International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 4: April 2016, pp 52-56. www.aetsjournal.com ISSN (Online) : 2394-6237

Fusion of Multimodal Biometrics using Feature and Score Level Fusion

S.Mohana Prakash, P.Betty, K.Sivanarulselvan

***Abstract*—**Abstract-Biometrics is used to uniquely identify a person's individual based on physical and behavioural characteristics. Unimodal biometric system contains various problems such as degree of freedom, spoof attacks, non-universality, noisy data and error rates. Multimodal biometrics is introduced to overcome the limitations in Unimodal biometrics. The presented methodology extracts the features of four biometric traits such as fingerprint, palm, iris and retina. Then extracted features are fused in the form of finger print, palm and iris, retina by Discrete Wavelet Transformation. Similarity scores are generated for each fused biometric traits by using a classifier. Using both feature and score level fusion optimization problem can be solved.

Keywords – multimodal biometrics; level of fusion, fusion methods

I. INTRODUCTION

A user can be checked based on the identification number (ID) or the user has specific knowledge as a password which user knows. These techniques have number of disadvantages. For example token (ID) might be lost, forgotten, missed or stolen. Password might not be remembered or confused. These techniques do not have an appropriate approach to differentiate authorized user and an imposter who may steal the token or knowledge. This technique will not provide any good security in access control and in financial transactions.

Biometric systems automatically identify or analyse a person's identity based on his physical and etiquette characteristics such as fingerprint, vein, Iris, Palmprint and face. It is a method of recognizing or analysing the identity of an individual person's physiological and etiquette characteristics.

Unimodal biometric systems rely on single biometric trait such as fingerprint, palmprint or iris, but these systems having some unavoidable problems.

1. Non-universality: Single source of biometric information might not be useful for some user authentication. For example an iris biometric trait may result in false texture because of contact lens of the user.

S.Mohana Prakash, P.G student, Department of computer science and engineering, Kumaraguru college of technology, Coimbatore, India. (Email: mpfedder284@gmail.com)

P.Betty, Assistant Professor, Department of computer science and engineering, Kumaraguru college of technology Coimbatore, India. (email: betty.p.cse@kct.ac.in)

K.Sivanarulselvan, Associate Professor, Department of computer science and engineering, Kumaraguru college of technology, Coimbatore, India. (Email: sivanarulsevan.k.cse@kct.ac.in)

2. Noisy data: low lighting on the user face or any biometric trait is an example for noisy data.

3. Intra class variations: the presence of wrinkles due to wetness in the fingerprint or palmprint can make a variation in the output and user can incorrectly communicate with the sensor

4. Spook attack: Forgery in hand signature is a good example for spoof attack.

It has been noted that some limitations of single modal biometrics systems can be addressed by integrating the information of multiple biometric trait such as fingerprint, palmprint, iris and retina. These systems will produce less damage to spoof attacks because it is not possible to spoof multiple biometric traits simultaneously and it also avoids the problem of non-universality and intra-class problems.

Multimodal biometric system can be classified into different levels based on the performance into feature-level, score-level and decision level fusion. In feature level fusion, the main idea is consolidating the obtained feature set of multiple biometric algorithms into a single feature trait, after the process of normalization, transformation and reduction is performed. Feature normalization: It is a process modifying the location (mean) and the scale (variance) via transform function to generate a feature value in order to group them in a common domain (e.g. Min-Max Normalization, Z-score normalization, median normalization etc.). Feature selection or Feature Transformation: In this algorithm dimensionality of a feature set can be reduced (e.g. Sequential Forward Selection, PCA, Sequential Backward Selection). It maintains raw information about the feature so it is more inequality than a score or decision level fusion. But, in feature level fusion features are extracted from different sensors are in the form of dimensions and types. It has a limitation that it is very difficult to fuse an image with higher dimension feature. In score level fusion, the image is reduced into single unit as a match score or similarity score by a classifier and that classifier trains and test the input data. Trained and tested data are compared to find the required image. On the decision level fusion that small unit of the feature is further divided into small class labels. The fusion is carried out decision or abstract level in the multi biometric system only when decisions are available. AND, Majority Voting, OR, Bayesian Decision Fusion Weighted Majority Voting are some of the available fusion strategy. The main challenges in this fusion with high efficiency, accuracy, secure biometric system.

Adaptive biometrics system is a model or template which is used to automatically update the intra-class variation in an operational data. The advantages are training data are limited

and input data of the temporal variations through adaptation are tracked. It has a significant attention from the research community. The main aim is gain the momentum to circulate the key advantage. This system need not to collect the biometric samples in a larger size. This convenience will reduce the maintenance of the biometrics system because it does not take larger or more biometric inputs.

II. Related Work

Kalian Veeramachaneni Lisa Ann Osadciw [1] proposed a method on adaptive multiple modal biometric management algorithm. The author proposes a decision level fusion technique, it describes the sensor management algorithm and in which manner the framework is applied in the security applications. This framework uses N biometrics sensors, mission manager, Particle Swarm Optimization (PSO) and Bayesian Decision Fusion Processor. PSO is the key success for the AMBM framework, which uses those sensors and identifies the optimal rule for each biometrics sensor by selecting the threshold value. The Bayesian Decision Fusion Processor is mainly used to combine the decision from multiple sensors and optimal fusion rule from PSO. The rules generated are ALLONE's which gives an optimal solution. AND, OR and NAND are the mostly used fusion rules which gives a poor performance.

Padma Polash Paul, Marina L. Gavrilova and RedaAlhajj [2] proposed a Multimodal Biometrics in decision level fusion using Social Network Analysis. Step 1: Feature extraction using Principal Component Analysis (PCA), here dimensionality of the input image is reduced and Fisher Linear Discriminant Analysis (FLDA), it is a mixture of Linear Discriminant Analysis and Principal Component Analysis . K-Nearest classifier is used to generate the similarity score and results the top matches by calculating the majority vote of the neighbours in the database. Step 2: Social network construction – Euclidian distance of the each biometric traits are calculated among the features. Match scores are generated using the Euclidian distance and those values are normalized to zeros and ones. SNA is mainly used to develop the confidence of the classifier. The metrics used to improve the confidences.

MayankVatsa, Richa Singh, AfzelNoore [3] proposed Unification of Evidence-Theoretic Fusion Algorithms: the existing fusion approaches in level-2 and level-3 fingerprint features are non-adaptive and it won't give a sure guarantee optimum performance improvements. In the first approach, proposed rule based unification framework to select an appropriate fusion algorithm. First, by using a feature extraction algorithm features are extracted which are all converted into belief assignment as Basic Probability Assignment. Secondly fusion, Sum Rule Fusion algorithm is used whether the condition is satisfied else Generalized Belief Assignments are generated using Evidence Theoretic Dezert Smarandache (DSm) theory fusion, finally decisions are made using Accept/Reject. Second approach is Adaptive Unification which uses 2v- GSVM classifier.

L. Mezai and F. Hachouf proposed a match Score-Level Fusion of Voice and Face Using Belief Functions and Particle Swarm Optimization. The proposed system consists of 4 steps: Step 1, using Denoeux and appriou models the match score generates of face and voice is converted into belief assignment. Step 2, Using PSO confidence factor is estimated. In general PSO with populated particles are randomly distributed over search space. Step 3, Using DS theory and PCR 5 combine rules the generated masses are combined to fuse face and voice modalities. Step 4, Decision is about accepting or rejecting the legal user using statistical classification technique.

SumitShekhar, M. Patel, Nasser M. Nasrabadi and Rama Chellappa proposed Joint Sparse Representation for Robust Multimodal Biometrics Recognition. Here it contains 2 major steps; feature level extraction- pre-processing is carried out the using Gabor filter features are extracted from the pre-processed image. Circular tessellation around the core points are extracted for all the filtered images. Next fusion technique, Joint Sparsity- Based Multimodal Biometrics Recognition contains some C – class specification and D modalities, the main aim is to find the class belongs to which test sample belongs to Y. Multimodal Multivariate Sparse Representation which is used to find the coefficients of joint sparsity from different biometric trait that makes joint decision. Robust Multimodal Multivariate Sparse Representation it generate a more general problem in which data are contaminated by noise, finally the robust fusion is made.

III. Methodology

In this paper, the main idea is to fuse 4 different biometric traits such as fingerprint, palm, iris and retina. Step 1, the process extracts the features of the different trait. Step 2, extracted features are fused by a combo (fingerprint, palm and iris, retina) by using Discrete Wavelet Transformation method. Step 3, a classifier is used to generate a match score for each fused trait. Step 4, it fuses the score generated by a classifier by using Discrete Wavelet Transformation.

A. Feature Extraction

Fingerprint, it is one of the more sensitive area in which minutiae feature is extracted that contains ridges and bifurcation. To process the image first grey scale image is converted binary image using the function im2bw (I, level). The output image is enhanced using the histogram equalizer method using the function histeq(). Fingerprint image is then thinned sing the function bwmorph ('thin',inf), it removes the boundary pixels of the object without breaking the object apart and these features can be extracted by using four functions.

Ridgeorient()

This function is used to find the orientation of the ridges and bifurcation in a fingerprint. First need to find the gradient of the image. Image gradient is a directional change in the intensity or colour in an image. There will be an even flow from low to high, higher value(1) indicates white colour and lower value(0) contains dark colour. Image gradient returns 2 arguments.

Gmag=$\sqrt{Gx^2 + Gy^2}$

Gdir- €=atan2(Gx,Gy).

Covariance data for the image gradients

Gxx = Gx.^2;

Gyy = Gy.^2;

Gxy = Gx.*Gy;

Ridgesegment()

It normalises the fingerprint image and segments the ridge and bifurcation region. This function normalises the binary thinned image value to have zero and unit standard deviation of the ridge region.

Normalization:

if ~isa(im,'double'), im = double(im); end

n = im - min(im(:));

n = n/max(n(:));

Segmentation:

It breaks the fingerprint image into modules of size i.e blocksize x block size and each region is verified with the standard deviation if it is above the threshold value means then it is the deemed part of the fingerprint.

Ridgefreq()

Frequencies of the ridges are estimated across the fingerprint image by deciding the ridge counts with in each block of the image.

Δ+(t)=v+tcotα with t>0; v- Orientation value.

Δ-(t)=v-tcotα with t<0; α- Orientation around v.

Ridgefilter()

By using the above computed values of ridgeorient, ridgefreq and ridgesegment, we can do filtering to enhance the fingerprint image. First filter orientation is processed by dividing the orientation into 180 degree, next need to find the valid frequency data that is nearest to 0.01. it converts the orientation matrix from radians to an index value to filter the fingerprint. Finally the relevant ridge and bifurcations are extracted.

Palmprint extraction

By using Region of Interest (ROI) we can extract the features. Firstly need to apply the Gaussian filter the palmprint image to remove the noise around the required feature and also it is used to smooth the image.

Gaussian Filter:

G(x,y)=$\frac{1}{2\pi\alpha^2} e^{-x^2+\frac{y^2}{2\alpha^2}}$

Next convert the output image into binary image using the method.

BW = im2bw(C, graythresh(C));

The boundaries are detected using the method.

[B,~,~] = bwboundaries(BW);

Centroid of the image can be located using the function regionprops(BW,'centriod');. It uses regionline and ouline to find the centroid. In which features such as central line, headline and

Outline- Edges are stored.

Regionline = [outline(i,2) outline(i,1) sqrt((outline(i,2) centroid(1))^2+(outline(i,1)

centroid(2))^2)];

it has 2 coordinates centroid x and centroid y, we need to sort the coordinates from top to bottom of the image. By using the distance we can reject the point based on score generated. Then apply rotation to find the centroid. The extracted features are centre line heart line and middle line.

Iris feature extraction

Iris, here central part of the iris retina is extracted by using k means segmentation that part is extracted.

Retina feature extraction

Retina, by using blood vessel segmentation algorithm blood vessel of the retina is extracted by using Kirsch's Template. The user takes single mask and 45 degree increments are rotated in all possible 8 compass directions. Output values are taken in which the template has a bigger value from all template and edges are extracted later.

hn,m=max($gij^z.fn + i, m + j$)

h1=[5 -3 -5;
-3 0 -3;
5 -3 -3]/15;
h2=[-3 5 -3;
-3 0 5;
-3 -3 5]/15;
h3=[-3 -3 -5;
5 0 -3;
5 5 -3]/15;
h4=[-3 5 5;
-3 0 -3;
-3 -3 -3]/15;
h5=[-3 -3 -3;
-3 0 -3;
5 5 5]/15;
h6=[5 -3 5;
-3 0 -3;
-3 -3 -3]/15;
h7=[-3 -5 -3;
-3 0 5;
-3 -3 5]/15;
h8=[-3 5 -3;
5 0 -3;
5-3 -3]/15;

Convolution (conv2):

It returns the middle portion of the matrix in the convolution of the same size as A.

Example

A = rand (3); B = rand(4); C = conv2(A,B)

Cs = conv2 (A,B,'same')

Cs = 2.3576 3.1553 2.5373
3.4302 3.5128 2.4489
1.8229 2.1561 1.6364

Finally blood vessel of a particular retina is extracted using the above function. Hence by these four methods the four biometric traits features are extracted.

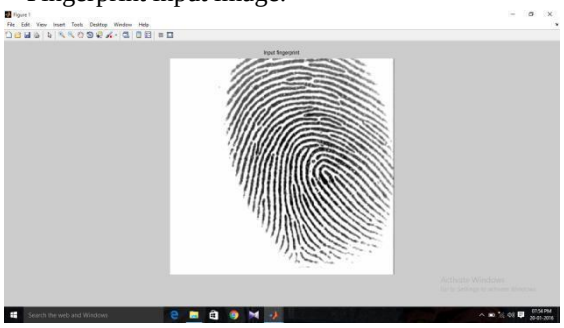
B. Multimodal biometric fusion

By using Discrete Wavelet Transform (DWT) fusion method, it combines the 2 biometrics for example fingerprint,

palmprint and iris, retina. It uses the function wavedec2 (), here the wavelet decomposition of the matrix is returned for all fingerprint, palm, iris and retina. After fusing these features we need to calculate the similarity score. Next by using neural network we train the images in the database, test the images according to the trained image by its match score and its similarity finally matched images are fused once again with DWT.

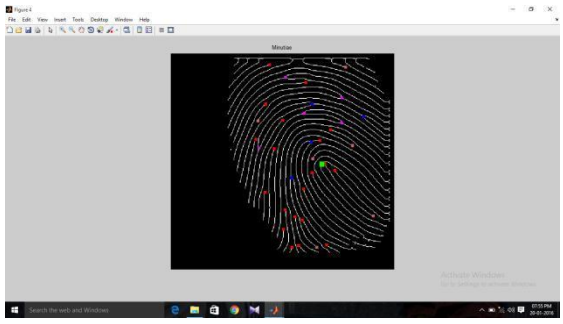
IV. EXPERIMENTAL RESULTS

Fingerprint input image:



Minutiae extracted fingerprint image:

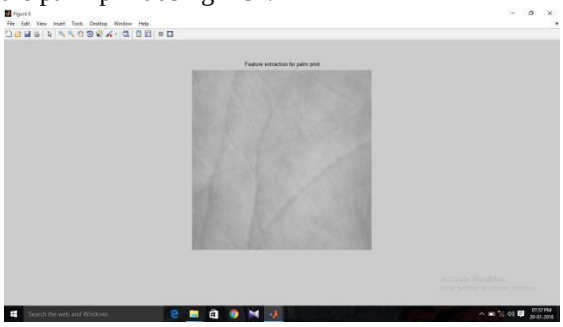
It contains both ridge and bifurcation which is denoted in different colours.



Palmprint input image

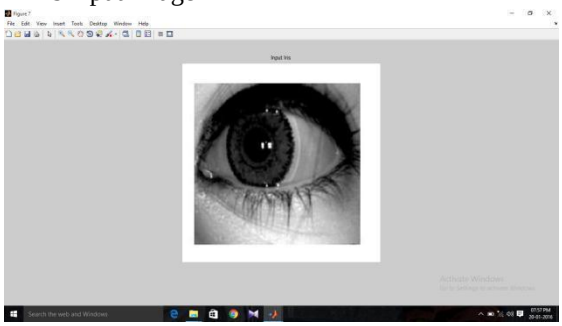
Extracted palmprint image:

It contains central, heart and head lines are the features of the palm print using ROI.

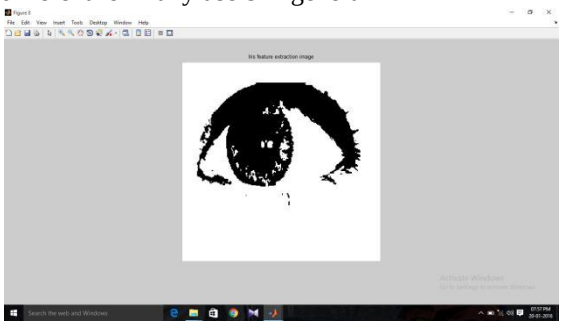


Iris

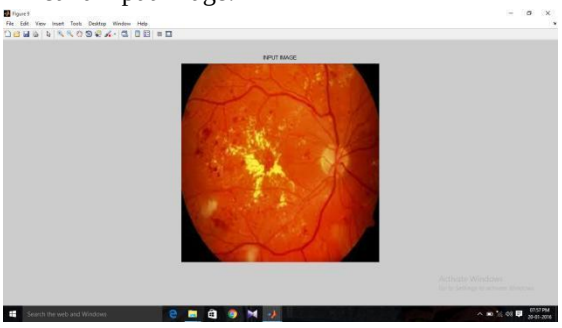
Iris input image



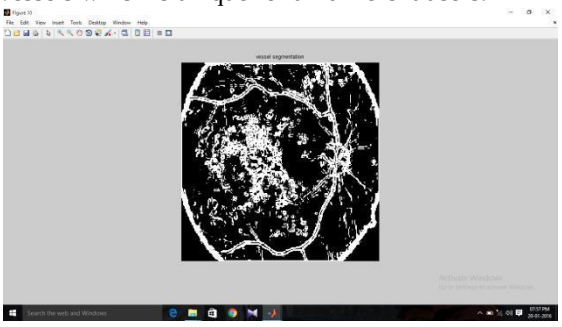
Iris extracted feature retina and eye lashes which will be different for many users in general



Retina input image:



Retina feature extracted image which contains only blood vessels which is unique for all different users.



By using Discrete Wavelet Transformation fingerprint, palm and iris, retina values are fused.

V. CONCLUSION

The domain of multimodal biometrics is new and existing

research area in the information science and they are used to understand the traits, accurate methods and personal reliable information representation of decision making and matching. There is a significance increment in activity over research to understand the biometric information system utilization and representation for decision making which can be used as public and security systems and mainly used to understand the complex processes behind biometric matching and recognition. In future the modelling techniques against forgeries more robust and efficient performance over fusion at decision level fusion. More than two traits cannot be used to identify and difficult to find the forgeries.

REFERENCES

[1] Padma Polash Paul, Marina L. Gavrilova, and RedaAlhajj "Decision fusion for multimodal biometrics using social network analysis" IEEE transactions on systems, man, and cybernetics: systems, vol. 44, no. 11, november 2014.

[2] A. K. Jain and A. Ross, "Fingerprint mosaicking," in Proc. IEEE Int. Conf. Acoust. Speech Signal Process, vol. 4.Orlando, FL, USA, 2002,pp. 4064–4067.

[3] C. Sanderson and K. K. Paliwal, "Polynomial features for robust face authentication," in Proc. IEEE Int. Conf. Image Processing (ICIP), vol. 3. 2002, pp. 997–1000.

[4] KalyanVeeramachaneni, Lisa Ann Osadciw, and Pramod K. Varshney "An Adaptive Multimodal Biometric Management Algorithm" IEEE transactions on systems, man, and cybernetics—part c: applications and reviews, vol. 35, no. 3, august 2005.

[5] L. Hong and A. Jain, "Integrating faces and fingerprints for personal identification," IEEE Trans. Pattern Anal. Machine Intell., vol. 20, no. 12, pp. 1295–1307, Dec. 1998.

[6] S. Prabhakar and A. Jain, "Decision-level fusion in fingerprint verification," Pattern Recognit., vol. 35, pp. 861–874, Feb. 2002.

[7] MayankVatsa, ,Richa Singh, and AfzelNoore, "Unification of Evidence-Theoretic Fusion Algorithms: A Case Study in Level-2 and Level-3 Fingerprint Features" IEEEtransactions on systems, man, and cybernetics—part a: systems and humans, vol. 39, no. 1, january 2009.

[8] J. Dezert, "Foundations for a new theory of a plausible and paradoxical reasoning," Inform. Security J., vol. 9, pp. 13–57, 2002.

[9] F. Smarandache and J. Dezert, Advances and Applications of DSmT for Information Fusion. Rehoboth, NM: Amer. Res. Press, 2004.

[10] L. Mezai and F. Hachouf "Score-Level Fusion of Face and Voice Using Particle Swarm Optimization and Belief Functions" IEEE transactions on human-machine systems.

[11] F. Alsaade, "Score-level biometric fusion," Ph.D. dissertation, Faculty of Engineering and Information Sciences,Hertfordshire Univ., Hertfordshire, U.K., 2008.

[12] Q. Bai, "Analysis of Particle swarm optimization," Comput. Inf. Sci., vol. 3, no. 1, pp. 180–184, Feb. 2010.

[13] SumitShekhar, Vishal M. Patel, Nasser M. Nasrabadi, and Rama Chellappa "Joint Sparse Representation for Robust Multimodal Biometrics Recognition" IEEE transactions on pattern analysis and machine intelligence, vol. 36, no. 1, january 2014