A Novel Algorithm for Fingerprint Identification using Ellipse Method

Asha M. J.
Department of Computer Science and Engineering
Rajagiri School of Science and Technology
Ernakulam, India
Email: ashamjoseph@gmail.com

***Abstract*—The purpose of developing a biometric identification system is to identify an individual quickly and accurately based on his physiological or behavioral characteristics. The system should ensure that only a person, whose biometric data is there in the database, is accepted. In order to satisfy these requirements, the system should give a false acceptance rate (FAR) approximately equal to zero and the speed of performing the identification should be very high. This paper proposes a fingerprint identification algorithm which gives a very low false acceptance rate with a very improved speed compared to other existing algorithms.**

I. Introduction

Systems used for high security applications need very accurate algorithms for person identification. Traditional methods like username and password are not reliable enough for high security electronic applications. Even though the biometric systems cannot give an absolute yes or no answer like the traditional methods, the former will give results with very high level of accuracy. According to the application requirements, a biometric system can be in verification or in identification mode In verification mode a person's biometric data is compared in a one-one manner with his/her data in the database for a match. This helps in positive recognition to ensure that a person's claim is correct and he is the intended user. In identification mode a one to many comparison of a person's data with all the available data in the database is made. This can be used for both positive as well as negative recognition to ensure that the person's details are there in the database. Earlier days biometric identification were used only for forensic applications, but now it is being used for several other civilian applications.

Biometric identification using fingerprints are in use for centuries and are the most popular method in use today. Fingerprints are the patterns of ridges present in human fingers. Fingerprint identification is done by studying the pattern of these ridges. During identification the discontinuities called minutiae are detected and these values are compared with already stored values in the template.

For fingerprint identification the algorithms available today do not satisfy the performance requirements for electronic transactions. Most of the algorithms in literature fail to satisfy the speed performance ratio needed for online fingerprint identification. Proposed is a fingerprint identification algorithm which gives a very low False Acceptance rate with an improved processing speed.

A. Literature Survey

Identification systems used for high security applications require a very accurate person identification. An ideal identification system should give an FAR of zero. For developing a biometric identification system, the issue that should be considered first is the choice of a human characteristic as a biometric. According to Jain et al [2], for a human characteristic to be a biometric characteristic it should have the following qualities:

- Universality, the characteristic should be present in all the users.
- Distinctiveness, the characteristics should vary in all the users.
- Permanence, the characteristics should be stable for a length of time.
- Measurability, the characteristic should be collectable.

Some other issues that need to be considered when developing a practical biometric system are:

- Performance is the attainable accuracy and speed and the resources required for this.
- Approval refers to the willingness of the users to accept it in their daily lives.
- Circumvention shows how easily the system can be fooled.

According to Jain et al [2], the main modules of a biometric system are:

- Sensor module is responsible for capturing a biometric trait using sensors.
- Feature extraction module is responsible for extracting the required features from the biometric data collected by sensor module
- Matcher module compares the output of feature extraction module with the data stored in the database and a matching score is generated.
- In System database module, biometric traits of the users is enrolled into the database during enrollment stage. Then the templates of enrolled users are extracted from database to get the matching score in matching module.

A number of biometric systems using DNA, ear, fingerprint, face, voice, gait etc. are in use today. DNA based biometric identification is a very complex and time consuming process which makes it unsuitable for online applications. Ear based biometric system [6] is not suitable for most of the online applications due to lesser accuracy and acceptability. Face when taken as the biometric suffers from variations due to illumination, pose, expression, occlusion and plastic surgery. It also suffers accuracy problems due to spectacles, head angle, hair and expression [8]. Gait is an input intensive and computationally expensive behavioral biometric [2]. Palm print based biometric suffers from problems due to damage of hand and non universality. Also the devices for capturing the palm print are very expensive. Hand geometry based biometric is not very distinctive and cannot be scalable to a very large population.

Accuracy of fingerprint verification is very high [9]. Nowadays embedding fingerprint based biometric in computer systems used for various applications have become affordable. Accuracy of currently available fingerprint recognition systems are suitable for verification systems and small or medium scale identification systems. But for identification systems involving millions of users, the currently available systems are not at all good enough [2]. Currently available identification systems take a large number of computational resources. Jain et al [2] says that if a biometric with FMR of 0.1% is used for identification in an airport security system, then if there are 200000 people then the system will give 200 false alarms. This situation is highly undesirable.

Fingerprint recognition algorithms available in literature generally have two stages, reference point location and fingerprint classification. Reference point location algorithms either detect a single reference point or two reference points. A single reference point detection method is given in Basha et al [7] which first finds one reference point (core) then all the minutiae of the fingerprint image is identified using crossing number method. After collecting the minutiae they are aligned around the core point in a circular manner and then only a predetermined number of minutiae are extracted for matching.

Jain et al in their paper [3] uses a segmentation algorithm based on the local variance of gray level to locate the ROI. The algorithm using summation method detects two discontinuities in the ridge (the ridge bifurcation and ridge ending).For matching Jain et al uses an alignment based method. Maio and Maltoni in their paper [10] extract minutiae from gray scale image using ridge line following method. This method follows the ridges and thus finds two discontinuities; the ridge ending and bifurcation. This approach even though accurate has a lot of conceptual complexity. Conti et al [7] uses an algorithm to detect the number of core and delta points in a fingerprint and to determine the fingerprint class.

The proposed algorithm is a modification of conti et al [7]. The algorithm proposed in this paper finds the two reference points; core and delta, classifies the image and then checks for minutiae around the reference points using Ellipse method.

1) Proposed Fingerprint Identification System: The fingerprint detection system consists of two stages fingerprint enrolment and identification. Fingerprint identification algorithm proposed in this paper consist of four steps; Fingerprint Enhancement, Reference Point location and classification, Minutiae Extraction and matching. The image is first preprocessed, then singularity points are extracted and in the matching stage a matching score is generated using the hamming distance. This approach requires lesser execution time since small number of minutiae only need to be analyzed. A detailed description of each stage is given below.

B. Fingerprint enrolment

In the enrolment phase first the image is enhanced to improve the image quality. Enhancement process increases the accuracy of feature extraction. From the enhanced image, the fingerprint class and minutiae information is extracted and stored in the database.

C. Image Enhancement

Before reference point location, image is enhanced to improve the image quality. According to [4] digital fingerprint image has regions of three categories, region which is well defined, corrupted but recoverable and unrecoverable. The task of enhancement algorithm is to improve the quality of first two regions and remove the third type of region.

1) Normalization: In the image enhancement [4] process, input image is first converted to gray-level image (if it is not a gray-level image), the gray-level image I is a $P \times Q$ matrix, in which (i, j) is the intensity of the pixel at the i^th row and j^th column. The mean and variance of I are calculated using equations (1) and (2)

$$M(I) = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} I(i,j) \tag{1}$$

$$VAR(I) = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (I(i,j) - M(I))^2 \tag{2}$$

The image is normalized as in equation (3)

$$N(i,j) = \left\{ \begin{array}{ll} M_0 + \sqrt{\frac{VAR_0(I(i,j)-M)^2}{VAR}} & if I(i,j) > M, \\ M_0 - \sqrt{\frac{VAR_0(I(i,j)-M)^2}{VAR}} & otherwise \end{array} \right\} \tag{3}$$

In the equation, required mean and variance are given by M_0 and VAR_0. In order to help in the subsequent processing steps, the clarity of ridge and valley structure needs to be improved. Normalization is applied to each pixel (i, j) in order to reduce the variations in grey level values.

2) Orientation Estimation: Next step in the enhancement is to find the orientation of the image. Orientation of a $P \times Q$ image is the ridge orientation of a block in an image. Here an image is divided into blocks and for each block orientation is estimated.

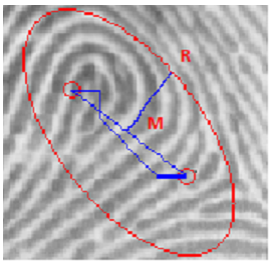

Fig. 1. EllipseMethod

In order to find the orientation [5] Image is first divided into $w \times w(16 \times 16)$ sized blocks. Then gradient$G_x(i,j) and G_y(i,j)$ are calculated at each pixel (i,j). Orientation of blocks with centre at pixel (i,j) is calculated using the formula given by Yang et al[5].

D. Reference Point Location, classification and minutiae extraction using Ellipse Method

For finding the reference point many methods are available in literature the Poincare index based method suggested by Kawagoe and Tojo [6] is the more accurate method. In the method, a Poincare index of 180^0, -180^0 and 360^0 corresponds to core, delta and double core respectively.

The number of core points and delta points will be different for different classes of fingerprints. An arch fingerprint has no core or delta points. There is only one core point for tended arch fingerprint. The left loop fingerprint and right loop has one core and one delta. There are two core and two delta points for a whorl fingerprint. For classifying the fingerprint the method used is directional map method [7]. Here the angle calculated is the angle between direction segment and horizontal axis. Angular variation is very high in the path connecting core and delta. In order to make all directions in the range $[-\frac{\pi}{2}, \frac{\pi}{2}]$ each angle greater than $\frac{\pi}{2}$ is set to $angle-\pi$. the resultant matrix is the directional map. For each element (i,j), the difference between (i,j), and its 8 neighbours is calculated. Then the maximum of these differences will give the point with highest angular difference.

$$maxangle(i,j) = max(angle(i,j) - kneighbour(i,j)), \quad k = 1,2,...,8. \quad (4)$$

The maximum angular difference points show a path from core point to delta point. In low quality images having only one core point the reference points can be approximated by following the path. Next step in the reference point location is to find the class of the finger print.

Fingerprint belongs to Left loop, Right loop, and Tended arch class if it satisfies the equations (5), (6) and (7) respectively. Where β is the angle that core-delta line makes.

$$abs(\beta - R_{angle}) > abs(\beta - L_{angle}) \quad abs(\beta - M_{angle}) > toleranceangle \quad (5)$$

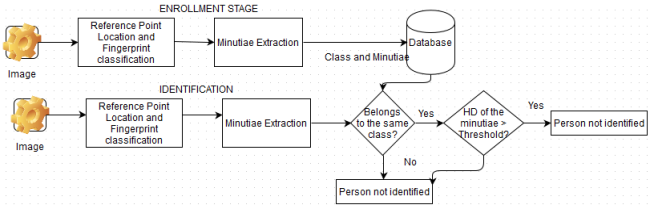

Fig. 2. ProposedSystem

$$abs(\beta - R_{angle}) < abs(\beta - L_{angle}) \quad abs(\beta - M_{angle}) > toleranceangle \quad (6)$$

$$abs(\beta - R_{angle}) < abs(\beta - L_{angle}) \quad abs(\beta - M_{angle}) < toleranceangle \quad (7)$$

If two core points are detected then it is a whorl fingerprint and if there are no core points then it is an arch fingerprint.

E. Minutiae Extraction

After finding the core and delta points, a line is drawn joining the two then the midpoint M of the core-delta line is found. Using the coordinates of M as centre, coordinates of core and delta as two foci an ellipse is drawn. The area of the ellipse can be taken as the needed ROI for minutiae extraction process as given in fig. 1. The ROI is then given for binarizing, Filtering and Thinning before extracting the minutiae. From the thinned region, using CN method [8] the minutiae can be extracted. After calculating the CN of each ridge pixel it can be classified into four types of minutiae.

- Ridge Ending, where the ridges end
- Bifurcation, where two ridges join
- Cross over, where two ridges crosses each other
- Islands, these are the isolated points

A ridge with a CN of zero correspond to an Island, a CN of 1 shows it is a ridge ending, 3 correspond to bifurcation and 4 correspond to cross over. For each minutiae extracted, its x and y coordinates, Orientation and its type are stored in the template.

F. Matching

For matching the features extracted, to the values in the database a serial mode of operation can be used. Matching is done in two stages. The finger print is checked in the first stage to find whether it belongs to the same class as the stored template. If the fingerprint belongs to the same class, then proceed to the next stage and match each minutia with the stored template using hamming distance (HD). If the matching score is below the threshold a match is found.

II. Experimental Results

The proposed biometric system using Ellipse Method provides a very good method for feature extraction. The algorithm consists of four steps, a fingerprint enhancement, reference point location, minutiae extraction and then a matching stage. First step in fingerprint reference point location is fingerprint

TABLE I
PROCESSING TIME COMPARISON

Algorithm using 16 minutiae matching around core point	8.0653
Proposed Ellipse Method	6.45224

enhancement. Enhancement can be done in both gray level image and in binary image. Here it is done in gray level image in order to reduce the loose of information. Gray level image is then normalized, checked the reliability and the output image is then given for finding the orientation. From the orientation estimation, the core and delta points are located using Poincare index method. A line is drawn from core to delta using the Direction map method and fingerprint classification is done. Second step is minutiae extraction. For that fist an ellipse is drawn with core and delta as foci. This ellipse is the needed ROI for minutiae extraction. The fingerprint classification information and the extracted minutiae information are stored in a database as template during enrollment. During Identification process, extracted information is compared with all the templates in the database to find a match.

In order to evaluate the proposed algorithm, fingerprint samples from [9] are used. Only those minutiae inside the elliptical region are taken for consideration. This increases the speed of processing than an algorithm based only on minutiae [8]. Since ridge ending, bifurcation, cross over and islands are detected there is a significant reduction in the FAR than that of [8]. The processing time of the minutiae extraction process is directly proportional to the image size. As the number of minutiae is increased there will be very high increase in processing time. As given in basha et al[8] if the number of minutiae is decreased from 18 to 6 the there will be 20% reduction in processing time. In [7] it takes only the count of reference point and the class of finger for identification. The accuracy of which can be improved by detecting the minutiae around these reference points. Also in this paper a serial mode of matching is used which helps to reduce the processing time even further

III. CONCLUSION AND FUTURE WORK

Proposed fingerprint identification algorithm gives a good method for fingerprint identification with a very low execution time compared to existing algorithms.This reduction is the execution time makes the algorithm suitable for online systems. The FAR is reduced to approximately zero using the proposed algorithm which makes it suitable for high security applications.

The proposed system has some disadvantages like if the data acquired is very noisy then the proposed algorithm fails to accept a genuine person. Also if the fingerprint data acquired from a user during enrollment phase change due to some unexpected reasons then also the proposed system may fail. Another problem with the proposed unimodal system is that there is a chance for a subset of users to not to possess the particular biometric trait.

The limitations of using a single biometric trait can be overcome by using a multiple biometrics. Such systems are known as multimodal biometric systems. As stated in [2] multimodal biometric system solves the problem of nonuniversality, as multiple biometric systems cover almost all the population. Also it will be difficult for an intruder to fool both the biometrics at a time. Future expansions that can be suggested to solve the problems of using a single biometric data are

- Use a fusion of fingerprint and iris features.
- Consider a limited number of meaningful descriptors for fingerprint and iris which can be fused at feature extraction level itself to improve the accuracy of the system.

REFERENCES

[1] Jain, Anil K and Hong, Lin and Pankanti, Sharath and Bolle, Ruud, *An identity-authentication system using fingerprints*, Proceedings of the IEEE 85, no. 9 (1997): 1365-1388.

[2] Jain, Anil K. and Ross, Arun and Prabhakar, Salil *An introduction to biometric recognition*, Circuits and Systems for Video Technology, IEEE Transactions on 14, no. 1 (2004): 4-20.

[3] Jain, Anil and Hong, Lin and Bolle, Ruud *On-line fingerprint verification*, Pattern Analysis and Machine Intelligence, IEEE Transactions on,19, no. 4 (1997): 302-314.

[4] Hong, Lin and Wan, Yifei and Jain, Anil *Fingerprint image enhancement: algorithm and performance evaluation*, Pattern Analysis and Machine Intelligence, IEEE Transactions on,20, no. 8 (1998): 777-789.

[5] Yang, Jianwei and Liu, Lifeng and Jiang, Tianzi *Improved method for extraction of fingerprint features*, Second International Conference on Image and Graphics, pp. 552-558. International Society for Optics and Photonics, 2002.

[6] Kawagoe, Masahiro and Tojo, Akio *Fingerprint pattern classification*, Second Pattern Recognition 17, no. 3 (1984): 295-303.

[7] Conti, Vincenzo and Militello, Carmelo and Sorbello, Filippo and Vitabile, Salvatore *A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems*, Second Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on 40, no. 4 (2010): 384-395.

[8] Basha, A Jameer and Palanisamy, V and Purusothaman, T *Efficient Multimodal Biometric Authentication Using Fast Fingerprint Verification and Enhanced Iris Features*, Second Journal of Computer Science 7, no. 5 (2011): 698-706.

[9] *Fingerprint Verification Competition FVC2002*, [Online]. Available: http://bias.csr.unibo.it/fvc2002/(2009, Nov.).

[10] Maio, Dario, and Davide Maltoni *Direct gray-scale minutiae detection in fingerprints*, Pattern Analysis and Machine Intelligence, IEEE Transactions on 19.1 (1997): 27-40.

[11] Kyong Chang Bowyer, K.W. Sarkar, S. Victor, B. *Comparison and combination of ear and face images in appearance-based biometrics*, Pattern Analysis and Machine Intelligence, IEEE Transactions on , vol.25, no.9, pp.1160,1165, Sept. 2003

[12] Lakshmiprabha, N. S. Bhattacharya, J. Majumder, S. *Face recognition using multimodal biometric features*, Image Information Processing (ICIIP), 2011 International Conference on , vol., no., pp.1,6, 3-5 Nov. 2011.