ISSN:0975-9646

A Multimodal Approach to Biometric Recognition

Richie M. Varghese

Department of Electronics and Telecommunication,
Maharashtra Institute of Technology,
University of Pune
Pune, Maharashtra, India

***Abstract*— Biometric recognition refers to an automatic recognition of individuals based on feature vectors derived from their physiological and behavioural characteristics. Biometric recognition systems should provide a reliable personal recognition scheme to either confirm or determine the identity of an individual. Applications of such a system include computer systems security, secure electronic banking, mobile phones, credit cards, secure access to buildings, health and social services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. A multimodal system could be a combination of fingerprint verification, face recognition, voice verification and smart-card or any other combination of biometrics. This enhanced structure takes advantage of the proficiency of each individual biometric and can be used to overcome some of the limitations of a single biometric. The fusion is performed at classifier or decision level using different algorithms. Performance of the developed system is then evaluated on a database with fingerprints/palm-prints from different people.**

***Keywords*— Biometrics, feature extraction, classification, multimodal, fusion.**

I. Introduction

Biometrics refers to the science and technology of measuring and analysing human body characteristics such as DNA, fingerprints, eye retinas, voice patterns, facial patterns, etc. for authentication purposes.

Any human physiological and/or behavioural characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- Universality: each person should have the characteristic.
- Distinctiveness: any two persons should be sufficiently different in terms of the characteristic.
- Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
- Collectability: the characteristic can be measured quantitatively.

A. Biometric System

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode.

- In the verification mode, the system validates a person’s identity by comparing the captured biometric data with her own biometric template(s) stored in the system database.
- In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match.

B. Fingerprint

From different researches it has been observed that no two persons have the same fingerprints, they are unique for each individual. They are hence considered the most popular type of biometric recognition method. Fingerprints have remarkable permanency and uniqueness throughout the time. From observations we conclude that the fingerprints offer more secure and reliable personal identification than passwords, id-cards or key can provide. Examples such as computers and mobile phones equipped with fingerprint sensing devices for fingerprint based password protection are being implemented to replace ordinary password protection methods.

A fingerprint is the composition of many ridges and furrows. But finger prints cannot be distinguished by their ridges and furrows. They can be distinguished by Minutia, which are some abnormal points on the ridges.

C. Palm-print

A palm print refers to an image acquired of the palm region of the hand. It can be either an online image (i.e. taken by a scanner or CCD) or offline image where the image is taken with ink and paper.

The palm itself consists of principal lines, wrinkles (secondary lines), and epidermal ridges. It differs to a fingerprint in that it also contains other information such as texture, indents and marks which can be used when comparing one palm to another.

Because fingerprints and palms have both uniqueness and permanence, they have been used for over a century as a trusted form of identification. However, palm recognition has been slower in becoming automated due to some restraints in computing capabilities and live-scan technologies.

II. SYSTEM SCHEMATIC

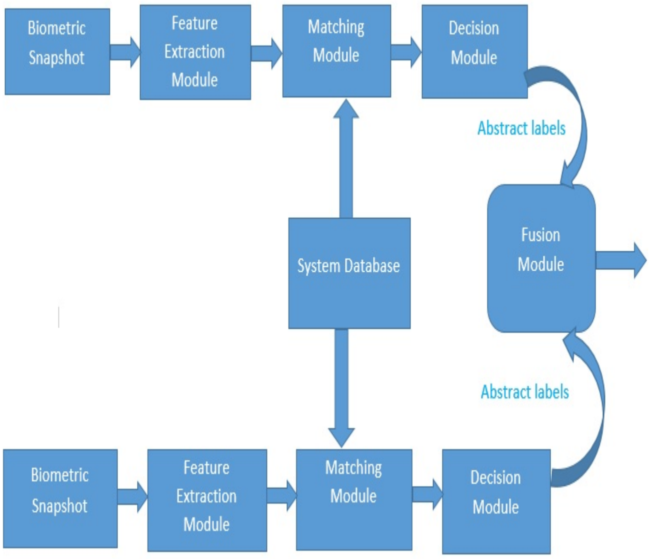


Fig.1 System block diagram

A. Biometric Sensor

A Biometric sensor is an electronic device used to capture a digital image of the biometric pattern. The most commonly used types of sensors include optical sensors, solid state sensors and ultrasound sensors.

B. Pre-processing

Input image is pre-processed which involves three sub stages such as:-
1) Image enhancement
2) Image binarization
3) Image segmentation

C. Feature Extraction Method

In the feature extraction module, the pre-processed image is used to extract the features. The feature extraction algorithms are applied to get feature vector of the biometric image. According to the biometrics selected and its application the feature extraction technique can be applied.

D. Matching Module

The stored templates are matched against the input templates to be recognized. The matching operation determines the degree of similarity between two vectors. A template matcher can combine multiple information sources.

E. System Database

In this process standard templates are stored with which the input image is compared and the result is given to the decision module.

F. Decision Module

It makes the final decision about whether to accept or reject the user.

III. SYSTEM DESIGN

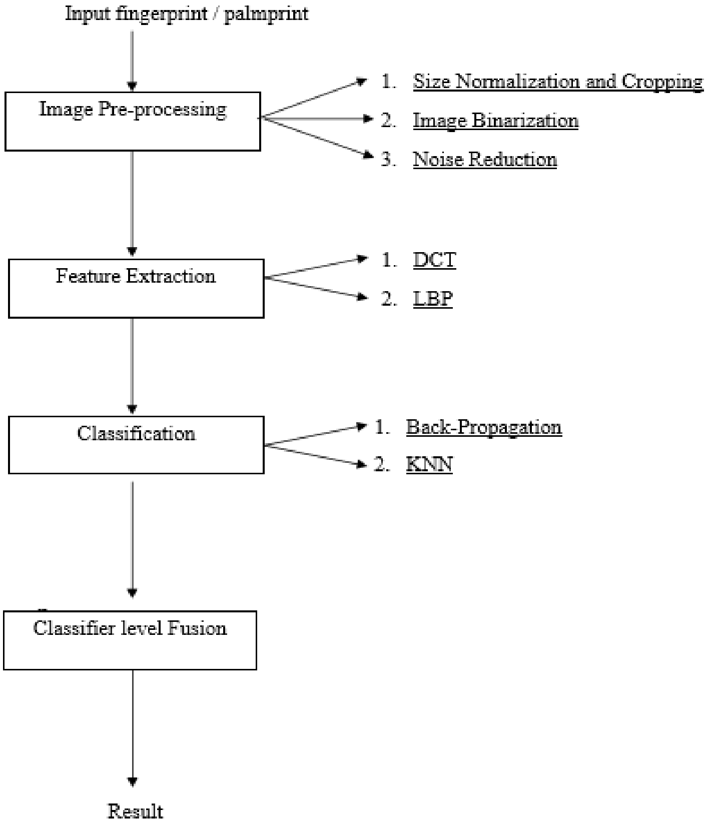


Fig.2 System design

A. Pre-processing Techniques

Pre-processing techniques are needed on colour, grey-level or binary document images containing text and graphics. In fingerprint recognition systems most of the applications use grey or binary images since processing colour images is computationally high.

1) *Image Enhancement:*

Image enhancement improves the quality of images for human perception by removing noise, reducing blurring, increasing contrast and providing more detail.

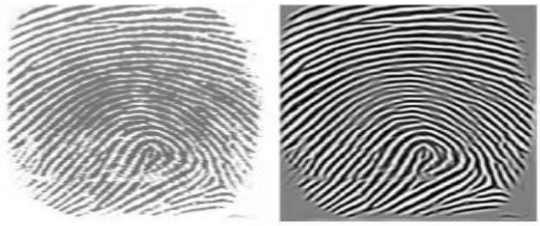


Fig.3 Original and enhanced image

2) *Image Binarization :*

In Binarization, the grey scale image is converted into binary image. Binary images are easy to process. The basic principle of converting an image into binary is to decide a threshold value, and then the pixels whose value are more than the threshold are converted to white pixels, and the pixels whose value are below or equal to the threshold value are converted to black pixels.

3) *Image Segmentation :*
After image enhancement the next step is fingerprint image segmentation. In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges and furrows is first discarded since it only holds background information. Then the bound of the remaining effective area is sketched out since the minutiae in the bound region are confusing with those spurious minutiae that are generated when the ridges are out of the sensor.

B. Feature Extraction Methods

Feature extraction and selection can be defined as extracting the most representative information from the raw data, which minimizes the within class pattern variability while enhancing the between class pattern variability. For this purpose, a set of features are extracted for each class that helps distinguish it from other classes, while remaining invariant to characteristic differences within the class. For the purpose of automation, a suitable representation i.e. feature extraction of fingerprints is essential. This representation should have the following properties: a) Retention of discriminating power of each fingerprint at several levels of resolution; b) Easy computability; c) Amenable to automated matching algorithms; d) Stable and invariant to noise and distortions; e) Efficient and compact representation. Here we have used two feature extraction methods:

- Discrete cosine transform
- Local Binary Patterns

1) *Discrete Cosine Transform (DCT) :*
Discrete Cosine Transform (DCT) has mostly used in the area of image processing, its basic operation is to take a signal and transform it from one type of representation to another, in this case the signal is a block of an image. The concept of this transformation is to transform as set of points from the spatial domain into an identical representation in a frequency domain. The two dimensional DCT then can be written in terms of pixel values f(i,j) for i,j =0,1,.............N-1 and the frequency-domain transform coefficients F(u,v) would be

$$F(u,v) = \frac{1}{\sqrt{2N}} c(u)c(v) \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i,j)$$

$$\times \cos\left[\frac{(2i+1)u\pi}{2N}\right] \cdot \cos\left[\frac{(2j+1)v\pi}{2N}\right] \quad .. (1)$$

For u,v =0,1,...,N-1

Where

$$C(u),c(v) = \begin{cases} \frac{1}{\sqrt{2}} & \text{For } u,v=0 \\ 1 & \text{Otherwise} \end{cases}$$

In order to extract the features of fingerprint image, block DCT-based transformation is employed. Each image is divided into sub blocks with (N x N) size. There are n x n coefficients in each block after DCT is applied. Only some of the DCT coefficients are to be computed for feature extraction, and they are enough to represent the information that are needed from the block.

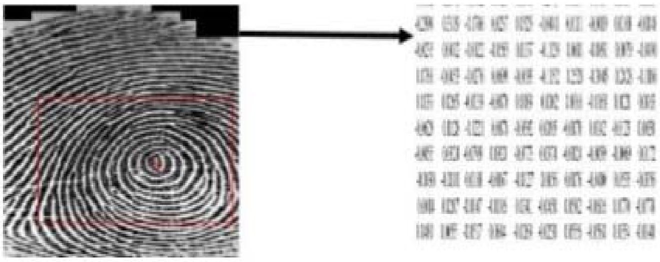


Fig.4 Feature extraction using DCT

2) *Local Binary Patterns (LBP) :*
Local Binary Pattern (LBP) is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighbourhood of each pixel and considers the result as a binary number. Due to its discriminative power and computational simplicity, LBP texture operator has become a popular approach in various applications. The most important property of the LBP operator in real-world applications is its robustness to monotonic gray-scale changes caused, for example, by illumination variations. Another important property is its computational simplicity, which makes it possible to analyse images in challenging real-time settings.

The LBP feature vector, in its simplest form, is created in the following manner:

- Divide the examined window into cells (e.g. 16x16 pixels for each cell).
- For each pixel in a cell, compare the pixel to each of its 8 neighbours (on its left-top, left-middle, left-bottom, right-top, etc.). Follow the pixels along a circle, i.e. clockwise or counter-clockwise.
- Where the centre pixel's value is greater than the neighbour’s value, write "1". Otherwise, write "0". This gives an 8-digit binary number (which is usually converted to decimal for convenience).
- Compute the histogram, over the cell, of the frequency of each "number" occurring (i.e., each combination of which pixels are smaller and which are greater than the centre).
- Optionally normalize the histogram.
- Concatenate (normalized) histograms of all cells. This gives the feature vector for the window.

C. Classification Techniques

1) *K-Nearest Neighbours (KNN) :*
The principle behind nearest neighbour methods is to find a predefined number of training samples closest in distance to the new point, and predict the label from these.

KNN classifier is best suited for classifying persons based on their images due to its lesser execution time and better accuracy than other commonly used methods. Although methods like SVM and Adaboost algorithms are proved to be more accurate than KNN classifier, KNN classifier has a faster execution time and is dominant than SVM.

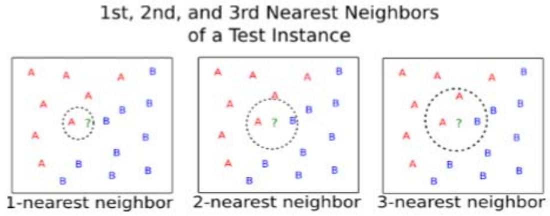
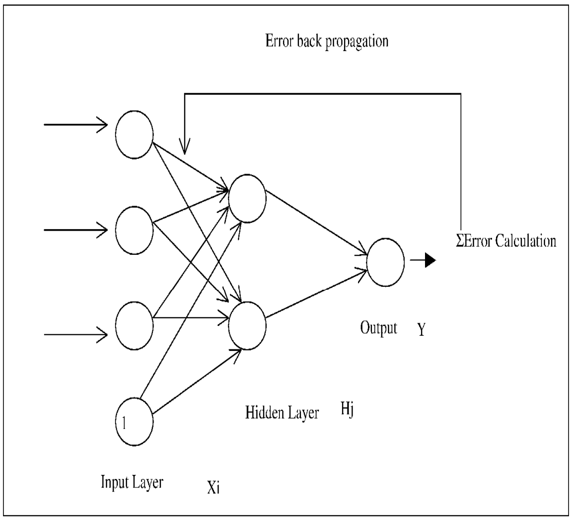


Fig.5 Classification using KNN

2) Back Propagation Neural Network (BPNN) :

Artificial Neural networks have been proved very effective in performing complex function in various fields. The ability of the BPNN to learn given patterns makes them suitable for such applications. Fingerprint recognition is one such area that can be used as a means of biometric verification where the BPNN can play a critical rule. BPNN can be configured and trained to handle such variations observed in the texture of the fingerprint.

Firstly the neural network has been trained before test the matching operation. Extracted features of all the images in the data set are the input of the neural network. With the help of these inputs the network has been trained and the network should be trained till then we get the minimum MSE value so that the desired number of true results can be obtained. For training the network, MATLAB neural network toolbox has been used.

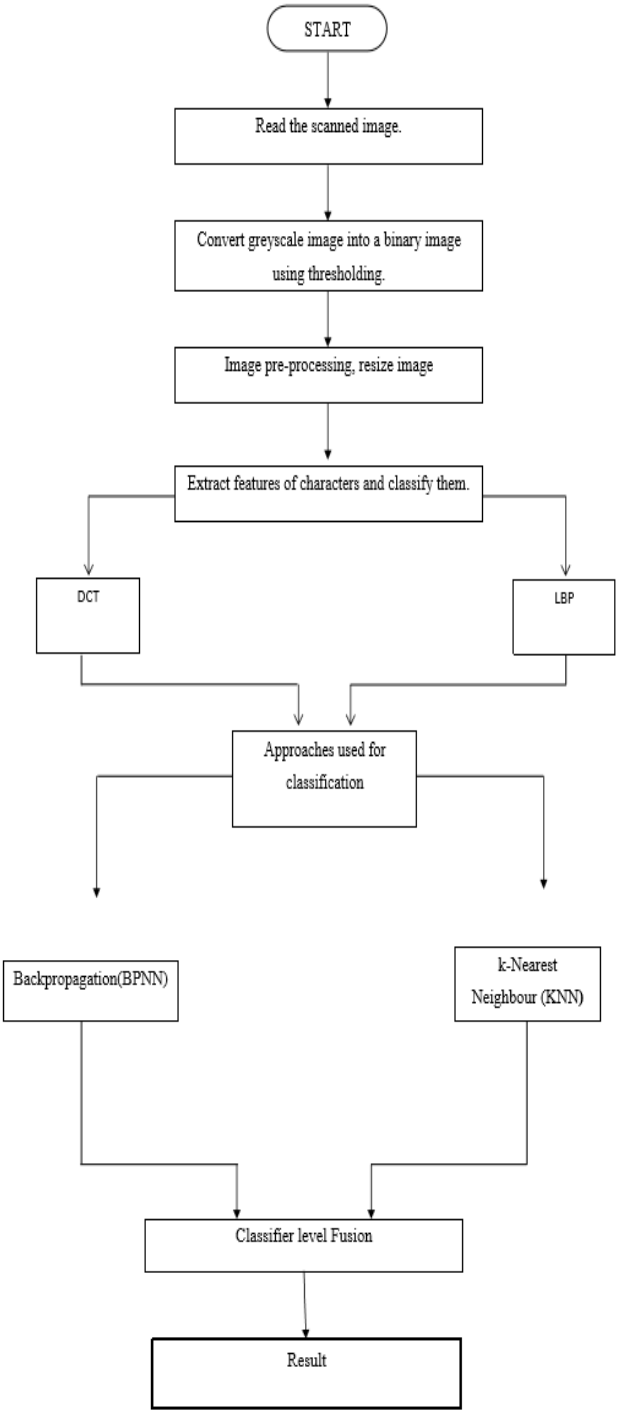


Notes: The weight connecting node *i* in the input layer to node *j* in the hidden layer is denoted by *Wji*, and the weight connecting node *j* to the output node is represented by *Vj*

Fig.6 Backpropagation neural network

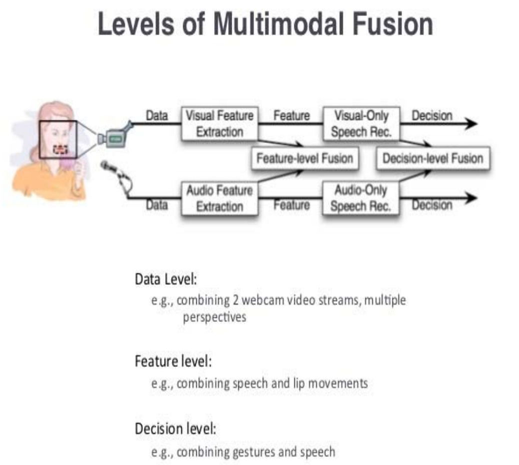
The recognition performance of Back Propagation network highly depends on the structure of the network and training algorithm. Feed forward back propagation neural network has been selected to train the network. The number of nodes in input, hidden and output layers will determine the network structure. All the neurons of one layer are fully interconnected with all neurons of its just preceding and just succeeding layers (if any). The network consists of 50 nodes in the input layer (corresponding to one feature in each of the50 zones). The output layer has 25 neurons corresponding to 4 images. Therefore, only the number of hidden layer nodes needs to be determined. The number of hidden nodes will heavily influence the network performance. We have arrived at 25 neurons for the hidden layer.

IV. IMPLEMENTATION OF THE SYSTEM


START
Read the scanned image.
Convert greyscale image into a binary image using thresholding.
Image pre-processing, resize image
Extract features of characters and classify them.
DCT
LBP
Approaches used for classification
Backpropagation(BPNN)
k-Nearest Neighbour (KNN)
Classifier level Fusion
Result

A. Multimodal Fusion

A multimodal approach uses a fusion technology where information from various unimodal approaches is combined. Pre-classification fusion refers to combining information prior to the application of any classifier or matching algorithm. In post classification fusion, the information is combined after the decisions of the classifiers have been obtained.


Levels of Multimodal Fusion

Data Level:
e.g., combining 2 webcam video streams, multiple perspectives

Feature level:
e.g., combining speech and lip movements

Decision level:
e.g., combining gestures and speech

Fig.7 Levels of multimodal fusion

Prior to classification/matching, integration of information can take place either at the sensor level or at the feature level. The raw data from the sensors are combined in sensor level fusion. For example, the face images obtained from several cameras can be combined to form a single face image. In sensor level fusion, the data obtained from the different sensors must be compatible, and this may not always be possible (e.g., it may not be possible to fuse face images obtained from cameras with different resolution). Feature level fusion refers to combining different feature vectors that are obtained by either using multiple sensors or employing multiple feature extraction algorithms on the same sensor data. Integration of information at the abstract or decision level can take place when each biometric matcher individually decides on the best match based on the input presented to it. Methods like majority voting, behaviour knowledge space, weighted voting, AND rule and OR rule, etc. can be used to arrive at the final decision.

B. Fusion at Classifier Level

It is often observed that different classifiers with essentially the same overall accuracy misclassify different test patterns. In decision level fusion, each classifier operating under a binary hypothesis, applies a threshold on the match score and renders its decision regarding the presence (=1) or absence (=0) of a genuine individual. The decisions from multiple classifiers are then fused in order to generate the final decision. Fusion at the decision-level is bandwidth efficient since only decisions, requiring a single bit, are transmitted to the fusion engine. Moreover, most commercial biometric classifiers grant access to decision-level information rather than score-level or feature-level information. Achieving optimality at the decision level, however, involves the selection of optimal decision thresholds and a fusion rule that minimize the classification error.

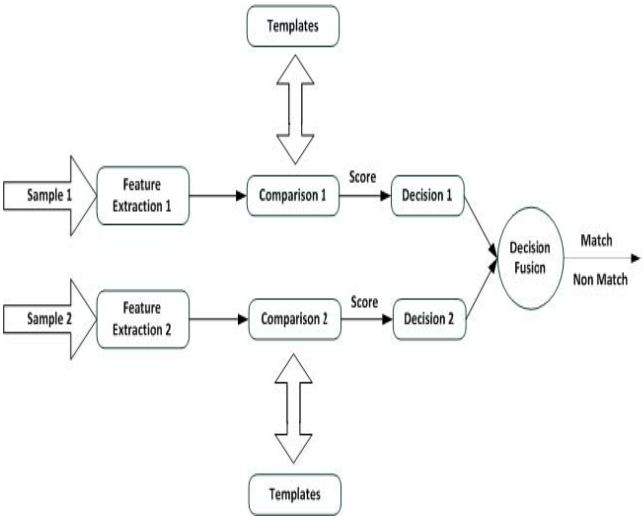


Fig.8 Classifier level fusion

1) Majority voting algorithm

In majority voting algorithm, we simply take the majority rule of the predictions by the classifiers. E.g., if the prediction for a sample is -

- classifier 1 -> class 1
- classifier 2 -> class 1
- classifier 3 -> class 2

- we would classify the sample as "class 1."

2) Weighted majority algorithm

In weighted majority algorithm, we add a weights parameter, which lets us assign a specific weight to each classifier. In order to work with the weights, we collect the predicted class probabilities for each classifier, multiply it by the classifier weight, and take the average. Based on these weighted average probabilities, we can then assign the class label.

C. Testing of Fingerprint/Palm-print

This is the final step of the proposed work. To test or recognize the fingerprint or palm-print first take any image from the data set and feed that image to the trained network then it gives the result by showing whether it matches to the right person or wrong.

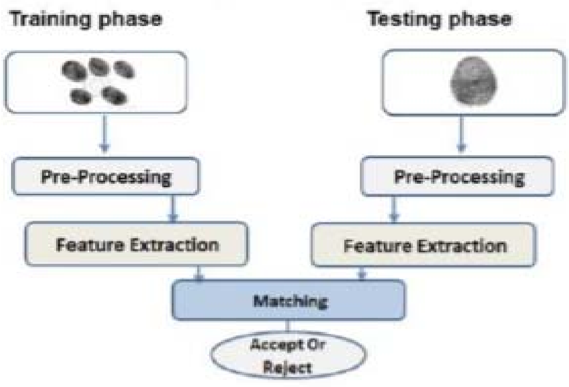
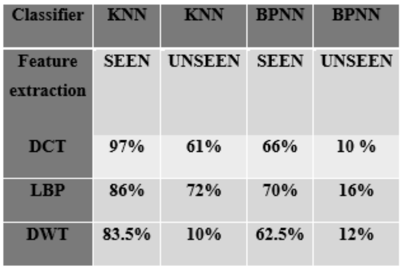


Fig.9 Training and testing of images

V. EXPERIMENTAL RESULTS

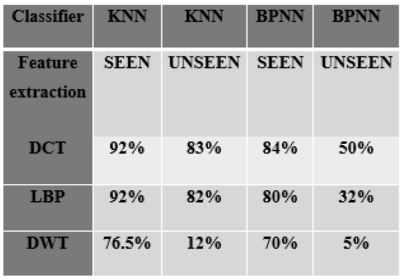
A. Efficiency of feature extraction methods and classifiers

Fingerprint:



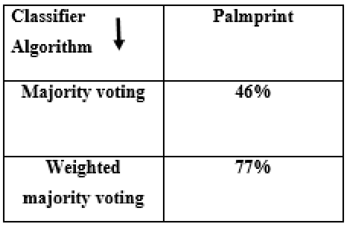
Classifier	KNN	KNN	BPNN	BPNN
Feature extraction	SEEN	UNSEEN	SEEN	UNSEEN
DCT	97%	61%	66%	10 %
LBP	86%	72%	70%	16%
DWT	83.5%	10%	62.5%	12%

Palmprint :



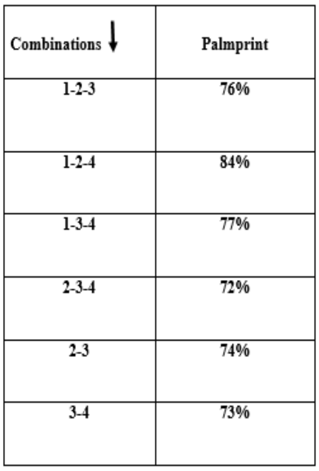
Classifier	KNN	KNN	BPNN	BPNN
Feature extraction	SEEN	UNSEEN	SEEN	UNSEEN
DCT	92%	83%	84%	50%
LBP	92%	82%	80%	32%
DWT	76.5%	12%	70%	5%

B. Fusion at Classifier Level

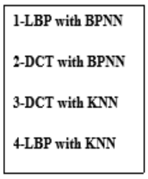


Classifier Algorithm ↓	Palmprint
Majority voting	46%
Weighted majority voting	77%

C. Combinations using weighted majority algorithm



Combinations ↓	Palmprint
1-2-3	76%
1-2-4	84%
1-3-4	77%
2-3-4	72%
2-3	74%
3-4	73%



1-LBP with BPNN
2-DCT with BPNN
3-DCT with KNN
4-LBP with KNN

The new multimodal approach using fingerprint and palm-print based on classifier level fusion has been evaluated. Experimental results indicate that a multimodal biometric system, which combines multiple biometric data, can achieve significantly better performance compared to a single biometric system. The system is implemented using the feature extraction method and classification method with the best accuracy, which is observed to be DCT with KNN according to the test results shown above.

Images of fingerprints and palm-prints fifty individuals are provided as input to the system. After pre-processing of input images, they are compared with the already pre-processed images of the same individuals in the template database. If the person is recognised correctly, the corresponding identity of the individual is displayed as the result, whereas if the person cannot be recognized due to technical errors, the result is displayed incorrectly or as null.

VI. CONCLUSION

Biometric systems offer several advantages over conventional authorization methods. This work focuses on using a multimodal approach to biometrics by fusing individual features of two traits, fingerprint and palm-print at the classifier level in order to develop an authentication system. Experiments are conducted to evaluate and analyse the performance of different feature extraction and classifier methods in order to create the most accurate and efficient system.

The reliability of any automatic biometric system strongly relies on the precision obtained in the feature extraction process. A number of factors damage the correct matching of fingerprints. Among them, poor image quality is the one with most influence. There is a scope of further improvement in terms of efficiency and accuracy which can be achieved by improving the hardware to capture the image or by improving the image enhancement techniques so that the input image to the thinning stage could be made better and could hence improve the future stages and the final outcome.

REFERENCES

[1]. Xiaoxin Xu Mingguang and et al, " Outdoor Wireless [1]L. Hong, Y.Wan, and A. K. Jain, “Fingerprint image Enhancement: Algorithm and Performance Evaluation,” IEEE Trans. Pattern Anal. Machine Intell.

[2] The Use of Two Transform Methods in Fingerprints Recognition Ismail Taha Ahmed Salah Sleibi Al-Rawi Khattab M. Ali Baraa Tareq Hammad University of Anbar - College of Computer.

[3] A KNN Research Paper Classification Method Based on Shared Nearest Neighbor - Yun-lei Cai, Duo Ji ,Dong-feng Cai Natural Language Processing Research Laboratory, Shenyang Institute of Aeronautical Engineering.

[4] Recognition of Fingerprints Enhanced by Contour let Transform with Artificial Neural Networks Adem Alpaslan ALTUN* and Novruz ALLAHVERDI, Department of Computer Systems Education, Technical Education Faculty, Selcuk University

[5] “Study of Local Binary Pattern for partial fingerprint identification”, IJMER – Miss Harsha V. Talele, Pratvina V. Talele.

[6] M.Kawagoe and A.Tojo, "Fingerprint pattern classification" Pattern Recognition,vol. 17, no. 3, pp. 295- 303, 1 K.Nandakumar,A.Ross, and A.K.Jain,"Incorporating ancillary information in multibiometric systems" Handbook of Biometrics.New York: Springer- Verlag, pp. 335-355, 2007.

[7] K. Nallaperumall, A. L. Fred and S. Padmapriya, “A Novel for Fingerprint Feature Extraction Using Fixed Size Templates”, IEEE 2005 Conference, pp. 371-374, 2005

[8] D. Maio, and D. Maltoni, “Direct gray-scale minutiae detection in fingerprints”, IEEE Transactions Pattern Analysis and Machine Intelligence, vol. 19(1), pp. 27-40, 1997.

[9] Digital Image processing using MATLAB” -by Steven L. Eddins

[10] Handbook of Fingerprint Recognition”, Springer, New York, pp. 141-144, 2003.

[11] Handbook of Fingerprint Recognition by Davide Maltoni, Dario Maio, Anil K. Jain & Salil Prabhakar

[12] Wikipedia link - http://en.wikipedia.org/wiki/Fingerprint_recognition