DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5742

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

MULTIMODAL BIOMETRIC SYSTEMS: A REVIEW

Dhruvi Patel
Computer Engineering
MPSTME, NMIMS
Mumbai, India

Sanyamee Patel
Computer Engineering
MPSTME, NMIMS
Mumbai, India

Aarvi A Thadeshwar
Computer Engineering
MPSTME, NMIMS
Mumbai, India

Ratnesh Chaturvedi
Computer Engineering
MPSTME, NMIMS
Mumbai, India

Abstract: The need for biometrics is rising with an increased need for security in every organization of the world. Every attribute, fingerprint, iris, knuckle print, face, palm print, is unique to an individual and can aid in recognition. Unimodal biometric systems involve the use of a single biometric attribute for identification. However, with the rise of duping, there is a requirement for constructing an efficient system using multiple biometric attributes. In multimodal systems, fusion of various biometric identities into a single vector is done using algorithms. This paper covers several different techniques used for biometric authentication. These use varying numbers of attributes. Our future project focuses on the research of different techniques of multimodal recognition in order to devise a technique that is robust and has an increased efficiency in recognition and identification.

Keywords: Unimodal biometrics, Multimodal Biometrics, Feature Vector, Fusion level, Score level, Decision Level

I. INTRODUCTION

Biometric recognition is a system which recognizes an individual based on some features derived from behavioral or physiological characteristics. Feature extraction is used to represent important parts of an image in the form of a feature vector. This approach is useful when image sizes are large and a reduced feature representation is required to quickly complete tasks such as image matching and retrieval.

Transformation of input data into a set of features is carried out. Features are distinctive properties of input patterns that help in differentiating between the categories of input pattern. Most of the real-life biometric systems are unimodal biometric recognition, which are based on single traits of biometric information. Such systems are affected by many problems like noise, non-universality, duping and unacceptable error rates etc. Hence multimodal biometric identification systems are becoming popular in these days.

Multimodal biometric systems have many advantages over unimodal systems, as combining evidence from various modalities through fusion greatly improves overall system accuracy.[1] A multimodal system reduces failure to enroll and resists unauthorized access, as it is difficult to spoof multiple biometric sources simultaneously. Multimodal systems can search large databases efficiently and quickly through use of simple but less accurate modality to narrow down the options in the database before applying complex and accurate modality on remaining data for final identification.

The disadvantages of multimodal systems are that it is expensive and necessitate the need for additional resources for computation and storage when compared to unimodal systems. Multimodal systems also require more time for enrolment or verification inconveniencing users. Lastly, system accuracy can be improved as compared to unimodal systems if proper techniques are followed when combining evidence from various modalities. In the future, we aim at improving the existing multimodal biometrics systems to make them more efficient.

II. STAGES IN A BIOMETRIC SYSTEM

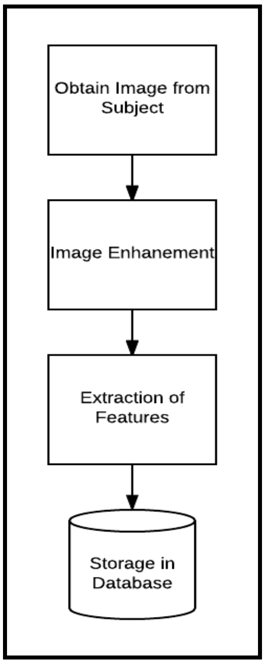


Figure 1. Registration

Every biometric system involves the processes of registration, verification and identification. Registration is the process of enrolling a user into the system for the first time, and consists of a number of steps, as shown in Fig. 1. After having acquired a scan of the attribute, various pre-processing techniques are used to correct image quality, reduce noise, and improve illumination and contrasts. From this, a numerical vector of n-dimensions is constructed to represent the image in the system.

Verification is the process of checking if the person is legitimate and registered in the database. It involves steps as depicted in Fig. 2. Identification involves a final decision once a match is made. These are achieved by obtaining a biometric trait from the system, which undergoes the same pre-processing techniques. A region of interest clips the image to only leave behind the area for feature extraction. The vector is compared with images in the database using the matching module, and a decision module delivers the final acceptance/ rejection.

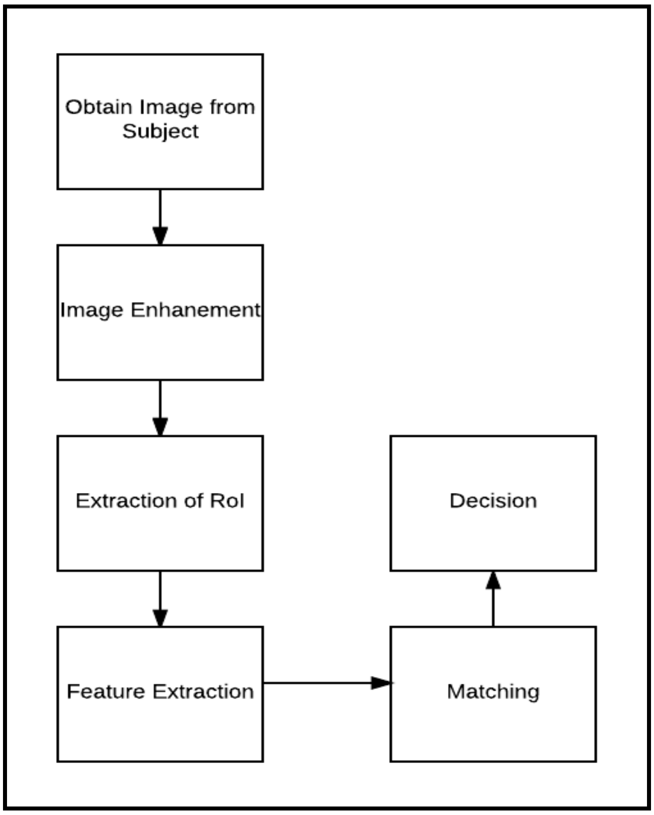


Figure 2. Verification and Identification

III. PRE-PROCESSING

For a fingerprint, the image is binarised using global thresholding, after which edge detection algorithms are used to detect the edge of the finger. Roberts cross operator, canny edge detector and the Sobel operators may be used. The Roberts cross operator uses 2-D spatial gradient measurement to detect high frequency areas in an image.

Another technique is that used in the iris registration, wherein a morphological flood fill operator changes connected background pixels to foreground pixels to detect edges when the flood fill reaches the boundary. Circular Hough Transform is the process of detecting the edge of the iris using an accumulator matrix. This matrix consists of values that detect the number of circles passing through a grid cell. Finding the local maxima leads to detection of the center of the circle.

The Viola Jones Algorithm detects the face on three key contributions: integral image for fast evaluation, Adaboost for finding the best features for extraction, and cascade classifier for composing each stage of the strong classifier into several stages.

In the detection of the knuckle-print, a Gaussian smoothing operation is applied to determine the X-axis of the coordinate system fitted from the bottom boundary of the finger. The bottom boundary can be easily extracted using a Canny edge detector. The detector uses smoothing, intensity gradient calculation and thresholding to determine the edges. The same detector is used to determine the Y-axis from the cropped sub-image extracted from the X-axis. The RoI coordinate system is extracted, where the rectangle indicates the area of the sub-image

IV. FEATURE EXTRACTION

The process of feature extraction involves using the transform domain or algorithms in the spatial domain.

A. Transforms

Transforms like the Haar, Walsh, Kekre and Slant can be used to process an image. [2] However, wavelet transforms are utilised since they do not lead to information loss. The components of the image along different axes are obtained using wavelets. Coiflet wavelet transform consists of scaling functions with vanishing moments. [3] A wavelet is said to have p vanishing moments if and only if the wavelet scaling function can generate polynomials up to degree p1. For at most p-1 polynomials, the wavelet coefficients are zero. This leads to a representation of scaling functions using a sparser set of wavelet coefficients.

Orthogonal transforms like DCT, Haar, Walsh and Kekre produce fractional coefficients of energy. These are usually concentrated in the upper left corner of the transform matrix. [4] These lead to vector extraction using only a small portion of the image containing the most important information. Another approach [5] utilises 2D-DCT and 2D-DFT to extract feature vectors. The DCT system first divides the image into blocks of size M x M, where M is mostly 8, which contain the transformed coefficients of the image. Every coefficient of a block is then transformed into a one-dimensional array by scanning the matrix in a zigzag manner. Each array is stored into a vector for a block. These vectors are then combined to result in a final vector for the entire image.

B. Block Truncation Coding and Bit Plane Slicing

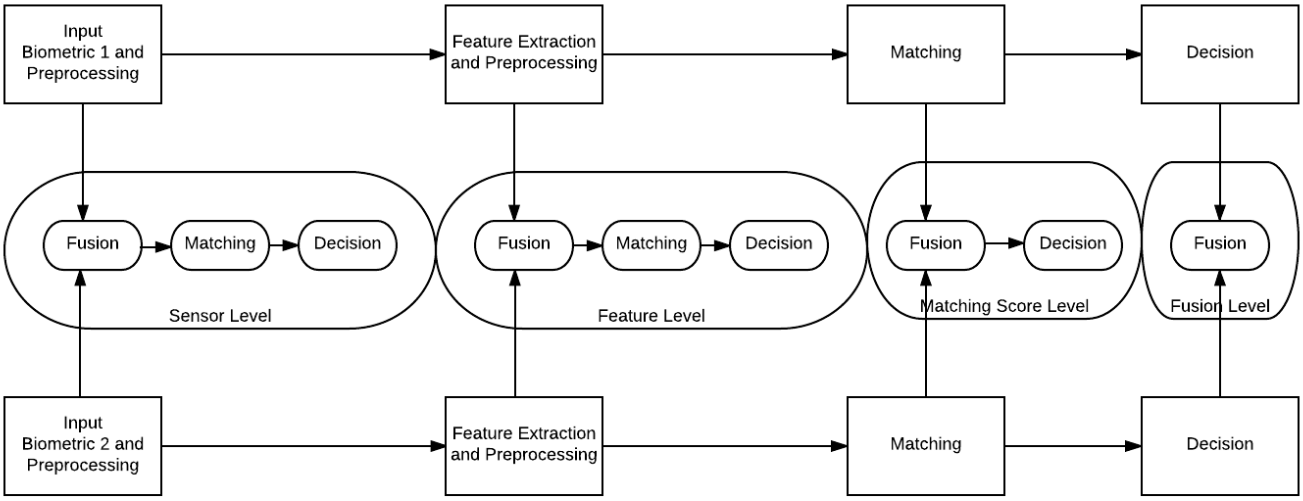
In this spatial domain approach the image is first divided into non-overlapping blocks, which are then coded one at a time. [6] Each pixel is coded with a binary bit-map and two mean pixel values. Further, the respective upper and lower components of the initial level are divided into subsets in the feature vector of the respective bit planes of the image.

Bit plane slicing divides the image into different planes in the order of the significance of the bits-MSB to LSB.

C. Principal Component Analysis

An image consists of primarily three color components: R, G and B. The intensity of each distinguishes an image from another. The extraction of, say, the R component will also extract G and B in a small number. Similar events occur when extracting G and B. Hence, the components are statistically correlated, at either a high or very low level. This leads to elimination of some of the other two components when one is being extracted. This leads to loss of information and is heavily undesired

Fig. 3. Fusion at various stages



Eigenvectors are used in the extraction of feature vectors using PCA. An eigenvector does not change direction upon application of a linear transformation on it. The covariance matrix of a set of points of an image is composed of a set of rotation and scaling functions. The rotation matrix is defined by the eigenvectors of the covariance matrix. An image can be de-correlated by rotating the points such that the eigenvectors become the new axes. This leads to discovery of otherwise unknown and uncorrelated components. These being independent, can be eliminated one at a time without affecting the other. Hence, the dimensionality of an image is reduced. Eigenvectors are widely used in face detection algorithms, in the form of Eigen faces.

D. Filters

A Gabor filter is used to detect an iris by convoluting the normalised model with the Gabor filter. [7] Essentially orientation-sensitive, these are used for texture analysis. The Gabor wavelet coefficients are quantised to result in a binary image of the iris code.

V. FUSION

The process of fusion involves the combination of features extracted. This can be done at the sensor, feature extraction, matching or decision levels (Fig. 3). [8]

A. Sensor Level

The process involves combination of biometric traits to form a single composite trait immediately after obtaining it from the sensor. Filters are applied to the images individually, after which combination and normalisation take place. Vectors are extracted and stored, which are then used for matching and decision making.

B. Feature Level

The feature vectors extracted are concatenated for feature fusion, but lead to an increased dimensionality and subsequent difficulty in matching score computations. Gabor filters are used to overcome this problem.

Fusion methods like mean-mean, max-min, img1, img2, mean-max are used for merging wavelet decompositions of two original images; applied to approximation coefficients and detail coefficients. This study uses mean-max fusion method. The steps involved in feature fusion strategy are:

1) Apply wavelet extension to obtain similar dimensions of Gabor and line feature vectors.

2) Coiflet wavelet transformation to decompose wavelet.

3) Mean rule applied for image fusion.

4) Max rule applied for image fusion.

The combined feature vectors are classified using SVM. SVM is useful for data classification. Classification usually involves training and testing data having some data instances. Each training set instance has one target value and many attributes. SVM aims to produce a model which predicts target value of data instances in the testing set which has only attributes.

When a set of features represented in space is given, SVM maps features non-linearly into n dimensional feature space. To avoid high computation, a kernel is introduced as the algorithm uses only the inputs of scalar products. Classification is solved by converting the problem into a convex quadratic optimization problem with a unique solution being obtained due to convexity The predictor variable is called an attribute in SVM; a feature is a transformed attribute. Vector is a set of features describing an example. Features define the hyper plane. SVM aims to locate the optimal hyper plane separating vector clusters with one class of attributes on one side of plane and the rest on the other. The distance between hyper plane and support vectors is the margin. SVM analysis hence orients the margin such that the margin between support vectors is maximized.

C. Matching Score Level

The scores of individual matches are combined in this method of fusion. Some techniques used are weighted sum rule, weighted product, linear discriminant, decision tree and

Bayesian Rule. Score level fusion is further explained in the Identification section.

D. *Decision Level*

The integration is done at an abstract level if the output of both decisions is a category label (and not a confidence level), i.e. the claimed identity is true or false. A majority rule is then applied to reach a final decision. If similarity value is the output of a model, then confidence values can be used for better accuracy in rank or measurement level. [9]

VI. IDENTIFICATION

The first model we study is based on the iris and palm-print images, at matching score level. After reading, these images are converted to YCBCR, YCGCR, YIO, YUV, LUV, and RGB. [10] The feature vectors are extracted after pre-processing. This query vector is compared with the template using different similarity criteria such as taxial distance, square chord, euclidean distance. The matching score is found for each and then combined. The following are the formulae for distance calculation for two feature vectors A and B:

$$\text{Euclidean distance} = \sqrt{\textstyle\sum_n (A-B)^2} \qquad (1)$$

$$\text{Taxial Distance} = \textstyle\sum_n |A-B| \qquad (2)$$

$$\text{Square chord} = \textstyle\sum_n (\sqrt{A}-\sqrt{B})^2 \qquad (3)$$

For iris identification, the Hamming distance can be calculated between the iris code and the test code. This is given as:

$$\frac{\|(\text{codeA} \otimes \text{codeB}) \cap \text{maskA} \cap \text{maskB}\|}{\|\text{maskA} \cap \text{maskB}\|} \qquad (4)$$

A decision tree is used to classify a feature vector which has been scored, into two classes-either the person's identity has been verified, or it hasn't. A decision is reached when a result is obtained from the decision tree. In the case of no identical class, there is no verification. Otherwise, for more than one class, the scores are summed only for those classes that are identical. This is done in order to achieve the smallest possible combined score.[7] A sample decision tree for iris and fingerprint recognition, where ISi is iris score, and FSi is fingerprint score, is as in Fig. 4.

Another similarity measurement criteria is that of mean square error. The feature vectors are compared with those in the database to find a match. If a match is found, the person is genuine.

In score level fusion, the vectors of the biometrics are extracted and compared with the stored templates. The match- ing scores of the attributes are then fused together. Thus the query image feature vector and template feature vectors can be compared using Mean Square Error. For two feature vectors, MSE is calculated as follows:

$$\frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2 \qquad (5)$$

Here, N indicates the size of vectors, x and y indicate the feature vectors. A low MSE value indicates a high level of similarity between the feature vectors.

VII. DECISION CRITERIA

There exist several mathematical methods for the system to give a final decision about the acceptance or rejection of the person being verified. Some of them are Genuine Acceptance Rate(GAR), False Acceptance Rate(FAR), and False Rejection Rate(FRR).

A. *Genuine Acceptance Rate*

Genuine Acceptance Rate, or GAR, is the degree to which the system correctly accepts an access attempt by an authorised user. This is given as:

$$\frac{\textit{Number of Correct Acceptance}}{\textit{Number of Identification Attempts}}$$

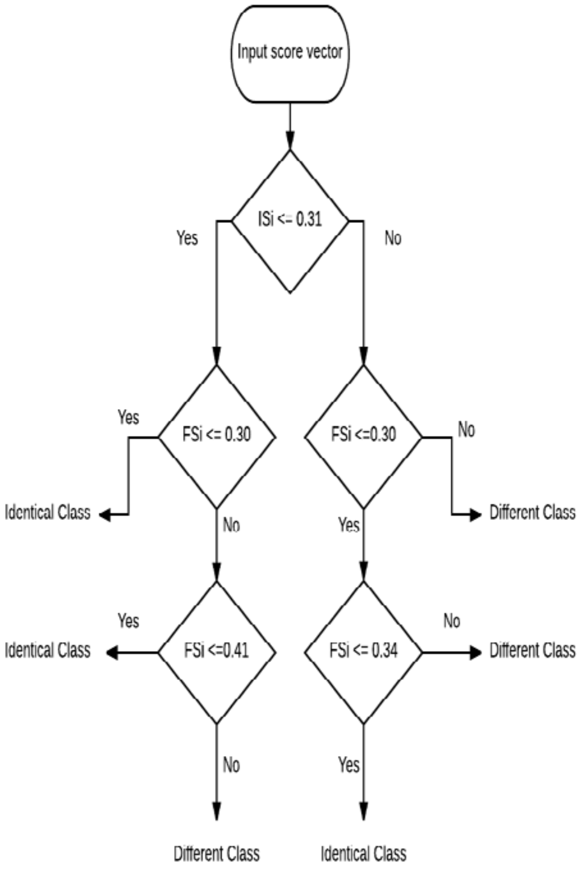


Fig. 4. A Decision Tree for Iris and Fingerprint Score

B. *False Acceptance Rate*

The false acceptance rate is the measure of the probability that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR is stated as:

$$\frac{\textit{Number of False Acceptance}}{\textit{Number of Identification Attempts}}$$

C. False Rejection Rate

False Rejection Rate (FRR) is the rejection of an authorized user. It is states as:

$$\frac{Number\ of\ False\ Recognitions}{Number\ of\ Identification\ Attempts}$$

Figure 5 shows the relation between the FAR and FRR, where the vertical axis denotes percentage and the horizontal axis denotes accuracy.

EER is the Equal Error Rate, which denotes the threshold values for FAR and FRR.

FAR gains the highest importance in practical applications, however, there exists the disadvantage of the FAR value providing only half the information. Hence, the FRR needs to be calculated too.

Hence, if a system is said to have a low FAR, it is necessary to find the value of FRR at this level of FAR. A very high level of FRR is undesirable even in such cases.

Practically, this scenario means that an unauthorised person is denied access. But, it would require the genuine user would have to try multiple times before gaining verification. This requires the system to be re-evaluated.

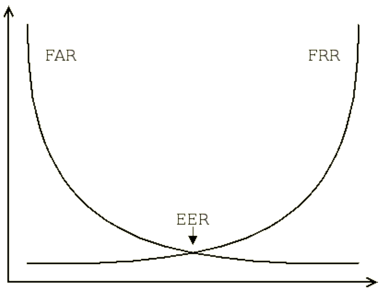


Fig. 5. Graph Describing Equilibrium point between FAR and FRR

VIII. PROPOSED WORK

Our paper proposes a fusion approach incorporating the second level decomposition of images. Each biometric will be decomposed and the LL bands extracted. Further, each LL band will be substituted for the other three bands in one of the biometric decompositions to produce a single image containing fused information. This can undergo inverse transforms to give a feature extracted fused image as output. Four attributes: finger, knuckle, iris and the face will be considered. Six transforms can be applied, each in combination with wavelet transforms. These will be compared to give an optimal solution.

IX. CONCLUSION

Multimodal biometrics are an upgrade from traditional biometric systems for increasing security and access control. Various methods exist for pre-processing, feature extraction, fusion, matching and decision, which have been briefly described in the paper. Combining the second level decomposition of four different biometrics (face, iris, fingerprint, knuckle print) in the fusion of biometrics is a dependable solution.

X. REFERENCE

[1] Oloyede, Muhtahir O., and Gerhard P. Hancke. ”Unimodal and mul- timodal biometric sensing systems: a review.” IEEE Access 4 (2016): 7532-7555.

[2] Thepade, Sudeep D., and Rupali K. Bhondave. ”Bimodal biometric identification with Palmprint and Iris traits using fractional coefficients of Walsh, Haar and Kekre transforms.” In Communication, Information Computing Technology (ICCICT), 2015 International Conference on, pp. 1-4. IEEE, 2015.

[3] Geetha, K., and V. Radhakrishnan. ”Multimodal Biometric System: A Feature Level Fusion Approach.” International Journal of Computer Applications 71, no. 4 (2013).

[4] Thepade, Sudeep D., Rupali K. Bhondave, and Ashish Mishra. ”Compar- ing Score Level and Feature Level Fusion in Multimodal Biometric Iden- tification Using Iris and Palmprint Traits with Fractional Transformed Energy Content.” In Computational Intelligence and Communication Networks (CICN), 2015 International Conference on, pp. 306-311. IEEE, 2015.

[5] Meraoumia, Abdallah, Salim Chitroub, and Ahmed Bouridane. ”Robust multimodal biometric identification system using Finger-Knuckle-Print features.” In Control, Engineering Information Technology (CEIT), 2015 3rd International Conference on, pp. 1-6. IEEE, 2015.

[6] Thepade, Sudeep D., and Rupali K. Bhondave. ”Multimodal identifi- cation technique using Iris Palmprint traits with matching score level in various Color Spaces with BTC of bit plane slices.” In Industrial Instrumentation and Control (ICIC), 2015 International Conference on, pp. 1469-1473. IEEE, 2015.

[7] Aizi, Kamel, Mohamed Ouslim, and Ahmed Sabri. ”Remote multi- modal biometric identification based on the fusion of the iris and the fingerprint.” In Electrical Engineering (ICEE), 2015 4th International Conference on, pp. 1-6. IEEE, 2015.

[8] ARAVALLI, NAGAMMA. ”Automatic System for Person Authentica- tion by Multimodal Biometrics- A Survey.”

[9] Jain, Anil K., Lin Hong, and Yatin Kulkarni. ”A multimodal biometric system using fingerprint, face and speech.” In Proceedings of 2nd Int’l Conference on Audio-and Video-based Biometric Person Authentication, Washington DC, pp. 182-187. 1999.

[10] Madane, Manisha, and Sudeep Thepade. ”Score Level Fusion Based Bimodal Biometric Identification Using Thepade’s Sorted n-ary Block Truncation Coding with Variod Proportions of Iris and Palmprint Traits.” Procedia Computer Science 79 (2016): 466-473.