International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

September-2019 Volume 6, Issue-5

Email: editor@ijermt.org www.ijermt.org

COMBINING FACE DETECTION AND FINGERPRINT MATCHING TECHNIQUE FOR AUTHENTICATION

Setu Maheshwari
Assistant Professor
Dr. B.T. Kumaon Instiitte of Technology,
Dwarahat

Sanchi Maheshwari
Assistant Professor
IET,Dr. B.R. Ambedkar University
Agra

ABSTRACT:

Face detection has been proven as the most interesting research field from the domain of image processing. In this paper, we are going to describe some important aspects of face detection, which are very much useful in many applications like face recognition, facial expression recognition, face tracking, facial feature extraction, gender classification, identification system, document control and access control, clustering and biometric science.

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 verification is the process of comparing query fingerprint with the existing fingerprint to verify.

KEY WORDS: Biometrics, privacy, fingerprint verification, minutiae matching, face matching.

INTRODUCTION:

Face detection‟ as the keyword itself reveals its meaning that it concerns about where a face is located in an image. Now it may seem very easy but in reality, we have to consider many constraints like single face or multiple faces, image rotation, pose etc. So, there may arise some false detected regions of an image, which do not contain any face. In spite of all these problems there are lots of techniques available.

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 that a 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.There are various types of biometric system like fingerprint recognition, face detection and recognition etc.these traits are used for human identification in surveillance system, criminal identification.

Face detection is a procedure by which we can able to extract face region from a human body. Now, the concept can be implemented in various ways but mainly we use four steps for this implementation. In the first step, we localize the face region that means we are anticipating those parts of an image where a face may present. In the second step we normalize the detected region, so that the alignments of various facial features are in the proper location. In the third step we extract various facial features like eyes, nose, mouth, etc. And in the forth step, we actually verify whether the anticipated parts are actually carrying out a face or not. We are doing this using some rules, template or image databases. The concept of extraction can be implemented by various techniques. There are a huge number of papers regarding the literature survey of face detection [3]. Most of the earlier work was on the frontal upright face, but recent work is mainly focus on non-frontal face with variation in their alignment. Also instead of still image, they are considering video stream images.

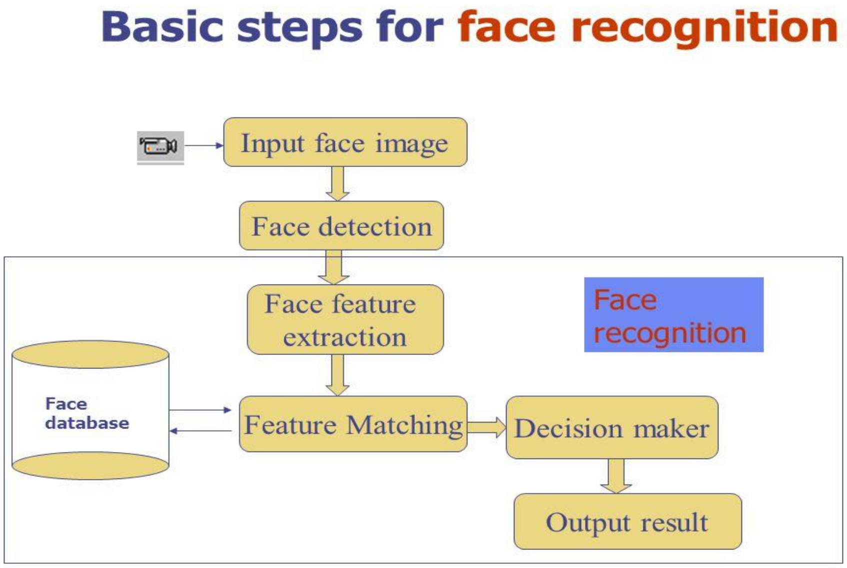


Fig. 1 Steps for Face Recognition

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.

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. 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 anumber 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.

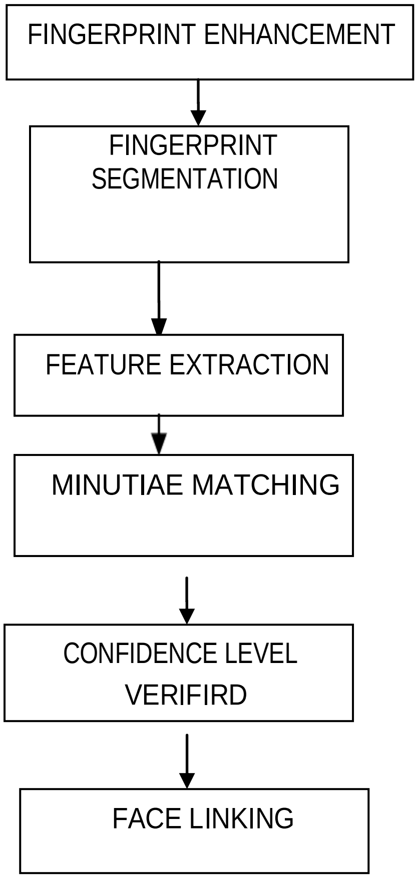


Fig: 2.1: Sequential stages for fingerprint to face linking.

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 fingerprintrecognition.

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.

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.

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 coordinate's andorientation.

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.

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.

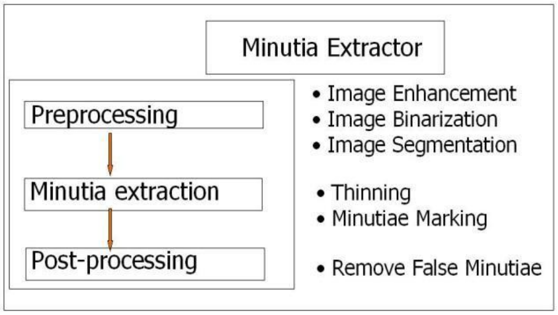


Fig: 2.2.: Minutia Extractor

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 andbifurcations.

The minutia matcher chooses any two minutiae's 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.

PROPOSED ALGORITHM FOR REMOVING FALSEMINUTIA:

- If the distance between one bifurcation and one termination is less than D and the two minutia's are in the same ridge, remove both of them. D is the average inter-ridge width representing the average distance between two parallel neighboringridges.
- 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 twoterminations.
-

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 minutiatypes.

PROPOSED ALGORITHM FOR MINUTIAMATCH

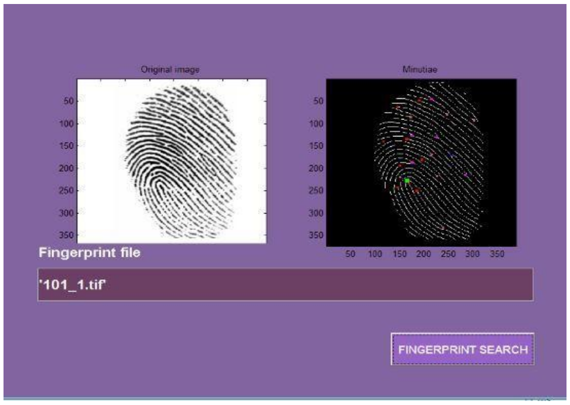
- In first step, we calculate the transformation matrix and save into avariable.
- In second step, we calculate the difference between template and query fingerprint.
- In third step each element of these feature vectors is a minutiae point, which may be described by different attributes such as location, 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 thefingerprint.
- In fifth step if confidence level which is 'S' satisfied that is greater than 0.99 then fingerprints matched with the correspondingface, finally the result isdisplayed.

FINGERPRINT TO FACELINKING

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 corresponding face shown in the result otherwise not matched**.**

EXPERIMENTAL RESULTS:

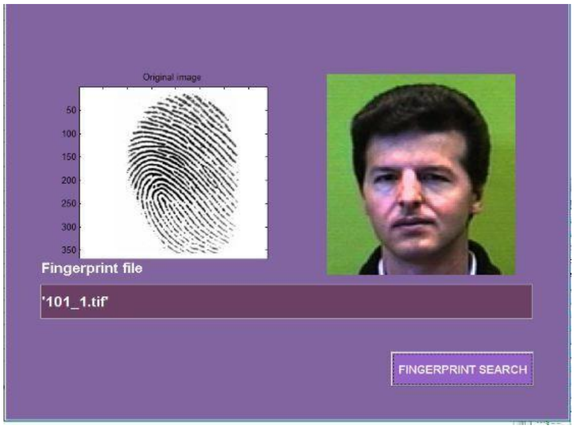
For our analysis, we use the database FVC2002 .we have taken total (9*8=72) fingerprint images and the template are used as a part of images. First we are giving a query fingerprint image then enhancement of fingerprint is done for removing noise and false ridges. Our feature extracting algorithm used 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.



Fingerprint file

'101_1.tif'

Fig.3.1 (a) fingerprint matching of person 1

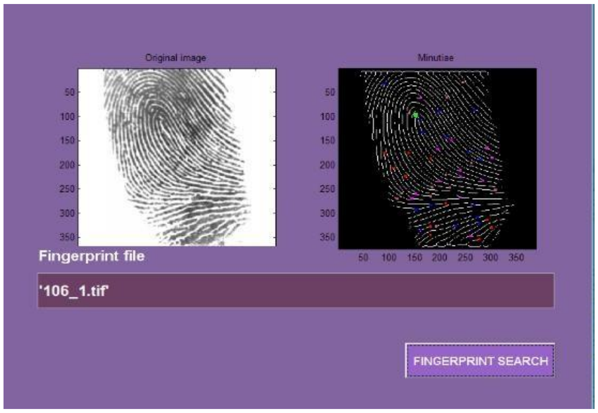


Fingerprint file

'101_1.tif'

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

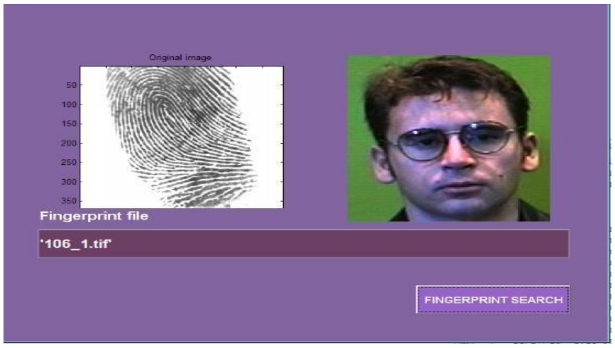
a. RESULT.2



Fingerprint file

'106_1.tif'

Fig.3. 2(a) fingerprint matching of person 2



Fingerprint file

'106_1.tif'

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

CONCLUSION

In this paper, we have covered a detail discussion on the various stages of any face detection technique. Also, some popular well-known face detection techniques are described very briefly. Recently, face detection techniques have been employed in different applications such as face recognition, facial feature extraction, detection of facial expression, which are also the subjects to be focused of this paper. Hence, before developing any kind of method of your choice, if you go through this paper, you will definitely get an overview of various ways used in face detection process.

REFERENCES

1. M. H. Yang, D. J. Kriegman, and N. Ahuja, “Detecting face in images: a survey,” IEEE Trans. Patter Analysis and Machine Intelligence, vol. 24, pp. 34–58, 2002..
2. K. Sobottka and I. Pitas, “Face localization and feature extraction based on shape and color information,”Proc. IEEE Int‟l Conf. Image Processing, pp. 483-486, 1996..
3. C. Lin, K.C. Fan, “Human face detection using geometric triangle relationship,” Proc. 15th ICPR, pp. 945–948, 2000.
4. K. Sobottka and I. Pitas, “Face localization and feature extraction based on shape and color information,”Proc. IEEE Int‟l Conf. Image Processing, pp. 483-486, 1996.
5. T. Sasaki, S. Akamatsu, and Y. Suenaga. Face image normalization based on color information. Tech. Rep. I.E.I.C.E., IE91-2, pp. 9–15 (1991).
6. C. Kotropoulos and I. Pitas, “Rule-based face detection in frontal views,” Proc. Int‟l Conf. Acoustics, Speech and Signal Processing, vol. 4, pp. 2537-2540, 1997.
7. C. Lin, K.C. Fan, “Human face detection using geometric triangle relationship,” Proc. 15th ICPR, pp. 945–948, 2000.
8. E. Hjelmas and B. K. Low, “Face detection: A survey,” Computer Vision and Image Understanding, vol. 83, pp. 236–274, 2001.

AUTHOR BIOGRAPHY:

Setu Maheshwari is currently working as TEQUIP-III Faculty Assistant Professor CSE in Dr. B.T. Kumaon Institute of Technology, Dwarahat.
His work includes Software Development, Publication of Books on C-lang, C++, Core Java, Data Structure, DBMS etc.

Sanchi Maheshwari is currently perusing PHD from Techno India University, Kolkata. Previously she was working as Assistant Professor CSE in Institute of Engineering & Technology Dr. B.R. Ambedkar University, Agra.
Her work includes Software Dovelopment.