ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Biometric Based Authentication for MANET Using Efficient Fingerprint

T. Priyanka[1], E.Ramaraj[2]
[1]M.Phil Research Scholar Department of Computer Science & Engineering, Alagappa University
[2] Professor, Department of Computer Science & Engineering, Alagappa University,
Karaikudi, Tamilnadu
[1]tpriyankamsccs@gmail.com
[2]Eramaraj@rediffmail.com

Abstract: - Human users find complex to remember password or passphrase. Hence, researchers, for a time-consuming phase, have been considering to use biometric traits of the user rather than memorable password or passphrase, in a challenge to produce tough and repeatable cryptographic keys. This paper propose an efficient approach based on fingerprint for creating a secure cryptographic key, where the security is more improved with the complexity of factoring large numbers. Initially, the features, minutiae points from fingerprint are extracted. Finally, extracted pattern is used for generating a 256-bit cryptographic key.

Keywords- Biometrics, Fingerprint, Minutiae, Cryptographic key.

I. INTRODUCTION

Biometrics refers the physical or behavioral characteristics of persons used for identity verification. Biometric systems have been used many physical body parts and personal features: hands, fingers, feet, irises, retinas, voices, signature, ears, teeth, veins and DNA. Unimodal biometric system use one biometric feature to identify individuals. Multimodal biometric system use combination of biometric features to identify individuals. Multimodal biometric systems use multiple characteristics to overcome the limitations that occur when using single biometric feature to identify individuals. Multimodal biometric systems execute better than unimodal biometric systems. Multimodal biometric authentication has newly evolved as an interesting research area. it is more reliable as well highly capable than knowledge-based (e.g. Password) and token-based (e.g. Key) techniques. The following are very few good advantages of multimodal biometrics 1) improved accuracy 2) in case if adequate data is not extracted from a specified biometric sample, it can serve as a secondary means of enrollment as well as identification or verification and 3) the capability to identify endeavors to spoof biometric authentication via non-live data sources mostly fake fingers.

II. LITERATURE REVIEW

Jagadeesan et al. [1] developed a approach for cryptographic key creation with fusion of fingerprint and iris biometrics features. The fingerprint extraction is based on minutiae and the iris feature extraction is based on Hough transform (Daugman's pproach) and canny edge detector. The minutiae points of fingerprint and texture properties of iris images were first extracted, and then they were fused to get the multibiometric pattern and then a 256-bit secure cryptographic key is generated from the multibiometric pattern.

Baig et al. [2] presented a paper for multimodal biometric based on fusion of both modalities (iris and fingerprint). They used the West Virginia University's multimodal database containing 400 images (4 enrolment images×100 users) for the experiment and the threshold is set to the equal error rate EER.

Jameer Basha et al. [3] described a new approch for fusion of iris and fingerprint at rank level; There are three implemented fusion methods are used to conduct experimental tests: logistic regression method, highest rank method, and Borda count method.

Radha and Kavitha [4] presented a paper fusion method of fingerprint and iris modalities. The method uses a combined feature of both fingerprint and iris.

The features of both modalities are extracted by using the log Gabor. A final match score is generated by using Hamming distance (HD). Experimental results were confirmed for 200 users on database and the execution time required to match is reduced to 0.15 seconds.

Abdolahietal [5] described a paper a multimodal biometric method (iris and fingerprint) using fuzzy logic and weighted code. After transforming fingerprint and iris features to a binary code, the result stage combination is used to merge the results. The work completed with better accuracy.

III. PROPOSED FRAMEWORK

In the proposed approach, fingerprint is used for cryptographic key generation, Since it is intricate for an intruder to spool multiple biometric characteristics concurrently, there are possibilities to give more security for key generation. The necessity to memorize or carry lengthy passwords or keys is converted by the biometrics in the cryptography. The following section describes the technique of extracting the minutiae points from the fingerprint photo

Minutiae points' extraction from fingerprint

The steps involved in the proposed method for minutiae extraction are as follows,

A. Image development based on local statistics with neighborhood operations
B. Extraction of ROI
C. Orientation field Estimation
D. Extraction of minutiae

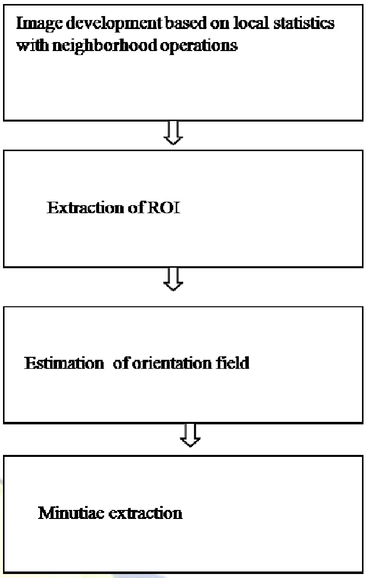


Image development based on local statistics with neighborhood operations
Extraction of ROI
Estimation of orientation field
Minutiae extraction

Fig.1 Process of Proposed Framework

Each step of this proposed framework is discussed in following manner.

A. Image development based on local statistics with neighborhood operations

To improve the fingerprint image, we use the technique based on local statistics. This process makes use of sliding neighborhood operations for picture improvement where, For processing the Sliding Neighborhood Operation the non-linear filter is used. initially, the input photo is processed with a sliding blocks. For every sliding block, the centre pixel of the sliding block is modified with the local response of the related sliding block (LR) when, condition 1,2 and 3 are satisfied. block

Condition 1: $Mb < KM * M F$
Condition 2: $Vb < KV * VF$
Condition 3: $Vb > KV * VF'$.

Otherwise, the local response is equal to the centre pixel value of the sliding block (Fb). The local response of the sliding block is designed based on the following equation, Local response, $LR = E \times Fb$

Finally, we get the improved fingerprint image, where the visual quality of the picture is considerably enhanced so that the identification of ridges can be simply achieved.

B. Extraction of ROI

ROI is the region of interest in the enhanced fingerprint image which is significance for extraction of minutiae points. Initially, the fingerprint is separated into non overlapping blocks of size 16x16. Then, the gradient of every block is created. The gradients standard deviation (SD) in X and Y direction are computed and added. The block is filled with ones merely if the resulting value exceeds the threshold value, else zero is filled in the block.

C. Orientation field Estimation

The gradient based method is used to estimate the orientation field of the fingerprint image. In gradient based methods, initially, the gradient vectors are calculated for a fingerprint by obtaining the part derivatives of gray force at every pixel. It is possible to specify a gradient vector as [gx, gy] T in Cartesian coordinates. In a fingerprint image, the gradient vectors, always point to the instructions of the peak difference of gray force that are vertical to the edges of ridge lines. A collection of two-dimensional direction fields is known as fingerprint orientation map. The magnitudes of these fields can be ignored. An orientation chart is generally denoted as a matrix θ_{xy}, where θ_{xy} Σ [0, Π].

D. Extraction of Minutiae

The minutiae point extraction used the enhanced fingerprint image. First apply the binarization and morphological operations to the enhanced fingerprint image to perform the extraction process. The process of converting a gray level image into a binary image is called binarization. Morphological operations are used to remove unnecessary bridges, spurs and line breaks. The ridge thinning algorithm is used for eliminating the unnecessary pixels till the ridges become one pixel wide. The Ridge thinning algorithm used for extraction of Minutiae points‟ in the proposed method has been used. once that, minutiae points are retrieved from the thinned fingerprint. The main minutiae features of fingerprint ridges are: ridge ending (the quick end of a ridge), bifurcation (a single ridge that splits into two ridges). The method of extraction of minutiae points such as ridge ending and bifurcation is discussed as:

(1) Standardize the fingerprint picture resulted from ROI extraction (FD) to the size of the thinned fingerprint.

(2) Compute the Euclidean space change of the fingerprint photo, FD.

(3) For every pixel (p(i)) excluding the boundary pixel in the thinned fingerprint, neighbor pixels, 1 2 8 p , p ,..., p are recognized.

Where, p1, p2 ,..., p8 are the values of the eight neighbors of p(i), opening with the east neighbor and numbered in counterclockwise order.

(4) Compute the value Q(i) for every pixel p(i).

$$Q(i)=0.5*\left[(p_8-p_1)+\sum_{i=1}^{7}(p_i-p_{i+1})\right]$$

(5) The position is said to be a ridge ending points, when Q(i) 1 and FD (i) >6 .

(6) The position is said to be a bifurcation points, when Q(i)> 3and FD(i) > 6 .

The recognized ridge ending and bifurcation points are denoted as minutiae points that are distinctive features identified within the fingerprint templates. These points are used for creating the secured cryptographic key generation.

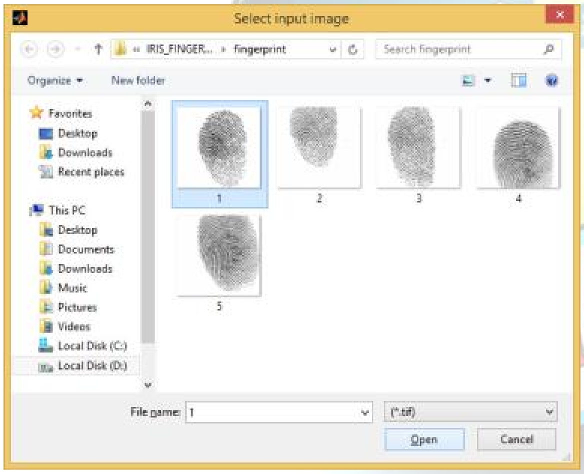
IV. RESULT AND DISCUSSION

In this paper a novel of fingerprint biometrics is used for authentication in order to get best cooperation among a zero FAR and its equivalent FRR; in our technique, fingerprint feature has more power and the system conclusion is made to have more middle values between bad and good identification; the weight is simply an admiration to the matching distance for each single biometric set by

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

fuzzy association function and most important concepts of fuzzy logic introduced which are fuzzy sets, fuzzy association function, and fuzzy deduction method. The fuzzy inference method mimics our human thoughts and this is mostly the reason we get enhanced results.

In fingerprint recognition both verification and identification process are implemented. The GUI allowing the user to load fingerprint images and then visualize the result of each step of the fingerprint recognition algorithm. The recognition process in the fingerprint identification system contains of matching the generated code from the input image with all codes stored in database; if the identification failed, the user is asked either to add or not the non identified image to a chosen database.



File name: 1
(*.tif)

Fig.2 Selection of input image

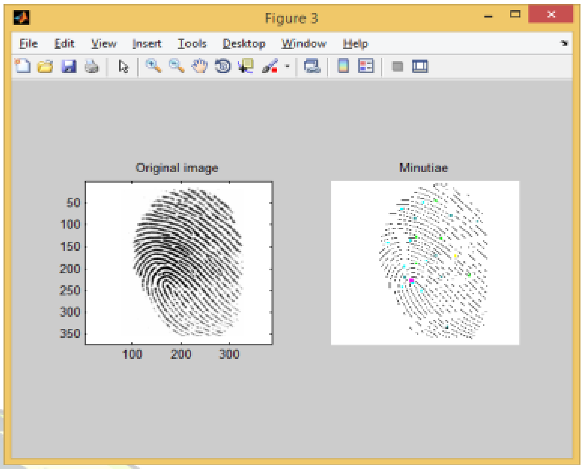


Fig.3 Extraction of Minutiae Points from Original Image

V. CONCLUSION

In this work, the biometric approach is used for authentication. The fingerprint image is used for Cryptographic key generation. The proposed approach enhances the security by incorporating the complexity of factoring the large number. The proposed method contains four steps namely, 1)Image development based on local statistics with neighborhood operations. 2) Extraction of ROI 3) Orientation field Estimation. 4) Extraction of minutiae. Initially, From the fingerprint image, the minutiae points are extracted for authentication. In a future, After fingerprint minutiae point extraction, the texture properties are extracted from iris images. Then, the extracted features are integrated at the feature level to create the multi biometric pattern and then 256-bit secure cryptographic key is generated from the multi biometric pattern for better security.

VI. REFERENCES

[1] Yan Yan and Yu-Jin Zhang, “Multimodal Biometrics Fusion Using Correlation Filter Bank", in proceedings of 19th International Conference on Pattern Recognition, pp. 1-4, Tampa, FL, 2008.

[2] Arun Ross and RohinGovindarajan, "Feature Level Fusion in Biometric Systems", in proceedings of Biometric Consortium Conference (BCC), September 2004.

[3] UmutUludag, SharathPankanti, SalilPrabhakar, Anil K.Jain, “Biometric Cryptosystems Issues and Challenges”, in Proceedings of the IEEE, vol. 92, pp.

948- 960, 2004. International Journal of Computer Applications (0975 – 8887) Volume 2 – No.6, June 2010 25

[4] P.Arul, Dr.A.Shanmugam, "Generate a Key for AES Using Biometric for VOIP Network Security", Journal of Theoretical and Applied Information Technology, vol. 5, no.2, 2009.

[5] Muhammad Khurram Khan and Jiashu Zhang, "Multimodal face and fingerprint biometrics authentication on space-limited tokens", Neurocomputing, vol. 71, pp. 3026-3031, August 2008.

[6] KornelijeRabuzin and Miroslav Baca and MirkoMalekovic, "A Multimodal Biometric System Implemented within an Active Database Management System", Journal of software, vol. 2, no. 4, October 2007.

[7] M Baca and K. Rabuzin, “Biometrics in Network Security”, in Proceedings of the XXVIII International Convention MIPRO 2005, pp. 205-210 , Rijeka,2005.

[8] N. Lalithamani and K.P. Soman, "Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced and Effective Scheme", European Journal of Scientific Research, vol.31, no.3, pp.372-387, 2009.

[9] A.Goh and D.C.L. Ngo, “Computation of cryptographic keys from face biometrics”, International Federation for Information Processing 2003, Springer-Verlag, LNCS 2828, pp. 1–13, 2003

[10] F. Hao, C.W. Chan, “Private Key generation from on-line handwritten signatures”, Information Management & Computer Security, vol. 10, no. 2, pp. 159–164, 2002.

[11] Chen, B. and Chandran, V., "Biometric Based Cryptographic Key Generation from Faces", in proceedings of 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp. 394 - 401, December 2007.

[12] N. Lalithamani and Dr. K.P. Soman, “An Effective Scheme for Generating Irrevocable Cryptographic Key from Cancelable Fingerprint Templates”, International Journal of Computer Science and Network Security, vol. 9, no.3, March 2009.