A Relative Analysis Of Multimodal Biometric Fusing Face, Ear And Fingerprint

Mrs.S.ArunaraniM.C.A.,M.phil., Dr.R.Gobinath

Abstract— In the field of security, biometrics technology is used to implement a lot of authentic and reliable system for combining the technology and science. Multimodal biometry depend on uni-biometrics combined by various fusion techniques such as sensor level, feature level, score level and decision level fusion techniques. A multimodal biometric system introduced here could be a comparative analysis of most used and famous unimodal and multimodal biometry like face, ear, fingerprint and a multimodal biometrics utilizing, face, finger print and ear biometrics. A comparative model is conferred in this paper is executed in MATLAB. Principle component analysis using eigenface vector, minutiae using thinning and MSER used for feature extraction. This model was trained and tested with two sets of database. Feature level fusion was tested in the database on the multimodal biometric system under consideration.

Index Terms— multimodal biometrics, feature fusion, MSER, eigen-face, thinning, Euclidean distance.

1 INTRODUCTION

Biometric technology represents the manner for having a precise and reliable human authentication system depend or biological traits as fingerprint, iris, face, palm print, hand print ear and finger knuckle or behavioral characteristics as voice gait, signature, and keystroke as in Fig. 1. The Physiologica characteristics of a person could never undergo any change due to time but the behavioral characteristics may be exposed to be modified over time. Any biometric system operate in two modes i.e., authentication and identification. In authentication, an individual's biometric trait is gathered and retained in the system's database. When an individual submi the biometric trait for authentication, it is compared to the biometric template in the system. Whereas, in the identification mode, an individual is recognized by collecting the biometric traits and compare it with the templates of all the users in the system's database for an exact match. Thus, the system performs a one-to-many comparison so as to confirm a person's identity.

In unimodal biometric systems, it is enforced to utilize only anyone biometric such as face, iris or any gait etc., but this system is not sufficient to provide the necessary accuracy and efficiency. Therefore to afford the necessary performance more than one biometric trait is utilized. This is referred as multimodal biometric system. In multimodal biometric system utilize multiple evidence of personal identification for human authentication. The modalities are captured and combined for the identification. The unification of the biometrics can be done at feature level, score level, sensor level or decision level fusion to overcome some of the limitations of the single biometric trait.

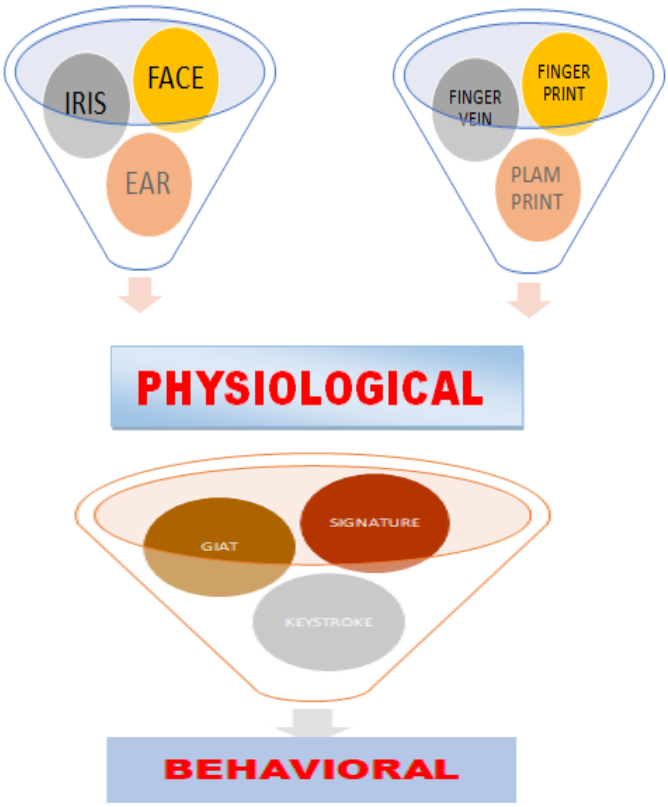


Fig. 1 Biometric traits types

Multimodal biometric cannot be deceived as multiple biometric traits are not easy to counterfeit but it is possible to forge one biometric characteristic. Thus multimodal biometric system provides a better protection and security. Biometrics in the multimodal system is fused at any one of the four level fusions. Sensor level fusion combines the raw biometric data and in feature level fusion the feature set originating from multiple sensors are combined together for processing, and in score level fusion the scores of biometric traits after combining is utilized to take the decision. or decision level that uses the matching scores consolidated via techniques like majority selection to either verify an

Mrs.S.Arunarani ,Research Scholar,Department of Computer Science,VISTAS,Pallavaram, Chennai.Assistant professor, Prince Shri Venkateshwara Arts and Science College,Chennai.sarunaarani@yahoo.co.in

Dr.R.Gobinath, Associate Professor, Department of Computer Science, VISTAS,Pallavaram Chennai.

need.)

identity or validate a claimed identity.
In this paper, the researcher combined three unimodal biometric to form a single multimodal biometric through which high accuracy is attained and it is compared with all the three traits as single biometrics. Our main goal of this experiment is to establish general standards for researchers to decide the biometrics which will attain the foremost correct and effective performance and suit the objective of their systems.

1.1 Working Principle of Biometric System

The basic principle of the biometric system is given as below. Some of the basic steps associated with biometric system are registration, dataset, data acquisition, data storage, feature extraction, matching.
Registration: In the beginning of the process, the user's biometric data is obtained from a person and it is stored in the form of guide for further use in the biometric system. It's referred as enrollment or registration method. This data are used for method such as authentication.

Biometric Dataset: The raw data bestowed by the user throughout registration is named as unprocessed image data, which is additionally referred as raw biometric sample. This Raw biometric information is used to create the biometric template by a process known as feature extraction as this raw data cannot be used for biometric matching process.

Data Acquisition: A special hardware is used for every biometric trait to acquire the necessary biometric information from the user. This is known as data acquisition process. For example, getting a palm print by placing the user's palm in a palm reader device.

Data Storage: Number of feature extraction algorithm is used to extract the necessary biometric information from the given raw data from the user. The size of the converted data varies from few bytes to thousand bytes.

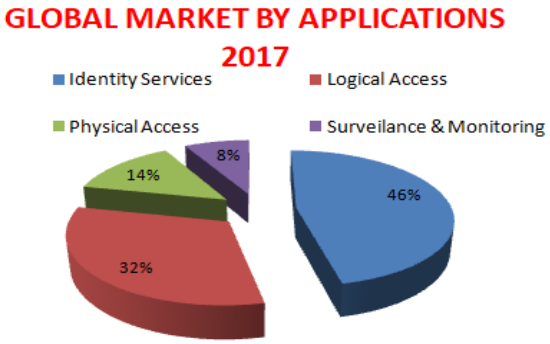
Feature Extraction: Identifying the unique characteristics from the given data is done in this process for biometric identification. This process is done during the registration process, and during the data storage process. Through this the interesting points of features are extracted from the acquired data.

Matching: At the time of verification, the stored template is compared with the live data. The obtained score is used to authenticate the human. The decision is made based on the score of the matching process.

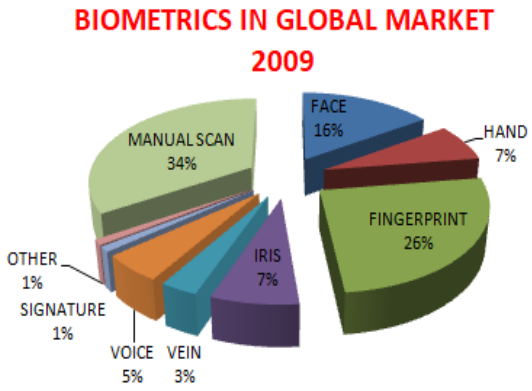
Fig2: A biometric system

Biometric Market Point of View:

In the advanced image processing, for the authentication of a person various biometrics are utilized over the last decades. According to the Acuity Market Intelligence report the mostly the biometrics are used for security purposes. The percentages of the market occupied by various biometrics are shown below.



Source: Acuity Market Intelligence.



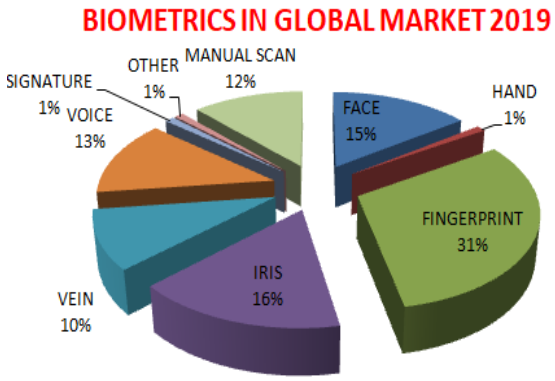


Fig 3 global market of Biometrics

2 RELATED VIEWS

In this section, the previous studies concerning the multimodal biometric systems are reviewed.
Liau et.al.[3] has used face and iris based on score level fusion in their paper. All different version of SVM is used in their work.. The efficiency of the multimodal biometrics recognition were enhanced by selecting a optimal subset of features. The experimental results pointed out that the introduced system had exhibited very promising results. In their work [5], somashekar et.al combined face and fingerprint based on a feature level fusion and decision level fusion for designing a multimodal biometric system. Initially, using Gabor and SIFT, features are extracted for both face and fingerprint of a person and

recognized the identification accuracy. Later the fusion of the biometric traits is recommended at feature level using all possible combinations of feature vectors. The available combination of features is delivered into fusion classifier of K-Nearest Neighbour(KNN), Support Vector Machine (SVM), Navie Bayes(NB) and Radial Basis Function(RBF). The best combination of feature vectors and fusion classifiers is recognized for the recommended multimodal biometric system. Exploratory results affirm that fusion combination outperforms individual. In their paper Soad Almabdy [4], introduced Deep learning, specifically the convolutional neural network (CNN), which has lately made excellent progress in FR technology. This paper explore the efficiency of the pre-trained CNN with multi-class support vector machine (SVM) classifier and the efficiency of transfer learning using the AlexNet model to achieve classification. The study deals with CNN architecture, which has so far listed the best outcome in the ImageNet Large-Scale Visual Recognition Challenge (ILSVRC) in the past years, more particularly, AlexNet and ResNet-50. In order to examine performance optimization of the CNN algorithm, recognition accuracy was used as a determinant. An accuracy range of 94% to 100% for models with all databases was achieved.

In their paper, Yik et.al.[6] suggest a new proposal of feature-level fusion multimodal biometrics system using indexing-first-one (IFO) hashing and integer value mapping strategy. Indexing-first-one hashing has proven survived from several major privacy attacks such as single-hash attack (SHA), attack via record multiplicity (ARM) etc. A weighted feature level fusion is recommended where multiple biometrics are given different weights based on the individual recognition result which then each biometrics will provide to the final matching result based on their respective weights. The observation is organized and result is verified using a multimodal fingerprint and iris database.

3 THE PROPOSED MODEL

The proposed model utilizes the biometric traits for authenticating a person. The model is executed based on the following 5 steps in its verification process:

a) The test images of the user are obtained by **Image Acquisition.**

b) The qualities of the acquired images are enhanced by **Preprocessing the images**.

c) The feature set necessary for further processing is obtained from **Feature Extraction process.**

d) The acquired set of features from each biometric trait are fused and it is tested with the images in the database. This is known as **Matching Process**.

e) The score from the matching process is utilized to take the final **Decision process**.

3.1 Image Acquisition

During the process the required data's from the biometric traits are acquired from the user using any hardware device. Here, Face image and Ear image are acquired through any digital camera and Fingerprint images are acquired from the user using a digital scanner. If the acquired images are not good in quality for further processing then it is utilized else the images are captured again from the same user.

3.2 Image Preprocessing

In preprocessing stage the images are cleaned from noise and only necessary portion from the image is utilized. The first step in this process is to resize the image according to the need. To do this the image is cropped. Next step in this process is converting the image to gray scale. For speedy recognition process the colored images are converted into gray scale. After the conversion the gray scale image is binarized. From the binarized image the region of interest is recognized and then it is utilized to acquire the necessary set of features.

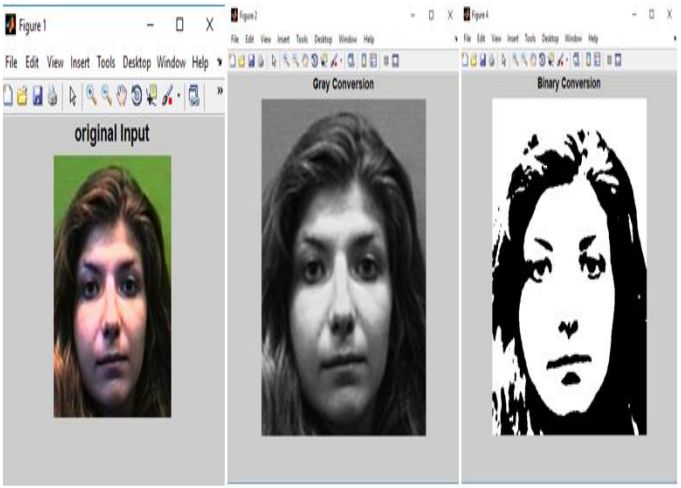


Fig 4. Face preprocessing

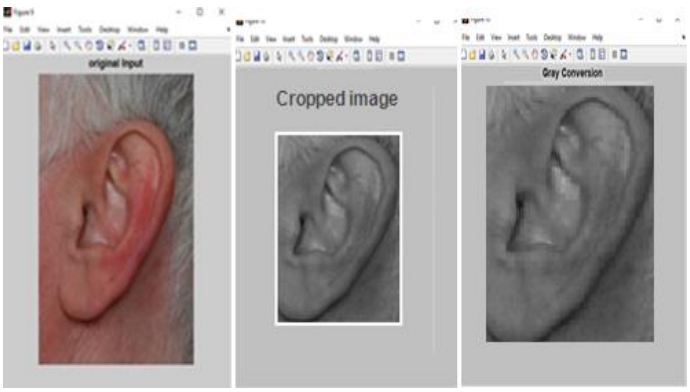


Fig 5 Ear preprocessing

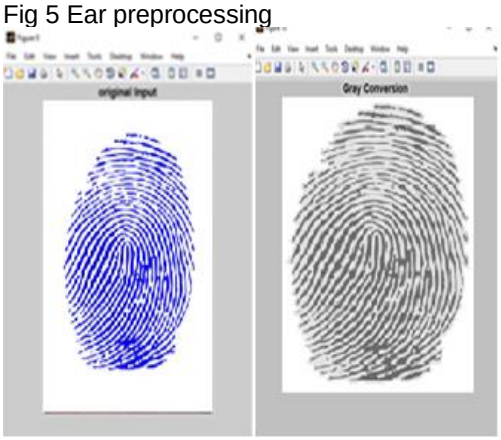


Fig 6. Fingerprint preprocessing

3.3 Feature Extraction Stage

At this stage, the set of features which are repetitive and which actually has the information necessary for the processing are extracted from the biometric traits using various algorithms. In Face biometric, the set of features are extracted through Principle Component Analysis using eigen face vectors, which is an unsupervised dimensionality reduction algorithm.
The steps in PCA algorithm are

1. Find the mean vector.
2. Accumulate all the data samples in a average adjusted matrix.
3. Produce the covariance matrix.
4. Calculate the Eigen vectors and Eigen values.
5. Calculate the basis vectors.
6. Represent every sample as a linear combination of basis vectors.

In fingerprint recognition, the thinning algorithm using minutiae is used to find the set of features for matching. First step in this process is to decrease the thickness of the ridges in the fingerprint image for accurate identification of the ridges and bifurcations in the given image. Next step is to identify the minutiae points from the refined images. Along with the orientation position, the locations of minutiae points are stored to form the required feature set. In ear, SURF technique is used to find the set of salient feature points where each point is associated with a descriptor vector of 128 feature elements. SURF provides very effective and highly distinctive features where a single feature can be used to correctly match its pair even in a large database of images.

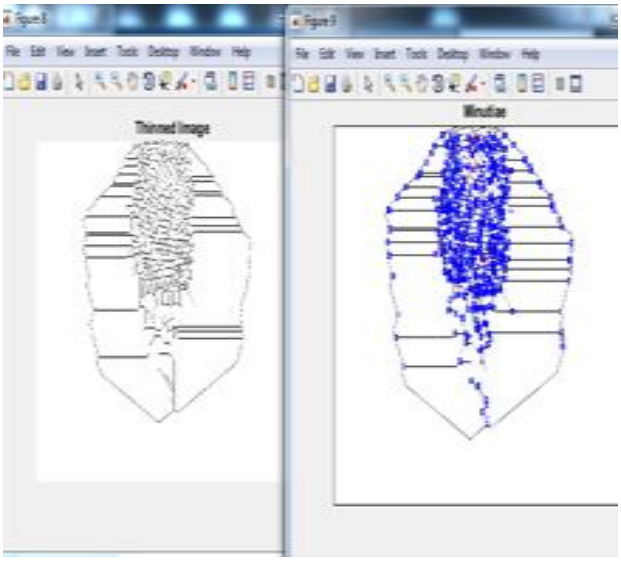


Fig 7. Minutiae extraction

MSER is used for identifying the region in the gray images. SURF is used to extract the feature set points in the region. Here the SURF points in a MSER region are grouped together to form a template. This technique was proposed to find correspondences between image elements from two images with different viewpoints. This method of extracting a comprehensive number of corresponding image elements contributes to the wide-baseline matching, and it has led to better stereo matching and object recognition algorithms.

3.4 Fusion Stage

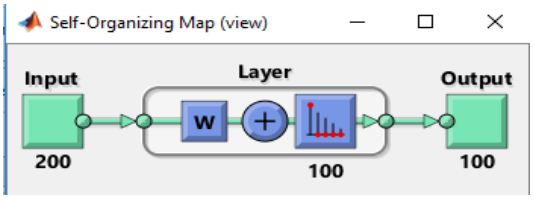
Fusion refers to the process of combining two or more biometric modalities to improve the performance of biometric systems. There are four standard fusion types including feature level fusion, score level fusion, decision level fusion and sensor level fusion. In this study, the researchers will only concentrate on applying feature level fusion .Feature level fusion refers to combining of different feature sets extracted from multiple biometric sources. In case of homogeneous feature sets, a single resultant feature vector can be calculated as a weighted average of the individual feature vectors, while in case of heterogeneous feature sets as in this study, they can be concatenated to form a single feature vector. Feature selection schemes are employed to extract the needed features from larger set of features, normalize features from multiple channels and include all in new feature vector (query vector) that has a higher dimensionality and represents a person's identity in a different hyperspace.
If 'n' traits of a subject are provided for training, the feature template for the subject is obtained by fusing the feature points of all the traits together.
Let 'n' biometric traits are available from a subject, and then fusion is represented by
FR_{fusion} = FR1 + FR2 +FR3 + ……..+ FRn
Where FR is the feature from each biometric traits and FR_{fusion} provides the feature points for the template.

3.5 Matching Stage

In the matching phase, the acquired fused information is compared with all other existing information in the database for the matching scores estimation. For matching process, K-nearest neighbor classifier along with Deep belief network is employed.

4 SIMULATION ENVIRONMENT

The projected model was executed using MATLABR2017 image process and computer vision libraries. Let discuss the check results running on neural network (deep self-organizing map) utilizing the NEURAL NETWORK TOOL enclose MATLAB. For cluster issues, the self-organizing feature map (SOM) is that the most ordinarily used network, as a result of once the network has been trained, there are several image tools which will be utilized to analyze the ensuing clusters.



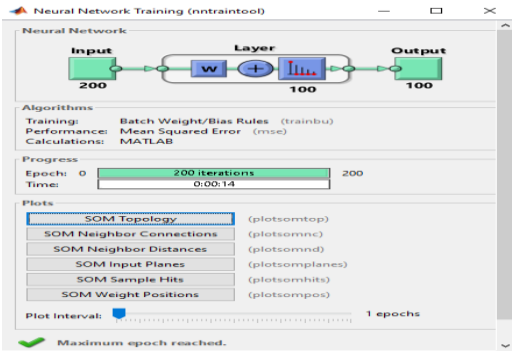


Fig 8. Network training

For SOM training, the weight vector related to every neuron moves to become the middle of a cluster of input vectors. Additionally, neurons that are adjacent to every alternative neuron in the topology ought to move near to one another within the input space, so it is attainable to visualize a high-dimensional inputs space within the two dimensions of the network topology.

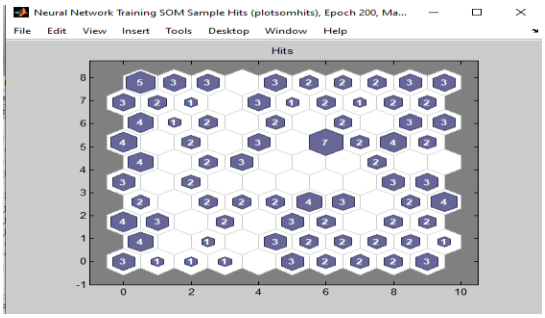


Fig 9. SOM Weight vector

This figure shows a weight plane for every part of the input vector. They're visualizations of the weights that connect every input to every neuron. (Darker colours represent larger weights.)

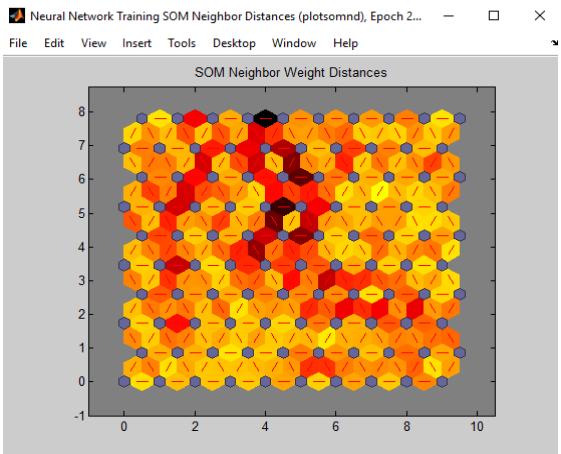


Fig10. SOM Weight plane

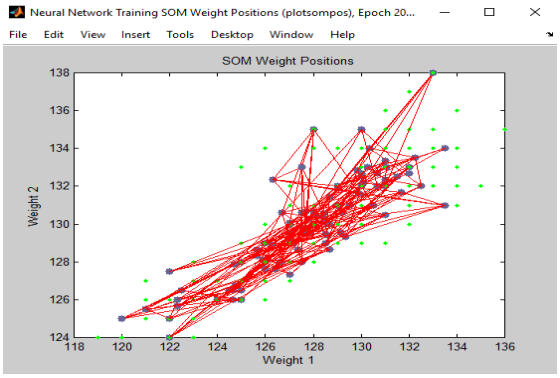


Fig 11. SOM Weight position

In this article root mean square error is employed to compute the performance of the system. RMSE is computed using the formula

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=}^{N}(O_i - P_i)^2},$$

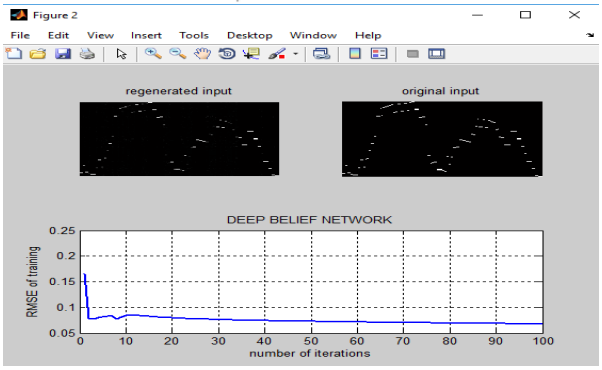


Fig 12. RMSE of training

4.1 Performance Metrics

Recognition Accuracy (RA) :

Recognition Accuracy is used in verification system and it is calculated as follows:

$$= 100 - \frac{(FAR+FRR)}{2}$$

False Acceptance Rate (FAR):

The false acceptance rate is defined as the probability of the process which wrongly accepts a unauthorized person as an authorize one. It is expressed in percentage.

FAR % = FalsePositive/(FalsePositive+TrueNegative)

False Rejection Rate (FRR):

The false rejection rate is defined as the probability of the process which wrongly rejects an authorized person from accessing the information. It is also expressed in percentage.

FRR % = FalseNegative/(TruePositive+FalseNegative)

5 RESULTS AND DISCUSSIONS

Two experiments were performed for evaluating biometrics, through the first experiment the proposed model was trained and tested using three biometric traits including face, ear and

fingerprint collected for each subject from three different databases. The database contains 100 subjects each with 3 images for face, ear and fingerprint biometrics. In the second experiment, the proposed model was trained and tested using three biometric traits including face, fingerprint and ear from three different databases. Totally 420 images of the biometric traits are used. Finally, through both experiments feature level fusion were tested and evaluated.

5.1. First Experiment with Unimodal Biometrics

The table given below demonstrates the recognition accuracy of the three studied uni-modal biometrics under consideration, clarifying that the finger print biometric achieved the highest recognition accuracy (94.9 %), while the ear biometric achieved the least accuracy (92.3%).

Table 1. Uni-biometrics recognition accuracy

UNIMODAL RECOGNITION	ACCURACY
Face	94.30%
Fingerprint	94.90%
Ear	92.30%

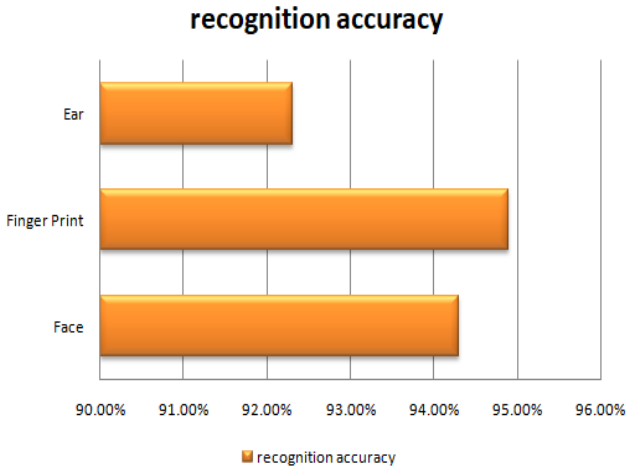


Fig 13. Unimodal recognition accuracy

Table2. unimodal recognition

UNIMODAL RECOGNITION	FRR%	FAR%
Face	0.28	0.24
Fingerprint	0.34	0.49
Ear	0.21	0.17

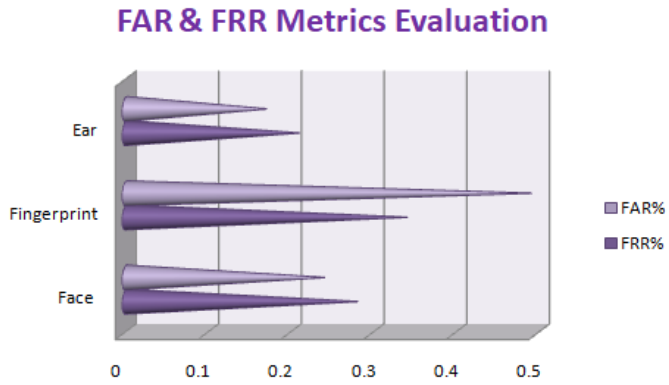


Fig 14. Unimodal FAR AND FRR chart

5.2. Second Experiment with Multimodal Biometrics

This subsection discusses the results of the two experiments' evolution based on FAR, FER and Accuracy metrics in terms of the implemented fusion type.

Feature Level Fusion

From the given table it is noticed that the face and ear multimodal achieved the highest FAR (0.14), while the face, ear and fingerprint multimodal achieved the least FAR (0.05). On the other hand, the face and finger print and the face multimodal achieved the highest FRR (0.09), while the other three multimodal systems achieved equal FRR values. As clarified in Fig. 15, the face, ear and finger print multimodal achieved the highest recognition accuracy (99 %), in which it is also comparable to the face, finger print and finger vein multimodal. The least accurate one was the ear and fingerprint multimodal achieving (91 %).

Table 3. Multimodal FAR and FRR Computation

MULTIMODAL RECOGNITION	FRR%	FAR%
Face +Ear	0.08	0.14
Face +Fingerprint	0.14	0.09
Fingerprint + Ear	0.10	0.07
Fingerprint + Ear+ Face	0.09	0.05

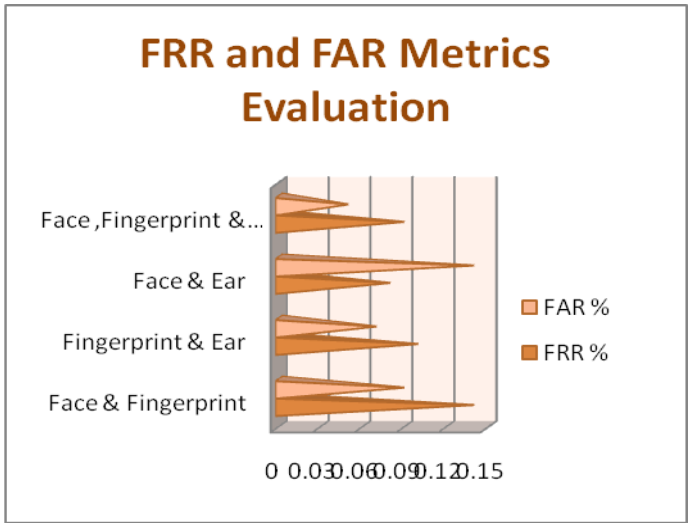


Fig. 15 FRR and FAR metrics evaluation in multimodal biometric systems

Table 4. Multimodal recognition accuracy

MULTIMODAL RECOGNITION	ACCURACY
Face +Ear	94.60%
Face +Fingerprint	93.10%
Fingerprint + Ear	91.40%
Fingerprint + Ear+ Face	99.70%

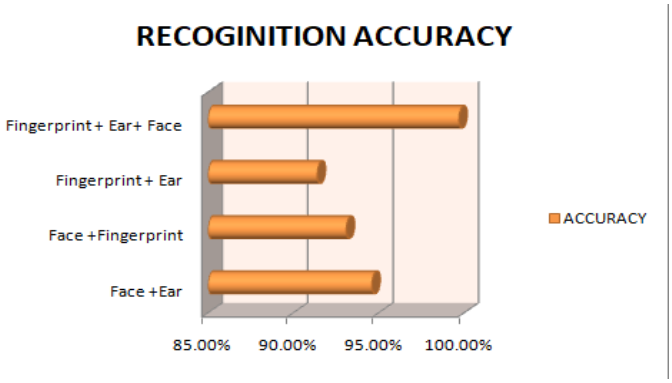


Fig16. Multimodal recognition accuracy

From the above results, it is observed that the uni-modal biometrics suffer from technical problems considering cameras and sensors which the researcher tried to simulate through distorting 20 % of the test dataset, to provide a real measurement of all systems. Examining the accuracy results of the uni-modals illustrates that finger prints have superiority over face which slightly affect integrating them in multimodal systems. It is also determined that the face, finger print and ear achieved really good results in terms of accuracy which can be imputed to the development in finger print scanners and the progress in preprocessing techniques as finger print represent the most exhausted biometric though researches.

6 Conclusion

The popularity of multimodal biometric systems has increased, due to the increasing need of seeking secured authentication. By using multimodal biometric systems, researchers become able to overcome the limitations of uni-modal biometric systems. So different fusing techniques had been released and exploited to build new accurate and effective multimodal biometric systems using two or three or even four biometrics. Hence, this paper presented and developed a comparative model based on MATLAB R2017b simulator, CASIA and KAGGLE databases to investigate the performance of multimodal biometric systems In this paper multimodal biometric system using face, ear and fingerprint is implemented. Feature level fusion is used as in involves high information and the results shows high accuracy in person authorization.

References

[1] M.Abernethy "User authentication incorporating feature level data fusion of multiple biometric characteristics". Doctoral Dissertation, Murdoch University(2011).

[2] A.Ross, A.K. Jain "Multimodal biometrics: an overview". European Signal Processing Conference. IEEE, (2004)

[3] Liau, Heng & Isa, Dino. (2011). "Feature selection for support vector machine-based face-iris multimodal biometric system". Expert Syst. Appl.. 38. 11105-11111. 10.1016/j.eswa.2011.02.155.

[4] Soad Almabdy and Lamiaa Elrefaei "Deep Convolutional Neural Network-Based Approaches for Face Recognition". Appl. Sci. 2019, 9(20), 4397; https://doi.org/10.3390/app9204397

[5] Somashekhar1 B M and Y.S.Nijagunarya."Fingerprint Fusion System For Identity Authentication Using Fusion Classifiers". International Journal of Computer Science & Engineering Survey

[6] (IJCSES) Vol.9, No.1/2/3, Aug 2018 DOI:10.5121/ijcses.2018.9301 1. [6] Yik-Herng Khoo,Bok-Min Goi, Tong-Yuen Chai, Yen-Lung Lai, Zhe Jin. "Multimodal Biometrics System Using Feature-Level Fusion of Iris and Fingerprint". ICAIP '18: International Conference on Advances in Image Processing June 2018 Pages6–10 https://doi.org/10.1145/3239576.3239599

[7] H.Benaliouche, M.Touahria, "Comparative study of multimodal biometric recognition by fusion of iris and fingerprint". Sci. World J. **2014**, 13 pp.

[8] A.J.Lakshmi, I.R.Babu, P.S.Kiran, "Multimodal biometrics in identity". Int. J. Inf. Technol. **5**(1), 111–115 (2012)

[9] B.M.Shruthi, M.M.Pooja, R.G.Ashwin, "Multimodal biometric authentication combining finger vein and finger print". Int. J. Eng. Res. Dev. **7**(10), 43–54 (2013)

[10] J.Galbally, S.Marcel, J.Fierrez, "Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition". IEEE Trans. Image Process. **23**(2), 710–724 (2014)

[11] He, F.; Liu, Y.; Zhu, X.; Huang, C.; Han, Y.; Chen, Y.: Score level fusion scheme based on adaptive local Gabor features for face–iris-fingerprint multimodal biometric. J. Electron. Imag- ing **23**(3), 033019 (2014)

[12] D.Menotti, G.Chiachia, A.Pinto, "Deep representations for iris, face, and fingerprint spoofing detection". IEEE Trans. Inf. Forens. Secur. **10**(4), 864–879 (2015)

[13] Hossain Md., Islam Md. "Fingerprint matching through minutiae based feature extraction method". Am. J. Sci. Technol. **2**(6), 262– 269 (2015)

[14] H.Mehrotra, A.Rattani, P.Gupta, "Fusion of iris and fingerprint biometric for recognition". In: International Conference on Signal and Image Processing, ppp. 1–6 (2006)

[15] A. P. Yazdanpanah, K. Faez and R. Amirfattahi, "Multimodal biometric system using face, ear and gait biometrics," *10th International Conference on Information Science, Signal Processing and their Applications (ISSPA 2010)*, Kuala Lumpur, 2010, pp. 251-254.doi: 10.1109/ISSPA.2010.5605477

[16] Lorenzo Luciano and Adam Krzyżak. 2009. Automated Multimodal Biometrics Using Face and Ear. In Proceedings of the 6th International Conference on Image Analysis and Recognition (ICIAR '09). Springer-Verlag, Berlin, Heidelberg, 451–460. DOI:https://doi.org/10.1007/978-3-642-02611-9_45

[17] Benaliouche, Houda & Touahria, Mohamed. (2014). Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint. TheScientificWorldJournal. 2014. 829369. 10.1155/2014/829369.