International Journal of Engineering Research & Management Technology ISSN: 2348-4039
November-2016 Volume 3, Issue-6
Email: editor@ijermt.org www.ijermt.org

FACE VERIFICATION USING FINGERPRINT MATCHING

Neha Sharma
Department of Computer Science Engineering
Faculty of Engineering and Technology
Agra College, Agra

R. K. Sharma
Department of Computer Science Engineering
Faculty of Engineering and Technology
Agra College, Agra

ABSTRACT: In biometric, fingerprint system has been researched from a decade.Fingerprintsare formed at about seven months of foetus development and further the finger ridges configuration of the same does not change throughout the whole life. Fingerprint recognition (sometimes referred as dactyloscopy) is the process of comparing query fingerprint with the existing fingerprint to verify. This paper is divided into two sub domain. First approach is fingerprint verification in which image enhancement, image segmentation, feature extraction and minutiae matching are performed. The second approach is confidence level matching which is used to be matched with the predefined value. If the result is satisfied then fingerprint verification is performed and the croessponding face is shown in the result.

KEYWORDS: Biometrics, privacy, fingerprint verification, minutiae matching, face matching.

I. INTRODUCTION

Biometric is used in the process of authentication of a person by verifying or identifying that a user requesting a network resource is who he, she, or it claims to be, and vice versa. It uses the property thata human trait associated with a person itself like structure of finger, face details etc. By comparing the existing data with the incoming data we can verify the identity of a particular person [4].There are various types of biometric system like fingerprint recognition, face detection and recognition, iris recognition etc., these traits are used for human identification in surveillance system, criminal identification.

Advantages of using these traits for identification are that they cannot be forgotten or lost. These are unique features of a human being which is being used widely. Recognition under widely varying conditions like frontal view, a 45° view, scaled frontal view, subjects with spectacles etc. are tried, while the training data set covers a limited views. Further this algorithm can be extended to interpret the facial expression of a person. The most relevant information to describe a face is derived from the entire face image [5]. These are the Eigen functions of the averaged covariance, or normalized correlation, of the ensemble of faces. Measuring and analyzing facial features are used to recognize a person's face by comparing facial structures to that of a known person.

Many approaches that overcame face recognition challenges have been devised over the years, however, one of the most accurate way to identify faces is to use what is called the Eigen face technique. The Eigen-face technique uses a highly effective combination of linear algebra and statistical analysis (P C A) to generate an identifying set of base faces, the Eigen faces, against which the inputs are tested, compared and ultimately matched. Although using a sophisticated statistical model to recognize a person by facial patterns is important to identify that the collected data is clean and normalized, the objective is to represent a face as a linear combination of a set of base face images. Mat lab is used to create a linear combination model. This paper will discuss the implementation of the algorithm and attempt a critique of whether or not it is a viable solution for a current real-time application. A fingerprint is the feature patterns of one finger It is believed with evidences that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have been used for identification and forensic investigation for a long time. A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width.

Fig: 1.1 Local Features: Minutia

However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are some abnormal points on the ridges. Among the variety of minutia types reported in literatures, two are mostly significant and in usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive. The fingerprint recognition problem can be grouped into two sub-domains: one is fingerprint verification and the other is fingerprint identification. In addition, different from the manual approach for fingerprint recognition by experts, the fingerprint recognition here is referred as AFRS (Automatic Fingerprint Recognition System), which is program-based. Fingerprint verification is to verify the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information like his ID number. The fingerprint verification system retrieves the fingerprint template according to the ID number and matches the template with the real-time acquired fingerprint from the user. Usually it is the underlying design principle of AFAS (Automatic Fingerprint Authentication System).Fingerprint identification is to specify one person's identity by his fingerprint(s). Without knowledge of the person's identity, the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database. It is especially useful for criminal investigation cases and it is the design principle of AFIS (Automatic Fingerprint Identification System).However, all fingerprint recognition problem, either verification or identification, are ultimately based on a well-defined representation of a fingerprint. As long as the representation of fingerprints remains the uniqueness and keeps simple, the fingerprint matching, either for the 1-to-1 verification case or 1-to-m identification case, is straightforward and easy.

II. PROPOSED METHOD

Fingerprints are the ridge and furrow patterns on the tip of the finger and have been used extensively for personal identification of people [7]. The biological properties of fingerprint formation are well understood and fingerprints have been used for identification purposes for centuries. Since the beginning of the 20th century fingerprints have been extensively used for identification of criminals by the various forensic departments around the world.

Due to its criminal connotations some people feel uncomfortable in providing their fingerprints for identification in civilian applications. However, since fingerprint-based biometric systems offer positive identification with a very high degree of confidence and compact solid state fingerprint sensors can be embedded in various systems. Fingerprint-based authentication is becoming more and more popular in a number of civilian and commercial applications such as, welfare disbursement, cellular phone access, and laptop computer log-in.

The availability of cheap and compact solid state scanners as well as robust fingerprint matchers are two important factors in the popularity of fingerprint-based identification systems. Fingerprints also have a

number of disadvantages as compared to other biometrics. Further, since fingerprints cannot be captured without the user's knowledge, they are not suited for certain applications such as surveillance.

Biometric which refers to identifying an individual based on his or her physiological or behavioral characteristics has the capability to reliably distinguish between an authorized person and an imposter. Since biometric characteristics are distinctive, cannot be forgotten or lost, and the person to be authenticated needs to be physically present at the point of identification, biometric is inherently more reliable and more capable than traditional knowledge-based and token-based techniques.

Biometric also has a number of disadvantages. For example, if a password or an ID card is compromised, it can be easily replaced. However, once a biometric is compromised, it is not possible to replace it. Similarly, users can have a different password for each account, thus if the password for one account is compromised, the other accounts are still safe. However, if a biometric is compromised, all biometrics-based accounts can be broken-in. Among all

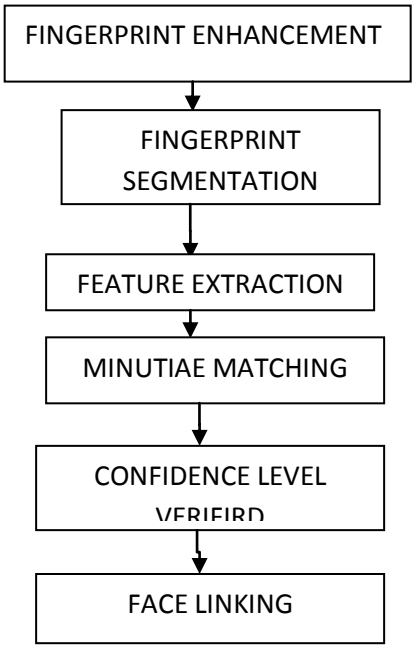

Fig: 2.1: Sequential stages for fingerprint to face linking.

a. Fingerprint Image Enhancement

Fingerprint Image enhancement is used for the purpose of making the image clearer for easy further operations. Since the fingerprint images acquired from sensors or other Medias are not assured with perfect quality, those enhancement methods, for increasing the contrast between ridges and furrows and for connecting the false broken points of ridges due to insufficient amount of ink, are very useful to keep a higher accuracy to fingerprint recognition.

Fingerprint image quality is an important factor in the performance of minutiae extraction and matching algorithms. A good quality fingerprint image has high contrast between ridges and valleys. A poor quality fingerprint image is low in contrast, noisy, broken, or smudgy, causing spurious and missing minutiae. Poor quality can be due to cuts, creases, or bruises on the surface of finger tip, excessively wet or dry skin condition, uncooperative attitude of subjects, damaged and unclean scanner devices, low quality fingers , weather changes and other factors. The goal of an enhancement algorithm is to improve the clarity of the ridge structures in a fingerprint.

b. Fingerprint Segmentation

In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges and furrows is first discarded since it only holds background information. Then

the bound of the remaining effective area is sketched out since the minutia in the bound region is confusing with that spurious minutia that is generated when the ridges are out of the sensor.

c. Minutia Extraction

Our research uses the minutiae-based fingerprint representation to design the systems due to the advantages of wide accessibility and stability. Minutiae-based fingerprint representation and matching are widely used by both machine and human experts. Minutiae representation has several advantages compared together fingerprint representations. Minutiae have been (historically) used to find out the features in fingerprint recognition tasks.

Its configuration is highly distinctive and several theoretical models use it to provide an approximation of the individuality of fingerprints. Minutiae-based systems are more accurate than correlation based systems and the template size of minutiae-based fingerprint representation is small. Forensic experts use this representation which has now become part of several standards [8] for exchange of information between different systems across the world. The reliability of minutia features plays a key role in automatic fingerprint recognition. Generally, the minutiae representation of a fingerprint consists of simply a list of minutia points associated with their spatial coordinates and orientation.

d. Algorithm Level Design

To implement a minutia extractor, a three-stage approach is widely used by researchers. They are preprocessing, minutia extraction and post processing stage [Figure 2.2].

For the fingerprint image preprocessing stage, we use Histogram Equalization and Fourier Transform to do image enhancement [1] and then the fingerprint image is binarized using the locally adaptive threshold method [6]. The image segmentation task is fulfilled by a three-step approach: block direction estimation, segmentation by direction intensity [2] and Region of Interest extraction . Most methods used in the preprocessing stage are developed but we form a brand new combination in our project through trial and error.

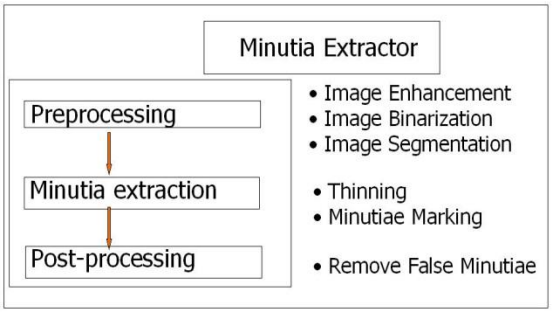

Fig: 2.2.: Minutia Extractor

For minutia extraction stage, three thinning algorithms [6] [3] are tested and the Morphological thinning operation is finally bid out with high efficiency and pretty good thinning quality. The minutia marking is a simple task as most literatures reported but one special case is found during our implementation and an additional check mechanism is enforced to avoid such kind of oversight. For the post processing stage, a more rigorous algorithm is developed to remove false minutia based on [6] [4]. Also a novel representation for bifurcations is proposed to unify terminations and bifurcations.

The minutia matcher chooses any two minutias as a reference minutia pair and then matches their associated ridges first. If the ridges match well [4], two fingerprint images are aligned and matching is conducted for all remaining minutia.

e. Proposed Algorithm For Removing False Minutia:

- If the distance between one bifurcation and one termination is less than D and the two minutias are in the same ridge, remove both of them. D is the average inter-ridge width representing the average distance between two parallel neighboring ridges.

- If the distance between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations.
- If two terminations are within a distance D and their directions are coincident with a small angle variation and they suffice the condition that no any other termination is located between the two terminations then the two terminations are regarded as false minutia derived from a broken ridge and are removed.
- If two terminations are located in a short ridge with length less than D, remove the two terminations.

Our proposed procedures in removing false minutia have two advantages. One is that the ridge ID is used to distinguish minutia and the seven types of false minutia are strictly defined comparing with those loosely defined by other methods. The second advantage is that the order of removal procedures is well considered to reduce the computation complexity. It surpasses the way adopted by [6] that does not utilize the relations among the false minutia types.

f. Proposed Algorithm for Minutia Match

- In first step, we calculate the transformation matrix and save into a variable.
- In second step, we calculate the difference between template and query finger print.
- In third step each element of these feature vectors is a minutiae point, which may be described by different attributes such as location, orientation, type, quality of the neighborhood region, etc.
- In forth step if the score value is greater than 0.99 then compute the similarity, otherwise does not recognize the fingerprint.
- In fifth step if confidence level which is 'S' satisfied that is greater than 0.99 then fingerprints matched with the croessponding face, finally the result is displayed.

g. Fingerprint to Face Linking

Finally fingerprints are matched to the given query on the basis of score value. If score value is greater 0.99 then particular fingerprint is matched and the croessponding face shown in the result otherwise not matched.

III. EXPERIMENTAL RESULTS:

For our analysis, we use the database FVC2002 .we have taken total (9*8=72) fingerprint images and the template are used as a part of images. First we are giving a query fingerprint image then enhancement of fingerprint is done for removing noise and false ridges. Our feature extracting algorithm used for finding the minutia after that these minutia is compared with our existing images in the database. If the confidence level is satisfied which is greater than 0.99then the given query fingerprint is matched with corresponding face otherwise it will show that the fingerprint is not matched with the given query images.

a. RESULT 1

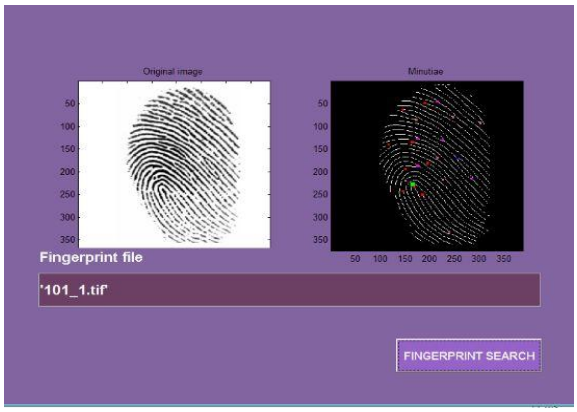

Fig.3.1 (a) fingerprint matching of person 1

Fig.3.1 (b) face verification of person 1 by fingerprint match

b. RESULT 2

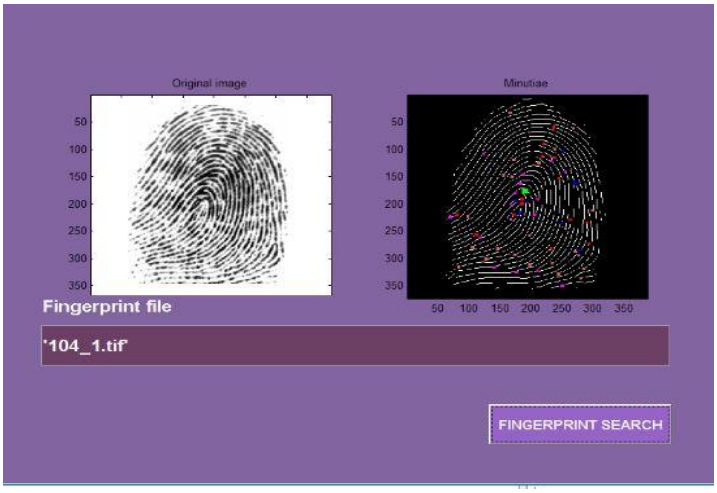

Fig.3.2 (a) fingerprint matching of person 2

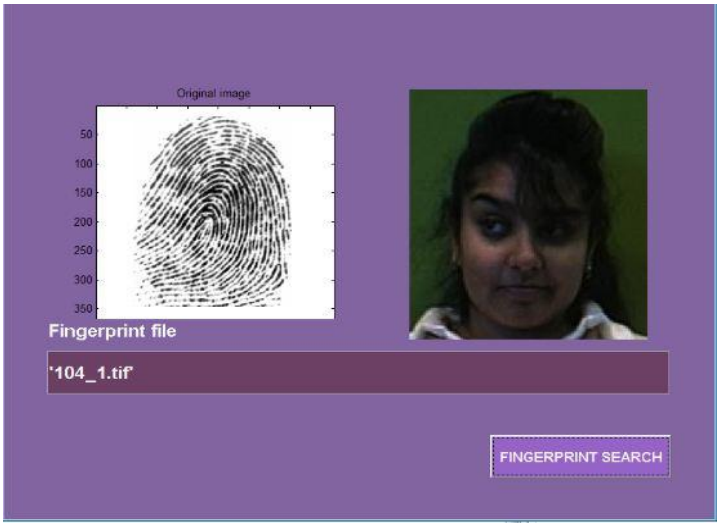

Fig.3.2 (b) face verification of person 2 by fingerprint match

c. RESULT 3

Fig.3. 3(a) fingerprint matching of person 3

Fig.3.3 (b) face verification of person 3 by fingerprint match

d. RESULT 4

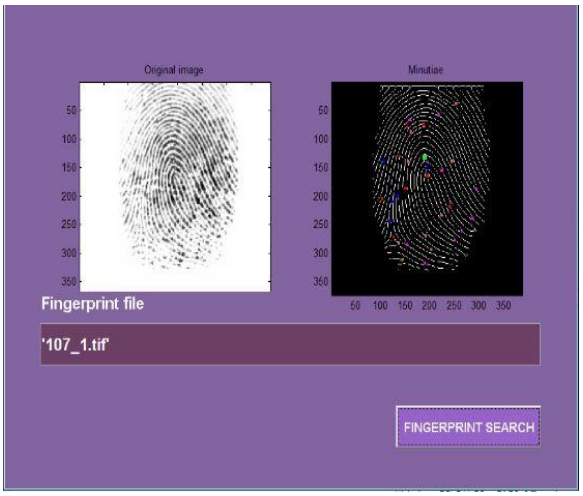

Fig: 3.4(a) fingerprint matching of person 4

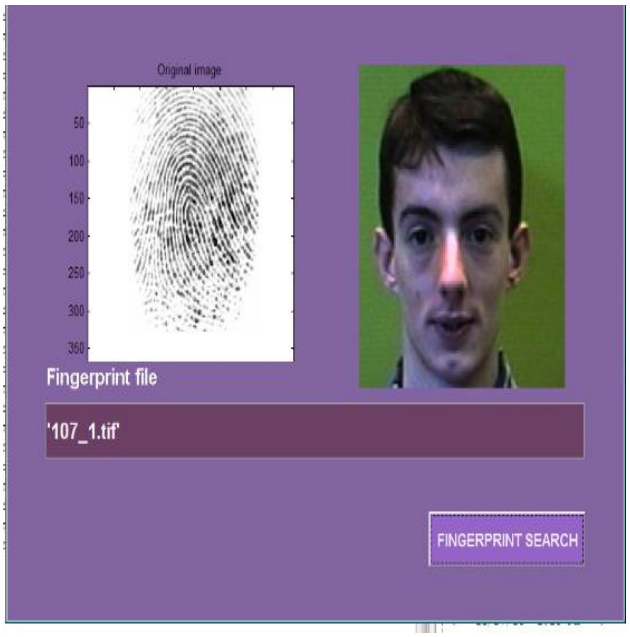

Fig.3.4 (b) face verification of person 4 by fingerprint match

e. RESULT 5

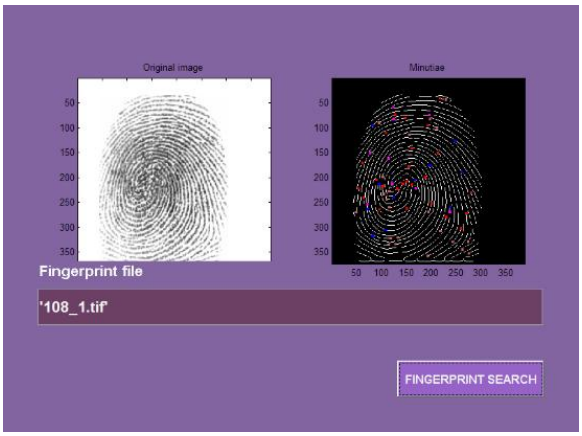

Fig.3. 5(a) fingerprint matching of person 5

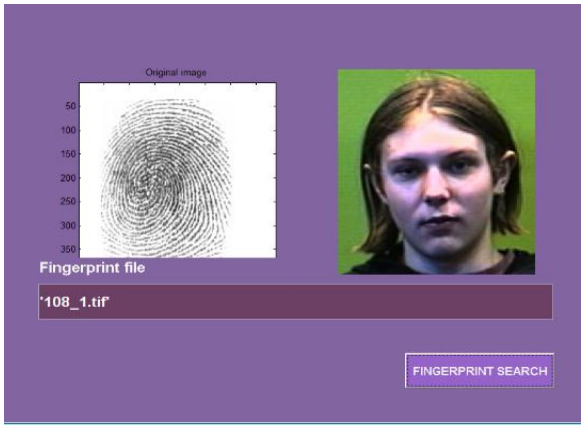

Fig: 3.5(b) face verification of person 5 by fingerprint match

IV. CONCLUSION

Due to security issues arising from the fingerprint verification, this paper proposes an algorithm of transforming fingerprint minutia and performs a fingerprint matching with showing the corresponding face. For over a decade, fingerprints have been one of the most highly used methods for process recognition. Automated biometric system has only been available in recent years. In this paper, we have aminutia matching with showing the corresponding face algorithm which gives a significant result. This paper makes a trade-off between accuracy and security.

In our future work, we are going to introduce a -captured by fingerprint scanner and facial image is captured by DSLR camera. It improves the accuracy of biometric security and makes the system safe and highly secured.

V. REFRENCES

1. Image Systems Engineering Program, Stanford University. Student project By Thomas Yeo, Wee Peng Tay, Ying Yu Tai.
2. N. Ratha, S. Chen and A.K. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, pp. 1657-1672, November 1995.
3. D.Maio and D. Maltoni. Direct gray-scale minutiae detection in fingerprints. IEEE Trans. Pattern Anal. And Machine Intell. 19(1):27-40, 1997.
4. Lin Hong. "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.
5. Alessandro Farina, Zsolt M.Kovacs-Vajna, Alberto leone, Fingerprint minutiae extraction from skeletonized binary images, Pattern Recognition, Vol.32, No.4, pp877-889, 1999.
6. L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui. Intelligent biometric techniques in fingerprint and face recognition. 1999, the CRC Press.
7. FVC2002 (fingerprint verification competition). http://bias.csr.unibo.it/fvc2002/
8. Bhabatosh Chanda and Dwijesh Dutta Majumder. Digital image processing and analysis. PHI Learning Pvt. Ltd., 2004.