International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 2 Issue: 3 08-Apr-2014,ISSN_NO: 2321-3337

Enhanced biometric authentication system using mixed fingerprints with emphasis on pre-processing

Aswathy Sankar[1], Angel.P[2]

Student, Dept. Computer Science, Maharaja Institute Of Technology, India [1].
Asst.Professor, Dept. Computer Science, Maharaja Institute Of Technology India[2]

.

ABSTRACT— *Fingerprint combination for privacy protection is a novel system for defensive fingerprint privacy by coalescing two dissimilar fingerprints into a new identity. Fingerprints are captured using a biometric scanner in real time. In the enrolment, two fingerprints are captured from two dissimilar fingers. An improved adaptive fingerprint enhancement method based on contextual filtering is used to process the images. Four updated blocks are 1.Preprocessing 2) global analysis3) Local analysis 4)Matched Filtering. The minutiae loci from one fingerprint, the orientation from the other, and the reference points from both fingerprints are extracted. Based on this extracted information, a combined minutiae template is engendered and warehoused in a database. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrolment. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against a combined minutiae template. By storing the combined minutiae template, the complete minutiae feature of a single fingerprint will not be conceded when the database is stolen. Furthermore, because of the similarity in topology, it is difficult for the attacker to extricate a combined minutiae template from the original minutiae templates. Thus, a new virtual distinctiveness is created for the two different fingerprints, which can be matched using minutiae-based matching algorithms. Compared with the existing techniques, our work has the advantage in crafting a better new virtual identity when the two dissimilar fingerprints are erratically chosen.*

Keywords — Combination, fingerprint, minutiae,privacy protection, image processing, successive mean quantization form.

1, INTRODUCTION

Today’s human authentication factors have been placed in three categories, namely what you know password, secret, personal identification number (PIN); What you have, such as token, smart card etc. and What you are, biometrics for, example. However, the first two factors can be easily fooled. For instance, password and PINs can be shared among users of a system or resource. Moreover, password and PINs can be illicitly acquired by direct observation. The main advantage of biometrics is that it bases recognition on an intrinsic aspect of a human being and the usage of biometrics requires the person to be authenticated to be physically present at the point of the authentication. Most of the existing techniques make use of the key for the fingerprint privacy protection, which creates the inconvenience. They may also be vulnerable when both the key and the protected fingerprint are stolen. Teoh propose a bio hashing approach by computing the inner products between the user's fingerprint features and a pseudorandom number (i.e, the key). The accuracy of this approach mainly depends on the key, which is assumed to be never stolen or shared. The work in imperceptibly hides the user identity on the thinned fingerprint using a key. The user identity may also be compromised when both the key and the protected thinned fingerprint are stolen. The works in combine two different fingerprints into a single new identity either in the image level. The experimental results show that the EER of matching two mixed fingerprints is about 15% when two different fingerprints are randomly chosen for creating a mixed fingerprint. If the two different fingerprints are carefully chosen according to a compatibility measure, the EER can be reduced. Contextual filtering is a popular technique for fingerprint enhancement, where topological filter features are aligned with the local orientation and frequency of the ridges in the fingerprint image. Existing methods typically keep various parameters such as local are size, constant. The strategy to keep parameters constant may fail in a real application where finger print image or sensor characteristics may vary, thus yielding varying image quality. Fingerprints captured with the same sensor may also vary depending on e.g. the gender and age of the user. The negative influence on fingerprint recognition system performance for individuals of different ages was demonstrated. In addition ,due to due to the spatially variable nature fingerprints, it is crucial to have a sufficient amount of data in each local image area so that the local structure of the fingerprint is enclosed. Hence, local area size should adapt to the data present. Different fingerprint sensor resolutions provide different normalized spatial frequencies of the same fingerprint spatial frequencies of the same fingerprint and this also requires adaptive parameters. This paper extends an existing adaptive fingerprint enhancement

2, MOTIVATION

With the widespread applications of fingerprint techniques in authentication systems, protecting the privacy of the fingerprint becomes an important issue. Traditional encryption is not sufficient for fingerprint privacy protection because decryption is required before the fingerprint matching, which exposes the fingerprint to the attacker. Therefore, in recent years, significant efforts have been put into developing specific protection techniques for fingerprint. The operational goals of biometric applications are just as variable as the technologies. Some systems search for known individuals; some search for unknown individuals; some verify a claimed identity; some verify an unclaimed identity; and some verify that the individual has no identity in the system at all. With the use of biometric devices, it became apparent that variations in the application environment had a significant impact on the way the devices performed.

3, SYSTEM ANALYSIS

In the enrolment phase, the system captures two finger prints from two different fingers; say fingerprints A and B from fingers A and B respectively. We extract the minutiae positions from fingerprint and the orientation from fingerprint s using some existing techniques. Then, by using our proposed coding strategies, a combined minutiae template is generated based on the minutiae positions, the orientation and the reference points detected from both fingerprints. Finally the combined minutiae template is stored in a database. In the authentication phase, two query fingerprints are required from the same two fingers, as what we have done in the enrolment; we extract the minutiae positions from fingerprint and the orientation from fingerprint. Reference points are detected from both query fingerprints. This extracted information will be matched against the corresponding template stored in the database by using a two-stage fingerprint matching. The authentication will be successful if the matching score is over a predefined threshold.

4, ALGORITHMS USED

4.1 The successive mean quantization transform

The SMQT uses an approach that performs an automatic structural breakdown of information. Let x be a data point and D(x) be a set of |D(x)| = D data points. The value of a data point will be denoted V(x). The form of the data points can be arbitrary, that is D(x) could be a vector, a matrix or some arbitrary form. The SMQT has only one parameter input, the level L (indirectly it will also have the number of data points D as an important input).The output set from the transform is denoted M(x) which has the same form as the input, i.e. if D(x) is a matrix then M(x) is also a matrix of same size. The transform of level L from D(x) to M(x) will be denoted SMQTL: D(x) →M(x)

4.2 Reference Point Detection

Given a fingerprint, the main steps of the reference point's detection are summarized as follows:

1) Compute the orientation O from the fingerprint using the existing orientation estimation algorithm. Obtain the orientation in Z complex domain, where

$$Z=COS(2O)+JSIN(2O) \qquad (1)$$

2) Calculate a certainty map of reference points

$$Cref=z*Tref \qquad (2)$$

Where "*" is the convolution operator and Tref' is the conjugate of

$$\mathrm{Tref} = (x + iy).\frac{1}{2\sigma^2\pi}.\exp(-((x^2 + y^2/2\sigma^2 \qquad 3)$$

4) calculate an improved certainty map:

$$C'ref = \begin{cases} Cref.\sin(Arg(Cref)) & \text{if } Arg(Cref>0 \\ 0 & \text{otherwise} \end{cases} \qquad (4)$$

Where Arg(z) returns the principal value of the argument of z (defined from -180 to 180).

5) Locate a reference point satisfying the two criterions:

(i) the amplitude of C'ref of the point (hereinafter termed as the certainty value for simplicity) is a local maximum, and

(ii) the local maximum should be over a fixed threshold T

6) Repeat step 4) until all reference points are located.

4.3 Query Minutiae Determination

The query minutiae determination is a very important step during the fingerprint matching. In order to simplify the description of our algorithm, we first introduce the local features extracted for a minutiae point in Mc

1) Lij is the distance between mic and mjc $\mathrm{Lij} = \sqrt{(\mathrm{xic} - \mathrm{xjc})2 + (\mathrm{yic} - \mathrm{yjc})2} \qquad (5)$

2) γij as the difference between the directions of mic and mij:

$$\gamma ij = \theta_{ic} \bmod \pi - \theta_{jc} \bmod \pi \qquad (6)$$

3) σij as a radial angle:

$$\sigma ij = R(\theta_{ic} \bmod \pi, \mathrm{atan2}(yjc\text{-}yjc, xjc\text{-}xic))$$

$$R(\mu 1, \mu 2) = \begin{cases} \mu 1 - \mu 2 & \text{if} \pi < \mu 1 - \mu 2 \leq \pi \\ \mu 1 - \mu 2 + 2\pi & \text{f } \mu 1 - \mu 2 \leq -\pi \\ \mu 2 - \mu 1 + 2\pi & \text{f } \mu 1 - \mu 2 > \pi \end{cases} \qquad (7)$$

For the i^{th} minutiae point mic in Mc, we extract a set of local features, where we assume mjc is the nearest, mkc is the second nearest and m_{lc} is the third nearest minutiae point

$$Fi = (Lij, Lik, Lil, \gamma ij, \gamma ik, \gamma il, \sigma ij, \sigma ik, \sigma il) \qquad (8)$$

International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 2 Issue: 3 08-Apr-2014,ISSN_NO: 2321-3337

Where we assume mjc is the nearest, mkc is the second nearest and mic is the third nearest minutiae point of mic . Suppose we detect k1(k1>=1) reference points from fingerprint A' andk2(k2>=1)reference points from fingerprint B'.

The query minutiae are determined as follows:

1)Select a pair of reference points: one from fingerprint A' and the other from fingerprint B'. Assume Ra' is located at ra'=(rxa',rya') with the angleβa',Rb' is located at rb'=(rxb',ryb') with the angle , βb' respectively.

2)Perturb Ba' by $\tau = \beta a' + K.\Delta$, where K is an integer and Δ is a perturbation size. We choose Δ =3×π/180 radians (i.e., 3 degrees) and -5<=k<=5. Thus, we have k=11 perturbed angles for the reference point Ra'

3) Generate a combined minutiae template Mc'for testing (hereinafter simply termed as a testing minutiae) from PA', OB', Ra' (with a perturbed angle) and Rb' using the proposed combined minutiae template generation algorithm. Note that the same coding strategy should be adopted for generating MC'(τ) and Mc. In total, we generate K testing minutiae MC'(τ).

Stage I --Minutiae Position Alignment

Among all the reference we define a reference point with the maximum certainty value as the primary reference point. Therefore, we have two primary reference points Ra and Rb for fingerprints A, B. Let's assume Ra is located at $r_a = (r_{xa,} r_{ya,})$ with the angle β_a , and is located at $r_b = (r_{xb,} r_{yb,})$ with the angle β_b The alignment is performed by translating and rotating each minutiae point

$P_{ic} = (x_{ic,} y_{ic,})$ by

$$(P_{ic})T = H.(P_{ia} - r_{a,})T + (r_b)T \qquad (11)$$

Where H is the rotation matrix

$$H = \begin{bmatrix} \cos(\beta_b - \beta_a), \sin(\beta_b - \beta_a) \\ -\sin(\beta_b - \beta_a), \cos(\beta_b - \beta_a) \end{bmatrix}$$

Stage II --- Minutiae Direction Assignment

Each aligned minutiae Position Pic is assigned with a direction θic as follows

$$\theta_{ic} = (O_B(x_{ic,}, y_{ic}) + \rho_i \pi \qquad (12)$$

Where ρ_i is an integer that is either 0 or 1.Following three coding strategies are proposed for determining the value of ρ_i

1) ρ_I is determined by

$$\rho_i = \begin{cases} 1 \text{ if } \mathrm{mod}\left(\mathrm{ave}_b\left(x_{ic,}, y_{ic}\right), \pi\right) - O_B\left(x_{ic,}, y_{ic}\right) > 0 \\ 0 \quad \text{otherwise} \end{cases} \tag{13}$$

Where ave_b is the average direction of the nearest neighboring minutiae points of the location (xic,yic) in fingerprint B 2) ρ_I is determined by

$$\mathrm{ave}_b\left(x_{ic,}, y_{ic}\right) = \frac{1}{n} \sum_{k=1}^{n} \theta_b^k \left(x_{ic,}, y_{ic}\right) \tag{14}$$

Where $\theta_{bk}(x_{ic},y_{ic})$ means the direction of the nearest neighboring minutiae point of the location (x_{ic},y_{ic}) in fingerprint , and is empirically set as 5 which is able to provide a good balance between the diversity and matching accuracy of the combined minutiae template

3) ρ_I is randomly selected from {0, 1}

Here we use coding strategy 2

4.4 Two-Stage Fingerprint Matching

Given the minutiae positions P_A 'of fingerprint A', the orientation O_B' of fingerprint B' and the reference points of the two query fingerprints.

Stage I --- Query Minutiae Determination

The query minutiae determination is the very important step during fingerprint matching. In order to simplify the description of the algorithm, introduce the local features extracted for a minutiae point in a combined minutiae template. The distance between two minutiae points in the combined minutiae is calculated and the differences between the minutiae directions are also taken. The radial angle is calculated, and the local features are extracted first.

Stage II --- Matching Score Calculation

For the combined minutiae templates that are generated using Coding Strategy 2, we do a modulo pi for all the minutiae directions in and, so as to remove the randomness. After the modulo operation, we use an existing minutiae matching algorithm to calculate a matching score between and for the authentication decision. For other combined minutiae templates, we directly calculate a matching score between MQ and MC using an existing minutiae matching algorithm .

International Journal of Advanced Research in
Computer Science Engineering and Information Technology
Volume: 2 Issue: 3 08-Apr-2014,ISSN_NO: 2321-3337

4.5 FINGERPRINT RECONSTRUCTION

Among the existing fingerprint reconstruction approaches is applicable to achieve excellent performance. We here adopt this approach for generating a combined fingerprint from a combined minutiae template. But the existing approach does not incorporate a noising and rendering step to make the reconstructed fingerprint image real-look alike. To create a real-look alike fingerprint image from a set of minutiae points, we further apply a noising and rendering step after adopting the work from existing reconstruction approach

5, IMPLEMENTATION

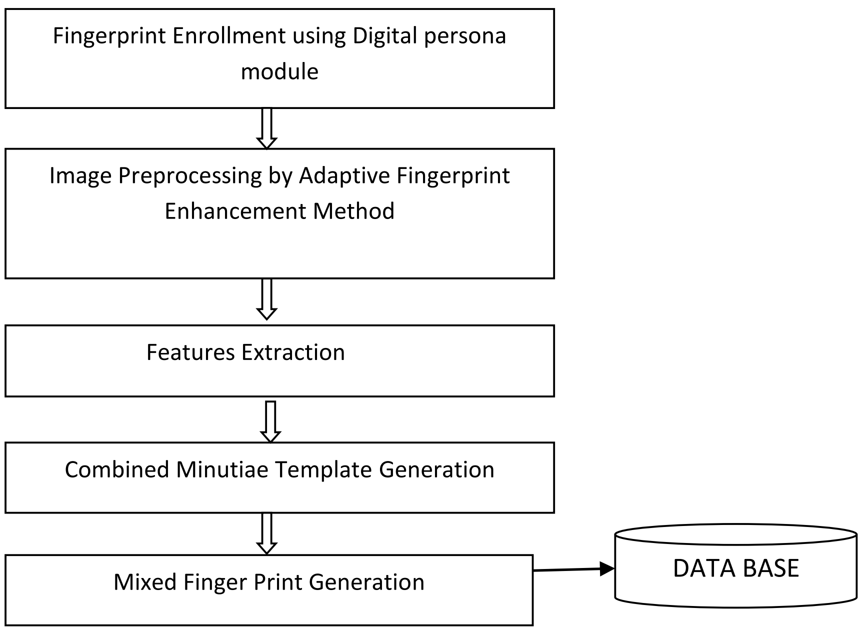

Fig1: Enrollment

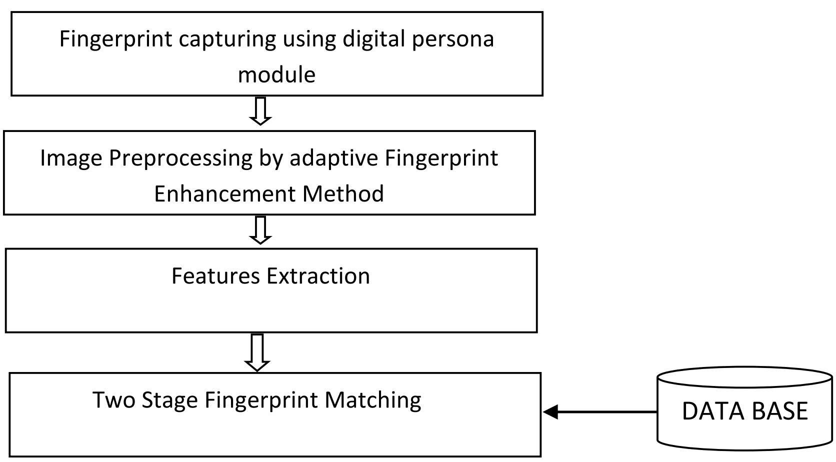

Fig2: Authentication

For the implementation, Mat Lab version R2008 is used. The general steps to be taken for the implementation of the proposed system are as follows:

1. Enrol two finger prints using digital persona fingerprint scanner in real time

2. Apply adaptive fingerprint enhancement method

3. Extract minutiae from one finger print

4. Extract orientation from the other fingerprint

5. Extract reference point from both the finger prints

6. A combined minutiae template is generated from the out puts of steps 2,3,4

7. The above template is stored in the DB

8. Generate a mixed fingerprint

Now the verification of the fingerprints is done against the stored template in database with the below steps.

1. After preprocessing the images captured from fingerprint scanner in real time using digital persona module extract minutiae from the same fingerprint.

2. Extract orientation from the other fingerprint

3. Extract reference point from both.

4. A combined minutiae template is generated from the out puts of 3 steps 1, 2 , 3

6, CONCLUSION

In this proposed system, an improved method of adaptive fingerprint technique is applied to the fingerprint images captured in real time for enhancing security. Thus, a new virtual identity is created for the two different fingerprints, which can be matched using minutiae-based fingerprint matching algorithms. The purpose of generating a combined fingerprint is to issue a new virtual identity for two different fingerprints, which should be matched using general fingerprint matching algorithms.

REFERENCES

[1]. Fingerprint Combination for Privacy Protection, Sheng Li, Student Member, IEEE, and Alex C. Kot, Fellow, IEEE.

[2].A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, “An analysis of bio hashing and its variants,” Pattern Recognit., vol. 39, no. 7, pp. 1359–1368, 2006

[3].A. Othman and A. Ross, “Mixing fingerprints for generating virtual identities,”in Proc. IEEE Int.Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011

[4].A.UhlandP.Wild,”Comparing&verification performance of kids and adults for fingerprint,palmprint,hand-geometry and digit print biometrics”, IEEE 3rd Int.Conf.Biometrics,Theory ,Appl.,Syste.,Mar 2009,pp.1-6

[5]J.S.Bartunek,M.Nilsson,J.Nordberg,andI.Claesson,”Adaptivefingerprint binarisation by frequency domain analysis”,in Proc.IEEE 40TH Asilomar onf.signals,Sys.Comput.Oct-Nov.2006,pp 598-602

[6]Sheng Li, Student Member, IEEE, and Alex C. Kot, Fellow, IEEE, “Fingerprint Combination for Privacy Protection,” ieee transactions on information forensics and security,vol.8,no.2,february2013

[7] L. Hong, Y. F. Wan, and A. Jain, “Fingerprint image enhancement: Algorithm and performance evaluation,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 20, no. 8, pp. 777–789, Aug. 1998.

[8]K.Nilsson and J. Bigun, “Localization of corresponding points in fingerprints by complex filtering,” pattern Recognition. Let., vol. 24, no. 13,pp. 2135–2144,

[9] VeriFinger 6.3. [Online]. Available: http://www.neurotechnology.com

[10] N. K. Ratha, S. Chikkerur, J. H Connell, and R. M. Bolle, Generating cancelable fingerprint templates,”Trans. Pattern Anal. Mach. Intell., vol. 29,no. 4, pp. 561–72, Apr. 2007

[11] A. Nagar, K. Nandakumar, and A. K. Jain, “Biometric template Tansformation:A security analysis,” in Proc. SPIE, Electron. Imaging,Media Forensics and Security, San Jose, Jan. 2010.

[12] S. Li and A. C. Kot, “Privacy protection of fingerprint database,” IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118, Feb. 2011

[13] A. Ross and A. Othman, “Visual cryptography for biometric privacy,”IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70–81,Mar. 2011.

[14] B. Yanikoglu and A. Kholmatov, “Combining multiple biometrics to protect privacy,” in Proc. ICPR- BCTP Workshop, Cambridge, U.K.,Aug. 2004

[15] A. Ross and A. Othman, “Mixing fingerprints for template security and privacy,” in Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona,Spain, Aug. 29–Sep. 2, 2011.

[16] S. Li and A. C. Kot, “Attack using reconstructed fingerprint,” in Proc.IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.