FUSION OF IRIS AND FINGERPRINT BIOMETRIC FOR RECOGNITION

Himanshi Budhiraja[1], Himani Tomar[2], Harshi Goel[3], Amar Singh[4]

UG, [1,2,3] Department of Information Technology Engineering,
[2]Senior Lecturer, Department of Information Technology Engineering,
Raj Kumar Goel institute of Technology for Women, Ghaziabad,
Gautam Buddh Technical University, Lucknow, (India)

ABSTRACT

This paper represents studies on fusion strategies for personal identification using fingerprints and iris biometrics. The purpose of our paper is to investigate whether the integration of fingerprint and iris biometrics can achieve performance that may not be possible using a single biometric technology. Biometrics comprises methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral. Multimodal biometric identification is based on iris and fingerprint biometrics, both performs better as compared to other available traits due to their accuracy, reliability and simplicity. The fusion of multiple biometrics helps to minimize the system error rates. Fusion methods include processing biometric modalities sequentially until an acceptable match is obtained. The results of this paper confirm that a multimodal biometric can overcome some of the limitations of a single biometric resulting in a substantial performance improvement.

Keywords: Iris, Fingerprints, Sum Rule and Fusion

I INTRODUCTION

Biometrics refers to the use of physiological or biological characteristics to measure the identity of an individual. These features are unique to each individual and remain unaltered during a person’s lifetime. These features make biometrics a promising solution to the society. The access to the secured area can be made by the user of ID numbers or passwords which amounts to knowledge based security. But such information can easily be accessed by the intruder and they can reach the door of society. The problem arises in case of monetary transactions and highly restricted to information zone. Thus to overcome the above mentioned issue biometric traits are used. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological and behavioral characteristics possessed by the user. Biometric technologies are thus defined as the automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic.

II IRIS VERIFICATION

Iris recognition has received increasing attention due to its high reliability for personal identification. The human iris, and annular part between the black pupil and the white sclera, has an extraordinary rich structure and provides many interlacing minute characteristics such as freckles, coronas, stripes, furrows, crypts and so on. There are four main approaches to iris representation: phase information coding, zero-crossing representations, shape description and texture analysis. The iris recognition system employed in this paper is based on the efficient algorithm that characterizes the critical points of local variation.

This figure illustrates the main steps of our method. First the background in the iris image is removed by localizing the iris. Then the annular iris region is normalized to a rectangular block of fixed size. After lighting correction and images enhancement, a set of ID intensity signals containing the main spatial variations of the original iris for the subsequent features extracted is constructed. We record the position local sharp variation points in each intensity signal as features by wavelet analysis. A matching scheme based on Exclusive OR calculation is proposed.

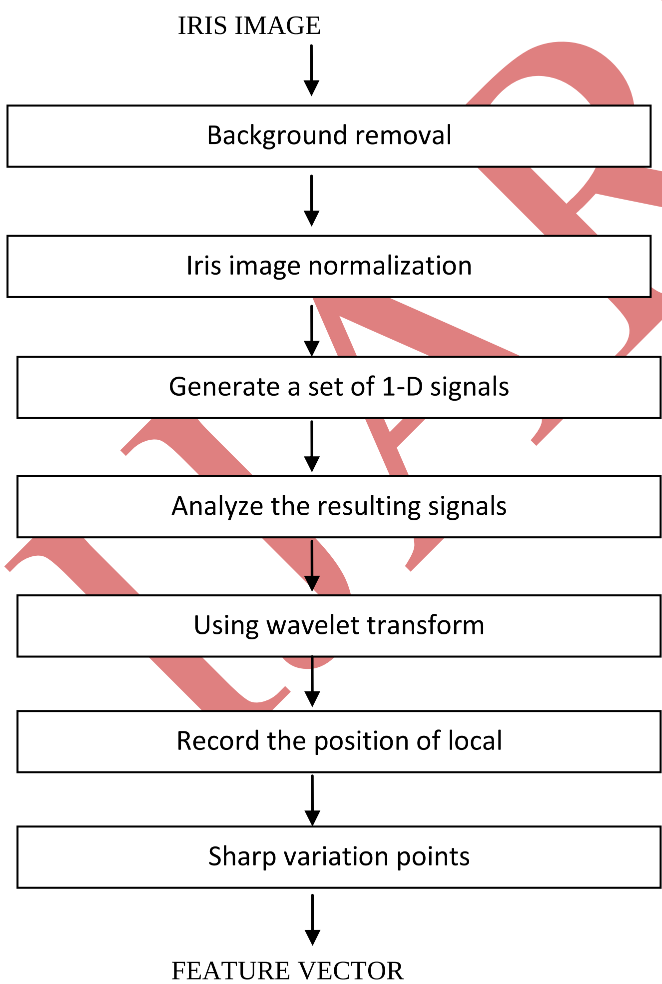

Fig1 : Major Steps In Iris Feature Extraction

2.1. Pupil Detection

Pupil is the darkest portion of the eye and is detected and removed from the eye image so that only iris pattern can be used for matching. The first step involved in pupil detection is to find the contours of the acquired iris image. Since the pupil region contains the lowest intensity values its edges can be formed easily. After edge detection the next step is to find the center of the pupil. Thus the process starts with dilating the edge detected image and the dilated image with filled pupil circle is used to find the Euclidean distance between the non-zero points the spectrum showing the largest filled circle can be formed within the set of pixels. Since the pupil is the largest filled circle in the image the overall intensity of the spectrum peaks in the center. This spectrum image can be used to compute the center of the pupil. The pixel position having the maximum value in the spectrum image corresponds to the pupil center. The radius of the pupil is the distance between the pupil center and nearest non-zero pixel.

2.1.1 Iris Detection

To find the outer iris boundary intensity variation approach is used. In this approach concentric circles of different radii are from the detected center. The circle having maximum change in intensity with respect to previous drawn circle is iris circle. The approach works fine for iris images having sharp variation between iris boundary and sclera. The radius of iris and pupil boundary is used to transform the annular portion to a rectangular block, known as strip.

2.1.2. Feature Extraction

Features are the attributes or values extracted to get the unique characteristics from the image. Features from the iris image are extracting using Haar Wavelet decomposition process [9]. In the wavelet decomposition the image is decomposed into four coefficient i.e., horizontal, diagonal, vertical and approximation. The approximation coefficients are further decomposed into four coefficients. The sequences of steps are repeated into five levels and the last level coefficient are combined to form a vector. The combined vector is binaries to allow easy comparisons between the iris codes for database and query image.

$$IC(i) = \begin{cases} 1 & FV\_(i) > 0 \\ 0 & FV\_(i) < 0 \end{cases}$$

The binaries feature vectors are passed to the matching module to allow comparisons.

2.1.3. Matching:

The comparison is done between iris code (IC) generated for database and query images using hamming distance approach. In this approach the difference between the bits of two codes are counted and the number is divided by the total number of comparisons.

$$MS_{Iris} = \frac{1}{N}\sum_{i=1}^{N} A_i \oplus B_i$$

Where A is the binary vector (iris code) for database image and B is the binary vector for query image while N is the number of elements. This matching score (MS_{Iris}) is used as input for the fusion module where the final matching score is generated.

III FINGERPRINT RECOGNITION

Fingerprint recognition is one of the most well known and publicized biometrics. Because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century, more recently become automated (i.e. a biometric) due to advancement in computing capabilities. Fingerprint identification for over a century is popular because of inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration.

3.1 Concept

A fingerprint usually appears as a series of dark lines that represent the high, peaking portion of the friction ridge skin, while the valleys between these ridges appears as white space and are the low, shallow portion of the friction ridge skin. It is based on the minutiae, or bifurcations (splits) along a ridge path. The images below present examples of fingerprint features: a) two types of minutiae and b) examples of other detailed characteristics sometimes used during the automatic classification and minutiae extraction processes.

The types of information that can be collected from a fingerprint's friction ridge impression include the flow of friction ridges(level 1 detail), the presence and absence of features along the individual friction ridges path and their sequence (level 2 detail) and the intricate detail of a single ridge. Recognition is usually is based on the first and second level of detail or just the latter. The major steps involved in fingerprint recognition using minutiae matching approach after image acquisitions are:

1. Image Enhancement
2. Minutiae Extraction
3. Matching

3.1.1. Image Enhancement

A fingerprint image corrupted due to various kinds of noises such as creases, smudges and holes. It is almost impossible to recover the true ridge/valley structure from the unrecoverable regions; and efforts to improve the quality of the fingerprint image in these regions may be futile. Therefore, any one known enhancement algorithm may be used to improve the clarity of ridges/valley structures of fingerprint images in recoverable regions due to mask out the unrecoverable regions. The steps involving in image enhancement are given in[12]. The process stars with normalization of input fingerprint image so that it has pre-specified mean and variance. The orientation image is estimated from the normalization input fingerprint image. Further, frequency image is computed from the normalized input fingerprint image and the estimated orientation image. After computation of frequency image the region mask is obtained by classifying each block in the normalized input fingerprint image into a recoverable or unrecoverable block. Lastly, a bank of Gabor filters which is tuned to local ridge and valley pixels in the normalized input fingerprint image to obtain an enhanced fingerprint image.

3.1.2. Minutiae Extraction

The enhanced fingerprint image is finalized and submitted to the thinning algorithm which reduces the ridge thickness to one pixel wide. The skeleton image is used to extract minutiae points which are the points of ridge endings and bifurcations. The location of the minutiae points along with the orientation is extracted and stored to form feature set. For extracting of minutiae points eight connected pixels are used [13]. The crossing number (CN) method is used to perform minutiae extraction. This method extracts the ridge endings and bifurcation from the skeleton image by examining the local neighborhood of each ridge pixel using a 3x3 window. The CN for a ridge pixel P is given by

$$CN = 0.5\sum_{i=1}^{8} | P_i - P_{i+1} |$$

$$P_9 = P_1$$

Where P_i is the pixel value in the neighborhood of P. After the CN for ridge pixel has been computed, the pixel can then be classified according to its CN value. A ridge pixel with a CN of one corresponds to a ridge ending, and a CN three corresponds to a bifurcation. For extracted minutiae points, the following information is recorded:

- x and y coordinates,
- orientation of the associated ridge segment, and
- type of minutiae(ridge ending or bifurcation)

3.1.3. Matching

The database and fingerprint query are used for minutiae extraction and stored as point in the two dimensional plane. A minutia is based matching essentially consists of finding alignment between the template and the input minutiae sets that results in the maximum number of minutiae pairings. Let A = $\{m_{1}......m_{m}\}$ and $\{m_{1}.......m_{n}\}$ be the set of minutiae points extracted from database and query images respectively. Where m={x,y,0}, x and y are the coordinates at particular minutiae point and 0 is the orientation. The two sets are paired using

$$Sd = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} < r_o$$

Minutiae in A and a minutia B considered to be matched if the spatial distance (sd) between them is smaller than a given tolerance r_o .

IV FUSION

No individual traits can provide 100% accuracy. Further, the results generated from the individual traits are good but the problem arises when the user is not able to give his iris image due to problem in exposure to light. As eye is the most sensitive organ of human body, the problem becomes severe when there some eye diseases. Thus in such a situation an individual cannot be recognized using the iris pattern and biometric system come to standstill. Similarly, the problem faced by fingerprint recognition system is the presence of scars and cuts. Thus, system takes noisy fingerprint as input which is not able to extract the minutiae points correctly and in turn, leads to false recognition of an individual. Thus to overcome the problem faced by iris and fingerprint, a novel combination is proposed for the recognition system. The integrated system also provide anti spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously.

V EXPERIMENTAL RESULTS

The results are tested on iris and fingerprint images collected by the authors. The database consists of three iris images (200x3) and two fingerprint images (200x3) per person with total 200 persons. The iris images are acquired using CCD camera with uniform light source. However, fingerprint image are acquired using an optical fingerprint scanner. For the purpose allowing comparisons two levels of experiments are performed. At the first level iris and fingerprint algorithm are tested individually. At this level the individual traits are computed and an accuracy curve is plotted. However in order to increase the accuracy of the biometric system as a whole the individual results are combined at matching score level. At the second level of experiment the matching scores from the individual; traits are combined and final accuracy graph is plotted. The overall performance of the system has increased showing an accuracy of 96.04% with FAR of 1.58% and FRR of 6.34% respectively. Receiver Operating Characteristic (ROC) curve is plotted for Genuine Acceptance Rate (GAR) against False Acceptance Rate (FAR) for individual recognizers.

VI CONCLUSION

The paper proposes a biometric personal authentication system using a novel combination of iris and fingerprint. For system deployment the combination is found to be useful as one needs a close up system and other needs contact. One modality is used to overcome the limitations posed by the other. The experimental results show that the accuracy of the system would increase on combining the traits. The system is giving an overall accuracy of 96.04% with FAR and FRR of 1.58% and 6.34%.

REFERENCES

[1] A. Ross & A. K. Jain, "*Information Fusion in biometrics, Pattern Recognition Letters*", 24(13), 2003, 2115-2125.

[2] W. Yunhong, T. Tan, & A. K. Jain, "*Combining Face and Iris Biometrics for Identify Verification*", Proceedings of Fourth International Conference on AVBPA, Guildford, UK, 2003, 805-813.

[3] S.C. Dass, K. Nandakumar, & A. K. Jain, "*A Principled Approach to Score Level Fusion in Multimodal Biometric System*", Proc. Of Audio- and Video-based Biometric Person Authentication (AVBPA), Rye Book, NY, 2005.

[4] G. Feng, K. Dong, D. Hu, & D. Zhang, "*When Faces Are Combined with Palm prints: A Novel Biometric Fusion Strategy*", International Conference on Bioinformatics and its Applications, Hong Kong, China, 2004, 701-707.

[5] L. Flom, & A. Safir, "*Iris Recognition System*", U.S. Patent No. 4641394, 1987.

[6] W. W. Boles, & B. Boashah, "*A Human Identification Technique Using Images of the Iris*".

[7] Raymond Thai, "*Fingerprint Image Enhancement and Minutiae Extraction, Technical Report*", the University of Western Australia, 2003.

[8] A. K. Jain, K. Nandakumar, & A. Ross, "*Score normalization in multimodal biometric systems*".