# A Highly Secure Integrated Biometrics Authentication Using Finger-Palmprint Fusion

Ephin M, N. A. Vasanthi

**Abstract**— Biometric authentication is the verification and identification of a person uniquely based on physical characteristics such as finger print, palm print, retina, iris, face etcetera or behavioral characteristics such as signature, gait, typing patterns, voice etcetera. Existing single modal biometric system has more error rate and provides less security than the combined one. To reduce the error rate and overcome the security flaw, multimodal biometric systems are used. Finger print is the most widely used technique and easy to use[3]. Palm print is more secure than finger print as it has more features like principal lines, wrinkles, texture, indents and marks compared to finger print and not available in public like photographs from which fake face or iris can be created. This paper presents a highly secure low cost biometric authentication scheme which makes use of both finger print and palm print features by fusing them for high level authentication. From the result it is concluded that the proposed scheme is highly secure, more economic, and user friendly. More over it has less error rate and high accuracy and offers better authentication.

**Index Terms**— Authentication, Biometrics, Fingerprint, Fusion, Palmprint, Security,.

## 1 Introduction

AUTHENTICATION is the first step of security requirement for accessing the resources of any kind of application in the real world. Traditionally password and user id is used for authentication. Now a day's biometric mechanism is becoming more and more popular for identification and verification all over the world. As biometric systems are distinctive to individuals, they are more consistent in authenticating individuality than token and knowledge-based identification methods. Token-based identification system includes driver's license or passport whereas knowledge-based identification systems includes a password or personal identification number[5]. Biometric data cannot be replaced by passwords or keys as it is personal privacy information which is individually and permanently related with a person. However, biometric systems offer privacy protection which has become the concern of public[6][7]. Fig. 1 shows a scanned fingerprint image.

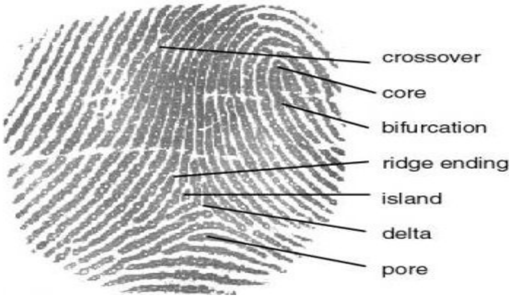

Fig.1 Fingerprint

A fingerprint can be identified based on minutiae that is the location and the direction of the ridge endings and/or the bifurcations along the ridge path[8]. These features are stored as templates for future use. In palm print information is more compared to fingerprint, which provides better security. There are many unique features in palm print like principal lines, wrinkles, minutiae points, singular points, and texture[9]. Again there is a problem of fake fingerprints[10]. In order to avoid this, fingerprint can be combined with any other biometric methods for more security. Fig. 2 shows a scanned Palmprint image.

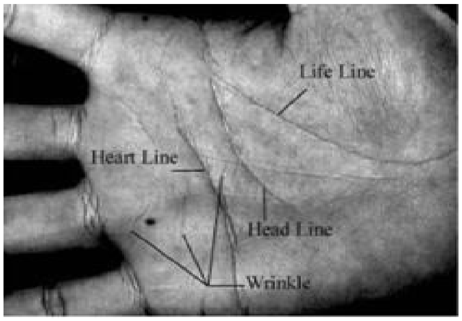

Fig.2 Palmprint

## 2 Evaluation Of Biometric Methods

A brief appraisal on different biometric methods is done based on A3C2P2U parameters[1][2][7][11]. A3C2P2U represents Acceptability, Cost, Complexity, Circumvention, Permanence, Performance, Universality and Uniqueness. These parameters impact more on real time biometric authentication systems from the perspective of user as well as business requirement. Table 1 shows the evaluation of biometric methods against A3C2P2U parameters.

Acceptability(A) refers to willingness of people in terms of cost and user friendliness. Cost(C1) refers to the expense for the device. Complexity(C2) refers to the difficulties with respect to ease of use. Circumvention(C3) is inversely proportional to security. Permanence(P1) relates the manner in which trait changes over time. Performance(P2) indicates completion of a given task measured against preset known standards of accuracy, speed etc. Universality(U1) is meant for every person using a system should possess the peculiarity. Uniqueness(U2) refers to distinctiveness. Acuuracy is based on Equal Error

Rate (EER), False Accept Rate (FAR) and False Reject Rate (FRR).

False Accept Rate: The prospect that the system imperfectly ties the input pattern to a non-matching pattern in the database. It processes the per cent of unacceptable inputs which are falsely assumed. False Reject Rate: the prospect that the system flops to identify a match between the input pattern and a matching pattern in the database. It processes the per cent of effective inputs which are falsely excluded. Equal Error Rate: the proportion at which both consent and discard errors are alike.

TABLE 1
EVALUATION OF BIOMETRIC METHODS AGAINST A3C2P2U

| Parameters / Techniques | A | C1 | C2 | C3 | P1 | P2 | U1 | U2 |
|---|---|---|---|---|---|---|---|---|
| Fingerprint | H | L | L | M | M | M | M | H |
| Palmprint | H | L | L | L | H | H | H | H |
| Face | H | M | M | H | M | L | H | L |
| Iris | M | H | H | L | H | H | H | H |
| Heart beat | L | M | M | M | L | L | H | M |

*Where H = High, M = Moderate, L = Low.*

## 3 THE PROPOSED SYSTEM

### 3.1 Block Diagram of The Proposed System

In this section, we present our proposed integrated biometric authentication system. System integrates fingerprint and palm print features for better authentication. Integrating the features of more than one biometric trait is termed as fusion. Template generated from the integrated features is stored in database against user id for easy retrieval of stored template. Block diagram of proposed integrated biometric authentication system using finger-palm print fusion is depicted in Fig.3.

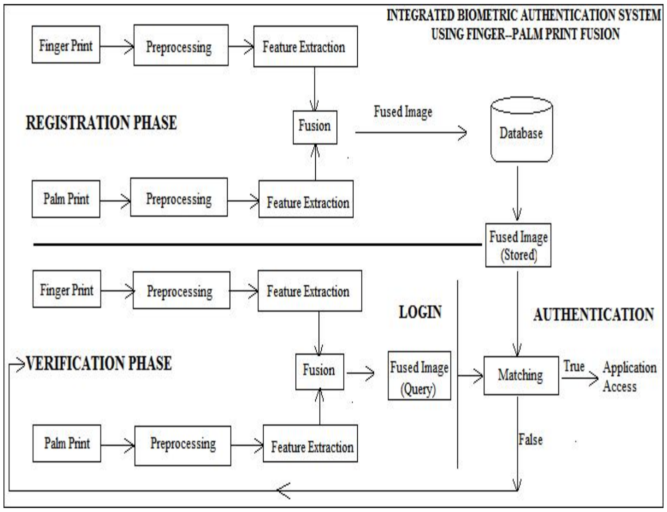

Fig.3 Block diagram of the proposed system.

### 3.2 Phases of Proposed System

Proposed system comprises of two phases namely Registration phase and Verification phase. Registration phase follows Storage Template Process (STP) to produce the output which is stored in database. Verification phase comprises of Login phase and Authentication phase. Login phase follows Query Template Process (QTP) to generate query template which is to be checked against stored template. Authentication phase follows Template Matching Process (TMP) to retrieve stored template and to calculate the distance between query template and the retrieved template. STP, QTP and TMP processes ate different phases are described in Table 2.

TABLE 1
STP, QTP AND TMP PROCESSES

| Phase | Registration | Login | Authentication |
|---|---|---|---|
| **Process** | STP | QTP | TMP |
| **Steps** | Ui =<br>{ IDi, FPi, PPi }<br>Ff =<br>{ FE(FPi) }<br>Pf =<br>{ FE( PPi) }<br>TSi =<br>{ FU(Ff, Pf) }<br>Di = TSi | Ui =<br>{ IDi, FPi, PPi }<br>Ff =<br>{ FE(FPi) }<br>Pf =<br>{ FE( PPi) }<br>TQi =<br>{ FU(Ff, Pf) } | Ri = TSi<br>DRi =<br>Di(TQi, Ri)<br>M = 1<br>if 0 <= DR < k<br>M = 0<br>if DR >= k |

*Where Ui = $i^{th}$ user , FP = Finger print, PP = Palm Print, Ff = Extracted feature of FF, Pf = Extracted feature of PP, FU = Fusion, TS = Stored Template, D = Data base, TQ = Query Template, R = Retrieved Template, DR = Distance between TQ and R, M = Matcher, k = Threshold value.*

Sample images used in our proposed system at Registration phase are given in figure 4. Also it shows the fused image.

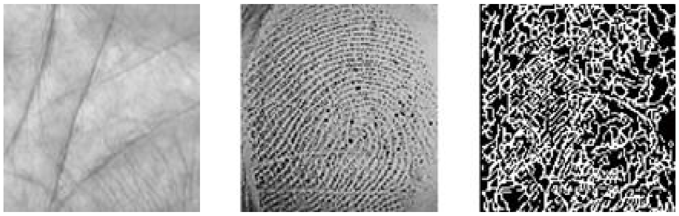

Fig.4 Sample Palmprint, Fingerprint, Query Image at Registration.

Suppose "N" users need to be given accessibility for a particular application, as a first stage all "N" users go through the registration phase. It is a One-Time enrollment phase in which user inputs id and place his/her hand on biometric scanner. The captured samples pass through preprocessing to enhance the quality of the image. Gabor filter is used for feature extraction[12]. Extracted features are fused using wavelet fusion to produce the template and stored in the database against user id for easy retrieval of stored data[13][14]. For fusion both the images are reset to same size and of same color. Sample images at Verification phase of our proposed scheme are given in figure 5. Also it shows the query and stored images.

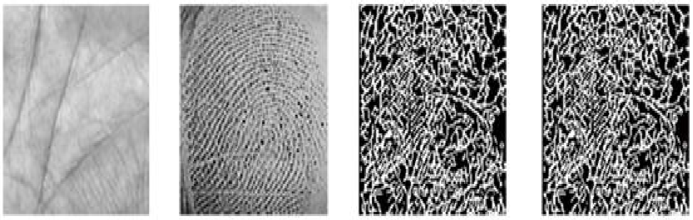

Fig.5 Sample Palmprint, Fingerprint, Query Image and Retrieved Image at Verification.

## 4 Result Analysis

Result analysis of the proposed system presented in this paper has been done with finger print and palm print images. Palm print samples obtained from Hong Kong Polytechnic University PolyU Palm Print Database and fingerprint samples from FVC2002 DB4B dataset. For result analysis similar 4 samples of 20 users totally 80 palm print images and 80 fingerprint images were taken. As we integrate fingerprint and palm print, proposed system combines the advantage of both the biometric methods. From the analysis we obtained the Error Rate of 0.625% and verification accuracy of 99.37%. Fig. 6 shows the plot of Equal Error Rate. The graph shows the error rate of integrated finger print and palm print which is less than that of unimodal fingerprint and palmprint. From the result it can be concluded that the proposed authentication scheme provides good performance, high level security and less error rate.

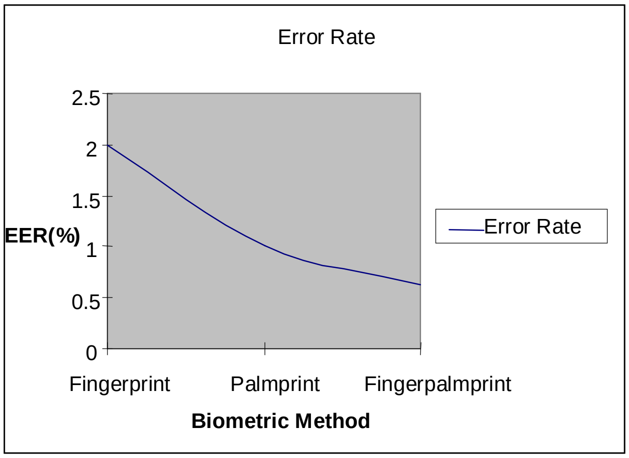

Fig.6 Equal Error Rate

## 5 Conclusion

To overcome the drawbacks of existing single modal biometric authentication schemes in terms of cost, complexity, security, efficiency and flexibility this paper presents an integrated biometrics authentication system using finger-palm print fusion which uses the best features of fused finger-palm print for better authentication. Quality of the images enhanced using low pass filter. Features were extracted using Gabor linear filter and fusion using wavelet fusion. From the result analysis we obtained the accuracy of 99.37% which is much higher than the single modal biometric systems. From the result analysis it is concluded that the proposed scheme is highly secure, more economic, user friendly etc., It can be used in all kind of applications including banking, physical area access in airport and all kind of access control.

## References

[1] Jain A.K, Ross A, Pankanti, Biometrics: a tool for information security. IEEE Transactions on Information Forensics and Security, Vol 2, Pp. 125-143, June.

[2] A.K Jain, P. Flynn and A. Ross, Handbook of Biometrics, Springer, 2007.

[3] Krishneswari, K. and S. Arumugam, "Multimodal Biometrics using Feature Fusion", Journal of Computer Science, Pp: 431-435, 2012.

[4] Verma & Pomona Mishra, "A Survey Paper on Palm Prints Based Biometric Authentication System", IJEEE, Pp: 20-27, 2012.

[5] Robert Richardson, "Computer Crime and Security Survey," Computer science Institute, 2010 / 2011.

[6] Robert Richardson, "Computer Crime and Security Survey," Computer science Institute, 2010 / 2011.

[7] Khurram, "Fingerprint Biometric-based Self-Authentication and Deniable Authentication Schemes for the Electronic world," IETE, Vol. 26, Pp.191-195, Jun 2009.

[8] D. Zhang and W. Shu, "Two novel characteristics in palm print verification: datum point invariance and line feature matching," Pattern Recognition, vol. 32, no. 4, pp. 691-702, Apr. 1999.

[9] R. Gayathri, P. Ramamoorthy, "A Fingerprint and Palmprint Recognition Approach Based on Multiple Feature Extraction", European Journal of Scientific Research, Vol 76, Pp: 514-526, 2012.

[10] W. Shu and D. Zhang, "Automated personal identification by palm print," Opt. Eng., vol. 37, no. 8, pp. 2359-2362, Aug. 1998.

[11] M. Turk and A. Pentland, "Eigen faces for recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, Mar. 1991.

[12] M. Turk and A. Pentland, "Eigen faces for recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, Mar. 1991.

[13] Wei-Yun Yau, Kar-Ann and Tai-Chen, "Fingerprint Templates Combination", Springer LNCS, Vol 3338, 2005.

[14] Chulhan Lee, Jaihie Kim, "Cancelable fingerprint templates using minutiae-based bit-strings", Springer Journal of Network and Computer Applications, Vol 33, Pp: 236-246, May 2010.

[15] D. Zhang, W.K. Kong, J. You, M. Wong,"On-line palmprint identification", IEEE Transactions on Pattern Analysis and Machine Intelligence 25 (9), Pp.1041–1050, 2003.

[16]Yong Jian Chin, Thian Song Ong, Michel K.O.Goh, Bee Yan Hiew,"Integrating palmprint and fingerprint for identity verification",Third International Conference on Network and System Security,2009.

[17] Mrs.Asmitha S Deshpande, S M Patil, Rekha Lathi, "A Multimodel Biometric Recognition System based on Fusion of Palmprint Fingerprint and Face", International Journal of electronics and Computer Science Engineering,ISSN-2277-1956.

[18] A. Kumar, D. Zhang, Integrating shape and texture for hand verification, in: Proceedings of Third International Conference on Image and Graphics, Pp. 222–225, 2004.