT_j} = \beta.\sum_{i=1}^{L}(\mathrm{FFS_{ij}})\ (\mathrm{FFS_{ij}}) \quad , \text{ for } j = 1 \ldots N_T \tag{21}$$

Mean and variance of $\mathrm{YT_j}$ is computed using Eq. (17) and (18) respectively.

$$\mathrm{mH_j} = \frac{\mathrm{YT_j}}{\mathrm{VaryYT_j}.\sqrt{\mathrm{L}}} \qquad \mathrm{j} = 1 \ldots \mathrm{N_T} \tag{22}$$

Implicitly, $\mathrm{mH_j}$ is like a autocorrelation of feature sets of face image data base. The threshold value TH is set half of the $\mathrm{mH_j}$.

$$\mathrm{TH_j} = \frac{1}{2}\,\mathrm{mH_j} \qquad \mathrm{j} = 1 \ldots \mathrm{R} \tag{23}$$

Step 2: Find image having q >= TH. This face image will be the closest match for the embedded face image.

It is possible that the above condition is held true for multiple face images. Among those images for which the difference q-TH is highest, gives the best match of face image whose face features are embedded as a watermark.

5. Experimentation and Results

Implementation of this watermarking scheme is tested to show the robustness of the proposed scheme against different attacks like salt and pepper noise, JPEG compression, brightness, cropping, row column blanking, row column copy, Additive White Gaussian Noise, and histogram equalization. Experimental results are obtained by taking five gray scale host images of 512 X 512 pixels. These images are split into 32 blocks per image, each block of size 16X 16 pixels.

The watermark is a face feature of face image of size 1024 obtained by applying PCA on train database of images containing 56 images of 7 persons. Indian face database is used for experimentation [20]. For this implementation redundant watermark is used. The values of the watermark represent a sequence of angles, in radians, which are used to rotate a specified pair of right singular vectors of the matrix V in every block. The strength of watermark β is varied between π/4 to π/6 which represents a compromise between the strength of the inserted mark and the quality of the watermarked image. Increasing the value of β implies larger variation in rotation angle thereby decreasing the image quality. Based on experimentation Scaling factor δ is set to four. By means of the secret key K, initially the 6th and 7th right singular vectors are selected from each block. For convenience the indices k and l are set to the same values. In further experimentation, different pairs of vectors are involved for rotation. It is recommended to avoid the rotation of 2nd and 3rd vectors, as it contains the prominent information of the image. The quality measure used to compute the amount of distortion introduced by the embedding process is the Peak Signal-to-Noise Ratio (PSNR). Using 5 host images, the average PSNR for the proposed scheme is computed, whose value is higher than 46 dB. A sample of the original image and watermarked image is presented in Fig. 2. It is observed that no visual artifacts are observed in the watermarked image. It is also observed that extracted face features, when correlated with faces features from database recognize correct face.

To check the rate of false detection of extracted watermark, the experimentation with two hypothesis H0 and H1 is carried out. The distribution of quality statistic q under the hypothesis H0 and H1 was verified using five different host images with face feature set of five different face images. Under hypothesis H0 the presence of these watermarks is checked by correlating 5 face feature set with the original un-watermarked image. On the other hand in hypothesis H1, five watermarks are embedded separately in five different host images, and subsequently applied the detection process. The distribution of quality statistic 'q' under hypothesis H0 and H1 is presented in Figure 3.

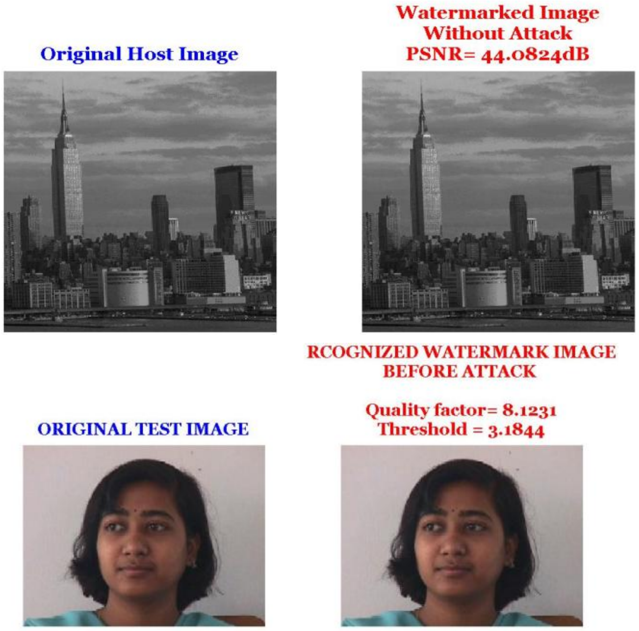
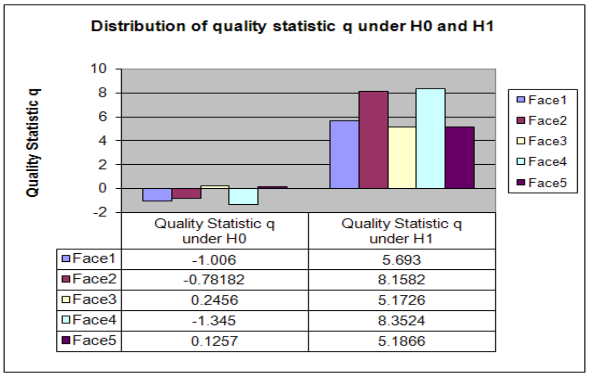


Figure 2. Original Host and watermarked host without attack with PSNR = 44.08 dB and face image whose features are embedded and recognized face image

From Figure 3, it is clear that the distributions of the output statistic 'q' in both null and alternative hypothesis are well separated. Thus, it is obvious that many thresholds between these distributions will yield both low false negative and false positive errors. For the detection of exact face features, the test statistics q is compared with the acceptance threshold TH, computed as a function of the mean of the distribution of q under the hypothesis H1. The ideal acceptance threshold for which the exact face features recognition errors are extremely low is TH_{ideal}= (mH1)/2.



	Quality Statistic q under H0	Quality Statistic q under H1
▪Face1	-1.006	5.693
▪Face2	-0.78182	8.1582
□Face3	0.2456	5.1726
□Face4	-1.345	8.3524
▪Face5	0.1257	5.1866

Figure 3 Distribution of Quality Statistics (q) under hypothesis H0 and H1

There are various attacks against which watermarked images were tested for its robustness and the average of the quality statistic q in each case is reported in Table 1.

`

Table 1. Robustness of the Proposed Scheme Against Common Attacks

Sr. No	Attacks	Factor	Average Quality Statistics q
1	Salt & Pepper	0.002	2.460356
2	Cropping	30%	2.36152
3	JPEG Compression	95 to 70	1.7090664
4	Row-Column Blanking	Cols= 50,99,192,300	3.594596
		Rows = 14, 169, 119, 320	
5	Row-Column Copying	Cols = 211-123, 256-11, 455-169, 359-50	3.048648
		Rows = 123-211, 11-256, 169-455, 359-50	
6	Brightness	0.8	3.136092
		1.2	3.584296
7	Scaling	Sx=0.8 Sy=08	0.0983364
8	Additive white Gaussian	1%	0.465846
9	Histogram Equalization		1.1402656

From the values of quality statistics ’q’ mentioned in the Table1, it gives low values for scaling and Gaussian noise, which indicates that watermark, may not survive under these attacks. Comparing the method with [14], it embeds pseudorandom sequence as a watermark and second is that it detect only underlying media is watermarked or not. On the contrary presented scheme embed the face feature watermark which is extracts the watermark and correlate with the face database for the identification purpose.

6. Conclusion

The study proposes a novel data hiding technique using an amalgamation of face recognition and watermarking. The watermarking algorithm discussed in this paper was developed with an objective of creating secure watermarking scheme for digital images for transaction tracking. This watermarking scheme records the recipient face feature in each legal sale or distribution of original media, where all legal recipients face database is maintained at owner’s side.

In this scheme original media is not required in the detection process for resolving legal ownership. This scheme preserves the orthogonal property of the singular vectors during the watermark embedding step, which permits a smooth recovery of the watermark. Left singular vectors can also be used for watermarking. It enlarges the space required for embedding and thus provides more security and possibility to insert watermark redundantly.

7. Future Work

The performance of this watermarking technique is tested by applying various attacks of watermarked image to test robustness and security and other features of digital watermarking. The current study can be extended to improve the robustness against geometric attacks using RST invariant transform like complex wavelet transform and Zernike moments. Fast PCA algorithm can be implemented for face feature extraction to increase speed of processing large face database. This approach can be extended for applications like biometric passport, where face features can be embedded in travel documents for validation, verification and prevention with regard to international security. In such application face features can be embedded in a machine readable zone. Technique can also be used to embed the face features in smartcard. At the access point extracted features can be verified with face features of the online captured face to allow the access. For a huge database of face image the computational speed of feature extraction process can be reduced using parallel computing using GPU platform.

References

[1] A. K. Jain and U. Uludag, "Hiding Biometric Data", IEEE transaction on Pattern Analysis and Machine Intelligence, Vol. 25, No.11, pp.1494-1498, **(2003)** November.

[2] L. Hong , A. Jain, "Integrating faces and fingerprints for personal Identification", IEEE transactions on Pattern Analysis and Machine Intelligence, Vol. 20, No. 12 , pp. 1295-1307, **(1998)** December.

[3] A. K. Jain, A. Ross and S. Prabhakar", An introduction to Biometric Recognition", IEEE transaction on Circuits and Systems forVideo Technology , Vol. 14, No. 1, pp. 4-20, **(2004)** January.

[4] R. Liu and T. Tan, "An SDV based Watermarking Scheme for Protecting Rightful Ownership", IEEE transactions on Multimedia, Vol. 4, No. 1, **(2002)** March.

[5] J. M. Shieh, D. C. Lou and M. C. Chang, "A semi-blind digital watermarking scheme based on singular value decomposition", Computer Standards and Interfaces, Elsevier, 28, pp. 428-440, **(2006)** April.

[6] H. C. Andrews and C. L. Patterson, "Singular value decomposition(SVD) image coding", IEEE transaction on Communication, Vol. 24, pp. 425-432, **(1976)** April.

[7] C. Chang, P. Tsai and C. Lin, "SVD based Digital watermarking Scheme", Elsevier Pattern recognition letters 26, pp. 1577-1586, **(2005)**.

[8] B. C. Mohan, S. Srinivaskumar and B. N. Chatterji, "A Robust Digital Image Watermarking Scheme using Singular Value Decomposition (SVD), Dither Quantization and Edge Detection", ICGSTGVIP Journal , 8, pp. 17–23, **(2005)**.

[9] X.-P. Zhang and K. Li, "Comments on SVD-Based Watermarking Scheme for Protecting Rightful Ownership", IEEE transaction on Multimedia , Vol. 7, No. 2, **(2005)** April.

[10] Y. Wu, "On the security of an SVD Based Ownership watermarking", IEEE transaction on Multimedia, Vol. 7, No. 4, **(2005)** August.

[11] K.-L. Chung, W.-N. Yang, Y.-H. Huang, S.-T. Wu and Y.-C Hsu, "On SVD-based watermarking algorithm", Elsevier ,Applied. Mathematics Computation, pp, 54–57, **(2007)**.

[12] J. C. Patra, W. Soh, E. L. Ang and P. K. Meher, "An Improved SVD-Based Watermarking Technique for Image and Document Authentication", Proceeding international Conference on Circuits and Systems (*APCCAS 2006)*, IEEE Asia Pacific, Singapore,, pp. 1984–1987, **(2006)** December 4-7.

[13] B. Chandra Mohan and S. Srinivas Kumar, "A Robust Image Watermarking Scheme Using Singular Value Decomposition", Journal of Multimedia, Vol. 3, No.1, **(2008)** May.

[14] A. Basso, F. Bergadano, D. Cavagnino, V. Pomponiu and A. Vernone, "A Novel Block-based Watermarking Scheme Using the SVD Transform", Algorithms, 2, pp. 46-75**, (2009)**.

[15] R. Bro, E. Acar and T. G. Kolda, "Resolving the sign ambiguity in the singular value decomposition", Journal Chemometrics,Wily interscience, 22, pp. 135-140, **(2008)**.

[16] S. Craver, D. N. Memon, B. L. Yeo and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications", IEEE Journal on Selected Areas in Communications, California, USA,, Vol.16, pp. 573-586, **(1998)** May.

[17] E. Anderson, Z. Bai, C. Bischof, S. Blackford, J. Demmel, J. Dongarra, D. J. Croz, A. Greenbaum, S. Hammarling, A. Mckenney and D. Sorensen, "LAPACK User's Guide", third edition. SIAM: Philadelphia, Philadelphia, USA.

[18] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownership of digital images", IEEE transactions on Image Processing, Piscataway, New Jersey, USA,; Vol 8, No.11, pp. 1534-1548, **(1999)** November.

[19] V. Perlibakas, "Face Recognition Using Principal Component Analysis and Wavelet Packet Decomposition", INFORMATICA,, Vol. 15, **(2004)**.

[20] http://vis-www.cs.umass.edu/~vidit/IndianFaceDatabase/.

Appendix

The angle α is the projection of vector $\mathrm{V_i}$ with positive axis K after watermark embedding. During the extraction process, we are expecting the same angle formed by vector $\mathrm{V_i}$ with positive k axis. To achieve this, we have to rotate vector $\mathrm{V_i}$ by an angle Ø so that its projection on plane P(k,l) will form the angle α with k axis. For this we have found the relation between Ø and α. This can be found by rotation transformation as given below.

$$\begin{bmatrix} \cos\emptyset & -\sin\emptyset \\ \sin\emptyset & \cos\emptyset \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x', \\ y \end{bmatrix}$$

The matrix V is a orthogonal matrix. The condition for orthogonal is maintained by rotating another vector $\mathrm{V_j}$ in the plane by same angle.

Vector $\mathrm{V_{ki}}$ and $\mathrm{V_{li}}$ are the two components of vector $\mathrm{V_i}$ on the two axes K and l before rotation.

The angle formed is $\theta = \mathrm{atan}\,(\mathrm{V_{li}}, \mathrm{V_{ki}})$

Let *l* and *k* represents the rows and *i* and *j* represents the column given by the key. Then after the rotation the two components of the vector v_i are:

1. l^{th} component: $v_{li}\cos\varphi - v_{lj}\sin\varphi$
2. k^{th} component: $v_{ki}\cos\varphi - v_{kj}\sin\varphi$

$$\tan\alpha = \frac{v_{li}\cos\varphi - v_{lj}\sin\varphi}{v_{ki}\cos\varphi - v_{kj}\sin\varphi}$$

$$\mathrm{x} = \mathrm{V_{ki}} \quad , \quad \mathrm{y} = \mathrm{V_{li}} \quad , \quad \mathrm{z} = \mathrm{V_{kj}} \quad , \quad \mathrm{w} = \mathrm{V_{lj}}$$

$$\tan\alpha = \frac{\mathrm{y}\cos\emptyset - \mathrm{w}\sin\emptyset}{\mathrm{x}\cos\emptyset - z\sin\emptyset}$$

$$\tan\alpha = \frac{y - \mathrm{w}\tan\emptyset}{x - z\tan\emptyset}$$

$$\mathrm{x}\tan\alpha - ztan\emptyset\, tan\alpha = y - w\, tan\emptyset$$

$$\mathrm{x}\tan\alpha - y = ztan\emptyset\, tan\alpha - w\, tan\emptyset$$

$$\mathrm{x}\tan\alpha - y = tan\emptyset[ztan\alpha - w]$$

$$\tan\emptyset = \frac{x\, tan\alpha - y}{z\, tan\alpha - w}$$

$$\tan\emptyset = \frac{x\, sin\alpha - \mathrm{y}\cos\alpha}{z\, sin\alpha - wcos\alpha}$$

Authors

Vandana Inamdar is a Ph.D scholar in College of Enginering, Pune University, India. She received bachelor and master degree from Shivaji University and Pune University respectively. More than twelve research papers in various international journals and reputed conferences are there to her credit. Her area of research is image processing, Multimedia applications and GPU computing.

Priti P. Rege received the B.E. and M.E. (Gold medal) degrees from Devi Ahilay University of Indore, India, and the Ph.D. degree from the University of Pune, India, in 2002. Since 1989, she has been with the College of Engineering, Pune, where she is currently working as a Professor in the Department of Electronics and Telecommunications. Her research interests include signal processing and pattern recognition. Several of her papers have appeared in leading journals and conferences. Dr. Rege was the recipient of “Nagarkar Fellowship” for carrying out research in subband coding of images.