ISSN No. 0976-5697

Volume 4, No. 3, March 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

A Reconsideration of schemes for Fingerprint Identification

Shaleen Bhatnagar*
Computer Science and Engineering
Pacific Institute of Technology
Udaipur, India
shaleenbhatnagar@gmail.com

Sarika Khandelwal
Computer Science and Engineering
Geetanjali Institute of technical studies
Udaipur, India
sarikakhandelwal@gmail.com

Neha Jain
Computer Science and Engineering
Mewar University Gangrar, India
neha.bordia@gmail.com

Abstract: Perhaps the most important application of accurate personal identification is securing limited access systems from malicious attacks. Among all the presently employed biometric techniques, fingerprint identification systems have received the most attention due to the long history of fingerprints and their extensive use in forensics. 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 identification. The aim of this paper is to review various latest minutiae based, correlation based and other global, local methods for fingerprint matching and status of success of concurrent methods with its advantage and disadvantage.

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

I. INTRODAUCTION

Biometric based recognition or we can say biometrics is a science of identifying and verifying the identity of a person according to its physical or behavioral characteristics. Biometric data are highly unique to each individual, easily obtainable non-intrusively, time invariant (no significant changes over a period of time) and distinguishable by humans without much special training. [1]. Biometrics in the high technology sector refers to a particular class of identification technologies. These technologies use an individual's unique biological traits to determine one's identity. The traits that are considered include fingerprints, retina and iris patterns, facial characteristics and many more.

Technology 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. It relies on "something that you are" to make personal identification and therefore can inherently differentiate between an authorized person and a fraudulent impostor. [3]

II. 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]

Fingerprint has the highest average value.

Figure 1: A fingerprint image obtained by optical sensor

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

Table I: Average calculation on the basis of features of Biometric system [3]

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumventi	Average
Face	100	50	75	100	50	100	50	75
Fingerprint	***75***	***100***	***100***	***75***	***100***	***75***	***100***	***89.3***
Hand geometry	75	75z	75	100	75	75	75	78.6
Keystrokes	50	50	50	75	50	75	75	60.7
Hand veins	75	75	75	75	75	75	100	78.6
Iris	100	100	100	75	100	50	100	89.3
Retinal scan	100	100	75	50	100	50	100	82.1
Signature	50	50	50	100	50	100	50	64.3
Voice	75	50	50	75	50	100	50	64.3
Gait	75	50	50	100	50	100	75	71.4

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.

III. CHALLENGES 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. Çavuso glu [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.

IV. 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]

V. ACKNOWLEDGMENT

This paper reviews different fingerprint identification approaches, fingerprint identification is one of the oldest and most common form of biometric identification. As a result, it's a common misconception that fingerprint recognition is a completely solved problem. The truth is,

the research on fingerprint recognition never stops due to its complexity and Intractability. Major challenge in Fingerprint recognition lies in the pre processing of the bad quality of fingerprint images which also add to the low verification rate. Some of the directions for the future research work in the field can be listed as follows:

A. Enhanced feature extraction and matching:

We still need to improve algorithms for better feature extraction and matching in a robust manner, especially for low quality and degraded images obtained from cheap image acquisition devices.

B. Secure fingerprint-based identification systems:

Like any other identification technique, fingerprint identification is not completely immune to fraud. R. Capelli et. Al [14] described a technique to reverse engineer minutiae based fingerprint templates. Several potential threats to the identification systems are attacks on communication channels, presenting fake fingerprints, replacing software modules with trojans, attacks on databases etc. A considerable amount of research on fake-detection approaches and template-protection techniques is definitely needed to address the most critical security threats.

VI. 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] http://www.csse.uwa.edu.au/~pk/Research/MatlabFns