Multibiometric Authentication System Processed by the Use of Fusion Algorithm

Prashanth Purastu[1], Mr. T. Arul Kumaran[2], Sagar Bhattacharyya[3]

[1,3]UG Scholar, Department of Electronics and Telecommunication Engineering, Sathyabama university, Chennai, India
[2]Assistant Professor, Department of Electronics and Telecommunication Engineering, Sathyabama university,Chennai, India

Abstract *— The present day authentication system is mostly uni-model i.e having only single authentication method which can be either finger print, iris , palm veins ,etc. Thus these models have to contend with a variety of problems such as absurd or unusual data, non-versatility; un authorized attempts, and huge amount of error rates. Some of these limitations can be reduced or stopped by the use of multimodal biometric systems that integrate the evidence presented by several sources of information. This paper converses a multi biometric based authentication system based on Fusion algorithm using a key. Our work mainly focuses on the fusion algorithm, i.e fusion of finger and palm print out of which the greatest features from the above two traits are taken into account. With minimum possible features the fusion of the both the traits is carried out. Then some key is generated for multi biometric authentication. By processing the test image of a person, the identity of the person is displayed with his/her own image. By the fusion algorithm, it is found that it has less computation time compared to the existing algorithms. By matching results, we validate and authenticate the particular individual.*

Keywords— Multi Biometrics, finger print, palm print, ROI, Euclidian distance, Feature Extraction, Fusion Algorithm and Key Generation.

I. INTRODUCTION

Verification of identity of a person automatically by means of biometrics is an important application in current scenario of life . Now authentication system is mostly uni -modal i.e having only single authentication method which can be either finger print, iris , palm veins ,etc. Thus this models have to contend with a variety of problems such as absurd or unusual data ,non-versatility, unauthorized attempts\ (Fraudulent) and huge amount of error rates. These limitations can be reduced or stopped by the use of multimodal biometric systems that integrate the evidence presented by multiple sources of information. Our work mainly focuses on the fusion algorithm based multi-biometric authentication. By processing and authentication of the test image of a person, the identity of the person is displayed with his/her own image. This can be accomplished by merging, for example, multiple traits of an individual, or multiple feature extraction [4,5] and matching algorithms operating on the same biometric. Such systems are known as multi bio metric systems.

While multibiometric systems have improved the precision and reliability of biometric systems, sufficient attention has not been paid to security of multi biometric templates. Security of multibiometric templates [6, 7] is especially crucial as they contain information regarding multiple individualities of the same user. Hence, multibiometric template protection is the main consideration of this work. The fundamental task in designing a biometric template protection scheme is to overcome the large intra user inconsistency among multiple acquisitions of the same biometric trait. This paper is ordered as follows. First section gives the overview about multi biometrics and its necessity, Section II describes the background of the work, Section III introduces the proposed finger print extraction algorithm and Section IV deals with the proposed palm print feature extraction algorithm. Then Section V narrates the proposed method of integrating the system as multi trait based with statistical analysis of GUI based system. Then, Section VI presents the Simulation results and discussion; finally the conclusion is given in Section VII.

II. LITERATURE SURVEY

Our paper includes the few contributions from the existing methodologies and they are taken into account from following reference papers .From [3] I .e, Multi feature-Based High-Resolution Palm print Recognition of may2011.This paper focuses on the algorithm that includes the following:

Use of multiple features, namely, minutiae, density, orientation, and principal lines, for palm print recognition to significantly improve the matching performance of the conventional algorithm.

Design of a quality-based and adaptive location field estimation algorithm which performs better than the existing system in case of sections with a large number of creases.

Use of a new fusion scheme for an identification application which performs better than straight fusion methods, e.g., weighted sum rule, SVMs, or Neyman-Pearson rule. Besides, we analyse the discriminative power of different feature arrangements and find that compactness is very

useful for palm print recognition.Paper [2] i.e A Unified Framework for Biometric Expert Fusion Incorporating Quality Measure.

This paper proposes a unified framework for quality-based combination of multimodal biometrics. Quality-dependent fusion algorithms aim to dynamically combine several classifier (biometric expert) outputs as a task of automatically derived (biometric) sample quality. Quality measures used for this purpose quantify the amount of conformance of biometric samples to some predefined criteria known to influence the system presentation. Planning a fusion classifier to take quality into consideration is difficult because quality measures cannot be used to separate genuine users from impostors, i.e., they are non discriminative yet still useful for classification. We put forward a general Bayesian framework that can utilize the quality information effectively.

The existing part of this kind of multi biometric includes extracting features of figure print and the palm print are extracted and then matching part it individually.

III. PROPOSED METHODOLOGY

As advanced Security is our main concern we overcame the limitations of the already existing systems and so we introduced a key which is generated and finger print and palm print is fused into single image for more security.

Our work mainly focuses on the fusion algorithm, i.e fusion of finger and palm print out of which the greatest features from the above two traits are taken into account. With minimum possible features the fusion of the both the traits is carried out. Then some key is generated for multi biometric authentication.

Advantages

1. Computation load needed for image processing purpose is much reduced, combined with very simple classifiers.
2. It takes less computation time.
3. Speed and very low complexity, which makes it very well suited to operate on real scenarios.

A. Features of finger print

In a fingerprint image, the main point of concern is the center of the region of interest. Therefore, locating the center point is an crucial step that influences the matching accuracy. However, it is found that it is insensitive to fingerprint

rotation. In this algorithm, core point is defined as the center point (xc, yc). The center point detection algorithm is used to find the centre point. The available features in a finger print is based on ridges and valleys. The features are given below in the Fig. 1.1

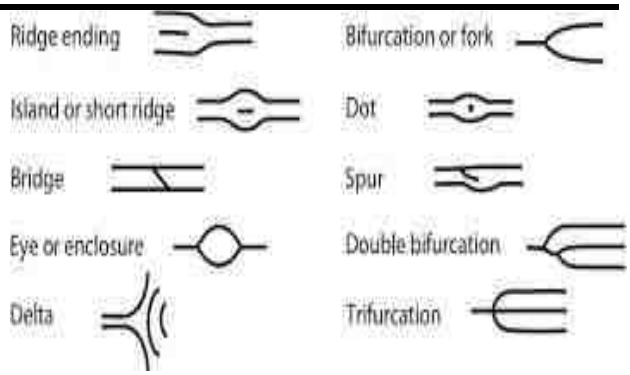


Fig 1: Various micro features of a finger print.

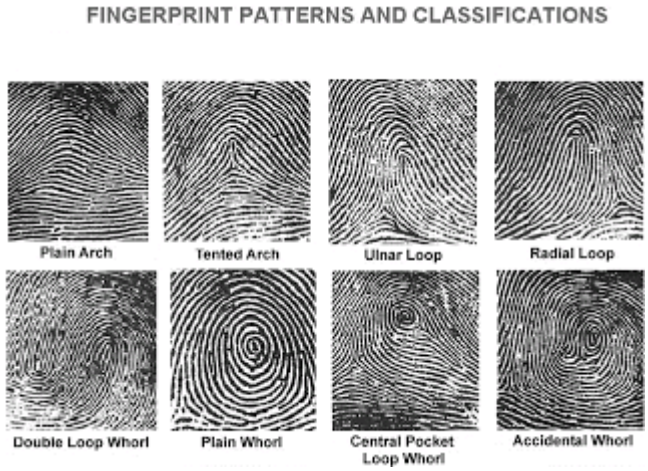


Fig .2: Pattern variations present in a human finger.

The most commonly employed method of minutiae extraction is the Crossing Number (CN) concept. This method uses the frame image and the minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a Matlab 3×3 window. The ridge pixel are then classified as a ridge ending, bifurcation or non- minutiae point. For example, a ridge pixel with a CN of one corresponds to a ridge ending minutia, and a CN of three relates to a bifurcation minutia.

B. Features of palm print

Since ridge patterns in different palmprint regions have different characteristics, the discrimination power of different regions also varies. In order to study this problem, a statistical experiment is conducted using the eight impressions of 15 different palms in the training set. All the palmprints are transformed into the same coordinate system manually. Next, the transformed palm print images are divided into non overlapped blocks of 64X64 pixels to reduce computational cost. The discrimination power of the 510 X 510 pixel local region centered at each block is studied. The size is chosen so that there are adequate features within to align successfully. When matching two palm prints [10-12], each block's local region is separately matched to the corresponding block's local region if they are valid palm print regions.

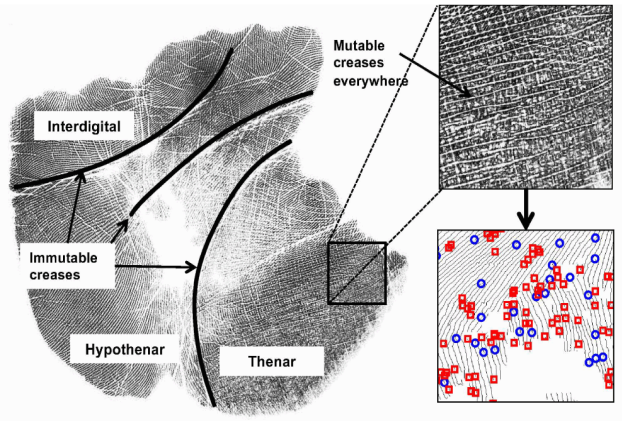


Fig.3: Features of a Palm print

C. **Finger and Palm print Authentication**:

Fingerprint matching is currently the question of deep research by both private and academic institutions. So fingerprints are developing as the most common and principal biometric for personal identification [8,9]. For the fingerprint matching problem, the input is some fingerprint images and the output is the probability that the fingerprints were taken from the same finger. This paper presents an enhanced feature extraction algorithm for fingerprint identification, it centered on the Euclidian distance between the center point and their nearest neighbor bifurcation and ridge ending minutiae's. This new work overcomes the problem of geometric rotation and translation over the acquisition phase of image fingerprints. Fingerprint matching outcomes from the suggested method are validated and the similarity score for the test data available is evaluated.

During the past years, many efforts have been tried through to use palm prints as a biometric modality. However, most of the existing palm print recognition systems are based on coding and matching creases, which are not as reliable . This affects the use of palm prints in large-scale person identification applications where the biometric modality needs to be distinctive. Recently, several ridge-based palm print matching algorithms have been proposed to fill the gap. Major contributions of these systems include consistent orientation field estimation in the presence of creases and the use of several features in matching, while the matching algorithms adopted in these systems simply follow the matching algorithms of fingerprints. However, palm prints differ from fingerprints in several aspects: i) Palm prints are much bigger and thus hold a large number of minutiae, ii) palms are more deformable than fingertips, and iii) the quality and perception power of diverse regions in palm prints vary significantly.

As a result, these matchers are unable to appropriately handle the distortion and noise, despite heavy computational cost. Motivated by the matching strategies of human palm print experts, a novel palm print recognition system was developed. This algorithm is based on principal line based feature extraction. The major creases are detected using edge detection and after processing the orientation and length based features are extracted. The overall features of palm print are shown in Fig 2.

IV. PROPOSED PALM AND FINGER PRINT ALGORITHM

A. Enrollment stage:

Step1: Detect the centre point.

Step2: Detect the bifurcation and ridge ending minutiae's

Step3: for i=l until Np, Compute the Euclidian distance between centre point and minutiae's point as follow:

ED (i)=((xc-xM(i)2+(yc-yM(i))2)1/2

Step 4: Sort the Euclidian distance vector between the center point and deduced minutiae's in ascending order.

Step5: Save the Euclidian distance vector in database.

B. Matching stage:

Step1: Detect the centre point.

Step2: Detect the bifurcation and ridge ending minutiae's

Step3: for i=l until Np, Compute the Euclidian distance between centre point and minutiae's point as follow:

ED(i)=((xc-xM(i)2+(yc-yM(i))2)1/2

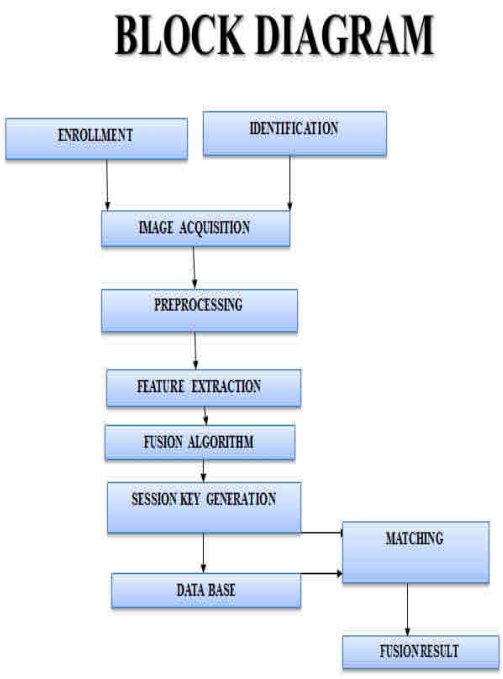
Step4: Sort the Euclidian distance vector between the center point and deduced minutiae's in ascending order.

Step5: Save the Euclidian distance vector in database.

Step6: Compute and compare the similarity rate between the desired vectors Sq with the saved Sp. where, • xc and yc are the spatial coordinates with x and y pixels for the center point. • xM and yM are the spatial coordinates with x and y pixel for bifurcation and ridge ending minutiae's.

The block diagram of the proposed palm print authentication system is shown in the Fig. 4. It contains in general four phases namely User interface, acquisition, recognition and matching [13,14]. In the user interface the user interacts with the system to enroll his/her palm print in the scanner. In acquisition the image captured is pre processed and certain modifications are done and the system accepts the palm to enroll. In recognition phase, the given user is recognized using matching algorithm present in matching phase. In matching phase, the test image is compared with the pre existing images and the user is given access depending upon the match. The following are the steps involved in proposed algorithm;

1. Enrolment and Image Acquisition
2 .Image enhancement
3. Feature extraction
4. Use of Fusion algorithm
5. Generation of secret key



Module-1:Enrolment and Image Acquisition

The image has been captured using a digital scanner under less than ambient illumination conditions. The flap of the scanner had been kept open during the acquisition process in order to obtain a uniform black background.

Fig. 4: Enrolment of finger print

Module-2: Image enhancement

Image enhancement is the process of improving the quality of the image acquiesced for a better view .It ensures that the image is improvised according to the required colour, contrast and pixels by adjusting the gray scale or RGB values.

Fig.5: Enhanced palm print image

Module-3 Feature Extraction

The features of a finger and the pit shows the region of interest are extracted in such a way that it shows the minutiae points of both the finger and palm print. This minutiae points are used to detect the main point of interest for the purpose of authentication.

The ROI is selected in such a manner that it contains the maximum feature information and features can be easily extracted.

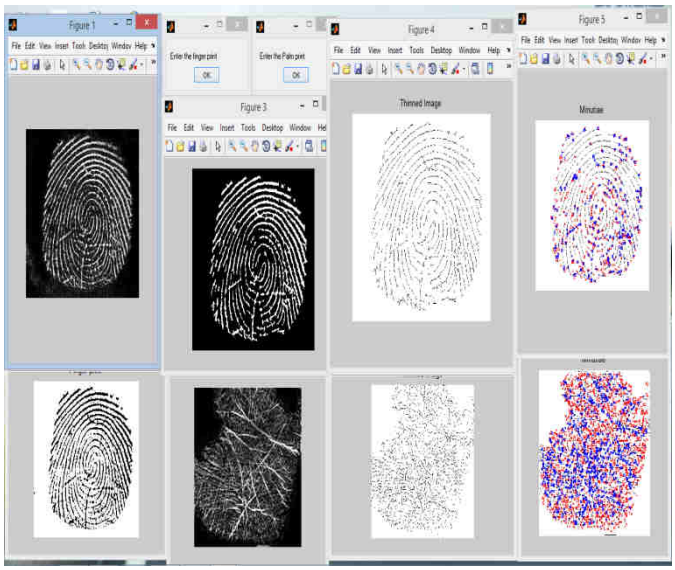


Fig.6: Extraction of minutiae

Module-4 Use of Fusion algorithm

Here we tried to fuse or hide one image over the other so that the security strength of the finger and palm prints that will be used for authentication is increased also the enrolment and execution time of the required process is decreased.

Module-5 Generation of secret key

Even after a image is hidden in another one by the process of fusion ,but their might be still few loop holes. These loopholes make provide a way for the spoolers' or the hackers

to get access to the image of the person and can get his personal data.In our project we have included a secret key generation algorithm for each individual users ,so that security of the individuals data is increased.

Table 1:Secret key values for both finger print & palm print

Serial no.	Identity	Fingerprint size	Palmprint size	Secret key
1	Sagar	22.5kb	11kb	3225248
2	Prashanth	29kb	11.3kb	3225266
3	Mani	30.3	7.9kb	3152265

V. SIMULATION RESULT

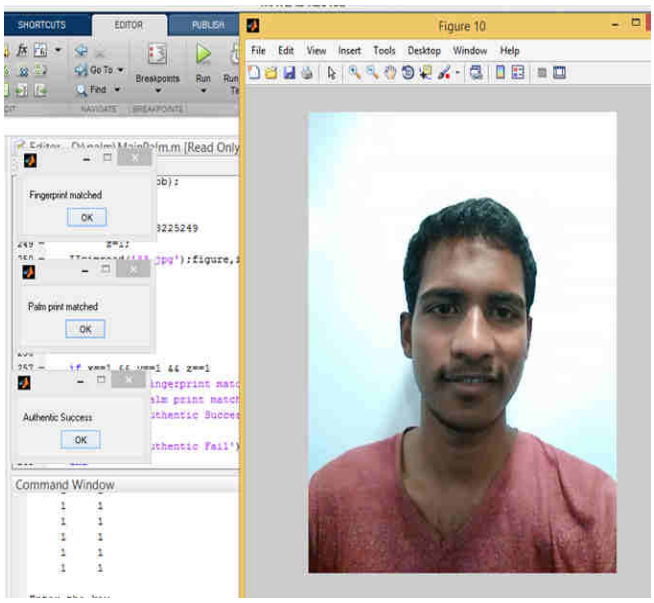


Fig.7: Simulated Result for a successful authentication

Using the MATLAB 2013 Ra tool, we were able to Generate the coding for the proposed system and execution results has been verified successfully for various cases.

VI. CONCLUSION

Thus a multi biometric based authentication using finger print and palm print was done. For fingerprint identification planned algorithm is generated on the basis of Euclidian distance between the center point and their nearest neighbor bifurcation and ridge ending minutiae's. For Palm print Authentication , principal line based algorithm is proposed. It uses macro features of the palm print to identify a person. By the proposed fingerprint and palm print algorithm, it is found that it has less calculation time and inhabits less memory space compared to the existing algorithms. Thus, an efficient and fast authentication is achieved. With the existing system which deals with the fusion and then authentication, this system concentrates on better feature extraction and matching accuracy. Since it is embedded with the GUI interface, the system can be used for commercial purpose too. The future work include the fusion algorithm ,the best features from the above two traits are taken into account. With minimum possible features the fusion of the both the traits is passed out. The fused image is then generated. It is formed in such a way that it is completely invertible to get back the original image back. Then a session key generation algorithm for randomly generating session key is also extended with the proposal.

REFERENCES

[1] Nagar, K. Nandakumar and A. K.Jain, "Multibiometric Cryptosystems Based on Feature-Level Fusion," IEEE Transactions On Information Forensics And Security, vol. 7, no.1, pp. 256-278, Feb 2012.

[2] Norman Poh and Josef Kittler, "A Unified Framework for Biometric Expert Fusion Incorporating Quality Measures," IEEE Transactions On PatternAnalysis And Machine Intelligence, vol. 34, no.1, pp. 3-17, Jan 2012.

[3] J.Dai and J.Zhou, "Multifeature Based High-Resolution palmprint Recognition," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 33, no.5, pp. 945-957, May 2011. Gurpreet Singh1 and Vinod Kumar2 ,Review On Fingerprint Recognition: Minutiae Extraction and Matching Technique : International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 10 No. 1 Oct. 2014, pp. 64-70

[4] Generation of Secret Key for Physical Layer to Evaluate Channel Characteristics in Wireless Communications : B.U.Prashanth1,*, Y.Pandurangaiah2, Appeared In proceedings of International Conference on "Emerging Research in Computing, Information, Communication and Applications" ERCICA 2013 pp: 251-255

[5] Fundamental Limits for Privacy-Preserving Biometric Identification Systems that Support Authentication: Tanya Ignatenko,and Frans M. J. Willems

[6] Multibiometric Cryptosystems Based on Feature-Level Fusion, Abhishek Nagar ,Karthik Nandakumar Anil k.jain published in IEEE transactions on information forensics and security,vol.7,no.1,february2011

[7] T. Ignatenkoand F.M.J. Willems, "Biometric Systems Privacy and Security Aspects", IEEE Transactions On Information Forencis and Securty vol.4, no.4, pp.956–973, Dec 2009.

[8] R.Plaga,"Biometrickeys:Suitableusecasesandachievabl einformation content,"Int.J.Inf.Security,vol.8,pp.447–454,2009

[9] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric templates from fingerprint-face features," in Proc. CVPR Workshop Biometrics, Minneapolis, MN, Jun. 2007.

[10] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in Proc. IEEE 2nd Int. Conf. Biometrics: Theory, Applications,andSystems, Washington, DC, Sep. 2008.

[11] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti, "Privacyaware biometrics: Design and implementation of timodal verification system, " inProc.IEEEAnn.Conf. Computer Security Applications, Los Alamitos, CA, 2008.