Novel Method of Identifying Fingerprint Using Minutiae Matching in Biometric Security System

Supriti Ghosh, Mohammad Abu Yousuf

Institute of Information Technology, Jahangirnagar University, Savar, Dhaka, Bangladesh

Abstract*—*Fingerprint is one of the best apparatus to identify human because of its uniqueness, details information, hard to change and long-term indicators of human identity where there are several biometric feature that can be recycled to endorse the individuality. Identification of fingerprint is very important in forensic science, trace any part of human, collection of crime part and proof from a crime. This paper presents a new method of identifying fingerprint in biometrics security system. Fingerprint is one of the best example in biometric security because it can identify personal information and it is much secure than any other biometric identification system. The experimental result exhibits the performance of the proposed method.

***Keywords*—Biometrics Database, Biometrics Security, Feature Extraction, Fingerprint identification, Minutiae Matching.**

I. INTRODUCTION

Fingerprint identification is one kind of system to relate two friction ridge or minutiae from human fingers. Now a day electronic voting system is also fingerprint based and Gabor filter is used to match fingerprint [1]. IT security experts are very cared about the security allegation of using biometric system on different places.

For identification of fingerprint several methods have been proposed in literature [3]-[8]. Anil K. Jain and Jiangiang Feng [3] has proposed a method to match latent fingerprint using automated fingerprint identification system (AFIS) but it is very difficult to match latent fingerprint because in latent fingerprint matching, the problems are bad eminence of ridge imitations, small finger part and large non-linear altercation and all of that the experimental result has shown that uniqueness, ridge feature map and ridge flow map are the most active structures. Mohammad Umer Munir and Dr. Muhammad Younas Javed [4] has proposed a method of fingerprint matching using Gabor filter and the method is used a set of 16 Gabor filters which they used to internment the ridge strong point at equally space out alignment. Anil K. Jain, Lin Hong, Sharath Pankanti and Ruud Bulle [5] has proposed a method of a sample programmed identity-authentication system that practices fingerprints to authenticate the uniqueness of an individual and the proposed algorithm is alignment-based adaptable identical algorithm but this algorithm cannot grip huge alignment mistakes and huge alterations. Lifeng Sha, Feng Zhao and Xiaoou Tang [6] has represented a method of finding rotation-invariant orientation point location and the method is based on Minutiae matching to identify fingerprint. A wavelet transform based algorithm for fingerprint enhancement has proposed by Ching-Tang Hsieh, Eugene Lai and You-Chuang Wang [7] and the algorithm can recover clearness and stability of ridge structures created on the multi resolution analysis of universal consistency and local alignment by wavelet transform. Anil K. Jain and Jiangiang Feng [8] has proposed another new method that is created in Euclidean distance between two parallel FingerCodes and Gabor filter is used to detention of both local and universal details in a fingerprint as a compressed static length FingerCode.

Biometric is based on the brain and heart signals. There is two kinds of biometric identification systems. One of them is token based identification systems. One of them is token based identification system and the example of this system is password or personal identification number (PIN). Biometric identifier is cared about the privacy system of this information. To use physical characteristics or behavioral characteristics of any human to define their identify, biometric system is very beneficial.

A series of ridges and lines on the surface of the finger are made by fingerprints and to confirm that each point is unique, there is a core around which patterns corresponding swirls, loops or arches. The ridges arrive from one side of the finger, increase in the center forming an arc and end the other side of the finger, increase in the center forming an arc and end the other side of the finger is one kind of pattern and this kind of pattern is called an arch. The ridges arrive from one side of a finger, procedure a curvature and from the equal side they arrive is one kind of pattern and this pattern is called loop. Whorl is a pattern and this pattern is called loop. Whorl is a pattern where ridges from circularly around a middle point on the finger.

In the analysis of fingerprints, Minutiae and patterns are very important because no two fingers have shown to be equal. Minutiae is based on the individual structures in finger scanning technologies and the ridges and furrows are characterized by this irregularities. Minutiae points are local ridge features that happen at otherwise a ridge bifurcation or a ridge ending and the ridge ending is the point where a ridge ends. Where a single ridge differences into two ridges is called bifurcations point.

False accept rate (FAR) and False reject rate (FRR) are two parameters and they are usually used dimension in today's commercial environment and they determine in today's commercial and they determine the system performance and accuracy. False reject is genuine individual as pretender which is mistakenly recognized and the false reject rate is the corresponding error rate.

In this paper, the first challenge is to collection of fingerprint in digital format using a sensor. Then the second challenge is to store the components. Then the third challenge is to employ feature extraction to procedure a feature vector. The components of the feature vector are mathematical characterizedof the biometrics system. The forth challenge is fingerprint matching to relate a result which relates features vectors and specifies the degree of similarity between the pair of biometrics data. The fifth challenge is decision-maker to a program and accommodate system specification.

Contribution of this paper lies in following four aspects:

1. Obtaining data achievement using a digital sensor in biometric security components.
2. A simple pre-processing step such as Minutiae matching system is used for fingerprint matching because Minutiae matching is one of the best matching because of its reliability of extraction.
3. Then using the biometrics database, fingerprint is checked to match.
4. Finally, evaluate the performance of fingerprint matching and make the decision which is provided here.

Fig. 1 represents the steps of fingerprint matching in biometric security which we have proposed in this paper.

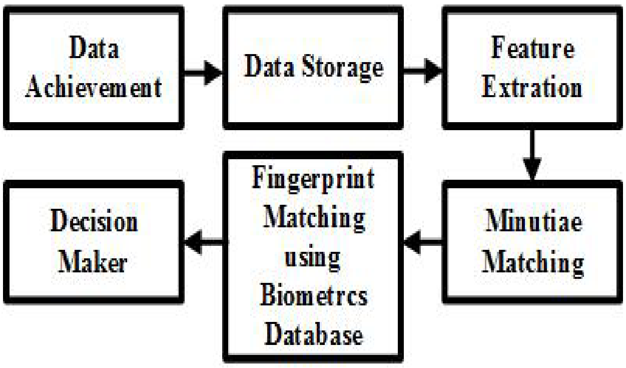

Fig. 1: The structure of proposed method

This paper is arranged as follows. In section II, there is discussed about the assessment of opposing fingerprint matching algorithm. Proposed methods is presented in section III. In section IV, the experimental results is given. After that in section V, there is discussed about the conclusion and discussions.

II. ASSESSMENT OF OPPOSING FINGERPRINT MATCHING ALGORITHM

The classifications of fingerprint matching techniques are of three categories which is dependent on the categories of features that is used to match fingerprint. They are Minutiae-based, correlation-based and Euclidean distance-based fingerprint matching.

2.1. Minutiae-based Fingerprint Matching

Minutiae-based fingerprint matching is fast but it is challenging to constantly extract minutiae in a deprived quality fingerprint image.

2.2. Correlation-based Fingerprint Matching

Correlation-based technique is to support the two fingerprint images and deduct the input image from the original image to realize if the ridges match. This technique is not too fast like Minutiae matching.

2.3. Euclidean distance-based Fingerprint Matching

Matching is based in a simple calculation of the Euclidean distance between the two equivalent feature routes and hence is enormously fast.

III. PROPOSED METHOD

The proposed method is identifying fingerprint using Minutiae matching in biometric security system because Minutiae matching is faster than other fingerprint matching techniques and this technique gives better result than others.

3.1. Data Achievement

Data achievement component obtains the biometric data in digital layout by using a sensor. In this paper, there is used an optical sensor contrived by digital biometrics. Optical sensor can change light emissions into electronic signals. It can operate on the standard of the frustrated total internal reflection (FTRL). LED light illuminate the glass platen. A charge-coupled device (CCD) array reflect and capture light tumbling on the ridges when a finger is positioned in the glass platen.

In Fig. 2, there represents a sensor which can take fingerprints.

3.2. Data Storage

The fingerprint image is stored in fingerprint database. The fingerprints are stored in the structures database along with the person identification number. To state a person using his identification number and fingerprints into a fingerprints database later the procedure of feature extraction is the impartial of the enrolment module.In this paper, the structures from a pattern is used to define or prove the identity of the matter, communicating the process of authentication.

Fig. 2: Optical sensor contrived by digital biometrics

3.3. Feature Extraction

Algorithm 1 represents the feature extraction procedure.

```
Algorithm 1: Feature Extraction
Step 1.   Find the reference point for the fingerprint image.
Step 2.   Tessellate the region around the orientation point.
Step 3.   Filter the region of concern in various directions.
Step 4.   Find the feature vector.
```

3.3.1. Finding Reference Point

Reference point has point, orientation and location. Five features like x and y coordinated, minutiae direction, type and quality is consisted by a minutiae. The secondary features are dots, incipient ridges and pores. A set of points represents the secondary features.

In Fig. 3, there represents fingerprints for finding reference point.

3.3.2. Tessellation

A collection of sectors define the spatial tessellation of fingerprint image which consists of the region of interest. Four concentric bands around the core point is used here and every band is 20 pixels wide and segmented into 32 sectors.Therefore there is 128 sectors and the region of importance is a circle of radius 100 pixels, focused at the reference point.

3.3.3. Filtering

To confirm that the performance of the structure is not pretentious by differences in value of fingerprint images, Gabor filter is one kind of band-pass filters of a fingerprint enhancement to eliminate the noise and store ridge structures is comprised in the Minutiae extraction module.

Fig. 3: Fingerprints for finding reference point

3.3.4. Feature Vector

Feature vector is the average of deviation from the mean. The average of deviation of each region in each of the sixteen filtered images defines the components of 2048 dimensional feature vector.

In Fig. 4, the fingerprints are represented.

Fig. 4: Fingerprints

3.4. Minutiae Matching

When a thinned ridge map is presented, Minutiae matching is a minor task. In minutiae matching, without loss of simplification, it has an importance of one and zero if a pixel is on a thinned ridge. The parameters of the ridge levelling heuristic are presently fixed to actual conventional values.

In Fig. 5, the steps of Minutiae matching is presented.

For fingerprint identification, histogram equalization and Fourier Transform is used in image enhancement. Using the nearby adaptive threshold method, image binarization is done.

In Fig. 6, the fingerprint image after Minutiae matching is represented.

3.5. Fingerprint Matching Using Biometrics Database

There is many different fingerprint biometrics technologies and all of these are available. To use a highly secure fingerprint in biometrics may be challenging and time-consuming.

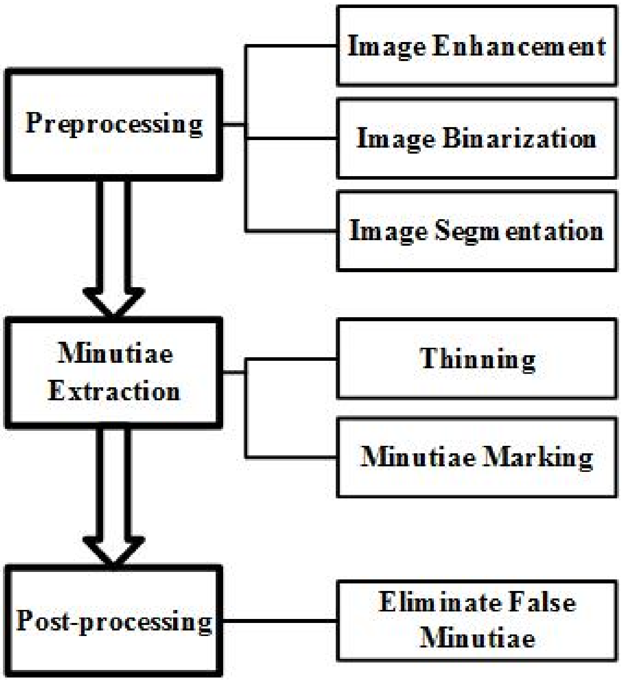

Fig. 5: Steps of Minutiae Matching

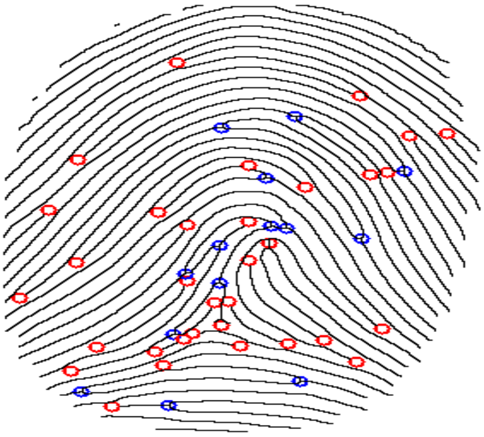

Fig. 6: Fingerprint image of Minutiae Extraction

3.6. Decision Maker

The final step of the proposed method is decision making. This paper is enabled to the user to first arrive one of the two fingerprints in a coordinated pair in a record that the programs protect nearby on the disk. Then, this paper enquires for a second copy to be matched against the record in the exploration for a match. The production values from each dimension were verified to identify fingerprint.

After that the decision is taken and it's much secured to identify fingerprint.

The Algorithm 2 represents the proposed method to identify fingerprint.

Algorithm 2: Fingerprint Identification

```
Step 1.   Collect data acquisition using digital sensor.
Step 2.   Store the image of fingerprint in fingerprint
          database with person identification system.
Step 3.   Determine the feature extraction.
Step 4.   Use the Minutiae matching steps for fingerprint
          matching.
Step 5.   Using biometrics database match the fingerprints.
Step 6.   Make the decision for fingerprint identification.
```

IV. EXPERIMENTAL RESULTS

The experimental results have shown about the no. of acceptance of fingerprint and the no. of rejection of fingerprints.

Table I shows the no. of pairs of fingerprints, the no. of false accepts, the no. of false rejects, the threshold values.

TABLE I. RESULT OF FINGERPRINT IDENTIFICATION

No. of Pairs	Results		
	Threshold Values	***No. of False Accepts***	***No. of False Rejects***
10	30	4 (9%)	1 (4%)
15	30	3 (8%)	1 (4%)
20	30	3(8%)	1(4%)
25	30	3 (8%)	1 (4%)
30	30	1 (8%)	1 (3%)

Here, threshold values are fixed for all of the pairs. And same threshold value is applied for both false accepts rate (FAR) and also for false rejects rate (FRR). Then, no. of false accepts rate (FAR) is better than no. of false rejects rate (FRR). In false accepts rate (FAR), there is a good percentage of acceptance. As the false rejects rate (FRR) is smaller than the false accepts rate (FAR), then the algorithm is in security and is active at all.

Here, the scheme was wider than the matching scheme which is obtained for the Algorithm 2. The FingerCodes are skilled of seizing more global and local information. The sincere distribution for this method was fairly thin since the Euclidean-distance based algorithm uses Gabor-filters.

V. CONCLUSION AND DISCUSSIONS

In this paper, the presented new method is identification of fingerprint using Minutiae matching in biometric security system. To understanding the main architecture of biometric security system is very important for this work and also to know about the process of finding out how a fingerprint verification structure works. To know about all specifications is also very important. The concern of mixture of an ideal algorithm for fingerprint matching that design a structure that equals the prospects in performance and correctness is of great anxiety to designer.

REFERENCES

[1] Sobia Baig, Ummer Ishtiaq, Ayesha Kanwal, Usman Ishtiaq and M. Hassan Javed, "Electronic voting system using fingerprint matching with Gabor filter." Procedings of International Bhurban Conference on Applied Sciences & Technologies, Islamabad, Pakistan, January 2011.

[2] Mary Lourde R and Dushyant Khosla, "Fingerprint identifications in biometric security systems," International Journal of Computer and Electrical Engineering, 1793-8163, Vol. 2, No. 5, October 2010.

[3] Anil K. Jain, Jianjiang Feng, "Latent fingerprint matching," IEEE Trans, PAMI, March 2009.

[4] Muhammad Umer Munir and Dr. Muhammad Younas Javed, "Fingerprint matching using Gabor filters," National conference on Emerging Technologies, 2004.

[5] Anil K. Jain, Lin Hong, Sharath Pankanti, Ruud Bolle, "An identity-authentication system using fingerprints," Procedings of the IEEE,Vol. 85, No. 9, September 1997.

[6] Lifeng Sha, Feng Zhao and Xiaoou Tang, "Improved FingerCode for filterbank-based fingerprint matching," IEEE ICIP, 0-7803-7750-8/03, 2003.

[7] Ching-Tang Hsieh, Eugene Lai and You-Chuang Wang, "An effective algorithm for fingerprint image enhancement based on wavelet transform," Pattern Recognition 36 (2003) 303-312, December 2001.

[8] Anil K. Jain, Satil Prabhakar, Lin Hong and Sharath Pankanti, "Filterbank based fingerprint matching," IEEE Transaction on Image Processing, Vol. 9, No. 5, May 2000.

[9] Ruude M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha and Andrew W. Senior, "Guide to Biometrics," Springer, 2013.

[10] NTSC Subcommittee on Biometrics, "Fingerprint Recognition," 2000.

[11] Bindu Garg, Arjun Chaudhury, Kunal Mendiratta, Vijay Kumar, "Fingerprint identification using Gabor filter," International Conference on Computing for Sustainable Global Development (INDIACom), 2014.

[12] Ankit Shrivastava, Devesh Kumar Shrivastava, "Fingerprint identification using feature extraction: A survey," Internation Conference on Contemporary Computing and Informatics (IC3I), 2014.

[13] Alessandra A. Paulino, Jianjiang Feng, Anil K. Jain, "Latent Fingerprint Matching Using Descriptor-Based Hough Tranform," IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[14] Vedpal Singh, Irraivan Elamvazuthi, "Fingerprint matching algorithm for poor quality images," The journal of engineering, 17th September, 2014.

[15] Xudong Jiang, Wei-Yun Yau, "Fingerprint Minutiae matching based on the local and global structures," IEEE Xplore, 0-7695-0750-6/00, 2000.

[16] D. K. Isenor, S. G. Zaky, "Fingerprint identification using graph matching," Pattern Recognition, Volume 19, Issue 2, 1986.

[17] G. Bebis, T. Deaconu, M. Georgiopoulos, "Fingerprint identification using Delaunay triangulation," International Conference on Information Intelligence and Systems, 1999.