ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 2, pp: (156-160), Month: October 2015 – March 2016, Available at: www.paperpublications.org

Fingerprint Feature Extraction, Identification and Authentication: A Review

[1]Farah Fayaz Quraishi, [2]Summera Ashraf, [3]Dr. Manzoor Ahmad Chachoo

[1, 2, 3] Department of Computer Science, University of Kashmir, Srinagar, Kashmir -190006, India

Abstract: **In the modern computerized world, due to high demand on fingerprint identification system, a lot of challenges keep arising in each phase of system, which include fingerprint image enhancement, feature extraction, features matching and fingerprint classification. Applications such as online banking and online shopping use techniques that depend on personal identification numbers, keys, or passwords. But there is the risk of data being forgotten, lost, or even stolen. One of the solutions to it may be biometric authentication methods which provide a unique way to identify, recognize and authenticate people. Fingerprints being the oldest methods of biometric authentication, are being explored at large. The main focus of the paper is to review fingerprint feature extraction, identification and authentication in different image/pattern based and minutiae-based fingerprints.**

***Keywords:* *Fingerprints, identification, feature extraction, authentication, AFIS*.**

1. INTRODUCTION

Fingerprint identification, also referred as “DACTYLOSCOPY”, is the method of verifying the fingerprints by comparing two instances of minutiae which can be extracted from human fingers, toes, or even the palm of the hand or sole of the foot. Fingerprint is one of the most researched and matured field of biometric authentication. The first known example of biometrics in practice was a form of fingerprinting being used in China (Joao De Barros, 2005).

Fingerprints offer a flawless and reliable means of personal identification, thereby, replacing other methods of establishing identities and authentication. The science of fingerprint identification and authentication outshines all other forensic sciences on the following grounds (E. Spinella, 2002):

1) Fingerprint details are permanent. Other visible human characteristics tend to change – fingerprints don’t. Although with age as the skin loses elasticity, fingerprints seem to be changed.

2) No two fingerprints have been ever found alike in many billions of humans and automated computer comparisons, although individuality has been recently challenged in many court cases. According to the empirical study, two individuals will not have more than seven common minutiae (E. Spinella, 2002, Maio and D. Maltoni)

Fingerprint Features Usually Considered:

***1) Coarse Features*:** also known by the name of singular-points, are suited during an identification for presorting in a very large database and include:

- ***Arch*:** These ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of finger.
- ***Loop:*** The ridges enter from one side of a finger, form a curve, and then exit on the same side.
- ***Whorl:*** Ridges form circularly around a central point on the finger.

***2) Fine Features*:** The major minutia features of fingerprint ridges are:

- ***Ridge Ending*:** point at which ridge terminates.
- ***Bifurcation:*** point at which single ridge splits into two ridges.
- ***Short Ridge* (Or Dot):** are ridges which are significantly shorter than the average ridge length on fingerprint.
- ***Core-Point*:** is the top-most point on the inner most ridge.
- ***Delta-Point*:** is the tri-radial point with three ridges radiating.

To identify and authenticate fingerprints, two steps are involved: Classification and Matching. Classification is the method of grouping fingerprints into a few types based on a criteria while fingerprint matching is a method that uses some sort of algorithm to assign the fingerprint to a particular person it belongs to, that is found in the database..

2. BACKGROUND

Fingerprints are constant, unique and form the most reliable criteria for identification (Pillay, 2009; Kanchan, T. Chattopadhyay, S., 2006). It has been shown that fingerprints provide high accuracy when compared with other existing biometric traits (A.K. Jain, P. Flynn, & A.A Ross; 2007). They are persistent in nature as they don't easily change with age, unlike face and voice patterns. Fingerprints are incomparably the most sure and unchanging form of all other forms of signature (Francis Galton, 1892). According to Dario Maio and Davide Maltoni, "fingerprints are defined by a set of ridge lines and they can run parallel, can terminate sometimes or can even intersect each other and the points where the ridge lines are terminated, are known as Minutiae (D.Maio and D.Maltoni, 1997)." According to Galton, "each ridge is characterized by numerous minute peculiarities called Minutiae, which may divide and almost immediately reunite, enclosing a small circular or elliptical space or sometimes the independent beginning or ending of ridges (Francis Galton, 1892)". In a fingerprint image, ridges are dark whereas valleys are bright. Ridges and valleys often run in parallel; sometimes they bifurcate and sometimes they terminate. A good quality fingerprint contains 25-80 numbers of minutiae (Neil Yager and Adnan Amin, 2004) which depend on the resolution and finger placement on the sensor. However, the fingerprint image captured through poor scanners, are found to have fewer number of minutiae points. The secretions in the fingerprints contain various chemicals and their metabolites which can be detected and used for the forensic purposes (Maio and D.Maltoni).

Automatic fingerprint authentication systems can be broadly classified into two categories [13].

1. Pattern (Image) based systems.
2. Minutiae based systems.

Literature Review Of Pattern / Image Based Fingerprint Authentication Systems.

Different authors have proposed different solutions to the problems of Pattern / Image Based Fingerprint Authentication Systems.

1. Bazen et al. (A. M. Bazen and S. H. Gerez, 2000] proposed a 3- step correlation-based fingerprint verification system.

Step 1: Firstly, small sized templates are selected in the primary reference fingerprint.

Step 2: Then using the technique of template matching, the query (secondary) fingerprint is found. The secondary fingerprint is the one to which the template matches the most.

Step 3: To authenticate fingerprint matching, comparing template position in both the fingerprints is done. If the template position in both the primary and secondary fingerprint is same, the fingerprints are authenticated, else the case is opposite.

Advantage:

i) More stable than methods where correlation is computed globally. In this method, correlation is computed locally as small templates are selected.

ii) Can tolerate the non-uniform local shape distortions in the fingerprint.

Dis-Advantage:

i) Computationally more expensive.

ii) Not able to deal with rotations of more than 10 degree.

2. Nandkumar et al. [K. Nandakumar and A. K. Jain,2004] proposed a local correlation-based fingerprint matching algorithm. In this algorithm, two different window sizes are used. One window is used for the minutia locations in the template image with window size of 42*42 pixels and another is used for the corresponding location in the query (secondary) image with window size of 32*32 pixels. The peak is detected by calculating the normalized cross-correlation between the query (secondary) window and the template window. All the possible correspondence from the alignment stage are tested and maximum correlation value over all the correspondence is taken as the matching score between the query and template image.

Case i): If the distance between the peak and center is more than 10 pixels, the correlation between the template and query (secondary) window is zero.

Case ii): If the distance between the peak and center is less than 10 pixels, then there is an absolute value of correlation between the query and template window. In all template windows, the local correlation with their corresponding regions in the query (secondary) images are found and their mean correlation is calculated.

Advantage:

i) More stable than methods where correlation is computed globally.

Dis-Advantage:

i) All minutiae points are to be extracted so that all the related problems remain in the system database.

ii) Proper alignment algorithm is used before matching.

iii) System is computationally expensive.

3. Owang et al. [Z. Ouyang, J. Feng, F. Su and A. Cai, 2006.] proposed a correlation-based matching method using two functions i.e. Fourier- Mellin descriptor (FMD) and phase only correlation (POC). Most likely FMD pair is calculated from the pair images and then the two fingerprints are aligned and other corresponding FMD pairs are checked if they are matched or not. For the calculation of similarity of two FMDs and the alignment parameters, the POC function is used.

Advantage:

i) Is fast.

ii) Does not require any minutiae or core information while taking rotation into account. .

Dis-Advantage:

i) Computationally more expensive.

ii) Requires efficient method for the extraction of local FMDs to improve the performance of the system.

4. Cavusoglu et al. (A.Cavusoglu and S. Gorgunoglu, 2007) proposed a robust correlation-based fingerprint matching algorithm. Before the application of correlation, the steps followed in the algorithm requires segmentation, ridge orientation, reference point detection and normalized operation algorithm. In the enrollment stage, a set of features, starting from the core, are obtained with different radius (r) and with different angles (θ). The set of features are obtained by rotating the query image. For each rotation, the normalized cross correlation values of both the template and the query images are calculated. Higher the value of cross correlation, higher is the similarity between the query and template image.

Advantage:

i) Is efficient in terms of storage as only a set of features of template image are stored instead of the whole template image.

Dis-Advantage:

i) Requires the accurate detection of core point.

ii) The method may fail in case the core is not present in the image.

Literature Review Of Minutiae-Based Fingerprint Systems:

Generally there are 2 steps involved in fingerprint matching algorithms, first to align the fingerprints and then find the correspondences between the two. The various matching algorithms already given include:

1. **Jain et.al** [Jain A.K., Hong l., Pankati S., Bolle R,1997] : the algorithm given by Jain et.al is capable of compensating for some of the non-linear deformations and then finding the correspondences. The problem with the technique is that for accurate alignment; size of the image should be large, which takes much memory and computation.

2. **Kovacs-Vajna** [Kovacs-Vajna Z.M., 2000] : uses a triangular matching algorithm to deal with the deformations of fingerprints. However, the main drawback of this technique is that without further verification the final results of this matching algorithm are not acceptable.

3. **Jiang and Yau** [Jiang X., Yau W.Y., 2000] use both the local as well as global structures of minutiae in which the local structure of a minutiae are used to describe the rotation and translation invariant feature of the minutiae in its neighborhood, while as global structure define the uniqueness of fingerprint. The main drawback in this technique is that it can't be used to compensate for real world distortions of a 3D elastic finger.

3. SUMMARY

The notable strengths of fingerprint recognition include:

- It provides a high level of recognition accuracy.
- User friendly as it doesn't require complex user-system interaction.
- Due to its small interface can be used in a broad range of applications , such as E-Commerce, PC's and mobile login.

Some of most common *CHALLENGES* faced while dealing with fingerprint biometric authentication include:

- Low quality of input (primary) images,
- Data security issues related with fingerprint systems,
- It is not yet proved that fingerprints are unique and families don't share elements of the same pattern,
- It is difficult to scan fingerprints of the elderly person as their skin loses elasticity and in some rare conditions can also leave some people with smooth, featureless fingertips.
- Small-area sensors embedded in portable devices may result in less information available from a fingerprint.

REFERENCES

[1] Joao De Barros, Biometric history, August, 2005

[2] E. Spinella, "Biometrics Scanning Technologies: Finger, Facial and Retinal Scanning", SANS Technology Institute, San Francisco, Dec., 2002. 3. D.;

[3] Maio and D. Maltoni, "Direct Gray-Scale Minutiae Detection in Fingerprints", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.19, no.1

[4] Pillay, V.V. Textbook of Forensic Medicine and Toxicology. 15th ed. Hyderabad: Paras Medical Publishers, 2009: 53-94.

[5] Kanchan, T. Chattopadhyay, S. Distribution of Fingerprint Patterns among Medical Students. Journal of Indian Acade-my of Forensic Medicine, 2006; 28(2): 65-68.]

[6] A.K. Jain, P. Flynn, & A.A Ross; Handbook of Biometrics; Springer, Secaucus, NJ, USA, 2007.

[7] Francis Galton, Finger Prints; Macmillan & Co., London, New York, 1892.

[8] D. Maio and D. Maltoni, "Direct Gray-Scale Minutiae Detection in Fingerprints", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.19, no.1, pp. 27-40, 1997.

[9] Francis Galton, Finger Prints; Macmillan & Co., London, New York, 1892

[10] Neil Yager and Adnan Amin; Fingerprint verification based on minutiae features: A review Pattern Analysis and Application, 7:94-113, February 2004

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

[12] 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

[13] P. Reid, "Biometric for Network Security",1st Indian Reprint, Pearson Education, New Delhi, 2004.

[14] A. M. Bazen and S. H. Gerez, "Directional Field Computation for Fingerprints based on the Principal Component Analysis of Local Gradients", Proceedings of 11th Annual Workshopon Circuits, Systems and Signal Processing, Veldhoven, Netherlands, pp. 1-7, November, 2000.

[15] K. Nandakumar and A. K. Jain, "Local Correlation-based Fingerprint Matching", Proceedings of Indian Conference on Computer Vision, Graphics & Image Processing, pp.1-6, Kolkata, December, 2004

[16] A. Cavusoglu and S. Gorgunoglu, "A Robust Correlation based Fingerprint Matching Algorithm for Verification", Journal of Applied Sciences, vol. 7, no. 21, pp. 3286-3291, 2007

[17] Z. Ouyang, J. Feng, F. Su and A. Cai, "Fingerprint Matching with Rotation Descriptor Texture Features", Proceedings of 18th International Conference on Pattern Recognition, Hong Kong, vol. 4, pp. 417-420, Aug., 2006

[18] S Pankati, S.Prabhakar, Jain A.K. "On the indiviaduality of Fingerprints." Pattern Analysis And Machine Intelligence,IEEE Tranactions on 24, no.8(2002) :1010-1025.

[19] Jain A.K., Hong l., Pankati S., Bolle R.,An Identity-authentication system using fingerprints, Proc.IEEE 85(9) pp:1364-1388,1997

[20] Kovacs-Vajna Z.M., A Fingerprint verification system based on triangular matching and dynamic time warping, IEEE Trans. Pattern Anal. Mach. Intel.22(11):1266-1276,2000

[21] Jiang X., Yau W.Y., Fingerprint minutiae matching based on the local and global structures, Proceeding of the International Conference on Pattern Recognition, pp. 1030-1041, 2000