(IJEACS) International Journal of Engineering and Applied Computer Science

Fingerprint and Palmprint Multi-Modal Biometric Security System

P Appala Naidu
Research Scholar
Rayalaseema University
Kurnool, AP, India

CH GVN Prasad
Dept. of CSE
SICET, JNTU-H
Hyderabad, India

Prasad B
Dept. of CSE
MLRITM, JNTU-H
Hyderabad, India

Bhanuja Bodla
Dept. of CSE
MLRITM, JNTU-H
Hyderabad, India

***Abstract*—In this work, fingerprint and palm print multi-modal biometric security system is proposed. In this proposed work some of the common features of finger print and palm print images are identified and the process is carried out for authentication. At first, the preprocessing steps are completed on chosen images which include binarization, thinning and minute extraction. Binarization is for identifying the important ridges of finger print and palm print images and later on thinning is applied to eliminate the repetitive pixels on the binarized images. Using minute extraction different angles are formed for the thinned images for choosing the specific area of the images. In the next step for identifying the specific area in the finger print images region of interest is carried out. After the initial stage (preprocessing) features are extracted by using Feature Extraction method from both the finger print and palm print images and all the extracted features are combined to form a feature vector element. Secrete key is generated using the fuzzy extractor from the biometric features and stored in the fuzzy vault. The generated key and obtained vector elements are stored in the database. In final stage authentication methods are carried out for the test images. In this method feature of finger print images and palm print images are extracted and verified with the fuzzy vault and then a secrete key is generated. If the key generate and key stored in database are matched then the process is successful authentication or else it is failure authentication.**

Keywords-Finger Print; Palm Print; Multi-Modal Biometrics; Binarization; Thinning; Minute Extraction; Fuzzy Extractor; Feature Extractions; Fuzzy vault.

I. INTRODUCTION

In single biometric structure we use only a solitary system e.g. Iris System, Fingerprint structure or Face Recognition System. Subsequently we stand up to heaps of issues while using single biometrics system. In some cases noise enters with the Biometrics of a man that we need to store, this outcomes in higher the false dismissal rate. Higher the false dismissal rates are seen when we store the biometric of a man because of more noise is entered in it. Database design can be stolen and it can be revoked by any intruder when we use the single biometric structure as it contains only a solitary arrangement. Many individuals confront the troubles in giving template due to harm or harm of physical piece of that individual and can't utilize that framework.

II. SURVEY

A. *Motivation*

To decide or check, man's interesting personality. The individual's character can be checked by utilizing Fingerprint, Palm print, Face, Iris, Voice. With this blend multimodal biometrics is shaped. From this biometrics biometric layouts can be framed and giving security to this format which is put away in database is vital.

B. *Scope*

Providing Biometric Security to any frameworks like Forensic science to bolster criminal examinations, burglary location and in biometric frameworks, for example, business recognizable proof gadgets, web based business, and so forth.

C. *Objective*

The main objective is to propose finger print and palm print multi-modal biometric security system, in which for the single user multiple biometrics like different finger print images and palm print images are collected and for the collected images template are generated and using fuzzy vault algorithm security key is generated. The template and key are stored in database and security is provided for them.

III. PROPOSED SYSTEM

In the proposed Fingerprint and Palmprint Based Multi – Modal Biometric System as shown in figure 5, we have two main modules Pre-processing and Feature extraction.

- *Pre-processing*
  1. Binarization
  2. Thinning
- *Feature extraction*
  3. Minutiae extraction

ISBN: 978-0-9957075-6-6 *DOI: 10.24032/ijeacs/0205/04*

i. Bifurcation

ii.Termination

4. Region of interest (ROI)

3.1 Pre-Processing

A multimodal biometric confirmation framework gathers the specimens of biometric elements. In the proposed framework as appeared in fig 5 we took from poly database the pictures of unique finger impression and palm print impressions. Optical finger print readers are used to take the finger impressions and for palm impression high quality cameras are used.

The impressions must be preprocessed before going for the accompanying stage. This step is done with the point of clearing undesirable data in the impressions, for instance, noise, reflections in the images. The goal of this step is to filter, binarize, upgrade and skeletonize the first gray impressions gotten by three different biometric characteristics.

The features which are extracted from the finger and palm impressions are combined and are used in multimodal biometric fuzzy vault model.

Binarization: Figure 1 and figure 2 highlights the ridges in the form of black color for finger impression and palm impression while furrows are highlighted in white color. 8-bit Gray image is transformed into a 1-bit image and ridges are assigned 0-value and furrows are assigned to 1-value.

.

Figure 1. Finger Print and its Binarized image

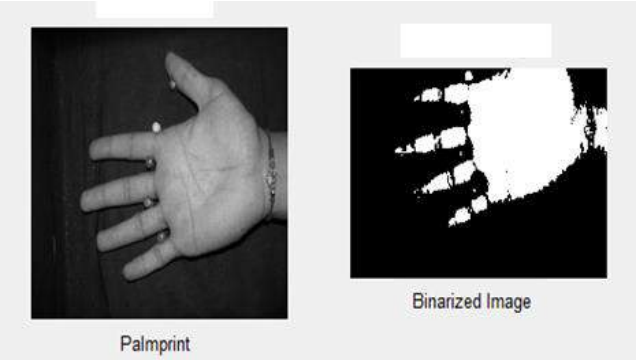


Figure 2. Palm Print and its Binarized image

A locally adaptable binarization system is performed to binarize the unique finger print image. In this technique picture is apportioned into pieces of 16 x 16 pixels. Pixel esteem is then set to 1 if its esteem is greater than the mean power estimation of the present square to which the pixel has a place.

Thinning: The main idea behind this process is not to eliminate ridge end points and not to break linking of the ridge.

By using MATALB redundant pixels of ridges can be eliminated with the help of morphological thinning function till the ridges are just one pixel wide and it is shown in figure 3 and figure 4.

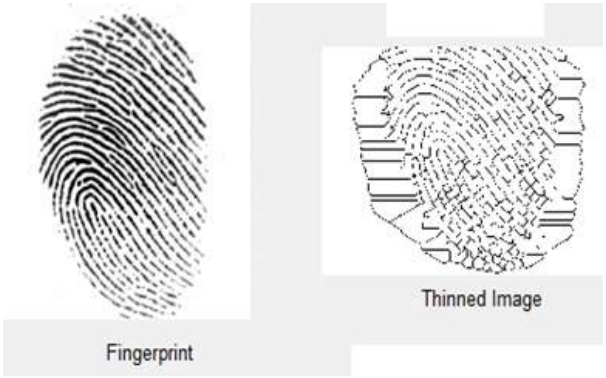


Figure 3. Finger Print and its Thinned image

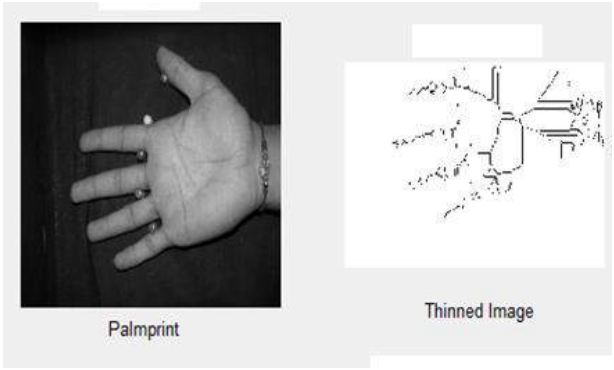


Figure 4. Palm Print and its Thinned image

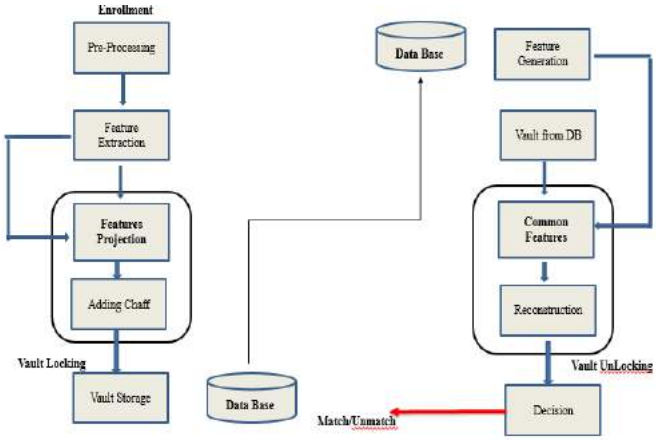


Figure 5. Proposed Multi Modal Biometric System

ISBN: 978-0-9957075-6-6 DOI: 10.24032/ijeacs/0205/04

3.2 Feature Extraction

After the initial step (preprocessing) in a given specific case we collect different four images for a specific person and preprocessing is carried out on those images and feature extraction as shown in fig 6 methods are done on it.

From the impressions taken above regular points are recognized and components are extricated. And along with the common points random points are also chosen and are added so that we can form vector elements.

From the finger and palm images, the features extracted we formed a vector so all the finger and palm vectors are concatenated so that unique vector method is formed.

In our proposal feature vector of a person is formed by taking 20 unique points and 10 chaff points from finger and palm impressions. The block diagram of the feature extraction process is shown in figure 6.

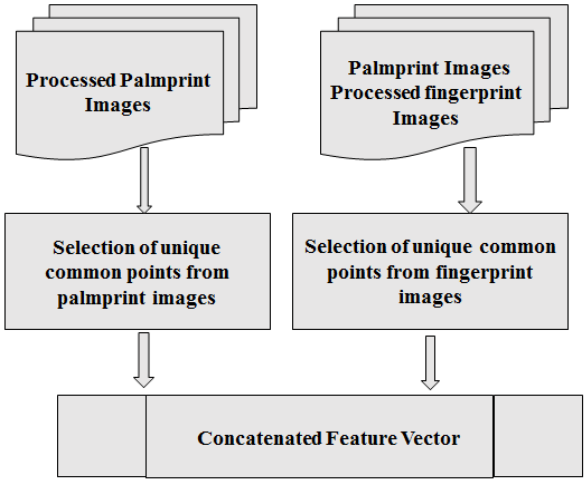


Figure 6. Feature Extraction Process.

3.2.1 Minutiae Extraction

A particulars descriptor comprises of edge introduction and recurrence at 76 equidistant focuses, consistently divided on 4 concentric circles around details. The four concentric circles, with span 27, 45, 63 and 81 pixels, contain 10, 16, 22 and 28 focuses, separately. The sweep and the quantity of focuses on each circle are chosen such that the descriptor values catch the most extreme data contained in the area of details.

Here both bifurcation and termination of ridges in both the fingerprint and palmprint are taken.

Bifurcation: The ridge pixels with three edge pixel neighbors are recognized as ridge bifurcations.

Termination: The ridge pixels with two ridge pixel neighbors are recognized as ridge terminations.

Introduction field is produced which not just demonstrates the edge framed by edge. It additionally speaks to the directionality of edges in the unique mark picture.

Locking and unlocking of fuzzy vault: The proposed multimodal biometric fluffy vault incorporates joined element points from palmprint and unique finger impression. The s proposed framework is appeared in Figure 5. At first the selected picture is preprocessed; the means taken after amid preprocessing are binarization, diminishing, details extraction, expulsion of false focuses and Region of Interest (ROI). The element focuses separated from both unique finger impression and palmprint pictures are intertwined and anticipated on the polynomial utilizing the proposed calculation.

In the event that a client wishes to conceal a mystery K utilizing his biometric format which is spoken to as an unordered set X. The client chooses a polynomial P that encodes the mystery K and assesses the polynomial on all components in X. Extra sham details focuses called refuse focuses which don't lie on the polynomial P are added to confound the programmer regardless of the possibility that he gets the entrance of the put away layouts. The waste focuses conceal the certified focuses lying on P from an aggressor. Since the focuses lying on P encode the entire data about the format X and the mystery K, concealing these focuses secures both the layout and the mystery key simultaneously.

The client can recuperate the mystery K from the vault V by giving another biometric test (inquiry). Give the question a chance to be spoken to as another unordered set X'. On the off chance that X' covers extensively with X, then the client can recognize many focuses in V that lie on P. In the event that satisfactory number of focuses on P can be distinguished and can reproduce P, then it is conceivable to decipher the mystery K. In the event that X' does not cover extensively with X, it is infeasible to reproduce P and the confirmation is unsuccessful. Since the mystery can be recovered from the vault notwithstanding when X and X' are not the very same, this plan is alluded to as a fuzzy vault.

In the proposed framework, multimodal fluffy vault for format security is executed for ensuring the biometric layout. Multimodal biometric innovation utilizes more than one biometric identifier to analyze the character of a man. This uses a blend of various biometric acknowledgment advances. Their execution is very much contrasted with single modular biometric frameworks. The proposed multimodal biometric fluffy vault incorporates joined element focuses from palmprint and unique mark.

3.2.2 Region of Interest (ROI)

Region of Interest (ROI) is helpful for the acknowledgment of each unique finger impression picture. The impressions area without powerful ridges and furrows is first disposed of in light of the fact that it just holds foundation data. It relies on upon the areas of details and the bearings of ridges at the particulars area. False details are influencing the exactness of coordinating. In this way, evacuating false details are fundamental to keep the framework successful.

ISBN: 978-0-9957075-6-6 DOI: 10.24032/ijeacs/0205/04

IV. System Methods

We use two different methods for the models used in the proposed multi modal biometric system.

1. *Individual Method (For Finger/Palm)*
   - Binarization
   - Thinning
   - Minutiae extraction
   - Biometric Authentication
2. *Direct Method*
   - Biometric Authentication

4.1 System Implementation

In the proposed Fingerprint and Palmprint Based: Multi – Modal Biometric System we have two main modules Pre-processing and Feature extraction and the above said modules are performed using MATLAB.

V. Experimental Results

For the proposed methods, from a single user sample images of finger print and palm print are collected and stored in any database. For the proposed system two biometric authentication cases should be verified. The cases are given below:

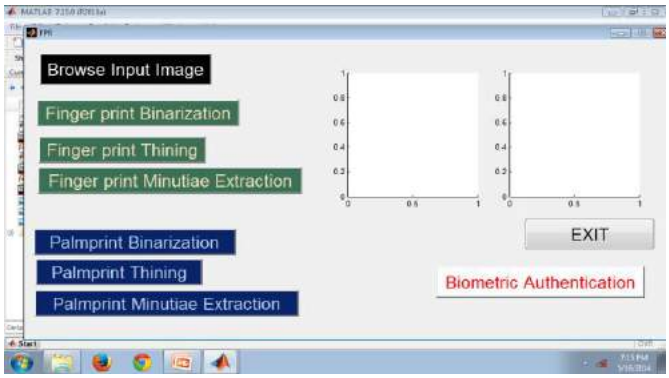
Case A: Successful Authentication
Input : Finger Print and Palm Print
Condition : Input should be of single person

Case B: Failure Authentication
Input : Finger Print and Palm Print
Condition : Input should be of different person

The experimental results for Case A and Case B for the proposed methods are explained below.

Proposed GUI of the System

The proposed GUI for the Finger Print and Palm Print multimodal biometric system is shown in the figure SS1. In this method the preprocessing modules for finger and palm are given.



SS 1: Proposed GUI for the system.

Method 1: Individual Method - Case A: Successful Authentication. The steps are given below.

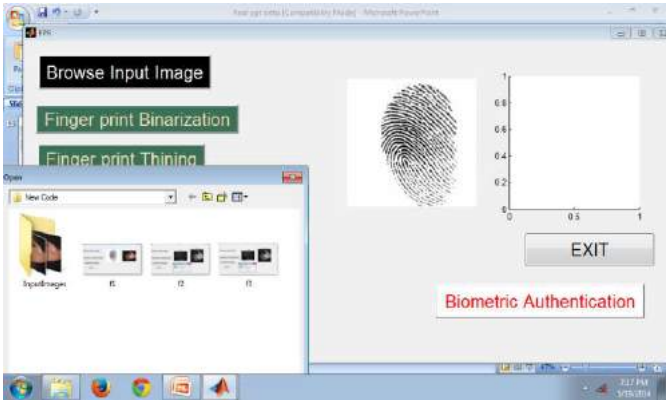
Step 1: Browse Finger Print Image

Need to browse the finger print image which is stored in the data base as shown in the figure SS2 by clicking on *Browse Input Image.*

SS 2: Browse Finger Print Image

Step 2: Browse Same Persons Palm Print Image

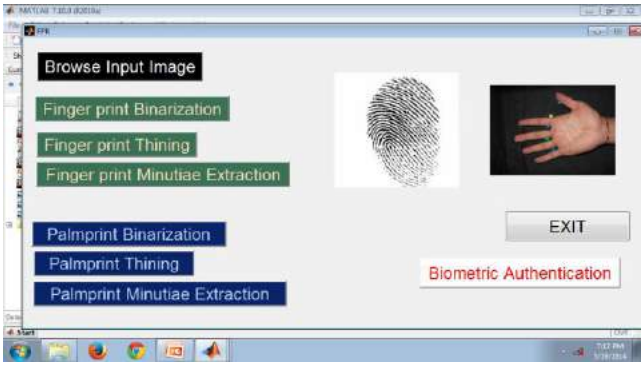
As the condition suggest in step 2 need to browse same persons palm print image which was chosen in step1is shown in figure SS3.



SS 3: Browse Same Persons Palm Print Image

Step 3: Input given Finger Print and Palm Print Images

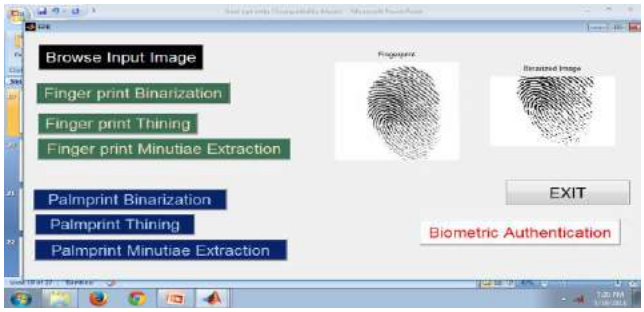
In this step the finger print and palm print images chosen are shown in figure SS 4.



SS 4: Input given Finger Print and Palm Print Images

Step 4: Finger print Binarization

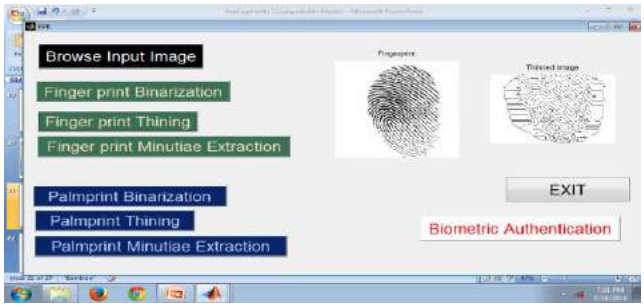
ISBN: 978-0-9957075-6-6 *DOI: 10.24032/ijeacs/0205/04*



SS 5: Finger print Binarization

When the user clicks on the Finger Print Binarization, the binarized image is shown as in figure SS5.

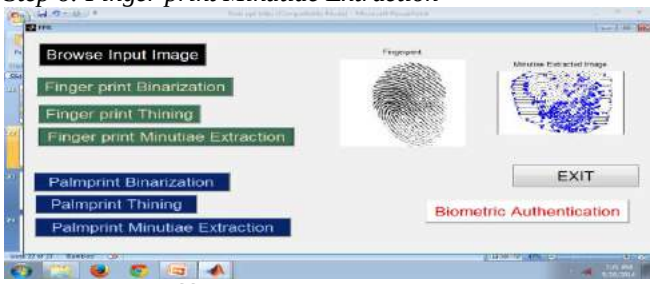
Step 5: Finger print Thining



SS 6: Finger print Thining

When the user clicks on the Finger Print Thining the thinned image is shown as in figure SS6 to eliminate the redundant pixels for the chosen finger print image.

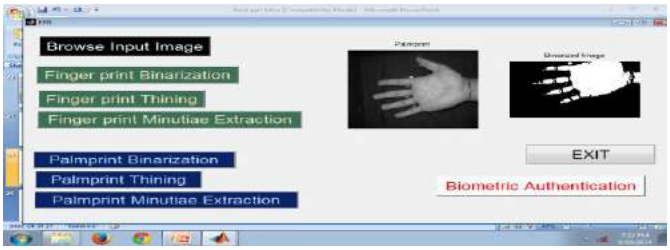
Step 6: Finger print Minutiae Extraction



SS 7: Finger print Minutiae Extraction

The Minutiae Extraction that consists of bifurcation and termination of the finger print image is taken from the step 5 and it is shown in the figure SS 7.

Step 7: Palm Print Binarization



SS 8: Palm Print Binarization

When the user clicks on the Palm Print Binarization, the binarized image is shown as in figure SS8.

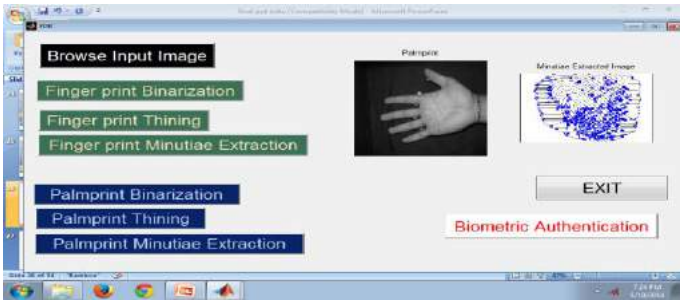
Step 8 : Palm Print Thining

SS 9 : Palm Print Thining

When the user clicks on the Palm Print Thining, the thinned image is shown as in figure SS6 to eliminate the redundant pixels for the chosen finger print image.

Step 9 : Palm Print Minutiae Extraction

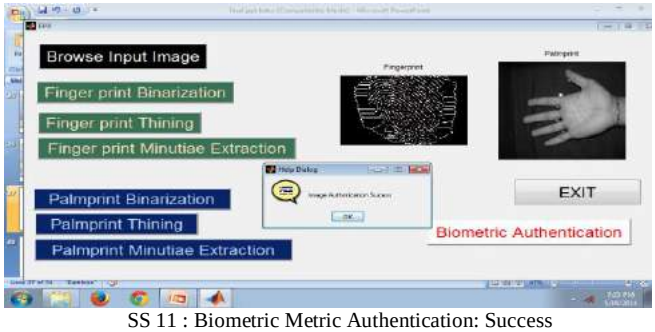
The Minutiae Extraction that consists of bifurcation and termination of the palm print is taken is shown in the figure SS 10.



SS 10 : Palm Print Minutiae Extraction

ISBN: 978-0-9957075-6-6 DOI: 10.24032/ijeacs/0205/04

Step 10 : Biometric Metric Authentication: Success



SS 11 : Biometric Metric Authentication: Success

The Finger Print image from the step 6 and the Palm Print image from step 9 are matched and if the images are matched then the authentication is given success is shown in figure SS 11.

Method 2: Direct Method - Case B: Failure Authentication. The steps are given below.

Step 1: Browse Finger Print Image

SS 12: Browse Finger Print Image

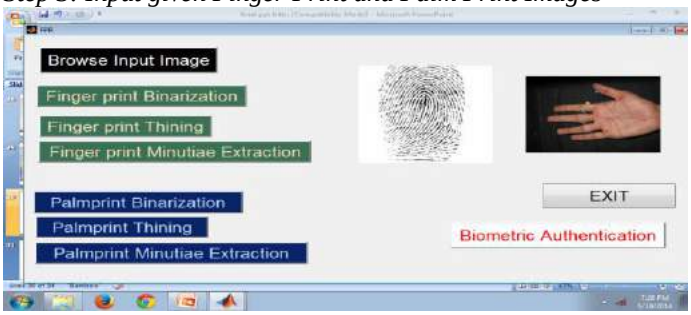
Need to browse the finger print image which is stored in the data base as shown in the figure SS12 by clicking on Browse Input Image.

Step 2: Browse Same Persons Palm Print Image

SS 13: Browse Same Persons Palm Print Image

As the condition suggest in step 1 need to browse same persons palm print image which was chosen in step1is shown in figure SS13.

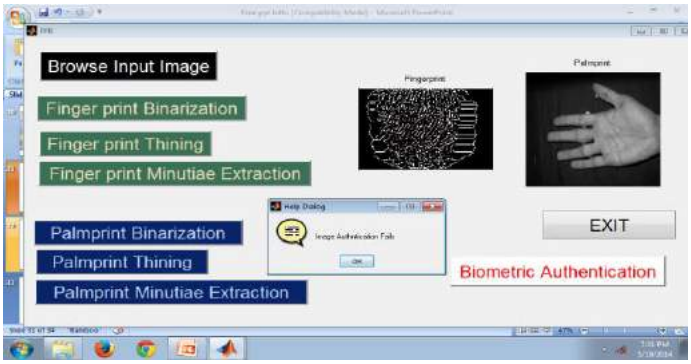
Step 3: Input given Finger Print and Palm Print Images



SS 14: Input given Finger Print and Palm Print Images

In this step the finger print and palm print images chosen are shown in figure SS 14.

Step 4: Biometric Metric Authentication: Failure Authentication



SS 15: Biometric Metric Authentication: Failure Authentication

The Finger Print image from the step 1 and the Palm Print image from step 2 are matched and if the images are matched then the authentication is given success and if the images are not matching than it shows Failure Authentication as shown in figure SS 15.

VI. CONCLUSION

In this proposal we have proposed fingerprint and palm print multi-modal biometric security system. Common features of finger print and palm print images are identified and the process is carried out for authentication. In the initial stage, the preprocessing steps are carried out on the chosen images which include binarization, thinning and minute extraction. In the next step for identifying the specific area in the finger print images region of interest is carried out. After the initial stage (preprocessing) features are extracted by using Feature Extraction method from both the finger print and palm print images and all the extracted features are combined to form a feature vector element. Secrete key is generated using the fuzzy extractor from the biometric features and stored in the fuzzy vault. The generated key and obtained vector elements are stored in the database. In final stage authentication methods are carried out for the test images. In this method feature of finger print images and palm print images are extracted and verified with the fuzzy vault and then a secrete key is generated. If the key generate and key stored in database are matched than the process is successful authentication or else it is failure authentication.

ISBN: 978-0-9957075-6-6 DOI: 10.24032/ijeacs/0205/04

REFERENCES

[1] Adler A (2003) Sample images can be independently restored from face recognition templates. In proceedings of Canadian Conference on Electrical and Computer Engineering, Montreal, Canada 2: 1163–1166.

[2] Ross AA, Nandakumar K, Jain AK (2006) Handbook of Multibiometrics. Springer 6.

[3] Jain AK, Feng J (2009) Latent palmprint matching. IEEE Transactions on Pattern Analysis and Machine Intelligence, USA 31: 1032-1047.

[4] Yanıkoğlu, Berrin and Kholmatov, Alisher Anatolyevich (2004) Combining multiple biometrics to protect privacy. In Proceedings of ICPR Workshop on Biometrics: Challenges arising from Theory to Practice, UK.

[5] Camlikaya E, Kholmatov A, Yanikoglu B (2008) Multi-biometric templates using fingerprint and voice. In Proceedings of SPIE Conference on Biometric Technology for Human Identification V, USA 6944.

[6] Juels A, Sudan M (2002) A fuzzy vault scheme. In Proceedings of IEEE International Symposium on Information Theory, 408.

[7] Juels A, Wattenberg M (1999) A fuzzy commitment scheme. In Proceedings of 6th ACM Conference on Computer and Communications Security, USA 28– 36.

[8] Freire-Santos M, Fierrez-Aguilar J, Ortega-Garcia J (2006) Cryptographic key generation using handwritten signature. In Proceedings of Biometric Technologies for Human Identification III, USA 6202: 225–231.

[9] Tuyls P, Akkermans AHM, Kevenaar TAM, Schrijen GJ, Bazen AM, et al. (2005) Practical biometric authentication with template protection. In Proceedings of 5th International Conference on Audio- and Video-Based Biometric Person Authentication, USA 436–446.

[10] Draper SC, Khisti A, Martinian E, Vetro A, Yedidia JS (2007) Using distributed source coding to secure fingerprint biometrics. In Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), USA 2: 129–132.

[11] Uludag U, Jain AK (2006) Securing fingerprint template: fuzzy vault with helper data. In Proceedings of IEEE Workshop on Privacy Research In Vision, USA 163-169.

[12] Feng YC, Yuen PC (2006) Protecting face biometric data on smartcard with reed-solomon code. In Proceedings of Computer Vision and Pattern Recognition Workshop, New York, USA 29.

[13] Dodis Y, Ostrovsky R, Reyzin L, Smith A (2008) Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM journal on computing 38: 97-139.

[14] Lee YJ, Bae K, Lee SJ, Park KR, Kim J (2007) Biometric key binding: fuzzy vault based on iris images. In Proceedings of Second International Conference on Biometrics, Seoul, South Korea 4642: 800–8

AUTHOR PROFILE

P. Appala Naidu, currently working as Asst Prof. in department of Computer Science and Engineering in Sri Indu College of Engineering and Technology(Autonomous), JNTU-H. Pursuing Ph. D in Computer Science and Engineering from Rayalaseema University, Kurnool-AP. Obtained M. Tech (CSE) degree from Acharya Nagarjuna University. Have overall 10 years of teaching experience. Guided many UG and PG projects as supervisor. Published several papers in international and national journals, conferences. Attended various FDP, workshops. Research areas include Image Processing and Data Mining. Member of IAENG, CSI.

Dr. CH GVN Prasad, M.Tech, Ph.D with experience of 23 years; 12 years IT industry, 8 years in National Informatics Centre, Govt. of India, as Scientist and Software Analyst in AT&T in US and 11 years Teaching as Professor and HOD of CSE dept. He is Currently Working as Professor in Department Of Computer Science & Engineering in Sri Indu College of Engg & Tech. Guided many UG, PG and Phd projects as supervisor. Published several papers in international and national journals. Research areas include Data Mining, Image Processing, Neural Netwoks and Network Security.

Prasad B, currently working as Assoc Prof. in department of Computer Science and Engineering from Marri Laxman Reddy Institute of Technology & Management (MLRITM) JNTU-H, Hyderabad. Prior to coming to MLRITM worked as Assistant Professor in various universities (Lovely Professional University, JNTU-H and Pondicherry University) and have total 10.5 Years of Teaching Experience. Pursuing PhD in Content Based Image Reterival through Clustering from Gauhati University, Guwahati. Received Masters Degree (M.Tech) in Distributed Computing Systems. from Pondicherry University. Received Bachelor's Degree (B.Tech) in Computer Science and Engineering from Kakatiya University. Research areas include Data Mining, Image processing and Cryptography. Member of IAENG, IFERP, ACM, CSI, IEEE. Supervised many UG and PG projects and present guiding one DST Project. Published several papers in international and national journals and conferences. Attended various FDP, workshops. Currently working on Multi-Modal Biometric Template Security: Fingerprint and Palmprint Based Fuzzy Vault including Human Face, Eye – Iris. And also on Content-Based Image Retrieval through Clustering.

Bhanuja Bodla, is studying B.Tech. in department of Computer Science and Engineering from Marri Laxman Reddy Institute of Technology & Management (MLRITM) JNTU-H, Hyderabad. Member of CSI. Currently working on IoT Based Security System using Raspberry pi. Successfully Developed a 3D Game -Bounty Rescuestep.