www.ijaceeonline.com ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 11, November 2018, pp. 9–16

Conceptual Design of Multiple Biometric System Using a Three Tier Approach

Ophelius Mhaaneeh Yinyeh
PG Scholar, Department of Computer Science,
University for Development Studies, Navrongo, Upper East Region, Ghana
Email: ophelius24@gmail.com

Elkanah Olaosebikan Oyetunji
Professor, Department of Mechanical Engineering,
Lagos State University, Lagos, Nigeria
Email: eoyetunji@yahoo.com

Nathaniel Kayode Oladejo
Senior Lecturer, Department of Mathematics,
Landmark University, Omu-Aran, Nigeria
Email: oladejonath@yahoo.com

Abstract: *The identification of people for goods, services and the general maintenance of security law and order has become topical agenda amongst governments, agencies and institutions the world over. There are numerous competing technologies and designs suggested to solve this issue. This paper suggests a design that would further improve on the identification and verification of subjects at high security installations in order to accurately and uniquely identify subjects. The proposed design is termed three tier; in tier one (1), the subjects biometric data is enrolled. This would be done using multiple traits and stored to the database. Tier two (2) would fuse these traits enrolled in tier one (1) pair wise and stored to the database. Tier three (3) would fused all possible traits acquired in tier one (1) and stored to the database. During verification or Identification mode, any of the tiers could be called upon to match the subject for authentication and this could be graduated depending on the level of security requirements needed for that service or entry to the facility or country.*

Keyword: *Biometric, Multiple, Three tier, Conceptual, Design.*

1. INTRODUCTION

To identify individuals in this global village uniquely, is becoming very pertinent especially that we are now interdependent as nations the world over.

In ascertaining the true identities of individuals, we will need to satisfy questions like "is he/she really who he/she claims to be?", "is this person authorized to use this facility or be provided with these services?" or "is he/she in the watch list posted by the government or the agency?" are routinely being posed in a multiplicity of scenarios.

From the onset of opening a bank account to receiving health care and gaining entry into another country, the questions stated previously need to be answered. The need for an acceptable and a dependable user authentication methods, has been intensified in the wake of heightened worries about security and swift advancements in networking, communication and mobility. Biometrics, is described as the science of identifying subjects based on their biological or developmental traits. This is beginning to gain reception as a genuine method for determining an individual's identity uniquely [17].

Biometrics has been approved and implemented in several large-scale identification application software, from border control to electorate ID issuance for public elections. While the technology is conceptually proficient, practically however in the real world, there are so many shortfalls associated with scanning (enrolling) large populations using just single (unimodal) biometrics. These challenges can be solved or improved by deploying multimodal biometrics systems [20].

Biometric systems have become the order of the day, finding acceptance and implementation amongst large civilian, commercial and forensic applications as a means of establishing uniqueness. These technologies rely heavily on the evidence of a subject's iris, retina, fingerprints, hand geometry, face, facial

Cite this paper:

Ophelius Mhaaneeh Yinyeh, Elkanah Olaosebikan Oyetunji, Nathaniel Kayode Oladejo, "Conceptual Design of Multiple Biometric System Using a Three Tier Approach", International Journal of Advances in Computer and Electronics Engineering, Vol. 3, No. 11, pp. 9-16, November 2018.

International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 11, November 2018, pp. 9–16

thermo-gram, signature, hand vein, voice, gait or odor to either validate or determine a person (subject) [5].

Several biometric systems and devices are single or "unimodally" designed. They are only comfortable with single feature and single source of data for authentication.

These technologies have to struggle with a variety of challenges such as:

(a) Noise in sensed data: a fingerprint image with a scar or a voice data altered by common cold, are but a few of the noisy data. Noisy or poor data captured from biometric devices could also be as a result from faulty or improperly maintained sensors or devices, for example the deposit of dirt on a fingerprint sensor or inappropriate ambient conditions due to the environmental influences that may contribute to a poor brilliance of a user's face in a face recognition device or camera.

(b) Intra-class variations: these disparities are characteristically caused by a user who is incorrectly interacting with the sensor intentionally or unintentionally. This usually occurs by incorrect facial pose or when the individualities of a sensor are modified during authentication.

(c) Inter class similarities: for an identification using a biometric system, making up of large number of data may contain some similarities of subject's biometric traits that may reduce the uniqueness of the system.

Unimodal systems are fast giving way because they have to deal with various challenges related to lack of secrecy, non-universality of samples/data, the ease of use/comfort and freedom while interacting with the system, spoofing attacks on stored data.

A lot of the bottlenecks presented by a single or unimodal biometric systems and devices would be done away with the employment of multiple biometric sources for the establishment of their identities accurately [3].

All those technologies known as multimodal biometric systems, are more reliable due to the presence of multiple, objectively autonomous pieces of evidence haggard from the same subject [1].

2. MULTIMODAL BIOMETRICS ELUCIDATIONS

In the process of uniquely identifying subjects for any purpose biometrically, solutions offered employing more than one biometric scanning option is referred to as multimodal. With such a wide-ranging definition, the term multimodal biometric technology can refer to any technology that combines diverse sorts of biometrics traits, either to work together as a multifactor identification or verification system or to allow a host of authentication possibilities. Software applications that fuse voice and face recognition, mobile devices that offer access control through iris or fingerprint, futureproof biometric platforms are ready to support and manage any single or multi-factor type of authentication; all these forms of identification fall under the canopy of multimodal systems.

The benefits are intrinsic to multimodal biometrics, the most prominent being improved levels of security and accuracy and greater levels of accessibility/flexibility. A banking technology, implemented online that employs both voice and face recognition to authenticate their customers using their user login for transactions is more protected than the implementation of either one of its modalities only. Conversely, a physical access control system that accommodates iris, finger print enrolment is in a pole position for any form of deployment and is highly rated for installation where finger print will do well and where finger prints may fade.

2.1 Why Multimodal Biometrics is Required

The followings are some of the reasons why multimodal biometrics are required:

- The handiness of multiple qualities makes the multimodal system more reliable.
- Multimodal biometric applications surges security and secrecy/integrity of user data.
- A multimodal biometric technology engages the fusion of traits or features to combine results from each subsystem and then presents a decision. This makes this type of system more accurate than others.
- In an event that any of the identifiers employed fails for known or unknown reasons, the system will still provide a very good level of security making use of other identifiers enrolled.
- Multimodal biometric technology can provide information about liveliness of the subject's traits being enrolled by employing liveliness recognition techniques. This makes them able to sense and manage the any possibility of spoofing by attackers [22].

2.2 The Operations of Multimodal Biometric System

A Multimodal biometric technology encompasses all modules a unimodal system has namely;

- Capturing stage/module
- Feature extraction module
- Comparison module
- Decision making module

Further, it has a fusion system to integrate the traits extracted from two dissimilar authentication methods.

International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 11, November 2018, pp. 9–16

Fusion of biometric traits can be prepared between the following established levels;

- Feature extraction level.
- Comparison of live traits/samples with stored biometric templates on a database.
- Decision making level.

From findings multimodal biometric technology records a very high rate when fusion are integrated at the initial stages than the systems that fuse the information at a future stage [22].

2.3 Fusion Scenarios in Multimodal Biometric Technology

There are a number fusion techniques and fusion scenarios suggested by several researchers in this field. They can be solitary/single biometric trait, multiple/many sensors. Single biometric feature, several classifiers (that is, texture based matcher and minutiae based matcher). Single biometric feature, multiple units (say, multiple fingers). Multiple biometric traits of a subject (for instance, fingerprint, iris, and palm print). These traits are then worked upon to confirm a subject's identity [22].

2.4 Some Design Factors with Multimodal Biometric Systems

Some few issues needs to be considered while planning a multimodal biometric system. Some of these factors are:

- Level of security you need to convey.
- The number of subjects who will use the system.
- Types of biometric traits/features you need to acquire during enrolment.
- The number of biometric traits from the subjects.
- The stage at which biometric traits needs integration/fusion.
- The procedure to be adopted to fuse the information acquired.
- The comparison between development cost versus system performance in the biometric system.

2.5 Purpose of Multimodal Biometrics

The level of security of a multimodal system has three primary components authentication, authorization, and accountability. The Authentication stage is the greatest of these three elements because it comes first.

Within the confines of ICT, authentication refers to either the process of verifying the identities of equipment or verifying the identities of the equipment's users which are predominantly humans. Biometric systems are becoming popular as a measure to identify human beings by measuring one's physiological or behavioral characteristics. Biometrics identifies the subject or person by what the person or subject is made up off rather than what the person carries, unlike the conventional authorization systems like smart cards.

Unlike the other forms of identification like the possession, knowledge based and personal identification systems, the biometric identifiers cannot be misplaced, guessed, forgotten or easily faked.
Irrespective of these visible advantages, the implementation and use of biometrics identification has been mired due to numerous reasons: the unreliable measurement recorded for so many applications for instance in face recognition. This is affected by pose, illumination and facial expression [2].

In addition, spoof attacks has become a nightmare to the biometric system. Farther, some subjects are not able to meet the requirements of single biometric systems due to disabilities, illness or accidents [4].
The multimodal biometric systems have proved to be superior in all spheres over unimodal biometric systems in several areas.

The suggestions of some of the confines corroborated by [6] of unimodal/single biometric technology are but not limited to:

1. Vulnerability of biometric sensors to noise. Noisy data acquired may lead to inaccurate matching, increasing false rejection rate of subjects.
2. Single biometric technology are also disposed to interclass resemblances within large population groups
3. Unsuitability with certain groups or population. Young children and Elderly people may have challenges enrolling in a fingerprinting system, as a result of their worn prints or immature fingerprint ridges.
4. It is established that, Unimodal biometrics is liable to spoof attacks. For instance, rubber fingerprints can be employed for spoofing, hence liveness tests are a must.

In [16] their research ascertained that, biometric systems are still vulnerable to certain type of attacks at various points in the biometric model. A spoofing attack which is submitting a stolen or copied biometric trait to the sensor to gain unlawful access to the biometric system is one of the weaknesses to the model.

They further revealed in their paper that, multimodal biometric systems are designed to increase the exactitude of the biometric system.

The existing tactics for anti-spoofing do not consider multiple biometric traits and also have a high false acceptance rate. In the quest to solve the problem of spoofing, they presented a new design method in multimodal biometric system combining traits (face, fingerprint and iris images). The mined biometric traits are combined and fed to a convolution neural network that uses a deep learning to sense spoofed features from real traits. They concluded their

International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 11, November 2018, pp. 9–16

research with the proposed method given better results than existing anti-spoofing methods [10].

[6], fused the data generated by multiple biometric traits, hence presenting a higher performance than the systems based on a single or one biometric modality or trait. They achieved this through coupling of biometric systems at the scores level since this is the most common and it has been proven effective than the rest of the fusion levels as per literature. Moreover, the scores at the score level from different modalities or traits are usually heterogeneous. In other to fuse these different modalities, there is the need to normalize the scores to transform these scores into a common domain before they can be combined.

In order to determine the best in their research, they examined the performance of numerous normalization techniques with various fusion technologies in a framework by implementing the combination of three unimodal systems based on the palmprint, face and the fingerprint. From their research, they proposed a new adaptive normalization method that takes into account the distribution of client scores and impostor scores.

From their experimental results conducted on a database of 100 people, revealed that the performances of a multimodal system depend on the choice of the normalization method and the fusion technique.

The researchers relied on the growing concern the world over, related to personal and property safety and the rapid growth of security and surveillance related technologies. They equally agreed like other researchers that, biometric system is one that can provide accurate and reliable scheme for person verification. They adduced that, the main aim of biometric based security system is to make sure that, the rendered service is accessed only by valid and the intended user(s). It was clear in their work that, multimodal biometric systems were gaining more popularity as it is capable of addressing most of the issues militating against the designing of a biometric systems such as: noise in sensed data, non-universality, large intra-user variations and vulnerability to spoof attacks. In conclusion they presented an overview of multimodal biometrics and its advantages, challenges, drawbacks and limitations [13].

The literature [15] indicated that, currently we have a lot of systems designed and implemented with the unimodal biometric systems for authenticating users. The recognition performance of single modal biometric systems having symptoms as attributed to noisy data in the subject, non-universality, intra-class variations, spoof attacks, or distinctiveness. To address these limitations, the design of multimodal biometric system that combines multiple source of information for an individual for recognition is paramount.

This is able to eliminate the innumerable problems faced by a single modal biometric system and to improve the recognition performance. They presented a multimodal biometric system by incorporating iris, fingerprint and face to identify a subject using Daugman's algorithm for iris recognition, WLD and Eigen faces for the face recognition end and minute feature and decision tree algorithm for fingerprint recognition area.

From their experimental estimations performed on a public dataset espoused the accuracy of their proposed design [21].

The introduction of biometric systems have expressively improved personal identification and verification, playing an important role in a person's global security. In this paper, the authors used multimodal biometric method to overcome this problem. Multimodal biometric system is one of the major areas of study identified with large application in recognition system [21].

2.6 Multi-Modal Biometric Verification

Verifying the claimed identity of an individual is critical in providing secure access to physical systems, devices and spaces. However, verification methods based on a single biometric type or algorithm may not provide adequate verification performance, not every one may be able to use a particular biometric. For instance, some face recognition algorithms cannot handle expressions whereas other algorithms may have problems with illumination changes. What was clear is that, there can be an advancement as far as the performance was concerned by employing different algorithms and intelligently fusing the results. Also, in some cases, one biometric may not be applicable at all. For instance, some subjects do not have good enough ridges in their fingerprints to be able to use fingerprint verification systems. It is believed that by using multiple biometric modalities, we will achieve not only improved security, but also a verification system that can be used by more people [11].

In [18] paper, a novel multimodal recognition system that trains a Deep Learning Network to automatically learn features after extracting multiple biometric modalities from a single data source, that is, facial video clips was presented. Utilizing different modalities, such as , frontal face, left ear, left profile face, right ear and right profile face present in the facial video clips, were used with the support of train supervised denosing autoencoders to automatically extract strong and non-redundant features. The learned traits are then used to train modality specific sparse classifiers to perform the multimodal recognition. In their research they employed constrained facial video dataset (WVU) and the unconstrained facial video dataset (HONDA/UCSD), the findings resulted in a 99.17%

International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 11, November 2018, pp. 9–16

and 97.14% rank-1 recognition rates, respectively. The multimodal recognition accuracy reveals the dominance and strength of the proposed approach notwithstanding of the illumination, non-planar movement, and pose variations present in the video clips [18].

Combining different extracts from traits obtained from different sources or modalities, known as information fusion, is by far one of the main factors of designing a biometric system employing more than one biometric trait. There are several stages or level at which the traits in biometric technology that fusion or combination can occur namely; senor level, feature extraction level, match score level, rank level, and decision level. Gaining grounds is also another emerging fusion method, which is growing recognition among researchers is the fuzzy fusion. Fuzzy fusion concentrates on the quality of the inputs or with the quality of any technology scheme components. Their paper discusses the associated challenges related to making the choice of appropriate fusion method for the application domain, to balance between fully automated versus user defined operational parameters of the system and to take the decision on governing rules and weight assignment for fuzzy fusion [20].

The traits under consideration are but not limited to their fingerprints, facial features, voice, irises and signatures, just to enumerate a few. While single modality biometric system have to contest with their greatest enemy being noisy sensor data, specifically to the biometric trait and intolerable error rates, the multimodal biometric system suffer from storage requirements as the data scanned are large, processing time, complicated security issues and the computational complexity applied in this technology.

A new method that provides a solution to error rate problem and security issues was presented. In their research, they suggested a method that employs Quick Response codes (QR codes), to embed the combined biometrics data and cloak it with a secure encryption technique such as DES or AES. In a bid to validate their research work and validate the biometric system, they used the Gaussian copula, which is a very accurate method for measuring data sequences similarity. From the results obtained from their research after putting their data through experimentation, it showed that the suggested method presented near perfect verification outcome as a results of great error correction ability of the QR codes. In applying this to images using two sequences; the original and the distorted images, their results scored very high recall rate on a sample of 260 cases from the CoMoFoD database [14].

In [14] their paper, suggested a new evolutionary method for adaptive combination of multiple biometrics to drum home the optimal performance for the desired level of security in the system. The score-level fusion rules were employed to achieve optimum system performance using a hybrid particle swarm optimization model. Their research pointed out that, the score-level will achieve expressively better and steady performance against the decision-level method. Literature has expressed scanty research on the potency of the adaptive multimodal fusion algorithm on real biometric data.

For every multimodal biometric system, a good fusion method is very important for combining features of traits from multiple biometric devices. [19] in their paper suggested a method of fusion using multiple features from hand vein biometric traits for multimodal biometric recognition. In this work, three different veins images were involved in their research, such as; dorsal vein, finger vein, and palm vein was developed. At this stage multiple traits from the input vein images were extracted by applying Radon transform, Hilbert–Huang transform and Dual tree complex wavelet transform for each of the vein images. After the extraction of the features, it is then taking through the feature level fusion employing the optimization algorithm known as the Group Search Optimization. After that, recognition is achieved using the trained features by different classifiers such as support vector machine, bayes classifier, fuzzy, k-nearest neighbor classifiers and neural network. This work was tested with finger vein, palm vein and dorsal vein images of the hand database. Their proposed method provides higher accuracy and lower equal error rate which shows the efficiency of the technique compared with the other existing techniques.

Multimodal authentication presents extra level of authentication/identification than unimodal biometrics which uses only one biometric trait such as fingerprint, face, palm print or iris [12]. A technique called minutiae matching and edge detection was used for this purpose. The performance of the proposed technique was evaluated, accuracy was measured and was detected to have been increased by minimizing the FAR (False Acceptance Rate) and FRR (False Rejection Rate) [12].

India is the largest democracy in the world, elections forms the cornerstone of their country. To guide this jealously, a number of measures were to be implemented to maintain the integrity of the electoral process and prevent any intrusion. Running a free and transparent elections has become a top agenda for all countries and most especially for India. Finding a solution for this large democracy is not a simple exercise. In every electoral cycle, privacy is as revered as the sanctity of the elections. To archive this, all structures to eliminate any form of coercion, buying, or selling of votes and intimidation were advised. In a bit to solve these and many other problems, [9] suggested a new state-of-the-art Electronic Voting Machine,

www.ijaceeonline.com ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 11, November 2018, pp. 9–16

designed in the quest for election legitimacy, to provide an affordable and robust state of the art biometric technology, implementing fingerprint traits of electorates, inculcating Near-Far Communication technology.

The household slogan, called cloud computing, stirs both academia, industry and technology lovers the world over, this is as a result of its capabilities of turning around the big dream of opening a new chapter in computing and revolutionize the industrial and production sector beyond the present experiences. Whiles this was being researched and implemented, hackers also invested their time in studying the new technology to enable them breach the security implemented. Some of the reliable security software rely heavily on solutions developed around cloud computing. In accomplishing the set goals in the research, the following solution were suggested, a three tier security in cloud environment has been proposed. A group of biometric features are extracted from user's face image first [9].

The traits extracted are then quantized and mapped to binary representation for feature point matching in the process. The resulting features produced from the quantization and mapping are then added to secret key (which will restrict unauthorized access) are bound using Face fuzzy vault scheme. When the authentication module is called, the key will be correctly retrieved in the process if the face vault matches correctly. Again to avert data from cloud service providers, the data is encoded while saving it on the cloud using Privacy, Honesty, Obtainability values which will categorize data in three rings. In an event of presenting data if user is authorized, then the password corresponding to the user gets extracted from the fuzzy vault and the retrieved password will give an indication to which data ring it belongs to [9].

As presented in the literature by several researchers, dual (two) or three combinations or fusion of traits has been designed in some cases and researched over time.

To fill this gap, a proposed design of a multiple traits fusion with flexibility of either downgrading where the need arises has been suggested. A more generalized design to accommodate as many scenarios and to thwart possible security breaches due to lost or non-availability of a particular bio-trait is to be investigated.

3. PROPOSED DESIGN

To satisfy a number of competing and stringent specifications for the development and implementation of biometrics systems, there is a need for an acceptable design that would solve some of the problems or challenges with the single or unimodal biometrics reviewed earlier in this paper. The failure of one biometric trait is very loud, and that needs to be attended to. In this design, a three phase or cycle is proposed termed, three tier. Tier one (1) takes the scan (multiple) or enrolment (multiple) of the biometric traits, Tier two (2) combines the traits pairwise as they are scanned or enrolled. In Tier three (3), all the traits are then combined.

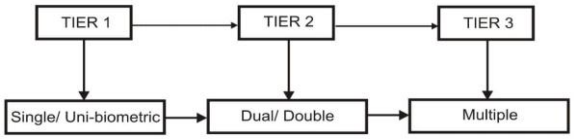

Figure 1 Enrolment Phase of three Tier Design.

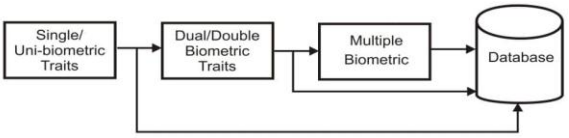

Figure 2 Scanning of traits during enrolment phase

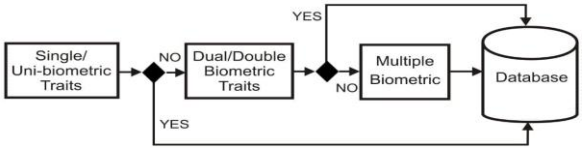

Figure 3 Verification or Authentication phase of three Tier Design

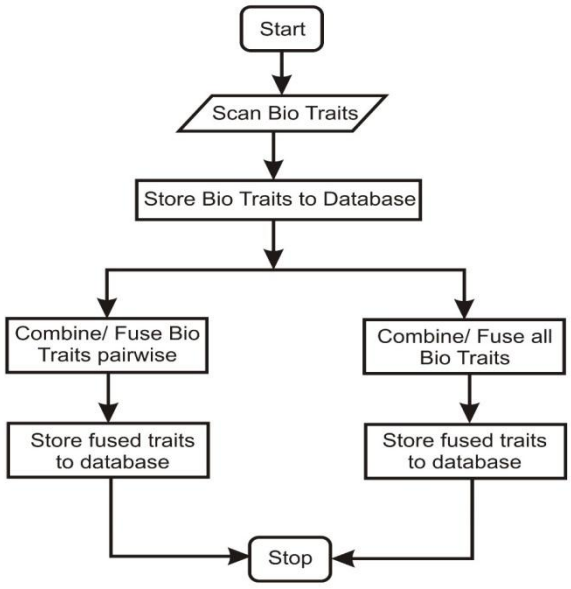

Figure 4 Flow Chart of three tier Design (Enrolment Mode)

This three step approach would present us with a flexible implementation and the cure situations were some subjects do not have a particular trait being requested for either enrolment or for verification.

International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 11, November 2018, pp. 9–16

It would also afford security check points to regulate the level of verification especially at high security installations or access points.

During authentication or verification, subjects can then be verified using either single verification, multiple or fused multiple verification. The system is then set to the security standards of the service provider, this would eliminate issues of missing biometric traits, fading of prints due to work hazards and other biological changes due to several conditions.

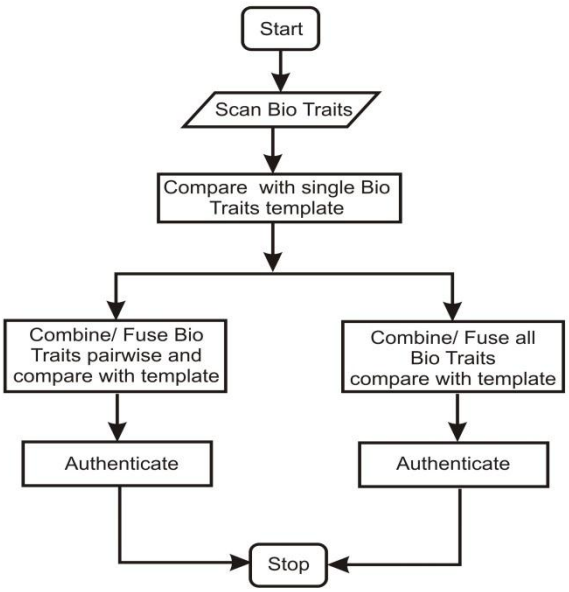

Figure 5 Flow Chart of three tier Design (Verification Mode)

4. CONCLUSION

In this paper a conceptual design of multiple biometric identification system is proposed as an alternative design to single or Uni-Biometric design and other forms of designs. This design promises to improve on the identification of subjects more accurately and reducing false accepts and rejects rates drastically. The various tiers however may increase time used for processing of subjects, the design is however opened to the implementation to be varied depending on the security requirements of the institutions or department implementing this type of identification system.

REFERENCES

[1] Kuncheva L. I., Whitaker C. J., Shipp, C. A., and Duin, R. P. W. (2000), "Is independence good for combining classifiers?," *in Proc. of Int'l Conf. on Pattern Recognition (ICPR), vol. 2, (Barcelona, Spain),* pp.168–171, 2000

[2] Monrose, F., and Rubin, A.D. (2000), "Keystroke Dynamics as a Biometric for Authentication", *Future Generation Computer Systems*, Vol. 16, No. 4 (2000) 351-359

[3] Ross A. and Jain K. (2003), "Information fusion in biometrics," *Pattern Recognition Letters*, vol. 24, pp. 2115–2125, Sep 2003.

[4] Feng G., Dong K., Hu D. and David Zhang (2004) "When Faces Are Combined with Palmprints: "*A Novel Biometric Fusion Strategy, Proceedings of First International Conference, ICBA 2004, (2004), Springer*, 701-707

[5] Jain K., Ross A., and Prabhakar S. (2004), "An introduction to biometric recognition*," IEEE Trans. on Circuits and Systems for Video Technology*, vol.14, pp.4–20, Jan 2004.

[6] Teddy Ko. (2005), "Multimodal Biometric Identification for Large User Population Using Fingerprint, Face and Iris Recognition", *Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop (AIPR05)* ,2005.

[7] Ajay Kumar, Vivek Kanhangad, Daqiang Zhang. (2010), "A New Framework for Adaptive Multimodal Biometrics Management" *Article in IEEE Transactions on Information Forensics and Security* 5(1):92 - 102 · April 2010

[8] Hemantha G. Kumar and Mohammad Imran. (2010), "Research Avenues in Multimodal Biometrics". *IJCA,Special Issue on RTIPPR* (1):1–8, 2010. Published By Foundation of Computer Science.

[9] Joshi V. and Sanghavi P. (2012), "Three tier data storage security in cloud using Face fuzzy vault," *2012 International Conference on Computing, Communication and Applications*, Dindigul, Tamilnadu, 2012, pp. 1-6. doi: 10.1109/ICCCA.2012.6179217

[10] Anouar Ben Khalifa, Sami Gazzah, Najoua Essoukri BenAmara. (2013), "Adaptive Score Normalization: A Novel Approach for Multimodal Biometric Systems" *International Journal of Computer, Electrical, Automation and Information Engineering*, 2013.

[11] Sayan Maity, Mohamed Abdel-Mottaleb, and Shihab S. Asfour. (2015), "Multimodal Biometrics Recognition From Facial Video Via Deep Learning", *Computer Science & Information Technology (CS & IT)*

[12] Das A., Dutta M. P. and Banerjee S. (2016), "VOT-EL: Three tier secured state-of-the-art EVM design using pragmatic fingerprint detection annexed with NFC enabled voter-ID card," *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, Pudukkottai, 2016, pp. 1-6.

[13] Mendu. Anusha, Vamsi Krishna, and T.V. (2016), "Multimodal Biometric System Integrating Fingerprint Face and Iris". *International Journal of Innovative Research in Computer and Communication Engineering.* ISSN(Online): 2320-9801 ISSN (Print): 2320-9798 Vol. 4, Issue 10, October 2016

[14] Bharathi Subramaniam, Sudhakar Radhakrishnan. (2017), "Multiple features and classifiers for vein based biometric recognition". *Computational Life Sciences and Smarter Technological Advancement* Biomed Res- India 2017 Volume Special Issue Issue Special Section.

[15] Chetan Jamdar and Amol Boke. (2017), "Review Paper on Person Identification System Using Multi-Model Biometric Based On Face". *International Journal of Science, Engineering and Technology Research* (IJSETR) Volume 6, Issue 4, April2017, ISSN: 2278 -7798

[16] Devakumar P., Sarala R. (2017), "An Intelligent Approach for Anti-Spoofing in a Multimodal Biometric System" *International Journal of Advanced Research in Computer Science and Software Engineering Volume 7, Issue 3*, March 2017.

International Journal of Advances in Computer and Electronics Engineering
Volume 3, Issue 11, November 2018, pp. 9–16

[17] Imran Khan, Auto ID & Security Multimodal Biometrics– Is Two Better Than One?, retrieved date: [15, September 2017], online available at: http://www.frost.com/prod/servlet/market-insight-print.pag?docid=80082644

[18] Oloyede Ayodele and Aderonke Adegbenjo, (2017) "Current Practices in Information Fusion for Multimodal Biometrics" *American Journal of Engineering Research (AJER)* e-ISSN: 2320-0847 p-ISSN : 2320-0936 Volume-6, Issue-4, pp-148-154 www.ajer.org

[19] Parkavi R., Babu, K. R. C. and Kumar J. A.. (2017), "Multimodal Biometrics for user authentication," *11th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, 2017, pp. 501-505. doi: 10.1109/ISCO.2017.7856044

[20] Saif Al Z. (2017), "Precise Multimodal Biometric Fusion Method Using Copula and QR Codes". *Biostat Biometrics Open Acc J*. 2017;1(5): 555572.02

[21] Vijayakumar Bhagavatula, "Multi-Modal Biometric Verification", retrieved date: [21, May 2017], online available at:https://www.cylab.cmu.edu/research/projects/2008/multimodal-verification.html

[22] Why Multimodal Biometrics is required, Retrieved date: [07, May 2017], online available at: https://www.tutorialspoint.com/biometrics/multimodal_biometric_systems.htm

Authors Biography

Ophelius Mhaaneeh Yinyeh is a PG Student of the Department of Computer Science in the Faculty of Mathematical Sciences in the University for Development Studies, Navrongo Campus, Ghana. He completed his B.Sc. in the Department of Computer Science, University for Development Studies. He completed his M.Sc. in the Department of Mathematics, University for Development Studies, Navrongo Campus. His research interests are Biometrics, Electronic Voting, Algorithm Design and Software Development.

Elkanah Olaosebikan Oyetunji is currently a Professor of Industrial and Production Engineering in the Department of Mechanical Engineering, Faculty of Engineering, Lagos State University, Epe Campus, Lagos, Nigeria. He graduated with a BSc (Hons) in Electrical Engineering from the University of Ilorin, Ilorin, Nigeria. He has an MSc and PhD in Industrial Engineering from the University of Ibadan, Ibadan, Nigeria. He has attended numerous national and international conferences. His research interest includes production scheduling/operations management (optimization), and algorithm design amongst others. He has published extensively in prestigious local and international journals. He is a Registered Engineer (COREN) and a Member of the following professional bodies: Nigeria Society of Engineers (NSE), Nigeria Institute of Industrial Engineering (NIIE), South African Institute of Industrial Engineering (SAIIE).

Nathaniel Kayode Oladejo is currently a Senior Lecturer in the Department of Mathematics, Faculty of Sciences and Engineering, Landmark University, Omu Aran, Kwara State, Nigeria. He had his B.Sc. degree in Mathematics from the University of Ado Ekiti, Nigeria, M.Sc. Mathematics from the University of Ilorin, Nigeria and MBA Finance from the Ladoke Akintola University of Science and Technology, Ogbomoso, Nigeria coupled with PhD in Applied Mathematics from the Kwame Nkrumah University of Science and Technology, Kumasi, Ghana. He has attended numerous national and international conferences. His research interest includes Optimization, Dynamics and control Theory. He has published extensively in prestigious local and international journals and had four (4) Mathematics text books to his credit. He is a member of Nigeria Mathematics Society (NMS), Nigerian Association of Mathematical Physics (NAMP), Ghana Mathematics Association (GMA), Ghana Mathematics Association of Sciences (GAS).

Cite this paper:

Ophelius Mhaaneeh Yinyeh, Elkanah Olaosebikan Oyetunji, Nathaniel Kayode Oladejo, "Conceptual Design of Multiple Biometric System Using a Three Tier Approach", International Journal of Advances in Computer and Electronics Engineering, Vol. 3, No. 11, pp. 9-16, November 2018.