Biometric Template Protection With Robust Semi – Blind Watermarking Using Image Intrinsic Local Property

Mita C. Paunwala *mpaunwala@yahoo.co.in*
Assistant Professor, ECC dept.
C.K.Pithawala college of Engg. & Tech.
Surat, 395007, India

Suparva Patnaik *ssp@eced.svnit.ac.in*
Professor, ECED
S V National Institute of Technology
Surat, 395007, India

Abstract

This paper addresses a biometric watermarking technology sturdy towards image manipulations, like JPEG compression, image filtering, and additive noise. Application scenarios include information transmission between client and server, maintaining e-database and management of signatures through insecure distribution channels. Steps involved in this work are, a) generation of binary signature code for biometric, b) embedding of the binary signature to the host image using intrinsic local property, that ensures signature protection, c) host image is then made exposed to various attacks and d) signature is extracted and matched based on an empirical threshold to verify the robustness of proposed embedding method. Embedding relies on binary signature manipulating the lower order AC coefficients of Discrete Cosine Transformed sub-blocks of host image. In the prediction phase, DC values of the nearest neighbor DCT blocks is utilized to predict the AC coefficients of centre block. Surrounding DC values of a DCT blocks are adaptively weighed for AC coefficients prediction. Linear programming is used to calculate the weights with respect to the image content. Multiple times embedding of watermark ensures robustness against common signal processing operations (filtering, enhancement, rescaling etc.) and various attacks. The proposed algorithm is tested for 50 different types of host images and public data collection, DB3, FVC2002. FAR and FRR are compared with other methods to show the improvement.

Keywords: Biometric Watermarking, Image Manipulation, Edge Block Analysis, Fingerprint Matching, Security System.

1. INTRODUCTION

Biometric technologies are defined as automated methods of identifying or authenticating the identity of a person based on unique physiological or behavioral characteristics. Biometric technologies used in well-designed ID systems ensure that the individual presenting a secure ID credential has the absolute right to use that credential. Biometric watermarking applications are broadly classified into two categories. In one scenario one biometric is embedded in another, which merely acts as a carrier to secure the former genuine biometric. In the second scenario, two biometrics first one embedded in the second biometric is further encoded in smart cards to enhance the security. Smart ID cards often provide the secure, convenient and cost-effective ID technology that stores the enrolled biometric template and compares it to the "live" biometric template. Smart cards are finding their applications in identification areas such as driving licenses, national identity cards, electronic passports, new generation credit cards, driving licenses etc. A secure ID system using smart card and biometric technology provides:

- Enhanced privacy, securing information on the card, allowing the individual to control access to that information and removing the need for central database access during identity verification.
- Improved system return on investment through the flexibility and upgradability that smart cards provide, allowing support of different authentication methods and multiple, evolving applications.

Ratha et al. [1] produce a generic biometric system with eight possible sources of attacks. The hierarchical positions of attacks are shown in the figure 1. These attacks can be any one or more from the followings, fake biometric (fake finger, a face mask etc), an old recorded signal (old copy of fingerprint, recorded audio signal of a speaker etc.), a feature extractor could be forced to produce feature value chosen by attacker than that of the actual one, synthetic feature set, artificially match score, manipulated template and a channel between stored template and matcher change the content of the stored template. All of these attacks decrement the overall efficiency of the system.

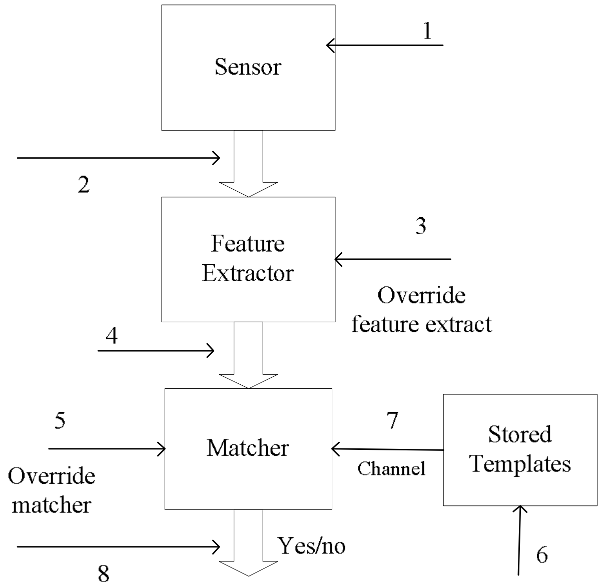


FIGURE 1: Generic biometric based system with possible attacks [2].

In [2] author points out that a biometrics based verification system works properly only if the verifier system gives guarantee that the biometric data came from the genuine person at the time of enrollment and also at the access time of the system. Though biometric data gives uniqueness to the person, it is not secure. However the user will not learn that his/her biometric is revealed as he/she leaves fingerprint on surface he/she touches and the face of the person can be easily captured by camera. As a solution to attacks at level 6, 7 and above mentioned problem we proposed an idea to hide biometric data into an visually uncorrelated host image to reduce the manipulation rate.

Many of the biometric security system have been proposed and reviewed in [3] [4] [5] [6] etc. Compared with other biometrics features, the fingerprint technique is the most solicited and has the largest market shares as well as it can be easily used and their features are highly reliable. There are several watermarking techniques which have been proposed and experimented with promising methods for copyright protection, authentication and other applications. Most of the recent work in watermarking can be grouped into two categories: spatial domain methods [7], [8], [9] and frequency domain methods [10], [11] and [12]. There is a current trend towards approaches that make use of information about the human visual system (HVS) to produce a more robust watermark. Such techniques use explicit information about the HVS to exploit the limited dynamic range of the human eye and are presented in [13] [14] and [15].

There have been only a few published papers on biometric watermarking of fingerprint images. In [16] author proposed Bio-hashing and cancelable fingerprint template transformation techniques based on six metrics to protect biometric trait, facilitates the security evaluation and vulnerable to linkage attacks. In [17] author proposed multiple watermarking algorithm in texture regions of fingerprint image using discrete wavelet transform. They used Face and text information as watermark. Their approach is resilient to common attacks such as compression, filtering and noise. In [18] spatial domain fragile watermarking method for fingerprint image verification was proposed. The method can localize any region of image that has been tampered. Authors conclude that their watermarking technique does not lead to a significant performance loss in fingerprint verification. The fragile watermarking method discussed is used to detect the tampering effect but fail for retrieving original biometric. In [19] author proposed scheme for template protection with steganography in which the secret key (which is in the form of pixel intensities) will be merged in the picture itself while encoding, and at decoding end only the authentic user will be allowed to decode. But author has not discussed sturdiness of algorithm for various channel attacks. In [20], a semi unique key based on local block averages was used to detect tampering of host images, which includes fingerprints and faces. The technique is robust enough to detect even the most minor changes and determine where such changes took place in the image. In [21] two spatial domain watermarking methods for fingerprint images are used, in which the first method utilizes gradient orientation analysis in watermark embedding and second method preserves the singular points in the fingerprint image. Multiple times embedding of watermark results in almost accurate retrieval of watermark but it fails against compression and rotation attacks since watermarking approach is in special domain.

Our proposed algorithm is intended for applications like electronic passport (Fig.2). The e-passport represents a major shift in passport technology, with the introduction of semiconductor chips and biometrics. The major security issues that need to be addressed while using a contact less chip to store secure information are skimming, eavesdrop ping, cloning etc. The problem can be solved by providing ID card along with user fingerprint data hidden inside, instead of having chip. The verification requires simultaneous submission of the live biometric and ID card. At an access control site, the same biometric, for example the fingerprint of the person possessing the card, will be sensed and at the same time the fingerprint feature hidden inside the card (Fig.2) is extracted for matching. Person identified as genuine or pretender based on match score obtained by proposed matching algorithm. Our approach can be used for other application in which user gives pin code/password and based on that, biometric data of particular user is accessed from data base and match with biometric of user present at the place (dash-dot line representation in Fig.2). However the idea can be extended for other trait or multimodality. An application scenario with various components is shown in Fig.2. It also presents interconnection of various sections.

Section 2 describes the detailed approach of minutiae extraction algorithm. Section 3 and 4 explains the proposed watermarking and matching algorithm respectively. The results obtained and concluding remarks are illustrated in section 5.

2. FINGERPRINT MINUTIAE EXTRACTION

In this work our main inclination is towards hiding of biometric template. This section briefly explains fingerprint minutiae (biometric template) extraction technique. To employ fingerprint minutiae extraction step sensed print undergoes few necessary steps. In this work we have routed the raw finger print through steps like a) pre-processing: to extract level fingerprint area and remove the boundary, morphological OPEN operation to removes peaks introduced by background noise and CLOSE to eliminates small cavities generated by improper pressure of fingerprint b) thinning: required to remove erroneous pixels; destroy the integrity of spurious bridges and spurs, exchange the type of minutiae points and miss detect true bifurcations. c) False minutiae removal: required to remove false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking. Furthermore, all the earlier stages themselves occasionally introduce some artifacts which later lead to spurious minutia. Finally, we get the feature vector comprising of minutiae position and orientation, later used for matching purpose.

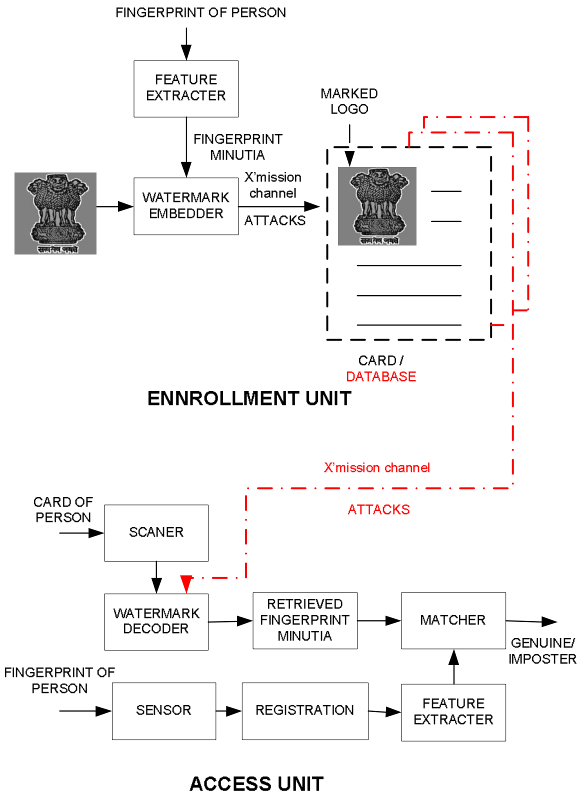


FIGURE 2: Application Scenario.

3. PROPOSED WATERMARKING APPROACH

We have proposed a DCT based semi-blind watermarking technique. In which watermark (fingerprint minutiae template) is embedded by modulating low frequency band AC coefficients of 8 x 8 block by its estimated values. Estimation is done using the DC coefficients of 8 neighboring blocks**.** In [22] authors provide the relation between estimated AC coefficient and neighborhood DC coefficients but not considered the variations in the image for AC coefficient estimation. The proposed method considers the local block variations in the image and accordingly AC coefficients are estimated with different equations. Linear Programming based optimization technique [23] is then considered to calculate weights based on image content. Furthermore each watermark bit is embedded multiple times to ensure robustness against various attacks and signal processing operations.

3.1 Optimization procedure

Any linear program (LP) consists of four parts: a set of decision variables, parameters, objective function, and a set of constraints. The objective function is to fulfill the decision-maker's desire (objective), whereas the constraints which shape the feasible region usually come from the decision-maker's environment putting some restrictions/conditions on achieving the objective.

3.1.1 Block wise DCT Computation

In the proposed approach linear programming based optimization is used to estimate the coefficients using the neighborhood knowledge. Original image X of some arbitrary size M x N is divided into 8 x 8 blocks. Let x_{ij} be a pixel value from the block, then 1≤ i ≤8 and 1≤ j ≤8. Each block is transformed into y_{ij} by applying two dimensional DCT (Discrete Cosine Transform).

Each x_{ij} block is then categorized into smoother block or edge blocks by measuring block variance.

$$v = \frac{\sum_{i=1}^{8}\sum_{j=1}^{8}\left(x_{ij}-\mu\right)^2}{63} \qquad (1)$$

Where μ is mean of block. Variance being very sensitive to uncertainties is used as a decisive parameter to decide the block sensitivity with further uncertainties. The blocks with variance (v) greater than threshold (th) are classified as edge blocks and block variance equal or less than threshold (th) are marked as smoother blocks. Optimization procedure is applied only to smoother blocks. Variance being very sensitive to uncertainties is used as a decisive parameter to decide the block sensitivity towards uncertainties. Watermark embedding causes intensity alteration leading to rise in uncertainties. Blocks with lesser sensitivity are suitable for embedding.

3.1.2 Weight Computation

To calculate the weight, first known AC coefficients values of benchmark images are used. AC prediction method uses unquantized DC values of a 3x3 neighborhood blocks to estimate the AC coefficients for the center block. As shown in Fig. 3 estimation of various AC coefficients of block-5 is done using DC1~DC9.

DC1	DC2	DC3
DC4	DC5	DC6
DC7	DC8	DC9

FIGURE 3: Neighborhood of DCT blocks.

AC components AC(1,2) and AC(1,3) represents the horizontal variations. Hence, DC4, DC5 and DC6 are considered in the objective function. AC components AC(2,1) and AC(3,1) represents the vertical variations. Hence, DC2, DC5 and DC8 are considered in the objective function. AC(2,2) represents the diagonal variations. Hence, DC1, DC3, DC7 and DC9 are considered. Decision variables are K1 to K14. Objective functions to be optimized are given below:

$$\begin{aligned}
AC(1,2) &= k_1 * DC4 + k_2 * DC6 \\
AC(2,1) &= k_3 * DC2 + k_4 * DC8 \\
AC(2,2) &= k_5 * DC1 + k_6 * DC3 + k_7 * DC7 + k_8 * DC9 \\
AC(1,3) &= k_9 * DC4 + k_{10} * DC5 + k_{11} * DC6 \\
AC(3,1) &= k_{12} * DC2 + k_{13} * DC5 + k_{14} * DC8
\end{aligned} \qquad (2)$$

Constraints are -1≤ $k_1, \ldots, k_{14}$ ≤ 1. The solution of the above equation gives optimal weights.

3.1.3 Semi Blind Watermarking Approach

Technique of watermarking proposed here avoids use of host image for watermark detection and hence is blind. Discrete Cosine Transform is not rotation invariant and hence is not robust against rotation attack. As a solution we will transmit principal direction of watermarked image along with it hence is semi blind. Principal direction is the direction along which there are more straight lines. The Radon transform along this direction usually has larger variations. The variance of the projection of Radon transform of the image at this direction is locally maximum. If the variance of the projection has more than one local maximum, we may calculate the second derivative of the variance to distinguish between all local maxima.

As we know, most of the signal energy of the block DCT is compressed in the DC component and the remaining energy is distributed diminishingly in the AC components in zigzag scan order. For watermarking, robustness and imperceptions are the challenges. Hiding of watermark bit in DC co-efficient gives more robustness but perception of watermark is then a major issue and vice versa is true for high frequency AC coefficients.

In our approach we have selected AC co-efficient nearest to DC coefficient for each smoother blocks as in Fig.3, unlike the DC coefficient used in choi's method [24] for hiding watermark (fingerprint minutia). Furthermore we embed each watermark bit multiple times to get robustness. Embedding steps are as given below.

Step 1: Apply radon transform to the host image and calculate the variance for all angles between 0 - 179 degree.
Step 2: Find out local maxima by applying second order derivative. Find out corresponding direction where maximum is projected. The resultant direction is known as principal direction of host image (ϕ_o).
Step 3: Convert minutia points into binary pattern 'w'.
Step 4: Apply 8 x 8 DCT to the host image and categorized edge block and smoother block.
Step 5: Select the AC_i ,1≤ i ≤5 coefficient nearest to its DC coefficient of smoother block and estimates its value ($\hat{AC_i}$) from its neighborhood blocks DC$_j$, 1≤ j ≤ 9 co-efficient as in Eq.(2).
Step 6: Modulate each selected AC coefficient with following translation rule

```
$For\ \ w(k) = 1$
  $if\ \ AC_i > \hat{AC}_i$
    $then\ \ AC_i = AC_i + TH_i$
  $else$
        $AC_i = \hat{AC}_i + TH_i$
$for\ \ w(k) = 0$
  $if\ \ AC_i < \hat{AC}_i$
    $then\ \ AC_i = AC_i - TH_i$
  $else$
        $AC_i = \hat{AC}_i - TH_i$
```

where, TH$_i$ is threshold value which gives robustness against various attacks. Higher the value of TH$_i$, robustness is better but at the same time perceptibility (artifacts) is high. So selection of TH$_i$ is a tradeoff between robustness and imperceptions. Its value is decided locally, as 10-20% of corresponding coefficient.
Step 7: Embed each watermark bit at multiple location.
Step 8: Apply inverse 8x8 DCT with modified AC coefficients values to get watermarked image.

At the decoding side, before extracting watermark bit first find principal direction of watermarked image (ϕ_r). If watermarked image is rotated then principal direction of the watermarked image is different than that of transmitted direction. Take a difference of both direction and de-rotate watermarked image by difference angle (ϕ_d). Decoding of watermark bit requires estimated value $\hat{AC_i}$ of coefficient and original AC_i to extract watermark bit. If $AC_i > \hat{AC_i}$ then extracted bit is '1', otherwise if $AC_i < \hat{AC_i}$ then extracted bit is '0'. Each watermark bit gathered from multiple locations and maximum of that is considered as retrieved bit. The technique proposed here is semi blind watermarking as it requires knowledge of principal direction (ϕ_o).

4. MATCHING APPROACH

Matching stage used here is similar to that proposed in [25], establish the number of consequent minutia pairs to compute the final matching score after alignment. The difference of our approach is only that, we calculates minutiae matching score based on similarity between matching minutiae pair by avoiding triangular matching method and fix feature vector length to avoid complexity. Furthermore, we limit the ridge orientation between 0° and 180°. Matching task can be easily completed, if two minutia patterns are exactly aligned. However, in practice, such a situation is rarely encountered.

Non-linear deformation of fingerprint makes impossible to have exact location of minutia point than that in the template. Also location and direction error makes matching task complex. Therefore, the matching algorithm needs to be elastic which means that it should be capable of tolerating, the deformations due to the location and direction errors and non-linear deformations to some extent. Keeping the above idea as the target, we have proposed a relaxed idea as the part of matching algorithm in this paper.

In alignment stage, the global structure of a minutia describes a rotation and translation invariant feature of the minutia in its neighborhood. The novel structure of each minutia we construct in this paper is not sensitive to noise because it only depends on the global finger print orientation field which is relatively robust to noise. Our structure capturing the affluent information on fingerprint ridge-orientation pattern which is more discriminative than the local minutia structure described in [26].

4.1 Feature Vector Structure

A minutia point *M_k* detected from a fingerprint can be described by a feature vector given by

$$F_k = (x_k y_k \phi_k), \tag{3}$$

Where, (x_k, y_k) describes the location and $Ø_k$ is the ridge orientation. Note that in a fingerprint image, there is no difference between a local ridge orientation of 0° and 180°, since the ridges oriented at 0° and the ridges oriented at 180° in a local neighborhood cannot be differentiated from each other. So, the value of $Ø_k$ is commonly set in the range from 0 to π according to the Eq. (4). Given a minutia point M_k with orientation $Ø_k$, we define a grid structure with N directional metric. Principal axis oriented along the orientation of M_k.

$$\phi_k = \begin{cases} \phi_k & if \;\; 0 \le \phi_k < \pi, \\ \phi_k - \pi & if \;\; \pi \le \phi_k < 2\pi \end{cases} \tag{4}$$

Let $\theta_1 = Ø_k$, $\theta_2 = \theta_1 + 360/N$ and $\theta_N = \theta_{N-1} + 360/N$. We plot N metric along the angles [θ_1, θ_2, θ_3,…θ_N] with respect to X axis through the minutia point M_k as shown in Fig. 4(a). Grid nodes as shown in Fig. 4(b) are marked along each metric at an interval of τ starting with the minutia point M_k. Larger the value of N and smaller the value of τ will increase the size of feature vector. This will give better accuracy at the cost of increased computational complexity. By defining the orientation of grid nodes as, (1 ≤ dm ≤ N), we calculate the relative direction between minutia M_k and grid nodes as

$$\psi^k_{i,d_m} = d\psi(\phi_k, \phi^k_{i,d_m}) \tag{5}$$

is free from the rotation and translation of the fingerprint. Where, ϕ^k_{i,d_m}, represents the orientation of grid nodes. The orientation of grid node falls in furrows is considered as 0 degree. We have considered five grid nodes for each directional metric, specified feature vector of size 1 x 15 for each minutiae point as shown in Eq. (6). The final feature vector F_k of a minutia M_k that describes its structure characteristic with global fingerprint orientation field is given by Eq. (7).

$$[0.12, 0.78, 0, 0, -0.15, -0.15, -0.15, 0.58, 0.78, 0, 0, 0, 0.78, 0.78, 0] \tag{6}$$

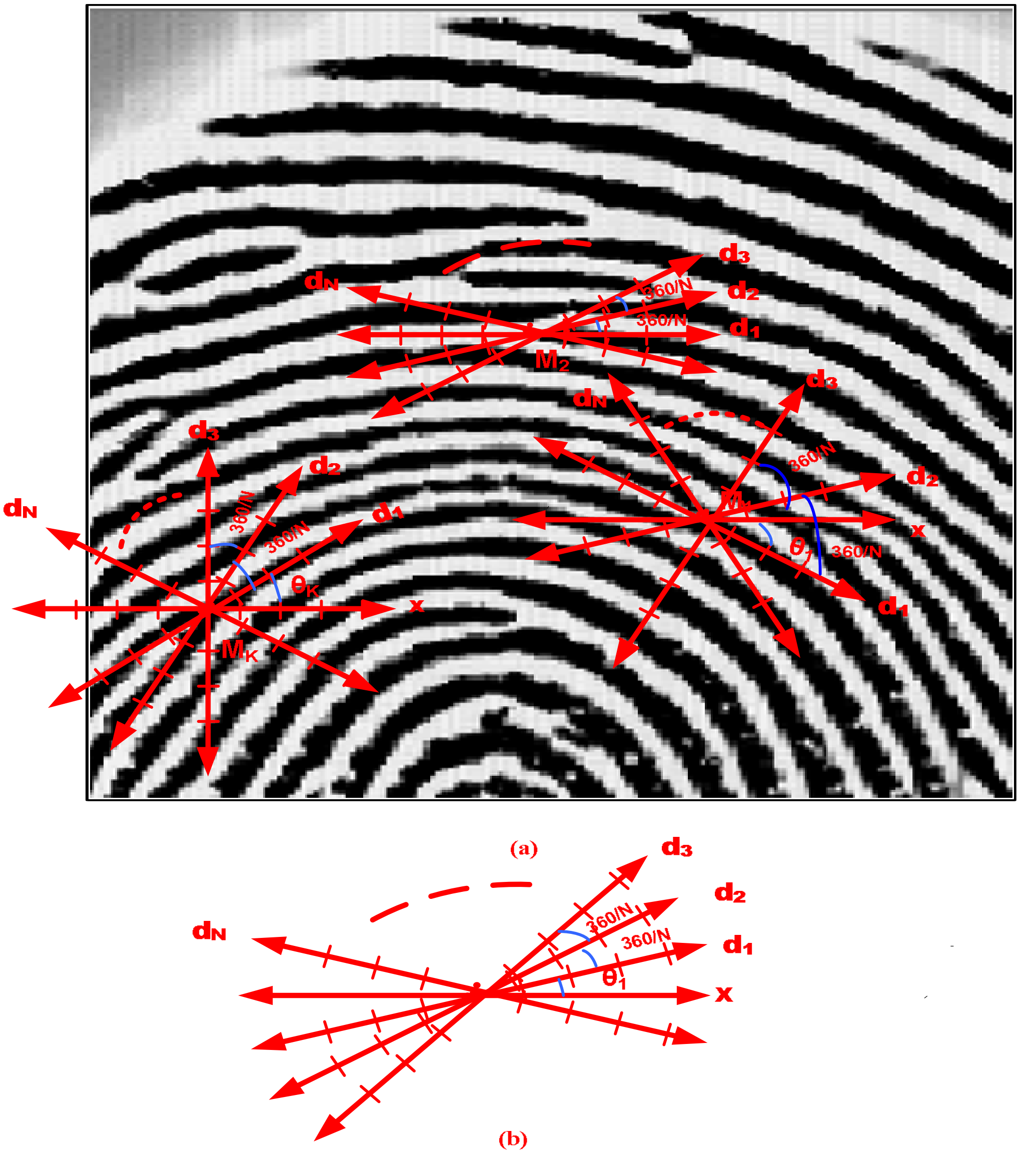
$$F_k = \left\{ \left\{ \psi^k_{i,d_m} \right\}_{i=1}^{n^k_{d_m}} \right\}_{m=1}^{N} \tag{7}$$

Where, $n^k_{d_m}$ gives number of grid nodes along the direction metric d_m corresponding to kth minutiae. The structure feature vector F_k is invariant to rotation and translation of the fingerprint.

Suppose F_i and F_j are the structure feature vectors of minutia *i* from input fingerprint and minutia *j* from template fingerprint, respectively. A similarity level is defined as

$$S(i,j)=\begin{cases}\dfrac{T-\left|F_i-F_j\right|}{T} & if\left|F_i-F_j\right|<T,\\ 0 & otherwise\end{cases} \tag{8}$$

Where, $|F_i - F_j|$ is the Euclidean distance between feature vectors F_i and F_j and *T* is the predefined threshold between 0 and 1. Here the selection of the value of *T* is tradoff between FAR and FRR, high value of T increases FAR and opposite is true for FRR. Here, the similarity level describes a matching assurance level of a structure pair and define as *S(i, j)*, 0≤ *S(i, j)* ≤ 1, instead of simply matched or not matched. *S(i, j)*=1 implies a perfect match, while *S(i, j)*=0 implies a total mismatch.



(a)

(b)

FIGURE 4: (a) N lines around a minutia detail (b) Grid nodes organized on directional metric.

4.2 Matching of Global Minutiae Structure

With the defined feature vectors, we compute matching score based on consequent minutia pairs. Degree of similarity between two fingerprint decides genuine/imposter attempt. In order to compute matching score, we need to identify a set of consequent minutia pairs from template and input fingerprint.

System identifies a user truly if the match score is computed with reliable consequent point pairs. In order to have reliable consequent point pair input finger must be properly aligned with template fingerprint. The alignment stage is intended to recover the geometric transformation between the two fingerprint impressions. In our work, the rigid transformation, i.e., translation vector ($t =[tx, ty]^T$) and rotation angle (*Ø*), is recovered by the best-matched structure pair that exhibits the largest similarity value in Eq. (8). The best-matched minutia structure pair (s1, s2), minutia s1 from the input fingerprint and another s2 from the template fingerprint is obtained by maximizing the similarity level as

$$S(s_1, s_2) = \max_{i,j}(S(i,j))$$

$$\phi = D(s_2) - D(s_1) \text{ and } t = P(s_2) - R_{\phi}(s_1) \qquad (9)$$

Where, $R_{Ø}$ denotes the 2 × 2 operator of counter clockwise rotation used to find the position of rotated minutia (s1) and the position of a minutia s2 are denoted by $P(s2) =[x(s2), y(s2)]^T$. Direction of minutia is denoted by *D(s)*. Applying the estimated geometric transformation onto the minutiae from the test fingerprint we obtain the list comprising the aligned minutiae. Also, the orientation field from the test fingerprint will be aligned using the estimated transformation simultaneously.

The non-linear deformations and deformations due to the location and direction errors can be tolerate to some extent by having elastic matching algorithm, achieved by selecting bounding box Bg in the feature space instead of an exact matching. A small size bounding box *Bg* is chosen to get two consequent minutiae lists L1 and L2 which are from the template fingerprint and the test fingerprint, respectively. The pairs with the largest similarity level values in Eq. (8), which, also fall in the bounding box *Bg* are considered as consequent minutiae pairs. Here the size of bounding box is tradeoff between the false acceptance rate (FAR) and the false rejection rate (FRR).

4.3 Matching Score Computation

With the introduction of our minutia structures and similarity of consequent minutia pairs, matching score can be determined by Mm. Let N1 and N2 denote the number of minutiae located inside the intersection of the two fingerprint images for test and template fingerprints, respectively. The minutia matching score Mm can be calculated according to the following equation.

$$M_m = \frac{\sum_{i,j} S(i,j)}{\max\left\{N_1, N_2\right\}}, \qquad (10)$$

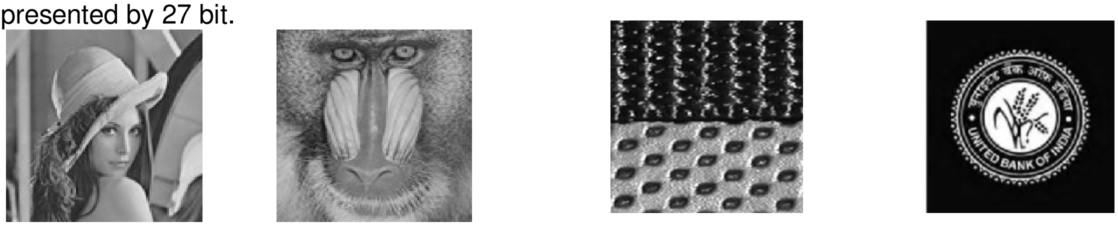
where i, j is the consequent minutiae pair, one from test fingerprint and another from template fingerprint, respectively, and S(i, j) is computed according to Eq. (8).

5. EXPERIMENTAL EVALUATION

Experiments are performed on four bench mark images as given in Fig. 5 to calculate the optimal weights. All objective functions are simplified by using above four images based on image content. Variance threshold of 1000 is selected to distinguish smoother blocks from edge blocks. Weights derived from experiments are given in Table 1.

The algorithm proposed above is tested on the public domain collection of fingerprint images, DB3 in FVC2004. It comprises 800 fingerprint images of size 300×480 pixels captured at a resolution of 512dpi, from 100 fingers (eight impressions per finger). Individual minutiae data sets contained between 25 to 35 minutiae points, with an average of 30 minutiae points. Experiment is performed for 50 different types (low freq, medium freq., high freq., highly textured etc.) of host images of size 512 x 512. Out of them results for four images shown in Fig. 6 are presented here.

Before hiding, first watermark (fingerprint minutia) is converted into bit stream. Each minutia is represented by 27 bit.



(a) Lena (b) Mandrill (c) Texture (d) Bank logo

FIGURE 5: Benchmark Images

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

TABLE 1: Weights of Objective functions

We watermark each host image with our method as well as with Choi's method. Let **I** (i, j) the original host image and **I**'(i, j) is the watermarked image. We measure the imperceptibility of watermark by calculating PSNR value as per Eq. (11).

$$PSNR = 20\log_{10}(255 / RMSE)$$
$$where, RMSE = \left\{\sum [I(i,j) - I'(i,j)]^2 / N^2\right\}^{1/2} \quad (11)$$

Here N is total no. of pixels in Image I.

(a) (b) (c) (d)

FIGURE 6: Host images (a) Texture (high frequency) (b) cameraman (medium frequency) (c) India logo (low frequency) (d) Bank logo (low frequency)

PSNR values for four types of images are listed in Table 2. It shows that the PSNR value of our method is higher than Choi's method. This is because in Choi's method watermark is embedded into DC Coefficient, which decides the block average. So, even a small variation in DC coefficients only effects intensity of all the pixels within the block and hence results in low PSNR.

Image	Imperceptibility Measurement PSNR		Quality Factor (Q)	Compre - ssion (BPP)	Watermark Extraction BER(%)		FAR (%)		FRR (%)	
	Our Method	Choi's			Our Method	Choi's	Our Method	Choi's	Our Method	Choi's
Texture	37.2025	35.7245	90	2.8527	0	0.93	0.17	0.20	0.18	0.21
			80	2.1015	0	0.93	0.17	0.20	0.18	0.21
			75	1.8981	0	0.93	0.17	0.20	0.18	0.21
Cameraman	38.2340	34.8972	90	2.1323	0	2.47	0.17	0.24	0.18	0.22
			80	1.4608	0	2.47	0.17	0.24	0.18	0.22
			75	1.2816	0.1	2.47	0.17	0.24	0.18	o.22
India logo	48.7235	36.8863	90	2.5463	0	0.93	0.17	0.20	0.18	0.21
			80	1.8955	0	0.93	0.17	0.20	0.18	0.21
			75	1.7143	0	0.93	0.17	0.20	0.18	0.21
Bank logo	42.0910	39.6230	90	1.9196	0	1.35	0.17	0.20	0.18	0.21
			80	1.4365	0	1.35	0.17	0.20	0.18	0.21
			75	1.3010	0.5	1.35	0.17	0.20	0.18	0.21

TABLE 2: Watermark Extraction Error Rate due to JPEG Compression and Matching Accuracy of fingerprint

We have compared the robustness of our method with existing Choi's method under different channel attacks like compression, salt & pepper noise and rotation. Comparison is done based on watermark extraction error rate, False Acceptance rate (FAR) and False Rejection Rate (FRR).
The results in Table 2 illustrate the extraction error rate for JPEG compressed watermarked image. With the same measuring parameter, Table 3 shows the extraction error rate for salt & pepper noise attacked watermarked image. Table 4 shows results for measuring parameter after combine above two attacks. In all cases our method appears better than Choi's method. Our matching algorithm results FAR and FRR as 0.17% and 0.18% respectively, without watermarking, which remains exactly same with our watermarking technique without any attack. In presence of different attacks FAR and FRR undergoes minor change, unlike to Choi's method. These are highlighted in Table 2, 3 and 4. Proposed technique is also robust against various signal processing operations like enhancement (gamma=), rescaling (512-256-512) and filtering (average). For all mentioned operation FAR and FRR of the system remains same as without watermarking approach.

Image	Watermark Extraction BER(%)		FAR (%)		FRR (%)	
	Our Method	Choi's	Our Method	Choi's	Our Method	Choi's
Texture	0	1.33	0.17	0.19	0.18	0.21
cameraman	0.02	2.25	0.17	0.24	0.18	0.24
India logo	0.08	1.45	0.17	0.19	0.18	0.21
Bank logo	0.01	3.97	0.17	0.26	0.18	0.25

TABLE 3: Watermark Extraction Error Rate due to salt & pepper noise (Density = 0.02) and Matching Accuracy of fingerprint

Image	Quality Factor (Q)	Watermark Extraction BER(%)		FAR (%)		FRR (%)	
		Our Method	Choi's	Our Method	Choi's	Our Method	Choi's
Texture	90	0.32	1.36	0.17	0.20	0.18	0.21
	80	0.32	1.36	0.17	0.20	0.18	0.21
	75	0.32	1.36	0.17	0.20	0.18	0.21
cameraman	90	0.74	3.39	0.17	0.24	0.18	0.22
	80	0.74	3.35	0.17	0.24	0.18	0.22
	75	0.44	3.35	0.17	0.24	0.18	0.22
India logo	90	0.2	4.23	0.17	0.26	0.18	0.26
	80	0.2	1.59	0.17	0.20	0.18	0.22
	75	3.2	4.26	0.23	0.24	0.21	0.22
Bank logo	90	0.39	4.45	0.17	0.26	0.18	0.26
	80	0.39	4.43	0.17	0.26	0.18	0.26
	75	2.9	4.39	0.20	0.26	0.20	0.26

TABLE 4: Watermark Extraction Error Rate due to above combined attacks and matching accuracy of fingerprint

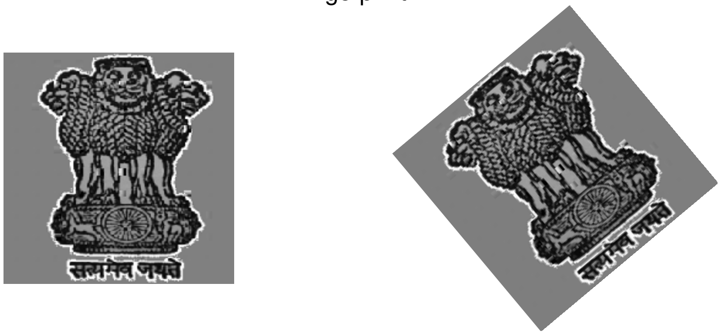


FIGURE 7: (a) Watermarked Image (b) Watermarked Image Rotated at 40°

We have also tested robustness of our algorithm for rotation attack. Fig.7 (a) and (b) shows watermarked and watermarked image rotated at 40° angle respectively. Plot of variance of the projections of Radon transformed coefficients for both images are shown in Fig.8 (a) and (b). For rotated image two local maxima was observed. To distinguish between these two maxima, we have calculated 2nd order derivative of the variance as shown in Fig.9.

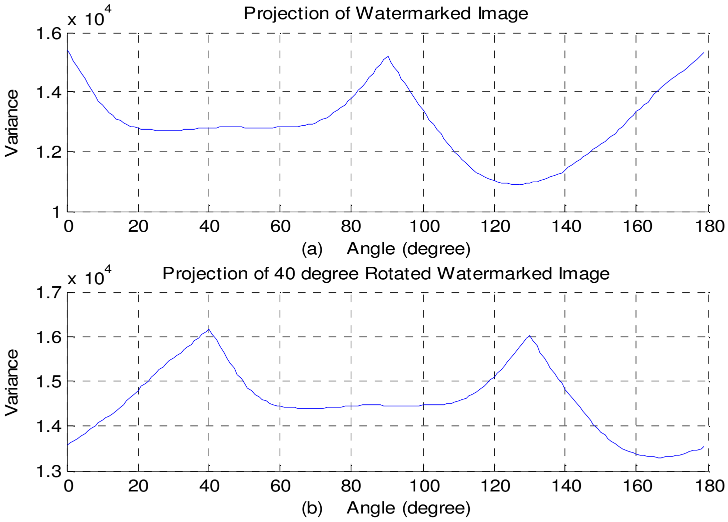


FIGURE 8: Variance of projection at different angles for (a) Watermarked Image (b) Rotated watermarked image

In Fig.9 maxima of rotated image is noted at 130°(ϕ_r). The transmitted watermarked image maxima is at 90°(ϕ_o) (Fig.8(a)). The difference between these angles is the required de-rotation angle ϕ_d .

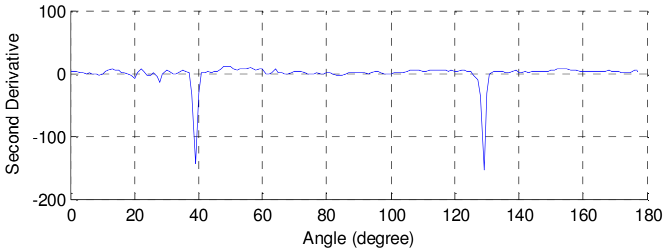


FIGURE 9: Second Order Derivative of 8(b)

Image	Rotation Angle ($Ø_d$)	Watermark Extraction BER(%)	FAR (%)	FRR (%)
Texture	15	6.5	0.27	0.27
	35	7.5	0.28	0.28
	75	6.5	0.27	0.28
cameraman	15	8.5	0.3	0.31
	35	8.5	0.3	0.31
	75	8.5	0.3	0.31
India logo	15	10	0.35	0.33
	35	8	0.29	0.29
	75	9	0.29	0.29
Bank logo	15	Destroyed	Destroyed	Destroyed
	35	Destroyed	Destroyed	Destroyed
	75	Destroyed	Destroyed	Destroyed

TABLE 5: Watermark Extraction Error Rate due to Rotation attack and Matching Accuracy of fingerprint

Table 5 illustrates the performance of security system in terms of FAR and FRR for rotated watermarked image. Here, high watermark extraction error rate is observed due to interpolation bit during de-rotation.

6. CONSLUSION & FUTURE WORK

In this paper we present application scenario of security system. In order to overcome the problem of security of fingerprint data we introduced strong semi-blind watermarking algorithm which hides fingerprint data into host image. Thus fingerprint data is protected while transmitted through channel/client to server.

Feature points (minutia points) of fingerprint with explained minutia extraction algorithm are extracted. Our minutia extraction algorithm gives strong feature points by removing false minutia and finally we have 25 to 30 minutia points per finger. These minutia points are embedded into host image by proposed semi-blind watermarking algorithm which is decided by neighborhood based estimation criteria. Our estimator uses AC coefficients as container unlike DC coefficient in Choi's method. It is difficult to set strength of watermark bit in DC coefficient because human eyes are very sensitive to the variation in DC component. In our approach modification in AC coefficients reduces the chances of perceptibility of watermark even with large strength of watermark bit. The payload capacity we obtained is far better than Choi's method. Furthermore, the global channel attack which affects original value as well as estimated value and our watermark extraction algorithm extract watermark bit based on relative value between both, gives good robustness against attack like JPEG compression and salt & noise. Even though we are not able to get 100 percent watermark bit pepper under attacks, our strong distortion-tolerant matching algorithm gives FAR and FRR that are almost same as FAR and FRR without watermarking approach. Our proposed idea can also be used for multimodal system provided, watermarking approach should have high capacity.

7. REFERENCES

[1] N.K. Ratha, J.H. Connell, and R.M. Bolle, "*An Analysis of Minutiae Matching Strength*," Proc. Third Int'l.Conf. Audio- and Video-Based Biometric Person Authentication, pp. 223-228, June 2001.

[2] B. Schneier, "*The Uses and Abuses of Biometrics*," Comm. ACM, vol. 42, no. 8, p. 136, Aug. 1999.

[3] Yi Chen, "*Extended Feature Set and Touchless Imaging for Fingerprint Matching*", Ph.D Theses, University of Michigan State, 2009.

[4] Salil Prabhakar, "*Fingerprint Classification and Matching Using a Filterbank",* Ph.D Theses, University of Michigan State, 2001.

[5] Panyayot Chaikan, Montri Karnjanadecha, "*The Use of Top-View Finger Image for Personal Identification"* Proceedings of the 5th International *IEEE* Symposium on image and Signal Processing and Analysis, 343-346, Nov. 2007.

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

[7] Ashourian, M.; Enteshary, R., "IEEE Conference on Convergent Technologies for Asia-Pacific Region", TENCON, Vol. 1, pp 428-431, 2003.

[8] B. Verma, S. Jain, D. P. Agarwal, and A. Phadikar, "A New color image watermarking scheme," *Infocomp, Journal of computer science*, vol. 5,N.2, pp. 37-42, 2006.

[9] X. Wu and Z.-H. Guan, "A novel digital watermark algorithm based on chaotic maps," *Physics Letters A*, vol. 365, pp. 403-406, 2007.

[10] Feng Yang, Lei Li, "An adaptive, SVM -based watermarking in frequency domain", International Conference on Wavelet Analysis and Pattern Recognition, pp. 465 – 469, Hongkong, 30 sep., 2008.

[11] L. Chun-Shien, H. Shih-Kun, S. Chwen-Jye, and L. Hong-Yuan Mark, "Cocktail watermarking
for digital image protection," *Multimedia, IEEE Transactions on*, vol. 2, pp.209-224, 2000.

[12] W. Lu, H. Lu, and F.L. Chung, "Robust digital image watermarking based on subsampling," *Applied Mathematics and Computation*, vol.181, pp. 886-893, 2006.

[13] Wang-sheng Fang, Kang Chen, "A Wavelet Watermarking Based on HVS and Watermarking Capacity Analysis", IEEE International Conference on Multimedia Information Networking and Security, pp. 141-144, Hubei, Dec., 2009.

[14] Hongping Xu, Xiaoxia Wan, "International Conference on Computer Science and Software Engineering", pp. 245- 248,Hubei, Dec., 2008.

[15] Yanhong Zhang, "Blind watermark algorithm based on HVS and RBF neural network in DWT domain", WSEAS Transactions on Computers, Volume 8, Issue 1, January 2009.

[16] Nagar Abhishk, Nandkumar Karthik, Jain Anil k., "*Biometric Template Transformation: a security analysis*," Proc. SPIE, the International Society for Optical Engineering, vol.7541, 2010.

[17] Noore A., Singh R., Vatsa M. and Houck M.M., " *Enhancing Security of Fingerprints Through Contextual Biometric Watermarking*", Journal of Forensic Science International, Vol. 169, Issue 2, Pp. 188-194 ,July 2007.

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

[19] Chander Kant, Ranjender Nath & Sheetal Chaudhary, "Biometrics Security using steganography", International Journal of Security, Vol. 2 : Issue (1).

[20] S. Jain, “*Digital Watermarking Techniques: A Case Study in Fingerprints & Faces*,” Indian Conf. Computer Vision, Graphics, and Image Processing, pp. 139-144, Dec. 2000.

[21] B. Gunsel, U. Uludag, and A.M. Tekalp, “*Robust Watermarking of Fingerprint Images*,” Pattern Recognition, vol. 35, no. 12, pp. 2739-2747, Dec. 2002.

[22] Yulin Wang , Alan Pearmain, “*Blind image data hiding based on self reference”* Pattern Recognition Letters 25, 1681–1689, 2004.

[23] Hiller and Lieberman, *“ Introduction to Operations Research*,” Seventh edition, Tata McGraw-Hill, 2001.

[24] Choi, Y., Aizawa, I., “*Digital watermarking using interblock correlation*”, In: Proc. Internat. Conf. on Image Processing, vol. 2, pp. 16–220, 24–28 October 1999.

[25] J. Qi. and Y. Wang, "*A robust fingerprint matching method*", Pattern Recognition, vol. 35, pp.1655-1671, 2005.

[26] X. Jiang, W.Y. Yau,” *Fingerprint minutiae matching based on the local and global structures*”, Proc. of the 15th International Conference on Pattern Recognition, vol. 2, pp. 1038–1041, 2000.