Grenze International Journal of Computer Theory and Engineering , June 2016

Performance Evaluation of the Automatic Fingerprint Recognition System

Shabir Ahmad Sofi[1], Sabah Bashir[2], Haseeb Asif[3] and Roohie Naaz[4]
[1-4]NIT Srinagar, J&K, India
Email: shabir@nitsri.net

***Abstract*—The biometric characteristics that are used in the authentication system are unique for each person. The major advantage of the biometrics is that you have always with your way to authenticate yourself. Furthermore biometrics make it possible to know who is authenticated and where. Fingerprint is taken as proffered technique for the biometric authentication because of the public acceptability, ease of use, economy of scale, easy installation and availability. There are two approaches to fingerprint recognition minutia base and image based but in this paper we limit to the minutia based recognition. In this paper we evaluate the minutia as per three stage approach and given the performance evaluation especially for the false minutia and the fingerprint classifiers. The estimation of the previously used scheme and the new scheme is analysed and the results were appreciating.**

***Index Terms*— Fingerprint, authentication, recognition, biometric, minutia, ridge, primary grouping ratio, false minutiae.**

I. INTRODUCTION

To restrict illegal access into systems and emphasis a very effective technique for that can be biometric authentication. The techniques of great importance against less detectable passive attacks as it is not based on some memory based password system that can be cracked but rely on human gestures, behavior and physical characteristics unique to each person. Biometrics techniques can be divided in two main sets: physiological or behavioral. A physiological biometric method is something that is physical, and that belongs to you. The behavioral biometric consists in something that you do in your everyday life. Physiological biometric technique includes Fingerprint Recognition, Eyes, Face recognition, Voice Recognition, DNA, etc. Behavioral biometric technique includes Signature, Keystrokes etc.

The Biometric authentication has several advantages. First, the biometrics authenticates only people. It cannot authenticate computer as the classical authentication methods which are based on IP address or public key. The biometric characteristics that are used in authentication systems are unique for each person. The major advantage of the biometrics is that you have always with you your way to authenticate yourself. For example, you can forget a password or lost an access card. It is impossible to forget your fingerprint, your gait, your signature. Furthermore biometric makes possible to know exactly who has been authenticated and where. A password or an access card can have been borrowed by someone. With a biometric authentication system, it cannot happen. There are a lot of interesting advantages but also some drawbacks to the biometric authentication.

Grenze ID: 01.GIJCTE.2.2.23

II. RELATED WORK

A. Fingerprint Recognition

The fingerprint is taken as the preferred technique for biometric recognition because:
1) Wide public acceptability as against iris or retinal scan. 2) Ease of use 3) economy of scale
4) Easy installation and availability with high accuracy
Our method focuses on restricting entry into a system on basis of biometric characteristics of an individual, or more specifically, based on individual's fingerprints. To capture the fingerprints, current techniques employ *optical sensors* that use a CCD or CMOS image sensor; solid state sensors that work on the transducer technology using capacitive, thermal, electric field or piezoelectric sensors; or ultrasound sensors that work on echography in which the sensor sends acoustic signals through the transmitter toward the finger and captures the echo signals with the receiver. Fingerprint scanning is very stable and reliable. It secures entry devices for building door locks and computer network access is becoming more common. Recently a number of banks have begun using fingerprint readers for authorization at ATMs.
The three basic techniques for finger print authentication are:

1. Minutiae based matching stores minutiae as a set of points in a plane and the points are matched in the template and the input minutiae.
2. Correlation based matching superimposes two fingerprint images and correlation between corresponding pixels is computed.
3. Ridge feature based matching is an advanced method that captures ridges Finger print comprises of ridges and valleys. The ridges are the dark area of the fingerprint. The ridges form so-called minutia points: ridge endings (where a ridge end) and ridge bifurcations (where a ridge splits in two). In this, the overall characteristics of the fingerprints (minutia points, ridge thickness, curvature, or density) are compared with the registered template. The fingerprints of individuals are unique, even for twins. The main technologies used to capture the fingerprint image with sufficient detail are optical, silicon, and ultrasound.

A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy was very high [3]. Patterns have been extracted by creating an inked impression of the fingertip on paper. Today, compact sensors provide digital images of these patterns. Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse. Since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners. Solid state sensors overcome this and other technical difficulties because the coated silicon chip itself is the sensor. Solid state devices use electrical capacitance to sense the ridges of the fingerprint and create a compact digital image. In real-time verification systems, images acquired by sensors are used by the feature extraction module to compute the feature values. The feature values typically correspond to the position and orientation of certain critical points known as minutiae points [4]. The matching process involves comparing the two-dimensional minutiae patterns extracted from the user's print with those in the template. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources.
The fingerprint recognition problem can be grouped into two sub-domains: one is fingerprint verification and the other is fingerprint identification. As shown in fig. 1 automatic the fingerprint recognition system (AFRS). The fingerprint recognition system constitutes of fingerprint acquiring device, minutia extractor and minutia matcher. The testing database in the paper is from the available fingerprints provided by Fingerprint Verification Competition 2002 (FVC2002). So no acquisition stage is implemented.
There are two approaches for fingerprint recognition, first approach is minutia based, represents the fingerprint by its local features, like termination and bifurcations. The second approach, which uses image-based methods [6][7], tries to do matching on the global features of a whole fingerprint image. To implement a minutia extractor, a three-stage approach is widely by researchers which include preprocessing, minutia extractor and post processing stage. In preprocessing stage Histogram equalization and Fourier Transform do the image enhancement [9], and then the fingerprint image is binarized using locally adaptive threshold method [12]. The image segmentation is fulfilled by a three step approach which includes block direction estimation, segmentation by direction intensity [4] and region of interest extraction by Morphological operations.

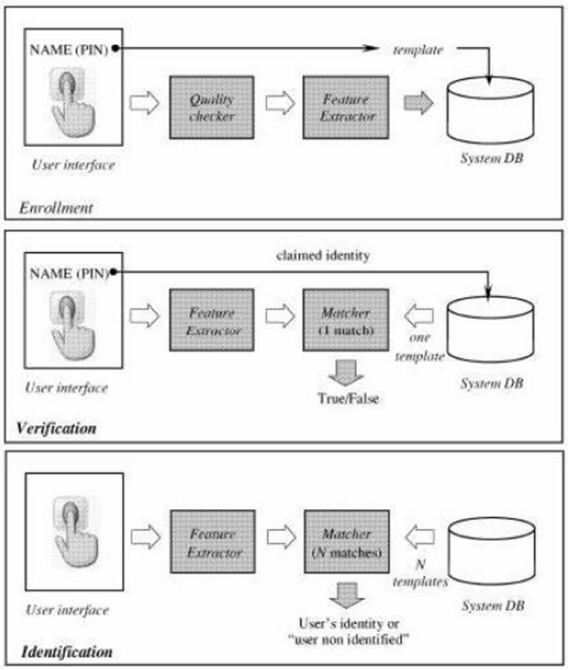

Figure 1: Fingerprint Recognition System

For minutia extraction stage, three thinning algorithms [12][2] are tested and the morphological thinning operation is finally bid out with high efficiency and pretty good thinning quality. A more rigorous algorithm is developed for the post processing stage so as to remove false minutia. A novel representation for bifurcation is proposed to unify testimonials and bifurcations [12][1]. The minutia matcher chooses any two minutias as reference minutia pair and matches their associated ridges. If the ridges match well [1], two fingerprint images are aligned and matching is conducted for all remaining minutia.

III. Performance Analysis of Previous and New Scheme for Removing False Minutiae Minutia Post Processing

The preprocessing stage does not totally heal the fingerprint image. Actually all the earlier stages themselves occasionally introduce some artifacts which later lead to spurious minutia. This false minutia will significantly affect the accuracy of matching if they are simply regarded as genuine minutia. So some mechanisms of removing false minutia are essential to keep the fingerprint verification system effective. The different types of false minutia are specified in following diagrams:

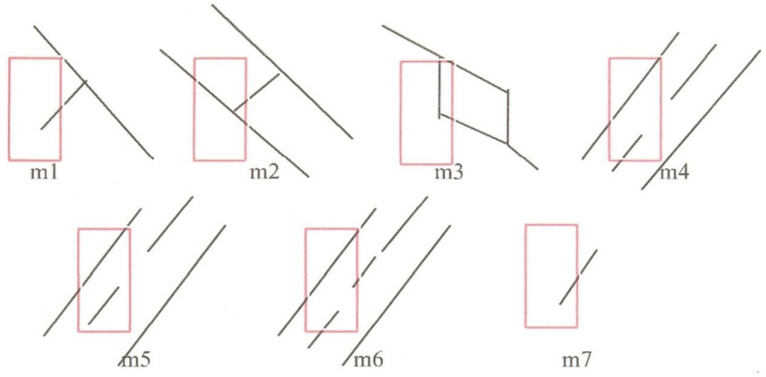

Fig. 2 False Minutiae

As shown in fig. 2 m1 is a spike piercing into a valley. In the m2 case a spike falsely connect two ridges. M3 has two near bifurcations located in the same ridge. The two ridge broken points in the m4 case have nearly the same orientation and a short distance. M5 is alike the m4 case with the exception that one part of the broken ridge is so short that another termination is generated. M6 extends the m4 case but with the extra property that a third ridge is found in the middle of the two parts of the broken ridge. M7 has only one short ridge found in the threshold window.
In case m1, m4, m5 and m6 [9][2] have not false minutia removal by assuming the image quality fairly good and has not systematic healing method to remove those spurious minutia.
We propose the following procedures in removing false minutia:

1. If the distance between one bifurcation and one termination is less than D and the two minutias are in the same ridge (m1 case), remove both of them. D is the average inter ridge width representing the average distance between two parallel neighboring ridges.
2. If the distance between two bifurcations is less than D and they are on the same ridge, remove the two bifurcations (m2, m3 cases).
3. If two terminations are within a distance D and their directions are coincident with a small angle variation and they suffice the condition that not 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 (cases m4, m5, m6).
4. If two terminations are located in a short ridge with length less than D, remove the two terminations (m7).

The proposed procedures has two advantages in removing false minutia, 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 and the second advantage is that the order of removal procedures is well considered to reduce the computational complexity. It surpasses the way adopted which does not utilize the relation among the false minutia types. For example, the procedure 3 solves the m4, m5 and m6 cases in a single check routine and after the procedure 3, the number of false minutia satisfying the m7 case is significantly reduced.

IV. Unify Terminations and Bifurcations

Unification representation for both termination and bifurcation is used because of the acquisition condition during the fingerprint record. Each minutia is completely characterized by x-coordinate, y-coordinate and orientation.
The orientation calculation for a bifurcation needs to be specially considered. All the three ridges deriving from the bifurcation point have their own directions [9][13].

V. Matching Stage

The matching algorithm for the minutia needs to be elastic since the strict match requiring that all parameters (x, y, θ) are the same for two identical minutia is impossible due to the slight deformations and inexact quantization of minutia. The elastically match minutia is achieved by placing a bounding box around each template minutia. If the minutia to be matched is within the rectangular box and the direction discrepancy between them is very small, then the two minutia 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 minutia of the template fingerprint. The score is 100 x ratio and ranges from 0 to 100. If the score is larger than a pre-specified threshold, the two fingerprints are from the same finger. However the elastic match algorithm has large computation complexity and is vulnerable to spurious minutia.

VI. Efficient Minutia Matching

If fingerprint templates are stored in a particular manner then it will increase the efficiency of biometric device e.g. in Henry Classification System which allows for logical categorization of ten-print fingerprint records into primary groupings based on fingerprint pattern types. This system reduces the effort necessary to search large numbers of fingerprint records by classifying according to gross physiological characteristics. Henry classification assigns each finger a number according to the order it is located in the hand, beginning

with the right thumb as number 1 and ending with left little finger as 10 The system also assigns a numerical value to fingers that contain a value 16, fingers 3 and 4 have value of 8, and so on, with the final two fingers having a value of 1. Fingers with non-whorl pattern, such as arch or loop pattern, have a value of zero. According to Henry Classification system, finger number and finger values are assigned by calculating the ratio of one plus the sum of the values of the whorl-patterned, even-numbered fingers, divided by one plus the sum of the values of the whorl-patterned, odd numbered fingers.
PGR=1 + (Sum of whorled, EVEN finger value) 1 + (Sum of whorled, ODD finger value), where PGR=Primary Grouping Ratio
Problem with existing system:
Above method work very efficiently when we have plan prints of all fingers of both hands. We assign weights to the person prints and calculate PGR. On the basis of PGR factor the search goes to particular domain and identified the proper match. But if we have only one fingerprint as input print, then there will be problem as in this case we can't find PGR factor.

VII. Performance Evaluation of Previous Approach and Proposed One for Fingerprint Classification

Proposed work is based on the theory of fingerprint classification, we store only single fingerprint of person in the database. This single print can be thumb print or print of index finger. One obvious advantage of this approach is that it will considerably reduce the amount of memory required to store the fingerprint template as only one print is stored instead of 10 prints for an individual.

VIII. Working

Enrollment process: during the enrollment process, sensor senses the fingerprint, then next step is feature extraction, here minutiae points are extracted. After this step we put a classifier to check the classification of input template that whether it is left-loop, right-loop, arch or whorl. After classification the input template will be stored in particular domain. A domain is the database contains the templates of same classification. Normally the fingerprints are classified as whorl, arch and loop. Loops make up nearly 65% of all fingerprints, whorls are nearly 30% and perhaps 5% are arches. These classifications are relevant in many large scale forensic applications, but are rarely used in biometric authentication.
Verification process: Here the fingerprint or the finger is placed on a sensor and then its features are extracted and a final template is generated for matching. Now this template will not be matched with every template in the database rather it extracts its classified domain out of 4-domain and will perform match from this extracted domain. This process, no doubt will be fast and more efficient especially when the stored database is very large, more than 1,00000 templates. Let D and T be the representation of the Database Template and Stored Template respectively. Each minutia may be described by a number of attributes, including its location in the fingerprint image, orientation, type etc. Most common minutiae matching algorithms consider each minutiae as triplet m = {x, y, --) that indicates the minutiae location coordinates and the minutiae angle.
D = {m1, m2, ……mn} mi = {xi, yi, _i} I = 1……m
T = {m'1, m'2, ……..m'n} mj = {x'j, y'j, _'j} j = 1…..n
Where m and n denotes the number of minutiae in D and T respectively.
Database template and the Stored template will be matched, if we calculate Spatial Distance (SD) and direction difference (DD) that will not be below than specified value r0 and _0 or we can write as:
SD (m'1, m1) = sqrt [(xí-xi)2 + (yí-yi)2] >=r0 ---------- (1)
Similarly
DD (m'1, m1) >= 0 ---------- (2)

IX. Fingerprint Classifier

It classifies the input fingerprint into four major categories namely Left-Loop, Right-Loop, Whorl and Arch. The proposed classifiers works on the basis of singular point (Delta) extracted. If there are two deltas then it will be counted as whorl or twin loop. If there is no delta then it will be counted as arch. If only one delta is there then it will be either left loop or right loop. We further find the category of loop by measuring relative position ®. If relative position, R of delta with respect to symmetry axis is R = 1 means the delta is on the right side of symmetry axis then it will be left loop otherwise it will be right loop.

Performance estimation of the propose scheme:
Let the database has more than 1,50,000 templates stored in it. Let us input a single template at the sensor and started to identify it from their database. It takes 25-30 minutes to identify and also gives 34 matched templates. These 34 templates have to be matched and it consumes around 5-6 hours being quite complex.
Performance of the existing system: For the best case the template is first match and the time required = 1 x 1 = 1ms
For worst case i.e. the template is last match, Time required = 1 x 50,000 = 150seconds = 2.5 minutes.
For an average case, time required = approximately 1-2 minutes.
Performance of proposed system: For the best case i.e. the template is first match, time required = 1 x 1 = 1ms
For the worst case we assume 1,50,000 templates and according to the classification there will be 45,000 whorls (30%) + 48,000 Left loop (32%) + 49,500 Right Loop (33%) + 7,500 Arch (5%0 at first stage we get the classification and accordingly particular domain will be extracted . The time taken by each classification is as under:
For whorl = 1ms x 45,000 = 45 seconds
For Left Loop = 1ms x 48,000 = 48 seconds
For Right loop = 1ms x 49500 = 49.5 seconds
For Arch = 1ms x 7,500 = 7.5 seconds
Average time = 150/4 = 37.4 seconds
That is for an average case the time required is approximately 20-24 seconds

X. CONCLUSIONS

1. The proposed procedures has two advantages in removing false minutia, 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 and the second advantage is that the order of removal procedures is well considered to reduce the computational complexity. It surpasses the way adopted which does not utilize the relation among the false minutia types.
2. Performance factor = Time taken in worst case of existing system/Proposed system, that is the proposed system is four times better than the existing one.

The proposed procedures and the performance factor evaluation needs more experimentation with different databases which can be taken care as the futuristic work.

REFERENCES

[1] Lin Hong, “Automatic Personal Identification Using Fingerprints”, Ph.D. Thesis, 1998.
[2] D. Maio and D. Maltoni, “Direct Gray-scale Minutiae Detection in Fingerprints”, IEEE Trans. Pattern anal. And Machine Intell, 19(1), pp.27-40, 1997.
[3] Jain, A.K., Hong, L., and Bolle, R. (1997), “On-Line Fingerprint Verification”, IEEE Trans. On Pattern anal. And Machine Intell, 19(4), pp. 302-314.
[4] N. Ratha, S. Chen and A.K. Jain, “Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images”, Pattern Recognition, Vol. 28, pp.1657-1672, November 1995.
[5] Alessandro Farina, Zsolt M.Kovacs-Vajina, Alberto leone, Fingerprint Minutiae Extraction from Skeltonised Binary Images, Pattern Recognition, Vol. 32, no.4, pp.877-889,1999.
[6] Lee, C.J., and Wang, S.D.: Fingerprint Feature Extraction using Gabor Filters, Electron. Lett. 1999, 35(4),pp.288-290.
[7] M.Tico, P. Kuosmanen and J. Saarinen, Wavelet Domain Features for Fingerprint Recognition, Electroni. Lett., 2001, 37(1), pp.21-22.
[8] L. Hong, Y.Wan and A.K. Jain, “Fingerprint Image Enhancement: Algorithms and Performance Evaluation”, IEEE Transactions on PAMI, Vol. 20, No. 8, pp. 777-789, August 1998.
[9] Image Systems Engineering Program, Stanford University. Student Project by ThomasYeo,WeePengTay,YingYuTai. http://ise0.stanford.edu/class/ee368a_proj01/dropbox/project22/finger/
[10] FVC2000. http://bias.csr.unibo.it/fvc2000/
[11] FVC2002. http://bias.csr.unibo.it/fvc2002/
[12] L.C.Jain, U.Halici, I. Hayashi, S.B.Lee and S. Tsutsui. Intelligent Biometric Techniques in Fingerprint and Face Recognition. 1999, the CRC Press.
[13] M.J. Donahue and S.I. Rokhlin, “On the Use of Level Curves in Image Analysis,” Image Understanding, Vol. 57, pp. 652-655, 1992.