International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S3, September 2019

Multi-Modal Authentication using Machine Learning Algorithm

Anil Kumar Gona, M. Subramoniam

***Abstract:**In the present era of information technology, there is a need to implement verification and approval strategies for security of resources. Whereas, there are number of approaches to demonstrate validation and approval, yet the biometric verification beat every other method. At first, biometrics began off with straightforward unimodal framework, the higher requirement for security had offered ascend to a prevalent framework known as multimodal verification framework. Multimodal verification confirmation has pulled in compelling interest, on account of its hugeness towards the constant application In this research proposal, an effective framework for multimodal verification authentication systems based on machine learning algorithm is employed.*

The utilized structure tends to the characteristic issues of client burden and framework wastefulness in multimodal confirmation verification frameworks.

I. INTRODUCTION

Biometric security is an emerging method has received the attention in recent years by verifying a person's identity with the help of access control methods. As the level of security violation and transaction fraud increases the need for highly secure identification and personal verification is verification visible. Verification authentication is a process of measuring the unique characteristics of a person such as voice pattern, the iris or retina pattern of the eye, finger print pattern [1]. Their applications can be categorized into five main groups such as forensic, government, commercial, health-care, travelling, and immigration. Unimodal biometrics is the system that uses only one biological sample to check and they are limited against accuracy and hacking. To overcome this limitation, the multimodal verification system is developed which combine samples from multiple sources of information in order to improve reliability and recognition control security.If the user cannot possess a single valid biometric trait, still they can be enrolled into a system by using another valid biometric trait.The key to multimodal biometrics is the combination of various steps of identifying an imageat the feature extraction, matching score, or decision levels and application of fusion methods Feature extraction is the process of selecting a subset of relevant features from a set of features.Biometric fusion can be defined broadly as the use of multiple types of biometric data or methods of processing to improve the performance of biometric systems. The selection of best fusion rule and estimating the parameters has become one of the most active research area in multimodal biometric security.The fusion methods are of sample level, template level, score level and decision level of fusion. In which the score and decision level fusion contains the best solution as they are easily implemented.In decision level, the multiple accept and reject decisions are consolidated from multiple sensors to form one decision information. Bayesian framework can be used as the basis of a fusion decision system that automatically adapts the security level. However, the score-level approach generates applicably stable performance and requires a less iterations to generate better performance as compared to the decision-level approach. The features of individual biometricsamples are extracted from their preprocessed imagesand they are compared with the stored template to obtain the matching scores.It adopts optimization methodology perform decision analysis. The methods like Particle Swarm Optimization (PSO), Artificial Bee Colony (ABC), Ant Colony Optimization (ACO) provides better results [9].PSO possess an adaptive combination on finding an optimal fusion rule and estimates the parameters.Although selection of feature and elimination of noise is still seems to be a challenging task.The practice of adopting algorithms on optimization sometimes produce complexity and loss of accuracy. To satisfy these criteria, a Machine Learning System is proposed in this paper to provide an effective optimization process [10]. It is a type of Artificial intelligence method, which makes the computer with the ability to learn without being programmed explicitly. To make the biometric authentication fully automated and to reduce the error and rejection rate of the system, the Machine learning system is introduced.

II. LITERATURE VIEW

K. O. Bailey et al. a conduct bio metric framework that combined on client information from console, mouse, and Graphical User Interface (GUI) connections. Consolidating the modalities results in a progressively exact validation choice dependent on a more extensive perspective on the client's PC movement while requiring less client communication to prepare the framework than past work..

Manuscript published on 30 September 2019.

***** Correspondence Author (s)
Anil Kumar Gona, PhD Scholar, Dept of Electronics and communication Engineering, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai, Tamilnadu, India. (Email: anilkumarece@cvsr.ac.in)
Dr. M. Subramoniam, Asst Professor, Dept of Electronics and communication Engineering, Sathyabama Institute of Science and Technology (Deemed to be University), Chennai, Tamilnadu, India.(Email: subramoniam.enc@sathyabama.ac.in).

Testing over 31 that combination procedures altogether improved social biometric validation precision over single modalities all alone. Between the two combination strategies displayed, include combination and a group based order strategy, the gathering technique played out the best with a False Acceptance Rate (FAR) of 2.10% and a False Rejection Rate (FRR) 2.24%

H. Saevaneeet al. proposed a novel content based multimodal biometric approach using phonetic investigation, keystroke elements and social profiling. Test examinations demonstrated that clients can be separated by means of their content based passage, with a normal Equal Error Rate (EER) of 3.3%. In light of these discoveries, a system that had the option to give strong, ceaseless and straightforward confirmation was proposed.

M. I. Ahmad a novel combination system called non-stationary element combination where another structure of interleaved lattice was developed utilizing nearby highlights extricated from two modalities for example face and palm print pictures. A square based Discrete Cosine Transform (DCT) calculation was utilized to develop an intertwined highlight vector by extricating free component vectors from each spatial picture. This melded highlight vector contains nonlinear data that was utilized to prepare a Gaussian Mixture Models (GMM) based factual model. The model gives precise estimation of the class restrictive likelihood thickness capacity of the intertwined highlight vector. The proposed technique delivered acknowledgment rates as high as 99.7% and 97% when tried on benchmark databases-ORL-PolyU and FERET-PolyU individually. These rates were accomplished utilizing 23% low recurrence DCT coefficients. The new strategy was appeared to beat existing element level combination techniques including strategies dependent on coordinating and choice level combination. Q. Zhang et al. proposed a novel structure for sequential multimodal biometric frameworks dependent on semi-directed learning systems. The proposed structure tended to the characteristic issues of client bother and framework wastefulness in parallel multimodal biometric frameworks. Further, it propelled the sequential multimodal biometric frameworks by advancing the separating intensity of the more fragile yet more client advantageous trait(s) and sparing the utilization of the more grounded yet less client helpful trait(s) at whatever point conceivable. They proposed to utilize semi-directed learning methods to reinforce the matcher(s) on the more fragile trait(s), using the coupling connection between the more fragile and the more grounded attributes. A dimensionality decrease technique for the more fragile trait(s) in view of reliance augmentation was proposed to accomplish this reason.

III. PROBLEM IDENTIFICATION

Multimodal biometrics possess high level of security and robustness compared to the unimodal but it produce lot of restriction, as it need to collect the similar characteristic from the database.The general possible problems and limitation in biometric authentication is given below

1. Selection of fusion algorithm- Finding the suitable and best fusion algorithm is the main problem in multimodal biometrics. There are many of fusion algorithms to select but it should be noted that the algorithm should increase the verification rate during the development of the optimization system.

2. Invariance- Most of the metrics used in biometric authentication shows invariance. In face recognition, the geometry of the face changes due to aging or change in expression. In hand and finger recognition, variation may occur due to if any injuries occurred in it. Deviation of voice tone may also possibly happen in voice recognition.

3. Speed- The speed of a multi modal verification popularity machine is also an vital issue for actual time programs in particular while deployed in public locations consisting of airports and stadiums. Therefore, developing an correct as well as time-green set of rules is of outstanding studies interest.

4. Scalability- Testing with considerably large databases and getting suited results is some other huge mission to be addressed. Most of the proposed verification structures are examined with databases containing less statistics topics. The get entry to of facts from unique bench marked database is taken into consideration as a hassle.

5. Automation- Most of the procedures are manual or semi-computerized requiring a few manual intervention. However, for actual-time programs, popularity ought to be executed in a fully automated form.

6. Vulnerability- Spoofing is the biggest threat to authentication systems. Multi modal in addition to uni modal verification systems are once in a while liable to spoofing. The potential threats because of fake or artificial hands has to be eliminated through adopting a best set of rules, which can distinguish unique and pretend snap shots.

7. Reliable recognition- Recognition of image and their characteristics is a big challenge in biometric authentication.The patterns of movements (gaits) of two individuals of the same family or coincidentally of two different persons can be similar.Therefore, the reliability in recognizing the image is sometimes lost.

8. Accuracy- The accuracy of a multimodal biometrics system is normally calculated in terms of image acquisition errors and matching errors.The problem in acquiring a perfect image and matching them with the data attributes is still visible in multimodal type of authentication

IV. MOTIVATION

In recent times, our country is facing many threatening problems created by the terrorists attack. It is necessary to control and protect all the important public properties. One way to make this possible is establishing anautomated security system. The traditional security systems were designed based on passwords; Non-public identification numbers (PINs) or smart cards, which may face problems such as forgetting the password or loss of cards etc.To overcome this problem and to make the security system stronger biometric authentication method is used.There have been a number of cyber-attacks and security breaches on companies and large organizations all around the world, so biometric is a resolution taken to make all the documents and properties of recognized organization safe.

It is hard to overstate the big impact of cell phones verification that the telephone has had on all elements of life. That has given a high delight within the customer's overview. Verification for Time and Attendance technology brings efficiency to the administrative center by way of maintaining higher tabs on the employees in a given personnel. Thus, these things motivate us to do research on biometrics to improve its efficiency to resist against theft and hacking.

V. RESEARCH GAP

In biometric authentication, many approaches has been implemented and used so far. Most of the researchers has left some details to be mentioned in their implementation work. The main problem is that, the use of large number of samples from the database. The current verification structures are tested with databases containing facts from much less than 500 topics. This is may be satisfied with the aid of attempting the big statistics technique. The most efficient modality selection for fusion is emerging as an important studies problem. From the to be had set, which modalities should be fused to accomplish a assignment at a particular time instant must be stated. PSO and Adaptive Inertia PSO, ABC and ACO are the common techniques used for performing the optimization procedure. Machine learning algorithm can be combined with the PSO, which minimizes the chance of false matches.The optimization procedure adopt to investigate all the possible matches. However, if the condition occurs that no input sample is matched, the earlier proposed systems might fail. That failure is avoided by using the machine learning system, which will provide new identity to the unknown input sample

VI. PROPOSED SYSTEM

The general architecture of the proposed method is given by the image acquisition, selection of feature and fusion methodologies.

Image Acquisition- The images to compare can be taken from any of the universal database system. The database system contains the biological metrics like face, iris, finger, and ear sample images. The common databases used for acquisition of image are as follows

Face databases- (FERET) PolyU, Olivetti Research lab

Eye databases- CASIA Iris image, DRIVE retinal images

Finger print- FPR 620, FVC 2000 and FVC 2004

Ear database- USTB Ear imagesare the databases used for acquiring the images.

Preprocessing- The Region of Interest (ROI) method is used for selecting a particular best region from the input image acquired from the database.The ROI method takes place before the preprocessing procedure. The regional image selected may containvarious noises and inaccuracies. In order to remove those noises, it has to be passed into the following stages like image enhancement, edge detection and filtering methods.

Feature extraction- The process of getting a meaningful feature or detail from the ROI subset of measured data is called feature extraction. The selected features are expected to contain the relevant information from the selected subset. Principal component analysis (PCA), Gabor method, Discrete cosine transform (DCT), Class specific discriminant analysis (CSRDA), Fisher face methods are the common methods used for extracting and selection of feature. Hybrid feature selection provides a new extracting algorithm of best feature selection and it is applied in our system.

Modal selection- The mode of operation to be performed for processing of the image is selected in this phase. In this paper, the sample image is allowed to pass through an optimization algorithm. The purpose of optimization algorithm is to compensate the missing or corrupted image details with good possibilities. Genetic algorithm (GA), Particle swarm optimization (PSO) are the algorithms used to perform modal selection in which PSO is preferred as it optimizes a problem by iterative determination. Improved PSO method of optimization is used in this research.

Fusion methodologies- Fusion of information in multimodal is formed by different levels of existence, which is used for the merging of characteristics to be verified. The multimodal fusion levels are as follows

(a) Feature level multimodal fusion

(b) Decision level multimodal

(c) Hybrid multimodal fusion

Here,multilevel fusion method adopts various level in a single determination, which possess more accuracy in deriving the features extracted.

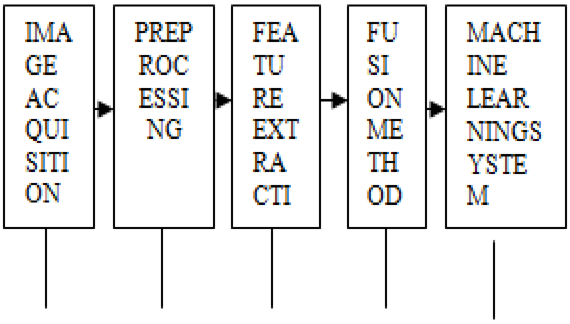
Machine Learning System

Machine learning explores the study and construction of algorithms that can learnfrom and make predictions on data. Decision Tree Learning (DTL), Association Rule Learning(ARL), Artificial Neural Network (ANN), Support Vector Machine (SVM), Bayesian Network,Regression, Genetic Algorithms (GA) are some of the common algorithms used in machine learning system. The Machine learning System consist of three phases. They are training, validation and testing.

Training-It is a set of data used to discover potentially predictive relationships. A test set is a set of data used to assess the strength and utility of a predictive relationship. The training process consist of a training dataset for which weknow both the input data as well as additional attributes that we want to predict.

Validation-This process actually can be regarded as a part of training set. Validation process is used for the selection of parameter and to avoid outfitting of the image. Thus, it is also called as parameter tuning method.

Testing- It is the process of comparing a device or its additives with the purpose to find whether it satisfies the specified necessities or not to induce the automation of biometrics machine learning system is introduced. The machine learning algorithm takes place when all the possible samples from the database does not matched with the training set sample. It will collect the input sample automatically as a new identification trait for an individual.



Block diagram- Multimodal biometric authentication

VII. POSSIBLE OUTCOME

The biometric security level is implemented with the help of best apparatus or experimental set- up design, which makes the algorithm to be executed in it.

Experimental set- up- The processing of the image and identification procedure is carried out usingMATLAB software packages.

The predictable outcome of the algorithms proposed is discussed as follows

Biometric- every verification characteristic has its personal strengths and weaknesses and therefore the selection sometimes depends upon on the applying. A verification machine is to be wise and reliable, should meet the specified needs or traits like Universality(availability)

Distinctiveness-It declares that any two persons should sufficiently have different characteristic. It is estimated by the False Match Rate (FMR), otherwise called "Type (II)

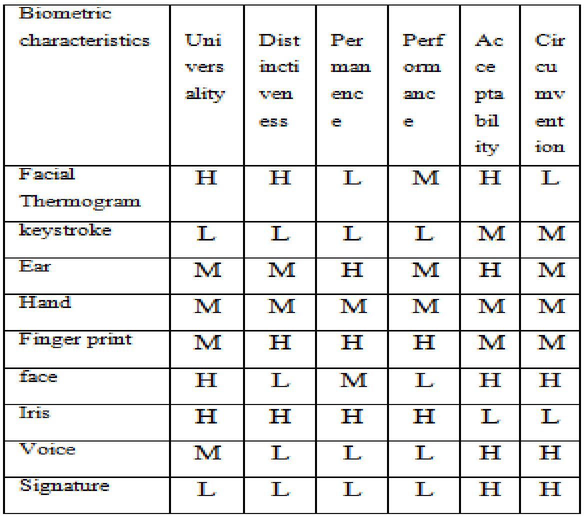
Blunder". Lastingness (strength) - the trademark ought to be steady over some stretch of time, which means the steadiness over age. Heartiness is estimated by the False Non-Match Rate (FNMR), otherwise called "Type (I) blunder".

Performance- It means to achieve verification accuracy, speed, and the resources required to the application.

Acceptability- The specific person population and the general public, in fashionable, have to haven't any objections to the measuring or collection of the verification characteristic. Acceptability is measured by way of polling the tool users.

Resistance to Circumvention- Tests and proofs how the machine resists fraudulent models easily.

Table 1. Comparison of biometric characteristics



Biometric characteristics	Universality	Distinctiveness	Permanence	Performance	Acceptability	Circumvention
Facial Thermogram	H	H	L	M	H	L
keystroke	L	L	L	L	M	M
Ear	M	M	H	M	H	M
Hand	M	M	M	M	M	M
Finger print	M	H	H	H	M	M
face	H	L	M	L	H	H
Iris	H	H	H	H	L	L
Voice	M	L	L	L	H	H
Signature	L	L	L	L	H	H

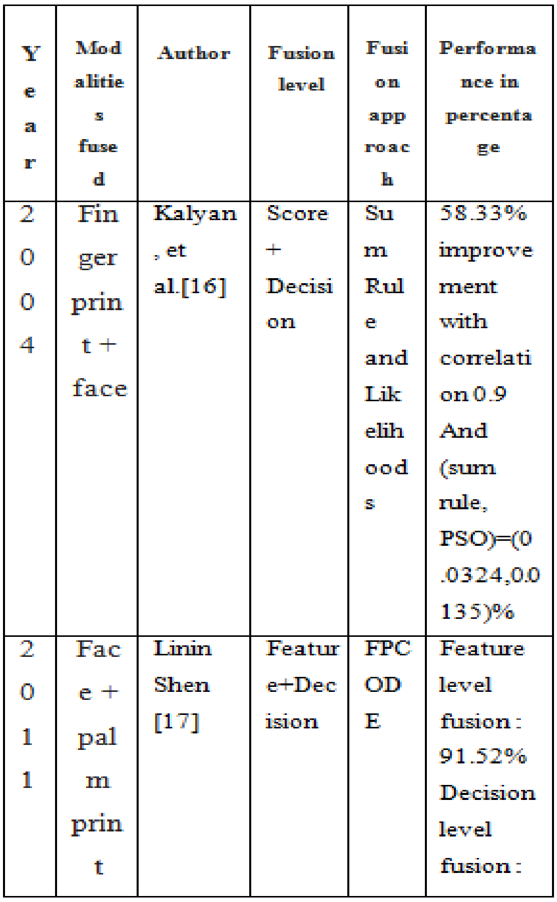
H-High, L-Low, M- Medium

From the above table1.Thesecurity level of the biometrics with respect to particular characteristics are mentioned. Based on the ranks obtained from the comparison, the proposed method is designed.

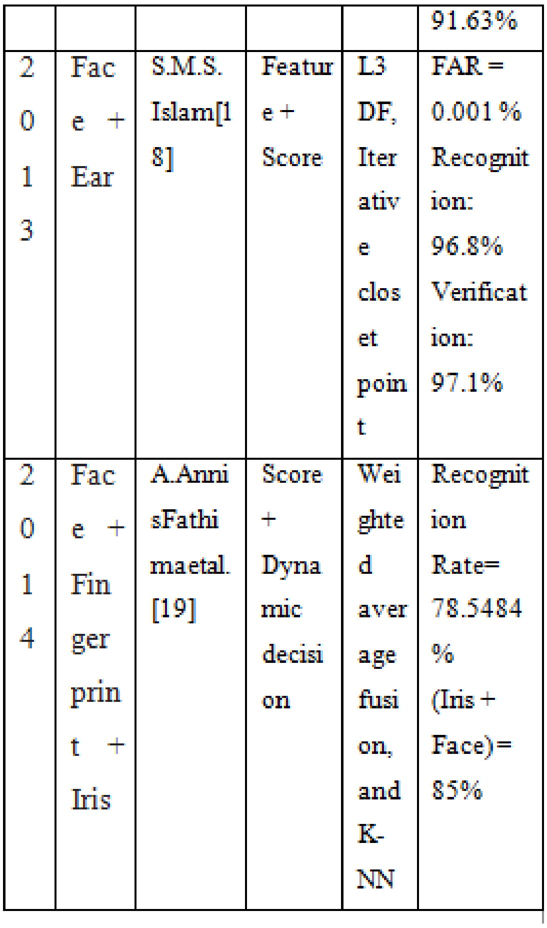
- Quality performance and metrics-
- False Accept Rate (FAR): Mistaking the biometric measurements from two different persons to appear as if they are from the same person due to large inter-user similarity.
- False Reject Rate (FRR): Mistaking 2 Verification measurements from constant person to seem that they're from 2 totally different persons because of giant intra-class variations.

1. Equal Error Rate (EER): For a simple empirical measure, it is used to differentiate the overall performance of a verification system this is defined at the factor wherein FRR and FAR are identical.

Table 2.Examples of previous research based different fusion in different levels



Year	Modalities fused	Author	Fusion level	Fusion approach	Performance in percentage
2004	Finger print + face	Kalyan, et al.[16]	Score + Decision	Sum Rule and Likelihoods	58.33% improvement with correlation 0.9 And (sum rule, PSO)=(0 .0324,0.0 135)%
2011	Face + palm print	Linin Shen [17]	Feature+Decision	FPCODE	Feature level fusion : 91.52% Decision level fusion :



					91.63%
2013	Face + Ear	S.M.S. Islam[18]	Feature + Score	L3DF, Iterative closet point	FAR = 0.001 % Recognition: 96.8% Verification: 97.1%
2014	Face + Fingerprint + Iris	A.AnnisFathimaetal.[19]	Score + Dynamic decision	Weighted average fusion, and K-NN	Recognition Rate= 78.5484 % (Iris + Face)= 85%

The above table2. Shows that how the modalities combination performs with particular fusion approach. In this research, we improved the efficiency of the performance and decreased theFRR possibilities by selecting a perfect fusion methodology and modalitiesbased on the optimization and machine learning system. Thus, the error rate can also be reduced to provide better outcome of the security level.

REFERENCES

1. EL-SAYED et al, "Multi-Biometric Systems: A State of the Art Survey and Research Directions,"(IJACSA) International Journal of Advanced Computer Science and ApplicationsVol. 6, No. 6, 2015
2. Shantha Kumar H.C, Janardhan Naidu, “An Efficient Personnel Authentication through
3. Multi modal Biometric System”, International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-1, January 2016.
4. Ashish Mishra, “Multimodal Biometrics it is: Need for Future Systems”, International Journal of Computer Applications (0975 – 8887)Volume 3 – No.4, June 2010
5. Atrey, Pradeep K., et al. "Multimodal fusion for multimedia analysis: a survey." Multimedia systems 16.6Springer-Verlag (2010): 345-379
6. Snelick, Robert, et al. "Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems." Pattern Analysis and Machine Intelligence, IEEE Transactions on 27.3 (2005): 450-455.
7. Meva, Divyakant T., and C. K. Kumbharana. "Comparative Study of Different fusion techniques in multimodal biometric authentication." International Journal of Computer Applications 66.19 (2013).
8. Poli, Riccardo. "Analysis of the publications on the applications of particle swarm optimisation." Journal of Artificial Evolution and Applications 2008 (2008): 3.
9. Singh, Sushil, and Sunil Pranit Lal. "Educational courseware evaluation using Machine Learning techniques." e-Learning, e-Management and e-Services (IC3e), 2013 IEEE Conference on. IEEE, 2013.
10. Bailey, K.O., Okolica, J.S. and Peterson, G.L., 2014. User identification and authentication using multi-modal behavioral biometrics. Computers & Security, 43, pp.77-89.
11. Saevanee, H., Clarke, N., Furnell, S. and Biscione, V., 2015. Continuous user authentication using multi-modal biometrics. Computers & Security, 53, pp.234-246.
12. Ahmad, Muhammad Imran, Wai Lok Woo, and SatnamDlay. "Non-stationary feature fusion of face and palm print multimodal biometrics." Neurocomputing (2015).
13. Zhang, Q., Yin, Y., Zhan, D.C. and Peng, J., 2014. A novel serial multimodal biometrics framework based on semisupervised learning techniques. Information Forensics and Security, IEEE Transactions on, 9(10), pp.1681-1694.
14. Palaniappan, R., Andrews, S., Sillitoe, I.P., Shira, T. and Paramesran, R., 2016. Improving the Feature Stability and Classification Performance of Bimodal Brain and Heart Biometrics. In Advances in Signal Processing and Intelligent Recognition Systems (pp. 175-186). Springer International Publishing.

AUTHOR PROFILE

Mr. ANIL KUMAR GONA is pursuing his PhD from Sathyabama University, Chennai, in the field “Integration of embedded system & Image processing using Machine Learning”. He received his Master’s degree in Computers and communication engineering from RRS College of engineering and technology, Hyderabad in 2011. He received his Bachelor’s degree in Electronics and Communication Engineering from S.R.T.I.S.T, Nalgonda in 2008. Currently He is working as an Asst.Professor in Anurag Group of Institutions (Formerly CVSR Engineering College) Hyderabad. He has 7 years of teaching experience. He has published 2 National and 4 International Journals. His research interests include embedded systems, Image processing, Machine Learning and Communication systems.