International Journal of Advanced Technology in Engineering and Science
Vol. No.4, Special Issue No. 01, March 2016
www.ijates.com
ijates
ISSN 2348 - 7550

MULTIMODAL BIOMETRIC RECOGNITION SYSTEM

Deepak A[1], Shrikant Shirsat[2], Sharon Alexander[3] and Ajit Yadav[4]

[1]*Assistant Professor,* [2,3,4]*Computer Engineering,*

St John College of Engineering and Technology, (India)

ABSTRACT

The main issue regarding the Unimodal Biometric System, that is the one, consisting of single biometric characteristics, is security. Even though Unimodal System provides security, it is easily susceptible to spoofing attacks. Thus it becomes necessary to increase the security of the Biometric System. Biometrics are mainly used as it varies from person to person making them unique from one another. In this paper, Multimodal Biometric Characteristics: Finger and Finger Knuckle print are used. By using Multimodal system the Accuracy, Reliability and Security is increased when compared with the traditional system. It also makes the system less vulnerable to various spoofing attacks. The fingerprint Recognition is done first by calculating the orientation flow field of the image then various morphological operations are performed in order to locate the features in the image. For the Finger Knuckle Print Scale Invariant Feature Transform is used to detect the features in Finger Knuckle Print. Then scores are calculated for both the biometric characteristics and the similarity between two images is calculated.

Keywords: Finger Knuckle Print, Minutiae, Multimodal System, Scale Invarient Feature Transform (SIFT), Unimodal System

I. INTRODUCTION

Biometric Traits are used to describe a human and differentiate him from other fellow human beings based on various characteristics which can be physical like fingerprints, palm print, iris etc or it can be emotional characteristics like writing, typing speed etc. These characteristics are used to provide authentication to the user. In many places biometric Characteristics are used to provide authentication to the user and it is the more secured way to provide security and mostly it is less likely to be tampered with. Thus due to this the vulnerability of the system due to various attacks is reduced.

Even though by using Biometric Characteristics the security is increased but still by using Unimodal System there may be chances that the system may be attacked by the intruders. So by using more than one characteristic that is by using Multimodal System the security of the system is increased. Biometric characteristics are used so as provide authentication to the user so that intruders are exempted from intruding.

There might be chances that sometimes due to improper acquisition of the biometric traits may be noisy or distorted, so in order to avoid the false matches we use a multimodal system. The chances of getting a false match gets reduced when a multimodal system is used as more the traits more are the chances of getting

similarity between two traits. The earlier works [1], [2] and [3] are sometimes ineffective in terms of getting the matches as they are unimodal system. So, in order to get more precise results Multimodal System are used.

The features that are mostly are used as minutiae are ridge endings and bifurcation. A finger print consists of Ridges and Valleys where the ridges are upper skin layer whereas the valleys are lower skin layer. Ridge Endings are the ends of a ridge and bifurcation is where the ridge splits into two. There are more patterns formed by ridge but these two are used at most for recognition purpose.

II. RELATED WORK

Biometric Recognition is a field that gained lots of attraction due to the uniqueness of the idea to use biometric characteristics in order to enhance security of a system. There were significant amount of work put together for using these Biometric Traits for matching purpose. Fingerprint Using Minutiae score matching [1] uses thinned images on which minutiae location and angle at which they are present is calculated. Fingerprint matching incorporating Ridge features with Minutiae [2] uses breadth first search for finding out the feature points. Adaptive Flow Orientation-Based Feature Extraction In Fingerprint Images[3] calculates the orientation and then by thinning the image locates the features in the image and then calculates the score of the image. Multimodal Finger Biometric Score Fusion Verification Using Coarse Grained Distribution Function[4] locates the features in finger and finger knuckle print and then calculates the score and combine them together.

The knuckle print is nothing but the back side part of our finger. In the previous days unimodal are more famous in biometrics recognition process but it less secure for the security purpose. Multimodal considers more than one features of Bio-metrics because it is a combination of more than one biometrics features and it provide more security to the complex system as compare to a unimodal system. In this paper we are providing both unimodal and multimodal based on several features. Various image morphological operations are performed on the image like Binarization, Thinning, Segmentation, Histogram Equalization. Finger print features are extracted based on the minutiae and ridges of our finger and knuckle feature based on the formation of line and the curve of line. Once the features are extracted then scores are calculated for both finger as well as knuckle print. After calculating the scores, the scores are fused.

III. ΕΞΙΣΤΙΝΓ ΣΨΣΤΕΜ

Biometric Recognition System has gained lots of importance over a period of time due to its uniqueness and effectiveness. Many systems use biometric system for the recognition purpose. Biometric system is not only used in authentication purpose, it is also used in crime scenes for gathering evidences. There are two types of systems existing in today's time: Unimodal system and Multimodal System. Biometric Traits such as Fingerprint, Finger Knuckle Print, Iris, Palm Print etc are used in identification of a human being. The identification process can be carried be carried out real time so as to authenticate a person in much faster time. The biometric Traits scores can be fused together to obtain a more secured result like in [4]. The [5] involves getting the fingerprint minutiae and then calculating the score value, then the highest score value obtained is given the highest priority in terms of matching. For the Finger Knuckle Print, in [8] a local convex direction

map is used that is used to align the image and then the region of interest is cropped where the key point are located.

3.1 Architecture

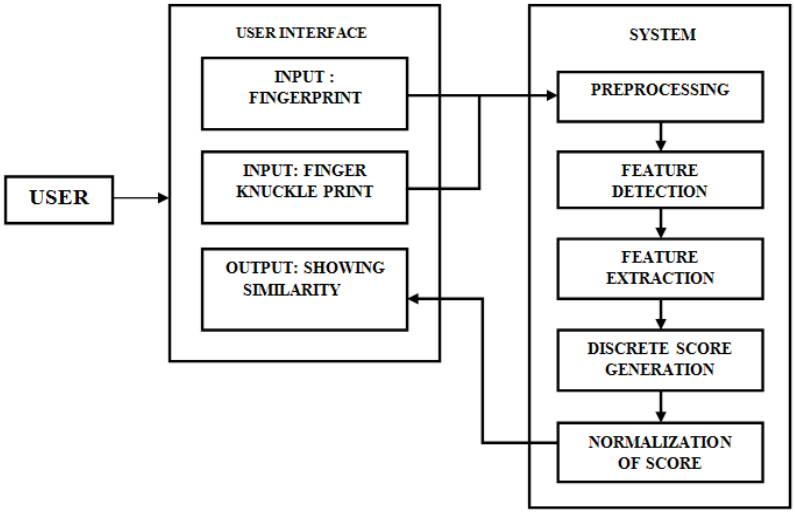


Fig. Architecture of proposed system

The user enters two input in the user interface: Fingerprint and Finger knuckle print. Then both the images undergoes pre-processing so that the image becomes suitable for detecting the minutiae within it and then after the pre-processing of the image the detection of the features within the image , that is location of the ridge termination and bifurcation is done. Then the extraction of the location where the feature is present is done. After this the score generation of the images is performed and then the scores are normalized. The output of the system shows the similarity between the images of finger and finger knuckle print with its original one to determine which one is most similar and which one is different.

3.2 Proposed Work

Various algorithms are proposed for the extraction of features in a fingerprint. The most basic steps in fingerprint matching: Binarization, Thinning and Feature Extraction as mentioned in [7] are used in detection of the minutiae. The whole point of processing the fingerprint image is to obtain a binary image of the ridges of fingerprint so that the location of the minutiae becomes easier.

We first give an input of gray scale image then process it in such a way that the resulting image has the values of ridges portion as black whereas the other parts of the images is white in colour. So, in order to get the binary image the [3] is referred in order to achieve the desired result.

Sometimes it may be possible that the image obtained of the fingerprint may be weak in terms of quality and texture. So, the orientation field is used to get the optimal ridge direction in the 16×16 window. A fingerprint image usually has region of interest which consist of the ridges and the valleys which are later used in the detection of the minutiae. Here segmentation of the image is done so that the noise and background areas are ignored while the extraction of the minutiae take place. A quality field is used to determine the quality of the image so that it could be determined whether the image is suitable for extracting the minutiae or not.

After the foreground and the background is identified then the next step is to identify the ridges present in the image. Here the image projected in the orientation field is considered. The ridge centre is projected and is shown at the peak. Before projecting the image it is smoothened first using an averaging mask along the direction of the orientation field. Commonly for segmentation thresholding is used in order to obtain a binary image that is suitable to detect the minutiae. During thresholding, the ridge pixels are assigned the value '0' whereas the valleys are assigned the value '1'.

After the ridge are located a 3×7 size window mask is applied to smooth the ridges located. After the ridges are smoothened then the skeleton image is obtained, that is the image is thinned so that the minutiae are extracted. Then these extracted minutiae are later used for checking the authentication of the user.

Later, post-processing of the image is done so as to eliminate the errors that may have occurred while capturing the image of the fingerprint.

So, basically we can describe the steps for extracting the fingerprint minutiae as:

- First of all, A Window of size 16×16 blocks is taken into consideration.
- Then the orientation of the image is found out so as to detect the background and foreground of the image.
- Then the ridges of the image is found out so as to get the minutiae.
- After detecting the ridges minutiae is located after Thinning and binarization is done.
- A 3×7 size window mask is applied to the ridges so as to smoothen the image.
- Minutiae are extracted by skeletonization of the image.
- Later post-processing of the image is done.

Finger Knuckle images are highly rich texture due to skin folds and creases hence it can be used as biometric identifier. The advantages of using FKP that they are easily accessible, contact-less image acquisition and the pattern formed is unique to different individuals.

There are many works done for capturing the Finger Knuckle Print and then detect the key points within the image and then we match the images. [6] introduces a method in which the image of the Finger Knuckle Print is divided into blocks of equal size and then the key point within the image are located.

FKP processing mainly consist of following four stages :

Image acquisition : System uses finger knuckle input image from camera having minimum resolution 1600x1200.

Extraction of region of interest: It is determined by drawing x axis and y axis over the knuckle print image.

Feature Extraction : [9]introduces method for detection and extraction of key-point. It is a vital part of FKP process this is done by using SIFT (scale invariant feature transform)

Each FKP image is divided into sub-blocks of 11x11 pixels. Enhancement operations is performed on that 11x11 block.

SFIT has following major operations:

Scale space extrema detection: The first computational search scans over all scales in an image position. It uses DoG(difference of Gaussians) function to find the potential interest point in an image.

Key point localization: once the potential interest point is found then it need to be refined to get more proper image. It uses Taylor series to get more accurate location of the stream.

Orientation assignment: to make the image invariant from the rotation operation this function is performed. It operates the local image properties. A neighbourhood is taken around the key point location depending on the scale.

Matching: FKP are matched with the corresponding features of all the knuckle-prints in the database. The matching scores between corresponding feature vectors are computed using nearest-neighbour-ratio method. Let Q and E be vector arrays of key-points of the query and the enrolled FKP respectively obtained using either SIFT.

Q = {q1; q2; q3; ..... qm}

E = {e_1; e_2; e_3; .....e_n}

Where qi and ej are the feature vector of key-point j in E respectively. If and are the Euclidean distance between and its first neighbour and that between and its second nearest neighbour respectively then,

$$Q_i = \begin{cases} \text{Matched} & \text{if ratio of neighbours are in T value} \\ \text{Unmatched} & \text{otherwise} \end{cases}$$

The matched key-points are removed from Q and E arrays. Process continues until there are no more matching points in both arrays. Total number of matching pairs considered as the matching score.

Fusion of matching score is the combination of finger print matching score and finger-knuckle print matching score to attain higher security level to the users.

$$\textit{score fusion} = \sum \textit{Normalization}\ (r1, r2)$$

it follows sum rule and attains good score value for improving recognition rate. Where r1 and r2 are the matching score values of finger-print and finger knuckle-print respectively.

3.3 Results

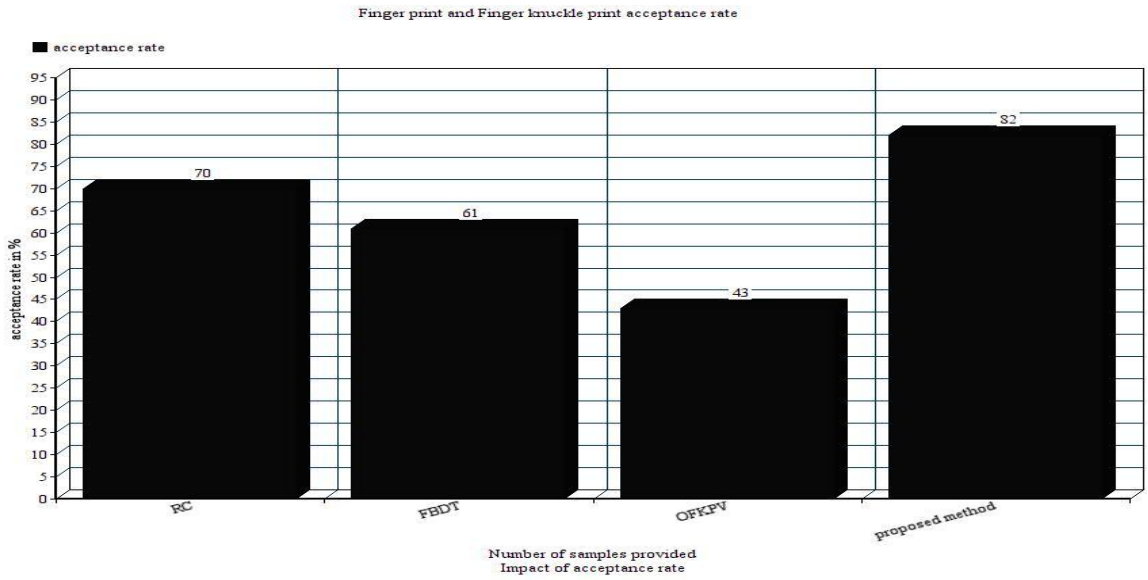
The proposed method described above has been implemented over the fingerprint database and finger knuckle print database.

The proposed work of finger print and finger knuckle print uses biometric score fusion mechanism. This mechanism is examined with the existing ridge count(RC) method , fuzzy binary decision tree (FBDT) and online finger knuckle print verification (OFKPV). For performing analytical experiment we have used PolyU database from Hongkong University for fingerprint and FVC2000 database for fingerprint. on the basis of results we have got from c#.net framework developed for proposed system, on an average 80 samples are considered and analyzed with help of graph given below.

3.3.1 Acceptance rate

The acceptance rate of proposed system is the ratio of no of authentic attempt accepted to that of total number of authentic attempts made using rating factor.

Genuine acceptance rate=No. of authentic attempts accepted /total no. of authentic attempts.



RC: Ridge count method

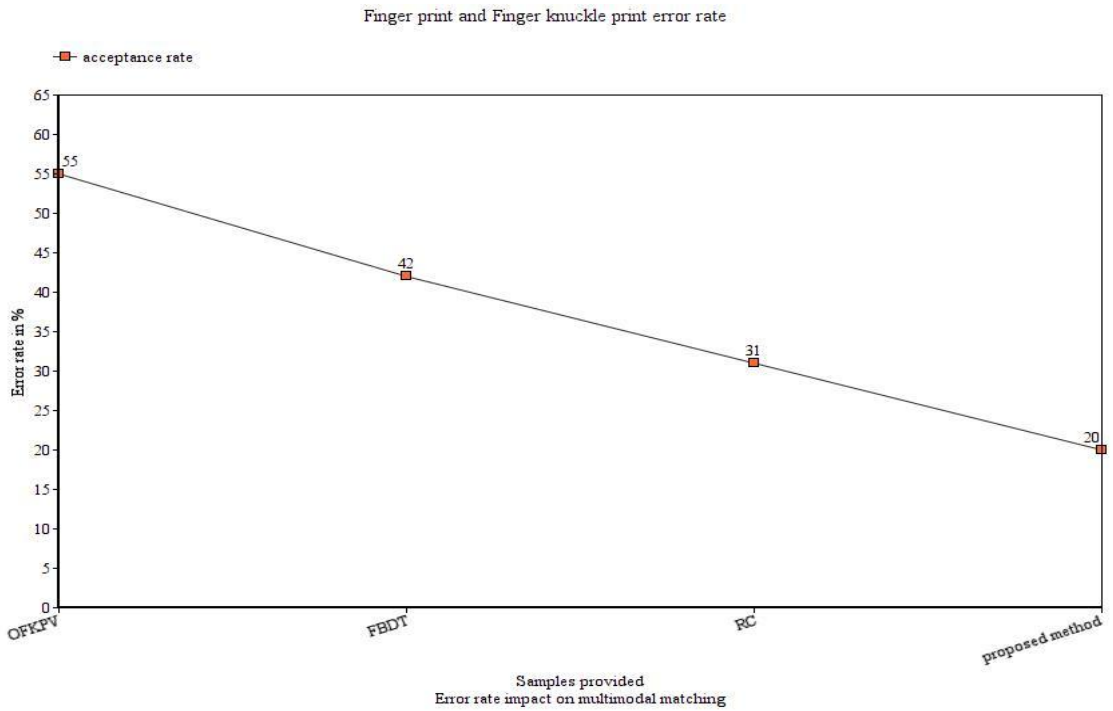
FBDT: Fuzzy binary decision tree

OFKPV: online finger print verification system

3.3.2 Matching error rate

The error rate on proposed mechanism is the ratio of number of authentic attempts refused for both finger print and finger-knuckle print with that of the total number of authentic attempts forms. It is measured in terms of percentage (%).

Error rate=No. of authentic attempts rejected /total no. of authentic attempts forms.



In above graph measure of error rate is done on sample images and compared against other three methods. Application of SIFT algorithm and minutie based finger print matching reduced the error rate by 30-40% compared to OFKPV and 20-30% compared to FBDT. Increase in score value results in lesser error rate than conventional ridge count(RC) system. Proposed system gives 10-20% less error rate than ridge count method.

IV. CONCLUSION

Multimodal are the unique combination of to days security trends. Every one needs more security or privacy of data with the unauthorized users or the parsons. This paper is based on feature extraction or minutiae extraction of the finger and knuckle print. In which basically ridge features are extracted based on ridge lengths, ridge type, ridge curvature direction based on this fours point minutiae feature are extracted.

Matching score represent the experimental value based on these value accuracy of the finger print matching are decided.

Calculated score of the finger print are matched with storing template image score if the score are correct than it will provide the authentication or some it will use for verification purpose. Matching methods are based on the quality of images. The ridge extraction feature are enhance the quality of images. Knuckle are the dorsal part of our finger knuckle feature extraction are provides the more accuracy to the system. Ratha algorithms are used for finger feature extraction or matching and SIFT are used for knuckle feature extraction.

V. ACKNOWLEDGEMENT

We are obliged and would like to thank our guide Deepak A for giving us valuable guidance and encouragement during the completion of the project. Without his continuous backing it would have been arduous for us to complete the project.

We are beholden to all the staff members for supporting us throughout the development of the project. We also express our sincere gratitude to our Principal Prof. Satish Takalikar for encouraging us and providing various facilities to us.

Last but not the least; we would like to thank our family and friends for constantly supporting us and encouraging us throughout the period of working for the project.

REFERENCES

[1] Ravi. J, K. B. Raja, Venugopal. K. R, Fingerprint Recognition Using Minutia Score Matching, International Journal of Engineering Science and Technology, Vol.1(2), 2009, 35-42

[2] Heeseung Choi, Kyoungtaek Choi, and Jaihie Kim, Fingerprint Matching Incorporating Ridge Features With Minutiae, Ieee Transactions On Information Forensics And Security, Vol. 6, No. 2, June 2011

[3] Nalini K. Ratha, Shaoyun Chen And Anil K. Jain, Adaptive Flow Orientation-Based Feature Extraction In Fingerprint Images, Pattern Recognition, Vol. 28, No. 11, pp. 1657 1672, 1995

[4] Mr.J.Stanly Jayaprakash1, Dr.S.Arumugam, Multimodal Finger Biometric Score Fusion Verification Using Coarse Grained Distribution Function, International Journal of Computer Science and I nformation Technologies, Vol. 6 (1) , 2015, 27-33

[5] P. Bhowmick, A. Bishnu, B. B. Bhattacharya, M. K. Kundu and C. A. Murthy, Determination of Minutiae Scores for Fingerprint Image Applications

[6] Rupesh Pawar, Beena Ballal, Ashwinkumar Padale, Rohan Sawant and Amar Garje, Biometric Authentication Using Finger Knuckle, International Journal of Computer Science & Communication Networks, Vol 5(2),88-91

[7] Romulo Ferrer L. Carneiro, Jessyca Almeida Bessa, Jermana Lopes de Moraes and Auzuir Ripardo de Alexandria, Techniques of Binarization, Thinning and Feature Extraction Applied to a Fingerprint System, International Journal of Computer Applications (0975 8887) Volume 103 - No. 10, October 2014

[8] Lin Zhanga, Lei Zhanga, David Zhanga and Hailong Zhu, Online Finger-Knuckle-Print Verification for Personal Authentication

[9] G S Badrinath, Aditya Nigam and Phalguni Gupta, An Efficient Finger-knuckle-print based Recognition System Fusing SIFT and SURF Matching Scores