RESEARCH ARTICLE OPEN ACCESS

Combining Two Biometric Systems for Generating Virtual Identities

N.Parthiban[1], G.Selvavinayagam[2],
PG Student[1], Assistant Professor[2],
Department of IT, SNS college of Technology, Coimbatore-India

ABSTRACT
The system explores the possibility of combining two biometric systems for generating virtual identities. In biometric system the physical or behavioural traits are used for fusion. Biometric authentication provides high level of security. The proposed approach is to combine the palm print and fingerprint image using an appropriate fusion scheme. 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. Two Biometric system provides False Acceptance Rate (FAR) and False Rejection Rate (FRR).These system provides more secure and reliable as compare to single biometric traits.

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

I. INTRODUCTION

The Biometric is used to recognizing a person and the term is derived from the Greek word *bio* (life) and *metric* (measurement). Biometric system identifies or verifies a person based on his or her physiological characteristics such as fingerprint, face, palm print, iris etc. or behavioral characteristics such as voice, writing style, and gait. Biometric system operates as verification mode or identification mode depending on the requirement. The verification mode validates a person with readymade template. The identification mode recognizes a person's identity by performing matching against multiple biometric templates. The biometrics is more secure compared to the traditional methods such as PIN, smartcard for verifying a person. Some of the biometric applications are financial transaction, access to computer, access to confidential documents.

In the system concentrate on the physiological features such as fingerprint recognition and palm print recognition. Authentication by using combining Biometrics offers high reliability due to the presence of multiple piece of evidence e and it is more difficult to Simultaneously forge multiple biometric characteristics than to forge a single biometric characteristic.

The 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.

Among the many current biometric technologies, fingerprint identification is the oldest and the most popular one. Fingerprint technology has low cost comparing to others and high user acceptance. It is the method of identification using the impressions made by the minute ridge formats or patterns found on the fingertips. For every individual the ridge patterns will be different throughout the life. Fingerprints will offer an infallible means of personal authentication. Other personal characteristics may change, but fingerprints do not. However some people do not have clear fingerprints because of their physical work or problematic skin.

The palm prints have many advantages compare to other biometric traits. The inner surface of the palm normally contains principle lines, wrinkles and ridges.

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 palmprint for personal identification will give a better security and accuracy.

II. PROPOSED METHOD

A. Block Diagram of the Proposed System

The Block Diagram of the proposed system consists of five process. In the Registration & Verification phase having process of Input image, pre-processing, feature extraction, fusion and matching as shown in the block diagram.

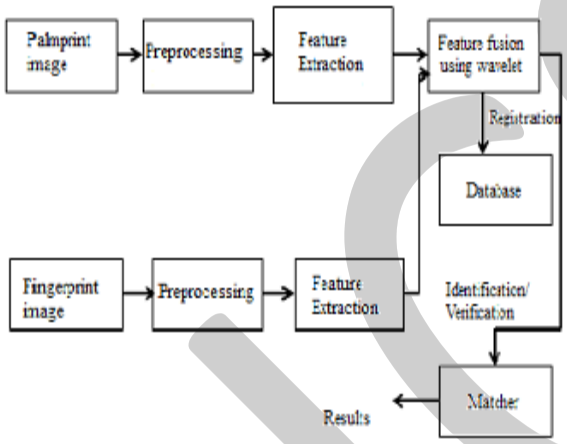

Fig.1 Typical Block Diagram of a Multimodal Biometrics

B. Block diagram process:

Special biometric scanners are used for image capturing. It may vary depending on the type of biometric traits used. At the pre-processing stage the image is enhanced to remove noise and unwanted areas. Different pre-processing methods are explained in the coming sections. Feature extraction gets effective features from the pre-processed biometric trait. Feature extraction for palmprint and fingerprint are different. After feature extraction fusion is carried out to combine different features and stored in the database as templates. A matching algorithm is used to compare it with the stored one in the database. Additionally verification phase to proceed a fused Query image for login purpose. If the fused query image is matched then it access the authentication phase. Otherwise its again repeat the verification phase.

III. FINGERPRINT RECOGNITION

Fingerprint-based recognition has been the longest serving, most successful and popular method for person identification. Fingerprints consist of a regular texture pattern composed of ridges and valleys. These ridges are characterized by several landmark points, known as minutiae, which are mostly in the form of ridge endings and ridge bifurcations. The spatial distribution of these minutiae points is claimed to be unique to each finger; it is the collection of minutiae points in a fingerprint that is primarily employed for matching two fingerprints.

Among all biometric traits, fingerprints have one of the highest levels of reliability and have been extensively used by forensic experts in criminal investigations. A fingerprint refers to the flow of ridge patterns in the tip of the finger. The ridge flow exhibits anomalies in local regions of the fingertip (Figure), and it is the position and orientation of these anomalies that are used to represent and match fingerprints.

Although not scientifically established, fingerprints are believed to be unique across individuals, and across fingers of the same individual. Even identical twins having similar DNA, are believed to have different fingerprints. Traditionally, fingerprint patterns have been extracted by creating an inked impression of the fingertip on paper.

Automatic fingerprint identification systems, that match a query print against a large database of prints (which can consist of millions of prints), rely on the pattern of ridges in the query image to narrow their search in the database (fingerprint indexing), and on the minutiae points to determine an exact match (fingerprint matching). The ridge flow pattern itself is rarely used for matching fingerprints.

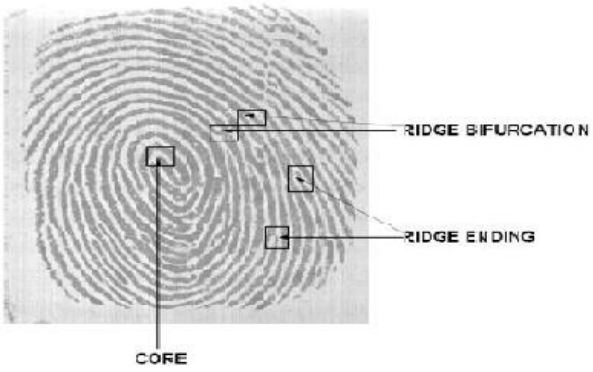

Fig.2 Sample Fingerprint Image

IV. PALMPRINT RECOGNITION

A palmprint recognition system consists of some major steps, namely, input palmprint image collection, pre processing, feature extraction, template storage or database. The input palm print image can be collected by using a palmprint scanner.

The image of a human palm consists of palmar friction ridges and flexion creases. Latent palmprint identification is of growing importance in forensic applications. Since around 30% of the latent prints lifted from crime scenes (from knifes, guns, steering wheels) are of palms rather than of fingers. Similar to fingerprints, latent palmprint systems utilize minutiae and creases for matching. While law enforcement and forensics agencies have always collected fingerprints, it is only in recent years that large palmprint databases are becoming available. Based on the success of fingerprints in civilian applications, some attempts have been made to utilize low resolution palmprint images (about 75 dpi) for access control applications. To our knowledge, palmprint recognition systems have not yet been deployed for civilian applications (e.g., access control), mainly due to their large physical size and the fact that fingerprint identification based on compact and embedded sensors works quite well for such applications.

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. Again there is a problem of fake fingerprints. In order to avoid this, fingerprint can be combined with any other biometric methods for more security.

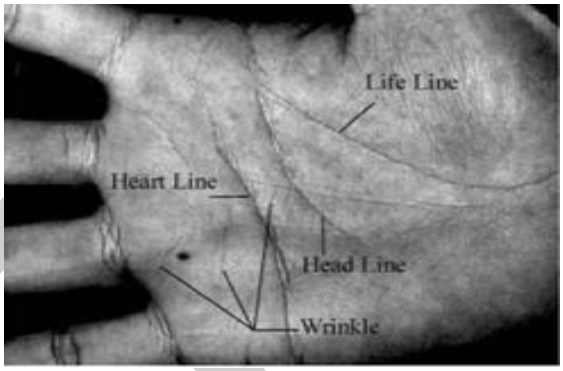

Fig.3 Palmprint Image

V. PRE PROCESSING

The images must be preprocessed before going for the next stage. Image preprocessing is done with the intention of removing unwanted data in the image such as noise, reflections .The objective of image processing stage is to filter, binaries, enhance and skeletonize the original gray images obtained by various biometric traits.

VI. FEATURE EXTRACTION

Wavelet transformation can capture prominent visual properties. The filter can be used to extract the rich line features of palmprint. Palmprint is more reliable biometric feature at it covers larger area than the fingerprint. The rich line features remain unaltered throughout the person's life. The wavelet approach can be used which transforms palmprint images into specific transformation domains to find useful image representations in compressed subspace. It computes a set of basis vector from a set of palmprint images, and the images are projected into the compressed subspace to obtain a set of coefficients called as wavelet code.

VII. FUSION STAGE

Different features are generated by fingerprint and palmprint recognizers respectively. Since the

matching levels output by the two traits are heterogeneous because they are not on the same numerical range, so feature level normalization is done to transform these levels into a common domain prior to combining them. The feature level consists of ridge information, which will passed to the decision stage.

VIII. MATCHING PROCESS

At the time of Enrollment, fingerprint and palmprint images will be acquired. Feature vectors are generated for each biometric trait and stored separately in the system database. At the time of authentication, when user wants to prove his/her identity fingerprint image will be acquired by using optical fingerprint reader. Palmprint image will be captured using web camera or CCD. These images again will undergo image preprocessing and feature extraction stage. Template will be compared with the respective template created at the time of Enrollment. Thus, a new virtual identity is created for the two different biometrics, which can be matched using minutiae-based matching algorithms.

IX. DECISION STAGE

Histogram of Feature fusion image will be compared against the set threshold value .This will decide whether this person is genuine or imposter. In this system we have given equal weight to both fingerprint and palmprint at fusion. We can change the weights of the individual modality according the modality for which we can find best results.

X. DATASET

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

XI. 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 wavelet based image 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.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.

2.A. Ross, K. Nandakumar, and A. Jain,Handbook of Multibiometrics. New York: Springer- Verlag, 2006, New York Inc..

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.A. Othman and A. Ross, “Mixing fingerprints for generating virtual identities,” in Proc. IEEE Int. Workshop Information Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov./Dec. 2011.

5.Shekhar Karanwal,”Secure and Reliable Multimodal Biometric Systems Using Two and Three Biometric Traits” IJARCSSE vol 3,july 2013.

6.Hafiz Imtiaz,Shaikh Anowarul Fattah,"A Wavelet Based Feature Selection Scheme for Palmprint Recognition" IJMER vol 1,pp 278-287.

7.Y. J. Chin, T. S. Ong, M. K. O. Goh, and B. Y. Hiew, "Integrating palmprint and fingerprint for identity verification," in Proc. of the Third International Conference on Network and System Security, 2009 .

8.Ephin M, N. A. Vasanthi "A Highly Secure Integrated Biometrics Authentication Using Finger-Palmprint Fusion" International Journal of Scientific & Engineering Research Volume 4, Issue 1, January-2013.

9.Dattatray V. Jadhav & Pawan K. Ajmera "Multi resolution Feature Based Subspace Analysis for Fingerprint Recognition" ©2010 International Journal of Computer Applications (0975 – 8887)Volume 1 – No. 13.

10.Anil K. Jain, Ajay Kumar"Biometrics of Next Generation: An Overview" TO APPEAR IN 'SECOND GENERATION BIOMETRICS' SPRINGER, 2010.

11.Mitul D Dhameliya, Jitendra P Chaudhari "A Multimodal Biometric Recognition System based on Fusion of Palmprint and Fingerprint" International Journal of Engineering Trends and Technology (IJETT) - Volume4,Issue5- May 2013.

12.Zain S.Barham "Fingerprint Recognition using MATLAB" Nov 2011.