An Efficient Biometric Authentication System for Generating Virtual Identities

N.Parthiban[1] G.Selvavinayagam[2]

[1] *PG student, Department of IT, SNS college of Technology,coimbatore-35.*
parthibann43@gmail.com

[2]*Assistant Professor, Department of IT, SNS college of Technology,coimbatore-35.*
ohmselva@gmail.com

Abstract : **The Proposed system aim to research on the possibility of combining two biometric data like fingerprint and palm print, at the image level in order to generate a new datum for generating virtual identities. Biometric system used to protect resources access from unauthorized users. Biometric authentication provides high level of security. The proposed approach is to combine the two biometric systems are fused using a feature level fusion scheme. The features are extracted using the Gabor filter. The comparison of database template and the input data is done with the help of matching algorithm. If the templates are matched it can allow the person to access the system. These system provides more secure and reliable as compare to single biometric traits. False Acceptance Rate (FAR) is reduced in this method and also improved the False Rejection Rate (FRR).**

***Keywords*- Biometrics, Palm print & Fingerprint trait, Fusion technique, Identification system, False Acceptance Rate (FAR), False Rejection Rate(FRR).**

I. INTRODUCTION

Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person. Biometric system identifies or verifies a person based physiological characteristics such as fingerprint, face, palm print, iris etc. or behavioral characteristics such as voice, writing style, and gait. The personal authentication systems using biometrics are more reliable, convenient and efficient than the traditional identification methods.

Multimodal biometric person authentication systems are important for many security applications such as government, defense, surveillance and airport security. Multimodal biometrics has become increasingly important, particularly because single modal biometrics has reached its bottleneck, non-universality noise in sensor data and spoofing. Thus the multi-biometric identification technology will certainly break the limitation of single biometric identification.

The 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. 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. This system provides a combination of palm print and fingerprint image levels the different pre-processing techniques, feature extraction, fusion techniques and varieties of matching algorithms for generating a virtual identity.

Authentication by using multimodal biometrics offers high reliability due to the presence of multiple piece of evidence and it is more difficult to simultaneously forge multiple biometric characteristics than to forge a single biometric characteristic. Fusion is a promising approach that may increase the accuracy of systems. The palm prints have many advantages compare to other biometric traits. The principle lines and wrinkles are formed between the third and fifth months of pregnancy and superficial lines appear after we born. Even identical twins have different palm prints. Combining both fingerprint and palm print for personal identification will give a better security and accuracy.

II. PROPOSED METHOD

A. Block Diagram of the Proposed System

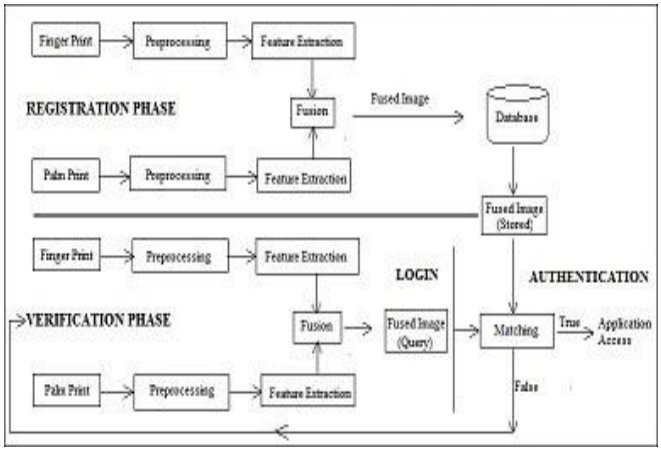

Fig.1 Block diagram of the proposed system

B. Block diagram process:

The proposed system of the block diagram shown in the figure. The block diagram consists of two phases. There are the following phases:

- Registration phase
- Verification phase.

Verification phase comprises of two phases:

- Login phase - Fused Image Query Process
- Authentication phase - Matching Process

In the Registration & Verification phase having process of Input image, pre-processing, feature extraction, fusion and matching process. If the templates are matched its access the system otherwise its repeats the login process.

III. FINGERPRINT RECOGNITION

A fingerprint is the representation of epidermis of a finger. It consists of a pattern of interleaved ridges and valleys. A fingerprint recognition system can be used for both verification and identification. These ridges are characterized by several landmark points, known as minutiae, which are mostly in the form of ridge endings and ridge bifurcations.

Fingerprints have been used for centuries for identification purposes. A fingerprint is an individual characteristic and no two fingers have identical ridge characteristics. Finger prints have both global features such as basic ridge patterns, pattern area, delta, type lines, ridge counts that are characterized by human eye. It is possible to have the same global features, but the local features remain unique. Minutiae are the major local features of a fingerprint, which consists of several components such as ridge ending, ridge bifurcation, ridge enclosure, spur, crossover or bridge, delta, core, etc.

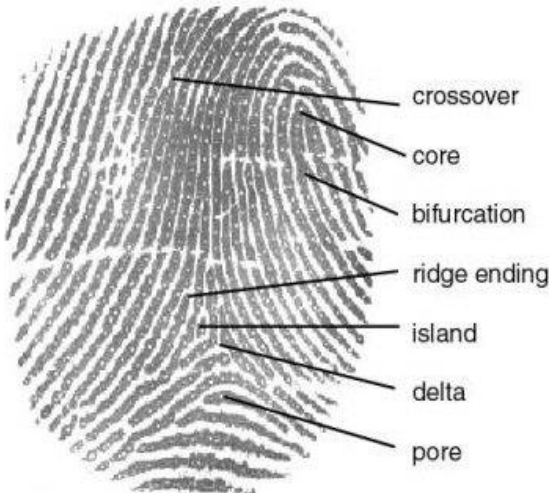

Fig.2 Sample Fingerprint Image

A verification system authenticates a person's identity by comparing the captured fingerprints with her own biometric template(s) pre-stored in the system. It conducts one-to-one comparison to determine whether the identity claimed by the individual is true.

An identification system recognizes an individual by searching the entire template database for a match. It conducts one-to-many comparisons to establish the identity of the individual.

IV. PALMPRINT RECOGNITION

Palm print recognition system offers two means to determine an individual's identity that is verification and identification. A palm print recognition system consists of some major steps, namely, input palm print image collection, pre processing, feature extraction, template storage or database.

The palm prints have many information compare to fingerprint. There are many unique features in palm print like principal lines, Wrinkles, minutiae points, singular points, and texture. The principle lines and wrinkles are formed between the third and fifth months of pregnancy and superficial lines appear after we born. Even identical twins have different palm prints.

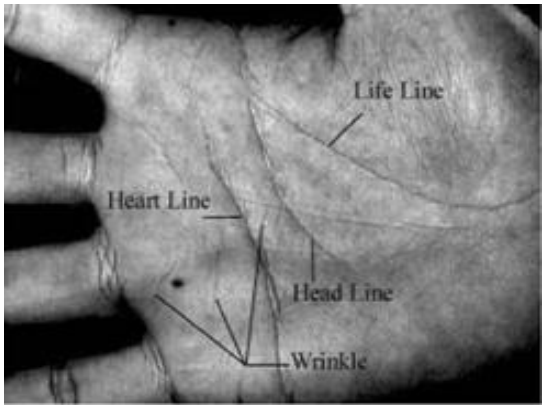

Fig.3 Palm print Image

In palm print information is more compared to fingerprint, which provides better security. Heart line, Head line and life line are considered as principle lines of palm print sample. Head line origination is from below the little finger and end near index finger. If a line is put from start point to end point its inclination can be observed in opposite direction in left a hand and right hand. Life line originates below the thumb region and encircles the thumb region and ends near the wrist shown in the figure.

V.SYSTEM DESCRIPTION

The block diagram consists of different stage of process.

1. Input image
2. Preprocessing
3. Feature extraction
4. Fusion
5. Matching process

1.Input image:

Special biometric scanners are used for image capturing. The input image is collects the samples from fingerprint and palm print database. The fingerprint samples are taken from FVC2002 DB4B dataset. The palm print samples are taken from Hong Kong Polytechnic University PolyU Palm Print Database.

2.Preprocessing:

The images must be preprocessed before going for the next stage. The captured or gathered samples are pass through preprocessing to enhance the quality of the image. The preprocessing techniques used to remove the unwanted data in the image such as noise, reflections .The preprocessing stage is used to filter, binaries, enhance and skeletonize the original gray images obtained by various biometric traits.

3.Feature extraction:

Gabor filter is used for feature extraction. The filter can be used to extract the rich line features of palm print. Palm print is more reliable biometric feature at it covers larger area than the fingerprint. In this paper Gabor filter approach can be used which transforms palm print images into specific transformation domains to find useful image representations in compressed subspace.

4.Fusion:

The feature level fusion is realized by simply concatenating the feature points obtained from different sources of information. The concatenated feature pointset has better discrimination power than the individual feature vectors. Different features are generated by fingerprint and palm print recognizers respectively. The feature level consists of ridge information, which will passed to the decision stage.

5.Matching process:

At the time of Enrollment, fingerprint and palm print images will be acquired. Feature vectors are generated for each biometric trait and stored separately in the system database. If the templates are matched it can allow the person to access the system. Thus, a new virtual identity is created for the two different biometrics, which can be matched using matching algorithms.

VI. FALSE ACCEPTANCE RATE

The false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

VII. FALSE REJECTION RATE

The false rejection rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system FRR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.

VIII. DATASET

In this study it is proposed to fuse palm print image with finger print image and extract feature using Gabor filter. Palm print of 20 users with 10 samples each were obtained from Hong Kong Polytechnic University Palm print Database. 20 fingerprints for fusion with palm print database was selected from FVC2002 DB4B dataset.

IX. CONCLUSION & FUTURE WORK

In this system it is proposed to investigate the verification accuracy of combining two biometrics using palm print and fingerprint. Palm print and finger print images were fused using feature level fusion techniques. The proposed method shows that multi modal biometrics are more efficient than conventional palm print based methods. So it is clear from these results that two biometric traits are more secure and reliable as compare to single biometric trait. Another reliable and security point is that it is impossible to reconstruct original images from the fused images. From it is conclude that the proposed scheme is highly secure, more economic, user friendly.

The future work will focus on more effective fusion strategy and special feature extraction algorithm of fused images, to achieve a more accurate to generate the virtual identity. To enhance the performance due to combine different biometrics using various fusion scheme.

REFERENCES

[1] Shweta Malhotra and Chander Kant Verma "A Hybrid Approach for Securing Biometric Template" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013.

[2] S. Li and A. C. Kot, "A Novel System for Fingerprint Privacy Protection," in Proc. 7th Int. Conf. Information Assurance and Security (IAS),Dec. 2011, pp. 262–266.

[3] J.Feng and A. K. Jain, "Fingerprint reconstruction: From minutiae to phase," IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 2, pp.209–223, Feb. 2011.

[4] R.Gayathri and P.Ramamoorthy "Feature Level Fusion of Palmprint and Iris" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012.

[5] Zain S. Barham and Allam Mousa "Fingerprint Recognition using MATLAB" Handbook of fingerprint recognition,2011.

[6] Ajay Kumar, David C. M. Wong, Helen C. Shen, Anil K. Jain, "Personal Verification using Palmprint and Hand Geometry Biometric".

[7] Karthik Nandakumar,Yi Chen, Sarat C. Dass, Anil K. Jain "Likelihood Ratio-Based Biometric Score Fusion" IEEE Transactions On Pattern Analysis And Machine Intelligence, VOL. 30, NO. 2, February 2008.

[8] Asem Othman and Arun Ross, "On Mixing Fingerprints" IEEE Transactions On Information Forensics And Security, Vol. 8, No. 1, January 2013.

[9] Ruifang Wang, Daniel Ramos, Julian Fierrez and Ram P. Krish, "Towards Regional Fusion for High-Resolution Palmprint Recognition"2012.

[10] Anil K. Jain, Arun Ross, Umut Uludag, "Biometric Template Security: Challenges And Solutions" Appeared in the Proceedings of European Signal Processing Conference (EUSIPCO), (Antalya, Turkey), September 2005.

[11] Gayathri, R. Ramamoorthy, P. "Fingerprint and palmprint Recognition Approach based on Multiple Feature extraction" European Journal of scientific research.Vol 76,2012.

[12] Albert, T., A. Ganesan, S. 2012. Application of Principal Component Analysis in Multimodel Biometric Fusion System.European Journal of scientific research,Vol 67,No 2.

[13] Deshpande, A., S., Patil, S., M., Lathi, R. 2012. A Multimodel Biometric Recognition System based on Fusion of Palmprint Fingerprint and Face. International Journal of Electronics and Computer Science Engineering. ISSN-2277-1956.

[14] J. You, W.K. Kong, D. Zhang, K.H. Cheung, "On hierarchical palmprint coding with multiple features for personal identification in large databases", IEEE Transactions on Circuits and Systems for Video Technology 14 (2) (2004) 234–243.