Cancelable Template Generation Based On Improved Quality Fingprint Image For Person Authentication

Janani.B, Dr. N. Radha

Research scholar
PSGR Krishnammal college for women
Coimbatore

Assistant professor
PSGR Krishnammal College for women
Coimbatore

ABSTRACT

Biometric based authentication system provides robust security and ease of use than conventional methods of verification system. Among various biometrics namely iris, face and gait recognition, Fingerprint recognition has been extensively used by several organizations for recognition and authentication purpose because of its low cost, usability and reliable performance. However, the performance of fingerprint identification techniques are extensively depends on the quality of the input fingerprint images. Due to the context of the image-acquisition process, most of the fingerprint images are found to be low or lack in quality. By concerning privacy issues, these types of low-quality fingerprint templates are easily accessible by intruders, thereby lacks the security. To address this issue, the present work proposes quality enhanced, secured biometric template which simultaneously combines the quality enhancement and cancellable template generation techniques for robust authentication purpose. The fingerprint quality can be improved by means of two-phase enhancement technique, learns the acquired input image by enhancing spatial and frequency domain of image respectively. After that, the cancellable fingerprint templates are generated by means of transforming the quality enhanced fingerprint minutiae distortedly by using Distortion Transformation. Experimental results show that the proposed algorithm efficiently holds various input image contexts and attains improved results in terms of quality and security when compared with some state-of-the-art methods, and thus improves the fingerprint-authentication systems performance.

Keywords: Fingerprint quality enhancement, Cancellable template generation, Two-phase filtering, Distortion transformation

I. INTRODUCTION

Biometrics is broadly described the art of recognizing an individual or person based on his or her behavioural or their physical qualities which is established for gaining acceptance to as a justifiable method for the purpose of an identity of individuals[1]. This system is largely implemented in the field of various forensic, civilian and commercial applications with the intention of launching identity in the cybernetics, computational intelligence and human–machine systems and computational intelligence[2][3]. In a modern multimodal biometric identification system is described which uses biometrics of iris and fingerprints for the particular security based applications [2]. Inoverviews of biometrics are discussed with a few research issues that required to be dealt for construction of biometric technology a valuable tool [3].

Among all the biometric, fingerprints are widely used biometrics by the experts of criminal investigations due to its reliability and its computational cost [4]. However, the performance of fingerprint recognition systems extensively depends on the quality of the fingerprint images. In general due to the contexts of image acquisition process from the sensors, the Fingerprint images are often found to be low quality shown in Figure 1. In general, noise occurred from input devices can be eliminated without difficulty by means of using simple filters yet, the flaw of ridge structures from each entity are not usually well defined, and it is difficult to improve the circumstances of these images. The fingerprint image quality might be poor or considerably dissimilar because of several issues, namely dryness, wetness, smears, pressure strength and so on, which show the way to several types of degradation in fingerprint images.
With this low-quality fingerprint, the secured authentication of the person is not possible. For the reason that biometric data do not differ greatly over time and are very exceptionally shared by two people. If the biometric data is stolen or misused by third party, privacy violations occur. Conventional methods for recognizing persons include Personal Identification Numbers (PINs) and ID which can be abandoned and reissued. However this is impossible with biometric data. In addition, privacy issues occur about sharing biometric data with law enforcement or commercial companies. In order to improve privacy and security in biometrics, cancellable biometrics has been recently developed [5], [6].

Cancellable biometrics utilizes distortedly transformed biometric data in place of the original biometric data for recognizing a person. Once a biometric data is said to be compromised, it can be rejected, and a biometric data of new set can be generated again. However, with these cancellable techniques, the secured template is attained in the non-enhanced template image thereby it is easy and chance for intruders to steal the templates and misused. To resolve the above research challenges, the proposed work deals on image quality enhancement and biometric template security using distortion transformation algorithm. This technique transforms the enhanced fingerprint minutiae features into the distort/hash form. With this generated template the user can get enrolled by storing their secured template in the system database. During verification, the prompted template of the user is matched with the stored template and thus the user can be recognized and authenticated.

The paper is outlined as follows: Section 2 describes the related works, section 3 describes the proposed system and its architecture. Experimental results are discussed in section 4 and the conclusion and possible future works are discussed in section 5.

II. RELATED WORK

This section discusses several quality enhancement techniques and template security algorithms used by several researchers to enhance the quality of fingerprint image and to store the template in secure manner.

Tahmasebi et. al [7] presented an Adaptive approach for fingerprint enhancement filter design. The designed filter adapts itself to the characteristics of input images and improves the efficiency of enhancement. In addition, the parameters of filters are estimated automatically without any requirement of predetermined parameters. In order to improve the efficiency of the enhancement process, this method uses various masks of filters are adapted for different image scales. This process performs faster and takes less computation time to process. However interconnected ridges are not efficiently enhanced.

Hong et al [8] presented directional Gabor filtering kernel for fingerprint enhancement approach. This approach enhances the image by appropriately employing oriented Gabor kernel, which has orientation and frequency selective properties. This permits the filter to be altered which provides maximal response to ridges at a definite orientation and frequency in the fingerprint image. Unlike Fourier bases or discrete cosine bases, the usage of Gabor elementary functions has the following problems: Gabor elementary functions do not form a rigid frame; and there is no justifiable reason for using the Gabor kernel over other directionally selective filters, namely directional derivatives of Gaussians or steerable wedge filters.

Ang et al. [9] presented a key-dependent transformation method for generating cancelable fingerprint templates from fingerprint minutiae. This method generates templates by determining its core point initially, and a line through the core point is specified. The orientation of the line is specified and determined in the range of 0° and 180° by using the key transformation function. By altering the orientation, different templates are generated. However, it is impractical to determine the exact location of core point.

Chulhan et. al [10] presented a method for generating cancelable fingerprint templates that do not require alignment and a method for building changing functions. By extracting translation and rotation invariant value from each minutia, cancelable templates of fingerprints are generated. After that the translation and orientation movement of each minutia is estimated by using two changing functions. Each minutia is rotated and moved by the transformed minutia by means of the orientation of a minutia as the reference direction. Once an ideal invariant value is extracted, the same minutia yields the same invariant values even if fingerprint images are changed. In this situation, the method does not corrupt performance because the geometric relationships between the original fingerprint templates are sealed in the transformed fingerprint templates.

JaiieKim et. al [11] presented an approach for template security based on cancellable biometric fingerprint. It transforms original biometric templates in a bit-string. The alignments are not necessary for transformation. One drawback is that the performance was ideal when each user had a different PIN and the two templates from the same fingerprint were not matched when the corresponding PINS were different.

Tulyakov et. al [12] presented a hash-based transformation method for secured template generation. For each minutia, the N nearest neighbour minutiae was found and M (MoN) hashed minutiae were generated using symmetric hash functions. The hashed minutiae were then stored in a database and compared to the query hashed minutiae. Unlike common hash functions, these hash functions showed good biometric properties. In the hash space, these researchers discovered the geometric relationship between the query and the enrolled fingerprint. However, they did not describe how

Figure 1(a) and (b): Two impressions of a user’s finger showing the poor quality of the ridges
the newly hashed minutiae could be generated when stored minutiae were compromised.

III. QUALITY ENHANCED, SECURED BIOMETRIC TEMPLATE GENERATION METHOD

In this section, initially two-phase fingerprint quality enhancement is performed by filtering techniques. In general the resultant information obtained from first stage enhancement technique is used for the second-phase enhancement technique. In First phase, spatial domain filtering technique is used. In which the ridge compensation filter will acquire the local ridge information to connect separately merged and broken ridges. The result obtained efficiently enhances the contrast of ridge and thereby blurs the image due to the utilization of neighbour information by the filter mask. In such case, second phase enhancement technique is used. In this phase, band pass filter is transformed and divided into angular and radial frequency domain. That is incorporated with the resultant of first phase enhancement and original image. The resultant image of this phase is the second stage enhanced image and improves the low-quality fingerprint image respectively. In this enhanced image, distortion transformation method is applied to generate secured biometric template. In this process fingerprint minutiae’s are distortedly altered and further matching are done with the transformed space. The complete architecture of the proposed system is shown in the Figure 2.

Figure 2: Proposed System architecture

1. FIRST STAGE FINGERPRINT IMAGE ENHANCEMENT

The key concept of the First Phase Fingerprint Image Enhancement technique is to compute unbiased local orientation and identify the feasible defects by means of using local orientation. This technique is broadly categorized into three stages namely: local fingerprint normalization, fingerprint orientation computation and compensation filtering of local ridges are briefly described as follows:

a) Local fingerprint normalization

In this, normalization of local fingerprint image is performed which reduces the variations in gray level values and intensity distribution is normalized for estimating the exact computation of local orientation.

Consider the input acquired fingerprint image, $Img$ can be decomposed into sub images. The normalization can be done on each pixel $(i, j)$ in the sub images as follows:

$$Norm(i,j) = M_0 + \text{coefficient} \times (Img(i,j) - M) \quad \rightarrow (1)$$

Coefficient $= \frac{V_0}{V} \quad \rightarrow (2)$

Where $Norm(i,j)$ denotes normalized subimage of image $Img(i,j)$, $M$ and $M_0$ denotes mean and desired mean value of sub image, $V$ and $V_0$ denotes the variance and desired variance values of sub image and coefficient denotes the normalized image amplificatory multiplication.

b) Fingerprint orientation computation

In this stage, dominant direction of the ridges are identified and estimated in various parts of original fingerprint images. This can be performed by dividing the image into different non-overlapping blocks in which each single orientation is mapped related to its probable orientation of the block.

The steps performed for the estimation of local orientation of fingerprint is pointed as follows:

1. Divide the original image into number of sub blocks
2. Obtain horizontal gradient value and vertical gradient value by using Sobel mask [13] in each pixel of block
3. Obtain horizontal and vertical gradient block by summing up all pixel gradients of its respective directions.

4. Determine orientation of block by using horizontal and vertical block gradients

The following equation shows the horizontal gradient \( G_{xx} \) and vertical gradient \( G_{xy} \) blocks and its orientation estimation \( O(x,y) \) as follows:

\[
G_{xx} = \sum_{u=-\lfloor w/2 \rfloor}^{\lfloor w/2 \rfloor} \sum_{v=-\lfloor w/2 \rfloor}^{\lfloor w/2 \rfloor} 2G_x(u,v)G_y(u,v)
\]

\[
G_{xy} = \sum_{u=-\lfloor w/2 \rfloor}^{\lfloor w/2 \rfloor} \sum_{v=-\lfloor w/2 \rfloor}^{\lfloor w/2 \rfloor} (G_x^2(u,v) - G_y^2(u,v))
\]

\[
O(x,y) = \frac{1}{2} \tan^{-1}\left(\frac{G_{xy}}{G_{xx}} \right)
\]

**c) Fingerprint Ridge- compensation filtering**

With the computed orientation information of fingerprint image form the above section; this stage compensates the artifacts of ridges by using local ridge-compensation filter with the rectangular window in order to match the local orientation.

This ridge-compensation filter can be done on each pixel \((i,j)\) in normalized image \(\text{Norm}(i,j)\) is defined as follows:

\[
\text{Ridgefltimg}(i,j) = \frac{\Sigma_{m=-\lfloor h/2 \rfloor}^{\lfloor h/2 \rfloor} \Sigma_{n=-\lfloor w/2 \rfloor}^{\lfloor w/2 \rfloor} \text{Norm}(i',j')} {{\Sigma_{m=-\lfloor h/2 \rfloor}^{\lfloor h/2 \rfloor} \Sigma_{n=-\lfloor w/2 \rfloor}^{\lfloor w/2 \rfloor} \text{Norm}(i,j)}}
\]

where \((i',j')\) denotes the pixel coordinate in the new axes , \(h\) and \(w\) are height and width of the enhanced window, \(n\) and \(m\) are the integer numbers determined by \(h\) and \(w\).

![Figure 3(a)](image-url) low quality image and (b) first stage enhanced image

**2. SECOND STAGE FINGERPRINT IMAGE ENHANCEMENT**

Even though the result obtained from the first phase spatial filtering improves the contrast of ridges, blur of image is resulted. To deal with this, the second phase enhancement technique uses the modified bandpass filter as frequency bandpass filter to improve the enhancement of fingerprint image. In general, this filter is separable in angular and radial domains. The enhancement of fingerprint image is done on both angular and radial domains and thus absolute enhancement of fingerprint ridges is achieved. Most significantly the parameters of frequency bandpass filter are obtained from both enhanced and original fingerprint image.

The frequency bandpass filters \(H(\rho,\phi)\) are expressed as separable functions by using polar coordinates \((\rho,\phi)\). The separable functions separates the filter in angular and radial domains respectively is described below:

\[
H(\rho,\phi) = H_\rho(\rho)H_\phi(\phi) \rightarrow (9)
\]

\[
H_\rho(\rho) = \frac{1}{2\rho BW} \exp\left(-\frac{\rho^2 - \rho_0^2}{2\rho BW}\right) \rightarrow (10)
\]

\[
H_\phi(\phi) = \begin{cases} 
\cos^2\frac{\pi}{2}\frac{\phi - \phi_0}{2\rho BW} & \text{if } |\phi| < \phi BW \rightarrow (11) \\
\text{otherwise}
\end{cases}
\]

In second phase fingerprint enhancement technique, the following operations are performed.

- Local Orientation estimation
- Local Frequency estimation
- Coherence Image
- Frequency Band pass Filtering

**a) Local Orientation estimation**

Similar to local orientation in step 2 of first phase enhancement technique, the dominant direction of the fingerprint ridges are determined. In this stage, the new orientation is estimated with the enhanced fingerprint image. The computation of new orientation is described as follows:

\[
\theta(x,y) = \begin{cases} 
\text{corr}_{\theta(x,y)} & \text{if } |\text{corr}_{\theta(x,y)} - \text{orig } \theta(x,y)| < t, \\
\frac{\Sigma_{i\in\text{win}} \text{corr}_{\theta(x,y)}}{W_{\text{win}}} & \text{else}
\end{cases}
\]

where orig \( \theta(x,y) \) denotes the pixel orientation in original image, \( t \) denotes threshold, \( W \) denotes window sizes and \( \text{corr}_{\theta(x,y)} \) denotes pixel orientation of enhanced image.

**b) Local Frequency estimation**

In this step, interridge separation in diverse region of the fingerprint images is calculated. Then the local frequency of the fingerprint image is computed by applying FFT [14] for different blocks.

Frequency = FFT (image _block) \rightarrow (13)

The new frequency is computed as similar to the computation of (12) by using frequencies both from the original and enhanced image. If the difference between both image frequencies is larger than the value of the threshold or equals the frequency of the enhanced image, then the new frequency equals its value to the average value of its neighbour value. Once the estimated frequency lies in the outside range , then the error correcting process of the
frequency can be done by [15]. Thus the resultant frequency is intended for radial filter design.

c) Coherence Image

In this step, Coherence defines the co-ordination between central block orientation and its neighbours in the orientation structure. In general, the coherence is corresponded to the dispersion estimate of circular data which is defined as follows:

$$C(x, y) = \frac{\sum_{(i,j) \in W} [\cos(\theta(x, y) - \theta(x_i, y_j))]}{WXW} \quad (14)$$

When the central orientation pixel is analogous to each of its neighbours and its size of the windows W, high coherence is resulted. From the resultant coherence image, angular filter bandwidth can be determined.

d) Frequency Bandpass Filtering

Initially the whole smoothing filtered image is divided into overlapping sub images and for each sub image certain operations are performed which is described as follows:

1. Obtain the FFT of each sub image by dc component in FFT domain.
2. Angular filter is applied in which local image central orientation and its bandwidth is directly proportional to the Coherence Image by using (11).
3. Radial filter is applied in which it is presented in the centre of the local frequency image by using (10).
4. The block of image gets filtered by concatenation results of all filters.

$$\text{Filtered image} = f \times \text{angular filter} \times \text{Radial filter}$$

5. Finally, the reconstruction of enhanced image is performed by using

$$\text{Enhanced Image} = \text{IFFT (Filtered image)}$$

Figure 4(a) low quality image, (b) first stage enhanced image and (c) second stage enhanced image

3. CANCELLABLE TEMPLATE GENERATION USING DISTORTION TRANSFORMATION

In this section secured fingerprint templates are generated by transforming the enhanced fingerprint minutiae’s distortedly. To perform this circular regions constructed around each minutia are utilized. The constructed circular regions equal the fingerprint minutiae. Information of regions is illustrated by the region of minutiae pair. After this the hashing can be done on the circular regions to get the distorted form of image.

Let the minutiae Z(i) represented as (x, y, a) in the Cartesian coordinate framework in whereas (x, y) denotes the position of the minutiae and a denotes the orientation point. Assume that R(Z0) be the region and Z0 represents the centered minutia. Consider that R(Z0) has k minutiae then R(Z0) is denoted as \{Z0, Z1, .......Zk-1\}

The steps to obtain the secured template are as follows:

1. Convert all minutiae of regions R(Z0) from Cartesian to polar form
2. Rotate all minutiae of R(Z0) at one time to guarantee the orientation of Z0 equals 90 and obtain the converted minutiae as (ρ, 90°, α)
3. Hash all minutiae in region R(Z0) Consider the transform parameter a1, a2, b1, b2, c1, c2 a given by the user and hash values of minutiae are v1 and v2

$$V1 = a1* \rho + b1* \epsilon + c1* \alpha$$

$$V2 = a2* \rho + b2* \epsilon + c2* \alpha$$

4. Set of images of hashed minutia are returns as resultant.
5. Store the hashed region of image as a distortedly transformed template in the database.

IV. EXPERIMENTAL RESULT

This section discusses the results obtained for image quality enhancement and the cancellable template generation by using distortion transformation. The proposed system has been implemented using MATLAB R2010a. The fingerprint images are collected from FVC 2004 DB3-a, DB4-a database. The resolution of DB3-a is 512 dpi and DB4-a is 500 dpi. Each database consists of 800 fingerprint images i.e., there are 100 persons, and each individual has eight fingerprints.

The proposed system can be experimentally evaluated by using performance measures such as false rejection rate (FRR), false acceptance rate (FAR) and genuine acceptance rate (GAR).

False Rejection Rate (FRR)
FRR occurs when a biometric device rejects a genuine user and incorrectly labels that user as an intruder.

\[
\text{FRR}(n) = \frac{\text{Number of rejected verification attempts for a qualified person (or feature) } n}{\text{Number of all verification attempts for a qualified person (or feature) } n}
\]

(17)

False Acceptance Rate (FAR)

The FAR is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system’s FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

\[
\text{FAR}(n) = \frac{\text{Number of successful independent fraud attempts against a person (or characteristic) } n}{\text{Number of all independent fraud attempts against a person (or characteristic) } n}
\]

(18)

The following comparative Table 1 shows the experimental values obtained for Distorting transformation without enhanced image and Distorting transformation with enhanced image. The proposed distortion transform is a method of transforming fingerprint minutiae distortedly and achieving fingerprint matching in the transformed space.

<table>
<thead>
<tr>
<th>Techniques</th>
<th>FRR%</th>
<th>FAR%</th>
<th>GAR%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distortion without enhancement image</td>
<td>5.5</td>
<td>4.3</td>
<td>89.23</td>
</tr>
<tr>
<td>Distortion with enhancement Images</td>
<td>1.2</td>
<td>2.8</td>
<td>93.45</td>
</tr>
</tbody>
</table>

Table 1 Performance analysis of distortion transformation

Cancelable distortion transformation performances are done on low quality image and the enhanced image. The Table 1 shows the performances between both enhanced and non enhanced image. The FRR, FAR and GAR value is calculated for both images and shown in this table.

The above graph in figure 3 shows the performance visual aid of distortion transformation performance with low quality image and enhanced biometric fingerprint. The performance is measured with low quality fingerprint image and enhanced fingerprint image with different cancellable biometric transformation algorithms that are used to generate templates. Table 1 shows the performance measure of distortion transformation before and after image quality enhancement. Based on the obtained values the above graph can be plotted. From the above graph, it can be concluded that the proposed work cancellable distortion transformation on enhanced image gives the better result as compared to the cancellable distortion transformation on non-enhanced image. For the distortion transformation the GAR= 89.23% for low quality fingerprint image and 93.45% for enhanced fingerprint image respectively.

V. CONCLUSION

The proposed work is to enhance the fingerprint quality and transformed them into secured biometric template for robust authentication purpose. Low-quality fingerprint images are enhanced by using two-phase fingerprint enhancement technique and secured cancellable templates are generated by using Distortion transformation. With the enhanced image, the secured template can be generated by using distortion transformation which transforms the minutiae into secured distorted form. By performing the proposed technique, secured fingerprint templates are obtained in which original biometric information’s are not revealed. By applying these transformation techniques, security level gets increased. At the same time GAR, FAR, FRR values are calculated. Genuine acceptances rate get increased for enhanced image as 93.45% by applying this distortion transformation. Thus the experimental result of proposed system achieved secured recognition and authentication result when compared with the other
traditional methods. In future, the present work can be further extended using multimodal biometric system which will improve the level of security in user authentication.

REFERENCE


