An Enhanced 3-Tier Multimodal Biometric Authentication

Aman Kathed, Sami Azam, Bharanidharan Shanmugam, Asif Karim, Kheng Cher Yeo, Friso De Boer, Mirjam Jonkman
College of Engineering, IT and Environment
Charles Darwin University, NT, Australia
amankanthed1994@gmail.com,
{sami.azam, bharanidharan.shanmugam, asif.karim, charles.yeo, friso.deboer, mirjam.jonkman}@cdu.edu.au

Abstract- In today`s networked world the requirement for security frameworks are becoming tighter because of an increase in violations like PC hacking, unlawful access of ATM, cellphone and security ruptures in government agencies, and what's more, private structures. Lawbreakers exploit basic imperfections in the traditional security frameworks. For these security issues, biometric acknowledgment framework is utilized for identifying individuals using distinguishable and exclusive proof. Biometrics of an individual can`t be hacked effortlessly as opposed to a password. A multimodal framework can consolidate any number of free biometrics and make any biometric system a lot stronger than using only one biometric as user's confirmation device. The combination of numerous biometrics reduces the framework mistake rate as well. Combination strategies incorporate a strategy of converging biometric modalities consecutively until the point that an adequate match is reached. This paper proposes a block diagram of multimodal biometrics; likewise, discusses the utilization of biometric frameworks and their leeway over the unimodal biometric framework and how a combination of different biometrics can substantially decrease the framework's error rate

Keywords- Authentication, Biometrics, Multimodal, Fusion, Matching score, Unimodal, Verification.

I. Introduction

The proposed research 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 can 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.

Credit card extortion, for instance, costs the business a huge amount of dollars every year, the absence of powerful client identification systems is one of the primary reasons of credit card fraud.

Generally, passwords (information-based security) 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. Biometrics authentication systems refer to the programmed identification (or confirmation) of an individual (or an asserted personality) by utilizing certain physiological or behavioral attributes of that individual. 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 [1]. 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 [2]. 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) [3].

II. Biometrics

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.

A. Types of Biometrics, Biometric system and Characteristics

There are two types of Biometrics, namely, Physiological and Behavioral [4]. Physiological Biometrics includes a face, fingerprint, iris retina, DNA etc. Behavioral 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 [5]. 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.

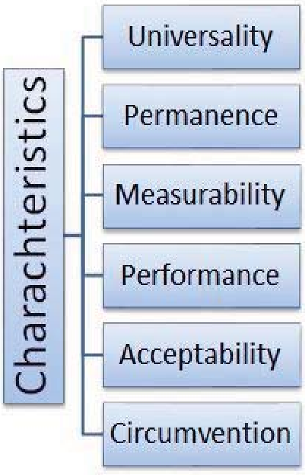

Fig. 1. Characteristics of Biometrics [5]

1. *Universality* implies that everyone utilizing a framework should have the attribute. Other characteristics are also shown in Figure 1 and discussed below:
2. *Uniqueness* implies the characteristic should be adequate for people in the important ranks with the aim that they can be recognized from each other.
3. *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.
4. *Measurability* (collectability) identifies with the simplicity of procurement or estimation of the characteristic.
5. *Performance* refers to the accuracy achieved and speed of the implemented solution.
6. *Acceptability* signifies how well the people of different position in society accept the framework.
7. *Circumvention* identifies with the straightforwardness with which an attribute may be imitated using a similar substitute.

B. 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 [6].
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) [7].
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 [7].
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.

III. 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 [3]:

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 number 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.

A. 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 [8].

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 [10].
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. 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 (may require unique mark outputs and, utilizing voice acknowledgment, a talked pass-code) [11].

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 [12].

A. Types of Multimodal Biometric System

The different kinds of multimodal biometric frameworks are examined underneath [19]:

1. **Multi-algorithmic biometric frameworks**: These frameworks take a solitary biometric test from a solitary sensor, after which it is utilized in at least two distinct calculations.
2. **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 detect pictures of different fingers.
3. **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.

B. Advantages of Multimodal Biometric System

The accuracy of a multimodal biometric framework is estimated by the error rate of picture securing and coordinating. Picture securing errors incorporate inability to select (FTE) rate and to obtain (FTA) rate. False non-coordinate rates (FNMR) is used to determine the 'Coordinating Errors' in which an honest to goodness subject is rejected and a false match rate (FMR) is accepted where a wrong individual is allowed to get into. Multimodal frameworks have a near-zero FTA, FTE, FNMR and FMR rates [13].

In a situation where a great many individuals should be enlisted in a framework and a few people may confront issues with a specific biometric quality, multimodal frameworks can cover this constraint by utilizing an alternate biometric for that portion of the populace. This will guarantee nearly zero inability to-enlist (FTE) rate.

V. FUSION

In multimodal biometrics more than one biometric modality is used; having more than one decision channels. Biometric fusion is a mechanism that can combine the classification results from each biometric channel. In a view to boost the strengths and to reduce the weaknesses of the individual measurements, Multimodal biometric fusion links measurements from multiple different biometric traits [20]. Multimodal Biometrics have various levels of fusion: feature level, sensor level, matching score level and decision level shown in Figure 2. Fusion of various types such as matching score, rank, and division levels have been thoroughly studied in the literature. Remapping fusion often consists of the feature level along with the sensor level whereas Post-mapping fusions are generally formed with the aid of decision level and matching score level. Generally, there are some difference in how data is integrated in *pre* and *post* mapping fusion. For the later it is integrated after mapping into decision space/matching score, while for the former the data integration takes place before any application of the classier [14].

A. Pre-mapping fusion I:

Sensor level Fusion: In sensor level fusion, combination of the biometric qualities comes from various sensors like video camera, scanners for thumbprint or iris Scanner etc., to merge those into a combined biometric entity. For instance, sensor fusion level may incorporate identifying a speech signal at the same time with two different microphones. Though fusion at this level is expected to enrich the biometric recognition accuracy, but as because the data from different modalities are not often compatible, thus such fusion cannot always be employed for multimodal biometrics [15, 21].

B. Pre-mapping fusion II:

Feature Level Fusion: In feature level fusion, feature vectors are extracted one by one, before which signal sourced from different biometric channels are first pre-processed. Using specific fusion algorithm, these feature vectors can be combined to formulate a composite feature vector. This composite feature vector is then employed for the classification process. Concatenation of feature vectors acquired from face and the fingerprint modalities is an instance of a system that is multimodal in nature. It has been found that fusion at the feature level is supposed to project better performance while comparing with fusion at the score level and decision level [16]. The primary reason is that the feature level contains more useful information about the raw biometric data. However, there are doubts on the practicality of such fusion types. For instance, in number of cases, the given features might not be compatible due to differences in modalities. Also, such concatenation may result in a feature vector with a significant high dimensionality.

C. Post-mapping fusion I:

Matching Score Level: In this type of fusion, instead of combining the feature vectors, these are processed separately and the individual matching score is calculated, then depending on the accuracy of each biometric channel, matching level can be fused to gain composite matching score. Decision module then subsequently works with this composite matching score once received. As the performance of this fusion level is reasonably decent and simple, this seems to be the most appropriate fusion level at present. Further, this type of fusion may be broken down into two sub-categories. First is 'combination' where a scalar fused score is derived by normalizing the input matching scores within the equivalent range and subsequently joining such normalized scores together. The second sub-category of fusion is known as 'classification' [17].

D. Post-mapping fusion II:

Decision Level Fusion: In this approach, a separate pre-classification for each of the modalities take place.

Based on the fusion of the outputs of several different modalities, the final classification is obtained. In this method, for each biometric type, a distinct decision is taken at a considerably delayed stage [18], severely limiting the a key factor which could have been a prime catalyst in enhancing the accuracy of the system through the fusion process. Thus, fusion at such a level is considered least effective.

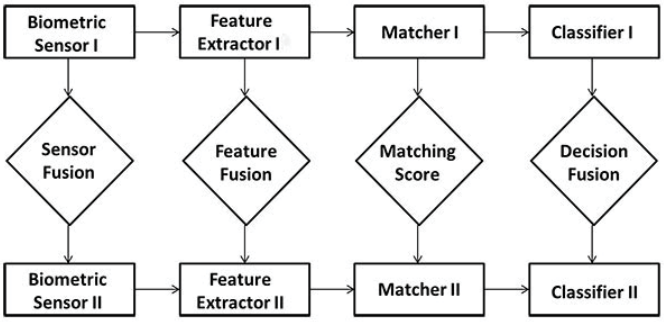

Fig. 2. Fusion levels in Multimodal Biometric Systems [18]

VI. Proposed Architecture

The proposed architecture works in a way that the biometric modality, face, and iris are captured and then fused at feature level and the result is stored in the database. The stored result is then matched with input provided and if the match works the system is made to send OTP. This has to be recorded as user's voice and then compared with the voice data set which is already in the voice database. If there is a match the system is ready for use, in any other case the access is denied.

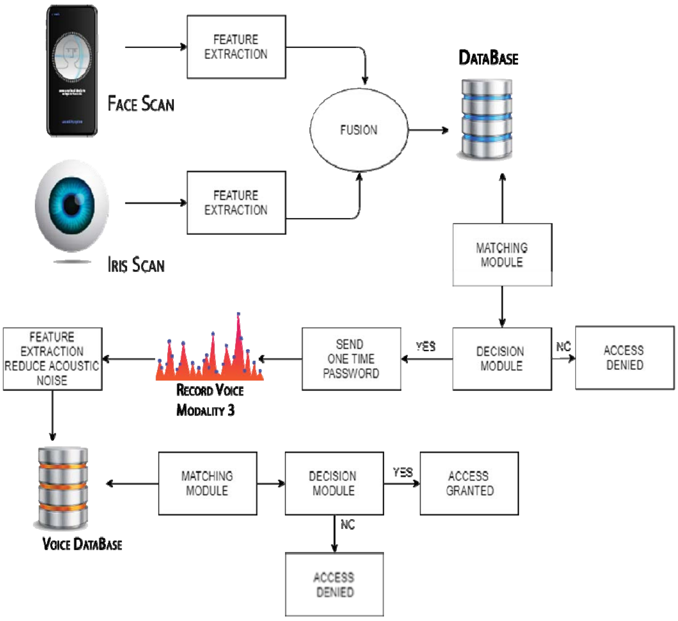

Fig. 3. Proposed architecture

The proposed architecture is unique in providing access to the files and folder which needs top-notch security as they have relevant high-security or personal data. The idea of using three modalities is to generate a list of criterions which needs to be authenticated for any access to be provided. Generating OTP on the registered number is another attempt to increase the security layer which has a 4-digit number which has to be read over the phone and the voice frequency is matched with the voice already registered in the database at the initial phase.

The proposed android application has a simple user interface which has two enrolment buttons for face enrolment and fingerprint enrolment, once the enrolment of these two biometric modalities is done, fusion of the characteristics is carried out in the background by pre mapping fusion also known as feature level extraction. The feature fusion score is stored in the database and matched with the score and then proceed if there is a match. The match triggers another system which sends in the OTP which is 4-digit password combination sent to the mobile. Once OTP is received the system triggers another pop up with voice verification mechanism, the OTP when read over that interface matches user's voice already stored in a database while the enrolment phase and when the voice and OTP match the final outcome is achieved. The framework uses face and iris scan, which often works better to address the noise issue especially prone to finger scanning. The system is now ready for use and illustrated in Figure 3.

VII. Conclusion & Future works

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.

References

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

[2] R. Parkavi, K.R. Chandeesh and J. Ajeeth, "Multimodal Biometrics for user authentication". 11th International Conference on Intelligent Systems and Control (ISCO), 2017.

[3] R. Singh, J. Gothwal 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. Koong, 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 ElectronicsMagazine, 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. Delac and M. Grgic, "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. Pankanti and R. Bolle, "An identity-authentication system using fingerprints", Proceedings of the IEEE, 85(9), 1997, pp.1365-1388.

[11] M. Madhivhanan and R. Ravi, "Fingerprint-Sclera based Multimodal Biometric Authentication System using Hybrid Genetic Intelligent Technique for System on Chip Application", Taga Journal, vol.14, 2018.

[12] N. Bansal, "Enhanced Rsa Key Generation Modeling Using Fingerprint Biometric" (Doctoral dissertation, NIT, Jamshedpur), 2018.

[13] O. Ogbanufe 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. Niu, "Multimodal biometric authentication based on score level fusion of finger biometrics", Optik-International Journal for Light and Electron Optics, 125(23), 2014, pp.6891-6897.

[15] R. Snelick, U. Uludag, A. Mink, M. Indovina 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.

[16] D. Jagadiswary and D. Saraswati, "Biometric authentication using fused multimodal biometric", Procedia Computer Science, 85, 2016, pp.109-116.

[17] K. Kumar and M. Farik, "A review of multimodal biometric authentication systems", International Journal Of Scientific & Technology Research, 5, 2016, p.12.

[18] J. Wayman, A. Jain, D. Maltoni and D. Maio, "An introduction to biometric authentication systems", In Biometric Systems (pp. 1-20). Springer, London, 2005.

[19] E. Stefani and C. Ferrari, "Design and Implementation of a Multi-Modal Biometric System for Company Access Control", Algorithms, vol. 10 (61), 2017.

[20] D. Kaur and K. Gaganpreet, "Level of Fusion in Multimodal Biometrics: a Review", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3(2).4, 2013.

[21] M. Gudavalli. "Multimodal Biometrics -Sources, Architecture and Fusion Techniques: An Overview", International Symposium on Biometrics and Security Technologies, 2012, pp.27-34.