Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 4 (2024)

Multimodal Biometric Authentication Based on Advanced Data Mining & Machine Learning Techniques

[1]B. Karthikeyan, [2] D. Suryaprabha, [3] B. Narasimhan, [4] S. Manikandan

[1]Assistant Professor, Department of Information Technology, Nehru Arts and Science College (Autonomous), Thirumalayampalayam Coimbatore - 641105

[2]Assistant Professor (SG), Department of Information Technology, Nehru Arts and Science College (Autonomous), Thirumalayampalayam Coimbatore - 641105

[3]Assistant Professor (SG), Department of Computer Science, Nehru Arts and Science College (Autonomous), Thirumalayampalayam Coimbatore – 641105

[4]Ph. D Research Scholar, Department of Computer Science, Nehru Arts and Science College (Autonomous), Thirumalayampalayam Coimbatore – 641105

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 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 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 preprocessing 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. Here MATLAB is used for implementation. The performance of the algorithm is evaluated by FVC-2004 Dataset for fingerprint and CASIA Dataser for Iris. The database includes multimodal data from 106 individuals. The database is obtained with authenticated agreement from the research website experimental analysis.

Keywords*: Multimodal-Biometrics, FingerPrint, Iris, Artificial Bee Colony, Neural Network*

1. 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 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.

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 where as 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 psychoemotional 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, Palmprint, 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 thermogram, 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 twins.

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.

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.

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 palmprint at score or representation levels. Fusing these on other hand, attributes like hand geometry or finger surface with palmprint 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 enrol 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 enrol 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.

2. Literature Review :

In (2015) J. S. Arteaga-Falconi [1] proposed a versatile biometric authentication calculation dependent on electrocardiogram (ECG) is proposed. With this calculation, the client will just need to contact two ECG terminals (lead I) of the cell phone to get entrance. The calculation was tried with a mobile phone case heart screen in a controlled lab try at various occasions and conditions with ten subjects and furthermore with 73 records acquired from the Physionet database. The acquired outcomes uncover that our calculation has 1.41% false acknowledgment rate and 81.82% genuine acknowledgment rate with 4 s of signal procurement.

In (2016) Z. Sitová et al [2] presented hand movement, orientation, and grasp (HMOG), a lot of conduct features to consistently validate cell phone clients. HMOG features inconspicuously catch unpretentious small scale development and direction elements coming about because of how a client handles, holds, and taps on the cell phone. They assessed authentication and biometric key age (BKG) execution of HMOG features on information gathered from 100 subjects composing on a virtual console. Their outcomes recommend this is

because of the capacity of HMOG features to catch particular body developments brought about by strolling, notwithstanding the hand-development elements from taps.

In (2017) N. Kihal [3] propose an Ocular biometrics alludes to the utilization of features of the eye for individual acknowledgment. For example, the exceptional and stable surface of the iris has been perceived as a ground-breaking visual biometric trademark. In this investigation, the creators propose to improve biometric authentication with a multimodal visual biometric framework dependent on the iris design and the three-dimensional state of the cornea. They show how the cornea can be utilized as a biometric quality for individual acknowledgment and afterward, they propose an intra-visual fusion with iris features to improve the general execution of the framework.

In (2018) K. Zhou [4] propose a user-centric biometric authentication scheme (PassBio) that empowers end-clients to scramble their very own templates with proposed light-weighted encryption conspire. During authentication, every one of the templates remain encoded to such an extent that the server will never observe them legitimately. Be that as it may, the server can decide if the separation of two scrambled templates is inside a pre-characterized limit. Their security examination demonstrates that no basic data of the templates can be uncovered under both latent and dynamic assaults.

In (2019) S. Vhaduri [5] presents an understood wearable gadget client authentication component utilizing blends of three sorts of coarse-grain minute-level biometrics: behavioral (step counts), physiological (heart rate), and hybrid (calorie burn and metabolic equivalent of task). From their investigation of more than 400 Fitbit clients from a 17-month long wellbeing study, they can validate subjects with normal exactness estimations of around .93 (stationary) and .90 (non-inactive) with equivalent blunder paces of .05 utilizing parallel SVM classifiers. Their discoveries likewise demonstrate that the hybrid biometrics perform superior to anything different biometrics and conduct biometrics don't have a noteworthy effect, not with standing during non-inactive periods.

3. Methodolodies:

Biometric Recognition Process:

The biometric recognition framework contains two primary phases, enrolment phase and recognition phase as appeared in Figure 1. In the enrolment phase, the framework obtains the biometric data, breaks down this data and concentrates a particular features set, at that point it manufactures the feature templates (e.g., like the preparation procedure for a classifier). In the recognition phase, the framework, correspondingly, gains biometric data and concentrates features, however as opposed to putting away these features in the feature templates, it compares it with the stored one to confirm the client identity.

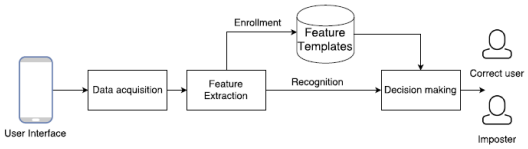

Figure 1: The operation of a biometric recognition system

There is a lot of essential modules should be incorporated into any authentication framework by and large which are as per the following:

A. Data acquisition module: It is the initial phase in the framework where the crude biometric data is gathered by one of the sensors, for example, camera or touchscreen sensor. The nature of the gathered data is significant in light of the fact that it will influence on the successor modules of the recognition procedure. The nature of data is affected by the utilized sensors and the environment in which the data was gathered.

B. Feature extraction module: Before separating the particular features, the crude data must be preprocessed, distinguish and expel anomalies, improve the data quality, particularly if the data gathered in an uncontrolled domain with uncooperative clients. At that point, when the data is cleaned and handled, arrangement of

discriminative features are extracted. The extracted features rely upon the sort of crude data, for instance if the gathered data contains timestamps, fleeting feature could be extracted.

C. Feature templates: It is a stored database that contains a connection of the extracted feature vectors for a particular client (i.e., gadget proprietor). It is worked during the enrollment phase and utilized during the recognition phase to be compared with the caught feature test to confirm the guaranteed identity.

D. Matching and decision-making module: It utilized uniquely during the recognition procedure, by compare it with the extracted features against the stored feature templates to create a coordinating score to settle on a choice. The choice approves the guaranteed identity to see it is real client or fraud.

Problem Statement

Gabor-Hog (Existing Model):

The Gabor-HoG descriptor is made up of multi-scale and multi-directional gradient histograms measured from Gabor-Filters, thus encoding by this gives brief data regarding scale-based LocalRidgeOrientations (LRO). The fingerprint and iris detection system used by Gabor-HoG descriptor and it follows 8 rules. By these 8 rules, Gabor-HoG derives rich knowledge regarding the LRO as compared to its traditional 4 rules. For Gabor-HoG descriptor, feature maps are first created by filtering a Gabor-Filter bank of four scales and creates eight orientations from a fingerprint and iris image. The HoG is then determined using 3*3 cells from the individual feature chart. The HoG descriptors derived from all function maps are normalized to reduce the impact on rows and ridges of differences in grey levels and to eliminate features affected by noise from the sensor. The descriptors are eventually concatenated as shown in Figure 2.

Work Flow

The Gabor-HoG descriptors are obtained from a fingerprint and iris which represent various fingerprint and iris characteristics. The fusion of the descriptors is supposed to increase device reliability and more knowledge regarding the fingerprint and iris is accessible in the fused descriptors. The aim is to combine the descriptors to optimise the similarity between the resultant descriptor and them. CanonicalCorrelationAnalysis (CCA) is a mathematical tool for identifying linear combinations between two groups, with maximal correlation. It uses CCA for fusion in this context.

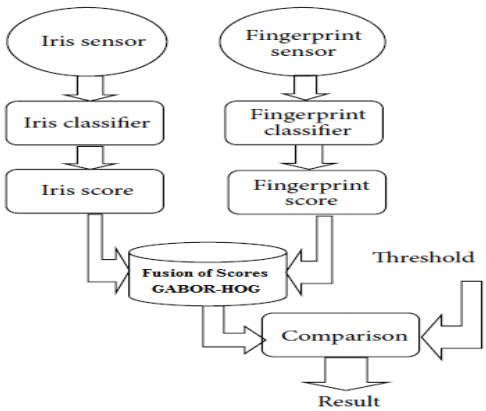

Figure 2: Base Paperarchitecture

First Phase: "Multimodal Biometric Score Level Fusion Using Advanced Optimized Fuzzy Inference System"

For Score-level fusion for MBS, this research provides a unique "Advanced Optimized Fuzzy Interference System (AOFIS)" method in this phase. In particular, its focus is on fusing and its possible use for iris and fingerprint biometric recognition. Independent comparison scores received from fingerprints and iris then that are integrated into Score-level to determine if the individual is authentic or an impostor relying on scores from fusion techniques.

Second Phase: "An Advanced Convolutional Based Fusing By Score Level For Multi-Modal Biometric Authentication"

A novel MBS approach is proposed in this research that uses a hybrid of iris and fingerprint features at the score-level. Specifically, the extraction of features and categorization are the two main components of this system. When classifying individuals, it employed the "Advanced-CNN (ACNN)" framework to combine scores through feature selection and categorize source images as authentic or fake.

Third Phase: "Swarm Intelligence Approaches For Score Level Fusion In Multimodal Biometric Authentication"

In this phase for creating a template we propose a Swarm-Intelligence based algorithm "Artificial Bee Colony (ABC) with Artificial-Neural-Network (ANN) as a hybrid model (ABC-ANN)". The ANN refers to parallel distribution processors created by processing neurons features that possess a natural propensity for storage of experiential expertise and ensuring that it is accessible for usage. The designs of ANNs owe their inspiration to the anatomy of the brain which is a real-world model of error-tolerant parallel processing that is both rapid and powerful. ABC algorithm presumes the presence of a set of operations that resemble certain features of the activity of honey bees. Fitness values to create a strong biometric template refer to food source quality which is strongly linked to food location. The procedure mimics bees' search for precious food sources giving rise to an analogous procedure for discovering optimum solutions.

Work Flow:

Figure 3 gives the various steps of our Multi-modal recognition methodology and the overall research architecture given as follows:

- There is a level in the degree of fusion of the biometric knowledge of iris and fingerprint (here both existing and proposed methods are being used: the existing model here we used was Gabor-HOG fusion and AOFIS based on Fuzzy-Logical reasoning is used as proposed).
- The fusion technique of Gabor-HOG is used by concatenating scores of each trait.
- The other fusion strategy is based on the decision of scores while the fusion process is AOFIS.
- Normalization of scores is essential only for the existing system before its fusion.
- Fusion by fuzzy reasoning doesn't require normalization of scores and the streamlined fuzzy inference method just requires decisions.
- The judgement of the true or the imposter is compared and addressed with appropriate criteria in the upcoming segment.

For each person, biometric trait Gabor-HOG fusion methods have the same weight, yet certain biometric traits are more accurate than others, they have greater durability and tolerance to attacks. In our method, however, the fusion with the fingerprint gives Iris more weight. Weight is not a number for the matching score but a preference of intermediate values for the matching size.

In this research work, two systems were applied to allow a distinction between the identification outcomes (in terms of accuracy and rate of errors) and the correct one for the combination of iris and fingerprint biometric recognition method is finally identified based on the outcomes. Initially, the design is focused on the fusion of scores between existing model Gabor-HOG. Then the proposed AOFIS fusion together with iris and fingerprint decisions are focused on the second design.

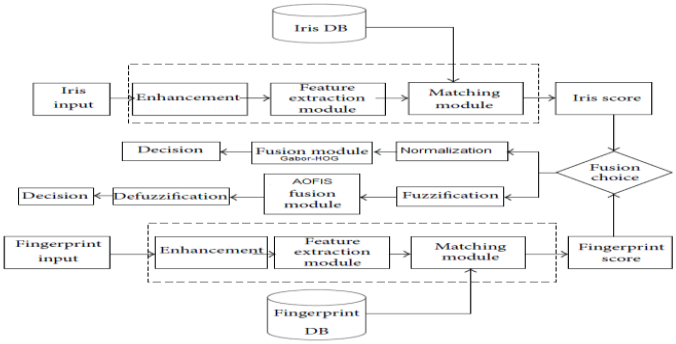

Figure 3:Phase 1 Architecture Training And Testing

The method through which FL is used to produce the mappings from inputs to outputs is called the AOFIS. The inference procedure incorporates all components of membership roles, including "IF-THEN" rules including FL-based operators.

The "FL-Toolbox" within Matlab has not one but two distinct FIS types: the "Sugeno-Model (SM)" and the "Mamdani-Model (MM)". In this case, the MM is implemented to structure recommendations for selected features. Figure 4.8 as well as Figure 4.9 shows how the AOFIS in MATLAB works. When a function is chosen, AOFIS develops rules and determines the fuzzy output results. From inputted Iris and Fingerprint image, it ensures here that "User is Authorized on Unauthorized." There are 2 fuzzy rules in AOFIS's architecture, both of which are grounded in the "first-order" concept of an MM.

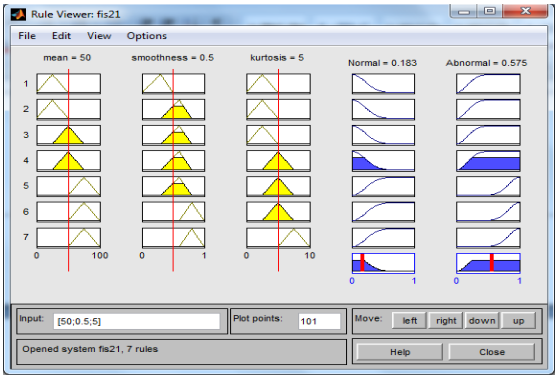

Figure 4: Rule 1 for Selected features using AOFIS

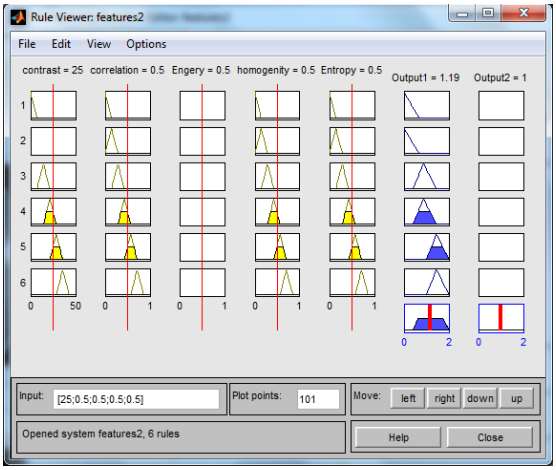

Figure 5: Rule 2 for Selected features using AOFIS

The categorization precision is calculated using the "Receiver Operating Characteristics (ROC)". The "Confusion Matrix" was used to determine how a certain classification performed by comparing the number of "True Positive (TP)", "True Negative (TN)", "False Positive (FP)", and "False Negative (FN)" outcomes.

- Input biometric templates are properly classified as positive if the TP specifies the classifier's test value as positive. This TP is only valid for "Authorized" users.
- The FP calculates the frequency of misleading chances across the entire set of test samples. For some reason, the FP is considered "Authorized" even though it only belongs to "Unauthorized Users".

The critical spots are identified on a graph known as the ROC curve. A classifier's TP and FP ratings may be related to one another. "Sensitivity" refers to TP, whereas "Specificity" refers to "1-FP". The TP score is the percentage of instances when the intended category was properly recognized. The FP score indicates the percentage of imprecise information that was incorrectly identified as precise information. The observed ROC for the proposed AOFIS-based MBS is shown in Figure 5.

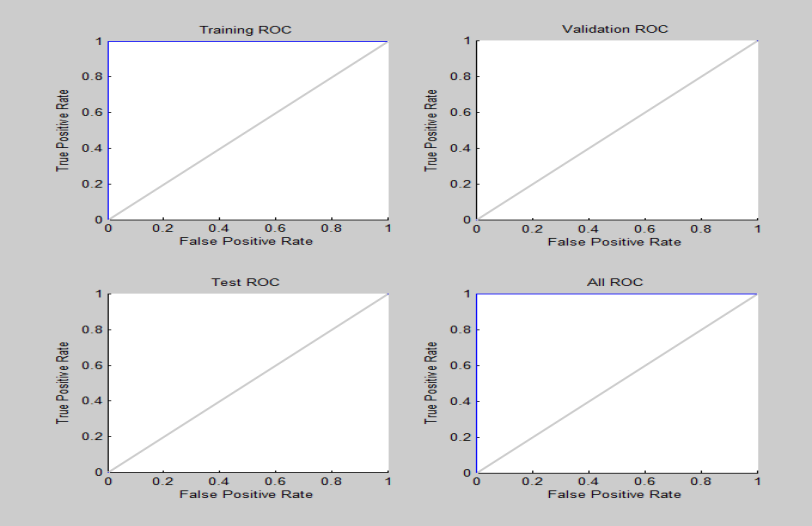

Figure 6: ROC Curves

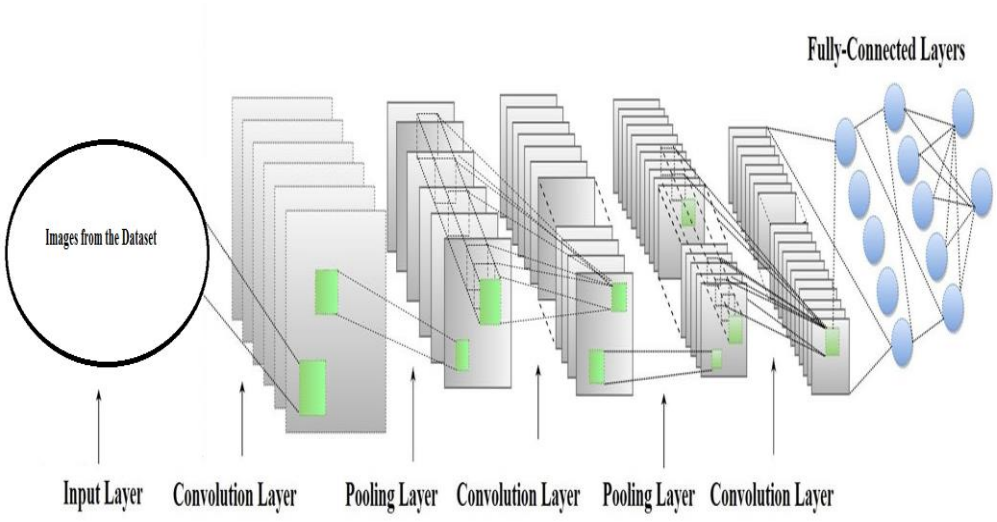

Figure 7: Architecture of the CNN Network

Figure 7 depicts the "First CL", which is composed of "6 AM" layered on top of each other and has been the result of "6 kernels" individually convoluted over the entire source image. Therefore, the building blocks of every AM are identical neural grids. The CL's AM is outlined as per the following Equation (5.1):

$$y^{j(r)} = \max\left(0, b^{j(r)} + \sum_i k^{ij(r)} * x^{i(r)}\right)$$

Eq→5.1

The "i^{th}" input "$x^{i(r)}$" and the "j^{th}" output "$y^{j(r)}$" of AM are given in Equation 5.1. The bias of the "j^{th}" output-map is denoted by "$b^{j(r)}$", and convolution is indicated by "*". The "Convolution Kernel" between the "i^{th}" input-map as well as the "j^{th}" output-map is denoted by "$k^{ij(r)}$".

This would be discussed further on, non-linearity is introduced into the network using the "ReLU Activation Function (y = max (0,x))"

Score-Level Fusing

The results of iris and fingerprint categorization were fused through its classifier applying a score-level fusing approach to generate the symmetrical outcome of the 2nd FCL across all ACNN paradigms. Fusing at the score level is a two-step process. Normalization was performed on the aggregate scores from all ACNN methods, and then scores were fused to produce a single ACNN score. The approach ultimately reveals the identity of the person with the highest aggregate score.

The scores have been fused by applying the "Arithmetic Mean Rule (AMR)" as well as the "Product Rule (PR)". The AMR calculates an overall rating by adding the scores allotted for each trait and afterward dividing that total by its cumulative number of traits.

The AMR is calculated using the following Equation (5.10):

$$S = \sum_{t=1}^{j} S_t / j$$

Eq→5.10

Here, "S_t" is the sum of all possible scores on a trait "t", and "j" is the number of traits. In the PR, the fusing score is obtained by multiplying the values of the two components. The following Equation (5.11) was used to determine it:

$$S = \prod_{t=1}^{j} S_t$$

Eq→5.11

In this case, "S_t" stands for the trait "t" score-vector, and "j" is the sum of all traits.

4. Results And Discussions

To validate and perform an appraisal and evaluation of this proposed phases 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.

(iii) First, the procedures are carried out separately in a unimodal fingerprint framework. Different feature extraction methods are used in each phases 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.

(ii) Secondly, the procedures are carried out separately in a unimodal iris recognition system. The extractor of features for Iris is based on the different methods on each phases. This produces an Iris code composed of bitstreams called Iris code. The corresponding score is given by the distance of hamming.

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

(iv) Finally, the authentication process is applied by utilizing the different classifiers in each phases 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 database with 60% are utilized for the classifier testing and validation.

(i) Genuine Recognition Attempts: Here finger impression 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 template 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 of remaining by a unique person, also symmetric matches are prevented.

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

Biometric systems' authenticity is assessed by analyzing error rates of various kinds. Diagrams showing the distributions of real and fake scores about error rates that have been used. The perfect biometric authentication would provide a score distribution in which real and fake profiles never overlapped. Thus, the absence of FAR and FRR may be achieved by setting the threshold such that it lies between the two distributions, allowing for simple separation of real and impostor scores.

Due to biometric systems' fallibility, there is a degree of overlap between the genuine and impostor scores. Therefore, when a score is located within the overlap zone, it is difficult to determine whether or not it is legitimate. A smaller overlap zone means a more accurate solution, whereas a larger overlap region indicates less accuracy.

The threshold has been the deciding factor in determining whether a user is legitimate or not. If the imposter's score is higher than the threshold, it's considered FAR, whereas if the true score is lower, it's considered FRR.

Table :1 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

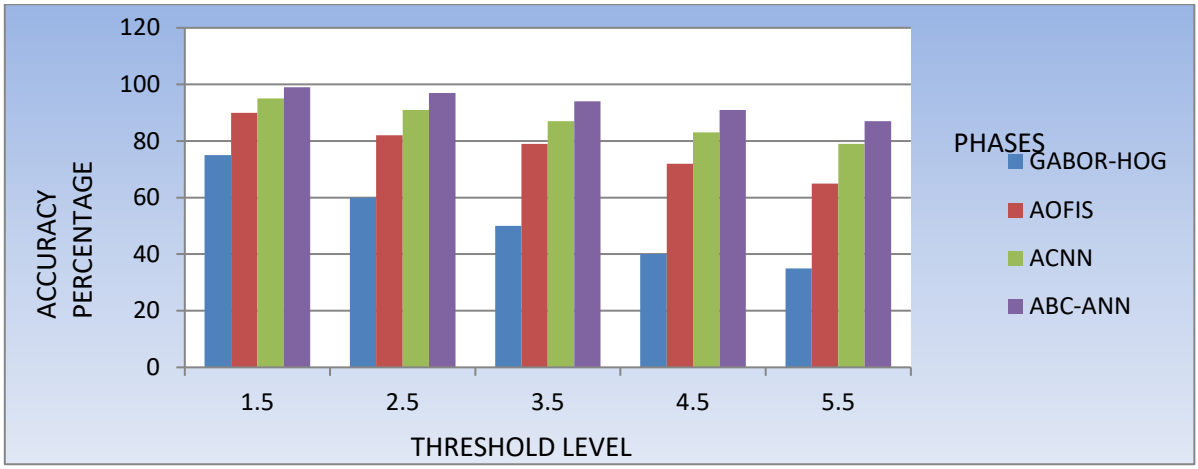

Figure 8 Accuracy Comparison Graph

5. Conclusion:

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.

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

References

[1] Farmanbar, M., & Toygar, Ö. (2017). Spoof detection on face and palmprint biometrics.

a. *Signal, Image and Video Processing, 11*(7), 1253-1260. doi:10.1007/s11760-017-1082-y

[2] Dantcheva, A., Elia, P., & Ross, A. (2016). What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics. *IEEE Transactions on Information Forensics and Security, 11*(3), 441-467. doi:10.1109/tifs.2015.2480381

[3] Chowdhary, C. L. (2019). Analysis of Unimodal and Multimodal Biometric System.

a. *Intelligent Systems*, 125-150. doi:10.1201/9780429265020-7

[4] Hammad, M., Liu, Y., & Wang, K. (2019). Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint.

a. *IEEE Access, 7*, 26527-26542. doi:10.1109/access.2018.2886573

[5] Valdes-Ramirez, D., Medina-Perez, M. A., Monroy, R., Loyola-Gonzalez, O., Rodriguez, J., Morales, A., & Herrera, F. (2019). A Review of Fingerprint Feature Representations and Their Applications for Latent Fingerprint Identification: Trends and Evaluation. *IEEE Access, 7*, 48484-48499. doi:10.1109/access.2019.2909497

[6] Hammad, M., & Wang, K. (2019). Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network. *Computers & Security, 81*, 107-122. doi:10.1016/j.cose.2018.11.003

[7] Karthikeyan, B., & Sengaliapan, M. (2019). A brief survey in biometric authentication and its applications. *Journal of Information and Computational Science, 9*(11), 10-30.

doi:10.12733.JICS.2019.V9I11.535569.1122

[8] Yang, W., Wang, Z., & Zhang, B. (2016). Face recognition using adaptive local ternary patterns method. *Neurocomputing, 213*, 183-190. doi:10.1016/j.neucom.2015.11.13

[9] Nayana, P., Mathew, D., & Thomas, A. (2017). Comparison of Text Independent Speaker Identification Systems using GMM and i-Vector Methods. *Procedia Computer Science, 115*, 47-54. doi:10.1016/j.procs.2017.09.075

[10] Zhang, H., Patel, V. M., & Chellappa, R. (2017). Low-Rank and Joint Sparse Representations for Multi-Modal Recognition. *IEEE Transactions on Image Processing, 26*(10), 4741-4752. doi:10.1109/tip.2017.272183

[11] Duan, Y., Lu, J., Feng, J., & Zhou, J. (2018). Context-Aware Local Binary Feature Learning for Face Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 40*(5), 1139-1153. doi:10.1109/tpami.2017.2710183

[12] Zhang, X., Cheng, D., Dai, Y., & Xu, X. (2018). Multimodal Biometric AuthenticationSystem for Smartphone Based on Face and Voice Using Matching Level Fusion. *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*. doi:10.1109/compcomm.2018.8780935

[13] Alsaadi IM (2015) Physiological biometric authentication systems, advantages disadvantages and future development: A review. Int J Sci Technol Res 12: 285-289.

[14] Kaur G, Singh G, Kumar V (2014) A review on biometric recognition. International Journal of Bio-Science and Bio-Technology 4: 69-76.

[15] J. S. Arteaga-Falconi, H. Al Osman and A. El Saddik, "ECG Authentication for Mobile Devices," in IEEE Transactions on Instrumentation and Measurement, vol. 65, no. 3, pp. 591- 600, March 2016. doi: 10.1109/TIM.2015.250386