A New Approach of Biometric Fingerprint verification

Sachin Harne [1], Vishnu Kumar Mishra [2], Pooja Agrawal [3]

[1] **Department of Computer Science, Dr. C.V. Raman University, Bilaspur, INDIA**

[2] **Department of Computer Science & Engg, GDRCET, Bhilai, INDIA**

[3] **Department of Computer Science, Dr. C.V. Raman University, Bilaspur, INDIA**

***Abstract**:*
Biometric authentication is an excellent way to security nowadays. Now it has been proven that each and every individual has its own biometric feature such as *Fingerprint, Iris, Footsteps, Face and Voice* which is different from other. These can be used to identify individual. Using biometric not only guarantees identification but it guarantees fast identification. Now day's technologies are exploring the features of biometric authentication for rapid and fast identification of individuals. Top it companies such as Nokia, Samsung, Motorola are using these features in mobile technology to securely authenticate right person. Again companies such as IBM, HP and HCL are using these technologies to provide fast and secure login to the devices. Fingerprint matching is the process used to determine whether two sets of fingerprint ridge detail come from the same finger. There exist multiple algorithms that do fingerprint matching in many different ways. Some methods involve matching minutiae points between the two images, while others look for similarities in the bigger structure of the fingerprint. Conventional security systems used either knowledge based methods (passwords or PIN), and token-based methods (passport, driver license, ID card) and were prone to fraud because PIN numbers could be forgotten or hacked and the tokens could be lost, duplicated or stolen. To address the need for robust, reliable, and foolproof personal identification, authentication systems will necessarily require a biometric component. This paper gives a brief review in the area of fingerprint verification.

Keywords: Fingerprint, biometric, Minutiae based technique, correlation based technique.

I. INTRODUCTION

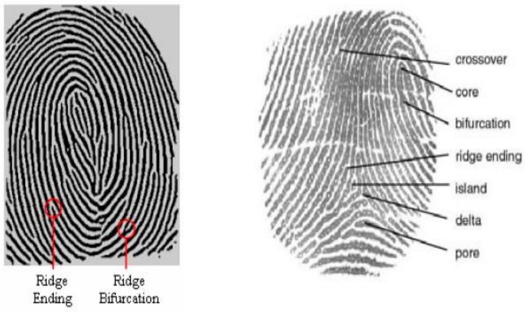
Fingerprint Verification brings a new dimension to biometrics in this information society era, while biometrics brings a new dimension to individual identity verification [2].In an increasingly digitized world the reliable personal authentication has become an important human computer interface activity. National security, e-commerce and access to computer networks are now very common where establishing a person's identity has become vital. Existing security measures rely on knowledge-based approaches like passwords or token-based approaches such as swipe cards and passports to control access to physical and virtual spaces, but these methods are not very secure. Tokens such as badges and access cards may be duplicated or stolen. Passwords and personal identification number (PIN) numbers may be stolen electronically. Biometrics such as fingerprint, face and voice print offers means of reliable personal authentication that can address these problems and is gaining citizen and government acceptance[3].

Automatic fingerprint recognition has become a widely used technology in both forensic and biometric applications. Despite history of thousand years during which fingerprints have been used as individual's proof of identity and decades of research on automated systems, reliable fully automatic fingerprint recognition is still an unsolved challenging research problem. Moreover, most of the research thus far, assumes that the two fingerprint templates being matched are approximately of the same size and cover large areas of the finger tip. However, this assumption is no longer valid. The miniaturization of fingerprint sensors has led to small sensing areas and can only capture partial fingerprints. Partial fingerprints are also common in forensic applications, where small usable portions of latent fingerprints must be matched with large previously enrolled complete fingerprints.

Biometrics	Universality	Uniqueness	permanence	collectability	Performance	Acceptability	Circumvention	Average
Finger print	75	100	100	75	100	75	100	89.29
Face	100	50	75	100	50	100	50	75.00
Hand Geometry	75	75	75	100	75	75	75	78.57
KeyStroke	50	50	50	75	50	50	50	53.57
Iris	100	100	100	75	100	50	100	89.29
Retinal Scan	100	100	75	50	100	50	100	82.14
Signature	50	50	50	100	50	100	50	64.29
Voice	75	50	50	75	50	100	50	64.29

2. FINGERPRINT

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Because of their uniqueness and consistency over time, fingerprints have been used for over a century, more recently becoming automated (i.e. a biometric) due to advancement in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration. [4]



As shown in fig.1. Skin on human fingertips contains ridges and valleys which together forms distinctive patterns.

These patterns are fully developed under pregnancy and are permanent throughout whole lifetime. Prints of those patterns are called fingerprints. Injuries like cuts, burns and bruises can temporarily damage quality of fingerprints but when fully healed, patterns will be restored. Through various studies it has been observed that no two persons have the same fingerprints, hence they are unique for every individual.

3. PROBLEMS WITH FINGERPRINT IDENTIFICATION

Some of the common challenges related with fingerprint technology are low quality or degraded input images, noise reduction, data security related issues with fingerprint systems etc. The low quality or distorted fingerprint images are perhaps the most common problem. The degradation can be of types like natural effects like cuts, bruises etc or it may be appearance of gaps on ridges or parallel ridge intercepts. The fingerprint enhancement techniques not only have to enhance the quality of image but at the same time also have to reduce noise. Much work has been done in this field and most commonly used method for this is application filter. O'Gonnan and Nickerson [5] proposed the first method which employed contextual filtering for fingerprint enhancement. Hong et al. [6], reported fingerprint enhancement based on the estimated local ridge orientation and frequency clarification of ridge and valley structures of input. Khmanee and Nguyen [7] proposed a method to develop 2D gabor filters for this purpose. Wang [8] proposed another method using log-Gabor filters. Çavusoglu [9] suggested a fast filtering method based on referenced mask of parabolic coefficients. Cheng and Titan [10] proposed scale space theory in which enhancement was done by first decomposing a series of images and then reorganizing them to a finer scheme using a cursor. Also recently, M.S.khalil et. Al [11] proposed a method for to verify an enhanced fingerprint image using four statistical descriptors which characterize a co-occurrence matrix.

4. TECHNIQUES FOR FINGERPRINT IDENTIFICATION

The existing popular fingerprint identification techniques can be broadly classified into three categories depending on the types of features used [12]

A. Correlation-based matching:

Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations).

B. Minutiae-based matching:

This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets that result in the maximum number of minutiae pairings

C. Pattern-based (or image-based) matching:

Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.[13]

5. Hausdorff Distance

A fast, reliable method for comparing binary images based on the generalized Hausdorff measure. The generalized Hausdorff measure provides a means of determining the resemblance of one point set to another, by examining the fraction of points in one set that lie near points in the other set (and perhaps vice versa). There are two parameters used to decide whether or not two point sets resemble one another using this measure: (i) the maximum distance that points can be separated and still be considered close together, and (ii) what fraction of the points in one set are at most this distance away from points of the other set. Hausdorff-based distance measures differ from correspondence-based matching techniques, such as point matching methods and binary correlation, because there is no pairing of points in the two sets being compared. Often in matching and recognition problems, the two images are allowed to undergo some kind of geometric transformation in the matching process. In this case we are concerned with finding the transformations of one image that produce good matches to the other image. We have developed efficient search techniques for the case where the transformation is a translation, or a translation and a scaling.

When talking about distances, we usually mean the shortest : for instance, if a point X is said to be at distance D of a polygon P, we generally assume that D is the distance from X to the nearest point of P. The same logic applies for polygons : if two polygons A and B are at some distance from each other, we commonly understand that distance as the shortest one between any point of A and any point of B. Formally, this is called a *min* function, because the distance D between A and B is given by :

$$D(A,B) = \min \{ \min \{ d(a, b) \} \} \qquad \text{eq. 1}$$

$$a \in A \quad b \in B$$

$$H (A, B) = \max \{ h (A, B), h (B, A) \} \qquad \text{eq. 2}$$

which defines the Hausdorff distance between A and B, while eq. 1 applied to Hausdorff distance from A to B (also called directed Hausdorff distance). The two distances h(A, B) and h(B, A) are sometimes termed as *forward* and *backward* Hausdorff distances of A to B. Although the terminology is not stable yet among authors, eq. 2 is usually meant when talking about Hausdorff distance. Unless otherwise mentioned, from now on we will also refer to eq. 2 when saying "Hausdorff distance".

If sets A and B are made of lines or polygons instead of single points, then H(A, B) applies to all defining points of these lines or polygons, and not only to their vertices. The brute force algorithm could no longer be used for computing Hausdorff distance between such sets, as they involve an infinite number of points.

```
1. From a1, find the closest point b1 and
   compute d1 = d ( a1, b1 )
2. h(A, B) = d1
3. for each vertex ai of A,
   3.1 if ai+1 is to the left of aibi
              find bi+1 , scanning B counterclockwise with CheckForClosePoint from bi
          if ai+1 is to the right of aibi
              find bi+1 , scanning B clockwise with CheckForClosePoint from bi
          if ai+1 is anywhere on aibi
              bi+1 = bi
   3.2 Compute di+1 = d (ai+1 , bi+1 )
   3.3 h (A, B) = max { h (A, B), di+1 }
```

REFERENCES

[1] Jain LC, Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press, 1999.

[2] A.K. Jain, R. Bolle and S. Pankanti, Biometrics: Personal Identification in a etworked Society, Kluwer Academic Publishers, 1999.

[3] D. Polemi, "Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable," Final Report, April 1997.

[4] http://www.biometrics.gov/documents/fingerprintrec.pdf

[5] W. Sheng, G. Howells, M.C. Fairhurst, F. Deravi,and K.Harmer, "Consensus fingerprint matching with genetically optimised approach", Pattern Recognition, Vol. 42, pp. 1399-1407, 2009.

[6] J. Feng, "Combining minutiae descriptors for fingerprint matching", Pattern Recognition, vol.
41,pp. 342-352, 2008.

[7] L. O’Gonnan, J.V. Nickerson, Matched filter design for fingerprint image enhancement, in:International Conference on Acoustics, Speech, and Signal Processing, 1988, pp. 916–919.

[8] L. Hong, Y. Wan, A. Jain, Fingerprint image enhancement: Algorithm and performance
evaluation,IEEE Trans. Pattern Anal. Mach. Intell. (1998) 777–789.

[9] C. Khmanee, D. Nguyen, On the design of 2D Gabor filtering of fingerprint images, in: First IEEE Consumer Communications and Networking Conference,CCNC 2004, 2004, pp. 430-435.

[10] W. Wang, J. Li, F. Huang, H. Feng, Design and implementation of log-Gabor filter in fingerprint image enhancement, Pattern Recognition Lett. 29 (2008) 301–308.

[11] A. Çavuso lu, S. Görgüno lu, A fast fingerprint image enhancement _ _ algorithm using a parabolic mask, Comput. Electr. Eng. (2008) 250–256

[12] Anil Jain , Lin Hong , Ruud Bolle,On-Line Fingerprint Verification, IEEE Transactions on Pattern Analysis and Machine Intelligence, v.19 n.4, p.302-314, April 1997.