ISSN:2231-0711

Asha M. J et al | IJCSET |July 2013 | Vol 3, Issue 7, 256-260

BIFEMIT- A Novel Algorithm for Biometric Identification

Asha M. J.[#], Shimmi Asokan[*]

[#]*Department of Computer Science and Engineering, Rajagiri School of Engineering and Technology*
Ernakulam, Kerala, India

[*]*Rajagiri School of Engineering and Technology*
Kakkanad, Kerala, India

***Abstract*— For an intruder who tries to access a high security system, it is easy to spoof a single biometric trait than multiple traits. Identification used for high security applications need the application data to be protected from any unauthorized access. These systems need to ensure that only a genuine person's data is accepted. For high security applications involving large amount of data, there should be approximately zero false acceptance and very less false rejections and the processing time should be less. Proposed is a multimodal biometric identification algorithm which uses features extracted from fingerprint using an ellipse method and iris features. For iris, matching scores are generated by template partitioning method. The two biometrics is fused using a modified form of rank level fusion. This algorithm gives approximately zero false acceptances and takes very less processing time.**

***Keywords*— Identification, Fingerprint, Iris, Rank level fusion, False acceptance, False Rejection, Processing time.**

I. Introduction

Uni-modal biometric systems using a single biometric have some limitations like noise in the acquired data, non-universality and intruder attacks. The system may fail to accept a genuine person, if his sensed biometric data is noisy. For example if there are large amount of dust accumulated in the fingerprint acquisition device or in the hand of a user, the fingerprint image acquired will not be able to give the necessary level of accuracy. Another reason for failure of a uni-modal system is non-universality, i.e. a subset of users may not have the particular trait. Also for an intruder it is easy to spoof a single biometric. Most of the problems for a uni-modal system can be alleviated by using multiple biometric traits. In a multimodal system two or more biometric traits are used for identification. Almost all the users of the system will have at least one of the biometric traits and also for an intruder; it will not be an easy task to spoof all the biometrics.

In the proposed algorithm, fingerprint and iris are used as two biometric traits for identification. Fingerprint is the pattern of ridges present in a person's fingers. Discontinuities in ridges called minutiae are extracted from fingerprint during identification. In the proposed algorithm, fingerprint feature extraction and classification is done using an ellipse method. By using ellipse method there is a significant reduction in the region of interest. As a result there is a reduction in the processing time. Ridge ending, Bifurcation, Cross over and Island are extracted from each fingerprint. This improves the accuracy of the system. Fingerprint classification also contributes towards the accuracy of the system. Increase in accuracy decreases the false acceptance and false rejection rates.

Iris is the circular region in human eye which has two boundaries iris-pupil boundary and iris-sclera boundary. Iris identification is done by studying the unique pattern of iris. In the proposed algorithm, for iris matching, template partitioning method is used.

Fusion of the fingerprint and iris is done at rank level using a modified logistic regression. The proposed biometric identification algorithm reduces the processing time to a great extend compared to the algorithms in the literature. Using proposed algorithm, false acceptance rate (FAR) is reduced approximately to zero and there is very less false rejection rate (FRR).

II. Literature Survey

There are a number of issues that need to be considered when designing a multimodal biometric system [15]. Following are the main issues:

- The number and the type of biometric traits
- The level of integration
- Algorithm used for identification
- The method used for fusion
- Cost performance ratio

The number and type of the biometric traits depends on the application requirements. Jain et al [2] in their paper studied about different biometric traits. DNA based biometric identification is a very complex and time consuming process which makes it unsuitable for online applications. Ear based biometric system [11] 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 [12]. Gait is an input intensive and computationally expensive behavioural 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. Iris is the externally visible doughnut shaped region of eye bounded by pupil and sclera. The unique structure of iris will not change during person's lifetime.

The systems used for iris recognition is not very expensive and satisfies the requirements for online iris recognition. Fingerprint formation begins at the early stages of the growth of a person and remains permanent for the entire life. Fingerprint identification is proved to be accurate [13].

There are different levels of integration. In Sensor level integration, biometric data from multiple sensors are combined at the data acquisition level itself to obtain a combined form, from which features can be extracted. Feature extraction level fusion is used in [16]. In feature level fusion large amount of information is available for processing which will give accurate results. The drawback of this level is that the application vendors may not give access to the feature level data. Matching score level fusion used in [17] is a better method for feature fusion. Speed of processing can be further increased by using a rank level fusion. In [18], a fuzzy fusion is used.

For identification several algorithms are available in literature. The algorithm given in [8] is a fingerprint identification algorithm based on single core point detection and minutiae extraction around that core point. In this algorithm the number of minutiae to be considered is predetermined. By predetermining the number there is a reduction in accuracy. The paper also states that, if there is reduction of minutiae from 18 to 6 then there will be 20% reduction in processing time and this is one of the motivations for the proposed ellipse method. In the paper [8] the algorithm compares various rank level fusion methods and using logistical regression the time required for matching is 0.65min.

In [7] using direction map method core and delta are extracted and fingerprint is classified. The count of the core and delta points, and fingerprint class were stored in a template along with iris features. Here a template level fusion is performed. For matching, hamming distance based matching score is calculated. This method gives a FAR of 0 and an FRR of 5.71% when tested using 8 iris form BATH iris image and 8 fingerprints from FVC2002 database of 10 users [7]. FVC2002DB2B when tested using the algorithm in [7] gives a FAR of 1.35% and FRR of 5.71%. Using the MATLAB environment on a general-purpose Intel P4 at 3.00GHz processor with 2-GB RAM memory the algorithm in [7] takes 4.60sec for pre-processing fingerprints and 3.56sec for pre-processing iris. The matching stage takes 0.37sec.

Proposed algorithm first finds the core and delta points and then using ellipse method extracts minutiae from the elliptical region. The fingerprint classification information and minutiae information are then stored in a template. Extracted iris information is also stored in the template. The matching score of iris and fingerprint is calculated separately and are fused using a modified rank level fusion. The algorithm shows a very good performance with a reduced speed compared to existing algorithms.

III. Proposed Multimodal Identification System

Proposed biometric identification is done in 3 steps, fingerprint identification, iris identification and rank level fusion of fingerprint and iris. Fingerprint and iris identification is done in parallel. The two ranks generated are combined using logistical regression.

A. *Fingerprint Identification Using Ellipse Method*

Fingerprint identification algorithm has five steps.

1) *Pre-processing*: The fingerprint need to be pre-processed in order to extract accurate features from it. Pre-processing consists of mainly two stages, Normalization and Orientation Estimation.

Normalization, also called contrast stretching, is done to reduce the variations in gray level values. Contrast stretching to the range 0-255 will give a very good environment for processing.

For finding the orientation, image is first divided into w (16×16) sized blocks. For each block the x gradient and y gradient are calculated. Orientation of each block is calculated using the method given in [5]. The output of orientation estimation is the direction map.

2) *Reference Point Location*: For reference point location Poincare index method of Kawagoe and Tojo [6] is used. A Poincare index of 180^0 corresponds to core and -180^0 corresponds to delta. For core and delta extraction a direction map method is used. In direction map method, for each point, the sum of the difference between the point and its neighbours is calculated. Maximum of this will give the points with highest angular difference. The centroid of this will give the core point. Then the point with maximum angular difference in negative direction will give the delta point.

$$\text{maximum\_angular\_difference}(i,j) = \max(\text{direction\_map}(i,j) - \text{k\_neighbor}(i,j)) \quad (1)$$

In some low quality images it will be difficult to get the delta point. In that case a line is drawn through maximum value points from core. A delta point is approximated near the edge of the direction map.

3) *Fingerprint Classification and ROI extraction using Ellipse Method:*

For finding the class of the fingerprint the method in [7] is used. From figure the elliptical region is the needed ROI for minutiae extraction.

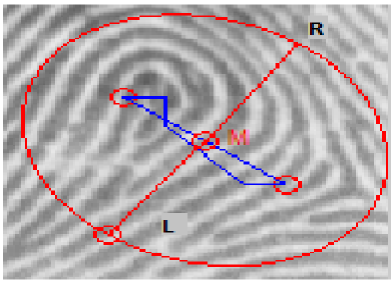

Fig. 1 Ellipse Method

Fingerprint belongs to Right loop, Left loop, and Tended arch class if it satisfies the equations (2), (3) and (4) respectively [7].

$$abs(\beta - R_{angle}) > abs(\beta - L_{angle}) \quad abs(\beta - M\_{angle}) > \text{tolerance angle} \quad (2)$$

$$abs(\beta - R_{angle}) < abs(\beta - L_{angle}) \quad abs(\beta - M_{angle}) > \text{tolerance angle} \quad (3)$$

$$abs(\beta - R_{angle}) < abs(\beta - L_{angle}) \quad abs(\beta - M_{angle}) < \text{tolerance angle} \quad (4)$$

Where β is the angle the core-delta line makes with the horizontal axis. L_{angle} is the angle that L point from figure 1 makes in the direction map and R_{angle} is the angle that R point makes. If two core points or two delta points are detected then it is a whorl fingerprint and if there are no core points then it is an arch fingerprint.

4) Minutiae Extraction:

After finding the core and delta points, a line is drawn joining the two. Using the coordinates of midpoint M of the core-delta line as centre and core and delta as foci an ellipse is drawn. The area of the ellipse can be taken as the needed ROI for minutiae extraction. From the ROI four types of minutiae are extracted.

- 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

Before extracting the minutiae, the elliptical region is binarized, and then thinned to infinity to get a single value for each ridge pixel. From the thinned image, for each pixel, sum of the pixel values of its 8 neighbours is calculated. A ridge pixel with a sum of zero correspond to an Island, a sum of 1 shows it is a ridge ending, 3 correspond to bifurcation and 4 correspond to cross over. Then calculate the number of ridge ending, bifurcation, cross over and islands. In the template, store the count of each type of minutiae and class of the fingerprint along with x and y coordinates of ridge endings and bifurcations.

5) Ranking

For ranking, a hamming distance based matching score is generated. Ranking is done in the order of the matching score. Then the matching scores and the first 10 ranks is passed to the fusion module.

B. Iris Identification

Iris identification is done in four stages. First the boundaries of iris are localized. Then from the extracted iris region, noise is removed. Iris is normalized by Daugman's model [21]. After normalization iris is encoded into a template. Matching is done using template partitioning.

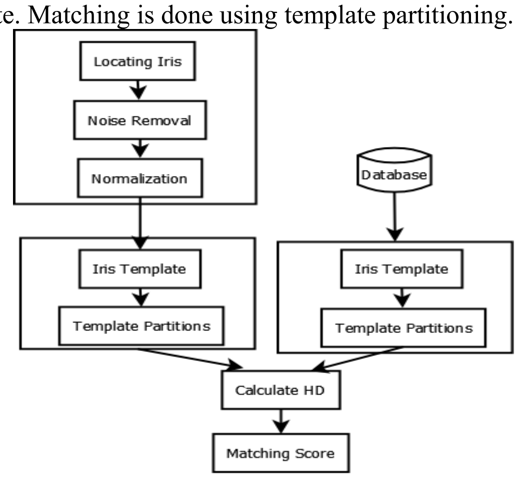

Fig. 2 Iris Identification

1) Locating the iris:

Locating the iris means separating iris from the eye image. Iris has two boundaries the iris-sclera boundary and iris-pupil boundary. For separating the iris a circular Hough transform [22] is used. Segmentation of iris will give the centre coordinates and radius. After iris segmentation pupil is segmented and the radius and centre of pupil is found out. For detecting the boundaries canny edge detection method is used [23].

2) Noise Removal

Mainly three types of noise are present in eye images; the eye lids, eye lashes and specular reflection. Eye lashes and specular reflection is removed by thresholding. Eye lids are removed by fitting a line using linear Hough transform [22].

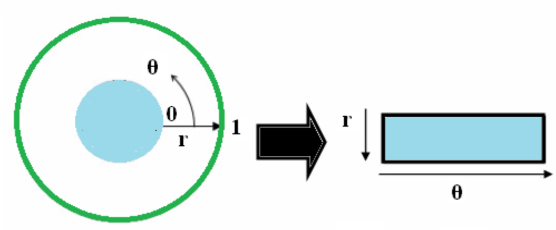

Fig. 3 The rubber sheet model (adopted from [21]).

3) Normalization and Encoding

After noise removal, the iris image is converted from Cartesian coordinate to polar coordinate using Daugman's model [21]. The model is given in fig.3. After the normalization iris is encoded into a template.

4) Matching

For matching the iris, a new method is used. In the template partitioning method, there are 5 steps:

- Partition the iris into n partitions
- According to accuracy and priority of each partition, assign weight to each partition.
- Calculate the hamming distance of each partition with the stored template in the database.
- Calculate matching score using the equation (5)

$$\frac{\sum_{i=1}^{N} HDi \times Wi}{N} \qquad (5)$$

- Ranking is done in the order of matching score. The first 10 of these ranks along with the matching scores is given to the fusion module.

C. Fusion

For fusion of the two biometric data, a modified rank level fusion strategy [20] is used. During enrolment an average of the matching scores of two biometric traits is calculated and the value is stored in the database as template. Later during identification, after calculating the matching scores of two models, average of the matching scores is compared with the already stored value in the database. If the present value is greater than the stored value, then a rank level fusion is performed.

Rank level fusion is done using logistic regression. The two biometric traits are assigned a weight according to the accuracy during enrolment. Then using equation (6) a matching score is generated. The process is outlined in Fig. 4.

$$\frac{\sum Ranki \times Wi}{N} \quad (6)$$

In this equation W_i is the weight assigned to each of the N modalities and $Rank_i$ is the rank. The person is identified if he has a matching score below a certain threshold.

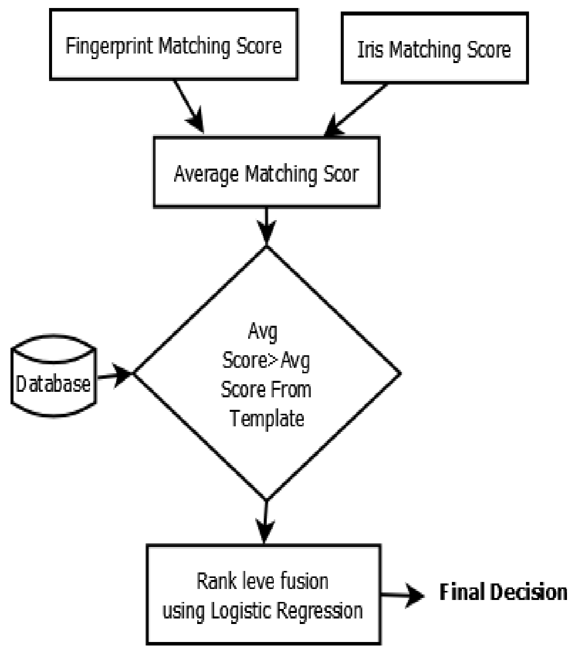

Fig. 4 Fusion

D. Experimental Results

The proposed fingerprint identification algorithm has 4 stages, pre-processing stage, reference point location, classification, minutiae extraction and then a matching stage. Pre-processing can be done in both gray level and binary images. But in order to get more accurate features gray level image is used. From the normalized fingerprint image the direction of ridges is calculated and this value is stored in direction map. Using the direction map, core and delta values are calculated. For low quality images delta is approximated by fitting a line from core to delta though maximum value points and then the fingerprint is classified. Minutiae are extracted from the ellipse drawn using core and delta as foci.

For iris identification first the iris region is taken out from the eye image, and then this is normalized into Cartesian coordinate and encoded into a template. For matching, a template partitioning method is used. The matching scores from fingerprint and iris are fused at the rank level to get a combined rank and matching score. This score is then compared with the threshold, if it is less, a match is found.

The fingerprint classification information and the extracted minutiae information and the iris template are stored in a database during enrolment. During Identification process, extracted information is compared with all the templates in the database to find a match.

Fingerprint samples from FVC2000 [13] and iris samples from CASIA [19] are used for identification. Since minutiae from the elliptical region only is considered, the processing time is reduced to large extend than the algorithm based on a large number of minutiae [14], [8], [7].

The processing time of the minutiae extraction process is directly proportional to the image size. As the number of minutiae is decreased there is a decrease in processing time. The table I shows a comparative study of the processing time using different algorithms.

Proposed fingerprint algorithm is a modification of [7]. 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. Since ridge ending, bifurcation, cross over and islands are detected, there is a significant reduction in the FAR than that of [8]. Table II shows the FAR and FRR of the methods used in [8] and the proposed method.

TABLE I
PROCESSING TIME COMPARISONS

Algorithm	CPU time
Algorithm using minutiae matching around core point[8]	8.0653
Proposed Ellipse Method with whole minutiae matching	6.45224
Proposed algorithm for fingerprint	3.9468
Proposed BIFEMIT algorithm	4.5663

TABLE II
FAR AND FRR COMPARISON

Algorithm	FAR	FRR
Algorithm using minutiae matching around core point [8]	0.06	0.4
Proposed fingerprint algorithm	0	0.333
Proposed fingerprint and iris algorithm	0	0.06

IV. CONCLUSION AND FUTURE WORK

Proposed fingerprint and iris algorithm proves to be a good method for fingerprint identification. It gives very less FAR and FRR rates and improved CPU usage. This makes the algorithm suitable for mission critical applications involving large amount of data.

In order to make the algorithm suitable for very large population with reduced processing speed and memory utilization, a future work that can be done is a fuzzy method of fusion of fingerprint and iris features.

High security applications need more privacy of the data. For the system to be useful for high security systems, a second enhancement is suggested. This enhancement is a system that provides high security for the images by using some sort of encryption.

Also using this algorithm a low cost embedded biometric identifier for use in less expensive systems can be made as a future work.

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" 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", Information Processing (ICIIP), 2011 International Conference on , vol., no., pp.1,6, 3-5 Nov. 2011.

[13] "Fingerprint Verification Competition FVC2000", [Online]. Available: http://bias.csr.unibo.it/fvc2000/(2000, Aug.).

[14] Farina, Alessandro, Zsolt M. Kovacs-Vajna, and Alberto Leone, Fingerprint minutiae extraction from skeletonized binary images." relax Pattern recognition 32.5 (1999): 877-889.

[15] Ross, Arun, and Anil K. Jain. "Multimodal biometrics: An overview." Proceedings of 12th European Signal Processing Conference. 2004.

[16] Ross, Arun, and Rohin Govindarajan. "Feature level fusion in biometric systems.", see http://www. wvu. edu/ bknc/2004% 20Abstracts/Feature% 20Level% 20Fusion% 20in% 20Biometric% 20Systems. Pdf (2004).

[17] Ko, Teddy. "Multimodal biometric identification for large user population using fingerprint, face and iris recognition.", Applied Imagery and Pattern Recognition Workshop, 2005. Proceedings. 34th. IEEE, 2005.

[18] Conti, Vincenzo, et al. "Fuzzy fusion in multimodal biometric systems." Knowledge-Based Intelligent Information and Engineering Systems. Springer Berlin Heidelberg, 2007.

[19] "CASIA Iris Image Database", [Online]. Available: http://www.sinobiometrics.com.

[20] MONWAR, MD. "A MULTIMODAL BIOMETRIC SYSTEM BASED ON RANK LEVEL FUSION." (2013).

[21] Daugman, John. "How iris recognition works." Circuits and Systems for Video Technology, IEEE Transactions on 14.1 (2004): 21-30.

[22] Hough, Paul VC. "Method and means for recognizing complex patterns." U.S. Patent No. 3,069,654. 18 Dec. 1962.

[23] J. Canny, "A computational approach to edge detection," IEEE Trans. Pattern Anal. Mach. Intell., vol. 8, no. 6, pp. 679–698, Nov. 1986.