ISSN 2278-3091

Volume 10, No.3, May - June 2021

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse471032021.pdf

https://doi.org/10.30534/ijatcse/2021/471032021

# Multi-Modal Biometrics Systems: Concepts, Strengths, Challenges and Solutions

**Achimba Terfa[1], Alaaga James[2], Kwaghbee Sever[3]**

[1]Department of Mathematics and Computer Science, University of Mkar, Benue State, Nigeria, terfaachimba@gmail.com
[2]National Agency for Food and Drug Administration (NAFDAC), Abuja, Nigeria, jimonline4u@gmail.com
[3]Department of Mathematics and Computer Science, University of Mkar, Benue State, Nigeria, kwaghbees@gmail.com

## ABSTRACT

Authentication is a very important aspect of computer security. Most systems employ strategies such as Password-based authentication, Multi-factor authentication, Certificate based authentication which are accompanied with a lot of challenges. To address this issue, most security systems have introduced the use of biometrics for authentication. Unimodal biometrics systems have many limitations regarding performance and accuracy. The use of Multimodal biometrics systems for authentication is recently attracting the attention of researchers due to its capacity to overcome most of the drawbacks of Unimodal biometric systems. This paper focuses on the use of biometric technology for authentication. The strengths of multimodal biometric systems, together with the challenges of multimodal biometric systems are presented. The paper also suggests solutions to the challenges of multimodal biometric systems.

**Key words**: Authentication, Biometrics, Multi-modal, Security.

## 1. INTRODUCTION

Information Technology has no doubt created a platform for connectivity and increased a lot of activities in different areas (sectors) such as governance, politics, business, education, banking, e-commerce and social interaction. The spread of Information Technology has also been accompanied with security challenges such as unauthorized access. So the need for adequate security cannot be over-emphasized. User authentication, which can be used to provide security, has been in growing demand. Authentication can be defined as a technique used by a computer in verifying the identity of individuals who want to have access to that systems' resources [1].

It is a method that prevents unauthorized users from accessing sensitive information. It is used to provide access control to systems such as Automated Teller Machines, National Identity Management, Credit Card and Smart Security, Border Crossing, Fund Transfers etc. Most authentication systems focus on the use of Password- based authentication, multi-factor authentication, certificate based authentication. These methods have their limitations which include loss, forgetfulness, false security, brute force attacks and other attacks by fraudsters. Authentication systems that use passwords and PINs cannot prevent situations where a person has more than one identity.

The use of biometric technology is one of the most appropriate strategies that provide solutions to these limitations. Biometrics can be defined as human characteristics and trait related metrics [2]. Biometrics technology involves the use of physical, behavioral and physiological characteristics of individuals as a means of identification and verification [3].The behavioral or physiological features can be used as a biometric verifier as long as it satisfies the following criteria: Universality, Distinctiveness, Permanence, Collectability, Performance, Acceptability and Resistance to circumvention [2, 4]. Universality means every person must have the characteristics, distinctiveness implies that no two persons should possess the same characteristics. Permanence means that the characteristics must be invariant for a time period as long as possible; Collectability indicates that the characteristics must be quantitatively measured with ease; Performance refers to the accuracy of which the identification and verification is achieved under different working and environmental conditions. Acceptability indicates the degree to which users are willing to accept the given characteristics; Resistance to circumvention indicates how difficult it is to defraud a system based on these characteristics. Physiological features are the physical characteristics of an individual which includes faces, fingerprints, palm prints, hand geometry, deoxyribonucleic acid (DNA), retina, iris, odor, ear and veins. Behavioral characteristics are related to the pattern of behavior specific to a person. These include signature, speech, gait, lip movement, typing styles (dynamics of typing).Behavioral characteristics analyze the way users interact with a computerized system. Most of these behavioral and physiological features are discussed in detail by [2] and [4].

The traditional methods of authentication which involves the use of passwords, PINs and Keys can prevent situations where more users use the same identity, but cannot prevent multiple enrollment i.e. situations where a person has more than one identity. Using biometric technology for authentication will deal with this situation and many other limitations previously mentioned. The use of biometric systems can be appreciated due to factors like speed, precision, ease of use and costs. Biometric authentication requires comparing a registered or enrolled biometric sample against newly biometric sample. During Enrollment, a sample of biometric trait is captured, processed by a computer and stored for later comparison. Biometric recognition can be used for identification where a person is identified from an enrolled population by searching a database for a match. It can also be used for verification where the system authenticates a person's claimed identity [4].

Biometrics systems have been divided into two categories, which are: Unimodal and Multimodal biometric systems [1]. Unimodal biometric systems use only one trait of an individual for identification and verification while Multimodal biometric systems use more than one biometric modality for identification and verification.

This research focuses on multimodal biometric systems because of its ability to provide increased level of security. The strengths, challenges of Multimodal biometric systems and proposed solutions to these challenges are presented.

## 2. APPLICATIONS OF BIOMETRIC SYSTEMS

Biometrics are used in forensic applications such as criminal identification and prison security [5]. They can also be used in Surveillance systems where criminals and suspects are identified. The use of biometrics systems for surveillance also helps to prevent and discourage unlawful behavior in gatherings. It is used to find out the undesirable behavior of a group of individuals.

Biometric Technology can be used for Logical Access Control where Biometric characteristics are used for gaining access to a computer network in a workplace or a remote connection from a distance.

It can be used in Time and Attendance based applications where we can keep track of hours employees have worked. This can help in dealing with the issue of ghost workers.

Banking and Finance sectors use biometrics for authentication [1,6].Biometrics systems are used to secure medical records. Biometrics recognition systems are used in many areas such as passport verification, airports, buildings, mobile phones, identity cards [9].

## 3. UNIMODAL BIOMETRIC SYSTEMS

A Unimodal biometric system is a system that uses a single source of biometric information to perform authentication. Its mode of operation involves acquisition of biometric data from individuals, performing feature extraction on such data, comparison of extracted features against the template in the database and then making decisions [7, 8].The feature set extracted from the acquired biometric data is compared against stored templates in database and a matching score is generated. Using this score, the decision making module either confirms or denies a person's claimed identity. Unimodal biometric systems are often affected by the following limitations [2,3,4,7,8,9,10,11,12,13].

**a. Noisy Data:** These are noisy signals captured from sensors as a result of imperfect conditions (dirt, humidity, dust etc) and also incorrect usage of the sensors. Noisy data reduces accuracy of the biometric system and can lead to false rejection.

**b. Non- universality:** Some individuals may not be able to provide a given modality for recognition due to illness or a disability.

**c. Intra-class variation:** This is a situation where the biometric data acquired from an individual during verification is not identical to the data that was used for generating the individuals' template. This increases the false Rejection Rate (FRR).

**d. Lack of individuality:** Identical biometric features as may be observed form faces of identical twins, mother and daughter, father and son etc.

**e. Non- invariant representation:** An intra-class variation that arises from varied interactions with the sensors. This might be due to expression variations where a characteristic is repeatedly captured by a sensor or use of different sensors during enrolment and verification, changes in environmental conditions, scars in biometric trait etc [2].

**f. Inter class similarities:** Similarities between biometric features of multiple users. This increases False Acceptance Rate (FAR).

**g. Spoofing:** This is the act of forging or imitating biometric features by an imposter to circumvent a biometric system.

## 4. MULTIMODAL BIOMETRIC SYSTEMS

In addition to the limitations posed by Unimodal biometric systems, high- security applications and large–scale civilian recognition systems place accuracy necessities that can't be met by Unimodal biometric systems [14]. It is therefore necessary to move beyond biometric systems that are based on a single source of modality.

Multimodal Biometric systems are systems that utilize more than one type of biometric characteristics for authentication. A multimodal biometric system eliminates some limitations of Unimodal biometric systems, increases security and ensures confidentiality of data. Multimodal Biometric systems offer several advantages due to their high recognition efficiency and greater security as compared to the Unimodal biometric systems [7, 15, 16, 17].A multimodal biometric system, just like any general biometric system has four important modules. The Sensor Module is the module that captures biometric trait in form of raw biometric data. The Feature extraction module compares the extracted feature set with the stored templates in order to generate the matching scores while the matching module generates the matching scores by comparing the extracted feature set with the templates in the database. The Decision module then uses the matching score to determine an identity or validate a claimed identity. Figure 1 shows a view of a multimodal biometric system.

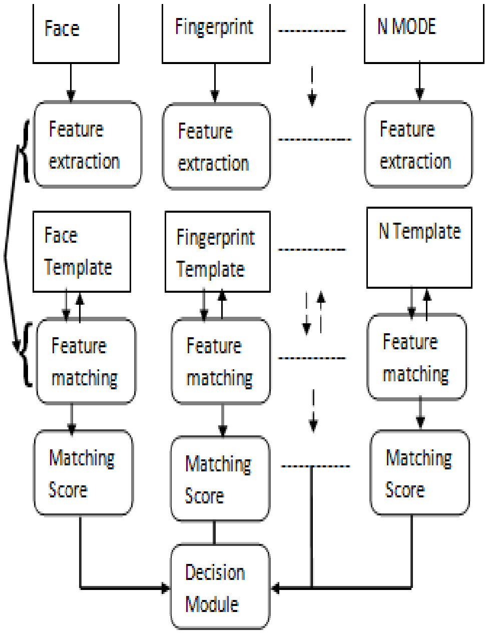

**Figure 1**: A typical Multi-modal biometric system [2].

In addition, Multimodal biometric systems have a phase called fusion. Biometric fusion is a technique that combines the classification results from each biometric channel, and this is used for decision making.

### 4.1 Fusion Levels

The process of combining the classification results of each biometric channel is known as biometric fusion [18].Fusion in Multimodal biometric systems can be done at different levels. The first is fusion prior to matching and the second is fusion after matching [6, 8, 12].

Fusion prior to matching occurs before any matching or any use of classifier. This includes Sensor Level Fusion and Feature Level Fusion. After matching fusion occurs after the mapping into matching score or decision is made. This includes Matching Score Level Fusion, Rank Level Fusion and Decision Level Fusion.

**(i)Sensor Level Fusion:** In this level, data from each sensor is combined and new data is produced. Features can be extracted from the new data that is produced. Sensor level fusion can be done only if the sources are sample of the same biometric trait that is obtained from using multiple compatible sensors or if many instances of the same biometric trait are obtained by using a single sensor [8].

**(ii)Feature level fusion:** In this level of fusion, feature vectors extracted from multiple sources of information are further integrated into a single feature vector. Some reduction techniques are needed in order to choose only useful features. The extracted features contain more useful information about the biometric data, making fusion at this level perform better than fusion at the score and decision levels [7, 8]. Feature level fusion is easy to achieve if the modalities are closely related or if it is an integration of same modality feature with multiple sensors. However, due to the complexities involved in providing a common set for different modalities, fusion at the feature level is difficult to achieve[2,8]**.**

**(iii) Match Score Level Fusion:** This is a measure of the similarity between the input biometric and the template biometric feature vectors. Individual scores generated from the matching of features with the already stored templates are combined to make a final decision. This method is also known as measurement level fusion or confidence level fusion [6]**.**

**(iv) Rank Level Fusion:** This level involves combining ranks associated with an identity and determining a new rank that would be used in establishing the final decision. This fusion level is usually applied for person identification rather than verification.

**(v)Decision Level Fusion:** In this level of fusion, separate decisions from each biometric trait are merged. This is regarded as the simplest form of fusion because only the final output of the individual modalities is combined to make a final decision.

### 4.2 Strengths of Multimodal Biometric Systems

The advantages of Multimodal biometric systems include the following: reduces False Acceptance Rate (FAR) and False Rejection Rate (FRR), achieves a certain degree of flexibility, can be seen as a fault tolerant system because it remains relevant even when one biometric character fails or is not sufficient i.e. even if someone lacks a biometric trait, the system authenticate the person using other traits. They address the issue of non- universality and also the issue of noisy data; facilitate challenge response mechanism by asking users to present random subsets of traits and also make it difficult for an imposter to spoof multiple biometric traits simultaneously[23]. Multimodal systems have multiple levels of authentication and even if a particular factor is compromised, the remaining factors will secure the system.

### 4.3 Challenges of multimodal biometric systems

Even though the use of Multimodal biometric systems is accompanied with several advantages, its implementation still faces some challenges.

Multimodal biometric systems involve the use of multiple devices to capture data and this leads to higher cost of development [19, 20].

The use of too many modalities lead to issues of low user acceptance because most people do not like passing through too many scans as this may cause inconveniences and discomforts.

Using many modalities also means that individuals have to make contact with many devices, exposing such individuals to diseases such as COVID-19, Chicken Pox e.t.c

Some multimodal biometric systems try to avoid cost and other complexities by making use of only 2 biometric modalities, but this is still susceptible to spoofing attacks.

Multimodal biometric systems also face issues of template security. Many proposed multimodal biometric systems store their biometric templates as unprotected templates in the database [19]. This is an issue of concern because physiological features are fixed and not changeable, so compromising these biometric templates lead to security threat since the templates can't be reissued.

Other challenges include difficulty in design and implementation [1], failure of sensors to show consistency, complex and unverifiable matching algorithms [2].

### 4.4 Proposed Solutions

To ensure the design and deployment of authentication systems with high level of accuracy and fewer complexities, most of the challenges facing Multimodal biometric systems need to be addressed. This will also enhance public acceptance and growth of the technology.

The issue of using multiple devices to capture biometric traits can be solved by reducing the number of devices to one. This can be achieved by designing a Multimodal biometric system that makes use of a single device to obtain biometric traits. An example will be a multimodal system that uses a single scanner to capture biometric traits like palm vein and hand geometry. Another example is a multimodal system that uses a single vision sensor to obtain facial images, periocular region and gesture videos. This will solve the problems of costs, low user acceptance, discomforts and inconveniences as users don't need to pass through too many scans. The use of one device to obtain biometric traits also makes sure that individuals need less or no contact with the devices, solving the problem of been exposed to diseases such as Covid-19, chicken pox etc.

Although it is difficult to spoof multimodal biometric systems, this is still possible since many of these systems make use of only 2 modalities. This problem can be solved by the introduction of a liveness detection technique in Multimodal biometric systems since many of these systems lack the liveness detection technique.

The issue of template security can be addressed by introducing multimodal biometric systems that will protect biometric templates using encryption techniques. Since biometric templates can't be reissued, it is necessary to introduce encryption techniques that will improve the security of biometric data and maintain high recognition accuracy. Combining encryption techniques with biometrics will provide better security [21].

The introduction of a multimodal system that uses a combination of facial images, periocular region and gesture video earlier mentioned is also of great importance in situations where the stored biometric features are exposed. Behavioral features such as gestures, unlike physiological features, can be freely changed. So even if the stored biometric traits are compromised, the users can change the behavioral features such as gestures. This can improve the process of person authentication.

It is also necessary to design specific Integrated Development Environments (IDES) for developing biometric application that would ease the work of programmers. It is believed that these IDEs will make development and research in this area to occur at a faster rate, solving the problem of difficulty in design and implementation of multimodal biometric systems [1].

## 5. CONCLUSION

This research presents the importance of using biometric characteristics for authentication. The drawbacks of Unimodal biometric systems which limit its performance and accuracy are also presented. The strengths of Multimodal biometric systems are also presented. Using Multimodal biometric systems for authentication is better as compared to Unimodal biometric systems, as it offers increased security and improved recognition rates. The research has also identified some challenges accompanying the use of multimodal biometric systems, and suggested solutions to the identified challenges. Multimodal biometric systems improve the performance of biometric authentication [22]. Therefore, adopting the use of biometric technology will no doubt result into robust security systems and will go a long way to create one of the most secured forms of authentication.

## REFERENCES

[1] K.Kumar and M. Farik, "**A Review of Multimodal Biometric Authentication**", International journal of scientific and technology research volume 5, issue 12, 2016.

[2] G.B. Iwasokun, S.S. Udoh and O.K. Akinyokun, "**Multi-Modal Biometrics: Applications, Strategies and Operations",** Global Journal of Computer Science and Technology: G Interdisciplinary Volume 15 Issue 2 Version 1.0,2015.

[3] O.Chike, "**Multimodal Biometric Technology System Framework and E- Commerce in Emerging Markets**", International Journal of Advanced Computer Science and Applications, Vol. 4, No.7, 2013.

[4] E. Lupu and P. G. Pop, "**Multimodal biometric systems overview**",ACTA TECHNICA NAPOCENSIS, Electronics and Telecommunications, Volume 49, Number 3, 2008.

[5] S. Kumar and E. Walia, "**Analysis of various Biometric Techniques**", International Journal of Computer Science and Information Technologies, Vol. 2 (4) ,1595-1597 ,2011.

[6] G.W. Mwaura, W. Mwangi and C. Otieno, "**Multimodal Biometric System:-Fusion of Face and Fingerprint Biometrics at Match Score Fusion Level**", International journal of scientific & technology research volume 6, issue 04, 2017.

[7] H. Purohit and P.K. Ajmera, "**Multimodal Biometric Systems: A Brief Study**", International Journal of Innovative Technology and Exploring Engineering ISSN: 2278-3075, Volume-8 Issue-7 May, 2019.

[8] U. Gawande and Y. Golhar, "**Biometric security system: a rigorous review of unimodal and multimodal biometrics techniques**", International Journal of Biometrics, Vol. 10, No. 2, 2018.

[9] B. Ammour, L. Boubchir,T. Bouden and M. Ramdani, "**Face–Iris Multimodal Biometric Identification System**",Electronics2020,9,85;doi:10.3390/electronics9010085,2020 www.mdpi.com/journal/electronics

[10] M. Elhoseny,E. Essa, A. Elkhateb, A. E. Hassanien and A. Hamad, "**Cascade Multimodal Biometric System Using Fingerprint and Iris Patterns**", Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2017, Advances in Intelligent Systems and Computing 639, DOI 10.1007/978-3-319-64861-3 55.

[11] S. Verma and R. K. Singh, "**Multimodal Biometrics Information Fusion for Efficient Recognition using Weighted Method**", International Journal of Engineering Research and General Science, Volume2, Issue4, 2014.

[12] P. Byahatti and S.M. Hatture, "**A Fusion Model for Multimodal Biometric System**", International Journal of Engineering Research & Technology ISSN:2278-0181 Published by, www.ijert.org NCETAIT - 2017 Conference Proceedings.

[13] H. Benaliouche and M. Touahria, "**Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint**", The Scientific World Journal,Volume 2014

[14] D. Jagadiswary and D. Saraswady, "**Biometric Authentication using Fused Multimodal Biometric**", International Conference on Computational Modeling and Security, 2016.

[15] R.S. Choras, "**Multimodal Biometrics for Person Authentication**", Security and Privacy From a Legal, Ethical, and Technical Perspective.DOI:
http://dx.doi.org/10.5772/intechopen.85003

[16] K.Sasidhar, V.L Kakulapati, K. Ramakrishna and K.KailasaRao, "**Multimodal Biometric Systems – Study to improve accuracy and performance**", International Journal of Computer Science & Engineering Survey, Vol.1, No.2, 2010.

[17] S. S. Yadav, J. K. Gothwal and R. Singh, "**Multimodal Biometric Authentication System: Challenges and Solutions**", Global Journal of Computer Science and Technology, Volume 11, Issue 16, Version 1.0, 2011.

[18] P.Subramanian, K.N.Krishna, R.M.Sebastian and N.U.Rahman, "**Multibiometric systems**", International Journal of Chem. Sci.: 14(S3), 2016.

[19] E. Tarek, O. Ouda and A. Atwan, "**Image-based Multimodal Biometric Authentication Using Double Random Phase Encoding**", International Journal of Network Security, Vol.20, No.6, PP.1163-1174, 2018.

[20] H. Choi and H. Park, "**A Multimodal User Authentication System Using Faces and Gestures**", Biomed Research International, Hindawi Publishing Corporation, Article ID 343475, 2015.

[21] S.Kumar, S.Paul and D.K.Shaw, "**Design and Modeling of Real Time Multimodal Biometric Authentication System**", Journal of Computer Science, 2017.

[22] S. Sunder and R. Singh, "**Multimodal Biometric System Based: Integrating Strategies Approach at Feature Level**", International Journal of Recent Development in Engineering and Technology, Volume 3, Issue 6, 2014.

[23] A.Ashraf and I. Vats, "**The Survey of Architecture of Multi-Modal (Fingerprint and Iris Recognition) Biometric Authentication System**", Int. Journal of Engineering Research and Application, Vol. 7, Issue 4, (Part -3), 2017.

[24] Y. Elmir, Z. Elberrichi and R. Adjoudj, "**A Hierarchical Fusion Strategy based Multimodal Biometric System**", The International Arab Conference on Information Technology (ACIT'2013).

[25] I Iqbal, "**Description of Research Design using Articles for Biometrics Technology Security and Countermeasures**", International Journal of Advanced Trends in Computer Science and Engineering, Volume 10, No.1, January - February 2021.