IMPLEMENTATION & RESULT OF GABOR-HOG, ADVANCED OPTIMIZED FUZZY INFERENCE SYSTEM, ADVANCED CONVOLUTIONAL NEURAL NETWORK, ARTIFICIAL BEE COLONY (ABC) WITH ARTIFICIAL-NEURAL-NETWORK (ANN) (ABC-ANN).

B. Karthikeyan[1] & Dr. M. Sengaliappan[2]

[1]*Research Scholar, Department of Computer Science, Kovai Kalaimagal College of Arts and Science, Coimbatore.*

[2]*Associate Professor and Head, Department of MCA, Nehru College of Management, Coimbatore.*

ABSTRACT

Biometric is emerging technology in identification and authentication of human being with more reliable and accurate. It is hard to imitate, forge, share, distribute and cannot be stolen, forgotten. Combining multiple biometric systems is a promising solution to provide more security. It eliminates the disadvantages of uni model 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 methods in this research depicts a multimodal biometric algorithm which is designed to recognize individuals for robust and secured authentication using normalized score level fusion techniques for optimization in order to reduce False Acceptance Rate and False Rejection Rate and to enhance accuracy. In this research work, the multimodal biometric algorithm integrates Iris and Finger Print biometric traits for their best biometric characteristics. Each biometric trait is adapted for pre-processing techniques such as localization and normalization, before recognition in order to improve the image quality and recognition rate, each trait 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 Machine Learning Algorithms for robust authentication, enhanced security and accuracy. It eliminates the flaws, vulnerabilities and threats of using uni-modal biometric algorithm for authentication. This research were categorized into three phases with different techniques are combine to perform efficiently and yield best results in optimization. Finally, the performance of

the algorithms in different phases is evaluated by metrics as False Acceptance Rate, False Rejection 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 FVC-2004 Dataset for fingerprint and CASIA Datasets for Iris. The database includes multimodal data from 106 individuals. The database is obtained with authenticated agreement from the research website experimental analysis. All the biometric data are obtained from the same person, it impacts accuracy. The experimental results show that accuracy is improved in Phase 3 when compared to Phase 1 and 2 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 higher Accuracy and hence proves that multimodal biometric algorithm provides best authentication.

INTRODUCTION

BIOMETRICS

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 behavioural 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. Behavioural characteristics of biometrics are Gait analysis, Keystroke dynamics, Signature, Voice ID, Mouse use characteristics, and Cognitive biometrics.

Biometrics provides security in terms of verification and identification modes. Verification means how a person can be uniquely identified by evaluating one or more distinguishing biological traits. It compares 1:1 matching and verifies a claimed identity with only one template whereas identification is done with 1:N matching, means many comparisons are made by verifying an input template with whole database to identify a person. It consumes more time because it verifies with entire database and it possess the characteristics of static, high risk, covert, physiological, and centralized database in nature.

Traditional methods of identifying a person are classified as something you know such as password, PIN, or piece of privacy information, something you have such as key, smart card or token. But biometric is identifying a person by something you are. Traditional methods such as possession and knowledge based approaches are easily guessed by imposters because of 25% of people seem to write their PIN on their ATM card and other factors like this. Estimation of annual identity fraud damages in USA alone is $1 billion in credit card transactions, $1 billion in fraudulent cellular phone use, and $3 billion in ATM withdrawals.

The vulnerabilities and threats of traditional identification systems such as forgotten, stolen, lost, forged, duplicated, spoofed, hacked and shared are eliminated and the limitations of unimodal biometric systems such as noise in sensed data, intra-class variations, distinctiveness, non-universality, susceptibility to circumvention, spoof attacks, unacceptability and inter class similarities.

BIOMETRIC TRAITS

These attributes are regarded as more dependable as unique attributes of an individual which do not alter because of changes in psych emotional states. Physical systems of identification handle statistical features of an individual such as fingerprint, iris, face, hand geometry, DNA, Ear Pattern, Lip Biometrics, Vein Biometrics, Palm print, and Heart Sound. In this research work we used both fingerprint and Iris biometric traits.

Fingerprint:

Fingerprints are vastly considered as a reliable biometrics recognition technique. Fingerprint scanners are available for affordable costs and being incorporated at a rapid pace in laptops and other portable ICT gadgets. Almost all fingerprint recognition systems examine the unique patterns of ridges and valleys. Moreover, the arrangements of small unique marks on the fingerprint are called minutiae. They may be recognized and distinguished by their kind x and y which coordinate by direction.

Iris:

Iris in the eye possesses attributes which may be used for identifying individuals with a degree of accuracy better than other biometric systems. Similar to fingerprint and thermo gram, an iris pattern is singular and can be used for differentiating even identical twins. Images of the iris may be obtained through usage of video cameras within a distance of one meter. It is a biometric identification tool which utilizes high-resolution images of the iris of the eye which is adequate for authentication purpose. It is an internal organ that is protected from all damage and wear. It is virtually flat and uniform in all

situations and has a textile that is distinguishable even amongst the genetically identical twin

BIOMETRICS TYPES

Biometric systems are recognition systems that have their basis in a model that obtains biometric features from an individual and extracts a group of particular vectors which are contrasted with a set of models from the dataset.

(i) Unimodal Biometrics

Unimodal biometric verification systems are more dependable than traditional authentication models. These systems carry out person recognition on the basis of one of the sources of biometric data. These systems often face the restrictions and issues given below:

- Lack of universality in certain features
- Noise from the signals obtained because of wrong usage by clients or other environmental factors like humidity, dirt or dust.
- Fingerprints with scars, modified voice because of a cold are instances of noise-filled input or defective or incorrectly maintained sensors.
- Lack of safety of the used sensors.
- Restrictions of the discriminative capacity of the biometrics system because of great in-class and less inter-class difference.
- Recognition performance of systems has an upper limit at a particular level.
- High error rates for unimodal biometrics systems.
- Lack of permanence and variability with time of the biometric feature.
- Possibility of fraud through voluntary or involuntary duplication of biometric feature.

Unimodal biometric systems are the most popular one used in several applications. Due to its disadvantages and shortcomings of the unimodal system, several users are turning toward multimodal biometric systems for providing maximal levels of correct authentications.

(ii) Multimodal Biometrics

Restrictions of the unimodal biometric system may be the reason for the usage of multimodal biometric system. It utilizes several sensors or biometrics for overcoming the various restrictions in the unimodal system. Multimodal biometric system is anticipated to be more dependable because of the presence of several and independent sets of proof of identity. The system is also capable of meeting the rigorous performance requisites

demanded by several applications. Certain multimodal systems involve human-computer dialogue-based interaction systems where users interact with the computer through either voice or vision or similar pointing devices for completing particular tasks. Multimodal biometric system refers to that which is capable of utilizing several physical or behavioural characteristics for enrolling, verifying and identifying individuals.

The multimodal biometric system addresses the issue of lack of universality. Since several features are used, it ensures adequate population coverage. Furthermore, the multimodal biometric system provides anti-spoofing strategies by ensuring that it is hard for intruders to concurrently spoof several biometric features of legitimate users.

Multimodal systems are capable of combining several independent biometrics and overcoming certain restrictions which arise from utilizing merely a single biometric feature as a verification tool. Multimodal biometric systems are typically resilient to spoof attacks as they are harder to spoof several biometric features than to spoof one feature. Since they provide excellent accuracy rates and excellent protection against frauds. In multimodal biometric systems, failure in one particular tool will not considerably impact the person identification because others may be used with success. Therefore, fraudulent attacks may be reduced to a minimum by enhancing the efficacy of the total system. Multimodal biometric systems possess the potential to be vastly employed in a huge range of common applications such as ATM security, credit card transactions, access to databases and so on. Decisions made by multimodal biometric systems are either 'genuine individuals' or 'imposter'. ***Thus, in this research work we used multimodal biometric system due to its vast advantages.***

Advantages of Multi-Biometric Systems over a Unimodal Biometric System:

- Improved security: Since multimodal systems use several biometric features from a single person and are more difficult to spoof or obtain two or more attributes from a person.
- Multiple Fingerprints Scanner support
- Multiple IRIS Scanner support

Applications

- Multi-biometric systems are used in India for generating the Aadhar Card. The multimodal system utilizes facial recognition, iris recognition and fingerprints recognition.
- Multi-biometric systems are used in airports and banking sectors.

FUSION IN BIOMETRICS

Fusion is an advanced method that shows a lot of potential in increasing the accuracy of the system. Several biometric features such as fingerprint, palm vein, finger surface, facial feature, iris and hand geometry are fused with palm print at score or representation levels. Fusing these on other hand, attributes like hand geometry or finger surface with palm print enables all the features to be extracted from the samples. Information fusion is required for arriving at a unanimous decision with regard to multimodal biometric systems. Biometric sensors offer raw image information obtained from the person to be verified. Signal processing algorithms extract the feature vectors from the raw information and matching algorithms offer match data. All these data from various sources are fused for the decision making procedure.

Fusion is proven to enhance the accuracy of biometrics classification and surpass the shortcomings of individual classifiers. In addition, in the case of a missing modality, multimodal biometric fusion systems are capable of performing classification decisions through the usage of one of the present modalities in a conventional method. Multimodal biometric fusion is like (in spirit) bagging, stacking and other methods for fusing complementary classifiers. For instance, in bagging, outputs of two or more classifiers may be fused through voting for achieving more accurate classification outcomes. In fusion many types are available such as feature level fusion, score level fusion, etc. In this research we used score level fusion.

Score-Level Fusion:

Here, matching score outputs of several experts are fused for generating novel output (scalar or vector) which may be used for making decisions. Fusion in this level is the most common one because it is easy to access and process match scores as opposed to raw information or features set which is extracted from the raw data. Fusion schemes at this level are grouped into three: density-based strategies (generative method), classifier-based strategies (discriminative method) and transformation-based strategies.

PERFORMANCE MEASUREMENTS OF BIOMETRICS

- The biometric systems efficiency is found in conditions of false rejection rate (FRR), false acceptance rate (FAR), failure to enroll rate (FER), enrolment time, and verification time.
- The false acceptance rate (FAR) is predominant while protection is a priority whereas low false rejection rate are appreciated whilst comfort is the precedence.
- The failure to enroll rate (FER) is the metric to measure the number of person's whose biometric could not be enrolled. Both the enrolment and recognition

occasions are primary reasons in deciding upon or checking of procedure efficiency.

- The enrolment time is that timeline in between and together with the pictures of the biometric pattern and developing the stored template of that sample. The verification time is a time required to finish the matching of the individual.

PHASE 1 (ADVANCED OPTIMIZED FUZZY INFERENCE SYSTEM)

- To validate and perform an appraisal and evaluation of our proposed model with existing Multi-modal biometric recognition schemes, we used upcoming procedures.
- (i) For this application, we used data for IRIS images from the datasets CASIA Iris-V2 and we used data for Fingerprint images from the datasets FVC2004 fingerprint image, which were free sources for researchers
- (ii) First, the procedures are carried out separately in a unimodal iris recognition system. The extractor for Iris is based on the method of Daugman. Daugman produces an Iris code composed of bit streams called Iris code. The corresponding score is given by the distance of hamming.
- (iii) Secondly, the procedures are carried out separately in a unimodal fingerprint framework. The extraction method to retrieve the information was carried out using a Minutia based fingerprint recognition. It locates the area of concern and the Region of Interest (ROI) for minutiae extraction. The Matching was done according to the distance of Euclidian.
- (iv) Finally, the authentication process is applied by utilizing the Gabor-HoG fusion match and AOFIS fusion matching inside a Multi-modal biometric identification with integrated iris and fingerprint.

The database is first to split into two parts: 40% of the database is allocated for registration for calculation of classifier parameters and database with 60% are utilized for the classifier testing and validation.

- (i) Genuine Recognition Attempts Here finger impression of each template was compared with the finger impressions of remaining by a unique person, also symmetric matches are prevented.
- (ii) Imposter Recognition Attempts: Here first finger impression template was compared with the first impressions of a remaining person, also symmetric matches are prevented.

- (iii) Genuine Recognition Attempts: Here iris of each template was compared with the iris of remaining by a unique person, also symmetric matches are prevented
- (iv) Impostor Recognition Attempts: Here first iris template was compared with the first iris of remaining person, also symmetric matches are prevented.
- Tests were carried out on a series of image data of 50 participants for studies utilizing the proposed framework. These involve five fingerprint images from the fingerprint database FVC 2004 and five CASIA-Iris V2 iris image database.
- The Error Rates are termed as FAR and FRR. The False Acceptance Rate (FAR) is to validate the risk of an individual becoming misidentified as another user.
- The False Rejection Rate (FRR) is to validate the possibility that a reported person is not detected by the method. According to the statistical analysis we have used the above experiments to determine the inter-class and intra-class thresholds to identify the FAR and FRR. By varying the threshold values we can identify which method provides better efficiency.
- The performance of False Acceptance Rate (FAR) was compared for both Gabor-HOG and AOFIS with different threshold levels shown in Table 3.1 and Figure 3.1. The threshold level means about the quality of the images from 1.0 good quality to 5.0 bad quality.

TABLE 3.1 FAR Comparison

Threshold	Gabor-HOG	AOFIS
1.5	0.4	0
2.5	0.7	0.1
3.5	1.3	0.3
4.5	2.7	0.6
5.5	3.9	0.9

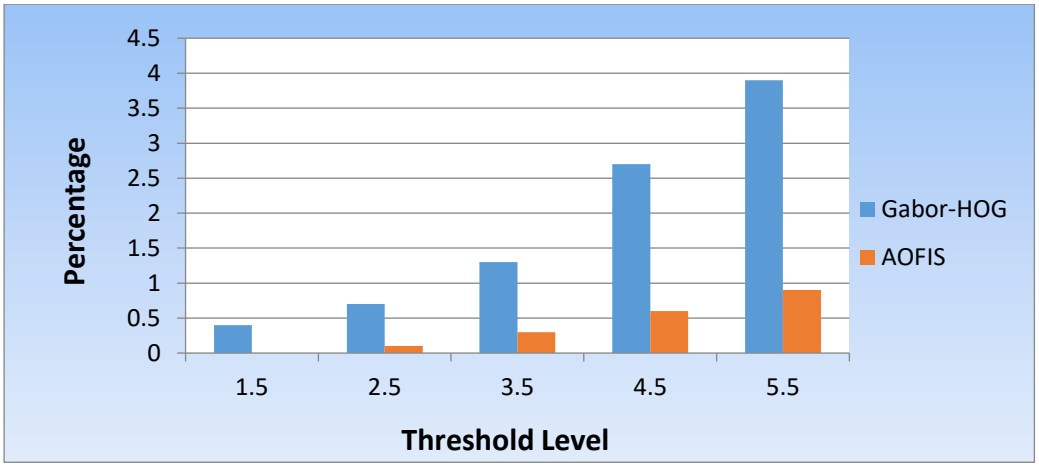

FIGURE 3.1 FAR Comparison Graph

The performance of False Rejection Rate (FRR) was compared for both Gabor-HOG and AOFIS with different threshold levels shown in Table 3.2 and Figure 3.2.

TABLE 3.2 FRR Comparison

Threshold Level	Gabor-HOG	AOFIS
1.5	10	0
2.5	30	4
3.5	45	15
4.5	70	25
5.5	95	30

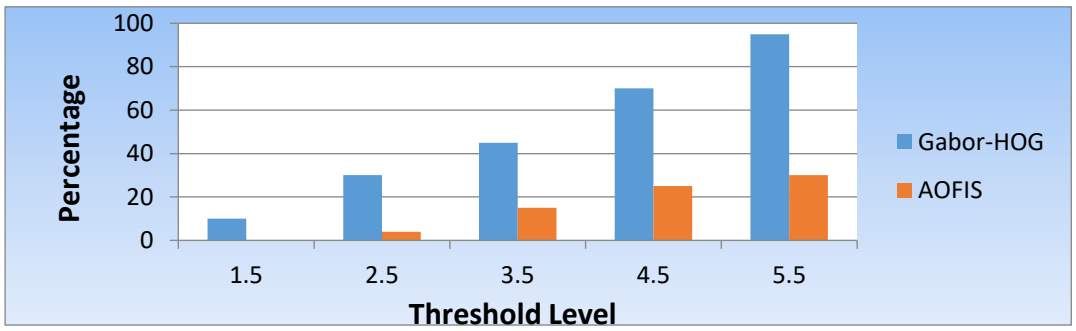

FIGURE 3.2 FRR Comparison Graph

ACCURACY:

Comparison of the accuracy is done for both existing and proposed models. For biometrical application the accuracy of the process is evaluated as follows:

$$AC = 100 - \frac{FRR + FAR}{2}.$$

Based on the findings, it concludes that the accuracy of the proposed AOFIS decision-making method is higher than that of the existing Gabor-HOG method.

This study reveals that the method introduced offers better performance following the results of individual unimodal systems and the results of multimodal systems applied with typical matches.

The performance of Accuracy was compared for both Gabor-HOG and AOFIS with different threshold levels shown in Table 3.3 and Figure 3.3.

TABLE 3.3 Accuracy Comparison

Threshold Level	Gabor-HOG	AOFIS
1.5	75	90
2.5	60	82
3.5	50	79
4.5	40	72
5.5	35	65

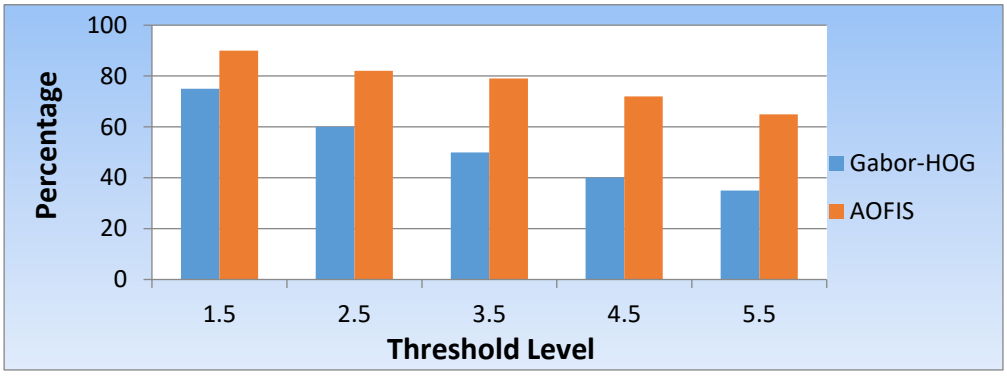

FIGURE 3.3 Accuracy Comparison Graph

The storage space complexity is evaluated as the amount of memory space is consumed to store the constructed template in the server. The space complexity is measured in terms of KiloBytes (KB). The lower value of space complexity ensures better performance of the technique.

Table 3.4: Storage Comparison

NUMBER OF USER DATA	GABOR-HOG	AOFIS
10	**390**	**230**
20	**460**	**310**

30	570	430
40	790	610
50	970	750

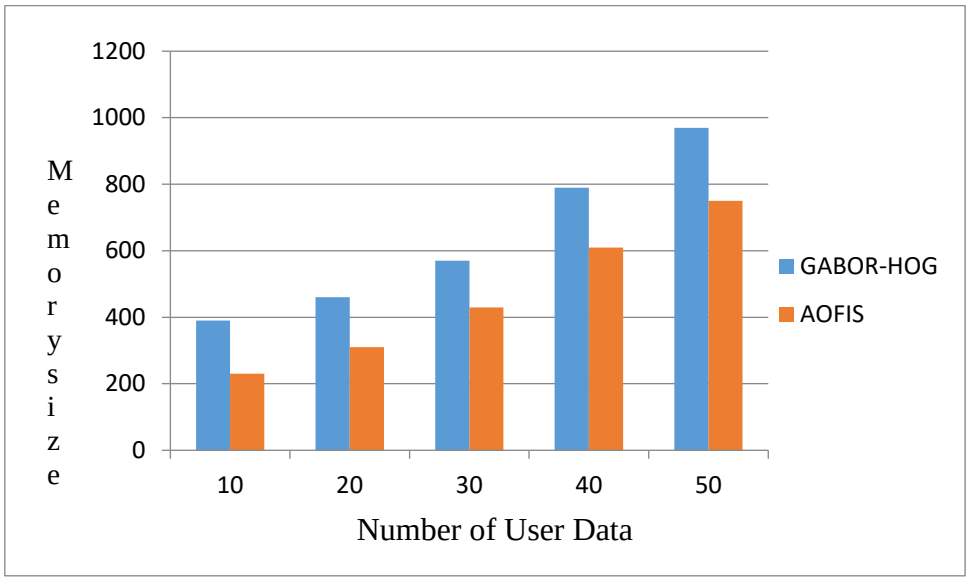

FIGURE 3.4 Storage Comparison Graph

Phase 2 (ADVANCED CONVOLUTIONAL NEURAL NETWORK)

To validate and perform an appraisal and evaluation of this proposed ACNN model with existing AOFIS multi-modal biometric recognition schemes, we used upcoming procedures:

(i) For this application, we used data for IRIS images from the datasets CASIA Iris-V2 and we used data for Fingerprint images from the datasets FVC2004 fingerprint images, which were free sources for researchers.

(ii) First, the procedures are carried out separately in a unimodal fingerprint framework. The ridge thinning method was used for feature extraction to retrieve the information was carried out using a Minutia based fingerprint recognition. It locates the area of concern and the Region of Interest (ROI) for minutiae extraction.

(iii) Secondly, the procedures are carried out separately in a unimodal iris recognition system. The extractor of features for Iris is based on the method of Dogman's Rubber Sheet Model. This produces an Iris code composed of bit streams called Iris code. The corresponding score is given by the distance of hamming.

(iv) Thirdly, the Matching was done according to the distance of Euclidian.

(v) Finally, the authentication process is applied by utilizing the ACNN classifier with Score-Level fusion matching inside a Multi-modal biometric identification with integrated iris and fingerprint.

The database is first to split into two parts: 40% of the database is allocated for registration for calculation of classifier parameters and a database with 60% is utilized for the classifier testing and validation.

(i) Genuine Recognition Attempts: Here finger impressions of each template were compared with the finger impressions of remaining by a unique person, also symmetric matches are prevented.

(ii) Imposter Recognition Attempts: Here first finger impression templates were compared with the first impressions of a remaining person, also symmetric matches are prevented.

(iii) Genuine Recognition Attempts: Here iris of each template were compared with the iris remaining by a unique person, also symmetric matches are prevented.

(iv) Impostor Recognition Attempts: Here first iris template was compared with the first iris of the remaining person, also symmetric matches are prevented.

Tests were carried out on a series of image data of 50 participants for studies utilizing the proposed framework. These involve five fingerprint images from the fingerprint database FVC 2004 and five CASIA-Iris V2 iris image databases.

The Error Rates are termed as FAR and FRR. The False Acceptance Rate (FAR) is to validate the risk of an individual becoming misidentified as another user.

The False Rejection Rate (FRR) is to validate the possibility that a reported person is not detected by the method. According to the statistical analysis we have used the above experiments to determine the inter-class and intra-class thresholds to identify the FAR and FRR. By varying the threshold values we can identify which method provides better efficiency.

The performance of FAR was compared for both AOFIS and ACNN models with different threshold levels shown in Table 4.1 and Figure 4.1.

The threshold level means about the quality of the images from 1.5 good quality to 5.5 bad quality.

Table 4.1: FAR Comparison

Threshold	AOFIS	ACNN
1.5	0	0
2.5	0.1	0

3.5	0.3	0.1
4.5	0.6	0.3
5.5	0.9	0.5

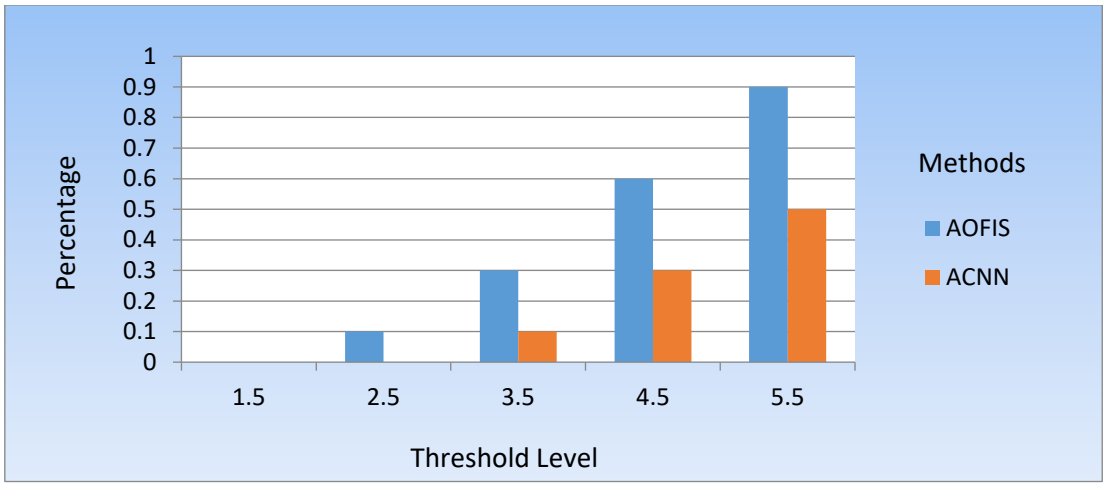

Figure 4.1: FAR Comparison Graph

The performance of FRR was compared for both AOFIS and ACNN models with different threshold levels shown in Table 4.2 and Figure 4.2.

Table 4.2: FRR Comparison

Threshold	AOFIS	ACNN
1.5	0	0
2.5	4	1
3.5	15	6
4.5	25	11
5.5	30	16

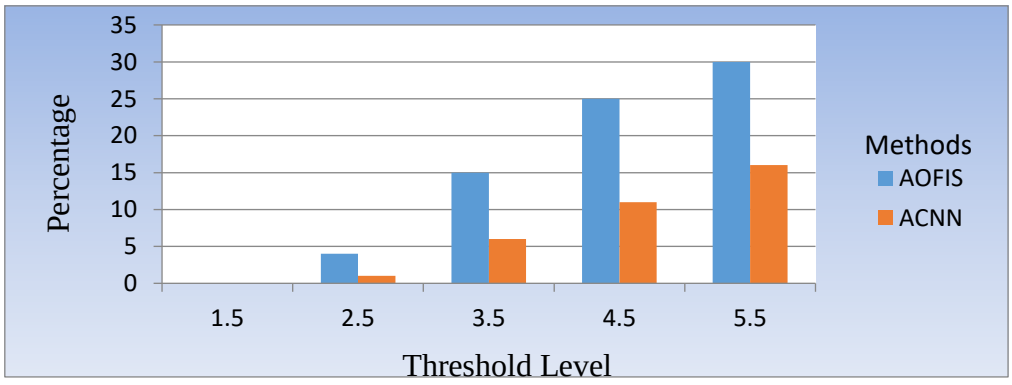

Figure 4.2: FRR Comparison Graph

Accuracy:

Comparison of the Accuracy-Rate is done for both AOFIS and ACNN models. For biometrical application the accuracy of the process is evaluated as follows:

$$AC = 100 - \frac{FRR + FAR}{2}.$$

Based on the findings, it concludes that the accuracy of the ACNN method is higher than that of the AOFIS method. This study reveals that the method introduced offers better performance following the results of individual unimodal systems and the results of multimodal systems applied with typical matches. The performance of Accuracy was compared for both AOFIS and ACNN models with different threshold levels shown in Table 4.3 and Figure 4.3.

Table 4.3: Accuracy Comparison

Threshold	AOFIS	ACNN
1.5	90	95
2.5	82	91
3.5	79	87
4.5	72	83
5.5	65	79

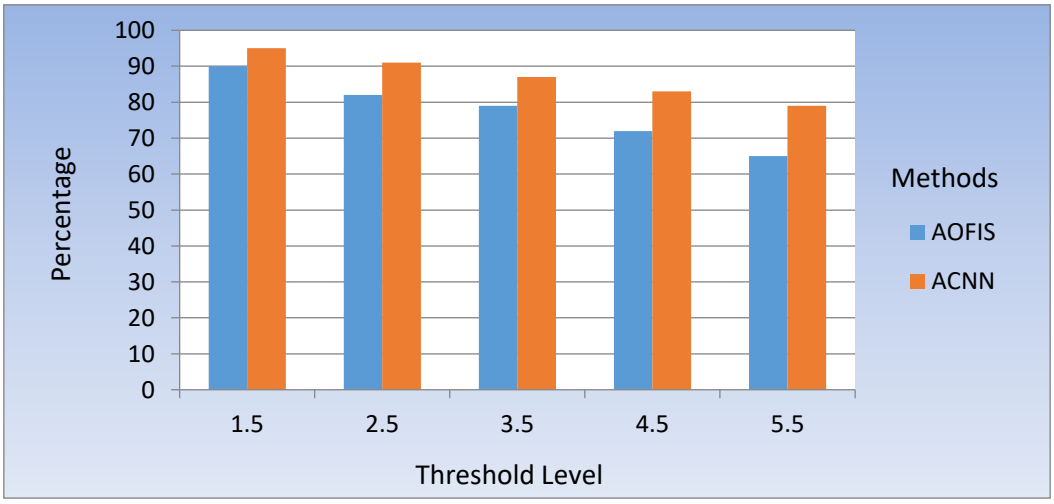

Figure 4.3: Accuracy Comparison Graph

The storage space complexity is evaluated as the amount of memory space is consumed to store the constructed template in the server. The space complexity is measured in terms of KiloBytes (KB). The lower value of space complexity ensures better performance of the technique.

Table 4.4: Storage Comparison

NUMBER OF USER DATA	GABOR-HOG	AOFIS	ACNN
10	390	230	190
20	460	310	280
30	570	430	370
40	790	610	460
50	970	750	550

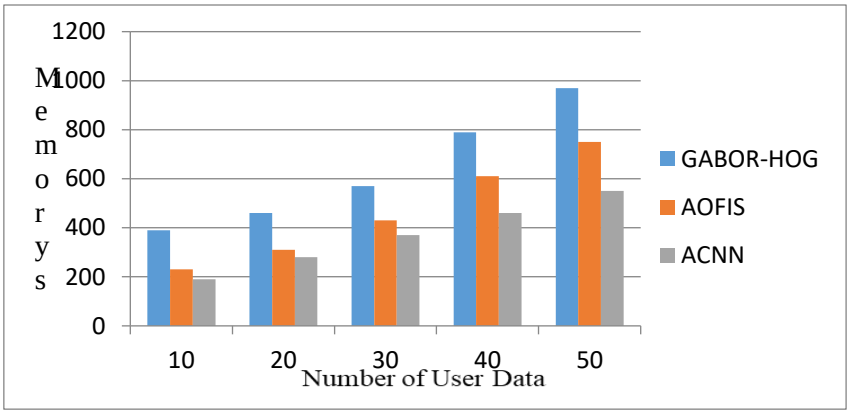

FIGURE 4.4 Storage Comparison Graph

Phase 3 (ARTIFICIAL BEE COLONY WITH ARTIFICIAL-NEURAL-NETWORK)

Tests were carried out on a series of image data of 50 participants for studies utilizing the proposed framework. These involve five fingerprint images from the fingerprint database FVC 2004 and five CASIA-Iris V2 iris image databases.

The Error Rates are termed as FAR and FRR. The False Acceptance Rate (FAR) is to validate the risk of an individual becoming misidentified as another user.

The False Rejection Rate (FRR) is to validate the possibility that a reported person is not detected by the method. According to the statistical analysis we have used the above experiments to determine the inter-class and intra-class thresholds to identify the FAR and FRR. By varying the threshold values we can identify which method provides better efficiency.

The performance of FAR was compared for both proposed and existing models with different threshold levels shown in Table 5.1 and Figure 5.1. The threshold level means

about the quality of the images from 1.5 good quality to 5.5 bad quality. The results shows that phase 3 (ABC-ANN) produce lower FAR Rate when compare it with base paper (GABOR-HOG), phase 1 (AOFIS), phase 2 (ACNN)

Table 5.1: FAR Comparison

THRESHOLD LEVEL	GABOR-HOG	AOFIS	ACNN	ABC-ANN
1.5	0.4	0	0	0
2.5	0.7	0.1	0	0
3.5	1.3	0.3	0.1	0
4.5	2.7	0.6	0.3	0.1
5.5	3.9	0.9	0.5	0.3

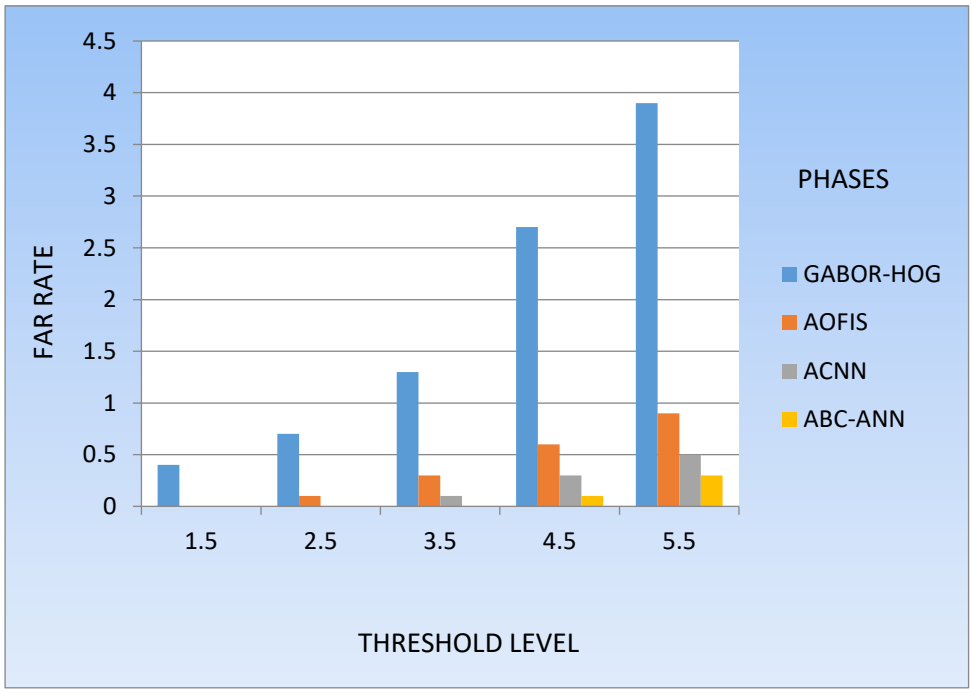

Figure 5.1: FAR Comparison Graph

The performance of FRR was compared for all phases and base paper models with different threshold levels shown in Table 5.2 and Figure 5.2. The threshold level means about the quality of the images from 1.0 good quality to 5.0 bad quality. The results shows that phase 3 (ABC-ANN) produce lower FRR Rate when compare it with base paper (GABOR-HOG), phase 1 (AOFIS), phase 2 (ACNN).

Table 5.2: FRR Comparison

THRESHOLD LEVEL	GABOR-HOG	AOFIS	ACNN	ABC-ANN
1.5	10	0	0	0

2.5	30	4	1	0
3.5	45	15	6	2
4.5	70	25	11	4
5.5	95	30	16	7

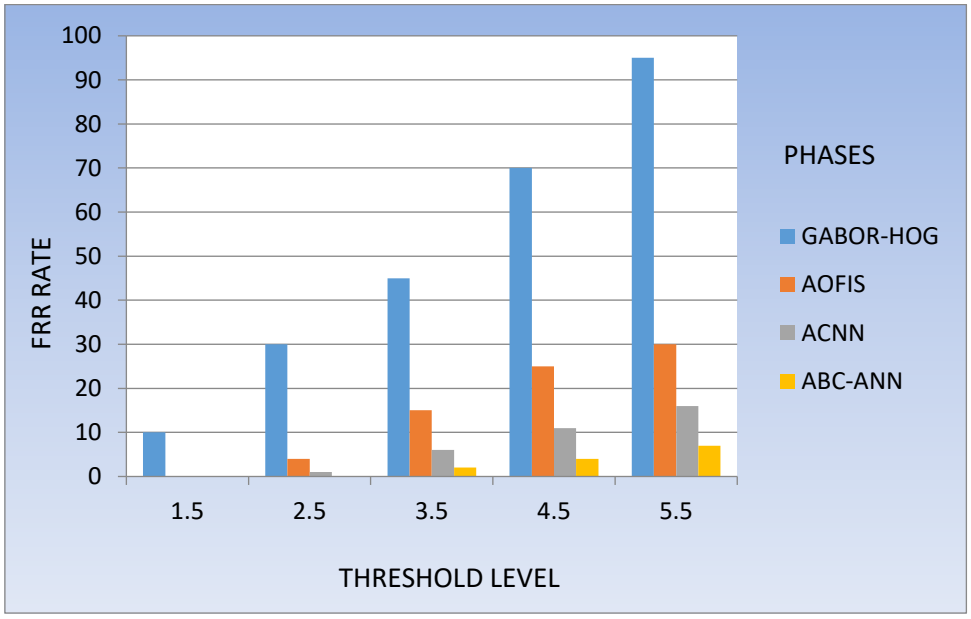

Figure 5.2: FRR Comparison Graph

Comparison of the Accuracy-Rate is done for each phases and basepaper models. Based on the findings, it concludes that the accuracy of the phase 3 method is higher than that of the base paper, phase 1 and phase 2 methods. This study reveals that the phase 3 offers better performance following the results of multimodal systems applied with typical matches. The performance of Accuracy was compared for all phases with different threshold levels shown in Table 5.3 and Figure 5.3.

Table 5.3: Accuracy Comparison

THRESHOLD LEVEL	GABOR-HOG	AOFIS	ACNN	ABC-ANN
1.5	75	90	95	99
2.5	60	82	91	97
3.5	50	79	87	94
4.5	40	72	83	91
5.5	35	65	79	87

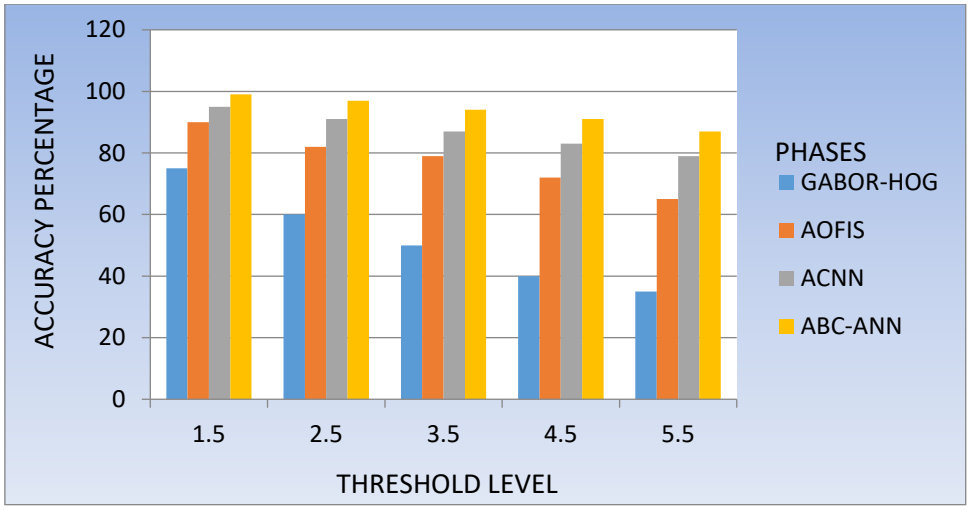

Figure 5.3: Accuracy Comparison Graph

The storage space complexity is evaluated as the amount of memory space is consumed to store the constructed template in the server. The space complexity is measured in terms of KiloBytes (KB). The lower value of space complexity ensures better performance of the technique.

Table 5.4: Storage Comparison

NUMBER OF USER DATA	GABOR-HOG	AOFIS	ACNN	ABC-ANN
10	390	230	190	90
20	460	310	280	160
30	570	430	370	230
40	790	610	460	310
50	970	750	550	390

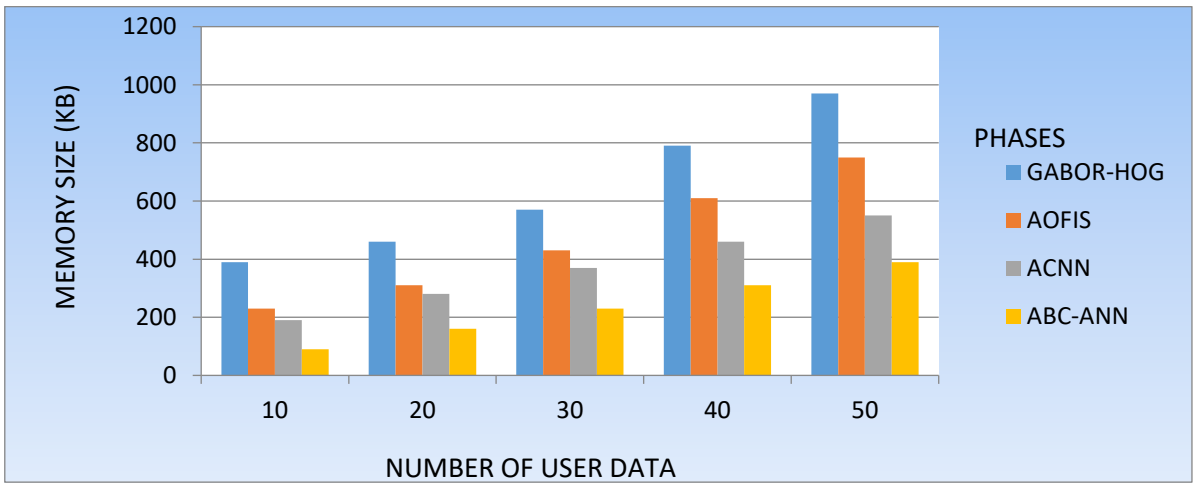

Figure 5.4: Storage (Memory Size) Comparison Graph

Table5.4 and Figure 5.4 shows the experimental results of the storage space complexity based on the different number of biometric templates.

The number of biometric template data is considered from the range of 10 to 50 which is taken as input while conducting the experiments.

The performance of Space complexity gradually changes in the above methods with the respect to the number of biometric template data in the server.

Here, the proposed model effectively minimizes the memory space than the existing models.

Conclusion:

MATLAB software is used for implementation of preprocessing, matching, normalization and optimization. The open source 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), 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 (EER) is determined when FAR and FRR are equal. When EER is low, the accuracy of the system is enhanced

REFERENCES

[1]. S. Dargan and M. Kumar, ``A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities,'' Expert Syst. Appl., vol. 143, Apr. 2020, Art. no. 113114, doi: 10.1016/j.eswa.2019.113114.

[2]. R. Vinothkanna and P. K. Sasikumar, ``A novel multimodal biometrics system with Fingerprint and gait recognition traits using contourlet derivative weighted rank fusion,'' in Computational Vision and Bio-Inspired Computing (Advances in Intelligent Systems and Computing), vol. 1108. Hong Kong: IEEE Press, 2020, pp. 950-963.

[3]. X. Zhang, D. Cheng, P. Jia, Y. Dai, and X. Xu, ``An efficient Android-based multimodal biometric authentication system with face and voice,'' IEEE Access, vol. 8, pp. 102757-102772, 2020, doi: 10.1109/ ACCESS.2020.2999115.

[4]. S. Ayeswarya and J. Norman, ``Improved usability for seamless user verication based on biometrics,'' Int. J. Adv. Sci. Technol., vol. 28, no. 7, pp. 379-391, 2019. [Online].

[5]. E. Schiavone, A. Ceccarelli, A. Carvalho, and A. Bondavalli, ``Design, implementation, and assessment of a usable multi-biometric continuous authentication system,'' Int. J.

Crit. Comput.-Based Syst., vol. 9, no. 3, pp. 215-247, 2019, doi: 10.1504/IJCCBS.2019.104490.

[6]. A. Prakash, ``Continuous user authentication based score level fusion with hybrid optimization,'' Cluster Comput., vol. 22, no. S5, pp. 12959-12969, Sep. 2019, doi: 10.1007/s10586-018-1819-6.

[7]. S. Wang, J. Yuan, and S. Chen, ``Quality-based score level fusion for continuous authentication with motion sensor and face,'' in Proc. 4th Int. Conf. Cryptogr., Secur. Privacy, Jan. 2020, pp. 58-62, doi: 10.1145/3377644.3377647.

[8]. S. M, ``A unique secure multimodal biometrics-based user authenticated key exchange protocol for generic HIoT networks,'' Int. J. Emerg. Trends Eng. Res., vol. 8, no. 5, pp. 1610-1619, May 2020, doi: 10. 30534/ijeter/2020/22852020.

[9]. R. M. Jomaa, H. Mathkour, Y. Bazi, and M. S. Islam, ``End-to-end deep learning fusion of fingerprint and electrocardiogram signals for presentation attack detection,'' Sensors, vol. 20, no. 7, p. 2085, Apr. 2020, doi: 10.3390/s20072085.

[10]. M. S. ElTokhy, ``Robust multimodal biometric authentication algorithms using Fingerprint, iris and voice features fusion,'' J. Intell. Fuzzy Syst., vol. 40, no. 1, pp. 647-672, Jan. 2021, doi: 10.3233/JIFS-200425.

[11]. Z. Sitová et al., "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 877-892, May 2016. doi: 10.1109/TIFS.2015.2506542

[12]. N. Kihal, S. Chitroub, A. Polette, I. Brunette and J. Meunier, "Efficient multimodal ocular biometric system for person authentication based on iris texture and corneal shape," in IET Biometrics, vol. 6, no. 6, pp. 379-386, 11 2017.doi: 10.1049/iet-bmt.2016.0067

[13]. K. Zhou and J. Ren, "PassBio: Privacy-Preserving User-Centric Biometric Authentication," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 12, pp. 3050-3063, Dec. 2018. doi: 10.1109/TIFS.2018.2838540.

[14]. S. Vhaduri and C. Poellabauer, "Multi-Modal Biometric-Based Implicit Authentication of Wearable Device Users," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 12, pp. 3116-3125, Dec. 2019. doi: 10.1109/TIFS.2019.2911170.

[15]. B. Karthikeyan, Dr. M. Sengaliappan. (2021). "An Advanced Convolutional Based Fusing by Score Level for Multi-Modality Biometric Authentication". Turkish Online Journal of Qualitative Inquiry (TOJQI), 12(9), 569–583.