IJCTA, 10(02), 2017, pp. 427-435
© International Science Press

Human Identification by Fusing Face, Palm Iris

Prathap* K.S. Vairavel and S.Valarmathy*****

Abstract : Unimodal biometric system has involved various researchers and achieved great success. Unimodal system alone may not be able to meet the increasing necessity of high accuracy in today's biometric system. Single biometric systems suffer from many challenges such as noisy data, non universality and spoof attacks. Multimodal biometric systems can solve these limitations effectively by using two or more individual modalities. In this technique fusion of iris, palmprint and face traits are used in order to improve the accuracy, security of the system and to identify the human. The main purpose is to look over whether the combination of palmprint, iris and face biometric can achieve performance that may not be possible using a single biometric technology. Gabor filter, Local Binary Pattern (LBP) and Binary Particle Swarm Optimization(PSO) based algorithms is used for palm, iris and face images. Scores which obtained from the Kernel Nearest Neighbour (KNN) and Support Vector Machine (SVM) classifiers are normalized first using minmax normalization. This system offers the high performance and to overcome the limitation of single modal biometrics. This proposed system is produces more reliable results than the existing system.

Keywords : Multimodal biometrics, PSO, SVM, KNN.

1. INTRODUCTION

A. Biometrics

Biometrics is the science and technology to measure and analyze biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as Palmprints, palmprints, eye retina irises, voice patterns, facial patterns and hand geometry for authentication purposes.

There are three categories of user authentication such as passwords, Personal Identification Numbers (PINs), and token. The leading approach on current control access is via password or PIN, but the weaknesses are the clearly documented, if they are easy to remember, they are usually easy to guess and hack into, but it is difficult to attack, it is usually difficult to remember, a lot of people write them down and never change them.

The problem with tokens are that they authenticate their presence, but they can be easily forgotten, lost or stolen and as it happens with the credit cards, can be falsely duplicated. As a result, biometry appears as a good solution, which is normally used, in addition to the previous verification methods, to increase security levels. A further very well known and vital area of application is the one used by the police to identify suspects. Palmprints are the most commonly used ones.

* Second year, M.E.[Instrumentation Engineering] Department of Electronics and Instrumentation Engineering Bannari Amman Institute of Technology Sathyamangalam, Erode, India, *Prathap.ie15@bitsathy.ac.in*

** Assistant Professor, (Sr. Grade), Department of Electronics and Instrumentation Engineering Bannari Amman Institute of Technology Sathyamangalam, Erode, India, *eievairam@gmail.com*

*** Professor and Head of the Department Department of Electronics and Communication Engineering Bannari Amman Institute of Technology Sathyamangalam, Erode, India

The following are used for the performance metrics for biometric systems:

1. **False Accept Rate or False Match Rate (FAR or FMR) :** The possibility is that the system wrongly matches with the input pattern to non matching template that is in the database. It measures the percent of unacceptable inputs which are wrongly accepted. In case of similar scale, if the person is fraud in reality, but the matching score is high than the threshold, then he is treated as genuine that higher the FAR and hence the performance also depend upon the selection of the threshold value
2. **False Reject Rate or False Non Match Rate (FRR or FNMR) :** The possibility is that if the system fails to detect a match between the input pattern and a matching pattern in the database. It measures the available percent of valid inputs which are wrongly rejected
3. **Receiver Operating Characteristic or Relative Operating Characteristic (ROC) :** The ROC plot is a visual categorization of the trade off between the FAR and the FRR. In general, the matching algorithm will always performs a result based on a threshold which determines that how close a template input needs to be considered for a match. If the threshold is reduced, there will be smaller false non-matches but high false accepts. Likewise, a more the threshold will reduce the FAR but increases the FRR. A common variation is the Detection Error Trade off (DET), which is obtained using normal deviate scales on both axes. This more linear graph shows the differences for higher performances.
4. **Equal Error Rate or Crossover Error Rate (EER or CER):** The rate at which both accept and the reject errors are identical in the system the value of the EER can be easily obtained from the ROC curve. The EER is a rapid way to compare the accuracy of devices with different ROC curves. In general, the device with the highest EER is less accurate.
5. **Failure To Enroll Rate (FTE or FER):** The attempt to generate a template from an input is unsuccessful. This is most frequently caused by low quality inputs
6. **Failure To Capture Rate (FTC):** In the regular systems, the probability that the system fails to detect a biometric input when presented properly,

B. Multimodal Biometric System

Multimodal biometric systems make use of more than one physiological or behavioral characteristic for enrollment, authentication or recognition. The National Institute of Standards and Technology (NIST) report recommends a system employing numerous biometrics in a layered approach. It is to combine different modalities to improve identification rates. The aim of multi biometrics is to reduce one or more of the following:

1. False Accept Rate (FAR)
2. False Reject Rate (FRR)
3. Failure To Enroll rate (FTE)
4. Susceptibility to artifacts or mimics

Multimodal biometric systems obtain input from single or multiple sensors that measures two or more different modalities of biometric individuality. For example a system with palmprint and iris recognition would be considered as multimodal even if the OR rule is being applied, allowing users to be verified using either of the modalities.

1. **Multi Algorithmic Biometric Systems :** Multi algorithmic biometric systems obtain a single sample from a single sensor and process that with sample of two or more different algorithms.
2. **Multi Instance Biometric Systems :** Multi instance biometric systems uses one sensor or possibly more sensors to capture samples of two or more different instances of the same biometric uniqueness. Example capturing images from the multiple palms

3. **Multi Sensorial Biometric Systems :** Multi sensorial biometric systems test the same instance of a biometric trait with two or more clearly with different sensors. Processing of the multiple samples can be done with one algorithm or combination of algorithms. Example iris recognition application could use both a visible light camera and an infrared camera coupled with a specific frequency.

C. Basic Structure Of A Biometric System

Biometric verification requires for comparing a registered or enrolled biometric sample against a newly captured biometric sample. During employment, a sample of the biometric trait is captured, processed by a computer, and stored for later evaluation.

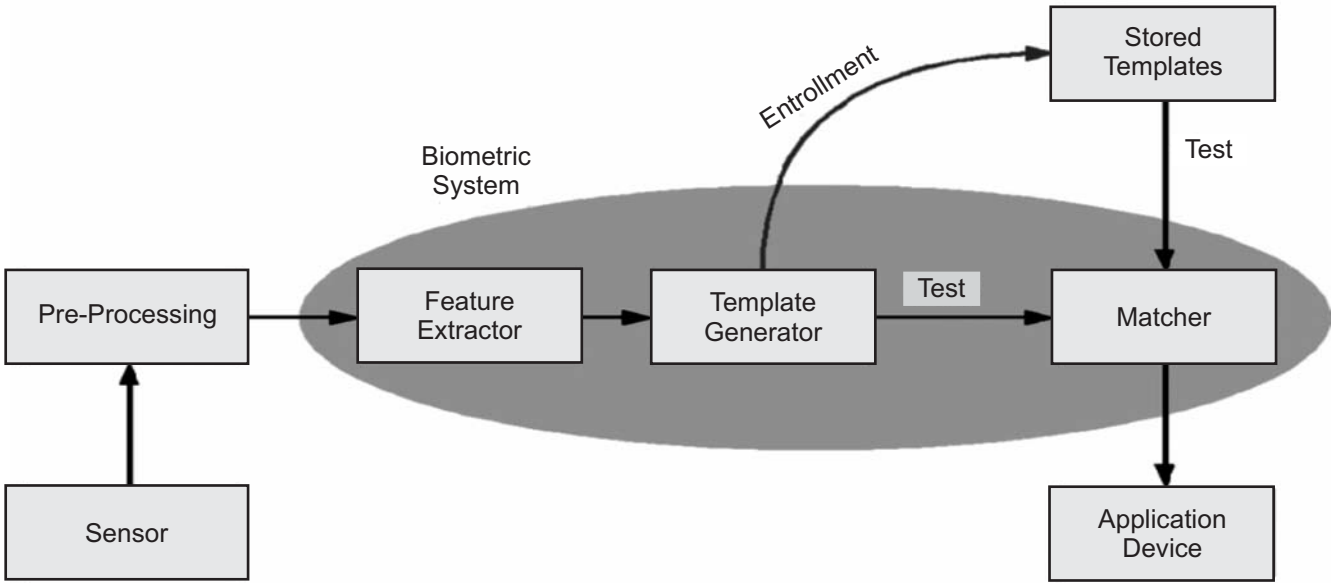

Figure 1: Main Modules of Palmprint Verification System

Biometric identification can be used in recognition mode, where the biometric system identify a person from the entire enrolled population by searching a database for a match based exclusively on the biometric. For example, an entire database can be searched to verify a person has not applied for right benefits under two different names. This is occasionally called as “one to many” matching. A system can also be used in authentication mode, where the biometric system authenticates a person’s claimed identity from their earlier enrolled pattern. This is also called as “one to one” matching. In most computer access or network access environments, verification mode would be used. A user enters an account, user name or inserts a token such as a smart card, but as a replacement for of entering a password, a simple touch with a palm or a glance at a camera is enough to verify the user.

2. PROPOSED SYSTEM

Biometric systems contain a number of modal like iris, face, palmprint and signature recognition systems are used to individually or integrate for authentication purpose. These authentications are offering the improvement of performance of the systems. In biometrics, both single and multiple modals contain different algorithms. These algorithms are used to recognize the person and also evaluate the performance of each algorithm. At first to capture the images of the modals by the number of sensors based on the physiological or behavioral traits. These sample images like iris, palmprint and face are added to the database and used to compare with the query database. Different algorithms are applied to extract and recognize the images of the given modals. The final verdict is prepared by score level fusion at correlation analysis is used to identify whether the person is authorized or not.

This algorithm is giving the quality matching value of experimental image and original, and matching the value query and template database individually. Finally fusing three modal for security purpose and to check the person authorized or not. Multimodal biometric systems are used to eliminate the limitation of single modals. The number of single modal like iris, palmprint, palmprint, face, signature, eye, etc. integrated and to form multimodal biometric system. In here three modals like iris, palm and face are integrated for the designing of multimodal biometric system. In this algorithm, compare the quality of the query and template images. Verdicts are prepared by results of score level fusion at the correlation analysis. This algorithm is used to ensure the security and recognize the genuine user as shown in the figure 2

3. IRIS RECOGNITION

The iris has a thin circular diaphragm, which lies between the cornea and the lens of the human eye. The iris is perforated close to its center by a circular aperture well-known as the pupil. The purpose of the iris is to control the quantity of light entering through the pupil and this is done by the sphincter and the dilator muscles, which regulate the size of the pupil. The standard diameter of the iris is 12 mm, and the pupil size can differ from 10% to 80% of the iris diameter. The iris consists of a various number of layers they are, the lowest is the epithelium layer, which contain dense pigmentation cells. The stromal layer lies above the epithelium layer and contain blood vessels, pigment cells and the two iris muscles. The density of stromal pigmentation determine the colour of the iris. The externally visible surface of the multi layered iris contains two zones, which often differ in colour. An outer ciliary zone and an inner pupillary zone are

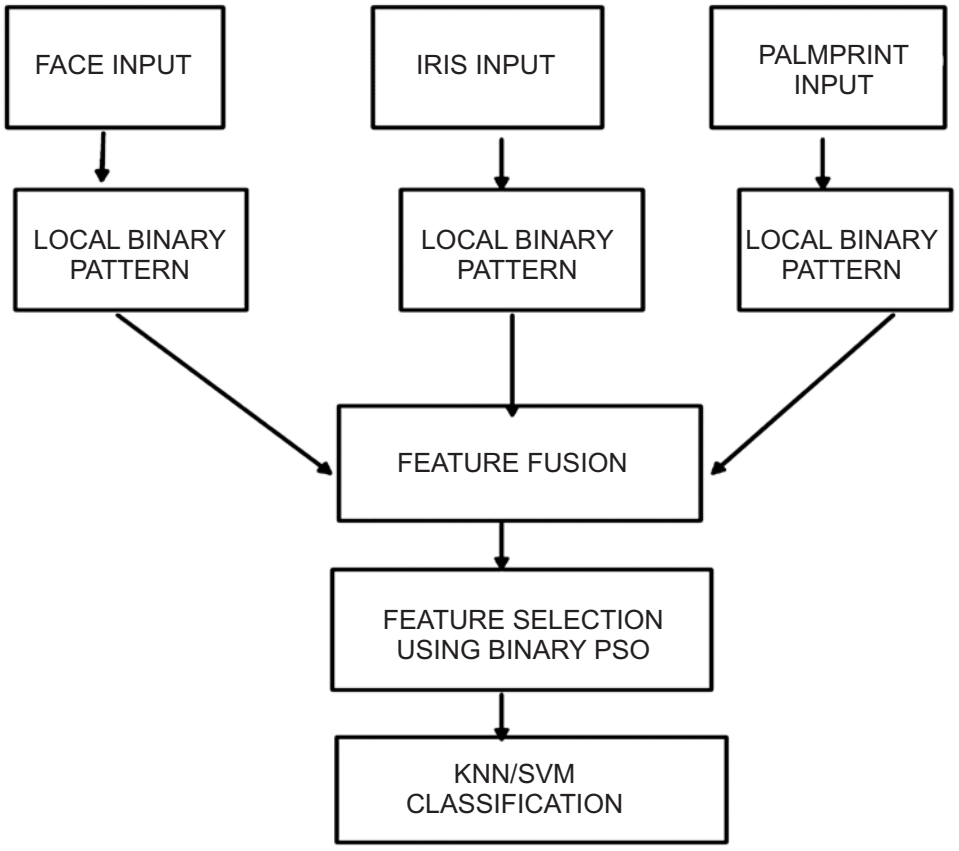

Figure 2: Block Diagram of Proposed Systems

these two zones divided by the collarette which appear as a zigzag pattern. Formation of the iris begin during the third month of embryonic life. The unique pattern on the surface of the iris is formed during the first year of life, and pigmentation of the stroma takes place for the first few years. Formation of the unique patterns of the iris is random and not related to any genetic factors . The only characteristic that is

dependent on genetics is the pigmentation of the iris, which determines its colour. Due to the epi genetic nature of iris patterns, the two eyes of an individual contain completely independent iris patterns, and identical twins possess uncorrelated iris patterns. The path of contour integration is changed from circular to arcuate, with spline parameters fitted by statistical estimation methods to model each eyelid boundary. Figure 3 shows the main modules of iris recognition system.

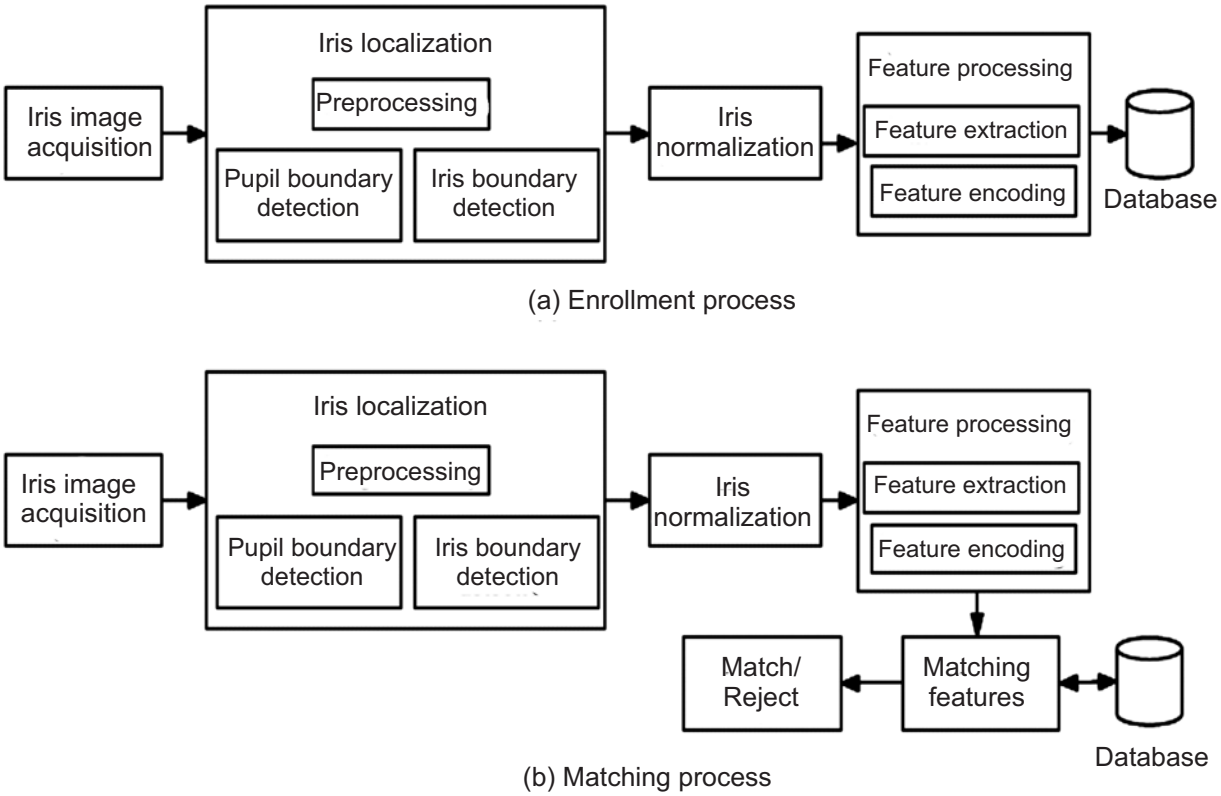

Figure 3: Main Modules of Iris Recognition System

4. PALMPRINT RECOGNITION

A Palmprint is the feature pattern of one palm Figure 4. It is an impression of the friction ridges and furrows on all parts of a palm. The ridges and furrows present good similarities in each small local window, like parallelism and average width as shown in the figure 4.

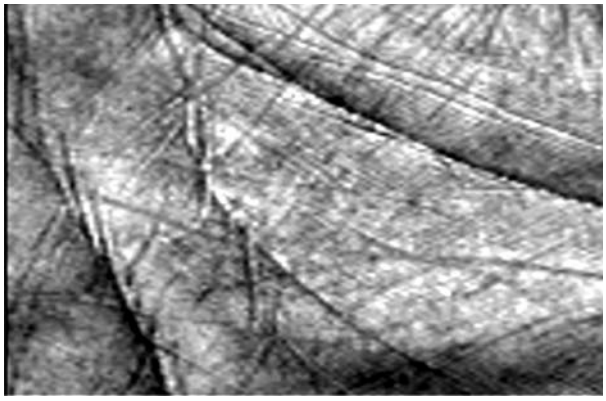

Figure 4: Palmprint Image from a Sensor

However, shown by intensive research on palmprint recognition, palmprints are not distinguished by their ridges and furrows, but by features called minutia, which are some abnormal points on the ridges Figure. Among the variety of minutia types reported in literatures, two are mostly significant and in heavy usage

1. Ridge ending - the abrupt end of a ridge
2. Ridge bifurcation - a single ridge that divides into two ridges

Minutiae are major features of a Palmprint, using which comparisons of one print with another can be made. Minutiae include:

1. Ridge ending - the abrupt end of a ridge
2. Ridge bifurcation - a single ridge that divides into two ridges
3. Short ridge or independent ridge - a ridge that commences, travels a short distance and then ends
4. Island - a single small ridge inside a short ridge or ridge ending that is not connected to all other ridges
5. Ridge enclosure - a single ridge that bifurcates and reunites shortly afterward to continue as a single ridge
6. Spur - a bifurcation with a short ridge branching off a longer ridge
7. Crossover or bridge - a short ridge that runs between two parallel ridges
8. Delta - Y shaped ridge meeting
9. Core – U turn in the ridge pattern

5. FACE RECOGNITION

The image will be scanned and stored into the database. Now two images of the same candidate will be stored into the database. The first step is to select desired images from the database then for comparisons them the next step is to detect faces from each image. The next step is to recognize that images as of the same candidate or not.

A. Face Recognition With LBP

The original LBP operator was introduced by Ojala et al. It is a powerful means of texture description. The face area is first divided into small regions from which LBP histograms are extracted and concatenated into a single vector see Figure 5

Figure 5: Facial Image Divided into 5x5 Regions

In each region the operator labels the pixels of an image by threshold the 3 x 3 neighborhood of each pixel with the center value and considering the result as a binary number or a decimal number.

$$\text{LBP} = p - 1\ s(f(x, y) - f(xp, yp)2p\ p = 0$$

Then the histogram of the labels can be used as a texture descriptor. Later the operator was extended to use neighborhoods of different sizes. Using circular neighborhoods and bilinearly interpolating the pixel values allow any radius and number of pixels in the neighborhood. Figure 6 illustrate the original LBP operator. Pixels of an image by threshold the 3 x 3 neighborhood of each pixel

For neighborhoods the notation (P, R) are used which means P sampling points on a circle of radius of R. See Figure 7 as an example of the circular (8, 2) neighborhood

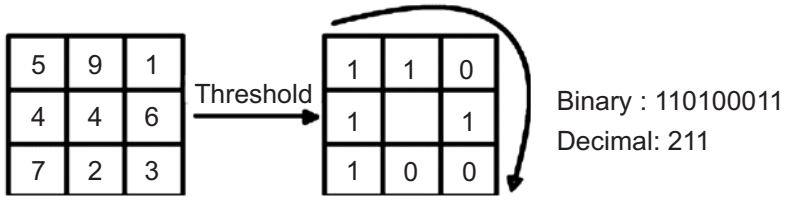

Figure 6: Basic LBP Operator

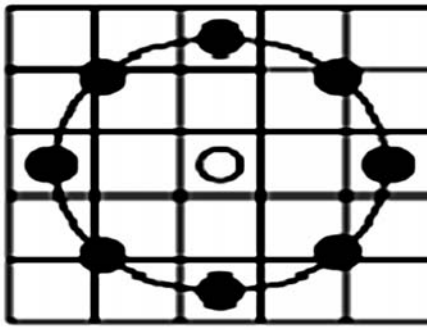

Figure 7: Circular (8, 2) Neighborhood

An LBP is called uniform if it contains at most two bitwise transitions from 0 to 1 or vice versa when the binary chain is considered circular. For example, 11100000, 00011110 and 11000001 are uniform patterns. Ojala et al. noticed that in their experimental results with texture images, uniform patterns account for a bit less than 90 % of all patterns when using the (8, 1) neighborhood and for around 70 % in the (16, 2) neighborhood.

Shengcai Liao et al. Proposed an improved method over the basic LBP in which multi scale block LBP are used. Multiscale LBP is an extension to the basic LBP, with respect to neighborhoods of different sizes. In MB LBP, the comparison operator between individual pixels in LBP is simply replaced with a comparison between average gray values of sub regions. Each sub region is a square block containing neighboring pixels or just one pixel particularly. The whole filter is composed of nine blocks. Take the size s of the filter as a parameter and n x n denoting the scale of the MB LBP operator (particularly, 3x3 MB LBP is in fact the original LBP). Note that the scalar values of averages over blocks can be computed very efficiently from the summed-area table or integral image. For this reason, MB LBP feature extraction can be very fast and it only incurs a little more cost than the original 3x3 LBP operator.

Other different version of LBP which outperform the original LBP are proposed by researches like completed LBP (CLBP), dominant LBP (DLBP) and LBP Histogram Fourier (LBP HF). For matching two facial images there are several possible dissimilarity measures have been proposed for histograms.

Histogram intersection : $$D(S, M) = \sum_i \min(S_{i,} M_i) \quad (1)$$

Log-likelihood statistic : $$L(S, M) = -\sum_i S_i \log M_i \quad (2)$$

Chi square statistic: $$x^2 (S, M) = \sum_i \frac{(S_i - M_i)^2}{S_i + M_i} \quad (3)$$

Where S and M represent the matched face images

6. PARTICLE SWARM OPTIMIZATION

The concept of PSO is that at each time step, changing the velocity (accelerating) of each particle toward its pbest and gbest locations (global version of PSO). Acceleration is weighted by a random term, with separate random numbers being generated for acceleration toward pbest and gbest locations. There is also

a local version of PSO in which, the addition to pbest, each particle keeps track of the best solution, called lbest, attain with a local topological neighborhood of particles. The (original) processes for implementing the global version of PSO are as follows:

Initialize a population (array) of particles with random positions and velocities on d dimensions in the problem space. For each particle, estimate the desired optimization fitness function.

Compare particle's fitness assessment with particle's pbest. If current value is in good health than pbest, then set pbest value equal to the current value and the pbest location equal to the current location in *d*-dimensional space.

Compare fitness assessment with the population's overall previous best. If current value is superior than gbest, then reset gbest to the current particle's array index and value.

Change the velocity and position of the particle according to Equations (4) and (5) respectively.

$$V_{id} = V_{id} + c_1 \times \text{rand}() \times (P_{id} - X_{id}) + c_2 \times \text{rand}() \times (P_{gd} - X_{id}) \quad (4)$$

where, V_{id} : velocity of the particle

X_{id} : current position of the particle

c_1 & c_2 : determine the relative influence of the cognitive and social components

rand() : random number between 0 and

P_{id} : personal best (pbest) of particle *i*

P_{gd} : global best (gbest) of the group

$$X_{id} = X_{id} + V_{id} \quad (5)$$

The acceleration constants c_1 and c_2 in Equation (11) represent the weighting of the stochastic acceleration terms that pull each particle toward pbest and gbest positions. Thus, adjustment of these constants changes the amount of tension in the system. Low values allow particles to roam far from target regions before being tugged back, while high values result in abrupt movement toward, or past, target regions.

Early experience with particle swarm optimization (trial and error, mostly) led us to set the acceleration constants c_1 and c_2 each equal to 2.0 for almost all applications. Vmax was thus the only parameter routinely adjusted, and often set it at about 10-20% of the dynamic range of the variable on each dimension.

Based on other parameters obtained from social simulation findings it was decided to design a "local" version of the particle swarm. In this version, particles have information only of their own and their neighbor's best, rather than that of the entire group. Instead of moving toward a kind of stochastic average of pbest and gbest (the best location of the entire group), particles move toward points defined by pbest and lbest, which is the index of the particle with the best evaluation in the particle's neighborhood.

7. RESULTS AND DISCUSSION

The feature extraction of iris, Palmprint and face recognition for authentication purpose using LBP based algorithm is done. The first sample image is compared to the template image of iris, palm and face. Finally fuse each modals using correlation analysis based algorithm and check whether the person is authorized or not. The simulation result for FAR versus GAR is shown in figure 8

8. CONCLUSION AND FUTURE SCOPE

The iris, palm and face features are extracted by using LBP based algorithms which has been applied and its performance is verified. The security level of each of this recognition has been analyzed through the MATLAB simulation. When comparing with other algorithms LBP based algorithm offers high recognition of iris, palmprint and facial images. This algorithm improves the reliability of biometric systems and it also improves the overall performance of the systems. In future, the Gabor filter will be implemented inorder to improve the quality of the images and show the comparitive result of accuracy by using with and without gobar filter.

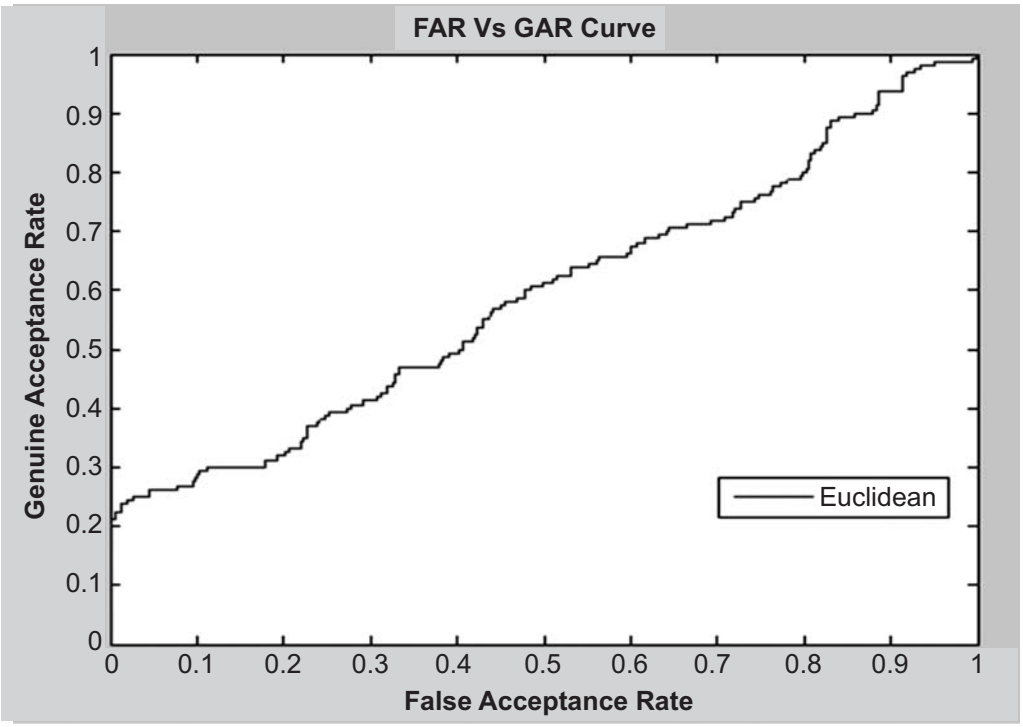

Figure 8: Simulation Window for FAR versus GAR

9. REFERENCES

1. Ashraf Aboshosha, Kamal A. El Dahshan and Eman A. Karam (2015), "Score Level Fusion for Palmprint, Iris and Face Biometrics", International Journal on Computer Applications, Vol. 111 – No. 4, 0975 – 8887, February.
2. Sumit Shekhar, Vishal M. Patel, Nasser M. Nasrabadi and Rama Chellappa (2014), "Joint Sparse Representation for Robust Multimodal Biometrics Recognition", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 36, No. 1, January.
3. Javier Galbally, Sebastien Marcel and Julian Fierrez (2014), "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Palmprint and Face Recognition", IEEE Transactions on Image Processing, Vol. 23, No. 2, February.
4. Hiew Moi Sim, Hishammuddin Asmuni, Rohayanti Hassan, Razib M. Othman (2014), "Multimodal Biometrics: Weighted Score Level Fusion Based on Non-Ideal Iris and Face Images", In Science Direct, Vol. 41, 5390–5404.
5. Geethu S Kumar, Jyothirmati C Devi (2014), "A Multimodal SVM Approach for Fused Biometric Recognition", International Journal of Computer Science and Information Technologies, Vol. 5 – No.3, 3327-3330.
6. Sameer P Patil, Tushar N Raka, Shreyas O Sarode, (2014), "Multimodal Biometric Identification System: Fusion of Iris and Palmprint", International Journal of Computer Applications, Vol. 97– No.9, 0975 – 8887, July.
7. Pooja Choudhari, Hingway S P, Sheeja S Suresh, Arati Wagh (2014), "Fusion of Iris and Palmprint Images for Multimodal Biometrics Identification", International Organization of Scientific Research, Vol. 04, Issue 08, 2250-3021, August.
8. Sakshi Kalra, Anil Lamba (2014), "Improving Performance by combining Palmprint and Iris in Multimodal Biometric", International Journal of Computer Science and Information Technologies, Vol. 5 (3), 4522-4525.
9. Qing Zhang, Yilong Yin, De-Chuan Zhan, and Jingliang Peng (2014), "A Novel Serial Multimodal Biometrics Framework Based on Semisupervised Learning Techniques", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 10, October.
10. SIREESHA V, SANDHYARANI K (2013), " Multimodal Biometric System using Iris - Palmprint: an Overview", International Journal of Engineering Sciences Research, Vol 04, Special Issue 01, 2230-8504.
11. Sanjekar P S and Patil J B (2013), "An Overview of Multimodal Biometrics", Signal & Image Processing : An International Journal (SIPIJ), Vol.4, No.1, February.