Transactions of the Nigerian Association of Mathematical Physics
Volume 13, (October – December, 2020 Issue), pp21 –30

MULTI-MODAL BIOMETRIC RECOGNITION SYSTEM

[1]Olayinka T.C., [1]Ogunrinola J.D., and [2]Olayinka A.S.

[1]Department of Mathematical and Physical Sciences, Samuel Adegboyega University, P.M.B. 001, Ogwa, Edo State, Nigeria
[2]Department of Physics, Faculty of Science, Edo University Iyamho, P.M.B. 007 Auchi, Edo State, Nigeria.

Abstract

Identification and authentication of users is one important thing in the world of security, not only does traditional method - Personal Identification Number (PIN), Identification Cards (ID cards) not confirm the identity of a user but is accompanied with spoofing, forging and other limitations. Biometric method, using one or more biometric trait of an individual such as fingerprints, gait, iris scan, etc eradicates the flaws of the traditional method. Biometric system consists of two types which are unimodal and multimodal biometric systems. Unimodal biometric system only uses a single biometric trait which has limited effectiveness in identifying people, mainly due to their susceptibility to changes in individual biometric features and presentation attacks. The identification of people using multimodal biometric systems attracts the attention of researchers due to its advantages, such as greater recognition efficiency and greater security compared to the unimodal biometric system. Multimodal biometric system consists of several techniques that builds its efficiency such as Gabor Filter Approach and Periocular Feature Extraction Approach. Multimodal biometric system is useful in a large population as it reduces distortion of data, noise in sensed data and allows efficiency of multi users. In this report contains the detailed research on multimodal biometric recognition system, its methodologies and challenges.

***Keywords*:** Spoofing, Sensor, Identification, extraction, fusion and verification

1.0 INTRODUCTION

1.1 Background of Study

As rampant as it is that identification and verification is becoming more exposed to spoofing, forging, overwriting and counterfeit. The use of traditional methods like passwords and identification cards are becoming obsolete and unreliable especially for security purposes because it can be easily replaced, lost or stolen [1]. Also, traditional method is not sufficient to proof the uniqueness of a user, therefore the introduction of biometric features such as fingerprints, iris scan, face, gait, palmprint now serves as a means of solving the problem of uniquely identifying a user [2].

The traditional method of identification and verification seems to be going vastly extinct. It does not stop spoofery or hacking or manipulation of passwords or duplication of identification cards which is supposed to serve as a means of uniquely identifying a user, else, the traditional method functions more for verification. Why do users of social media forget their password or have another person using their account without their consent or have problems logging in with their passwords? Why are there forged identification cards used to sit for examinations or used to get access into restricted areas? All the vulnerabilities attached to traditional method is alarming because it is not the best means of uniquely identifying a user. In the case of social media, passwords can be easily guessed or just take a little time to be fetched out by the cyber fraudsters, also password does not really show that the account owner is the one logging in, it is just a verification that a user is valid as well as identification cards or pass codes are not exempted because they all have a loose end that a hacker can use to overwrite or change them[3].

In many cases, fraudsters do not even need to spoof or hack social media accounts or verification codes via SMS since it can be gotten just by breaching data and spilling data into the ethernet. Names, passwords, phone numbers, date of birth, security questions and other methods of identification can be retrieved from the cyberspace or the cloud as a result of the global use of the internet.

Correspondence Author: Olayinka A.S., Email: solayinkaa@gmail.com, Tel: +2348062447411

1.2 Motivation of the Study

The world is becoming increasingly security conscious as new approaches to security is been researched which should be more reliable and authentic. In a system, authorized users should be granted access with higher accuracy while unauthorized users should be denied [4]. For example, physical access to a secure facility, e-commerce, computer networks, etc. Biometrics method has come in place to actively and uniquely identify a user with its unique features such as fingerprints, iris scan, face, gait, palmprint and so on, but as effective as these methods are, they still encountered one problem or another like noise in the sensed data, non-universality and susceptibility to circumvention. Improvement on these methods brought about the new category of using two or more biometric features, called the multimodal biometrics which has been developed recently. In this work, we present a literature review on the unimodal and multimodal biometric system, the multimodal biometric system architecture and the methodologies behind them.

2.0 LITERATURE REVIEW

2.1 Biometric System

Biometric is the measurement of biological and/or physical characteristics of an individual which is unique for identification and verification of an individual. It is a technology that uses the physical and/or behavioural characteristics of people to uniquely identify them. This method implements two processes, which are Enrolment an Authentication [5].Figure 1 shows the biometric system which is made up of two basic modes of biometric system of which are the enrolment and authentication modes. Enrolment is the process of registering or collecting a new user's biometric information and storing it into the biometric database for the use of authentication and identification. The first time an individual uses a biometric system is called the enrolment process. When the user places his fingers on the biometric device, the prints on the finger is been extracted by the feature extractor and stored into the biometric database which will in turn serve as a match to the person's print the next time he or she checks in on the device. This will then give a decision that the user is valid or invalid. In the diagram above, the first block (sensor) is the line between the real world and the system. It takes its objects as image(s) as an image acquisition system, though it can change in respect to the desired characteristics. The second block performs all processing of the objects or images retrieved from the sensor. It removes all redundancies such as background noise to use some kind of normalization. In the third phase, the correct features of the user gotten from the retrieved object or image is then extracted correctly in this phase in an optimal way which then creates a specific template of the object before storage and testing. During the matching stage, the obtained template is sent to a matcher that compares the taken template with the existing ones to see if anyone matches the template.

Authentication is the process by which the system performs a one-to-one comparison of a captured biometric with a specific template stored in the database in order to check for match and validity of the user, if the user is actually who they claim to be. Authentication process involves three steps. The first step is the generation of reference model and storage of model to database. The second step involves matching of samples with reference models to generate genuine and impostor score and calculate the threshold and lastly is Testing.

Identification mode involves the process by which the system does a one-to-many comparison against a biometric database to fetch out the identity of an unknown individual [6]. This process can only be achieved if the threshold contains the template in the biometric database for the biometric sample that was freshly obtained. Identification mode can be used for either positive recognition or negative recognition.

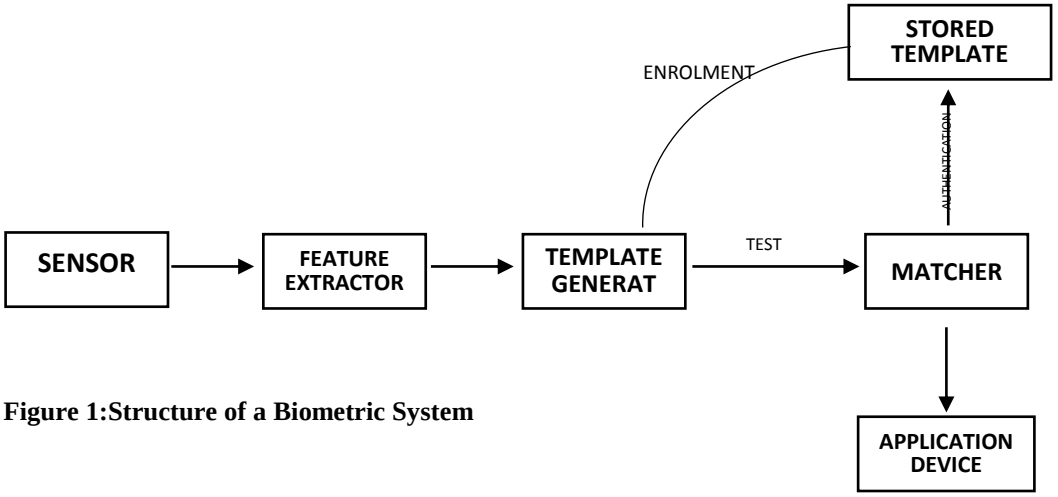


Figure 1:Structure of a Biometric System

2.2Features of a Biometric System.

The effectiveness of a biometric system is usually assessed on the following:

(a) **False Match Rate (FMR)**: FMRcan be defined as the expected ratio that the downloaded sample will be falsely matched to the template in the database, but will not be the test user pattern. FMR also measures the percentage of invalid inputs that are incorrectly accepted. If the indicator is high, there is high risk than unauthorized user can be granted access to the system parameters. FMR belongs to the group of matching errors.

(b) **False Rejection Rate (FRR)**: FRRinvolves the probability that the system fails to detect a match between the sample and the matching templates in the database. This measures the percentage of valid inputs that are incorrectly rejected.

(c) **Failure to Enrol Rate (FTE):**FTEmeasures the rate at which an attempt of creating a template of the input biometric trait is unsuccessful. This is common mostly when there are low quality inputs.

(d) **Failure to Capture Rate (FTC):**FTC is the probability that the system fails to capture a biometric trait input when presented correctly.

(e) **Equal Error Rate (EER).**EER is defined as the rate at which both error due to acceptance and rejection are equal. The EER is a quick way to compare the accuracy of devices with different Relative Operating Characteristic (ROC) curves. This means that, the device with the lowest EER is most accurate.

2.3 Categories f Biometric System

Biometric system can be categorised into two (2) systems:

1. Unimodal Biometric System
2. Multi-Biometric System.

2.3.1 Unimodal Biometric System

Unimodal system is a biometric identification system that uses a single biometric trait of the individual for identification and verification [7].Unimodal biometric system uses only one sensor to generate and store the biometric traits of an individual. Despite that biometric system has many inherent advantages, large scale deployment of biometric identification systems has been vulnerable due to some reasons. Hypothetically, unimodal biometric identification only accepts authorised user access whichmight seem very proficient but in reality, there are numerous challenges when enrolling large populations using the single biometric (unimodal) system [7, 8].

2.3.2 Limitations of Unimodal Biometric System

Unimodal biometric system of identification and verification has its limitations. However, it has an edge over traditional security methods because it cannot be stolen or shared. The Unimodal Biometrics systems installed in real world applications must encounter some of these variety of problems, which includes:

- **Uniqueness:** This means the trait should be different for individual irrespective of the population such that it can be appropriately distinguished from one another. While a biometric trait is expected to vary across individuals, there may be large similarities in the feature sets used to represent those traits, which means that, every biometric trait may have some theoretical upper bound in terms of discrimination capability.
- **Noise in sensed data:** The examples of noisy inputs of data includes: fingerprint with a scar, defective or improperly maintained sensors, voice altered by weather, poor illuminated face in face recognition system and so on. All these results to the biometric data to be incorrectly matched with templates in the database follow-on in giving access to a wrong user and declining the authorized user.
- **Non-universality:** It is obvious that every user is expected to possess its biometric trait and it may be impossible for some users whom their biometric feature cannot be extracted due to the poor quality of the ridges. Therefore, there is Failure to Enrol (FTE) rate associated with using a single biometric system.
- **Durability**: This relates to the way in which a trait changes over time. Precisely, a quality of the system may change over time with respect to the specific matching algorithm or set of rules.
- **Social acceptability:** This involves the waypeople or individual accept the technology such that they are prepared to allow their biometrics to be captured and assessed.
- Ease of circumvention refers to the ease with which a trait might be imitated using artefact or substitute.
- Other limitations are Population coverage, Size of equipment, Identity theft deterrence and Cost.

2.3.3 Multi-Biometric System

The multi-biometric system is a system that utilises more than one behavioural or physiological characteristics[9] and rely on the evidence presented by multiple sources of biometric information. The multi-biometric system has been introduced with the aim of reducing the FAR and FRR as well as to avoid spoof attacks. It is a system expected to be more reliable due to the presence of multiple, fairly independent pieces of evidence. Multibiometric systems address the problem of non-universality, since multiple traits can ensure sufficient population coverage. Furthermore, multi-biometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user [10].

Multi algorithmic biometric systems use two or more algorithms for processing a single sample of a single sensor. Multi-instance biometric systems process uses two or more different instances of the same biometric characteristics like multiple fingerprints of the same person. Multisensorial biometric systems use two or more distinctly different sensors to process the same characteristic. Different combinations of the biometric characteristics of the same individual can be used [2]. Multi-biometric systems are expected to be reliable due to presence of multiple, fairly independent pieces of evidence [8].

In Multi-Biometric System, there are variety of factors to consider in designing the system. These factors include: Choice and number of biometric traits., levels in the biometric system at which integration of information provided by the multiple traits should be done, methodology of integration, cost and matching performance.

The multi-biometric system is made up of different parts. Firstly, a multi-sensor system that allows obtaining data from various sensors using one biometric feature. Secondly, a system with multiple algorithms processing a single biometric feature. Thirdly, system consolidating multiple occurrences of the same body trait. Fourthly, system using multiple templates of the same biometric method obtained with the help of a single sensor and lastly a multimodal system combining information about the biometric features of the individual to establish his identity.Figure 2 depicts the Modal of Multi-Biometric System.

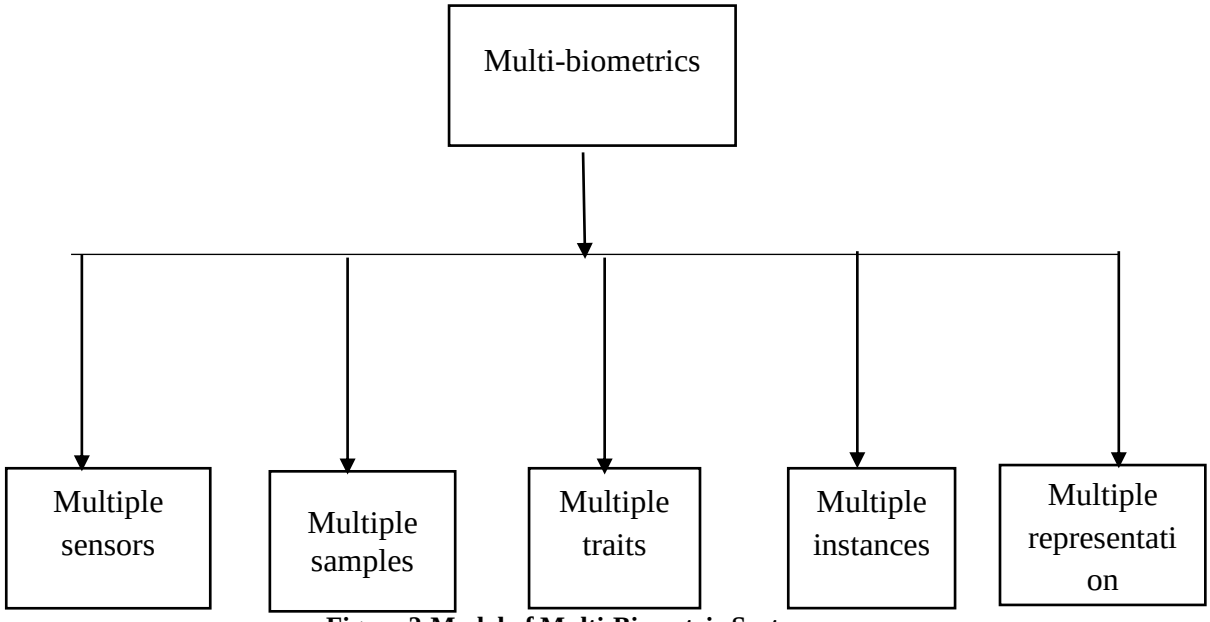


Figure 2:Modal of Multi-Biometric System

2.4 Approaches of Multi-Biometric System

1. **Multi-Sensor Systems:**Multi-Sensor Systems employ multiple sensors to capture a single biometric trait of an individual.
2. **Multi-Algorithmic Systems:**In Multi-Algorithmic Systems, it employs multiple feature extraction and/or multiple matching algorithms on the same biometric to improve the performance.
3. **Multi-Instance Systems:**Multi-Instance Systems use multiple instances of the same body trait. For instance, the use of multiple fingers for fingerprint verification.
4. **Multi-Sample Systems:** In order to account for variations of a biometric trait, a single sensor can be used to acquire multiple samples of the same trait [11].
5. **Multi-Modal Systems:** Multi-Modal Systems establish identity based on the evidence of multiple biometric traits.

2.5 Benefits of Multi-Biometric Systems

Mullti- biometric system is able to meet the stringent performance requirements imposed by various applications. Moreover, the system addresses the problem of non-universality, since multiple traits ensures sufficient population coverage [8] and also It provides anti-spoofing measures by making it difficult for an intruder to concurrently spoof the multiple biometric traits of a legitimate user.

2.6 Review of Related Works

According to Hanh *et al*. [12], it was proposed to extract face and fingerprint characteristics invariant to the rotation and scaling of Zernike moments (ZM). On who's basis is the fusion of facial features and fingerprints is realized. With the help of the unified Gabor filter, fingerprint codes and finger vein codes are generated. The extraction features were carried out by using a Supervised Local Canonical Correlation Analysis (SLCCA), and finally the NN-classifier [13].

In system described by Froba*et al.*,[14], texture parameters are extracted based on Gabor filters. Fusion of the palm print features is based on the wavelets which utilizes a Baud limited image product. The PCA is used to extract features of palm and face images. Fusion technique concatenated the feature vectors of the face and palm modalities into one fused vector, and feature selection is performed [15]

According to Al-Waisy, [16], the inner and outer boundaries of the iris region are detected using an integra-differential operator. At the end of this process, the iris template is transferred into normalized rom using Daugman's rubber sheet method. Then, a 2D Gabor filter is used to extract the iris features and the Hamming distance algorithm is used for decision making. As functioning as Daugman's system is, it has a limitation which is the requirement of a high-resolution camera to capture the iris image and its accuracy decreases when the iris is not in an imaging conducive area because of sensitivity and lightning conditions [17].

3.0 METHODOLOGY

3.1 Fusion Levels in Multi-Modal Biometric System

Biometric fusion can be defined as the process of combining the classification results of each biometric channel. Fusion can occur at different levels which are matching score level, sensor level, feature level, rank level and decision level [2,18].Figure 3depicts the various levels of fusion in a multimodalbiometric system.

In sensor level fusion, data from various sensors form one vector of which fusion of information obtained from the various sensors combine to form a single biometric feature. In the feature level fusion, the feature vectors of different biometrics are combined to form a single feature vector. In matching score level fusion, individual matching scores are found and a decision is made of the score to be used for classification or verification. In decision level fusion individual biometrics are used to make individual decisions and then a combined decision is arrived at and the resultant vector defines two main classes, that is, rejection and acceptance. In rank level fusion, the classifier determines the rank of each registered biometric identity (Figure 4and Figure 5).

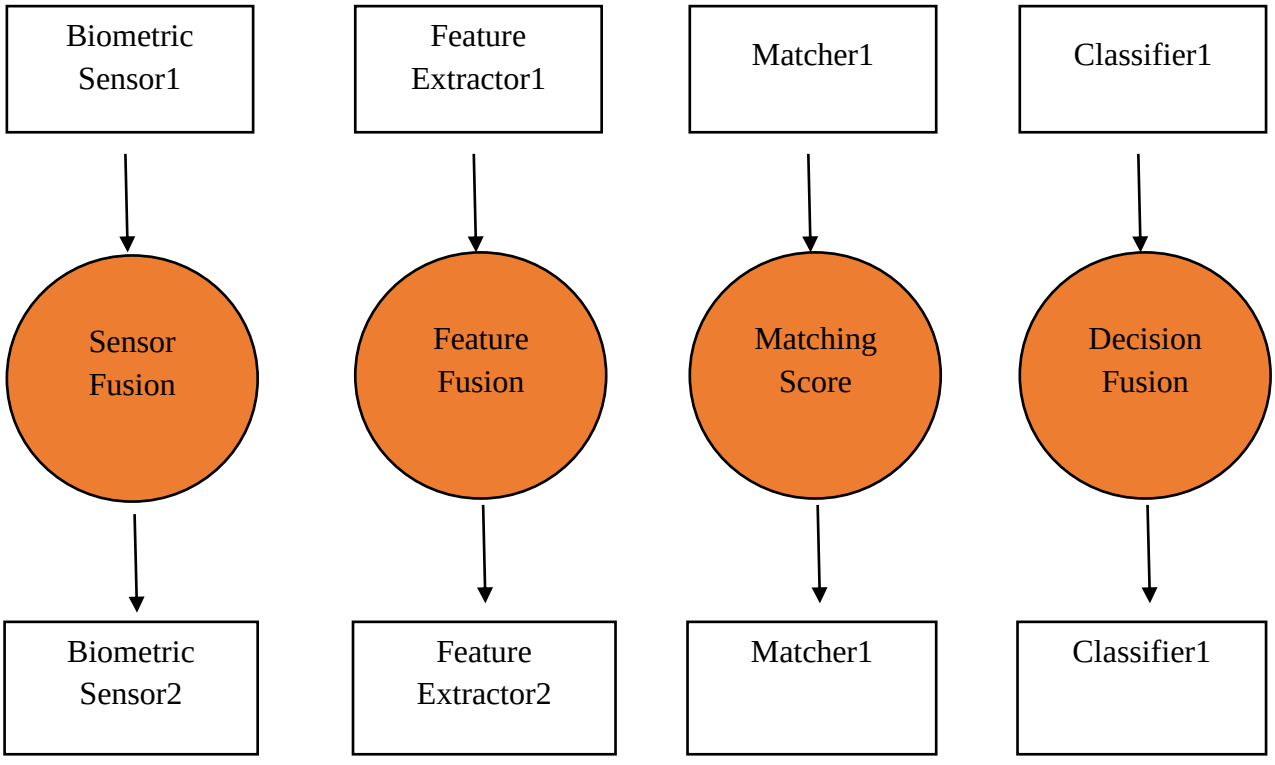


Figure 3: Fusion Levels in Multimodal Biometric System

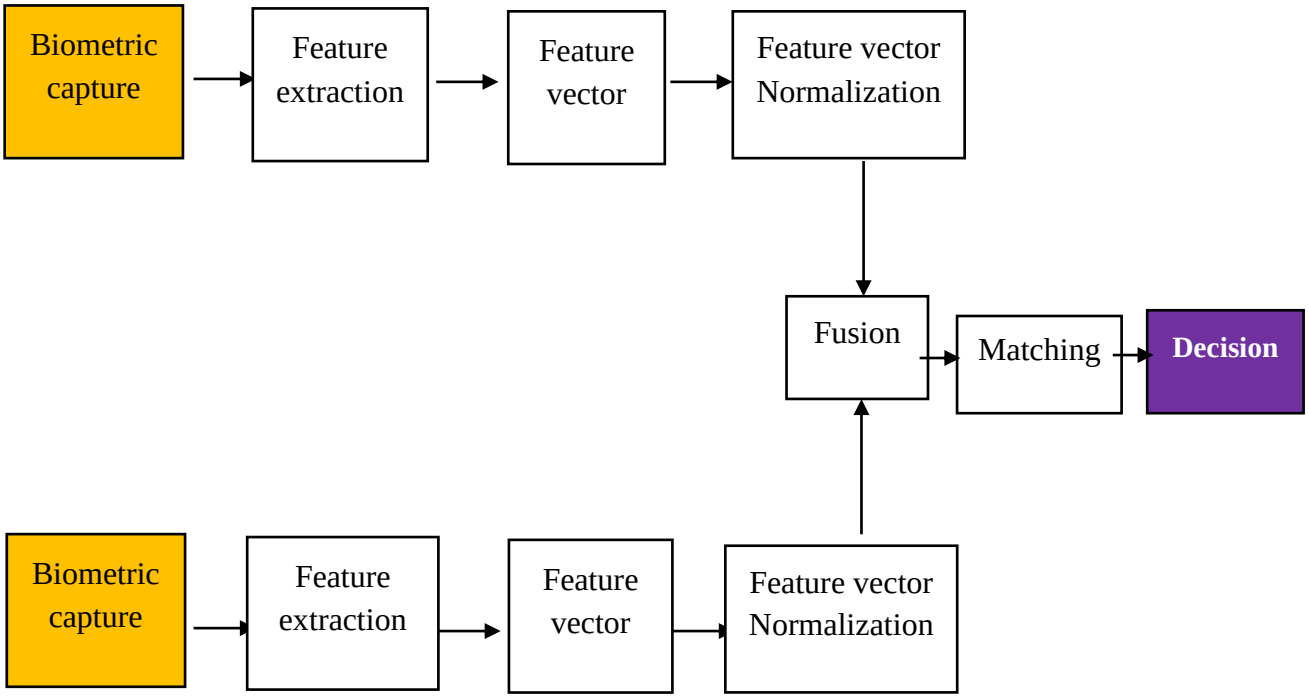


Figure 4: Feature level fusion

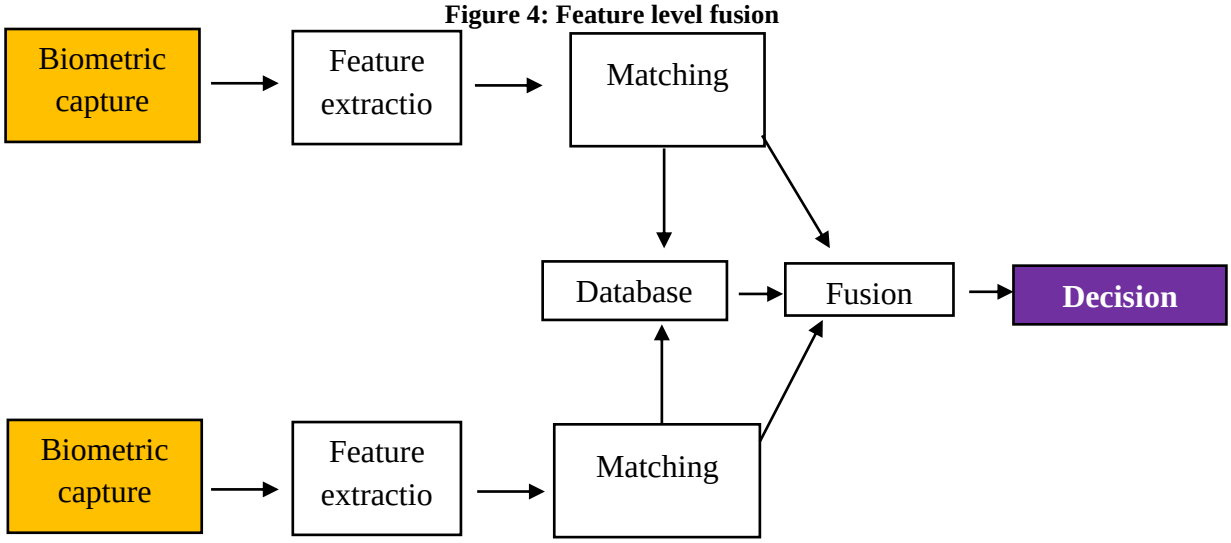


Figure 5: Rank level fusion

3.2 Architectural Model for Multi-Modal Biometric System

The multi-biometric system (dorsal vein + periocular + palm print) is presented in figure 3.4.

In this method, the first block is the pre-processing block, including noise elimination, Return On Investment (ROI) detection and normalization, and contrast normalization. For all three modalities, noise elimination for an image $f(x, y)$ is performed using median filtering operation [18].

$$F(x, y) = medium_{A1}\, f(x,y) = medium\ [f(x+r_2 y+s)] \quad (1)$$

where A1is the MF window.

Next step in pre-processing phase is Return On Investment (ROI) detection and normalization. This operation is quite different for dorsal vein images, palm print images, and periocular images. For dorsal vein images, we use distance transform to detect the dorsal image centre and build square ROI based on these centre coordinates [19]. The ROI design for palm print images is based on hand-specific points (finger valleys) and two angles [20]. The periocular region is detected based on the centre of the iris. Using the conventional algorithm for detecting the iris [5, 21] determined the centre of the iris and its diameter. The periocular area is a rectangle centred in the iris centre [22. 23].

After the Return On Investment (ROI) detection, we perform image size normalization and apply the contrast normalization by using CLACHE algorithm after which the image is divided into non-overlapping areas of equal sizes and histograms are obtained [5, 21]. Each histogram is then processed such that its height does not exceed the cut-off threshold. Figure 6, there are other processing blocks which includes feature extraction, feature selection, fusion and classification.

3.2.1. Gabor Feature Extraction

In biology models, the primary aspects of early visual processing in mammalian vision systems are the receptor fields which are modelled using the Gabor filters. Gabor functions are very similar to the receptive field profiles of a mammalian cortical simple cells. Imitation of mammalian vision system in object recognition systems leads to the efficiency of this feature extraction {5, 24}.

The 2D Gabor filter can be represented in this mathematical equation below:

$$Gab_{\infty,0}(x,y) = \frac{1}{2x\sigma_x\sigma_y} G_0(x,y) S_\infty 0(x,y) \quad (2)$$

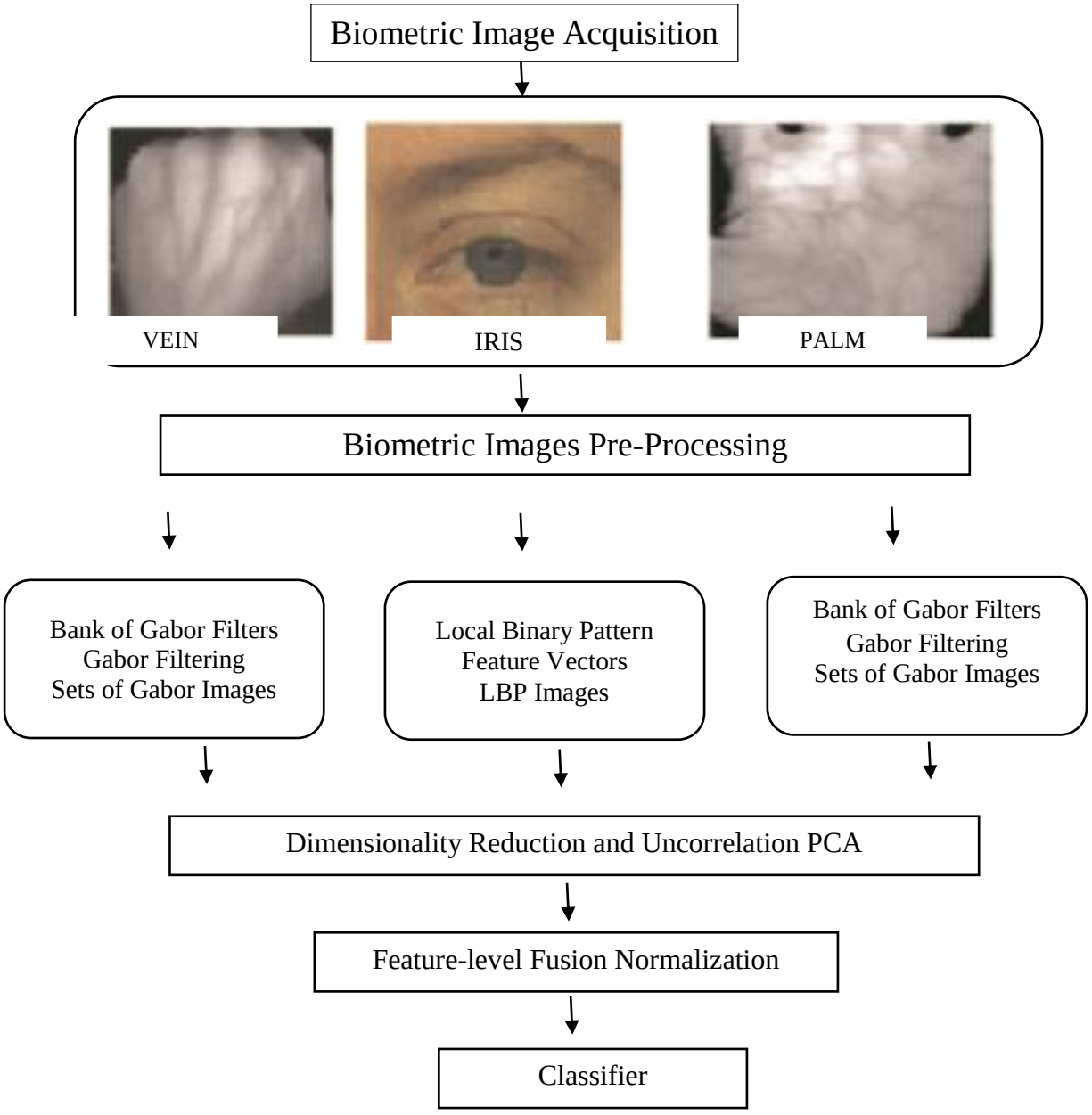
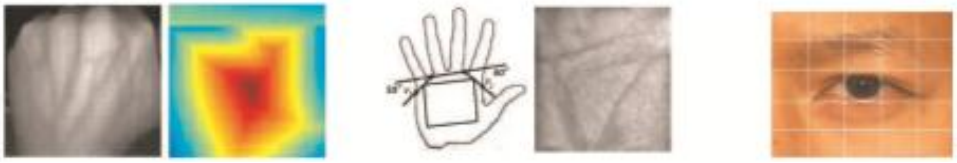


Figure 6: Biometric Image Acquisition



a) b) c)

Figure 7.ROI area for dorsal vein images (a), palm prints images (b), periocular images (c).

Figure 8. Images after Normalization and after applying the CLACHE algorithm.

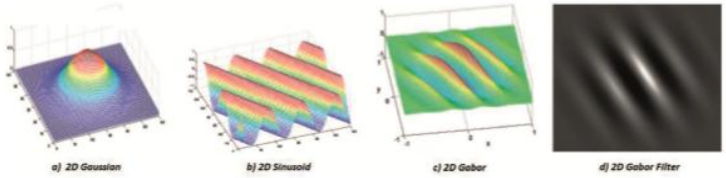


Figure 9. 2D functions and 2D Gabor Filter

3.2.2 Periocular Feature Extraction Using Local Binary Pattern (LBN) Method

The periocular area contains the iris, eyes, eyelids, eyelashes, and partially eyebrows. The LBP method can be used to describe the texture of the periocular area, and the feature vectors contains LBP features [25] as a texture descriptor. LBP divides the image into non-overlapping blocks of the same size. Local image features are calculated for each block separately. For a set of pixels belonging to a given block, the LBP values are calculated and then a histogram is created. The feature vectors (histograms) of each block are combined to form a global vector of features of the entire image. LBP analyses the local neighbourhood consisting of Gp points located on a circle with radius R and surrounding the centre point of Gc and checks whether the points of Gp are greater or lesser than the Gc point value. The LBP value of the Gc point is specified as follows:

$$LBP_{P,R} = \sum_{P=0}^{P-1} S(g_p - g_c)2^p \quad (3)$$

where Gp and Gc are the luminance values of the neighbourhood and centre point, respectively.

The idea of this operator is presented in the figure 10.

a) b)

Figure 10. The original image (a) and the resulting image of the LBP operator (b).

4.0 PROSPECTS OF MULTI-MODAL BIOMETRIC SYSTEM

Either in increasing the security, improving convenience or reducing cost, no biometric system can on its own achieve the goals of authentication and identification. Even the simplest most efficient and isolated biometric application is embedded in a larger system which involves the use of other technologies, environmental factors, business, security policies, political considerations and the likes, which in turn can reinforce the performance of any biometric system.

4.1 CHALLENGES OF MULTI-MODAL BIOMETRIC SYSTEM

However, multi modal biometric system is seen to be effectual, it has some challenges that are been looked into based on the upgrading and overhaul. These are some of the challenges:

- Designing inexpensive biometric sensors for integration with smartphones and wearable devices.
- Automating the process of generating adversarial spoof artifacts for a specific biometricsensorbycombining*3D*printingtechnologywith robotic process automation testing.
- Designing robust feature extraction and matching algorithms that can successfully operate on poor quality data.
- Developing methods to identify the original unmodified image from a given set of near-duplicatebiometricimagesandtoinferthetrailofphotometricandgeometricmodificationsthatproduced the other images.
- Developing methods for establishing the degree of correlation, at the biological level, between two or more biometrictraits.
- Designing novel sensors for acquiring biometric data from infants and toddlers.

5.0 CONCLUSION

Authenticating a user is not the same as identifying the user. Though traditional methods, using personal identification number (PIN), identification cards, and the likes can tell whether a user is allowed to have access into a system, yet it has not fully proved the existence and originality of the users. Biometric system as anauxiliary, with divers of methodologies and approaches has come in place to zero the Error Rates and give precise access to the authorised users. Theoretically, different approaches are being used to attack this problem of identification which brought about the use of unimodal and multimodal biometric systems.

Though unimodal system, still contains some characteristics that creates an open end for spoofing as a result of its non-universality, inconsistency in matching of the biometric traits and so on. Multi-modal biometric system serves as a solution to the difficulties in the unimodal biometric system. Multi-modal biometric system is useful in a large population as it reduces distortion of data, noise in sensed data and allows efficiency of multi users.

ACKNOWLEDGEMENT

A Eulogy to an Eminent Professor: Prof. John O.A. Idiodi

Unarguably some scholars are born and some are made. Permit me to rightly accord the 'born' perspective to my erudite scholar and mentor who I could unequivocally attest to the fact that my meeting with him in 2011 marked the beginning of my odyssey to fulfilling my life's destiny as ordained by God.

Our beloved Prof! You are not just a scholar for there are millions of scholars the world over, but you have unambiguously and meritoriously distinguished yourself from the millions of scholars. You have proved that a scholar can be a true mentor, a father, an advocate, a friend, confidant, and a colleague all at the same time. You are indeed a rare gem and posterity will ever attest to the positive influence you enshrined on the hearts and future of many of us who were opportune to pass through your mentorship.

Our Dear Professor, you will always remain revered and evergreen in our heart of hearts. You came! You saw! You conquered and won. Your meritorious and untainted service shall ever glow beyond the academic skies. We are convinced you are not tired, but as the chapter 3 and verse number 1 of the bible book of Ecclesiastes rightly averred: "To everything there is a season, and a time to every purpose under heaven…" Your service to humankind has outlasted many seasons but my Prof, it is our belief that your retirement from active service is a substantive evidence that cannot be controverted anywhere.

My Prof. I cannot possibly fathom all that you did but our collective prayer for you is this: May the good Lord bless you, strengthen you, cause his face to shine upon you, and add to you many more happier years in Jesus name. Amen. – Dr. A.S. Olayinka

REFERENCES

[1] Agarwal M. (2007). Design Approaches for Multimodal Biometric Systems, Ph.D. Thesis, IIT Kanpur, India

[2] Subramanian P., Nithin K., Rinku M., Sebastian and Najeeb U.R. (2016). ECE Department, AarupadaiVeedu Institute of Technology, CHENNAI (T.N.) INDIA.

[3] Pointer P. (2019). Why the sun is setting down on traditional identity verification methods. Itproportal.com.

[4] Naseem, I. Togneri, R and Bennamoun M. (2010). Linear regression for face recognition. IEEE transactions on pattern analysis and machine intelligence 32 (11), 2106

[5] Choras R.S. (2017). Biometric personal authentication using images of forearm vein patterns. In: International Conference on Signals and Systems; pp. 40-43

[6] Jain A.K. and Ross A. Introduction to biometrics. (2008). In Jain A.K; Flynn; pp.1-22. ISBN 978-0-387-71040-2.

[7] Thakkar D. (2019). Unimodal biometrics vs multimodal biometrics; biometric terminology, multimodal biometrics.

[8] Jain A.K., Ross A., and Prabhakar S. (2004). An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, January, 14(1)

[9] Nandakumar A.K Jain and A. Ross. (2005). Score normalization in multimodal biometric systems. Pattern Recognition, 38(12):2270–2285.

[10] Ross A. (2007). An introduction to multibiometrics. In: Proceedings of the 15th European Signal Processing Conference; pp. 20-24

[11] Banshidhar M., Mehrotra H., and Phalguni G. (2009). Multi-algorithmic iris authentication system. International Journal of Computer Science, 4:78–82.

[12] Long T.B., Thai L.H. and Hanh T. (2012) Multimodal biometric person authentication using fingerprint, face features. In: Anthony P, Ishizuka M, Lukose D, editors. Trends in Artificial Intelligence (LNCS 7458). Springer; pp. 613-624

[13] Ghouti L. and Bahjat A.A. (2009). Iris fusion for multibiometric systems. In: Proceedings of the IEEE International Symposium on Signal Processing and Information Technology; pp. 248-253

[14] Froba B., Rothe C. and Kublbeck C. (2000). Evaluation of sensor calibration in a biometric person recognition framework based on sensor fusion. In: Proceedings of 4th IEEE International Conference on Automatic Face & Gesture Recognition;. pp. 512-517

[15] Bokade G.U, Sapkal A.M. (2012). Feature level fusion of palm and face for secure recognition. International Journal of Electrical and Computer Engineering. 4(2):157

[16] Al-Waisy, A. S., Qahwaji, R., Ipson, P. and Al-Fahdawi, S. (2017). A Multimodal Biometric System for Personal Identification Based on Deep Learning Approaches. Seventh International Conference on Emerging Security Technologies. 163-168. 978-1-5386-4018-0/17/ ©2017 IEEE

[17] Ren X., Peng Z., Zeng Q., Peng C., Zhang J., Wu S. and Zeng Y. (2008). An improved method for Daugman's iris localization algorithm. ComputBiol Med 38(1):111–115

[18] Choras, R.S. (2018). A survey on methods of image processing and recognition for personal identification. In: Machine Learning and Biometrics, Rijeka, Croatia: InTech;

[19] Tanaka T. and Kubo N. (2004). Biometric authentication by hand vein patterns. In: Proceedings of the SICE Annual Conference; pp. 249–253

[20] Zhang D., Kong A., You J. and Wong M. (2018). Online palmprint identification. IEEE Transactions on Pattern Analysis and Machine Intelligence; 25:1041-1050

[21] Choras, R.S. (2019). Multimodal Biometrics for Person Authentication. IntechOpen, DOI: 10.5772/intechopen.85003.

[22] Sharma A., Verma S., Vatsa M. and Singh R. (2014). On cross spectral periocular recognition. In: Proceedings of International Conference on Image Processing;

[23] Woodard D., Pundlik S., Lyle J. and Miller P. (2010). Periocular region appearance cues for biometric identification. In: Computer Vision and Pattern Recognition Workshops; pp. 162-169

[24] Wang N., Li Q., El-Latif A.A.A., Yan X. and Niu X. (2013). A novel hybrid multibiometrics based on the fusion of dual iris, visible and thermal face images. In: Proceedings International Symposium on Biometrics and Security Technology; pp. 217-223

[25] Ojala T, Pietikäinen M. and Mäenpää T. (2002). Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Transactions on Pattern Analysis and Machine Intelligence;24(7):971-987