AN ENHANCED MULTI-MODAL BIOMETRIC AUTHENTICATION

DR. ANTO.A. MICHEAL
Professor
Department of CSE
antomicheal@tkrec.ac.in
Teegala Krishna Reddy Engineering College, Hyderabad

GAURAGALA PRASHANTHI
Department of CSE
prashanthig2k@gmail.com
Teegala Krishna Reddy Engineering College, Hyderabad

KESAVA ROHITH GIRIVARDHAN REDDY
Department of CSE
rohitgvreddy@gmail.com
Teegala Krishna Reddy Engineering College, Hyderabad

GAVVA PRASHANTH
Department of CSE
prashanthsdnr@gmail.com
Teegala Krishna Reddy Engineering College, Hyderabad

Abstract:

A multi-modal biometrics (MMB) system incorporates information as of more than one biometric modality for enhancing each biometric system's performance. The recognition system encompasses robustness, accuracy, along with recognition rate issues. The model deals with biometric authentication and its implementation in a 3-tier multimodal architecture which works on the basic principle of identification and authentication. As the applications of computers are increasing in every sector, the requirement of a dependable authentication plan to affirm the character of an individual is immense. The proposed MMB system is on FLSL fusion method and Modified Deep Learning Neural Network (MDLNN) to enhance the performance. The face, ear, retina, fingerprint, and front hand image traits are considered. This comprises image enhancement, segmentation, feature extraction, feature reduction, rule generation, and identification phases. The Viola-Jones Algorithm (VJA) segments the facial parts, and the Penalty and Pearson Correlation-based Watershed Segmentation (PPWS) algorithm eliminates the unwanted information in the ear, finger traits and also the blood vessel of the retina image. The features are extracted as of images, and are inputted to the MDLNN to classify the person as genuine or imposter.

I. INTRODUCTION

A biometric system that utilizes the information of biometrics as of one person aimed at authentication along with verification is a biometric system. Biometrics could be found anywhere from unlocking of mobiles to airport border control. MMB systems can manage the issues of non-universality and can limit imposters from spoofing biometric attributes of authentic people, for improving the recognition's accuracy. The main method involved in MMB is a fusion of different traits.

The proposed model deals with biometric authentication and its implementation in a 3- tier multimodal architecture which works on the basic principle of identification and authentication. As the applications of computers are increasing in every sector, the requirement of a dependable authentication plan to affirm the character of an individual is immense. Cases of such applications need to have a secure access to PC frameworks, workstations, PDAs, ATMs and even buildings to say a few. Without appropriate and strong authentication checking, these frameworks are vulnerable to the guiles of an attacker.

Generally, passwords and ID cards (token-based security) are a common and most used methods of confirming access to different applications. However, these systems are not completely secure as it can be breached when a secret key is revealed to an unapproved client or identification is pilfered by a fraudster. Biometric frameworks make utilization of fingerprints, geometry of hands, iris, retina, facial features, hand vein structure, mark, facial thermograms or even voiceprint to confirm a person's identity. These are

superior in the sense that these features can't be easily shared, stolen or breached like a conventional security strategy.

Biometrics frameworks have been categorized into two classes which are: unimodal and multimodal biometrics framework. The basic contrast between the two is that a Unimodal framework works with just a single characteristic or feature while a multimodal framework will employ multiple physical features, for example, a combination of a unique mark in the face, retina and voice. The focus of this research is particularly on multimodal biometrics arrangement of verification since it assures critical guarantee as far as security. Multi-biometrics aims to bring down one or more of the following: False Accept Rate (FAR), False Reject Rate (FRR) and Failure to Enroll Rate (FTE).

II Literature survey:

An improved face recognition method using Local Binary Pattern method:

Security system based on biometrics is becoming more popular everyday as a part of safety and security measurement against all kind of crimes. Among several kinds of biometric security systems, face recognition is one of the most popular one. It is one of the most accurate, mostly used recognition methods in modern world. In this paper, two most popular face recognition methods have been discussed and compared using average image on Yale database. To reduce calculation complexity, all training and test images are converted into gray scale images. The whole face recognition process can be divided into two parts face detection and face identification. For face detection part, Viola Jones face detection method has been used out of several face detection methods. After face detection, face is cropped from the actual image to remove the background and the resolution is set as 150×150 pixels. Eigenfaces and fisherfaces methods have been used for face identification part. Average images of subjects have been used as training set to improve the accuracy of identification. Both methods are investigated using MATLAB to find the better performance under average image condition. Accuracy and time consumption has been calculated using MATLAB code on Yale image database. In future, it will be helpful for further research on comparison of different face recognition methods using average images on different database.

Multimodal Biometrics for user authentication:

The main aim is to provide multilevel authentication in biometric systems. Multimodal biometric is the usage of multiple biometric indicators by personal identification systems for identifying the individuals. Multimodal authentication provides more level of authentication than unimodal biometrics which uses only one biometric data such as fingerprint or face or palm print or iris. In this, the fingerprint and iris of a person are used for the automatic identification of an individual by combining finger print and iris of a person at the matching-score level. A technique called Minutiae matching and Edge detection is used for this purpose. The performance of the proposed technique has been evaluated and accuracy has been increased by minimizing the FAR (False Acceptance Rate) and FRR (False Rejection Rate).

An introduction to biometric recognition:

A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones, and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition, or, simply, biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. By using biometrics, it is possible to confirm or establish an individual's identity based on "who the person is", rather than by "what the person possesses" (e.g., an ID card) or "what the person remembers" (e.g., a password). The brief overview of the field of biometrics and summarize some of its advantages, disadvantages, strengths, limitations, and related privacy concerns.

Online Learning Classifier based Behavioral Biometric Authentication:

In this project, the implementation of a behavioral biometric-based smartphone authentication technique with online training methods is done. The most obvious difference between online and traditional classification is that online methods allow model training and data collection to be in progress simultaneously. Therefore, the proposed authentication system is superior when dealing with time series data and its model can be updated to adapt the change of user's habit. To verify the feasibility of online

training methods used in behavioral biometric authentication, three online algorithms and four traditional classification algorithms are tested with collected dataset. They all achieved an accuracy over 96%. Two additional experiments are designed to test the stability of this authentication system. The results show that the system has the ability to prevent targeted attack, such as shoulder surfing. Furthermore, it keeps high performance that accuracy greater than 95% when user holds smartphone in different scenarios, sitting and walking. Finally, we conclude that online training methods based behavioral biometric smartphone authentication system is very stable with targeted attack and different unlock scenarios.

III. EXISTING SYSTEM

Biometrics are the technical term for measurements and related calculations pertaining to different aspects of our body features. It refers to measurements identified with human attributes. Biometrics verification (or practical confirmation) is utilized in software engineering to implement access control strategy as well as to use as a recognizable proof.

Biometrics are heavily used these days to recognize and identify individuals in several real-world applications.

Types of Biometrics, Biometric system and Characteristics:

There are two types of Biometrics, namely, Physiological and Behavioural. Physiological Biometrics includes a face, fingerprint, iris retina, DNA etc. Behavioural Biometrics includes keystroke, signature, and voice.

A simple biometric system consists of four basic components:

1. Feature extraction module where the data, that has been collected, is processed to extract feature vectors.
2. Sensor module which gathers the biometric data
3. Decision-making module in which a user is identified or a claimed identity is either rejected or accepted
4. Matching module where feature vectors are compared against those in the database or template.

Biometric frameworks have turned out to be more powerful and secure. The frameworks are known to be hard to hack or sidestep. Like some other frameworks, biometrics frameworks cling to an arrangement of qualities which guarantee the credibility and security of the framework. Figure 1 shows the characteristics of the biometrics followed by the explanation of each of these characteristics.

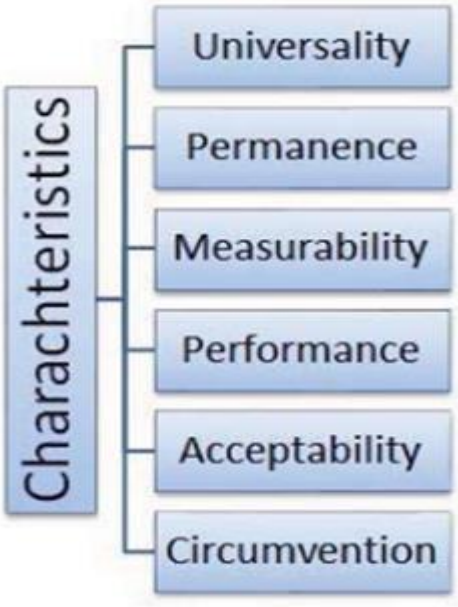


Fig.1 Characteristics of Biometrics

1. Universality implies that everyone utilizing a framework should have the attribute. Uniqueness implies the characteristic should be adequate for people in the important ranks with the aim that they can be recognized from each other.

2. Permanence identifies the degree to which a certain characteristic transform over some timespan. More particularly, a quality with 'great' Permanence will be invariant over the passage of time.
3. Measurability (collectability) identifies with the simplicity of procurement or estimation of the characteristic.
4. Performance refers to the accuracy achieved and speed of the implemented solution.
5. Acceptability signifies how well the people of different position in society accept the framework.
6. Circumvention identifies with the straightforwardness with which an attribute may be imitated using a similar substitute.

Factors for selecting the Biometric modality some critical elements that should be considered before choosing a specific methodology are:

1. Accuracy: It is one of the most critical of variables that should be evaluated while choosing a methodology. Once more, accuracy depends on a few different factors, for example, false acknowledgment rate (FAR), false reject rate (FRR), mistake rate, distinguishing proof rate and so forth.

2. High ability to thwart attacks: The across the board utilization of biometric acknowledgment frameworks in different sensitive applications requires assured and formidable defenses against all sorts of attack. In this manner, high significance is given to coordinate assaults where unapproved people can access the framework through communicating using open channels of the framework itself. Such an attack is known as caricaturing assaults and in this manner, the selected methodology should have a solid defense mechanism in place.

3. Cost-viability: This is a crucial factor to consider when choosing the adequacy and appropriateness of a specific methodology. A few modalities might be more practical than others. It is understood that the underlying work done on a biometric framework can frequently be remunerated for a short time which may often cause a speedier degree of profitability (ROI).

4. Client consent: The organization of a specific recognizable proof framework additionally relies upon how well it is acknowledged by the clients. In a few societies, certain modalities have a disgrace related to them and it can adversely affect the goal of the target system. In this way, it is essential to draw plans beforehand on modalities which are well worthy versus those that may cause some client acknowledgment issues.

5. Cleanliness: Another critical factor to consider before settling on modalities is that if it will require contact or is it contactless. Numerous associations want to utilize contactless modalities because of cleanliness reasons and furthermore for disease control.

UNIMODAL BIOMETRIC SYSTEM:

Biometric systems used in real-world applications are unimodal in majority of cases. These often depend upon the evidence of a single source of information to authenticate. Oftentimes verities of problems plague such systems, for instance:

1. Noise in the data that have been evaluated: (e.g., a fingerprint sensor may cause this scenario if it has been used repeatedly number of times)
2. Inter-class similarities: When large numbers of users are involved in a Biometric System, inter–class overlap can occur primarily in the feature space comprised of multiple users.
3. Intra-class variation: Such variations may be observed if the user incorrectly interfering with the sensor.
4. Spoof Attack: This attack transpires when signature or voice patterns are used in Biometric System.
5. Non-Universality: The Biometric System sometimes may be unable to acquire meaningful or useful Biometric data from a subset of users.

Majority of the drawbacks of the unimodal can be addressed by including multiple sources of information related to identification purposes. Apart from the advantages of such systems as discussed earlier, there are some certain other benefits as well in ensuring that a user in indeed present at the point where data is collected. This is achieved by engaging the user in a challenge-response type of actions where a random subset of biometric features is requested from the user. Some common multimodal biometrics is face and fingerprint, face and iris, iris and fingerprint etc.

Limitations of Unimodal Biometric Systems:

Regardless of having numerous natural preferences, the current biometric ID frameworks have faced number of limitations for different reasons. Biometrics is utilized as a part of numerous applications, for example, fringe control and voter ID issuance. Hypothetically, Unimodal biometric ID may appear to be considerably sound, however, there are various difficulties while enlisting population based only on a solitary (Unimodal) biometric. The significant issue with the Unimodal biometric framework is that a single metric is not appropriate for all applications and henceforth utilizing a multimodal biometric framework can address this issue.

Following are the constraints of Unimodal biometric frameworks:

1. Biometric sensor not performing against loud or unclear information:

The received biometric quality may be twisted because of defective procurement conditions. Such a fact can be observed in applications which utilize facial acknowledgment. The nature of the received facial pictures from the person that is trying to get clearance, may get influenced by light conditions and outward appearances. Another illustration could be in unique mark acknowledgment where a scanner can't read scratched fingerprints, and returning false database match [9]. An enlisted client may be erroneously dismissed while an impostor may be wrongly acknowledged in this manner.

2. Not very effective against specific groups of people:

Unique finger impression pictures won't be appropriately scanned for the elderly and youthful youngsters because of blurred fingerprints or immature unique finger impression edges. Even though the biometric attributes are found among all segments of human race, there could be exemptions where an individual can't produce a specific biometric. For instance, iris pictures won't be obtained if the subject has a neurotic eye condition.

3. Against Twins:

The facial acknowledgment may not work effectively for twins that are hard to distinguish as the camera won't have the capacity to handle twins.

4. May not work against parody assaults:

Unimodal biometric frameworks are not much of use against parody assaults where the information can be imitated or fashioned. For instance, unique mark acknowledgment frameworks can be effectively fooled using elastic fingerprint.

IV. PROPOSED SYSTEM:

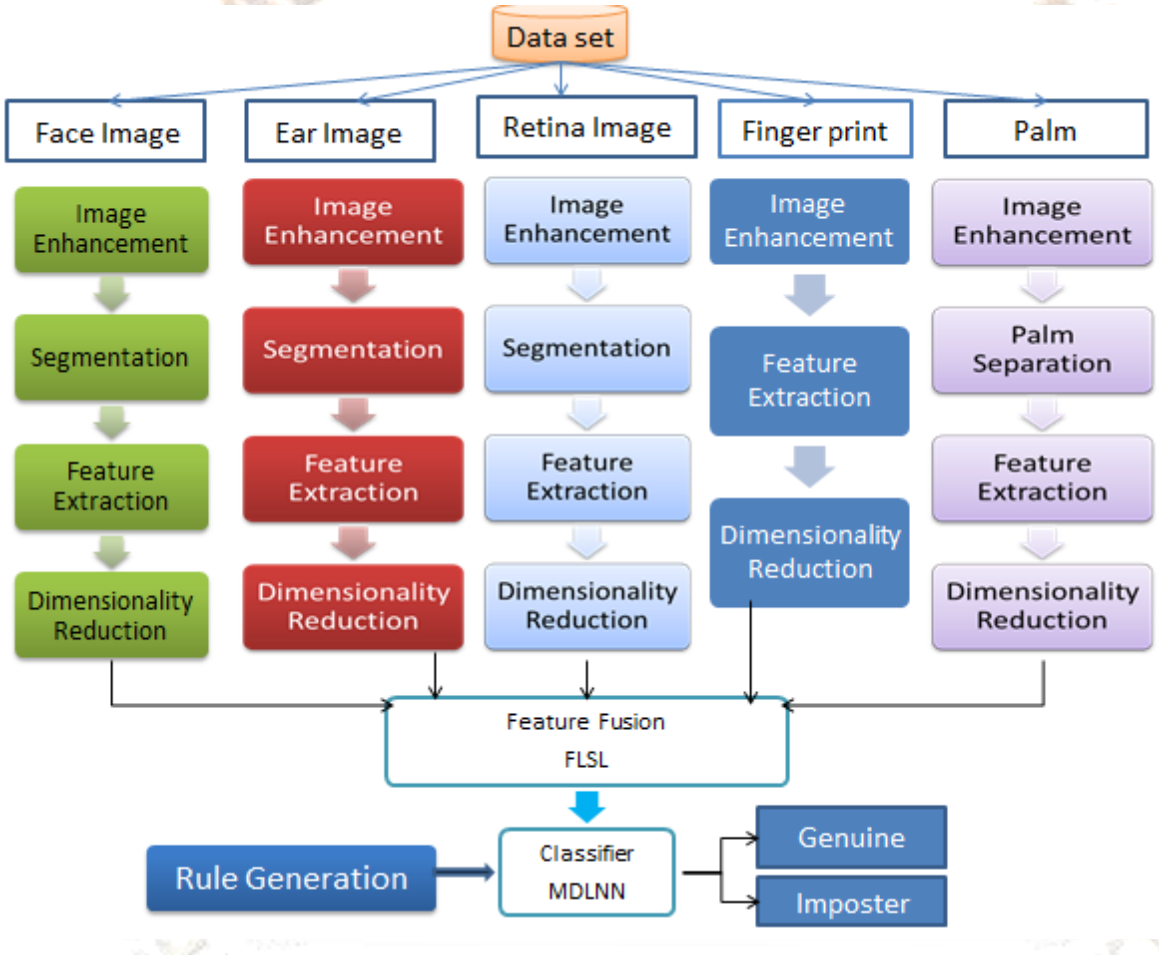
MULTIMODAL BIOMETRIC SYSTEM

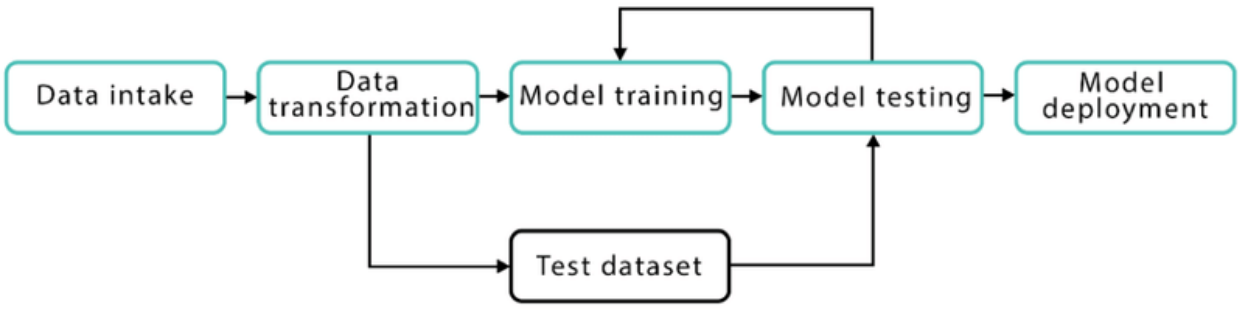
Multimodal biometrics refers to the use of a combination of multiple biometric modalities in a verification or identification system. Identification tactics based on multiple biometrics now days are on the rise.

To address the shortcomings of unimodal biometric frameworks, multimodal biometric frameworks utilize various sensors or biometrics. Biometrics such as iris acknowledgment frameworks can be balanced by maturing irises and finger examining frameworks can also be balanced by unclear or damaged fingerprints. Unimodal biometric do face issues even though these are restricted by the honesty of their identifier. Multimodal biometric frameworks can also get sets of data from a similar marker (i.e., sweeps of a similar finger or numerous pictures of an iris) or data from various other biometrics.

Multimodal biometric frameworks can intermix these unimodal frameworks successively. Combination of the biometrics data can happen at various phases of an acknowledgment framework. If there should arise an occurrence of highlight-level combination, the information itself or the highlights extracted from different biometrics are intermixed. Coordinating score level combination merges the scores produced by various classifiers relating to various modalities. At last, in the event of choice level combination, the outputs of various classifiers are joined by means of systems, for example, dominant part voting. Besides, highlight level combinations are accepted to be more successful than an alternate level of combinations. The stored information is enriched in this way and the calculated score get more accuracy. In this way, combination at the element level is required to give better outcome.

V.SYSTEM ACHITECTURE





Machine Learning Implementation

VI. CONCLUSION:

Dependable and strong identification systems are basic to numerous legislature and business forms. The customary information based and token-based strategies don't generally give strong individual acknowledgment. It is, along these lines, clear that any framework guaranteeing solid individual acknowledgment should fundamentally include a biometric part. This isn't, in any case, to express that biometrics information alone can provide fully error-free individual acknowledgment. However, the introduction of multimodal Biometric Authentication system can clearly have a high impact in this case and bring a significant sense of strength in security systems built upon multimodal biometric policy. This research work proposed a framework to achieve just that and it is believed such a system can provide high security in the future for any biometric identification system.

VII. FUTURE ENHANCENMENT:

Updates are best to continue the legacy of any applications. For this we propose to integrate with micro businesses into the research and try to make the security more robust and improve the accuracy. The use of multi-occurrence and multi-sensorial biometrics framework can be used to enhance the system security.

Multi-occurrence biometric frameworks

These frameworks employ at least one sensor to capture data of at least two distinct examples of the same biometric characteristic. A case of this could be a framework that detects pictures of different fingers.

Multi-sensorial biometric frameworks

These frameworks utilize at least two unique sensors to detect a similar example of a biometric characteristic. These scanned or captured tests are then handled utilizing a solitary calculation or a mix of calculations.

VIII. REFERENCES:

[1]. S.A. Saleh, S. Azam, K.C. Yeo, B. Shanmugam and K. Kamarhati, "An improved face recognition method using Local Binary Pattern method", IEEE International Conference on Intelligent Systems and Control (ISCO), 2017.

[2] R. Par Kavi, K.R. Chaldees and J. Ajeet, “Multimodal Biometrics for user authentication”. 11th International Conference on Intelligent Systems and Control (ISCO), 2017.

[3] R. Singh, J. Gottwald and S.S. Yadav, "Multimodal Biometric Authentication System: Challenges and Solutions", Global Journal of Computer Science and Technology, vol. 11 Issue 16, 2011.

[4] C.S. Kong, T. Yang and C. Tseng, "User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices", The Scientific World Journal, vol. 2014.

[5] A.K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition", IEEE Transactions on circuits and systems for video technology, 14(1), 2004, pp.4-20.

[6] Y. Cai, H. Jiang, D. Chen and M.C. Huang, "Online Learning Classifier based Behavioral Biometric Authentication", 2018 IEEE 15th International Conference on Wearable & Implantable Body Sensor Networks, 2018.

[7] S. Ghosh, A. Majumder, J. Goswami, A. Kumar, S.P. Mohanty and B.K. Bhattacharyya, "Swing-pay: One card meets all user payment and identity needs: A digital card module using NFC and biometric authentication for peer-to-peer payment", IEEE Consumer Electronics Magazine, 6(1), 2017, pp.82-93.

[8] A. Ross and A.K. Jain, "Multimodal Biometrics: An overview", In Signal Processing Conference, 12th European (pp. 1221-1224). IEEE, 2004.

[9] K. Dela and M. Grgich, "A survey of biometric recognition methods", In 46th International Symposium Electronics in Marine, vol. 46, 2004, pp. 16-18.
[10] A.K. Jain, L. Hong, S. Pandani and R. Bole, "An identity-authentication system using fingerprints", Proceedings of the IEEE, 85(9), 1997, pp.1365-1388.
[11] M. Madhavaram and R. Ravi, "Fingerprint-Sclera based Multimodal Biometric Authentication System using Hybrid Genetic Intelligent Technique for System on Chip Application", Toga Journal, vol.14, 2018.
[12] N. Bansal, "Enhanced Ras Key Generation Modeling Using Fingerprint Biometric" (Doctoral dissertation, NIT, Jamshedpur), 2018.
[13] O. Dogbane and D.J. Kim, "Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment", Decision Support Systems, 106, 2018, pp.1-14.
[14] J. Peng, A.A.A. El-Latif, Q. Li and X. Neu, "Multimodal biometric authentication based on score level fusion of finger biometrics", Opti International Journal for Light and Electron Optics, 125(23), 2014, pp.6891-6897.
[15] R. Sellick, U. Ulua, A. Mink, M. Indiana and A. Jain, "Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems", IEEE transactions on pattern analysis and machine intelligence, 27(3),2005, pp.450-455.

TECHNIX INTERNATIONAL JOURNAL FOR ENGINEERING RESEARCH
TIJER
OPEN ACCESS JOURNAL