Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 8. No. 2, 2020

Article Citation Format
Aranuwa, F.O. (2020):
Efficient Multimodal Biometric Authentication System based on Multilevel Decision Threshold
. Journal of Digital Innovations & Contemp Res. In Science., Engineering & Technology. Vol. 8, No. 2. Pp 49-58

Article Progress Time Stamps

Article Type: Research Article
Manuscript Received: 30th March , 2020
Review Type: Blind
Final Acceptance: 11th June, 2020

Efficient Multimodal Biometric Authentication System Based on Multilevel Decision Threshold

Aranuwa, F.O.
Department of Computer Science
Adekunle Ajasin University,
Akungba – Akoko, Ondo State, Nigeria
E-mail; felix.aranuwa@aaua.edu.ng
Phone: +2347031341911

ABSTRACT

The quest for efficient and reliable user authentication techniques motivated this research work. Undoubtedly, biometric technology has become a foundation of an extensive array of secured identification and personal verification solutions across the world. In fact, the technology has been widely adopted in the work environments and critical industry infrastructures for surveillance, forensic investigation and access control. However, parallel evolution of the biometric identification management market has identified that the use of single modality for identification purposes may no longer be an intelligent choice for many applications, as a result of their susceptibility to changes in individual biometric features and presentation attacks. Hence, the need for a biometric system with much higher accuracy and reliability, which is believed can be achieved by integrating the evidences from multiple biometric traits or sources in a single application. Meanwhile, researchers at different levels has proposed and combined the evidences from different sources or traits, but the time and computational complexities of combining these evidences in many applications remains an overt concept that call for an improvement. Therefore, in this research work, a multilevel decision threshold authentication mechanism with an intelligent fusion technique is presented. The level-based strategy deployed allows fusion and authentication at different levels systematically. The output of the system prototype developed to test the performance of the multilevel decision structure showed a good upshot in terms of reduction in computational intricacies and verification time. The performance of the system stands at (92%) AAR with FAR and FRR of (1.2%):(2%) and (2.5):(5.0) for fingerprint and face respectively.

Keywords: Multilevel, Authentication, Unimodal biometric, Multimodal biometrics, Computational complexity, Performance metrics

1. INTRODUCTION

The human body has this privilege of possessing features that are unique and exclusive to each individual. This exclusivity and unique characteristic has led to the field of biometrics and its application in ensuring security in various fields. Top benefits of biometric technology are authentication, data discretion, access control, accuracy and non-repudiation. The term biometrics can be referred to as body measurements and calculations related to human characteristics (Kaspersky, 2020).

According to Stanley, Jeberson, and Klinsega (2009) biometrics is described as the most secured and convenient authentication tool that cannot be stolen, forgotten, borrowed or forged. Their study identified a number of features that make biometrics a reliable authentication tool. These include: universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention.

Typical examples of biometric characteristics or traits are depicted in Figure 1. Any of the biometric traits can be used in an authentication or identification system depending on the application scenario.

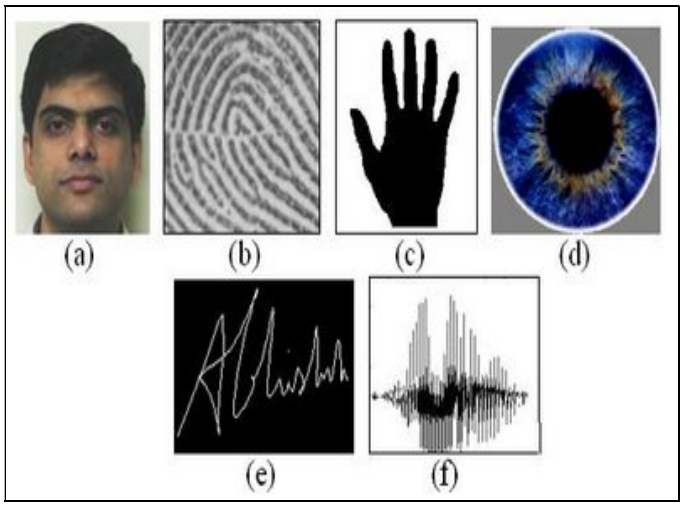

Figure 1. Typical Examples of biometric characteristics: (a) face, (b) fingerprint, (c) hand geometry, (d) iris, (e) signature, and (f) voice (Jain,2008a).

According to Ross and Jain, (2006), when a single trait is used in an application it is called unimodal biometric, while combination of two or more traits in an application is referred to as multimodal biometrics. However, studies have revealed that Unimodal biometric systems have limited effectiveness due to their susceptibility to changes in individual biometric features and presentation attacks, (Choras, 2019; Aranuwa, 2020). The latter paradigm offers a greater recognition efficiency and considerable improvements in reliability with reasonable overall performance in many applications. However, the issue of efficient and effective integration of the evidences obtained from different traits remains an obvious concept that attracts research attention. Hence, this work presents a classical multilevel decision threshold authentication mechanism for efficient multimodal biometric system that can overcome the challenges of the conventional methodologies.

According to Hermosillo et al, (2002), the problem of establishing fusion and correspondences between two or more images is fundamental in computer vision. It is one of the building blocks for a number of challenging problems. For images acquired through similar sensors, they can be realigned by a direct comparison or sum of their intensities. This results in matching algorithms that essentially look for the geometric transformation between the two images which minimizes the sum of the squared differences between their intensity values. In the case of images acquired from different traits as we have in multimodal biometrics system, realignment of the invariance of the intensity may not be valid and suitable. However, to cope with the challenges, acquisition of modalities must be realigned separately to allow for an accurate fusion of complementary information and decision making processes for efficiency of the system.

2. LITERATURE REVIEW

2.1 Overview of Multimodal Biometrics

As the technology world evolves, challenges to implement secure personal identification protocols with biometric technology are increasing and the need for accurate human identification is higher than ever in many authentication and security application across the world. Additionally, parallel evolution of the biometric identification management market has identified that the use of single modality for identification purposes may no longer be an intelligent choice for many applications in the industries (Shahnewaz, 2020).

According to Choras (2019), single modality biometric systems has been displaying limited effectiveness in identifying people, due to their susceptibility to changes in individual biometric features and presentation attacks. Hence, the identification of people using multimodal biometric systems attracts the attention of researchers due to the advantages it offers, such as greater recognition efficiency and security compared to the unimodal biometric system. Other benefits offered include:

Accuracy*:* It is more accurate than any single biometric trait and offers high level of convenience at the same time.
Fraud resistance*:* In multimodal biometrics, it is very difficult for an imposter to spoof or attack multiple traits of genuine user simultaneously or at the same time in any application, (Sanjekar and Patil, 2013).
Flexibility and User acceptance*:* It is flexible with higher user acceptance, as users are given more than one choice. If one trait changes or is obscured, may be as a result of a medical mask or subsystem failure, the other traits compensate.

By definition, Multi-modal biometrics are systems that are capable of combining more than one physiological or behavioral characteristic in a single application. It could takes input from single or multiple biometric devices for measurement or input from two or more different biometric characteristics. Figure 2 depicts multimodal biometrics scenarios.

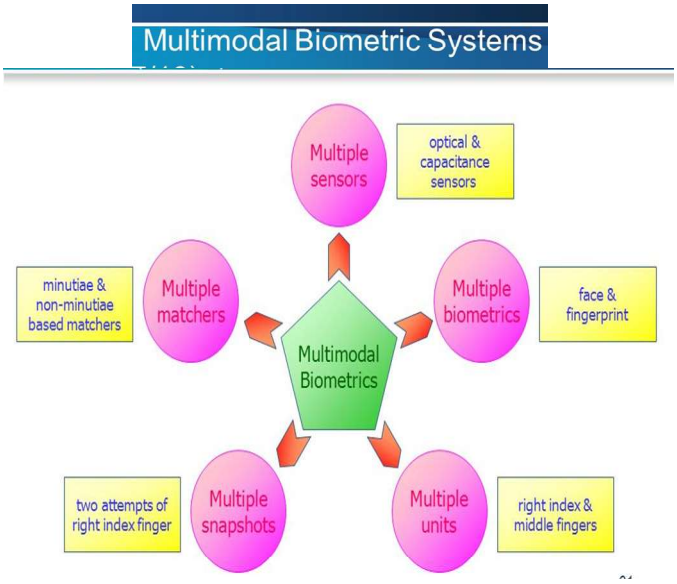

Figure 2. Multimodal Biometrics Scenarios

2.2 Information Fusion Methodologies in Multimodal Biometrics System

According to Aranuwa (2020), since the new paradigm are designed to use more than one source or trait of biometric characteristics, the fusion methodology that will effectively and efficiently consolidate the evidences must be intelligent. Meanwhile, different fusion techniques such as rule based, statistical methods and machine learning algorithms has been proposed and used for biometric information fusion at different levels, e.g, sensor level, feature level, match score level, rank level and decision level (Benaliouche and Touahria, 2014). However, the top four of these fusion methodologies were comparatively presented based on their pragmatic characteristics, robustness and reliability in Aranuwa (2020).

Earliest efforts in combining multiple biometrics for person recognition or authentication can be traced back to mid-nineties (Brunelli and Falavigna, 1995; Bigun et al., 1997a; Hong and Jain 1998; Kitler et al., 1998; Ben-Yacoub, 1999). In all these works, the common practice was to combine biometric evidences at the score level with the conventional techniques. Matching at score level is also known as fusion at the measurement level or confidence level. At this level the biometric matchers output a set of possible matches along with the quality of each match (matching score) and it is relatively easy to access and combine the scores generated by these different matchers. Figure 3 illustrates different levels of data fusion possibilities. With respect to biometric authentication, two early theoretical frameworks for combining different machine experts are described by Bigun et al, (1997) and Kitler et al, (1998), the former from a risk analysis perspective (Bigun, 1995), and the later from statistical pattern recognition point of view (Duda et al, 2001). Both of them concluded under some mild conditions that may not hold in practice, that weighted average of all the different opinions provided by the systems in the form of similarity scores is a good way of conciliating these evidences from different sources. The approach certainly improves performance of multiple biometric systems but in the other way round reduces the system's throughput because of its time and computational complexity.

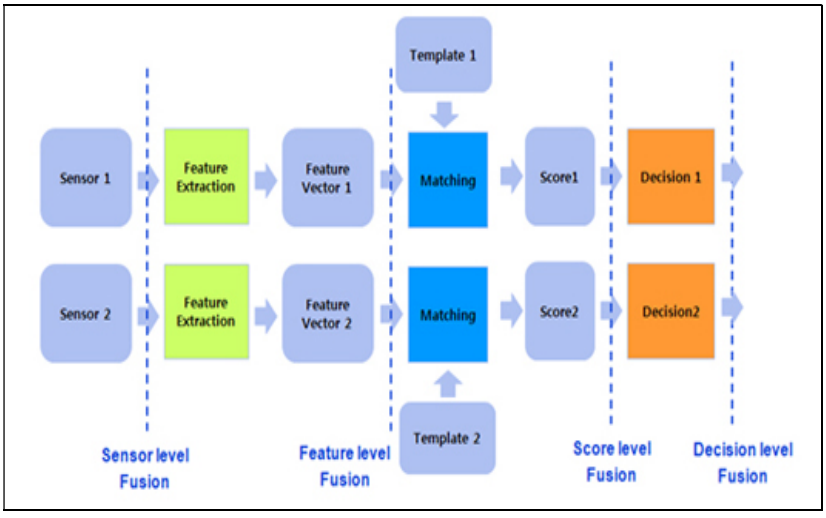

Figure 3. Levels of fusion possibilities.

3. THE ARCHITECTURE OF THE MULTILEVEL DECISION THRESHOLD AUTHENTICATION SYSTEM – (MDTAS)

This architecture of the system – (MDTAS) is composed of four major stages as shown in Figure 4. The first stage is the acquisition of the data pertaining to the two traits proposed in this work, employing applicable sensors and feature vectors created independently with user's details. This stage defines the human machine interface and it is pivotal to the performance of the biometric system. The feature acquired is processed and a salient feature extracted to represent underlying traits. The acquired data depending on the sensor used may be subjected to a signal enhancement algorithm in order to improve its quality. During enrolment, this feature set is stored in the database in templates form. The feature extracted from a claimed identity is compared against the stored template in the database to generate match scores. The number of matching features between the input and the template feature sets is determined, and a match score is reported appropriately.

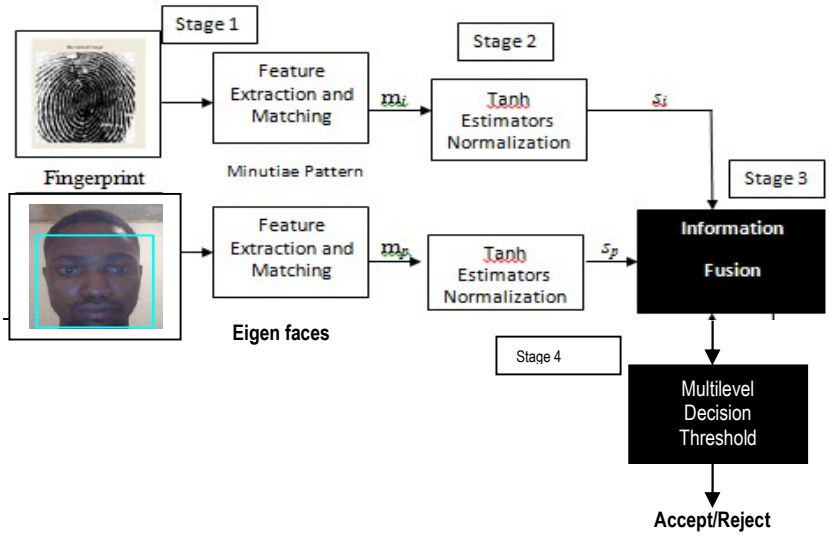

Figure 4. The structure of the Multilevel Decision Threshold Authentication System – (MDTAS)

The second stage is the normalization of feature sets, which is achieved by inbreeding a *tanh* estimator normalization algorithm.

The third stage is the deployment of the fusion techniques proposed (modified Dempster shafer rule of combination) which was achieved by inbreeding the *tanh* estimator into the original Dempster shafer theory as presented in (Aranuwa, Olabiyisi & Omidiora, 2013). Dempster–Shafer Theory (DST), is a mathematical theory of evidence that provides a useful computational scheme for combining information from multiple sources. It is a powerful tool for combining accumulative evidences and changing priors in the presence of new evidences (Brest, 2010). The fourth stage is the computation of multi-level decision threshold for final decision of authentication.

The mass of each evidence or classifier is combined recursively using the equation stated in equation 1-4:

$$m_{1,2}(C) = \sum_{A \cap B = C} \frac{m1(A)\ X\ m2(B),}{1 - K} \qquad \forall\ C \in \Omega \qquad \text{.....Equation 1}$$

Where, m_1 represent basic belief assignment (bba) of evidence A and,m_2 represent basic belief assignment (bba) of evidence B, while Ω represent the belief function and K is defined as,

$$\sum_{A \cap B = \theta} m1(A), X\, m2(B)$$

……..Equation 2

Specifically, the combination (called the joint $m_{1,2}$) is calculated from the aggregation of two bba's m_1 and m_2. A and B are used for computing new belief function for the focal element C. The mass final is represented as:

$$mfinal = (m1) + (m2)$$

……..Equation 3

Where $(+)$ shows the rule of combination and final result is obtained by applying the threshold t to *mfinal*. The upshot is expressed as follows:

$$\text{Result} = \begin{cases} \text{Accept, if } mfinal \geq t_1 \text{ OR } t_2 \text{ OR } t_3 \\ \text{Otherwise Reject,} \end{cases}$$

.....Equation 4

where t_1 = threshold value for fingerprint, t_2 = threshold value for face and, t_3 = threshold value for fingerprint + face. With this approach, the problem of time and computational complexity is considerably circumvented.

A prototype to test the mechanism was developed. The result from the trial came up with good upshot in terms of good acceptance rate, accuracy, reduced computational intricacy and time taken during verification.

Figure 5, Figure 6, Figure 7 and Figure 8 show the interfaces of the logon page, main menu, enrolment and verification page for both fingerprint and face respectively.

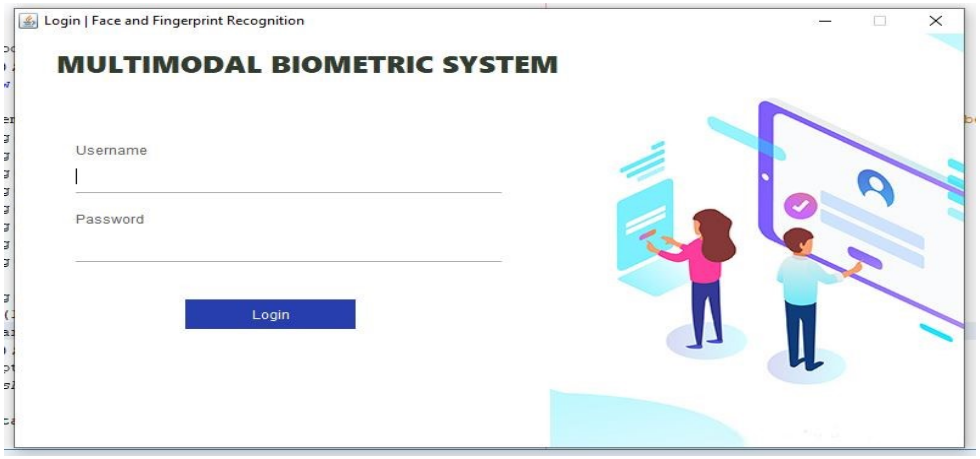

Figure 5: Log in Page

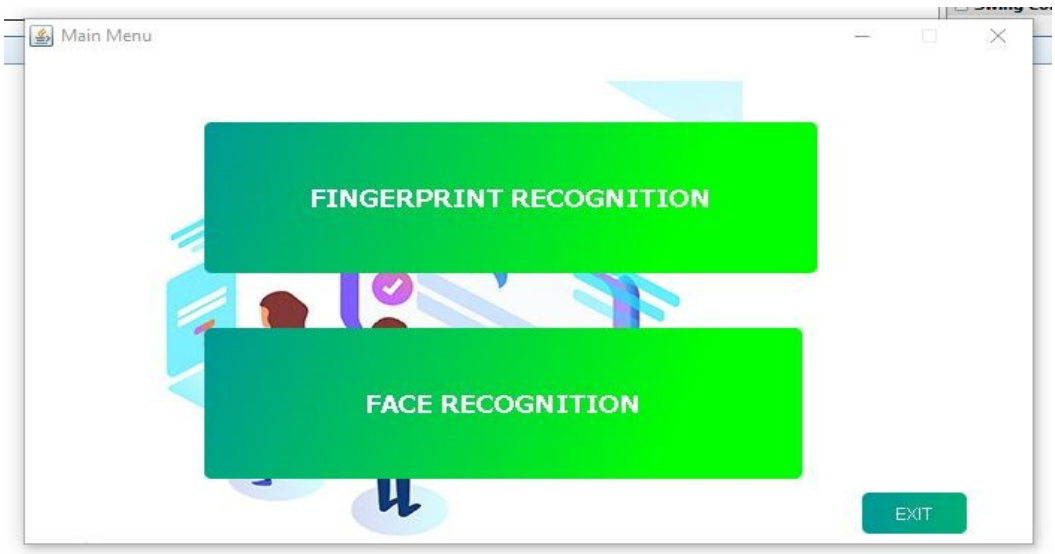

Figure 6: Main Menu Page

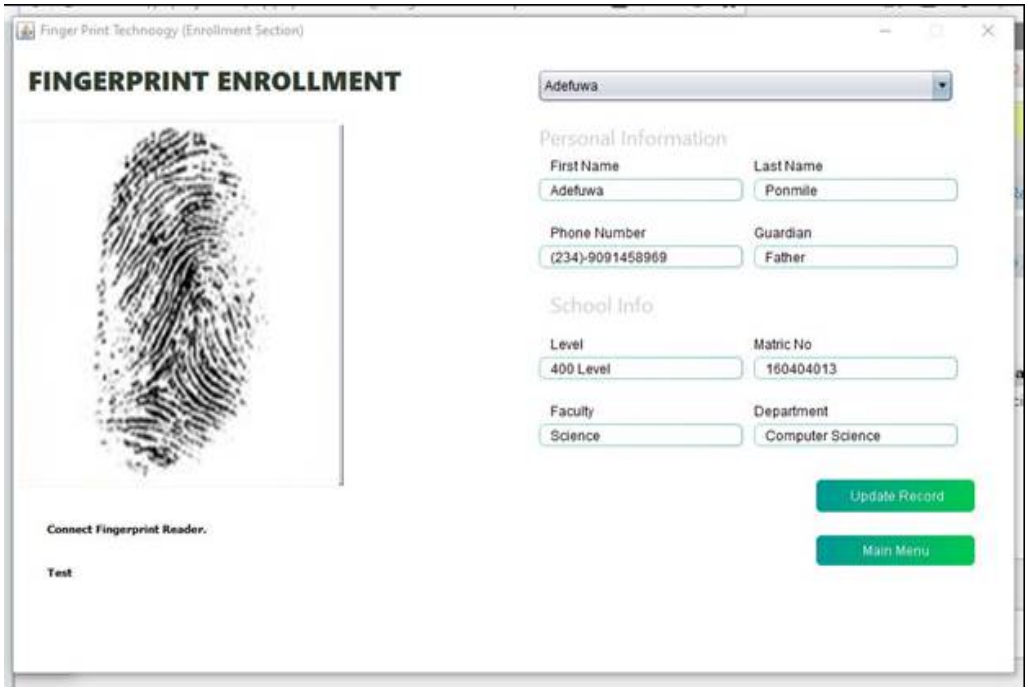

Figure 7: Fingerprint Enrolment Page

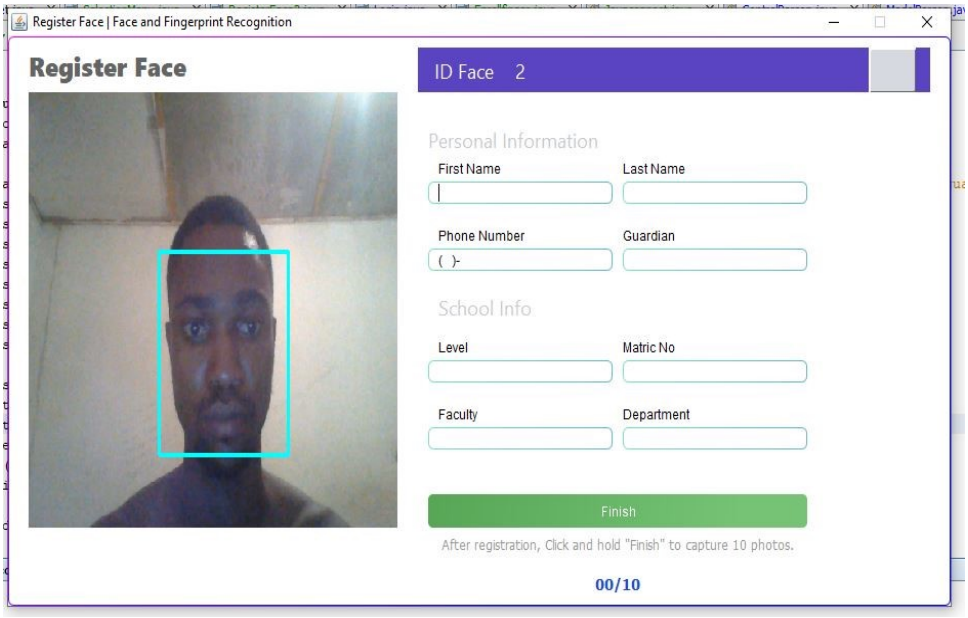

Figure 8: Face Registration Page

Table 1: Showing The Sample Data Acquired

Identity	Fingerprint m1	Face m2
P1	10.04	80.7
P2	14.01	88.5
P3	16.05	79.6
P4	13.03	81.5
P5	18.02	85.6

3.1 Performance Metrics for Reliable Biometric System

Generally, an important issue for the adoption of biometric technologies is to establish the performance of individual biometric modalities and overall systems in a credible and objective way. One performance parameter is the measure of the errors in biometric system which is usually tested in terms of false acceptance rate (FAR), false rejection rate (FRR), failure to enroll rate (FER), during enrollment and verification. False Acceptance Rate (FAR) is defined as the ratio of impostors that were falsely accepted over the total number of impostors tested described as a percentage. (i.e FAR = Number of accepted imposter claims / Total number of imposter accesses x 100%). This indicates the likelihood that an impostor may be falsely accepted and this must be minimized in high-security applications. False Reject Rate (FRR) is defined as the ratio of genuine clients that are falsely rejected to the total number of genuine clients tested described as a percentage. (i.e FRR = Number of rejected genuine claims / Total number of genuine accesses x 100%).

This indicates the probability that a valid user may be rejected by the system. Ideally this should also be minimized especially when the user community may be put-off from using the system if they are wrongly denied access. In this type of application, a number of 'clients' may be enrolled onto the system, both genuine and impostor. The impostor may be someone who is not enrolled at all or someone who tries to claim the identity of someone else either intentionally or otherwise. When being verified the genuine clients should be recognized and impostors should be rejected.

In order to estimate FAR and FRR, a set of genuine and impostor matching scores have to be generated. The decision to accept or reject is based on a pre-defined threshold. If the distance is less than this threshold then we can accept the sample. A unique measure however, can be obtained by combining these two errors into the Total Error Rate (TER) or Total Success Rate (TSR) where:
TER = FAR + FRR / Total number of accesses x 100 and,
TSR = 1 – TER.

Another important performance parameter is the verification time, which is defined as the average time taken for the verification process. This may include the time taken to present the live sample. The actual verification time will critically depend on user training, operating environment and psychological conditions.

4. CONCLUSSION

The set objective for this work was focused at presenting an efficient multimodal biometrics authentication system based on multilevel decision threshold, which has been achieved. The mechanism engaged the modified Dempster shafer rule of combination, an intelligent integration technique suitable to overcome the challenges associated with computational complexity and high verification time in the conventional methodologies. The results from the system prototype developed to test the efficiency of the mechanism showed that the mechanism suitably showed an improvement in terms of efficiency and accuracy, reduction in computational intricacies and verification time. The performance of the system stands at (92%) Actual Acceptance Rate (AAR) with FAR and FRR of (1.2%):(2%) and (2.5):(5.0) for fingerprint and face respectively. This will in no small measure contributes to the general improvement and efficiency of the biometric systems as a whole. However, the work can be improved upon in several ways, especially for the case of multiple classes. The researcher in future work will consider full implementation of the proposed meachenism with larger database, different traits and fusion at different levels.

REFERENCES

1. Aranuwa, F.O (2020). Information Fusion Schemes for Reliable Biometric System. American Journal of Biometrics and Biostatistics (AJBB) 4(1): 001-005. USA. Available at: https://www.scireslit.com/Biometrics/AJBB-ID18.pdf
2. Aranuwa, F.O., Olabiyisi, S.O. & Omidiora, E.O (2013): "An Intelligent Classifier Fusion Technique for Improved Multimodal Biometric Authentication using Modified Dempster-Shafer Rule of Combination". Computing, Information Systems and Development Informatics (CISDI) Journal). Baton rouge, USA, Volume 4: No 1, March, 2013 pg 1-8. ISBN 978-2257-44-7, ISSN 2167-1710. Available online at: http://www.cisdijournal.net.
3. Benaliouche, H and Touahria, M (2014). Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint. Hindawi Publishing Corporation. The Scientific World Journal Volume 2014, Article ID 829369, pg 1-13 http://dx.doi.org/10.1155/2014/829369
4. Ben-Yacoub S.B, (1999). "Multi-modal Data Fusion for Person Authentication using SVM". Proceedings of the second International Conference on Audio and Video-based Biometric Person Authentication (AVBPA'99) pp.25-30.
5. Brest B. (2010): Workshop on Theory of Belief Functions (http:/bafas.iutlan.univrennes1.fr/belief2010/) (Brest, 1 April 2010).
6. Brunelli, R. and Falavigna, D. (1995), "Personal Identification Using Multiple Cues". IEEE Trans. on Pattern Analysis and Machine Intelligence 17(10), 955-966.
7. Bigun, E., Bigun, J., Duc, B. and Fisher, S. (1997), "Expert conciliation for multi modal person authentication systems by Bayesian statistics". Proceedings of the first International Conference on Audio and Video-based Biometric Person Authentication 327–334.
8. Choras, R. S (2019). Multimodal Biometrics for Person Authentication DOI: http://dx.doi.org/10.5772/intechopen.85003. Book Chapter pg 1-17
9. Duda, R. O. and Hart, P. E. (2001), "Pattern Classification and Scene Analysis. New York: John Wiley & Sons Hermosillo, G, Chefd'hotel, C and Faugeras.O (2002). Variational Methods for Multimodal Image MatchingInternational Journal of Computer Vision 50(3), 329–343.
10. Hong, L, and Jain,A. K (1998). "Integrating faces and fingerprints for personal Identification," IEEE Transactions on PAMI, vol. 20, pp. 1295–1307, Dec 1998.
11. Jain, A. K. (2008a), Microsoft ® Encarta ® 2008 ©, 1993-2007-Microsoft Corporation.
12. Kaspersky A.O (2020). What is Biometrics Security? How It Works. Kaspersky Lab: Retrieved 5/10/2020. https://www.kaspersky.com/resource-center/definitions/biometrics
13. Kittler, J., Hatef, M., Duin, R. P. W. and Matas, J. (1998), "On combining classifiers". IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(3): 226–239.
14. Ross, A. and Jain, A.K. (2006): "Multimodal Biometrics: An Overview", Proceedings of 12th European Signal Processing Conference (EUSIPCO), (Viena Austra), pp.1221-1224, Sept., 2006.
15. Stanley, P., Jeberson, W., and Klinsega V.V. 2009. Biometric Authentication: A Trustworthy Technology for Improved Authentication. 2009 International Conference on Future Networks, , pp. 171-175.
16. Shahnewaz , S (2020). The Advantages of Multimodal Biometric Systems for Human Identification. Retrieved from M2Sys Blog on 8/10/2020. https://www.m2sys.com/blog/
17. Sanjekar, P. S. and Patil, J. B (2013). An Overview of Multimodal Biometrics Signal and Image Processing: An International Journal (SIPIJ) Vol.4, No.1, February 2013 DOI: 10.5121/sipij.2013.4105 57.