ISSN:0975-9646

Authentication Using Minutiae Based Fingerprint Matching Scheme for Smart Phones

Irene Getzi S
Department of MCA,
Jyoti Nivas College, Bangalore

Abstract— We live in the era of information explosion and the smartphones are changing the way the information are accessed and processed. The Smartphones are used in a wide range of applications and contains vital information regarding personal and business. As more and more security breaches happening all over the world in different forms as a threat to the information industry, the end user should have the protection and privilege of using the information without any doubt in his mind. Hence, the access to data to and from the mobile devices requires secure authentication. Traditional password and PIN number schemes are not adequate to protect the end user from accessing the information as well as it is cumbersome. On other hand, biometric based authentications on are easy to carry out, natural to use, and invulnerable to forgery. The popular biometric used to authenticate a person is fingerprint which is unique and permanent throughout a person's life. In this paper, a method is proposed for secure authentication using minutiae based fingerprint matching scheme.

Keywords—smartphone authentication, fingerprint recognition, minutiae based extraction, biometric *authentication, alignment-based fingerprint matching*

I. INTRODUCTION

The usage of smart phones is increasingly on rise and changing the way the computations are made. Smart phones are personal devices, containing the most sensitive private information such as emails, contact details, documents, and images, financial, business and medical records. Moreover, mobile devices are increasingly used in two-factor authentication schemes in many applications including payment systems. There is a need to employ a strong authentication scheme that can reduce the risk posed by mobile devices, and this paper proposes an approach using finger prints as an effective and convenient tool.

A biometric system uses behavioral or/and physiological data for identifying a person. The behavioral biometric parameters such as signature, gait, speech is not constant and may vary with aging and situation. However physiological characteristics such as face, fingerprint, palm print and iris remains unchanged throughout the life time of a person. As per the prediction by Gartner reports that 30% of companies will use biometrics on mobile devices by 2016 as biometrics not only provides a higher security assurance, but they offer a better experience for the end-user. [8]

The more recent smart phones such as iPhone 5s, ATRIX are built with embedded fingerprint sensors and thus pave the way for authentication using fingerprints. Fingerprint authentication is a highly secure form of biometric authentication since every individual's fingerprints are unique.

Fingerprints are widely used in biometric recognition systems over decades due to its feasibility, distinctiveness, permanence, accuracy, reliability, and acceptability. Fingerprint is a pattern of ridges, furrows and minutiae, which are extracted using sensors. A good quality fingerprint contains 25 to 80 minutiae depending on sensor resolution and finger placement on the sensor. [2]

This paper presents a novel approach for authentication in Smartphones using minutia of fingerprints. The paper is organized as follows. The next section contains the structure of fingerprints, the popular methods used in fingerprints recognition systems and related work using minutia-based extraction. The section 3 analyses the different minutia based schemes which includes several stages such as pre-processing, thinning, and alignment based matching schemes. The next section discusses the results and future enhancements.

II. BACKGROUND STUDY

Fingerprints have been used for centuries for identification purposes. A fingerprint is an individual characteristic and no two fingers have identical ridge characteristics. Finger prints have both global features such as basic ridge patterns, pattern area, delta, type lines, ridge counts that are characterized by human eye. It is possible to have the same global features, but the local features remain unique. Minutiae are the major local features of a fingerprint, which consists of several components such as ridge ending, ridge bifurcation, ridge enclosure, spur, crossover or bridge, delta, core, etc.

Pattern area is the part of the fingerprint that contains all the global features. However, some local features may be found outside the pattern area. Core point is the approximate center of the fingerprint, and is used as the reference point for reading/classifying the print. More specifically it is defined as the topmost point on the innermost upwardly curving ridgeline.

The different techniques of Fingerprint recognition systems are classified broadly into different categories namely:

1) ***Correlation-based matching:*** Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments such as various displacements and rotations. The drawbacks in such systems are fingerprint quality is often too low, thus noise and contrast deficiency can produce false minutiae or hide valid ones.
2) ***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 drawback of this approach is the performance degrades by nonlinear distortions in fingerprint images.
3) ***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. [1].

III. MINUTIAE-BASED MATCHING METHOD

The uniqueness of a fingerprint is exclusively determined by the local ridge characteristics and their relationships. The ridges and valleys in a fingerprint alternate, flowing in a local constant direction. The two most prominent local ridge characteristics are: ridge ending and ridge bifurcation. A ridge ending is defined as the point where a ridge ends abruptly. A ridge bifurcation is defined as the point where a ridge forks or diverges into branch ridges. Collectively, these features are called *minutiae.* Two fingerprints match if their minutiae points match. This approach has been intensively studied, also is the backbone of the current available fingerprint recognition products.

Algorithm:

Step 1: Pre-processing the finger prints to enhance its quality.
Step 2: Binarization of pre-processed fingerprint to highlight the ridges and furrows
Step 3: Thinning of binarized image
Step 4: Extract the Minutiae points
Step 5: Matching of test fingerprint with the template.

A. *Pre-processing*

The fingerprints captured through sensors normally will be of poor quality and may contain noise signals. Pre-processing is done to enhance the quality. The general processing approaches may not be suited due to non-static nature of fingerprints. Hence the popular preprocessing techniques such as histogram equalization, contrast stretching is as first step followed by filtering which will be applied after dividing the image into sub regions.

1) *Histogram Equalization:* Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information. The original histogram of a fingerprint image has the bimodal type the histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced.
2) *Fingerprint Enhancement using Filters:* The image is divided into small processing blocks (e.g. 32 by 32 pixels) and enhanced using filters like Gabor, Gaussian filters or FFT, STFT, wavelet Fourier transform is performed. The enhanced image after the transformation has the improvements to connect some falsely broken points on ridges and to remove some spurious connections between ridges.

B. *Fingerprint Image Binarization*

This process is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. Commonly used approach is to have a global threshold value ‘t’ and assign the pixels which are greater than or equal to ‘t’ to 1; otherwise 0. A locally adaptive binarization method is also used to binarize the fingerprint image. The procedure transforms a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs. [5]

C. *Estimating the Direction*

The fingerprint image is divided into blocks of 16*16 and direction for each block is estimated by gradient value using sobel filters. For each block the certainty value is computed and if it is below a threshold limit can be discarded as background blocks. Then the region of interest is computed deleting the background. [5]

D. *Thinning Process*

The binarized image is thinned to reduce the thickness of all ridge lines to a single pixel width to extract minutiae points effectively. Thinning does not change the location and orientation of minutiae points

compared to original fingerprint which ensures accurate estimation of minutiae points. Morphological operations such as dilation and erosion [2] [5] as well as block filters [2] are used to thin the ridges. The thinned ridges are subjected to morphological operations to remove isolated points and spikes.

E. *Extracting Minutiae*

Extracting the minutia in most of the fingerprint recognition systems is restricted to the two features namely ridge endings and ridge bifurcation. A ridge ending is defined as the point where a ridge ends abruptly. A ridge bifurcation is defined as the point where a ridge forks or diverges into branch ridges. Collectively, these features are called minutiae. A good quality fingerprint typically contains about 40–100 minutiae. For each 3x3 window, if the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is termination point and if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch or bifurcation point.

Extracted minutiae may contain several false ones and are eliminated by comparing the distance between one bifurcation and one termination, the distance between two bifurcations or two terminations with the average inter-ridge width representing the average distance between two parallel neighbouring ridges.

F. Matching the Minutiae with Template

The extracted minutia can then be compared with the template already stored in the mobile device. The finger prints can be matched only when both are recorded in the same direction and angle. If not an alignment step is performed taking one minutia from same reference point from both the image; a similarity check is done and if the correlated value is greater than the threshold, each set of minutia is transformed to a new coordination system by applying translation and rotation for all other minutia with respect to the reference minutia.

After we get two set of transformed minutia points, the elastic match algorithm is used to count the matched minutia pairs by assuming two minutia having nearly the same position and direction are identical. Elastically matching the minutia is achieved by placing a bounding box around each template minutia. If the minutia to be matched is within the rectangle box and the direction discrepancy between them is very small, then the two minutiae are regarded as a matched minutia pair. Each minutia in the template image either has no matched minutia or has only one corresponding minutia. The final match ratio for two fingerprints is the number of total matched pair over the number of minutia of the template fingerprint. [1]

Other methods used in the matching process includes, using 17-D feature vector and analysis using vector machines[5], SIFT based matching schemes[6], using phase spectral analysis[3], using fuzzy neural networks(FRFNN) and minutia score matching methods.[2].

IV. RESULTS AND DISCUSSIONS

The algorithm using binarization and alignment-based matching [2] is tested in the *Intel core i5* machine and giving the promising results. Since recent mobile devices are coming with good processing capabilities, implementing the algorithm in the smart devices is feasible. However, the following improvements can be considered. The alignment and matching stage can be optimized since the algorithm involves large computations. Instead of extracting all the minutia points, partial extraction [5] can be applied by considering minutiae originating from the core point. In future the proposed method will be implemented with the enhancements suggested in the mobile devices.

V. CONCLUSIONS

Smartphones are coming up with enormous processing capabilities and storage capacities and are being used for wide range of applications and contains personal and confidential data. If a mobile device falls into the wrong hands, it's possible that sensitive information and data could be compromised. Since recent mobile devices are coming up with fingerprint scanning technology, fingerprint based authentication provides a natural and convenient technique. This paper presented minutiae based fingerprint authentication scheme which gives promising results and well tested in other environments.

REFERENCES

[1] Parul Mishra, Ajit Kumar Shrivastava, Amit Saxena, *Enhanced Thinning Based Finger Print Recognition*, International Journal on Cybernetics & Informatics (IJCI) Vol.2, No.2, April 2013.

[2] Ravi J, K. B. Raja, Venugopal K. R, *Fingerprint Recognition Using Minutia Score Matching*, International Journal of Engineering Science and Technology, Vol.1 (2), 2009, 35-42.

[3] Natasha Singh et al., *Fingerprint Recognition and Identification by Minutiae Detection and Phase Spectrum Analysis Algorithm*, International Journal of Software and Web Sciences 4(2), March-May, 2013, pp. 109-115.

[4] Jianjiang Feng, *Combining minutiae descriptors for fingerprint matching, Elsevier*, Pattern Recognition 41 (2008) 342 – 352.

[5] Tsai-Yang Jea, Venu Govindaraju, *A Minutia-Based Partial Fingerprint Recognition System*, Elsevier, Pattern Recognition 38 (2005) 1672 – 1684.

[6] Ru Zhou, Dexing Zhong, and Jiuqiang Han, Fingerprint Identification Using SIFT-Based Minutia Descriptors and Improved All Descriptor-Pair Matching, Sensors 2013, 13, 3142-3156; doi:10.3390/ s130303142

[7] V. Vijaya Kumari and N. Suriyanarayanan, "*Performance Measure of Local Operators in Fingerprint Detection"*, Academic Open Internet Journal, vol. 23, pp. 1-7, (2008).

[8] (2014) Zdnet website [Online]. http://www.zdnet.com/30-percent-of-companies-will-use-biometric-identification-by-2016-7000025942/ by Larry Barrett, February, 2014.