RESEARCH ARTICLE

Multimodal biometric authentication algorithm at score level fusion using hybrid optimization

E. Sujatha [1] Nil, A. Chilambuchelvan [2]

[1] Associate Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai. India

[2] Dr.A.Chilambuchelvan, Professor, Department of CSE, RMD Engineering College, Chennai

Abstract: Biometric is emerging technology in identification and authentication of human being with more reliable and accurate. Combining multiple biometric systems is a promising solution to provide more security. It eliminates the disadvantages of unimodal biometric systems such as non-universality, noise in sensed data, intra-class variations, distinctiveness, spoof attacks and traditional method of authenticating a human and their identity. The proposed method depicts a multimodal biometric algorithm is designed to recognize individuals for robust and secured authentication using normalized score level fusion techniques with hybrid Genetic Algorithm and Particle Swarm Optimization for optimization in order to reduce False Acceptance Rate and False Rejection Rate and to enhance Equal Error Rate and Accuracy.

Keywords: Multimodal biometrics; Authentication algorithm; Score level fusion; Optimization

1. Introduction

Biometrics was initially used as anthropological technique of anthropometry to law enforcement, creating an identification system based on physical measurements by Alphonse Bertillon French police officer and biometrics researcher in 18th Century. Biometric is a process of uniquely identify human by their physiological or behavioral characteristics. Physiological characteristics are genetically implied and possibly influenced by the environment. They are Iris, Finger Vein, Finger Print, Hand Geometry, Palm print, Ear, Retina, Face, DNA, Odor, Vascular imaging, Sweat pore, Lips, and Brainwave. Behavioral characteristics of biometrics are Gait analysis, Keystroke dynamics, Signature, Voice ID, Mouse use characteristics, and Cognitive biometrics.

Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, in the military and wide scope in commercial applications are already benefitting from these technologies.

Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods such as the utilization of passwords or PINs. Identification methods are Something you know - a password, PIN, or piece of personal information, Something you have - a card key, smart card, or token like a Secure ID card, Something you are - a biometric. The vulnerabilities and threats of traditional authentication systems like passwords are forgotten, stolen, lost, forged, duplicated, spoofed, hacked, shared, are eliminated. The limitations of unimodal biometric systems can also be resolved such as noise in sensed data, intra-class variations, distinctiveness, non-universality.

In this research work, the multimodal biometric algorithm integrates Iris, Finger Vein and Finger Print biometric traits for their best biometric characteristics. Each biometric trait is adapted for preprocessing techniques such as localization and normalization, before recognition in order to improve the image quality and recognition rate, each trait

doi: 10.18063/wct.v2i1.415

is recognized by individual recognition algorithm. Matching algorithm provides score and the score is normalized before fusion. Normalization brings the homogeneity for score to apply fusion rule, because in multimodal biometric environment different modalities produce heterogeneous scores. Score level fusion approach is applied to integrate scores from different multimodal biometrics and optimized using hybrid Genetic Algorithm and Particle Swarm Optimization for robust authentication, enhanced security and accuracy. It eliminates the flaws, vulnerabilities and threats of using uni-modal biometric algorithm for authentication. Genetic Algorithm and Particle Swarm Optimization techniques are combine to perform efficiently and yield best results in optimization. Finally, the performance of the algorithm is evaluated by metrics as False Acceptance Rate, False Rejection Rate, Equal Error Rate and Accuracy for authenticating a person as genuine or imposter. These parameters plays vital role in assessing the performance of the algorithm. Here MATLAB is used for implementation. The performance of the algorithm is evaluated by SDUMLA-HMT Chimeric Database, the Machine Learning and Data Mining Lab, Shandong University (SDUMLA-HMT) set up the Homologous Multi-modal Traits Database named as SDUMLA-HMT Database. The database includes real multimodal data from 106 individuals. The original database is obtained with authenticated agreement from the lab. This multimodal biometric database provides Iris, Finger Vein, Finger Print templates and used for experimental analysis. All the biometric templates are obtained from the same person, it impacts accuracy. The experimental results show that accuracy is improved when compared to unimodal biometric system, traditional methods and other combination of multimodal biometric system for authentication. So the multimodal biometric authentication algorithm is applied to various wider scopes of applications such as border control, physical access control and network security. The proposed method discusses how False Acceptance Rate and False Rejection Rate are reduced and it determines Equal Error Rate and Accuracy and hence proves that multimodal biometric algorithm provides best authentication.

2. Literature review

The recent scenario demands highly secured and robust authentication algorithm to get rid of vulnerabilities and threats. Emerging biometric technology can improve the safety and security. After September 11, 2001 attack the world realized the importance of public safety and the need for data security. Resetting the forgotten passwords costs makes expensive for the corporate companies in the traditional security system. Biometric based authentication system is adapted for designing novel authentication algorithm. Multimodal eliminates the flaws of unimodal biometric systems and traditional authentication systems.

The evolution of biometric technology focus the significance and where the future technology of world travels can be identified by several papers and their authors contributed the research work.

Introduction, motivation and scope of multimodal biometrics using score level fusion techniques and sensors, how more than one biometric trait can be combined to form efficient algorithm, is referred in Kalyan Veeramachaneni *et al*. (2005), Hong & Jain (1998). Importance of biometrics and its applications, future trends of biometrics, efficiency of biometric technologies are studied from Frischholz & Deickmann (2010), Hong Jain *et al*. (1999). Iris recognition techniques and its comparison with other techniques are discussed in Mayank Vatsa *et al*. (2004). Iris with Fingervein multimodal algorithm with score level fusion and performance of the algorithm are known from Mohamed Touahria *et al*. (2014), Shruthi *et al*. (2013), Nurhafizah Mahri *et al*. (2010), Prakash Chandra Srivastava *et al*. (2010). Chimeric Database for evaluation is obtained from SDUMLA-HMT Shandong University, China with license agreement for use. Score level fusion techniques importance and effectiveness are obtained from Romaissaa Mazouni *et al*. (2011), Poh *et al*. (2005). Hybrid Particle Swarm Optimization and Genetic Algorithm is efficient comparatively with other techniques is referred from Cherifi Dalila *et al*. (2015), Eberhart *et al*. (1998).

3. Proposed system

The Proposed System has multiple stages as preprocessing, recognition, normalization, fusion and optimization and analysis stage. In preprocessing stage the template stored in database is fetched and noise is eliminated. Recognition of each biometric trait is done and the scores for each trait are obtained. Normalization makes the compatibility between scores of multimodal biometrics. It is mandatory before fusion. Fusion and optimization stage is adapted for inheriting the benefits of GA and PSO in fusion and optimization of scores.

3.1 Iris recognition

It is accurate and reliable over 200 millions of comparisons. It is easy to detect artificial irises. It possesses good biometric characteristics.

Preprocessing steps consists of localization and normalization. Localization includes canny edge algorithm as:

Smoothing – to filter out the noise, Gaussian filter is used.

$$H_{ij}=\frac{1}{2\pi\sigma^2}\exp\left(-\frac{\left(i-\left(k+1\right)\right)^2+\left(j-\left(k+1\right)\right)^2}{2\sigma^2}\right);1\le i,\ j\ \le\left(2k+1\right)$$

Finding gradients - to find horizontal, vertical, diagonal edges in the image.

Non maximum suppression – helps to suppress all gradient values except local maxima, also known as edge thinning technique.

Double thresholding – determines weak edge pixel by verifying between highest threshold and lowest threshold values.

Edge tracking by hysteresis –weak edge pixel caused by noise/color variation is removed by this method.

Preprocessing of Iris image by canny edge detection algorithm using Laplacian of Gaussian filter and normalization by pupil dilation is known as iris localization. During localization of preprocessing color image is converted into grey scale image and finding the centre of the pupil is called binarization of image. The formula for transforming polar to cartesian coordinates is as follows:

$X = r\cos\theta$

$Y = r\sin\theta$

This conversion helps in noise removal. Grey scale matrix values are training data. The radius of the pupil is obtained through this technique. The distance between pupil and the boundary of iris is unique. Inner and outer boundaries are not concentric. Pupil size varies from 10% to 80% of iris diameter. So iris provides highly robust and reliable recognition algorithm. Iris template size varies from 256 bytes to 512 bytes. Matching algorithm by hamming distance is done to obtain score. The score is normalized using z-score normalization technique. The SDUMLA –HMT Database is used, obtained using 5 different sensors from 106 individuals and it is chimeric database. Iris matching algorithm uses hamming distance, the formula is presented as:

$$HD=\frac{\sum_{j=1}^{N}x_j\left(XOR\right)Y_j\left(AND\right)Xn'_j\left(AND\right)Yn'_j}{N-\sum_{k=1}^{N}Xn_k\left(OR\right)Yn_k}$$

The hamming distance HD is calculated using formula, where Xj and Yj are the models to compare bit by bit, Xnj and Ynj are the noise masks for Xj and Yj , and N is the number of bits represented by each model. It produces score.

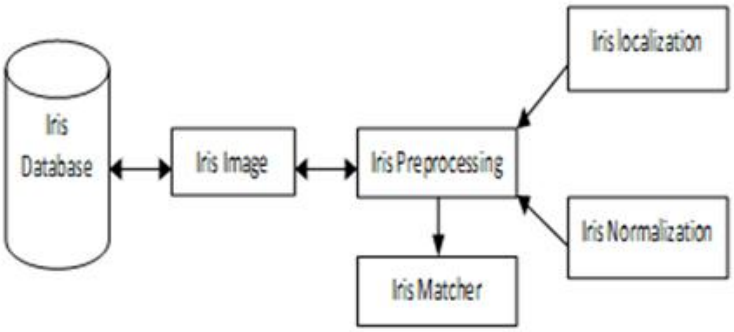

Figure 1; Iris Recognition.

3.2 Finger vein recognition

The finger vein database is composed of 3,816 images from 6 fingers of 106 individuals. Every image is stored in "bmp" format with 320×240 pixels in size, the finger vein database takes up around 0.85G Bytes in total.

Several pre-processing techniques used in finger vein authentication. The proposed algorithm consists of:

Segmentation - To increase the accuracy, we first make the background of the image black by setting those background pixels to zero.

Aligning the finger horizontally - either keep a tube-like structure in the hardware or align the images in the software algorithm. The edges are detected and the image is rotated such that the detected edges are now horizontal.

Image enhancement using contrast limited adaptive histogram equalization - to improve the image contrast, and brightness characteristics, reduce its noise content, and/or sharpen its details. It enhances the contrast of images by transforming the values in the intensity image. The AHE process can be understood in different ways. In one perspective the histogram of grey levels (GL's) in the output is maximally black; if it has the median value in its window the output is 50% gray's window around each pixel is generated first. The cumulative distribution of GL's, that is the cumulative sum over the histogram, is used to map the input pixel GL's to output GL's. If a pixel has s a GL lower than all others in the surrounding window.

Image normalization - The image is resized to 1/4th of the original size. It is the optimum scaling factor according to the various vein databases. The optimum scaling factor is 0.6.

Region of interest (ROI) extraction – removal unwanted area in the finger vein image increases accuracy. ROI focuses the range of the pair of the edge points is between 35% to 65% of the image height and the pair of the edge points is the widest pair among all pairs. Finally, the image is cropped vertically at the cropping points and horizontally at 5% from left border and 15% from right border.

The Hamming distance algorithm is used for matching. Score is normalized before fusion.

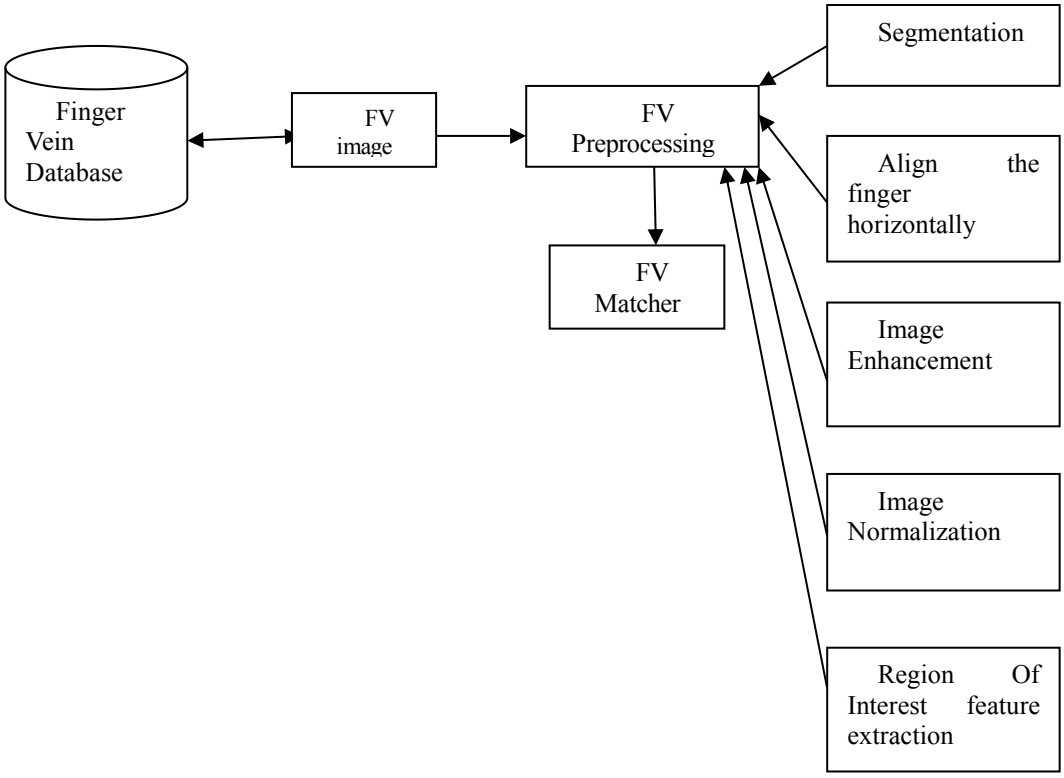

Figure 2; Finger Vein Recognition.

3.3 Finger print recognition

It is unique in identical twins, triplets, quadruplets, quintuplets. Burns, abrasions, cuts do not affect the ridge structure. Finger Print image is preprocessed as:

Enhancing FP image - Gabor filters optimally capture both local orientation and frequency information from a fingerprint image. Once the ridge orientation and ridge frequency are determined, then they are used to construct the Gabor filter. In fingerprint enhancement, Gabor filter can be tuned to specific frequency and orientation values. Gabor filter can enhance the ridges in the direction of local orientation effectively preserving the ridge structure.

Binarise the threshold - Binarisation is the process of converting the gray scale image into the binary image. For binarising an image we use threshold method in which a value is presetted and the pixels lower than this threshold value are represented as white and above than this value are represented by black color.

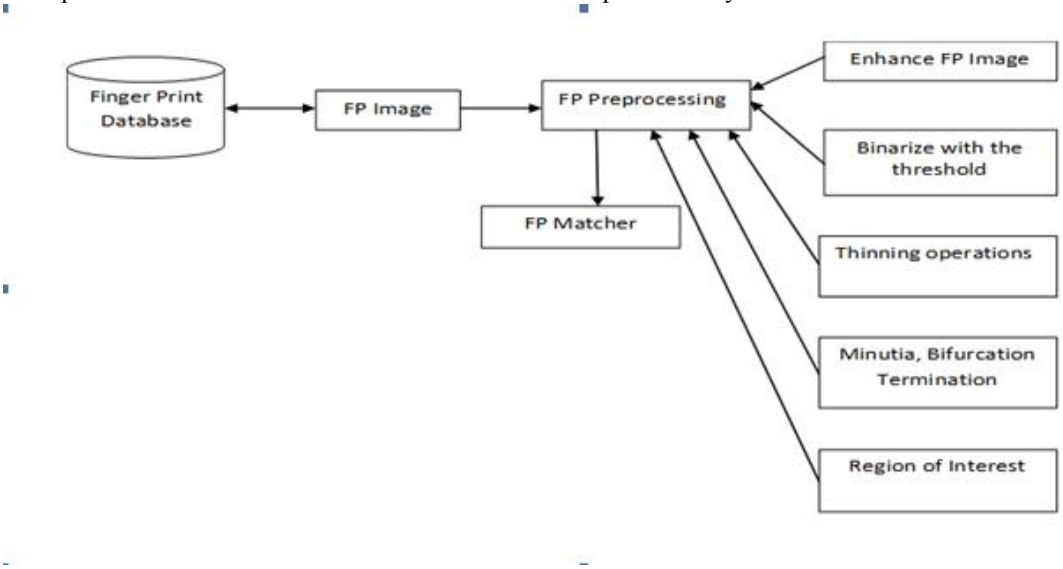

Figure 3； Finger Print Recognition.

Thinning operations – used to preserve the connectivity of the ridges. It is an iterative process.

Minutia, bifurcation termination - bifurcation means the features of the fingerprints do not get distorted during thinning.

ROI – full image is considered for region of interest.

Matching algorithm – direct comparison of two images pixel wise is done to obtain the score.

3.4 Normalization

Score level fusion approach is used for its accuracy and optimal performance. It can be easily combined with other biometric trait. It has enhanced response time and system performance. It provides lower communication bandwidth, easy to process and easily accessible. Scores are normalized using z-score normalization and the formula is as follows:

$$x'_k = \frac{x_k - \mu}{\sigma}$$

where x_k: the k^{th} matching score before normalization

x_k: the k^{th} matching score after normalization

μ: mean

σ: standard deviation

3.5 Score level fusion and optimization

Population based search methods and combination of deterministic and probabilistic rules. It is computationally efficient. It provides social, cognitive behavior. Literature survey suggests Genetic Algorithm (GA) and the

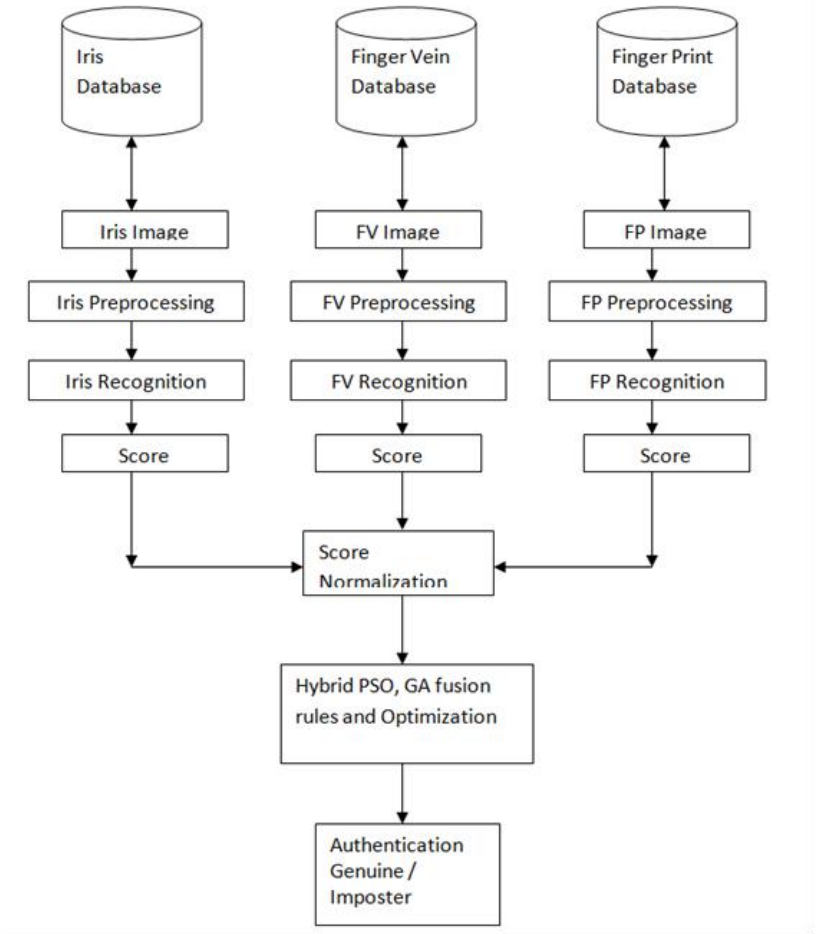

Figure 4; Proposed Architecture Diagram.

PSO algorithms. Both resulting populations are combined into one single population of N individuals, which are then sorted. So in this proposed work, the use of a hybrid algorithm GA-PSO to optimize the weights assigned to the different biometric modalities used in the fusion at the score level in order to Particle Swarm Optimization (PSO) performs efficient than the Brute Force Search (BFS), Adaptive Neuro Fuzzy Inference System (ANFIS), Support Vector Machine (SVM).increase performance and accuracy. The fitness function is defined as

Equal Error Rate (EER) and goal is to minimize ERR which is optima. The hybrid approach picks N initial individuals that are randomly generated. The N individuals are sorted by fitness, according to a user defined probability , the set is divided into two sub-sets and each set is assigned to GA,

$$Sf_i = \sum_{m=1}^{M} W_m \times S_i^m$$

$$Wm \in [0,1], \sum_{m=1}^{M} W_m = 1$$

4.Results and disscusion

The performance of the state of the art algorithm is discussed and their results are exhibited. To evaluate the efficiency of the algorithm the following database is utilized.

Biometrics fusion recognition is a newly arisen and active research topic in recent years. In 2010, the Machine Learning and Data Mining Lab, Shandong University (SDUMLA) set up the Homologous Multi-modal Traits Database which is named SDUMLA-HMT Database. SDUMLA-HMT Database includes 5 biometric traits, i.e., face, finger vein, gait, fingerprint and iris. SDUMLA will provide the SDUMLA-HMT Database freely of charge to biometrics recognition researchers in order to promote research. The SDUMLA-HMT database consists of face images from 7 view angles, finger vein images of 6 fingers, gait videos from 6 view angles, iris images from an iris sensor, and fingerprint images acquired with 5 different sensors. The database includes real multimodal data from 106 individuals. It's a Chimeric Database in which all the multimodal biometric samples are collected from the same person. It helped the research work in wide scope.

ROC (Relating Operating Curve) lies on x axis when FRR≠0, FAR=1 and ROC lies on y axis when FRR=0, FAR=0.

Genuine score < threshold = FRR

FRR= No. of false rejections / No.of genuine accesses

FAR=No. of false acceptances / No. of imposter accesses

The proposed method False Acceptance Rate and False Rejection Rate with their respective threshold values are listed:

Proposed Method FAR, FRR Values are listed in Table 1.

Threshold	FAR	FRR
0.010	0.00	99.00
0.015	0.00	72.15
0.020	0.00	30.71
0.025	0.00	20.05
0.030	0.00	0.02
0.035	10.05	0.01
0.040	40.19	0.00
0.045	70.10	0.00
0.050	99.00	0.00

Table 1. FAR, FRR Values.

When threshold increases, FAR decreases and FRR increases and vice versa. If FAR and FRR are equal it is known as ERR (Equal Error Rate). When ERR is low, devices are accurate.

The Equal Error Rate comparision Table 2 shows the proposed method is more efficient since EER decreases,

performance increases.

Multimodal Biometrics	Equal Error Rate
Finger Print	0.5
Finger Vein	0.145
Iris+Finger Print	0.038
Iris+Finger Vein	0.128
Finger Print+Finger Vein	1.21
Proposed Method (Iris+Finger Print+Finger Vein)	**0.03**

Table 2. Equal error rate (EER) comparisions.

The Equal Error Rate is shown in **Figure 5.**

Figure 5; Equal error rate.

Accuracy formula is presented as:

$$\text{Accuracy} = 100 - \left(\frac{\text{FRR} + \text{FAR}}{2} \right)$$

The Accuracy is compared with the existing biometric technologies as follows: The Accuracy is compared with the existing biometric technologies as follows:

Multimodal Biometrics	Accuracy
Finger Print	85
Iris+Finger Print	99.975
Finger Print+Finger Vein	98.78
Proposed Method (Iris+Finger Print+Finger Vein)	**99.99**

Table 3. Comparisions of accuracy.

The Comparisions of Accuracy is shown in **Figure 2.**

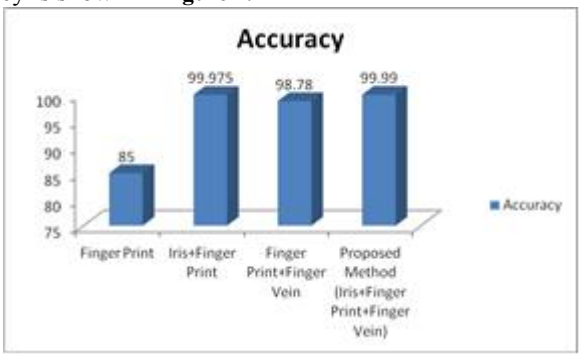

Figure 2; Comparisions of accuracy.

The Table 5.9 shows that the overall comparisons of this thesis work. Iris, Palm print, Face, Signature based Multimodal biometric algorithm yields 0.003, 0.250 of FAR, FRR respectively. Iris, Finger Vein, Palm print, Face based Multimodal biometric algorithm provides 1.0 and 0.91 values of FAR, FRR respectively. But Iris, Finger Vein, Finger Print based Multimodal biometric algorithm produced 0.00 and 0.02 FAR, FRR values. Since FAR, FRR values directly influences the Equal Error Rate and Accuracy, it is mandatory to observe the FAR, FRR values are low.

Biometric	FAR (%)	FRR (%)
Iris+Palm print+Face+Signature	0.003	0.250
Iris + Finger Vein + Palm print + Face	1.0	0.91
Proposed Method (Iris+Finger Vein+Finger Print)	0.00	0.02

Table 5.9. Overall comparisons of multimodal biometric systems.

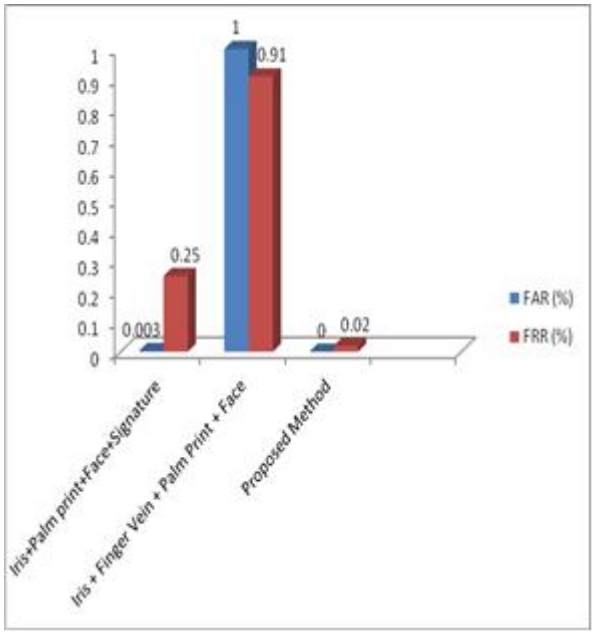

Figure 5.22; Overall comparisons of multimodal biometric systems.

5. Conclusion

Multimodal biometric authentication algorithm is designed using score level fusion techniques with hybrid Genetic Algorithm and Particle Swarm Optimization for developing optimized authentication system with enhanced accuracy and security.

This research work integrates more than two biometric traits for developing robust authentication algorithm. Iris, Finger Vein and Finger Print biometrics are integrated and opted out for their best biometric characteristics. It provides reliable and most promising solution for security systems. It also eliminates the disadvantages and limitations of unimodal biometric systems. Fusion rules are constructed using hybrid Genetic algorithm operations and Particle Swarm Optimization. It optimizes the accuracy and enhances security.

Each biometric trait is undergone preprocessing techniques in order to improve the quality of image for recognition. While recognition the image, the matching algorithm processes the image and produces score. The score is normalized before fusion, because the score is obtained from different biometric trait are heterogeneous in nature. To make it homogeneous, normalization method is adapted. For fusing scores, hybrid Genetic Algorithm and Particle Swarm Optimization is applied and optimization is also done. The decision is taken whether the claimed identity is genuine or imposter.

MATLAB software is used for implementation of preprocessing, matching, normalization and optimization. The SDUMLA-HMT data base is utilized for validating the authentication system with respect to metrics. This database is chimeric database which means all the biometric traits are obtained from the same person. This research work makes use of this database because of its chimeric nature.

Finally, the performance of the system is evaluated by the metrics False Acceptance Rate (FAR) and False Rejection Rate (FRR), Equal Error Rate (EER) and Accuracy. If the threshold is too high, False Rejection Rate is may increase. If the threshold is too low, then the False Acceptance Rate may increase. So the threshold is set in order to reduce FAR, FRR. The Equal Error Rate (ERR) is determined when FAR and FRR are equal. When EER is low, the accuracy of the system is enhanced.

India's national ID program called Aadhaar is the largest biometric database in the world. It is a biometrics-based digital identity assigned for a person's lifetime, verifiable online instantly in the public domain, at any time, from anywhere, in a paperless way.

In Future Multimodal Biometrics becomes the more promising and unavoidable feature of secured algorithms.

Biometrics makes password less world in near future. In future biometrics will be the door way to all the accessible systems.

6. Future work

Biometric is emerging trend in the research era, enhancement can be done in all dimensions. In this research work, the multimodal biometric template database is used for validating the authentication algorithm; instead, online feature extraction could be adapted for each biometric trait using multiple sensors.

Multi-instance: Multiple instances of the same body trait can be considered as input for recognition.

Multi-sensor: A single biometric trait is imaged using multiple sensors in order to extract different information.

Multi-algorithm: The same biometric data is considered for recognition using multiple algorithms.

Multi-sample: A single sensor is used to acquire multiple samples of the same biometric trait to obtain a more complete representation of the trait.

Cancellable biometrics: make a biometric template can be cancelled and be revoked like a password, as well as being unique to every application.

Cryptographic algorithms: If Biometrics concepts can be fused with cryptographic algorithms, the system would be more robust, reliable, and accurate.

Hybrid systems: Any combination of above methods may be implemented for high security systems.

Integrated approach: Combination of biometric scheme with non-biometric scheme such as possession or knowledge based schemes can be implemented for better performance of the system.

Recent biometric traits such as DNA, Brainwave, Body Odour, Finger nail bed, Heart patterns, Aging facial, Vascular pattern recognition, Dorsal Hand Vein recognition can be used for multimodal biometrics.

Fuzzy logic can be applied at fusion level in order to implement secured system for specific applications.

Various other factors can also be considered such as order of algorithms to improve speed, biometric transaction time, and biometric enrollment rate etc,

Biometric traits can be applied to medical applications for identifying the symptoms of disease in order to focus prevention.

References

1. Algorithm, Kalyan, Veeramachaneni, *et al*. An adaptive multimodal biometric management—part C: Applications and reviews. IEEE Transactions On Systems, Man, And Cybernetics 2005; 35(3): 344-356.
2. Hong L, Jain A. Integrating faces and fingerprints for personal identification. IEEE Trans. Pattern Anal. Machine Intell 1998; 20(12): 1295–1307.
3. Frischholz RW, Deickmann U. A multimodal biometric identification system. IEEE Comput 2000; 33(2).
4. Hong L, Jain AK, Panikanti S. Can multibiometrics improve perfomance? Proc. AutoID, Summit, NJ 1999; 10: 59–64.
5. Eberhart R, Shi Y. Comparison between genetic algorithms and particle swarm optimization. 7th Annual Conf. Evolutionary Programming, San Diego, CA 1998; 3.
6. Vatsa M, Singh R, Gupta P. Comparison of iris recognition algorithms. Mayank Vatsa Department of CSE ZIT Kanpur, India mayank-richa@ yahoo.com 0-7803-8243-91041$17.000 IEEE 2004: 354-358.
7. Yin Y, Liu L, Sun X, *et al*. SDUMLA-HMT: A multimodal biometric database (Eds.): CCBR 2011, LNCS 7098 © Springer-Verlag Berlin Heidelberg 2011: 260–268.
8. Comparative study of multimodal biometric recognition by fusion of Iris and fingerprint houda benaliouche. Mohamed Touahria Scientific World Journal doi: 10.1155/2014/829369 2014 ;(6).
9. Dalila C, Imane H, Amine NA. Multimodal score-level fusion using Hybrid GA-PSO for Multibiometric System. Cherifi Dalila and Hafnaoui Imane, Informatica 39 2015: 209–216.
10. Shruthi BM, Pooja M, Mallinath, *et al*. Multimodal biometric authentication combining finger vein and finger print. International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com 2013; 7(10): 43-54 .
11. Mahri N, Suandi SAS, Rosdi BA. Finger vein recognition algorithm using phase only correlation Nurhafizah Mahri†, Shahrel Azmin Sundi @Suandi and Bakhtiar Affendi Rosdi 978-1-4244-7065-5/10/$26.00 ©2010 IEEE 2010:1–6.

12. Prakash CS, Anupam A, Kamta NM, *et al*. I.J. Information technology and computer science. Published Online January 2013 in MECS (http://www.mecs -press.org/) DOI: 10.5815/ijitcs.2013.02.10 Fingerprints, Iris and DNA Features based Multimodal Systems: A Review 2013; 02: 88-111.
13. National science and technology council. Committee on Technology, Committee on Homeland Security, Subcommittee on Biometrics. www.biometrics.gov.
14. Poh N, Bengio S, Database. Protocol and tools for evaluating score-level fusion algorithms in biometric authentication. Pattern Recognition 2005; 39(2):223–233.