VOL. 10, NO. 16, SEPTEMBER 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

FINGERPRINT TEMPLATE SECRECY SAFEGUARD SYSTEM THROUGH GENERATION OF COMBINED TEMPLATE

A. Lenin Fred, J. Jerusalin Carol and Anisha Isaac
School of Computer Science and Engineering, Mar Ephraem College of Engineering and Technology, Marthandam, Tamilnadu, South India

ABSTRACT

A novel system for protecting the fingerprint privacy is proposed by combining three separate fingerprints of different fingers and enrolling it as a new template. Minutiae positions (ridge endings, ridge bifurcation) and the orientations with the reference points are extracted from all the fingerprints. The fingerprint which has the maximum ridge endings are taken as the main template. To this template the templates of the other two fingerprints are embedded to generate the combined minutiae template. The generated combined minutiae template is stored in a database for enrollment. If a complete minutiae feature of a single fingerprint is stolen the system will not compromise, since the combined minutiae template is only stored and also, it is difficult for the attacker to differentiate the original fingerprint and the combined fingerprint since the topology is the same. In the authentication stage, the three query fingerprints are given to the system and are matched against the stored template. It has been suggested to have a matching process of fingerprints comprising of two phases to compare the two query finger-prints against a combined minutiae template. Thus, a new virtual identity is created for the three distinct fingerprints, which can be matched using minutiae-based finger-print matching algorithms. Compared with the state-of-the-art technique, it has the advantage in creating a better novel virtual identity when the three different fingerprints are randomly chosen.

Keywords: multi-modal bio metrics, fingerprints, minutiae, multiple representation, feature level fusion, virtual Identity, template.

1. INTRODUCTION

Fingerprint identification is part of the most well-known and publicized biometrics. Because of its uniqueness and consistency, fingerprint biometrics has been served as the identification icon over centuries [1, 2]. Fingerprint identification process is based on the features such as i) minutia and ii) the ridge orientation.

Due to the widespread application of fingerprint technique protecting the privacy of the finger print becomes an important issue [3]. Many of the existing techniques make use of the encryption key [4] for the fingerprint privacy protection, which creates the inconvenience. The encryption key which is generated may be stolen or shared. The proposed method increases the privacy of the fingerprints by combining three different fingerprints.

2. REVIEW OF LITERATURE

The privacy of the fingerprint can be safeguarded by schemes like visual cryptography [5], mixed fingerprint [6] so that it cannot be exposed without operating a key. In [5] the fingerprint image is decomposed by using a visual cryptography schemeto produce two noise-like images which are stored intwo separate databases. During the process of authentication, the noise-like images are overlaid to create a temporary fingerprint image for matching. The shortcoming of cryptography scheme is that the storage space complexity is more. The combination of two different fingerprints as one new identity can be in the feature level or in the image level which is implemented in [7, 8]. In [9] the concept of combining two different fingerprints into a contemporary identity, the identity is created by combining the minutiae positions extracted from the two fingerprints, where the original minutiae positions of each fingerprint can be protected in the new identity. However, it is easy for the attacker to identify such a different identity because it contains many more minutiae positions than that of an original fingerprint. A similar method of this methodology is worked with the minutiae positions extracted from a fingerprint and the artificial points generated from the voice are brought together to produce a new identity [8].

In [6] different finger prints of an individual are combined in the image level. At the outset, based on the fingerprint FM -AM model [6], each fingerprint is decomposed into the continuous component and the spiral component. In [10] afresh virtual identity called as mixed fingerprint is formed for which the continuous component of one fingerprint is combined with the spiral component of the other fingerprint after making some arrangement. The image level based fingerprint combination technique [11] in has two advantages over other works: (i) it is hard for the attacker to differentiate between a mixed fingerprint and original fingerprints and (ii) already existing fingerprint matching algorithms can be utilized to match two mixed fingerprints. The main disadvantage of this approach is that unrealistic mixed fingerprints are visually produced which is resulted by the variations in the orientation and frequency between two different fingerprints.

The privacy of the fingerprint is protected by combining two different fingerprints into a new identity [12]. In the enrolment process two fingerprints are captured from two different fingers of the same individual,

VOL. 10, NO. 16, SEPTEMBER 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

where the minutiae positions from one fingerprint and the orientation from the other fingerprint with the reference points from both fingerprints are extracted. Based on this extracted information and the coding strategies, a combined minutiae template [12, 13] is generated and stored in a database. In the authentication stage, the system requires two query fingerprints from the same two fingers which are employed in the enrolment stage.

A fast fingerprint enhancement algorithm is proposed in [6] [14, 15], can adaptively improve the clarity of the ridge and valley structures of input fingerprint images. The main objective is to improve the quality of input images by enhancing the clarity of ridge structures of recoverable regions and to remove the unrecoverable regions which are harmful during minutia extraction. For extracting the minutia positions, the minutia extraction algorithm is used in which the performance is based on quality of input images. Experimental results show improved goodness index and verification accuracy [16].

One of the potential vulnerabilities in a biometric system is the leakage of biometric template information, which may result in serious security and privacy threats. Pattern-based schemes directly derive a fixed-length feature based on the global texture of the fingerprint pattern such as non invertible fingerprint transforms, fuzzy vault, and fuzzy commitment [17]. The problem here is the fingerprint template protection and the algorithms are still not sufficiently robust to be incorporated into functional fingerprint recognition systems. The methodology for biometric template protection is the template transformation approach [18-20], where the template, consisting of the features extracted from the biometric trait, is transformed using parameters derived from a user specific password or key. Only the transformed template is stored and matching is performed directly in the transformed domain.

3. METHODOLOGY

3.1 Fingerprint secrecy safeguard system

The Enrollment phase of the fingerprint privacy protection system is shown in Figure-1. The Authentication phase of the fingerprint privacy protection system is shown in Figure-2.

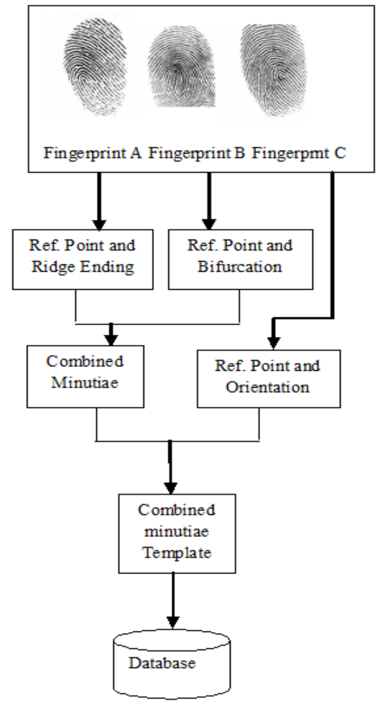


Figure-1. Enrollment phase.

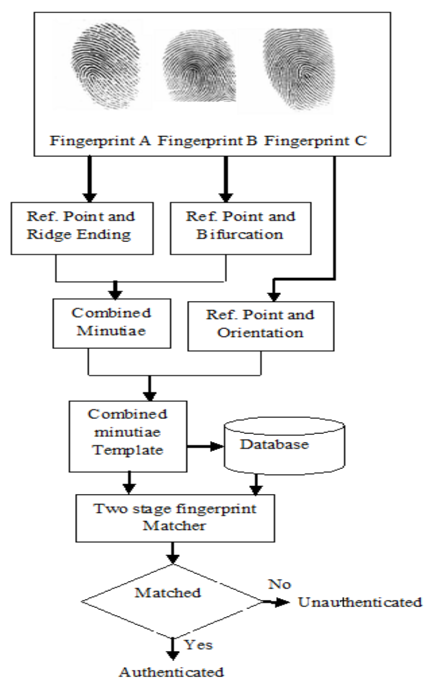


Figure-2. Authentication phase.

The privacy of the fingerprints is attained by combining three separate fingerprints. In the enrolment stage, three fingerprints images from three different fingers are taken as inputs, say fingerprint A, B and C. From

ARPN Journal of Engineering and Applied Sciences
©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

fingerprint A the ridge ending with the singular point and from fingerprint B ridge bifurcation with the singular point are extracted. The ridge ending and bifurcation from fingerprint A and B are extracted using the minutiae extraction algorithm and are combined to form a combined minutiae, by overlapping both the singular points. Then from the third fingerprint C orientation with the singular point is extracted and it is combined with the combined minutia to form the combined minutia template. In the authentication phase, three query fingerprint images are taken from three different fingers say fingerprint $A^{'}, B^{'}$ and $C^{'}$.Similar information taken during the enrolment phase are extracted from these three fingers. The combined minutiae template generated will be matched with the corresponding template stored in the database during the enrolment stage utilizing fingerprint matching system. The system authenticates the person if the matching score is above the predefined threshold T.

3.2 Detection of reference points

The singular point detection for all the three finger print is proposed with the use of complex filters. The extracted singular point is regarded as the reference for the three fingerprints. The following steps show the detection of singular points:

a. Using existing orientation estimation algorithm [5], the orientation O of the fingerprint image is obtained. The orientation computed is then expressed in the complex domain Z, where

$$Z=\cos(2O)+j\sin(2O) \qquad (1)$$

The kernel of the reference point is identified by calculating the certainty map of reference points. The convolution operation is performed for calculating the certainty map.

$$A_{ref}= Z * T_{ref} \qquad (2)$$

T_{ref} is the conjugate of T_{1ref} where "*" denotes the convolution operation.

$$T_{1ref}= (x+iy)\frac{1}{2\pi\sigma^2}.\exp\left(-\frac{x^2+y^2}{2\sigma^2}\right) \qquad (3)$$

b. The improved certainty map is calculated from T_{ref}

$$A^{'}_{ref} = \begin{cases} A_{ref}.\sin(Arg(A_{ref})) & if\ Arg(A_{ref})>0 \\ 0 & otherwise \end{cases} \qquad (4)$$

Where Arg (z) returns the principal value of the argument z and $A^{'}_{ref}$ is referred as the certainty value.

Two conditions are to be adhered to locate the reference point: (i) the amplitude of the certainty value is the local maximum. (ii) the value of the local maximum is over a fixed threshold T.

c. Step-4 is repeated until the reference points are identified.

d. In the case of an arch fingerprint image where there is no singular point, the maximum certainty value is regarded as the reference point for the fingerprint image.

3.3 Minutia detection

The minutia points namely ridge endings and ridge bifurcation is extracted from the fingerprints with the detected reference point. Every minutia position with its surrounding points should retain most of the interrelations in the vicinity. Minutia Cylinder Code representation associates a local structure to each minutia points connected with it. The central minutia is the minutia point placed in the centre of examined vicinity. The minutia points surrounding the central minutia within the given radius are the neighbour minutia. This structure encodes spatial and directional relationships between the minutia points and its neighbourhood (fixed-radius). This can be represented as a cylinder whose base and height are related to the spatial and directional information. The minutia cylinder consists of fixed length vectors known as cylinder codes that represent various possible minutia points present in local neighbourhood of central minutia. The cylinder is enclosed inside a cuboid whose base is aligned according to the minutia direction θ_m. The mapping is performed by

$$M : C \rightarrow x \qquad (5)$$

where set C is associated with the set X of possible configuration of neighbouring minutia represented by (x_p,y_p,θ_p). The neighbour positions (x_n,y_n,θ_n) with respect to the minutia (x_p,y_p,θ_p) is calculated as

$$\sqrt{(x_p-x_n)^2+(y_p-y_n)^2<r} \qquad (6)$$

Where 'r' is the radius of descriptor neighbourhood. The description of the minutia positions leads to a cylindrical shape with (x_p,y_p,θ_p). The value of the cylindrical shape is computed by estimating the probability of minutiae around the central minutia. By using Gaussian distribution, the probability is computed by assuming the differences in location and direction of two corresponding minutiae with a different impression of fingers. The cylinder can be

©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

concatenated as a vector, and therefore the similarity between two minutia cylinders can be efficiently computed.

3.4 Combined minutia generation

The combined minutia position $C_m$is obtained by combining the ridge ending positions of one fingerprint with the bifurcation positions of other finger print along with the reference point as follows. From the two fingerprints A and B the number of each ridge ending positions size (f_1) and size (f_2) are computed. The maximum size of the fingerprint is identified for the combining process. If the size(f_1) is greater than size(f_2) then the ridge endings of fingerprint A is combined with the ridge endings of fingerprint B and vice versa.

The main steps of the combined minutia are summarized as follows:

a) From the fingerprints A and B the maximum size (f_1) and size(f_2) are computed.

   if(size(f_1) > size(f_2))
   $f_1$ridge ending =>$f_2$ridge ending
   else
   $f_2$ridge ending => $f_1$ridge ending
   end

b) From the other fingerprint the ridge bifurcation is identified.

   $f3$bifurcation =>$f_2$bifurcation
   else
   $f_2$bifurcation => f_3 bifurcation
   end
   The point which has the crossing number as 3 is considered as the bifurcation point.
   The value 3 gives the bifurcation point

c) Combining the extracted minutia points (ridge endings and ridge bifurcation) with the reference points from two fingerprints A and B the combined minutia C_m is generated as follows.

$$C_m=\frac{h_0 f_1 + h_1 f_2 + h_2 f_3}{|h_0|^2 + |h_1|^2 + |h_2|^2} \tag{7}$$

h_0, h_1 and h_2 are the weight values.

3.5 Combined minutia template

The orientation O_c is extracted from fingerprint C.The set of combined minutia positions of fingerprint A and B, the orientation $O_c$of fingerprint C and the reference points of fingerprint A,B and C are combined to generate the combined minutia template C_c. The combined minutia template is done by aligning minutia positions and directions.

3.5.1 Alignment of minutiae positions

During the enrolment stage, the reference point that has the maximumcertainty value is considered as the primary reference points. So, the reference points of the fingerprints A, B and C are P_{ra}, P_{rb} and P_{rc}respectively. The assumption is that the P_{ra} is located at r_a=(r_{xa} ,r_{ya}) with the angleγ_a, P_{rb} is located at r_b=(r_{xb} ,r_{yb}) with the angle $\gamma_b$and P_{rc} is located atr_c=(r_{xc} ,r_{yc})with the angle γ_c. The alignment of minutia position is done by translating and rotating each minutiae into a new position. The minutia position P_{ia} is now positioned into a new pointP_{ic}. Therefore after the alignment of minutia positions the primary reference points P_{ra},P_{rb} and P_{rc} are overlapped in the same position. The translation operation is performed as follows:

$$(P_{ic})^T = H(P_{ia}-r_a)^T+(r_b)^T \tag{8}$$

$$H=\begin{cases}\cos(\gamma_b-\gamma_a), \sin(\gamma_b-\gamma_a)\\ -\sin(\gamma_b-\gamma_a), \cos(\gamma_b-\gamma_a)\end{cases} \tag{9}$$

The value of H gives the rotation matrix and $(P_{ic})^T$ is the transpose operator.

3.5.2 Assigning the Minutiae Direction

The aligned minutia positions has an assigned direction θ_{ic} which is given as

$$\theta_{ic}=o_B(x_{ic}, y_{ic})+\rho_i\pi \tag{10}$$

Here the range of $o_B(x_{ic}, y_{ic})$ is from 0 to π. Therefore, the range of θ_{ic} will be from 0 to 2π, which is the same as that of the minutiae directions of an original fingerprint. Sometimes the orientation which is derived from the fingerprint C falls outside the area of fingerprint. In this case the orientation value has to be predicted before the direction assignment. If the values of orientation are not well defined then here we predict the value as the nearest point of well defined orientation in O_c. A combined minutia template Cc is generated for enrolment if all the directions are assigned to a particular position.

3.6 Fingerprint matching

Fingerprint matching is the process done during the authentication stage. In the query fingerprints the minutia positions with the reference points of fingerprinting A' and B' and the orientation with the reference points of fingerprint C' are extracted and they are made into a combined minutia template C_c. This template generated is matched with the template stored during the

ARPN Journal of Engineering and Applied Sciences
©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

enrolment stage. The matching process includes the query minutia extraction and the calculation of matching score.

3.6.1 Query minutiae extraction

Query minutia extraction is the major step for the fingerprint matching. This query minutia determination goes easier when the local features are extracted for a minutia point. For extracting local features the following calculations are done:

1) D_{ij} is the distance between: M_{ic} and M_{jc}

$$D_{ij} = \sqrt{(x_{ic} - x_{jc})^2 + (y_{ic} - y_{jc})^2} \quad (11)$$

where M_{ic} and M_{jc} are the nearest minutia of C_c.

2) Ω_{ij} is the difference between the directions M_{ic} and M_{jc}.

$$\Omega_{ij} = \theta_{ic} \bmod \pi - \theta_{jc} \bmod \pi \quad (12)$$

3) σ_{ij} is the radial angle:

$$\sigma_{ij} = R(\theta_{ic} \bmod \pi, a\tan 2(y_{jc} - y_{ic}, x_{jc} - x_{ic})) \quad (13)$$

where $2\tan 2(y, x)$ is a two-argument arc tangent function in the range (-π,π) and

$$R(\mu_1, \mu_2) = \begin{cases} \mu_1 - \mu_2 & if\ -\pi < \mu_1 - \mu_2 \le \pi \\ \mu_1 - \mu_2 + 2\pi & if\ \mu_1 - \mu_2 \le -\pi \\ \mu_2 - \mu_1 + 2\pi & if\ \mu_1 - \mu_2 > \pi \end{cases} \quad (14)$$

$$Fi = (D_{ij}, D_{ik}, D_{il}, \Omega_{ij}, \Omega, \Omega_{il}, \sigma_{ij}, \sigma_{ik}, \sigma_{lj}) \quad (15)$$

The assumption is that M_{jc} is the nearest point to M_{ic}, M_{kc} is the second nearest point. After the local features are detected the query minutiae extraction is done as follows:

a) From the reference points detected a pair of reference points is selected from fingerprint A' and fingerprint B'. $P_{ra'}$ is located at $r_{a'} = (r_{xa'}, r_{ya'})$ with the angle $\gamma_{a'}$, $P_{rb'}$ is located at $r_{b'} = (r_{xb'}, r_{yb'})$ with the angle $\gamma_{b'}$ and $P_{rc'}$ is located at $r_{c'} = (r_{xc'}, r_{yc'})$ with the angle $\gamma_{c'}$ respectively.

b) The angle $\gamma_{a'}$ is disturbed with a perturbation size Δ which is given as $\tau = \beta_{a'} + k.\Delta$ where k is an integer. The value of Δ is chosen as 3 x π/180 radians (i.e.3 degrees) and $-5 \le k \le 5$.

c) From the extracted information a combined minutiae template is generated.

d) The point which differs least from the template C_c is taken as the query minutiae.

3.6.2 Calculation of matching score

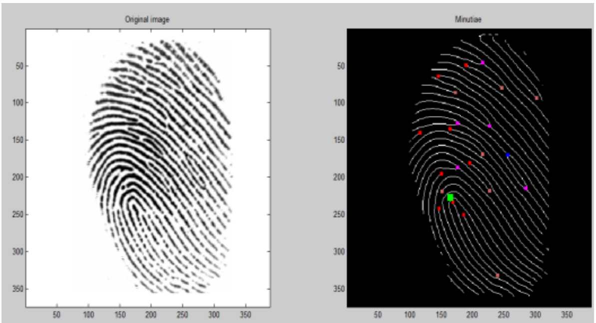
The module operation is carried out for finding the combined minutiae template. This also helps to remove randomness. For calculating the matching score, a minutiae matching algorithm is used. The matching score between C_c and C_q is found and if the score is above a predefined level the system authenticates the person.

4. RESULTS AND DISCUSSIONS

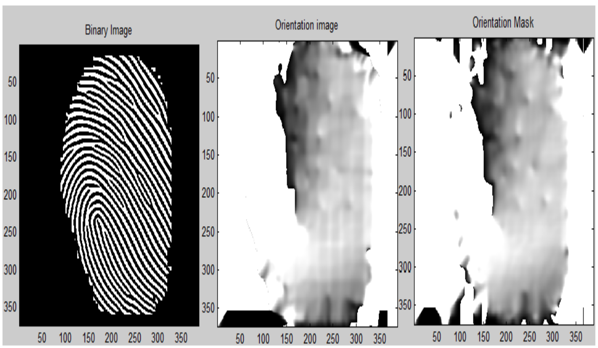
The objective of generation of combined fingerprint template is to eradicate the snoofing and increases the security level through virtual identity, it also reduces the space complexity. The experimental results show that our algorithm avoids 94% of spourious minutiae and drecesses the space complexity. The database used for this work is FVC2002 DB2 and FVC 2004. The data base is catogorized as good, average and poor by visual quality for experimental purpose. Each group comprises of about 100sets of finger print images. The fingers considered are thumb, index finger and middle finger. These three finger print images are considered as one set which belongs to one person.

The three finger print images are obtained one after the other and the features are extracted. The Figure-3(a) shows the input fingerprint along with the extracted features plotted on the fingerprint. Figure-3(b) shows the orientation of the fingerprint. Figures 4-6 shows the extraction process for all the three fingerprints. Figure-7 shows the receiver operation characteristic curve , this curve shows the effectiveness of the minutiae cylindrical code algorithm over the other algorithms. Figure-8 shows thetrue Prevalence curve which is obtained from the inputs got from the ROC curve.

VOL. 10, NO. 16, SEPTEMBER 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com



a)



b)

Figure-3(a). Minutia Extraction (b) Orientation Extraction.

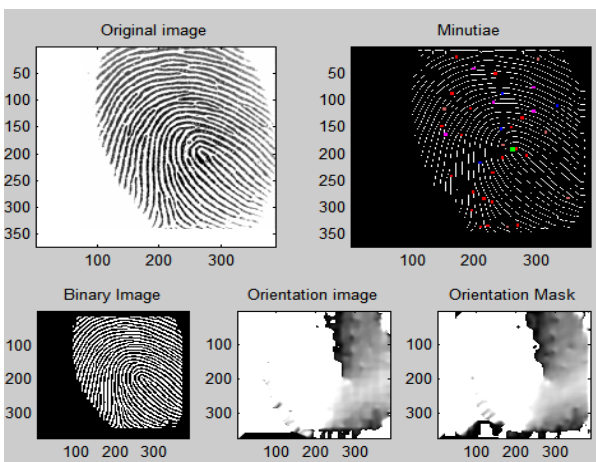


Figure-4. Minutiae extraction from first fingerprint.

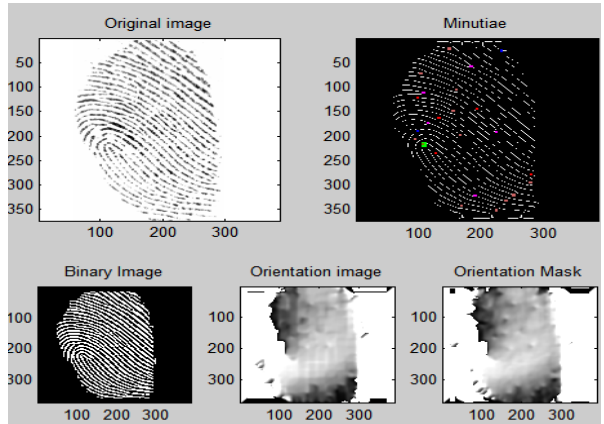


Figure-5. Minutiae extraction from second fingerprint.

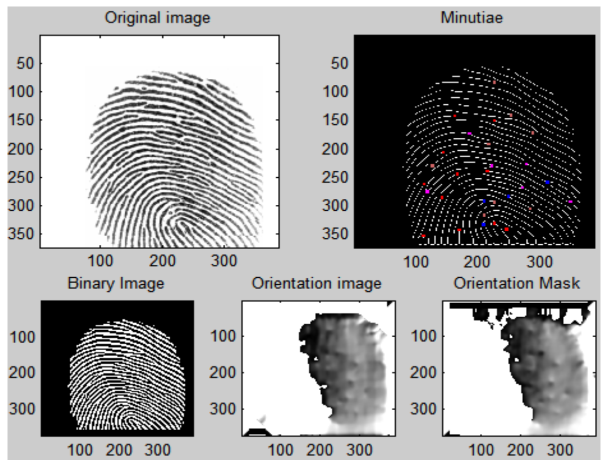


Figure-6. Minutiae extraction from third fingerprint.

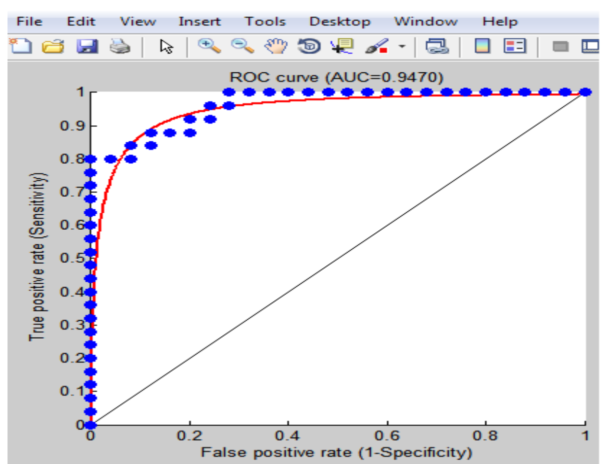


Figure-7. The ROC curve of FAR vs TPR.

ARPN Journal of Engineering and Applied Sciences
©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

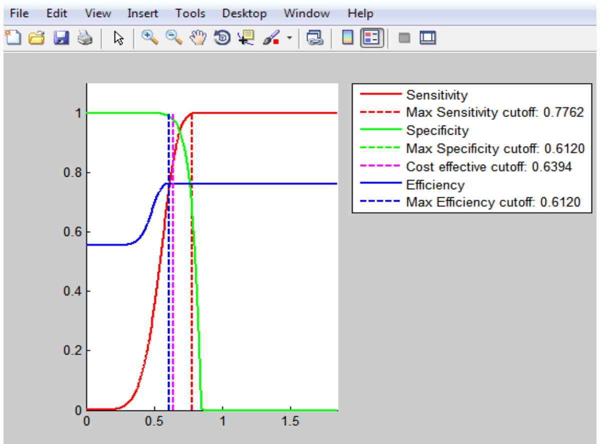


Figure-8. True prevalence curve.

1) Max Sensitivity Cut-off point= 0.78
2) Max Specificity Cut-off point= 0.61
3) Cost effective Cut-off point= 0.64
4) Max Efficiency Cut-off point= 0.61

5. CONCLUSIONS

A novel system for protecting the fingerprint privacy is proposed by combining three different fingerprints of separate fingers and enrolling it as a new template. Minutia positions (ridge endings, ridge bifurcation) and the orientations with the reference points are extracted from all the fingerprints. The fingerprint which has the maximum ridge endings are taken in which the ridge orientation is combined, to form the combined minutia. The combined minutia obtained is again combined with the orientation extracted from the fresh fingerprint. From this extracted information to combined minutia template is generated, which is stored in a database for enrollment. In the authentication stage, the three query fingerprints are given to the system and is matched against the stored template. It has been proposed to have a matching process of fingerprints comprising of two phases to compare the three query finger-prints against a combined minutiae template. Thus, a new virtual identity is created for the three distinct fingerprints, which can be matched using minutiae-based finger-print matching algorithms. Compared with the state-of-the-art technique it has the advantage in creating a better novel virtual identity when the three different fingerprints are randomly chosen.

REFERENCES

[1] Hong. L., Wan. Y. F., and Jain. A. 1998. Fingerprintimage Enhancement: Algorithm and Performance Evaluation. IEEE Trans. Pattern Anal. Mach. Intell. 20(8): 777-789.

[2] Arunprakash. k, Narayanan. R.C and Krishnamoorthy. K. 2015. Reduction of False Acceptance Rate Using Cross Validation for Fingerprint Recognition Biometric System. International Journal for Trends in Engineering and Technology. 3(1): 2349-9303.

[3] Priya Raul, SayaliSurve and Prof J.L. Chaudhari. 2015. Providing Authentication by Merging Minutiae Template. International Journal of Advanced Research in Computer Engineering and Technology (IJARCET). 4(3).

[4] Teoh. B. J. A., Ngo. C. L. D. and Goh. A. 2004. Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognit. 37(11): 2245-2255.

[5] Ross. A. and Othman. A. 2011. Visual cryptography for biometric privacy. IEEE Trans. Inf. Forensics Security. 6(1): 70-81.

[6] Ross. A. and Othman. A. 2011. Mixing Fingerprints for template security and privacy. In Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain.

[7] Yanikoglu. B. and Kholmatov. A. 2004. Combining multiple biometrics to protect privacy. In Proc. ICPR-BCTP Workshop, Cambridge, U.K..

[8] Camlikaya. E., Kholmatov. A. and Yanikoglu. B. 2008. Multi-biometric templates using fingerprint and voice. *Proc. SPIE*. 69440I: 69440I-1-69440I-9.

[9] Praveen N, Thomas. T. 2012. Multifinger Feature Level Fusion Based Fingerprint Identification. International Journal of Advanced Computer Science and Applications. 3(11).

[10] Khalil. M.S, Muhammad. D, KhanM. Kand Alghathbar. K. 2010. Singular points detection using fingerprint orientation field reliability. International Journal of Physical Sciences. 5(4): 352-357.

[11] Cappelli. R., Ferrara. M., and Maltoni. D. 2010. Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence. 32(12).

[12] Li. S. and Kot. A. C. 2013. Fingerprint Combination for Privacy Protection. In Ieee Transactions On Information Forensics And Security. 8(2).

ARPN Journal of Engineering and Applied Sciences
©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

[13] Sarnali Basak, Md. Imdadul Islam, M. R. Amin. 2012. Detection of Virtual Core Point of A Fingerprint: A New Approach. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, 2(2).

[14] Rajinikannan. M, Ashok Kumar. D and Muthuraj. R. 2010. Estimating the Impact of Fingerprint Image Enhancement Algorithms for Better Minutia Detection. International Journal of Computer Applications (0975-8887). 2(1).

[15] Babatunde. G.I, Charles. A.O, Kayode. B.A, Olatubosun. O. 2012. Fingerprint Image Enhancement: Segmentation to Thinning. International Journal of Advanced Computer Science and Applications. 3(1).

[16] Z Yao, J. Le Bars, C Charrier, C Rosenberger. 2015. Fingerprint Quality Assessment Combining Blind Image Quality, Texture and Minutiae Features. ICISSP 2015.

[17] Jain. A. K., Nandakumar. K., Nagar. A. 2011. Fingerprint Template Protection: From Theory to Practice. In: Proc. 7th Int. Conf. Inform. Assurance and Security (IAS). pp. 262-266.

[18] Nagar. A., Nandakumar. K. and Jain. A. K. 2010. Biometric template transformation: A security analysis. In: Proc. SPIE, Electron. Imaging, Media Forensics and Security, San Jose.

[19] Nandakumar. K., Jain. A. K. and Pankanti. S. 2007. Fingerprint-based fuzzy vault: Implementation and performance. IEEE Trans. Inf. Forensics Security. 2(4): 744-57.

[20] Kai Cao, Jain A.K. 2015. Learning Fingerprint Reconstruction: From Minutiae to Image. Information Forensics and Security, IEEE Transactions on. 10(1).