I.J. Image, Graphics and Signal Processing, **2015, 4, 51-59**
Published Online March 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2015.04.06

Accuracy Improvement in Palmprint Authentication System

Jyoti Malik[1], Dhiraj Girdhar[2]
[1]National Institute of Technology, Kurukshetra, India, [2]Computer Associates, Bangalore, India
E-mail: jyoti_reck@yahoo.com, girdhar.dhiraj@gmail.com

Ratna Dahiya[3], G. Sainarayanan[4]
[3]National Institute of Technology, Kurukshetra, India, HCL Technologies Pvt. Ltd, Chennai, India
E-mail: ratna_dahiya@yahoo.co.in, sai.jgk@gmail.com

Abstract—Biometric authentication has been emerged as a reliable means to control a person's access to physical and virtual places. Despite the various efforts made on biometrics, accuracy of the authentication/identification is the main concern and it has to be completely investigated. The paper presents critical analysis of the matching score values in such a manner that system accuracy is increased. Min Max Threshold Range (MMTR) technique is proposed that provides two levels of authentication and increase in accuracy is observed. The methodology of increase in accuracy is observed on various feature extraction methods.

Index Terms—Biometric system, palmprint, accuracy measurement, authentication.

I. Introduction

Biometric systems are being used for access-control, e-commerce and m-commerce activities and it is being considered as safe, secure and fast source for personal authentication. Biometric authentication system is dependent on various factors like cost, security, user acceptance, speed and accuracy etc. For identification/authentication, biometric system has to be evaluated on the parameter of accuracy because accurate authentication can prevent unauthorized access. A typical biometric system needs lots of volunteers for enrolment to make a large database. The various stages in biometric system like image acquisition, pre-processing etc. can affect system accuracy directly or indirectly. A biometric system is to be designed that can address various problems/factors affecting accuracy. The factors have to be resolved in such a manner that the accuracy of the system can be increased.

Security is an important issue with the advancement in information technology. USA, UK and several other countries are using biometric passport to control access from country borders [1, 2]. If the system is not accurate, an innocent person can be doubted/questioned as intruder/impersonator. Using biometric systems for access control or online banking, highly accurate judgment of person is required otherwise it can lead to great loss in terms of money and security. Improvement and increase in accuracy is desired in biometric systems [3, 4].

The aim of this paper is to present various factors affecting accuracy and improvement in accuracy validated by experimental results on palmprint biometric system. Section II presents accuracy and the factors affecting accuracy. Section III describes the proposed accuracy improvement framework implemented on various feature extraction based palmprint biometric system and concluded in section IV.

II. Accuracy and Factors Affecting Accuracy of a Biometric System

A. Accuracy of a biometric system

In password and token based authentication system, perfect comparison of user input data with stored template (password/token value) is possible. However, biometric authentication systems decision making is affected at every stage by various factors like noise in biometric sensor, illumination, environmental conditions, type of biometric used, feature extraction method, matching algorithm etc.

Accuracy of biometric system is measured in terms of image acquisition errors and image matching errors. Image matching errors are False match rate (FMR) and False non-match rate (FNMR). Image acquisition errors include Failure-to-enrol (FTE) and Failure-to-acquire (FTA). Accuracy can be defined in terms of FAR and FRR that considers both image matching and image acquisition errors.

$$Accuracy(\%) = \left(100 - \left(FAR(\%) + FRR(\%)\right)/2\right) \quad (1)$$

where, FAR is the percentage of number of wrongly accepted individuals over the total number of wrong matching,

FRR is the percentage of number of wrongly rejected individuals over the total number of correct matching.

B. Factors affecting Accuracy

There are several aspects that affect the accuracy in a biometric system, it can be design and implementation or security based aspects.

1. Selection of biometric

The selection of biometric for an application is determined by the properties of biometric characteristics and based upon the requirements of the application. For example, a facial recognition will not produce accurate/good results for highly security related applications as compared to iris recognition. The type of biometric chosen can also affects the accuracy of the system.

2. User Acceptance and Privacy

The sensors used to capture biometric significantly affect user acceptance. Stress, mood, motivation, comfort in using sensor etc. Of user can affect the accuracy of the system. The quality of sensor, ease of use, ability to handle injuries to the biometric identifiers etc. also plays major role in user acceptance and accuracy of the system. Privacy of user also should not be compromised while capturing biometric. It should be collected for specific reasons and under specific conditions to serve the purpose that is promised.

3. Biometric Fusion Strategy

Fusion of two biometrics can also affects accuracy of the system. The type and level of fusion of two biometric can lead to overall increase/decrease in accuracy. This is the case of multimodal biometric which is beyond the scope of this paper.

4. Enrolment and Verification Process

In real time authentication system, the accuracy of the system is poorly affected by if the enrollment and verification processes are not properly conducted. For good quality templates, it is better to give training session to individuals. The ability of the system to reject poor quality samples is required because poor quality templates can lead to reduction in accuracy of verification system.

Similarly, quality of samples captured during verification also plays an important role. Environmental factors, noise, illumination conditions can have great impact on accuracy. Sensors used during enrollment are sometimes different from the sensors used for verification. It can also be costly affair to re-enrol all the users because the earlier acquisition device is outdated.

5. Spoofing Attacks

Accuracy of biometric authentication system depends on the security of each component of the system. More vulnerability leads to less accuracy or failure of authentication system, if an imposter is able to access as authorized user. In palmprint authentication system spoofing using artificial mould or clone is not easily feasible because palmprint cannot be found on objects. Using liveness detector acquisition system can reduce the chances of spoofing using fake biometric.

6. Replay Attacks

Biometric templates are converted into digital information so that it can be further processed. If attacker can obtain the digital information by attacking weak component of the authentication system, it can lead to failure of authentication system if same information is injected/replayed to fool the system. It is advisable to encrypt the information but it cannot prevent replay attack. Combining nonce before encrypting biometric templates can serve the purpose.

7. Biometric Template Attack

Biometric templates stored in database are prone to risk of getting compromised. If the attacker is able to replace original template with imposter template, it will be easy to fool the system. To maintain the integrity and confidentiality of template, various steps like encryption or digital signature etc are to be taken.

8. Trojan Horse Attack

With Trojan horse attack, the decision making identifier of authentication system can be compromised. It can yield “yes” decision to all authentication attempts.

The various types of attacks like spoofing, replay, biometric template and Trojan horse can lead to system compromise/failure and affects accuracy of the system.

III. Proposed Reference Threshold Calculation Algorithm

A. Palmprint biometric system

Palmprint biometric is the impression made by palm of the hand. Palmprint biometric is considered more accurate than other biometric traits because it fulfils the maximum criterion for factors affecting accuracy as mentioned in section II. Palmprint biometric is user acceptable as it is not considered to be related to criminal records. It can be fused with hand geometry biometric by using the same acquisition device. Enrolment and verification of palmprint is user friendly and it can work for low resolution images [4]. The enrolment and verification system is shown in Fig. 1.

Because of its small size it can be combined with other factors of authentication to avoid attacks on the system. The attacks on system are more based on security and not on biometric selection. But it can play an important role in providing more factors/level in authentication against attacks.

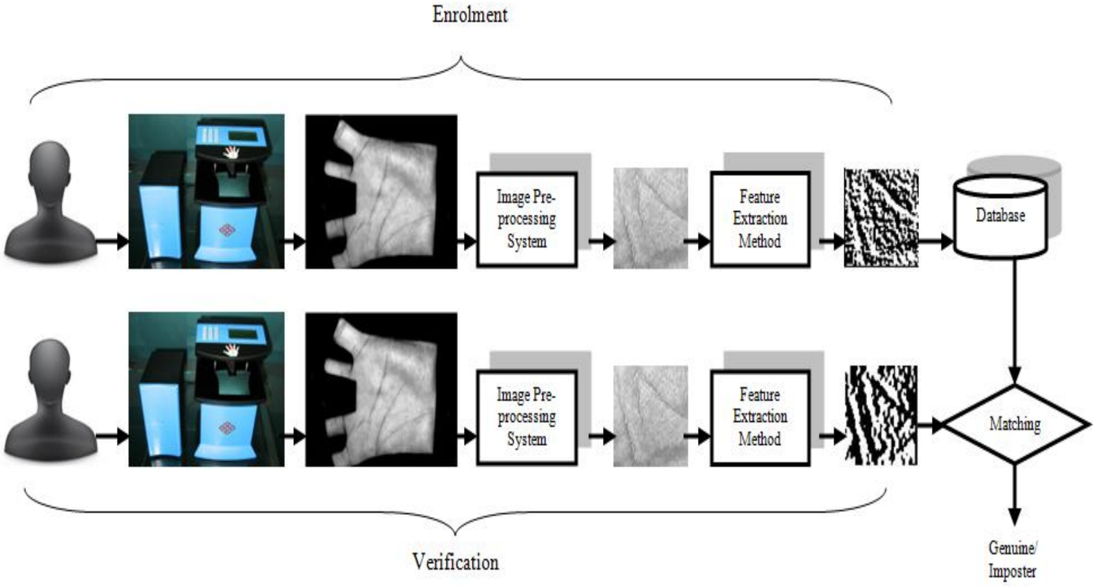

Enrolment
Image Pre-processing System
Feature Extraction Method
Database
Image Pre-processing System
Feature Extraction Method
Matching
Genuine/ Imposter
Verification

Fig. 1. Enrolment and verification in palmprint authentication system

B. Reference Threshold

Accuracy plays an important role in authentication system and it depends on the value of reference threshold chosen [20]. Reference threshold can be defined as a value which decides whether the person is genuine or imposter as shown in Fig.2.

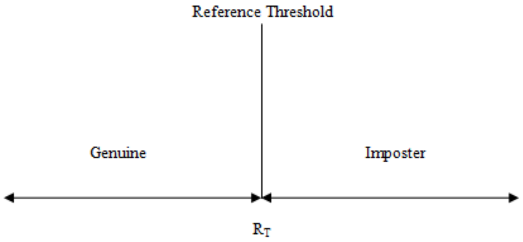


Fig. 2. Criteria of authentication

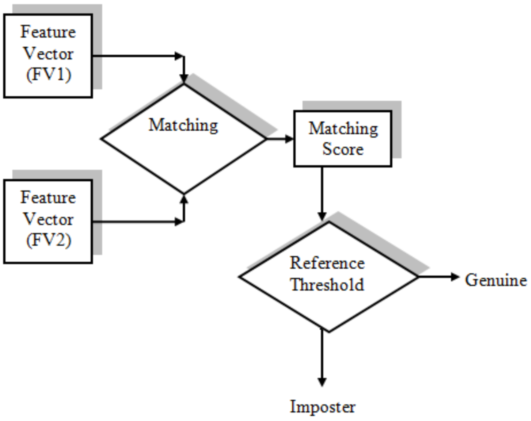


Fig. 3. Matching of two feature vectors

The feature vectors mentioned in Fig. 3 are basically palmprint biometric features stored in vector form. The palmprint line features are principal lines, wrinkles and ridges extracted from the palmprint. These line features are referred as feature vectors. The two feature vectors used in palmprint matching are: first from enrolment stage or database and second from authentication stage. A matching algorithm describes the degree of similarity between two feature vectors. The matching of two feature vectors and the matching score generated because of the comparison is analyzed on the basis of reference threshold. The feature vectors are basically features stored in vector form and referred as feature vector.

From Fig.3, if the matching score generated should be less than or equal to reference threshold, the user is considered as genuine. It is represented by (2) as

$$\left.\begin{array}{l} Matching\ \ Score \le R_{TH} \\ Matching\ \ Score > R_{TH} \end{array}\right\} \begin{array}{l} Genuine \\ Intruder \end{array} \tag{2}$$

So, choosing right value of reference threshold is very important in authentication system. Training of the system is done to find suitable value of reference threshold.

In real time authentication system, if a person's hand is compared with the samples present in the database, the authenticity depends on the matching score. Even if the same hands are compared in authentication system, there will not be 100% matching. The matching score (MS) will have some value, shown in Fig.4.

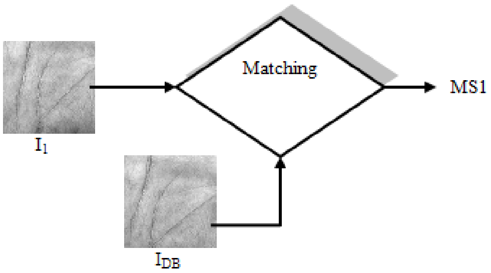


Fig. 4. Matching of I1 with IDB

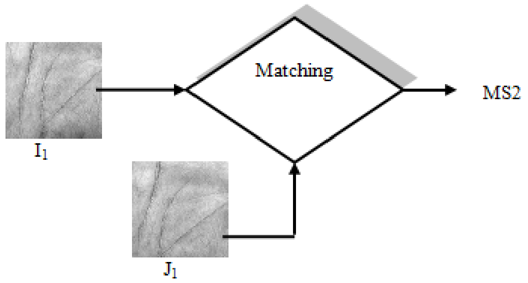


Fig. 5. Matching of I1 with J1

Similarly, when two very different hands are compared even then the matching score will have some value as shown in Fig.5.

It's the decision of correct value of reference threshold value which basically differentiates the same hands from different hands and it can also be concluded from Fig. 4 and Fig. 5. So, it is very important to choose correct value of reference threshold.

Choosing wrong value of reference threshold can lead to two kinds of possible errors: false matches (false acceptance) and false non-matches (false rejection). A false match is said to occur when an acquired template is erroneously matched to a template stored from enrolment, although belonging to two different persons. A false non-match occurs when an acquired template is not matched with the template stored from enrolment, although belonging to the same person. The error rates vary from one biometric to another and also depend on the setting of the threshold.

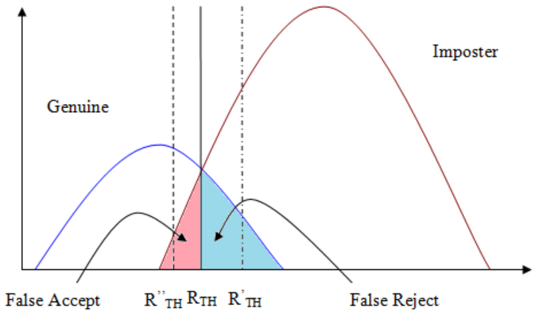


Fig. 6. Genuine and Imposter distribution

It is clear from Fig. 6 that the genuine and imposter distribution can be represented by Gaussian curve. There is overlapping of genuine and imposter distribution which has to be fine tuned to one value of reference threshold R_{TH}. Sliding of R_{TH} value to R'_{TH} leads to decrease in false rejection but increase in false acceptance. Similarly, Sliding of R_{TH} value to R''_{TH} leads to decrease in false acceptance but increase in false rejection. So, choosing a correct value of reference threshold is very important, otherwise it can lead to false acceptance or false rejection. The accuracy of the system increases if the value of FAR, FRR decreases as shown in (1).

C. *Min Max Threshold Range (MMTR)*

Authentication is done by choosing a reference threshold value but this value is sometimes not able to distinguish between genuine and imposter person. To decide the authenticity of the person, a range of threshold values for each individual are found out. The threshold values range will decide whether the person is genuine or imposter.

The main problem with reference threshold authentication is that single value is not good enough to decide the authenticity of the person. It can be seen in Fig. 7 that choosing reference threshold (R_T) is very important in an authentication system. If $R_T{}'$ is chosen as reference threshold, then the person earlier as genuine becomes imposter. It means the person is falsely rejected due to change in reference threshold value.

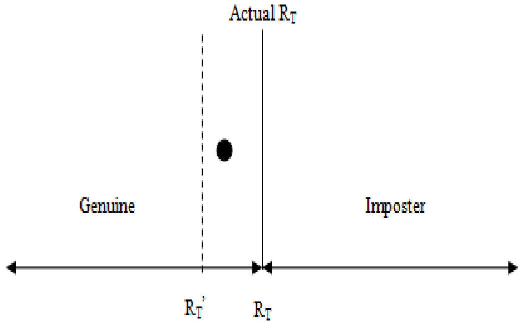


Fig. 7. False Rejection by shifting RT

Similarly, in Fig. 8, if $R_T{}'$ is chosen as reference threshold, then the person earlier as imposter becomes genuine. It means the person is falsely accepted due to change in reference threshold value.

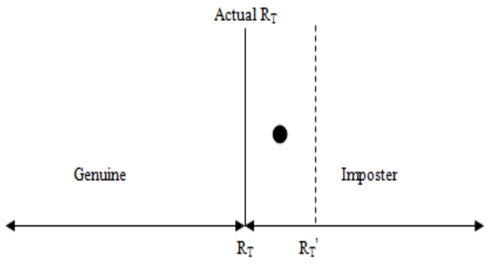


Fig. 8. False Acceptance by shifting RT

It can be seen from Fig. 7 and Fig. 8 that wrong selection of reference threshold can lead to increase in false acceptance and false rejection. In Fig. 9, if the matching score value T lies very close to reference threshold but greater than reference threshold value, there are chances of the person to be considered as imposter.

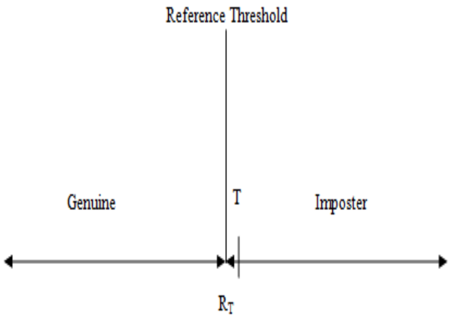


Fig. 9. Matching score (T) near reference threshold

In Fig. 10 if the matching score value T lies very close to reference threshold but less than reference threshold value, there are chances of the person to be considered as genuine.

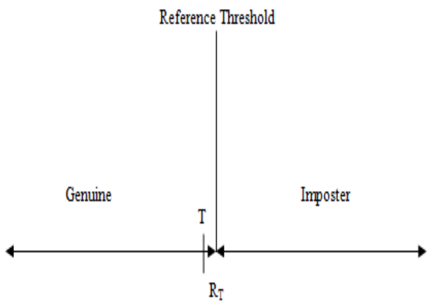


Fig. 10. Matching score (T) near reference threshold RT

In Fig. 11, R_T is the reference threshold value where FAR and FRR is minimum. If $R_T{}^{'}$ is chosen as reference threshold, FAR increase and similarly if $R_T{}^{''}$ is chosen as reference threshold then FRR increases. So, instead of choosing single value for authentication, range of values is chosen for authentication.

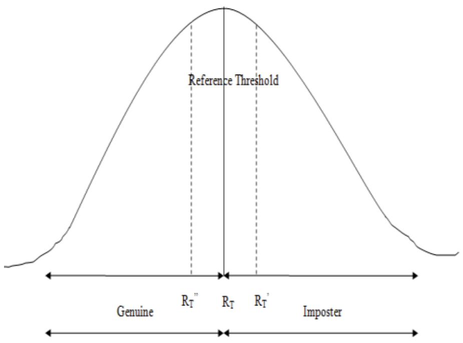


Fig. 11. Selection of reference threshold

In case of chances of false acceptance and false rejection with reference threshold values the person has to again go through the procedure of authentication. Reference threshold (R_T) and range of threshold values (T_{MAX} and T_{MIN}) together makes an authentication system, to authenticate a person. The various threshold values and R_T are arranged in the following manner in an authentication system as shown by Fig. 12.

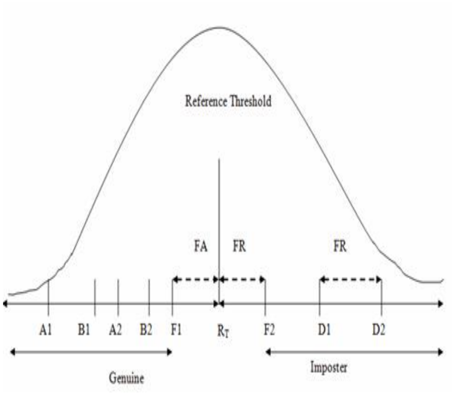
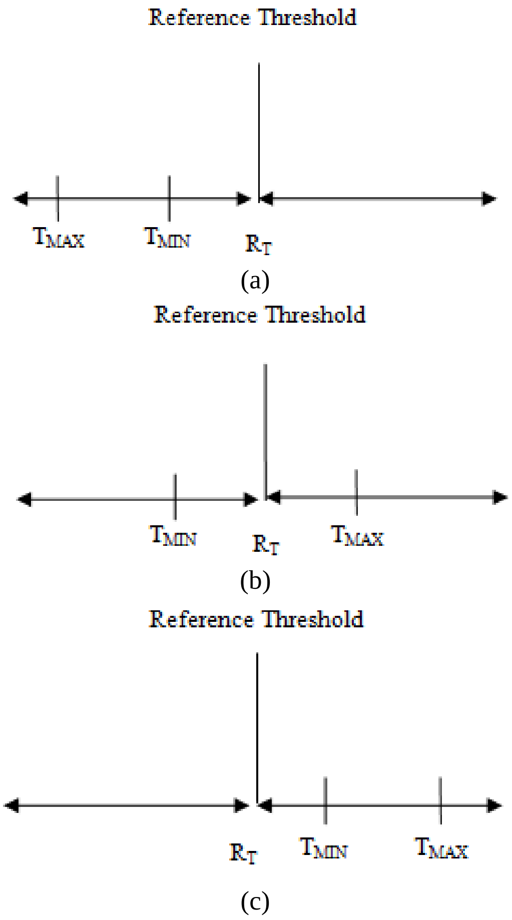


Fig. 12. Various threshold values and RT

All threshold values lie on a Gaussian curve. $A_{1,}$ A_2 are the threshold range for one person, $B_{1,}$ B_2 are the threshold range for another person. Similarly, $D_{1,}$ $D_{2,}$ $F_{1,}$ F_2 all threshold values lie on threshold scale. Suppose person A, matching score lies below R_T and in the range of $A_{1,}$ A_2, person A is considered genuine. Hence, in MMTR technique R_T and threshold range decides the authenticity of person, failure to fulfill one of the condition can leads to false acceptance or false rejection.

The values of $R_{T,}$ T_{MAX} and T_{MIN} can be arranged in any manner in an authentication system as shown by Fig. 13.



(a)

(b)

(c)

Fig. 13. Arrangement of RT, TMAX and TMIN values

In this work, Min Max Threshold Range (MMTR) method is proposed that helps in increasing overall system accuracy by matching a person with multiple threshold values. In this technique, firstly the person is authenticated at global level using Reference threshold (R_T). Secondly, the person is authenticated at local level using range of Minimum and Maximum thresholds (T_{MAX} and T_{MIN}) defined for a person. Generally, personal authentication is done using reference threshold but there are chances of false acceptance. So, by using the Minimum and Maximum Thresholds range of false accepted persons at personal level, a person is identified to be false accepted or genuinely accepted.

It can be noted in Fig. 14 if the person matching score is below R_T and within T_{MAX} and T_{MIN}, the person is considered genuine. If the person lies in the range shown by dotted arrows then it fulfills only reference threshold criteria and does not lie in the minimum maximum range, so the person is false accepted. In this manner, by providing second level of authentication, false acceptance can be avoided.

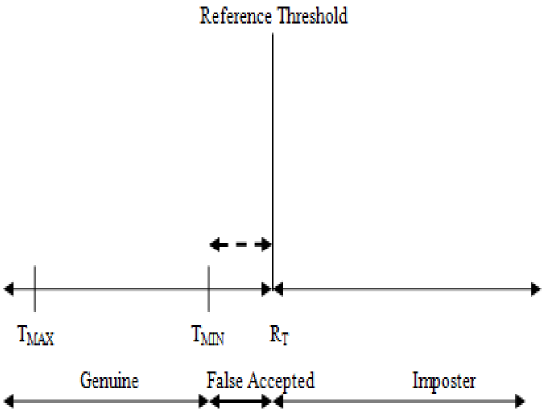


Fig. 14: Criteria of authentication with MMTR method to reduce FAR

In Fig. 15, if the person matching score is above R_T and within T_{MAX} and T_{MIN}, the person is considered genuine. If the person lies in the range shown by dotted arrows then it fulfills only reference threshold criteria and does not lie in the minimum maximum range, so the person is false rejected. In this manner, by providing second level of authentication, false rejection can be avoided.

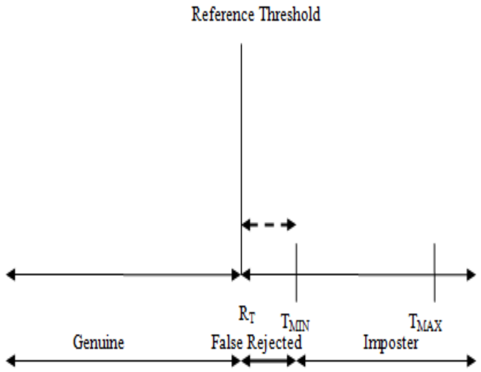


Fig. 15: Criteria of authentication with MMTR method to reduce FRR

MMTR is an effective technique to increase the accuracy of the palmprint authentication system by reducing the FAR/FRR [5, 6, 7].

D. Experimental Results and analysis on various feature extraction methods

Min Max Threshold Range (MMTR) method is about increasing the accuracy of the authentication system by reducing the FAR/FRR of the system. The PolyU palmprint database [8] is used to implement MMTR technique on palmprint biometric. MMTR method is applied on Real Wavelet [9], Sobel Code method [10][11], Canny operator [12], Phase Congruency method (line)[13][14][15], Phase Congruency method (corner) and Harris corner [16][17][18][19] etc. and significant increase in accuracy is observed. The selection of various types of feature extraction methods are as explained in table 1.

Table 1. Feature extraction methods used in MMTR method

Feature Extraction Method	Type of Method	Type of Feature to be extracted	Feature Matching Method	DB Preparation Time
Real Wavelet	Multi-resolution and intensity based method	Line	Hamming distance	1.36E-01
Sobel Code	Directional and Intensity based method	Line	Hamming distance	4.10E-02
Canny edge	Intensity gradient based method	Line	Hamming distance	4.73E-02
Phase Congruency	Intensity gradient invariant method	Line	Hamming distance	2.95E-01
Phase Congruency	Intensity gradient invariant method	Corner	Match by Correlation	3.24E-01
Harris	Intensity gradient based method	Corner	Match by Correlation	1.56E-01

Table 2. Threshold Values, FAR, FRR and Accuracy Values after MMTR for various feature extraction methods

Method	Reference Threshold	Without MMTR			With MMTR			% Accuracy Improvement
		FAR	FRR	Accuracy	FAR	FRR	Accuracy	
Sobel Code	0.879	0.0462	0.00025	96.7	0.0148	0.000121	99.2	2.5
Real Wavelet	0.804	0.155	6.73E-03	91.9	6.59E-02	8.94E-04	96.67	4.77
Phase Congruency (Line)	5.96E-01	7.10E-02	4.63E-04	96.4	2.65E-02	1.21E-04	98.6	2.2
Canny Edge	8.54E-01	9.47E-02	5.68E-03	95	9.54E-03	3.05E-03	99.3	4.3
Phase Congruency (Corner)	5.77E-01	4.92E-02	3.74E-04	97.5	2.01E-02	1.83E-04	98.99	1.49
Harris Corner	9.83E-01	4.29E-02	6.90E-03	97.5	2.14E-02	2.63E-03	98.8	1.3

Improvement in accuracy and reduction in FAR/FRR is achieved by using MMTR technique on various feature extraction methods. Table 2 tabulates the effect of MMTR on various parameters like FAR, FRR and accuracy. It can be concluded from Table 2 that Real Wavelet method performs better with MMTR method and 4.7% increase in accuracy is observed. Canny edge method also performs better and close to Real Wavelet method with an accuracy improvement of 4.3%. The improvement in accuracy, FAR and FRR is shown by bar graph in Fig. 16, Fig. 17 and Fig. 18.

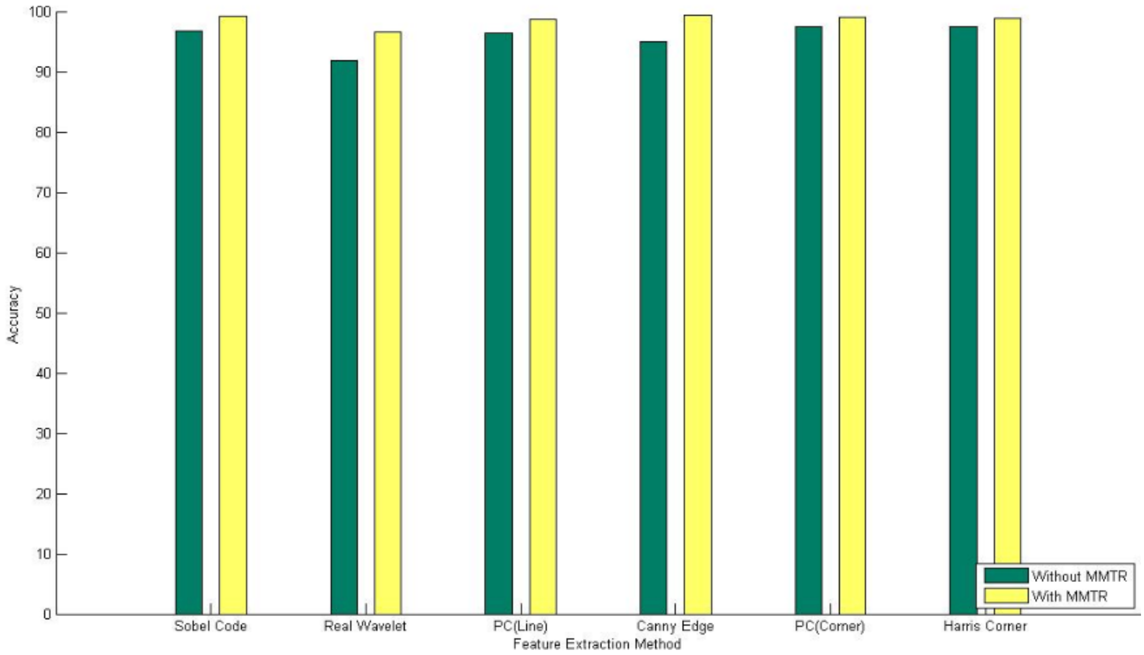


Fig. 16. Feature Extraction method Vs Accuracy without MMTR and with MMTR

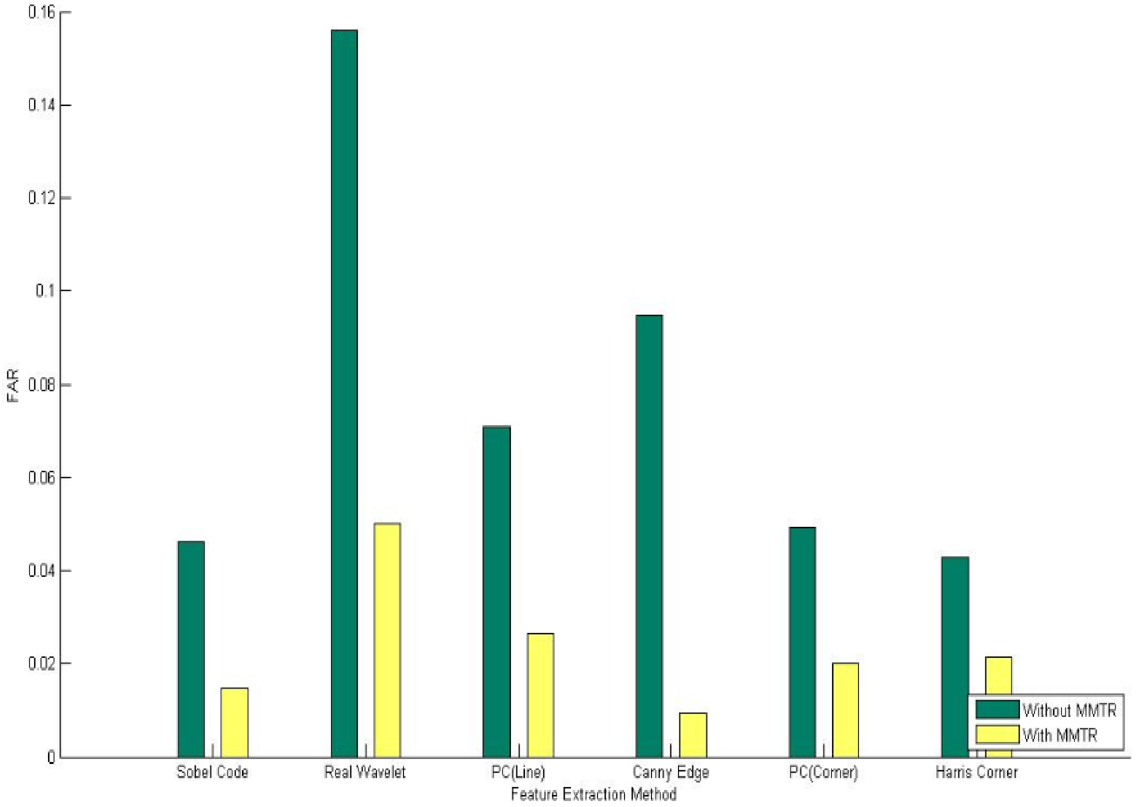


Fig. 17. Feature Extraction method Vs FAR without MMTR and with MMTR

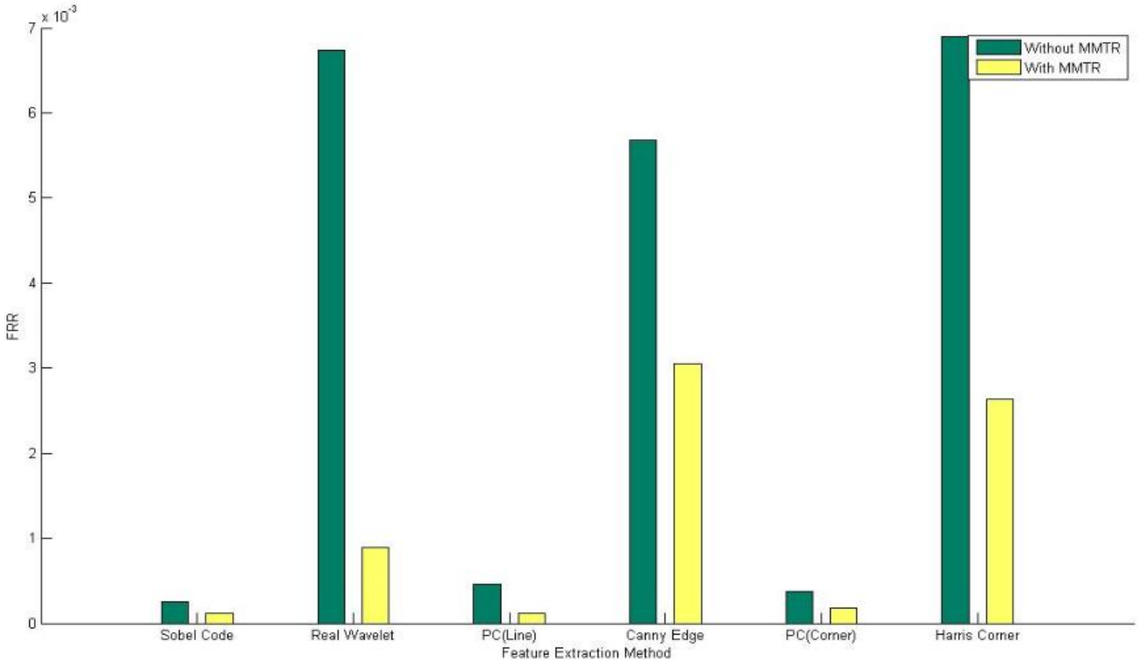


Fig. 18. Feature Extraction method Vs FRR without MMTR and with MMTR

IV. Conclusion

Traditional authentication using reference threshold is inadequate in terms of user authentication. The accuracy of biometric system is less in real world applications due to various critical factors. The accuracy of user authentication system can be increased using proposed MMTR technique. MMTR is applied on various feature extraction methods like Sobel Code, Real Wavelet, Phase Congruency line detector, Canny Edge, Phase Congruency corner detector, Harris corner method and two different matching methods like Hamming distance and Match by correlation method. Improvement in accuracy and reduction in FAR/FRR is achieved by using MMTR technique on various feature extraction methods and feature matching methods. Application of MMTR technique on various feature extraction and matching methods concludes its versatility.

References

[1] K. Jain, R. Bolle, and S. Pankanti, “Biometrics: Personal Identification in Networked Society”, United States of America: Springer Science Business Media, Inc. 2006.

[2] Woodward, Jr. J. D., Orlans N. M. and Higgins P. T., “Biometrics: Identity Assurance in the Information Age”, United State of America: The McGraw-Hill Companies, 2003.

[3] Zhang, D., “Palmprint Authentication”, Boston: Kluwer Academic Publishers, 2004.

[4] D. Zhang, W. Kong, J. You, M. Wong, “Online palmprint identification”, IEEE Trans. Pattern Anal. Mach. Intelligence, Vol. 25, No. 9, pp. 1041-1050, 2003.

[5] Jyoti Malik, G. Sainarayanan, Ratna Dahiya, “Min Max Threshold Range (MMTR) Based Approach in Palmprint Authentication by Sobel Code Method”, ELSEVIER, Procedia Computer Science, Proceedings of the International Conference and Exhibition on Biometric Technology, Volume 2, pp 149-158, 2010.

[6] Jyoti Malik, G. Sainarayanan, Ratna Dahiya, “Min Max Threshold Range (MMTR) based Approach in Palmprint Authentication by Phase Congruency Features”, IEEE Proceedings of International Conference on Signal and Image Processing (ICSIP), pp. 388-393, Chennai, 2010.

[7] Jyoti Malik, G. Sainarayanan, Ratna Dahiya, “Min Max Threshold Range (MMTR) Approach in Palmprint Authentication”, SpringerLink, Advanced Computing, Communication in computer and Information Science, vol. 133, part -5, pp. 438-449,2011.

[8] PolyU Palmprint Database. 2005. The Hong Kong Polytechnic University (PolyU), Palmprint Database. URL: http://www.comp.polyu.edu.hk/~biometrics/.

[9] Wu X. Q., Wang K. Q. and Zhang D., “Wavelet Energy Feature Extraction and Matching for Palmprint Recognition”, Journal of Computer Science and Technology, Volume 20, No. 3, pp. 411-418, May 2005.

[10] Wong K. Y. E., Jamal A. Dargham, Ali Chekima and G. Sainarayanan, “Palmprint Identification Using 5 x 5 Sobel Operator,” Proceedings of First Seminar on Engineering and Information Technology, pp. 208-211, 14-15 April 2008, Sabah Malaysia.

[11] Wong K. Y. E., Ali Chekima, Jamal A. Dargham and G. Sainarayanan, “Palmprint Identification using Sobel Operator,” 10th international Conference on Control, Automation, Robotics and Vision 2008, ICARCV 2008, pp. 1338-1341, 17-20 December 2008, Hanoi, Vietnam.

[12] CANNY J.F, “A computational approach to edge detection”, IEEE Trans. Pattern Anal. Mach. Intell., vol. 8, no. 6, pp. 112–131, 1986.

[13] Kovesi P, “Image features from Phase Congruency”, Videre J. Comput. Vis. Res., Vol. 1, No. 3, pp. 1–26, 1999.

[14] Yunyong Punsawad and Yodchanan Wongsawat, “Palmprint Image Enhancement Using Phase Congruency”, Proceedings of the 2008 IEEE International Conference on Robotics and Biometrics, pp. 1643-1646, February 21-26, 2009.

[15] V. Struc and N. Pavesic, “Phase Congruency features for palmprint verification”, IET Signal Processing, Vol. 3, Iss. 4, pp. 258-268, 2008.

[16] Harris and M.J. Stephens, “A combined corner and edge detector,” in 4th Alvey Vision Conference, Manchester, UK, pp. 147–151, 1988.

[17] Frank Nielsen, “Harris-Stephens' combined corner/edge detector”, September 2009.

[18] Konstantinos G. Derpanis, “The Harris Corner Detector”, pp. 1-2, 2004.

[19] Niels Chr. Overgaard, “On a Modification to the Harris Corner Detector”, Proc of the Symposium Svenska Sällskapet för Bildanalys, 2003.

[20] Jyoti Malik, Dhiraj Girdhar, Ratna Dahiya, G. Sainarayanan, “Reference Threshold Calculation for Biomteric Authentication”, MECS, I. J. Image, Grapics and Signal Processing, vol. 6, no. 2, pp. 46-53, January 2014.

Authors’ Profiles

Jyoti Malik received her B.Tech in 2002 from R.E.C, Kurukshetra University, Haryana, and M.Tech in 2004 from NIT, Kurukshetra, Deemed University, Haryana. Presently, she is pursuing her Ph.D. in the area of biometric authentication from NIT, Kurukshetra. Her research interests are Image processing, Pattern recognition and Signal processing.

Ratna Dahiya received her B.Tech from GBU, Pant Nagar and M.Tech and Ph.D. degree in Electrical Engineering from R.E.C, Kurukshetra, Kurukshetra University, Haryana, India. Currently, she is working as Asstt.Prof. in Electrical Engineering Department with the NIT, Kurukshetra (Deemed University), Haryana, India. Her research interests include Image processing, Pattern recognition, SMES, Induction Machines, Power quality, Motor drives and Renewable energy.

Dhiraj Girdhar received his B.E (Gold Medalist) in 2003 from Sant Longowal Institute of Engineering and Technology (SLIET), Sangrur, Punjab Technical University, Punjab. M.S. in 2007 from BITS, Pilani. Presently, he is working with Computer Associates, Bangalore. His research interests are Image processing, Pattern recognition, Multimedia and Cryptography.

G. Sainarayanan is currently working in HCL Technologies Pvt. Ltd., Chennai. He received his B.E., M.E., and Ph.D. degrees, respectively, from Annamali University, India, Bharathiar University, India, and University Malaysia Sabah, Malaysia, in 1998, 2000, and 2002. His research interests are in the areas of Vision rehabilitation, Medical imaging and Intelligent control.

How to cite this paper: Jyoti Malik, Dhiraj Girdhar, Ratna Dahiya, G. Sainarayanan,"Accuracy Improvement in Palmprint Authentication System", IJIGSP, vol.7, no.4, pp.51-59, 2015.DOI: 10.5815/ijigsp.2015.04.06