Journal of Advances in Mathematics and Computer Science

29(6): 1-13, 2018; Article no.JAMCS.28036
ISSN: 2456-9968
(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

Advanced Security through Biometric Systems and Reporting Techniques

Deepak Bhandari[1*] and Manavjeet Kaur[1]

[1]PEC University of Technology, Chandigarh, India.

Authors' contributions

This work was carried out in collaboration between both authors. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/JAMCS/2018/28036
Editor(s):
(1) Dr. Doina Bein, Professor, Applied Research Laboratory, The Pennsylvania State University, USA.
Reviewers:
(1) Radosław Jedynak, Kazimierz Pulaski University of Technology and Humanities, Poland.
(2) Utku Kose, Computer Sciences Application and Research Center, Usak University, Turkey.
Complete Peer review History: http://www.sciencedomain.org/review-history/27567

Original Research Article

Received: 30 June 2016
Accepted: 23 August 2016
Published: 04 December 2018

Abstract

World requires to evolve itself with a stringent personnel identification system due to increase in the number of assets and expansion in the number of stakeholders involved in their maintenance. This is constantly challenged by the newer threats. The system requires being high on quality factors such as availability, performance, robustness, durability with negligible downsides such as cost, partialness in its perusal. To ensure these high standards, society has been making way for biometric driven security schemes that are able to replicate the expected quality norms. But the existing biometric systems need to be more convergent to the customization that is oriented to the end user. Therefore, this paper intends to bring system and end user to a same platform of contribution. This is achieved when end user customizes the system as per his biometric requirement and the system can refer the user in case it is unable to exactly identify biometric traits during user authentication. Additionally, system ensures the information compliance to target audience along with a constant reporting culture as a minimum standard. This would introduce high reliability and maximum functionality to the technological ecosystem of the security world.

Keywords: Multimodal biometrics; user-defined weightage; OTP – One time password; reporting technique.

**Corresponding author: E-mail: deepak11287@gmail.com;*

1 Introduction

In today's high technology environment, people and related organizations have become increasingly dependent on the information systems. It is of highest concern that the information is properly accessed by the eligible contenders due to growing threats from unidentified resources with mala fide intentions. Previously, access cards and passwords were used to ensure that genuine users access the system or the information stack. But these solutions came up with the limitations of getting stolen, misplaced, forgotten etc [1]. To overcome such problems in the existing scheme of things, biometric has been approached and identified as a more preferred method of user authentication [2].

Biometrics can be referred as approach of individual recognition based on their behavioral and biological traits. This helps in securing assets that are utilized in shared space and needs to be restrained from everybody's access [3]. The intended group to be provided access is registered with their biometric characteristics in the system. Subsequently, system would ensure that every request for system access is validated and accepted only for the registered group of population.

Biometric system can also sometimes deliver inaccurate results [4] owing to reasons such as variations within persons, sensor performance, feature extraction and matching algorithms. Research community has upgraded itself with numerous technology advancements but role of the end user in safeguarding the security policy has been constrained [5]. User is expected to be a source of biometric traits after which system is made to control proceeding of user authentication with the help of database. Systems may accept or reject the identity after the checking the user database. In the proposed approach, a paradigm shift is provided wherein end user will become the driving force to authenticate biometric traits in case the system is unable to decide with clarity. It is identified that performance metrics and user confidence on the system transaction is enhanced by the proposed approach i.e. multimodal biometrics along with user defined weightage scheme, fuzzy logic and reporting techniques. Reason for the enhanced user confidence is the fallback option provided by the system to the genuine end user in case it identifies that end user has provided inexact biometric traits within accepted levels. Also, the intimation culture of the system is highly practical wherein system confirms the user of the successfully granted access, conditional access eligibility due to partially recognized biometric traits of the user. This ensures that system if not completely dependent only on its database but has a flexibility to think and react whenever it is unclear. Also, there is always a perfect sync up between the end user and system on system monitoring in the executed approach to keep the system in a secure state [6].

Fundamental objectives behind the proposed problem formulation are:

1. To study biometric traits, and a comparative analysis on unimodal and multimodal biometric technique.
2. Induction of fuzzy logic for decision making
3. To identify scope of improvement in system by using user-defined weightage scheme and introduction of a fallback option (OTP) for customers facing FRR.
4. To enable intimation and transaction information to end user for enhancing security and controlling damages in FAR scenarios.
5. To analyze performance of the proposed methodology using FRR, FAR and turnaround time of reporting techniques.

2 Biometrics and Multimodal Biometrics

Biometric system demands to operate under the environment and knowledge that there exist multiple physiological and behavioral characteristics in an object that are uniquely identifiable. They have capability to show characteristics such as universality, permanence, and acceptability [7]. Also, that they are acquired with relative ease by usage of specially designed infrastructure such as sensors and are numerically convertible. This lends possibility and induces environment to initiate system driven decisions in the identity

management domain. Therefore, biometric system is fundamentally a mathematically driven template identification system that acquires biometric information from an object, thereby extracting its prominent feature set. This feature set is collated to the already acquired feature set of the user that is stored in the user repository, and thereby invoking an action based on the collated results. Fig. 1 represents the major traits that can be acquired from a human body for biometric validation. These include fingerprint, gait, ear, eyes, hand geometry, palm print etc. Depending on the necessity, nature, and functionality of the system, biometric traits can be opted for user identity validation. The four modules utilized for user validation in biometrics are Sensor Module, Quality assessment and feature extraction module, match and decision making module, System database module [8].

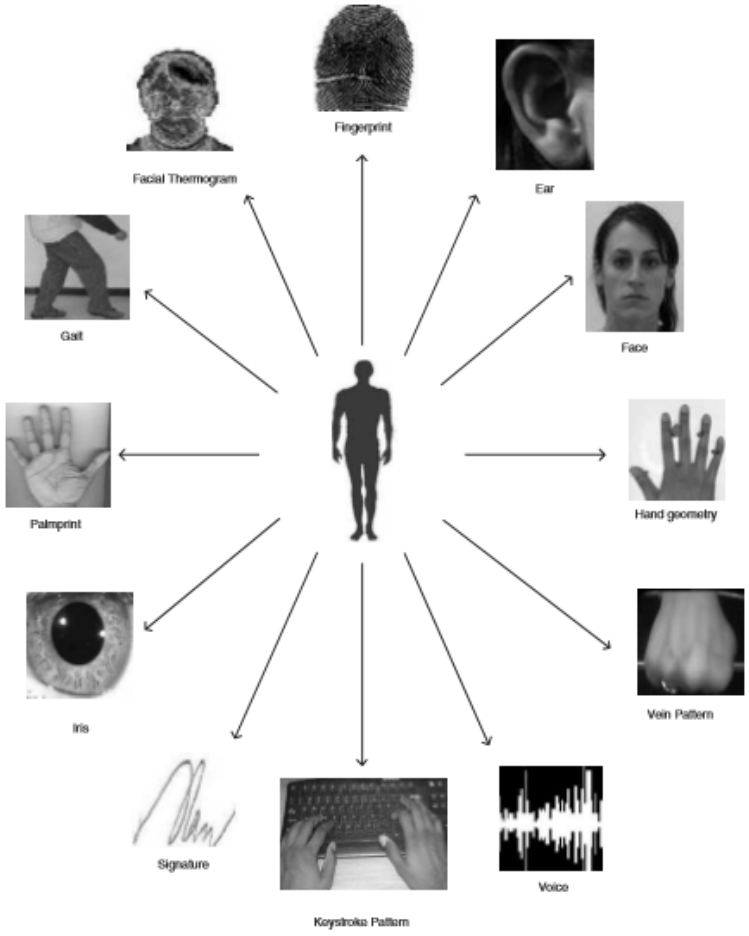

Fig. 1. Different biometric traits [Jain et al., 2008]

Unimodal biometric systems perform object recognition based on a single source of biometric information. In contrast to this, multimodal biometric systems utilize multiple source of biometric information making them more reliable, resilient and result oriented in their paradigm [9]. Limitations of unimodal biometrics are lack of universality, noisy signals, performance, fraud possibility, incompatibility whereas multimodal biometrics is better on these fronts. Multimodal biometrics has advantages of improving accuracy by considering multiple traits, multiple instances, reduced spoofing [10]. Different traits or instance can be fused at sensor level, feature level, matching score level, decision level [11,12]. Performance metrics for biometrics system is decide on FAR (False Accept Rate), FRR (False Reject Rate), FER (Fail to Enroll), GAR (Genuine Acceptance Rate), FTA (Fail to Acquire). This paper acquires fingerprint and face to execute

multimodal biometric scheme and fuses them at score level to improve on FRR metric and GAR gets enhanced proportionally. Multi-biometric system can use combination of other attributes as well, such as Fingerprint, Iris, hand geometry, palm print [13,14] depending on the need and criticality.

3 User-defined Weightage Scheme and Fuzzy Logic

Customizable system parameters and self-learning in system as per the user helps to improve performance and minimize the error rates. The degree of importance is assigned to each trait of the user to retrieve favorable results. This is highly useful in scenario wherein one of the biometric traits of the user gets degraded due to multiple factors. The performance in a multiple biometric system is enhanced by initiating user specific thresholds, and weight assignment to individual traits [15]. System is customized according to the user's biometric traits, with each biometric trait assigned a percent weightage out of combined value of 100. The executed approach in this paper requests degree of importance for finger print and face from the user. Default system configuration allocates 50 % weightage to both traits. Results in this paper show that user with high dependency on one of the traits show better results with user-defined approach.

The proximity score achieved for each biometric trait is fused together at score level by summation of weighted individual biometric score. The score obtained after summation of weighted scores is a normalized score of the different traits that will be accounted for triggering system action. Variations in this fusion approach can be applied for even better results [16]. The normalized score is used to classify biometric traits into different categories as per system configured bounds [17]. This paper categorizes combinational score of fingerprint and face under exact, proximity, average, poor groups with the help of fuzzy logic.

4 System Action and Reporting Techniques

The score categorization of traits after fuzzy logic will decide for system action. System logic can decides to provide prompt access grant or reject the ones performing poorly. This can be customized as per the requirement and criticality of the application. The utilized methodology in this paper provides prompt access only to the "exact" biometric traits and rejects the "poor" biometric traits. Traits falling under "Proximity" and "Average" categories will be provided with a fallback option to prove their authenticity. It is essential that the provided fallback option is equally secure that does not compromise on security and can simultaneously help to improve user satisfaction index. This paper used OTP (One time password) as a fallback option that is communicated to the end user on his registered touch points. One time password was used as a fall back option due to its strengths of only one time usage possibility, no need to remember, time validity and dynamic nature that makes it one of the most secure options [18]. As per results obtained, fallback option to the user decreases FRR (False Reject Rate) occurring due to poor hardware, traits degradation etc., thereby enhancing system performance.

This paper also brings forward the usage of reporting techniques for the purpose of intimation to the end user. Techniques used are E-Mail and Mobile SMS due to their wide availability with the world population. End user gains more confidence on the system's security by this approach because every transaction (either successful or failed) regarding his biometric traits is intimated. Cases wherein user is not involved in transaction but is receiving intimation indicates fraudulent attempt. System administrator or the end user can promptly initiate necessary action to control damages. In this paper, end user is communicated of the transaction information and OTPs on his registered email ID and mobile number that is acquired during user enrollment phase. OTP is chosen as a security technique for its strong security features [19].

5 Methodology

In the existing biometric systems, it is observed that focus is kept on the system improvement with their energies devoted to optimization of currently available data acquisition processes. In contrast, the proposed

methodology embarked hereby focuses on the idea of "inclusion of both system and user" in a single cluster of knowledge wherein system and user identify more with each other's capabilities. This is achieved by:

1. System's flexibility to customize itself to the user preferences
2. Providing secure fallback option for the user in case of inexact biometric traits
3. Enabling constant interaction between system and end user on the transactions

This methodology ensures that system and user are always at help for each other. On one hand, system can validate user's biometric traits and customize itself to the user preferences. On the other hand, it will be end user's intervention that will rescue the system in case it comes across an issue. Practically, both will be at service of each other to keep each other in secure state. The proposed methodology in the identified approach can be understood in a three step procedure as User enrollment/registration process, Functional flow, and Monthly reconciliation.

5.1 User enrollment/Registration process

For any system to validate end user, it is essential that the system procures and establishes a sound repository with clear details of the end user. Data acquisition environment needs to be simulated with the real time environment to avoid any issue during transaction in real environment. This is important because biometric samples such as for face can show variation in different light, positioning etc. [20]. Besides knowing the biometric details, this methodology procures contact details of the user also i.e. Email and Mobile number as contact points. Correct and clear data acquisition of biometric samples provides good foundation to a secure system. This is necessary because the stored sample details will be collated with sample collected during user's access attempt to retrieve a collation score. This collation score would be the reason for system's decision to grant access. User enrollment is done in four steps as: Acquisition of the biometric samples (Acquires traits), assigning criticality to traits (Assign weightage to traits), Personal details (Procures Contact details), and Data commit (Save acquired data to database). Fig. 2 explains the user enrolment process.

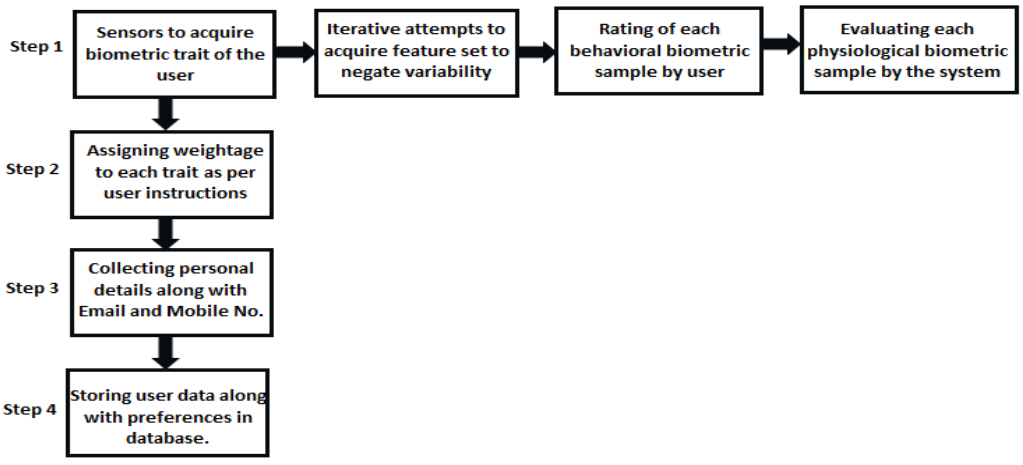

Fig. 2. User enrolment procedure

5.2 Functional flow

Functional flow targets at sharing the step by step stages from the point when a user provides its biometric traits to the point when system gets in agreement or disagreement with the user's authentication attempt.

Before the functional flow initiation, it is expected that there a sound user data repository is maintained during user enrollment. Also, the infrastructure used such as sensors during enrollment and authentication are of the same quality to retrieve best possible results.

This design can basically be categorized in four steps. As per the quality of biometric inputs provided, these are modulated by the system logic lying underneath. The steps are as:

5.2.1 Biometric sample evaluation

System evaluates provided biometric samples by the end user in comparison to the stored biometric traits in the user repository. Each trait is compared to generate a proximity score. All the traits are fused together with defined weightage for each trait as per the user configuration set down during enrolment. Finger print is evaluated [21] with minutiae points and face is evaluated using histogram approach [22,23]. The normalized score of different traits is identified as below:

Normalized value > 0.99 – Exact match
Normalized value between 0.75 and 0.99 – Proximity Match
Normalized value between 0.50 and 0.75 – Average Match
Normalized value less than 0.50 – Poor Match

The values mentioned above indicate the threshold scores for initiating system decisions [24].

5.2.2 Results with fuzzy logic

Biometric sample evaluation will evaluate a normalized score and provide the resultant categorization of biometric traits [25]. This would be expressed in degrees of exactness categorized under four major heads i.e. Exact, Proximity, Average, Poor. These categories would define system's next course of action. As per further filtration logic of the system, it would club the results of biometric evaluation under three heads as: Exact match with user database, Proximity or Average match with user database, Poor match with user database. Each of the three categories would invoke three separate business logic for decision making [26].

5.2.3 System action

System action is materialized on the fact that how closer the results have been to the desired and accordingly decides to be sensitized for actions. This means that higher the score resulting in closer to exactness category, lesser will be obstruction or review by the system for providing access. By this logic, system action categories are invoked. System action categories are:

(i) **Exact match with user database** – System access will be granted to the user. Also, user will be duly informed of this granted access along with transaction time on his registered touch point i.e. Email and Mobile number.
(ii) **Proximity or Average match with user database** – In case the system observes that provided biometric traits are in proximity or Average match, it would seek support from the user for further decision. This is realized by an OTP generated by the system as a fallback authentication. The OTP will be communicated to the user on his registered touch points i.e. Email and Mobile number. In case the user is genuine, he can access his mobile or email to know the OTP. This OTP can be used by the user for his identity acceptance by the system. Please note that system generates an OTP with an information that system administrator should be contacted in case this issue is regularly observed because there may be a need to review enrollment details of the user [27].
(iii) **Poor match with user database** - In case the system observes that biometric traits are in poor match with the database, system would intimate the end user though a dialog prompt that identity is not recognized and access request is reject. If required, user may meet system administrator for any corrective action.

5.2.4 Validate OTP

One time password is generated for the users with the proximity or Average match. This OTP is communicated to the end user on his registered touch points i.e. Email and Mobile number. This can be supplemented by security protocols for additional secrecy of the password transmitted. In case the access attempt is by a genuine user, he can gain the OTP from his Email or Mobile number. End user can use system service of OTP validator to validate himself through the OTP within 20 minutes of OTP generation [28]. OTP validator can choose either of the two decisions as per the correctness of OTP details. These are:

(i) **Valid OTP** – User will be granted access if the OTP details shared from end user is correct. Also, system would invoke an intimation message to the end user on registered Email and Mobile that access has been granted after successful OTP validation.
(ii) **Invalid or expired OTP** – User will be prompted with an error message by system in case an invalid or an expired OTP is shared. Access request is rejected.

5.3 User reconciliation

System procures each transaction's log. As a monthly process, the system administrator will review the system logs to identify the set of users who are constantly failing the biometric validation and generating OTP to access the system. In such scenario, administrator will have the user enrolment process of such users verified. In case required, fresh samples of the user will be taken to ensure that user validation process is smoothened for such regularly troubled users. Also, Security loopholes are identified through regular tracking of logs. Fig. 3 depicts the user reconciliation process.

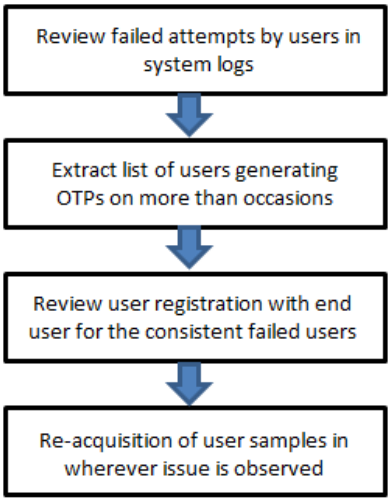

Fig. 3. User enrolment procedure

6 Results and Discussion

6.1 Unimodal and multimodal biometrics

Multimodal biometrics enhances security in personnel identification and displays higher accuracy in comparison to the unimodal approach. Multimodal biometrics removes dependence only on a single user trait to induce reliability in domain of identity validation. This paper utilized 80 finger print samples in which eight samples were rejected by the system during testing. Unimodal biometrics decided to reject all

these eight samples. But in multimodal biometric approach, normalized score of traits were used by the system to identify the object more discretely and provided better results. Results in Table 1 shows total user database of 40 in which 8 finger prints inputs of 4 genuine users are found inexact by the system. Graphical representation in the Fig. 4 shows the resultant score has improved by 77 % which clearly indicates that multimodal approach is preferable over unimodal approach for the cases where inexact biometric details are provided.

Table 1. Performance statistics comparison for Unimodal and multimodal

Total users with biometric details	User count with inexact finger prints	Biometric approach	Average score	Resultant score improvement (in % age)
40	4	Unimodal (Only Finger print)	0.39275	77.3
40	4	Multimodal (Fingerprint + Face)	0.696625	

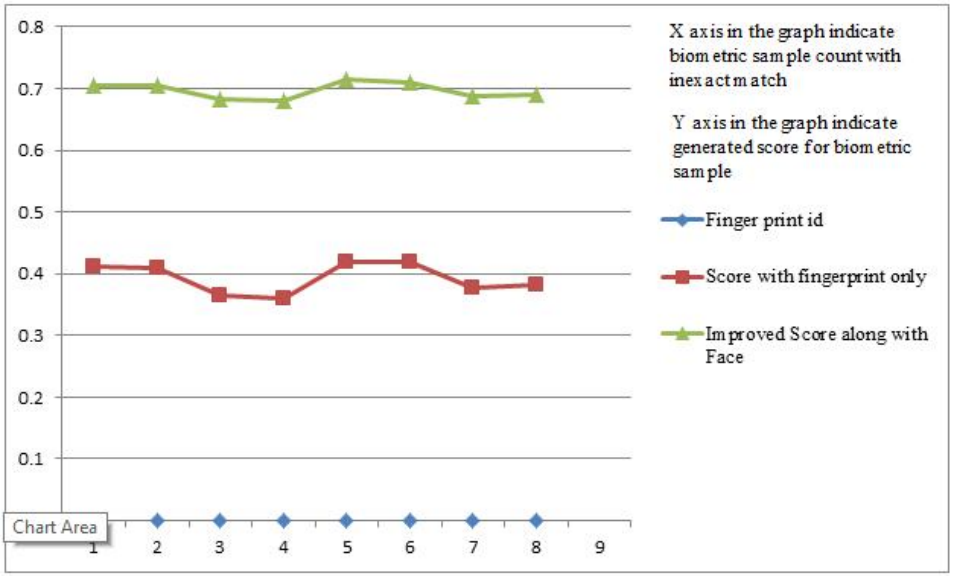

Fig. 4. Performance statistics comparison for Unimodal and multimodal

6.2 Default weightage and user-defined weightage scheme

Weighted biometric system along with user preferences of the weightage evaluates to a more personalized behavior by the system for the end user. This is observed as highly helpful for cases wherein one of the attributes cannot be acquired with high accuracy. For such cases, Table 2 shows comparison between a default weightage approach and user defined approach. It is observed that the user-defined weightage scheme score better in comparison to the default weightage wherein user will provide the priority or criticality of each biometric trait. As per the user inputs, system would evaluate validity and exactness of the provided traits. This is especially useful in accommodating particular set of users have undergone physical changes with time and expects system to behave accordingly. This paper results utilized user defined weightage (80:20) for face and finger respectively. Graphical representation in Fig. 5 shows that user-defined weightage scheme show improvement in scores by approximately 26 % indicating that user-defined schemes are more preferable for the users wherein one trait less critical.

Table 2. Performance statistics comparison for default and user-defined weightage

Total Users with biometric details	User count with inexact biometric traits	Multimodal Biometric Approach	Average Score	Resultant Score improvement (in % age)
40	4	With default weightage (50:50)	0.6966	26.15
40	4	With user defined weightage (80:20)	0.8787	

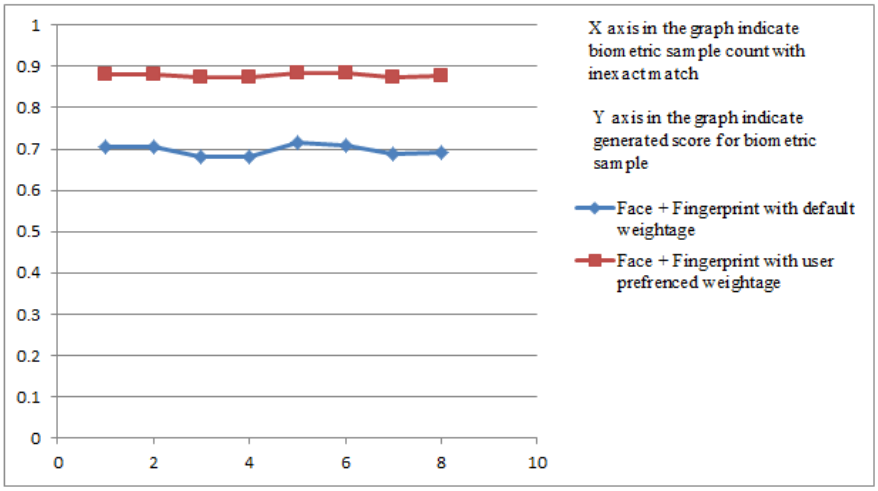

Fig. 5. Performance statistics comparison for default and user-defined weightage

Graphical representation in Fig. 6 shows comparison between unimodal, multimodal with default weightage scheme for traits and multimodal with user preference weightage scheme indicates uniform improvement. User database size of 40 users in which 4 users were identified who provided inexact biometric traits during testing.

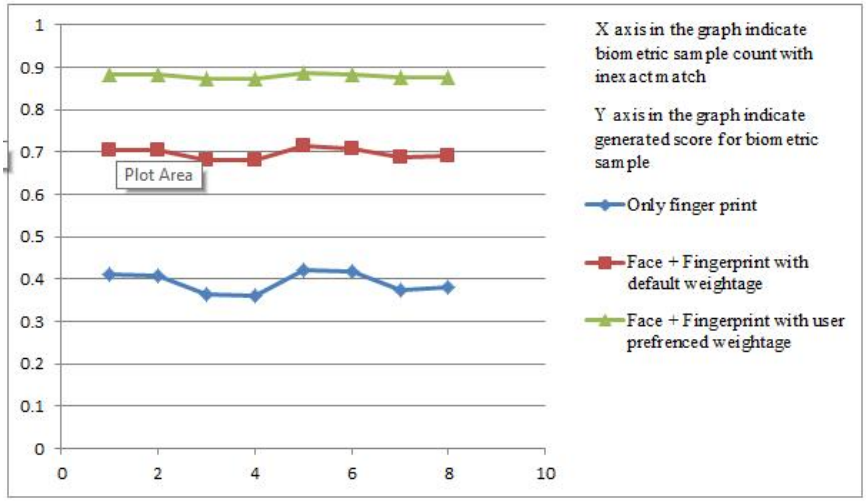

Fig. 6. Performance Comparison for unimodal, default weightage multimodal scheme and user-defined weightage scheme

6.3 Reporting techniques performance

Security is enhanced by reporting techniques i.e. Email and SMS. Prompt reporting techniques ensure that end user is updated of his transactions and is always in sync with the system findings. In case of urgency, user/admin may initiate corrective actions on priority. Below are the performance traits of reporting techniques.

Table 3 shows performance metrics for reporting used i.e. the turnaround time for both approaches in which they are able to reach the end user. As per the performance observed for the test set of 200 SMS and Email sent to the end user and administrator, email is identified as a technique with the lower delivery time. Both SMS and Email show a delivery rate of more than 90 % within a time period of 1 minute. This duration is calculated from time when reporting request is triggered from the server.

Table 3. Performance statistics for reporting techniques

Reporting technique	Message sent count	Delivered within 30 seconds	Delivered within 1 minute	Delivered within 3 minutes
Email	200	65%	97%	100%
SMS	200	21%	92%	99%
PS : Delay in communication is observed due to network glitches				

Graphical representation shown in Fig. 7 shows that majority of SMS and Email need delivery time of more than 30 secs from the time when the request from server is sent. Also, Email is seen as a higher performing technique out of the two.

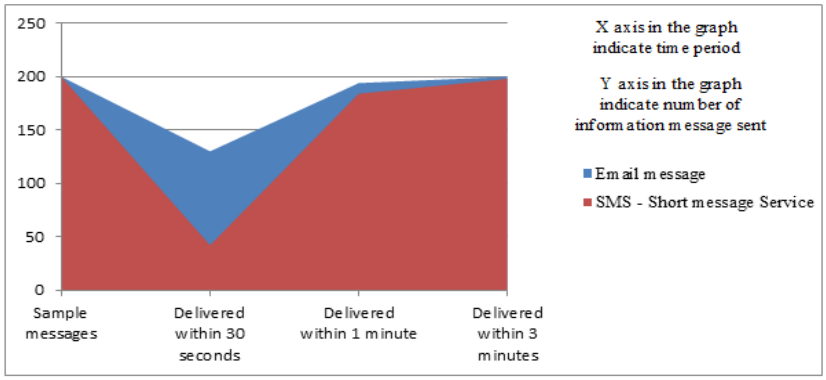

Fig. 7. Performance comparison for reporting techniques

6.4 FRR and FAR results

Damages in FAR scenario are substantially controlled by strong intimation layout of the system. End user can immediately take proactive action against the wrong access once intimated on his contact points.

FRR is found as minimized by the user referenced weighted multimodal scheme and OTP approach used here. This was validated on a user database of 40 users and 80 finger print samples.8 cases were observed wherein system could not exactly identify the end user's finger print and face image sample. In previous scenario these cases are rejected owing to inaccurate results. But in the used approach, end user will be shared with an OTP when normalized results are inaccurate or inexact in totality.

OTP is used for system login as a fallback approach and FRR is found reduced. Results show improvement in user identification by the system. Table 4 Shows performance statistics for the FRR received in multimodal and multimodal with OTP scheme.

Table 4. Performance statistics for multimodal approach with and without OTP

Total Users	Total Finger prints	Total Face images	Multimodal Approach	Users with inexact match	FRR
40	80	400	Multimodal Validation (Finger print + Face image)	4 users	10%
40	80	400	Multimodal Validation (Finger print + Face image) + OTP	3 users validate OTP successfully, 1 user provides invalid OTP	2.5%

Cases in which FRR can be observed is due to factors such as late OTP delivery, usage of expired OTP, usage of invalid OTP, wrong input of generated OTP by the end user.

Graphical representation shown in Fig. 8 indicates an performance improvement in FRR of approximately 7.5 % in multimodal with OTP scheme in comparison to the normal multimodal approach.

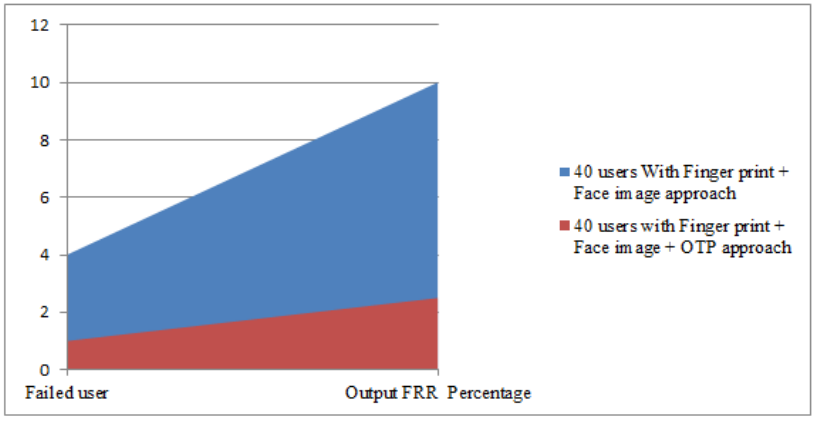

Fig. 8. Performance comparison multimodal approach with and without OTP

7 Conclusion

This paper identifies that multimodal biometrics is a better identity authentication technique in comparison to the unimodal identity authentication technique. This is supplemented by results wherein multimodal approach has shown improvement of around 77 % over unimodal approach for FRR scenarios. In addition to this, user defined weightage scheme is added to the normal multimodal computation algorithm to further improve FRR scenarios by approximately 26 %. User defined weightage is highly beneficial when one of the traits needs to be compromised due to user's biometric pattern. This FRR percentage is further lowered by inducing in OTP scheme in the existing algorithm to shows improvements by approximately 7 %. FAR is controlled by immediate intimation to the end user so that proactive action is taken to avoid damages.

All these results help in making it clear that isolated system causes degradation in performance and results. These problems can be at the user end or the system but it results in lowering the customer satisfaction index (CSI) which is expected to be ever improving. This research effort has retrieved positive results by enabling system as a flexible product which is ready to accommodate user's biometric needs. Also, system can seek help from end user in case of marginal results. By this system will re-bounce itself to clarity for personnel identification. Besides all this, security of the system is increased by knowing the transaction status through reporting techniques and immediate action initiation in case of any concern.

Therefore, paper concludes by determining the fact that if system and user are kept in a single cluster of knowledge in which they constantly share situations, expectations and results with each other, they can add value to each other's decision making and requirement realization.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Jain, Anil K, Arun Ross, Salil Prabhakar. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology. 2004;14(1):4-20.

[2] Jain A, Bolle R, Pankanti S, Eds. Biometrics: Personal identification in networked society. Springer Science & Business Media. 2006;479.

[3] Sarhan Shahenda, Shaaban Alhassan, Samir Elmougy. Multimodal biometric systems: A Comparative study. Arabian Journal for Science and Engineering. 2016;1-15.

[4] Taouche, Chérif, et al. Multimodal biometric systems. Multimedia Computing and Systems (ICMCS), 2014 International Conference on. IEEE; 2014.

[5] Jain AK, Ross A, Pankanti S. Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security. 2006;1(2):125-143.

[6] Flynn PJ, Jain AK, Ross AA, eds. Handbook of biometrics. Springer; 2008.

[7] Hong L, Jain A. Integrating faces and fingerprints for personal identification. IEEE Transactions on Pattern Analysis and Machine Intelligence. 1998;20(12):1295-1307.

[8] Ross A, Jain AK. September. Multimodal biometrics: An overview. In Signal Processing Conference, 2004 12th European. IEEE. 2004;1221-1224.

[9] Besbes Feten, Hanene Trichili, Basel Solaiman. Multimodal biometric system based on fingerprint identification and iris recognition. Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on. IEEE; 2008.

[10] Snelick R, Uludag U, Mink A, Indovina M, Jain A. Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2005;27(3):450-455.

[11] Ross A, Jain A. Information fusion in biometrics. Pattern Recognition Letters. 2003;24(13):2115-2125.

[12] Grover Jyotsana, Madasu Hanmandlu. Hybrid fusion of score level and adaptive fuzzy decision level fusions for the finger-knuckle-print based authentication. Applied Soft Computing. 2015;31:1-13.

[13] Bharadi, Vinayak Ashok, Bhavesh Pandya, Mr. Bhushan Nemade. Multimodal biometric recognition using iris & fingerprint. IEEE International Conference-Confluence 2014 IEEE Conference Record. No. 33936.

[14] Yang Fan, Baofeng Ma. A new mixed-mode biometrics information fusion based-on fingerprint, hand-geometry and palm-print. Image and Graphics, 2007. ICIG 2007. Fourth International Conference on. IEEE; 2007.

[15] Jain AK, Ross A. Learning user-specific parameters in a multibiometric system. In Image Processing. 2002. Proceedings. 2002 International Conference on. IEEE. 2002;1:I-57.

[16] Dlamini, Mloses T, Jan HP Eloff, Mariki M. Eloff. Information security: The moving target. Computers & Security. 2009;28(3):189-198.

[17] Jain Anil, Karthik Nandakumar, Arun Ross. Score normalization in multimodal biometric systems. Pattern recognition. 2005;38(12):2270-2285.

[18] Parmar H, Nainan N, Thaseen S. Generation of secure one-time password based on image Authentication. Computer Science & Information Technology. 2012;195206.

[19] Yinxiang Li, et al. Research on the S/KEY one-time password authentication system and its application in banking and financial systems. Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on. IEEE; 2010.

[20] Lakshmiprabha NS, Bhattacharya J, Majumder S. Face recognition using multimodal biometric features. Image Information Processing (ICIIP), 2011 International Conference on. IEEE; 2011.

[21] Olsen, Martin Aastrup, Vladimír Šmida, Christoph Busch. Finger image quality ssessment features–definitions and evaluation. IET Biometrics. 2016;5(2):47-64.

[22] Ballard, Michael J, Swainfand Dana H, Swain M. Indexing via color histograms. IEEE Transactions on Image Processing, Pág. 1990;390-393.

[23] Javed, Muhammad Younus, Usman Qayyum. Face recognition using processed histogram and Phase-only Correlation (POC). Emerging Technologies, 2007. ICET 2007. International Conference on. IEEE; 2007.

[24] Kumar Amioy, Ajay Kumar. Adaptive management of multimodal biometrics fusion using ant colony optimization. Information Fusion. 2016;32:49-63.

[25] Vasuhi S, Vaidehi V, Babu NN, Treesa TM. December. An efficient multi-modal biometric person authentication system using fuzzy logic. In ICoAC 2010. IEEE. 2010;74-81.

[26] Abdolahi M, Mohamadi M, Jafari M. Multimodal biometric system fusion using fingerprint and iris with fuzzy logic. International Journal of Soft Computing and Engineering. 2013;2(6):504-510.

[27] Anekar, Binay R, Vishal J. Online banking security system using OTP encoded in QR-code. International Journal of Advanced Research in Computer Science and Software Engineering. 2015;5(3).
ISSN: 2277 128X.

[28] Liao I-En, Cheng-Chi Lee, Min-Shiang Hwang. A password authentication scheme over insecure networks. Journal of Computer and System Sciences. 2006;72(4):727-740.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://www.sciencedomain.org/review-history/27567