Volume 6, Issue 1, January 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Performance Analysis of Quality Enhanced Cancelable Fingerprint Biometric for User Authentication

Janani.B, S. Mahalakshmi

Assistant Professor, GVG Vishalakshi College for women
Udumalpet, Tamilnadu, India

Abstract: Biometrics is an automatic identification of biological and behavioral characteristics of individuals. The main aim of the proposed work is to increase the system performance during authentication that is bounded with two major parameters. They are image quality enhancement and template security. The sensor, damaged skin, etc., will reduce the performance of the system during authentication. To improvise the system performance the quality of the images are enhanced by filtering techniques such as spatial filtering and frequency bandpass filtering. The extracted features enrolled through sensor are stored in database called "template", which are used for person authentication. The problem persist with the use of original template can be avoided using cancellable biometrics. In the present work, quality enhanced image is used to extract features and biohashing transformation is Applied to transform the original biometric. So the template security is also improved. The Experimental result of proposed system provides better result when compared with the existing system for the authentication of users.

Key Terms: Fingerprint enhancement, two-stage filtering, cancelable biohashing transformation.

I. INTRODUCTION

The increasing demand for more reliable and convenient security systems generates a renewed interest in human identification based on biometric [1] identifiers such as iris, fingerprints, voice and etc. Since biometrics cannot be lost or forgotten like computer password. Biometrics has the potential to offer higher security and more convenience for the users.

A common approach to biometric authentication is to capture the biometric templates of all users during the enrollment phase and to store the templates in a reference database. In the authentication phase new measurements are matched against the database information.

Fingerprint is composed of ridges and furrows on the tip of finger. It is generally used for personal identification because of its easier accessibility, individuality and reliability. Fingerprint recognition has emerged as one of the most reliable means of biometric authentication because of its universality, uniqueness, durableness, and accuracy. Generally speaking, fingerprint recognition algorithms are roughly classified into two classes [2]: minutiae-based [3] and image-based methods [6], which primarily use minutiae information or a reference point along with a number of ridge attributes for recognition. The wrong ridge structural information can be fatal to both classes of recognition algorithms. Since it can change the information of the minutiae points and reference points, and it may also cause some errors in feature extraction. To decrease the risk of recognition error, a robust enrichment algorithm is required, particularly for low-quality fingerprint images.

One of critical threat in biometric systems is the theft of biometric data [9]. Unlike passwords, when the biometric template is compromised, it cannot be cancelled or revoked. BioHashing presents good revocability properties because of its inability to deal an unordered set of points. FingerHashing was Applicationied to texture features which requires a reliable registration point instead minutiae even reputed more robust. This prevents compatibility with existing databases and commercial fingerprint sensors. This paper presents new method for enhancing fingerprint image quality by using spatial filtering and frequency filtering. It also presents a method for protecting minutiae templates with BioHashing process in order to satisfy criteria of privacy and revocability without lose of verification performance.

II. RELATED WORK

Tahmasebi and Kasaei [10] presented a novel Adaptive Approach for fingerprint enhancement filter design to improve the efficiency of enhancement process. Moreover, the filter parameters are automatically calculated and different filter masks are adapted for different image scales to improve the efficiency of the enhancement process. The algorithm is fast and required computational load is negligible.

Zhixin Shi and Venu Govindaraju [11] presented a novel use of chain code image representation in fingerprint image enhancement and minutiae extraction. For image enchantment binarization algorithm is used. The direction field is predicted from a set of selected chaincodes.

Marius et. al [12] presented new approach for fingerprint enhancement based on Short Time Fourier Transform (STFT) Analysis. The algorithm simultaneously estimates all the intrinsic properties of the fingerprints such as the foreground region mask, local ridge orientation and local frequency orientation. Furthermore these propose a probabilistic approach is robustly estimating these parameters and enhancement utilizes the full contextual information.

Ju Cheng Yang et. al [4] presented a novel algorithm for low-quality fingerprint enhancement in spatial domain. This method enhances ridges with a mixture of local normalization and ridge compensation filter in which this filter uses orientation of ridges. This method efficiently enhances the contrast among valleys and ridges of low-quality fingerprint images.

Chulhan Lee and JaihieKim [1] presented technique for template security based on cancelable biometric fingerprint. It transforms original biometric templates in a bit-string. 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.

Ratha et. al [13] Cancelable biometrics uses transformed or intentionally-distorted biometric data instead of original bio-metric data for identification. Because the transformation is non-invertible, the original biometric templates cannot be recovered from the transformed templates.

Tulyakov et. al [14] proposed a hash-based transformation method. For each minutia, the N nearest neighbor minutiae was found and M 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.

III. PROPOSED FINGERPRINT ENHANCEMENT SYSTEM

The term biometrics is flattering highly significant in computer security world. The human physical individuality such as face, hand geometry, fingerprints, iris and voice are known as biometrics. These features are used to grant an authentication for computer based security systems.

A. Phases of the Proposed Work

The Figure 1 demonstrates the proposed works of fingerprint enhancement system using three different phases are performed to enhance the low-quality fingerprint image and secure it. The low quality fingerprints are enhanced by two-stage enhancement based on blockwise processing. This is completed by decomposing the input fingerprint image into an array of distinct blocks and the discrimination of the blocks is obtained by computing the standard deviation of the matrix elements to remove the image background and obtain the boundaries for the region of interest.

To provide security for biometric template, technique called cancelable biohashing is used. Biohashing based template security is done with the extracted features with the computed features and biocode for each minutia in fingerprint is generated. The biocode is used by biohashing technique for storing templates.

B. Two-Stage Fingerprint Enhancement

a). First-Stage Enhancement

The first stage performs ridge compensation along the ridges in the spatial field. It will enhance the fingerprint's local ridges using the neighbor pixels in a small window with a weighted mask along the orientation of the local ridges. The main idea of the first-stage enhancement scheme is to estimate unbiased local orientation and compensate the possible defects by using the local orientation. The method consists of three steps:

i) Local normalization

Local normalization is used to decrease the local variations and standardize the intensity distributions in order to consistently estimate the local orientation.

Normalized image (i, j) $= M_0 +$ coeff *(img(i,j) –M) where, Coeff $= \frac{V_0}{V}$ [1]

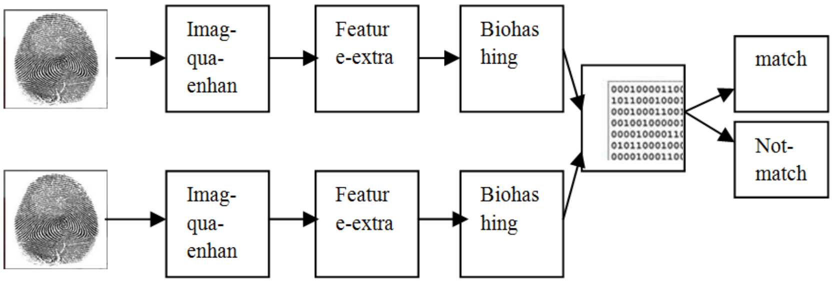


Figure 1 Proposed fingerprint enhancement systems

ii) Local Orientation Estimation

Local Orientation Estimation will determine the dominant direction of the ridges in different parts of the fingerprint image.

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

Where,

$$G_{xy} = \sum_{u=i-(w/2)}^{i+(w/2)} \sum_{v=j-(w/2)}^{j+(w/2)} 2G_x(u,v)G_y(u,v)$$ [3]

[[

$$G_{xx} = \sum_{u=i-(w/2)}^{i+(w/2)} \sum_{v=j-(w/2)}^{j+(w/2)} (G_x^2(u,v) - G_y^2(u,v)) \quad [4]$$

iii) Local Ridge-Compensation Filter

With the estimated orientation values in place, the final step compensates the ridge artifacts using a local ridge-compensation filter with a rotated rectangular window to match the local orientation.

$$\text{fltimg}(i,j) = \frac{(\sum_{m=-(w-1)/2}^{(w-1)/2} \sum_{n=-(h-1)/2}^{(h-1)/2} \text{norimg}(i',j')}{\left(\left((w-1)X\beta|\alpha\right) * h\right)} \quad [5]$$

b). Second-Stage Enhancement

First, the whole smoothing filtered image is divided into overlapping sub-images, and for each sub-image, the following operations are performed.

i) Local orientation estimation

This step determines the dominant direction of the ridges in different parts of the fingerprint image by learning from the images. The orientation estimation is similar with Step 2 in the first-stage filtering, which used the gradient method for orientation estimation.

$$\theta(x,y) = \begin{cases} \text{corr}\_{\theta(x,y)}, & \text{if}|\text{corr}\_\theta(x,y) \\ \frac{\sum_{(i,j)\in W} \text{corr}\ \ \theta(x,y)}{W\ X\ W}, else & \\ -\text{orig}\_\theta(x,y)| < t, & \end{cases} \quad [6]$$

ii) Local frequency estimation

This step is used to estimate the inter ridge separation in different regions of the fingerprint image. The local frequency is predicted by Applying FFT to the blocks by F=FFT (block_images), and the local frequency is pixel processing.

iii) Coherence image

The word coherence refers the relationship between the orientation of the central block and those of its neighbors in the orientation map. The coherence is related to the dispersion measure of circular data and it is defined as,

$$C(x,y) = \frac{\sum_{(i,j)\in W} |\cos(\theta(x,y) - \theta(x_i,y_i))|}{W\ X\ W} \quad [7]$$

iv) Frequency Band-Pass Filtering

First, the whole smoothing filtered image is divided into overlapping sub-images and for each sub-image various filtering operations like Angular filter, FT domain, , Filtered image, Radial filter, reconstructed image are performed. The reconstruct image is the final enhanced image by the proposed two-stage enhancement algorithm.

C. Template Generated using Biohashing

The process of biohashing for fingerprint is performed as follows:

For each minutia m do

i. compelling the region of interest ROI surrounding

ii. Filter the ROI in eight different directions using a bank of Gabor filters. Different to the original.

iii. Let Im be the °-direction filtering image for sector S_i= i{1.B* 16}.

iv. The feature vector or the Minucode is v={v_1,v_2,…..v_n} /u=B*16*8 with

$$\forall fi\theta\ \varepsilon F, fi = \frac{1}{ni} \sum_{ni} |Imi\theta\ (x,y) - \ Pi\theta|, ni \quad [8]$$

is the number of pixels in *Si* and *pi* is their mean..

IV. EXPERIMENTS AND RESULTS

The proposed system has been developed using MATLAB R2010a. The fingerprint images are collected from FVC 2004 DB3-a, DB3-a database. The resolution of DB3_a is 512 dpi and DB4_a is 500 dpi. Each database consists of 80 fingerprint images i.e., there are 10 persons, and each individual has eight different positions of a fingerprint.

A. Performance Measure

a).False Rejection Rate (FRR)

FRR occurs when a biometric device rejects a genuine user and incorrectly labels that user as an intruder.

$$\text{FRR}(n) = \frac{\begin{array}{c}\text{Number of rejected verification attempts} \\ \text{for a qualified person (or feature) n}\end{array}}{\begin{array}{c}\text{Number of all verification attempts for a qualified} \\ \text{person (or feature) n}\end{array}} \quad [9]$$

b). 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.

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

[10]

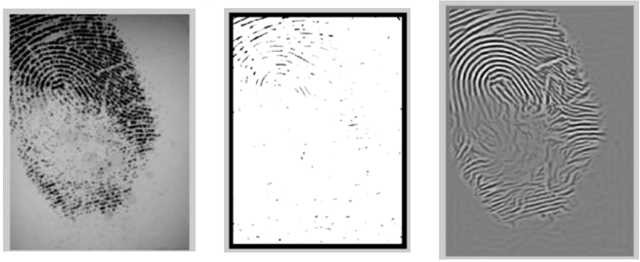
B. Experimental Results of the Two-Stage Enhancement

a). Spatial Filtering

Filtering operations that are performed directly on the pixels of an image are referred as Spatial Filtering. The process of spatial filtering consists of moving the filter mask from point to point in an image.

b). Frequency Filtering

Filters in the frequency domain can be used to calculate convolutions effectively from the entire image rather than from a small area of the filtered point in the spatial domain.



a) Original image b) Spatial filtered c) Frequency filtered

Figure 2 Enhanced fingerprint image using two-stage enhancement.

C. Experimental Results of the Cancellable Biohashing Template Security

Biohashing process was exclusively Applied to texture features of fingerprint. Mainly, these features are extracted using Finger Code in region of interest around the core point. Cancelable biohashing performances are done on low quality image and the enhanced image. The Table shows the performances between both enhanced and non enhanced image. The GAR value is calculated for both images and shown in this table and Figure 3 shows the chart comparison of the images.

Table 1 Performance measure in biohashing before and after image enhancement.

Techniques	FRR%	FAR%	GAR%
Biohashing without enhancement Image	2.3	7.0	81.12
Biohashing with enhanced image	1.9	5.2	91.82

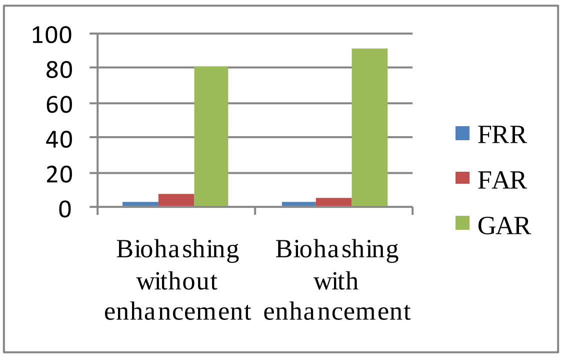


Figure 3 Performance of Biohashing with/ without image enhancement.

V. CONCLUSION AND FUTURE WORK

The proposed work combines the quality enhancement and cancellable template generation techniques 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 biohashing. By performing these techniques, 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 91.82% for biohashing. FRR, FAR and ERR values are reduced. 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 is can be further extended and explored to Multimodal biometric based system to effectively improve the authentication and security.

REFERENCES

[1] Jain, A. Ross and S.Prabhakar, " An introduction to biometric recognition", IEEE Transaction on Circuits and Systems for Video Technology, Volume.1, No.1, pp. -20, January 2000.

[2] D.Maltoni ,D.Maio, A.K.Jain, and S.Prabhakar, Handbook of Finger-print Recognition. Berlin, Germany: Springer-Verlag, 2003.

[3] X. He,J. Tian, L. Li, Y. He, and X. Yang, "Modeling and analysis of local comprehensive minutia relation for fingerprint matching," IEEE Trans. Syst., Man, Cybern. B, Cybern., Volume. 37, No. 5, pp. 120–1211, Oct. 2007.

[4] C. Lee, J. Y. Choi, K. A. Toh, S. Lee, and J. Kim, "Alignment-free can-celable fingerprint templates based on local minutiae information," IEEE Trans. Syst., Man, Cybern. B, Cybern., Volume. 37, No.8 , pp. 980–992, Aug. 2007.

[5] X. J. Tan, B. Bhanu, and Y. Q. A. Lin, "Fingerprint classification based on learned features," IEEE Trans. Syst., Man, Cybern. C, Application. Rev., Volume. 35, No. 3, pp. 287–300, Aug. 2005.

[6] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," IEEE Transaction Image Process., Volume. 9, No. 5, pp. 86– 859, May 2000.

[7] M. Tico, P. Kuosmanen, and J. Saarinen, "Wavelet domain features for fingerprint recognition," Electron. Lett. , Volume. 37,No. 1, pp. 21–22, 2001.

[8] J. C. Yang and D. S. Park, "A fingerprint verification algorithm using tessellated invariant moment features," Neurocomputing , Volume. 71, No. 10–12, pp. 1939–196, 2008.

[9] K. Rhodes, "Aviation security – Challenges in using biometric technologies". Testimony before the subcommittee on Aviation Committee on Transportation and Infrastructure, House of Representatives, May 2000.

[10] A. M. Tahmasebi and S. Kasaei, "A novel adaptive approach to fingerprint enhancement filter design," Signal Processing, Image Communication., Volume. 17, No. 10, pp. 89–855, 2002.

[11] Z. Shi and V .Govindaraju, "A chain code based scheme for fingerprint feature extraction," Pattern Recognition., Volume. 27, No. 5, pp. 62–68, 2006.

[12] Marius Tico, Member Pauli Kuosmanen "Fingerprint Matching Using an Orientation-Based Minutia Descriptor ",IEEE Transactions on pattern analysis and machine intelligence, Volume. 25, No. 8, august 2003.

[13] YounJoo Lee, Kang Ryoung Park, Sung Joo Lee, KwanghyukBae, and JaihieKim,"A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System",IEEE transactions on systems, man, and cybernetics: Volume. 38, No. 5, october 2008

[14] Tulyakov S, Chavan VS, Govindaraju V. Symmetric hash functions for fingerprint minutiae. In: International workshop on pattern recognition for crime prevention, security and surveillance, Bath, UK, 2005

[15] Y. Moon, J. Chen, K. Chan, K. So, and K.Woo, "Wavelet based Fingerprint liveness detection", IEEE Electronic Letter, Volume. 1, No. 20, pp. 1-2, September 2005.