Multimodal Biometrics System, Nigeria Identity Solution.

Nwani, Emmanuel Chinweuba ORCID ID: 0000-0003-2270-4167
Department of Computer Science, Federal Polytechnic Oko, Anambra State, Nigeria.
emmanuel.nwani@federalpolyoko.edu.ng +234 803 3361 0029

ABSTRACT

Biometrics involves the scientific and technological exploration of biological data from the human body. This entails capturing data, deriving distinctive features, and matching them with a template set in the database. Research indicates that single-mode biometric systems suffer from drawbacks in terms of performance and precision. In contrast, multi-modal biometric systems surpass their single-mode counterparts in performance, even when dealing with intricate scenarios. We assess the precision and performance of multi-modal biometric authentication through cutting-edge Commercial Off-The-Shelf (COTS) products. Our focus is on biometric systems centered around fingerprints and facial recognition, along with the decision-making and fusion techniques employed within these systems. The advantages of these multi-modal systems over single-mode.

KEYWORDS: Authentication, *Evaluation, Normalization Multimodal Biometrics, Fusion, face, fingerprint and Matching score.*

1. INTRODUCTION

Over the past few decades, Multimodal biometric systems (MBS) have played a pivotal role in enhancing identification and human security. This widespread adoption has led to the integration of MBS into diverse fields of application. Some instances of these multimodal systems involve human-computer dialogue interactions, where users engage with PCs using voice, visual cues, or other pointing devices to accomplish specific tasks.

Multimodal biometric systems refer to systems that harness or possess the potential to harness multiple physiological or behavioral attributes for purposes such as enrollment, verification, or identification. At its core, a biometric system operates as a pattern recognition system. It examines and interprets human physiological characteristics, such as fingerprints, retinal and iris patterns, voice tones, facial features, and hand measurements, to establish authentication, as well as behavioral characteristics.

The inherent nature of biometric identifiers prevents them from being misplaced. Despite their inherent advantages, unimodal biometric solutions exhibit limitations in terms of accuracy, enrollment rates, and vulnerability to spoofing attacks. This vulnerability is evident across various application domains; an example is face recognition, where accuracy can be affected by factors like illumination and facial expressions. It's important to note that

biometric systems are not entirely impervious to spoof attacks.

Example is fingerprint spoofing with rubber. A recent report by the National Institute of Standards and Technology (NIST) to US concluded that approximately two percent of the population does not have a legible fingerprint (NIST Report to the United States Congress). Inspite of using unimodal biometric system that have poor performance and accuracy, we study and propose a new approach to the multimodal biometric system. This new Multimodal biometric systems perform better than unimodal biometric systems and are popular even more complex also

2. MULTIMODAL BIOMETRIC SYSTEM

Multimodal biometrics systems makes use of multiple physiological or behavioral traits for the purpose of enrolling, verifying, or identifying individuals. According to the National Institute of Standards and Technology NIST report, it is advised to adopt a system that incorporates multiple biometrics in a layered manner. The rationale behind integrating different modalities is to enhance the overall recognition rate. The aim of muti biometrics is to reduce one or more of the following;

- ✓ False accept rate (FAR)
- ✓ False reject rate (FRR)
- ✓ Failure to enroll rate (FTE)
- ✓ Susceptibility to artefacts or mimics

Multimodal biometric systems gather input from a singule or multiple sensors, measuring two or more distinct modalities of biometric traits. For example, a system with face recognition and fingerprint would be considered “multimodal” even if the “OR” rule was being applied, allowing users to be verified using either of the modalities (M. Indovina, U. Uludag, R. Snelick, A).

2.1. Multimodal algorithmic biometric systems

Multi algorithmic biometric systems take a single sample from a single sensor and process that sample with two or more different algorithms.

2.2. Multimodal instance biometric systems

Multi-instance biometric systems use one sensor or possibly more sensors to capture samples of two or more different instances of the same biometric characteristics. Example is capturing images from multiple fingers**.**

2.3. Multimodal sensorial biometric systems

Multi-sensorial biometric systems sample the same instance of a biometric trait with two or more distinctly different sensors. Processing of the multiple samples can be done with one algorithm or combination of algorithms. Example face recognition application could use both a visible light camera and an infrared camera coupled with specific frequency.

3. FUSION IN MULTIMODAL BIOMETRIC SYSTEMS

Biometric fusion refers to a mechanism capable of amalgamating classification

outcome from individual biometric channels. We need to design this fusion.

Multimodal biometric fusion combines measurements from different biometric traits to enhance the strengths. Fusion at matching score, rank and decision level has been extensively studied in the literature. Various levels of fusion are: Sensor level, feature level, matching score level and decision level.

Sensor level Fusion:

We combine the biometric traits taken from different sensors to form a composite biometric trait and process.

Feature level Fusion:

Signals coming from different biometric channels are first pre-processed, and Feature vectors are extracted separately, using specific algorithm and we combine these vectors to form a composite feature vector. This is useful in classification.

Matching score level fusion:

Rather than combining the feature vector, we process them separately and individual matching score is found, then depending on the accuracy of each biometric matching score which will be used for classification.

Decision level fusion:

Each modality is first pre-classified independently.

Multimodal biometric system can implement any of these fusion strategies or combination of them to improve the performance of the system; different levels of fusion are shown in below figure-I

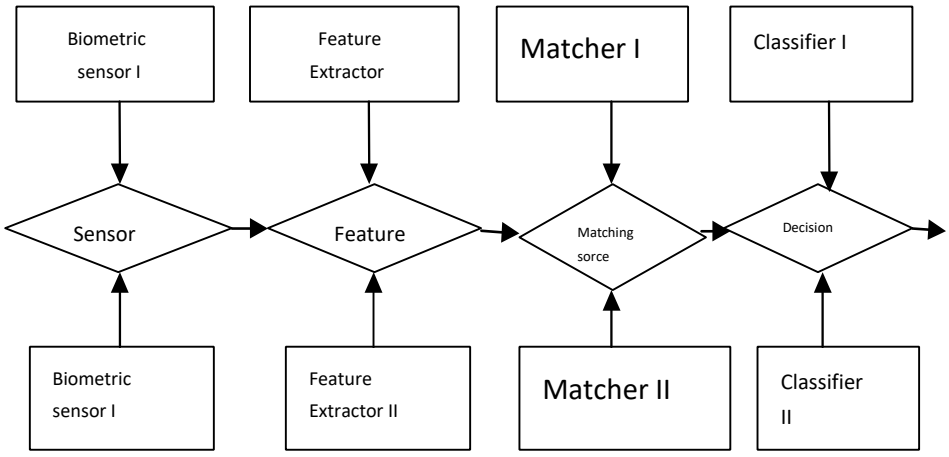


Figure –I. Fusion levels in multi modal biometric systems

3.1. Architecture

Discussing existing architecture, In a literature, A. Ross and A.K. Jain discussed a multimodal biometric system using fingerprint and face and proposed various levels of combinations of the fusion to

achieve greater and authentic result in Nigeria. This is shown in Figure-II

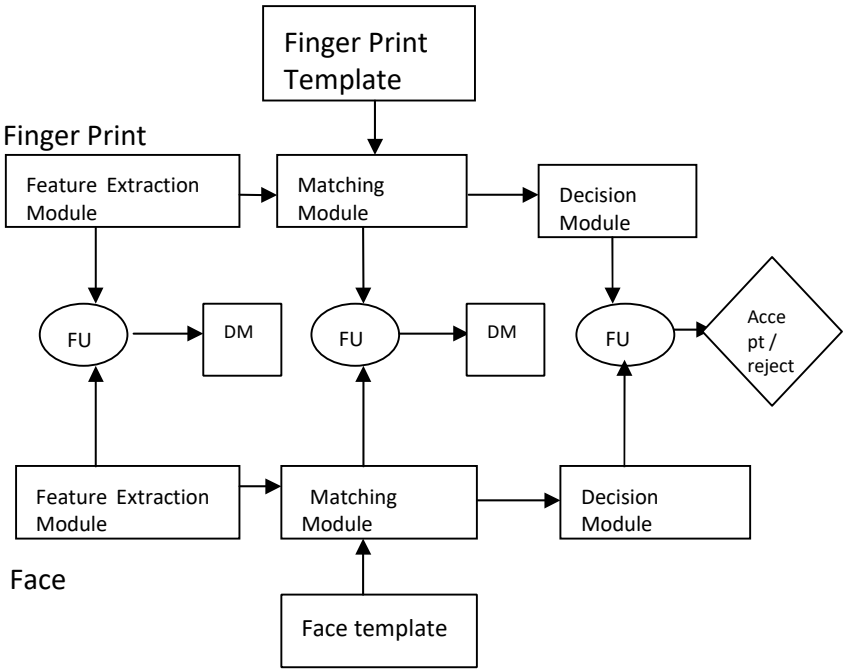


Figure – II Multimodal biometric system using face and fingerprint

(FU – fusion DM – Decision Module)

P.J. Huber has proposed a correlation Filter bank based fusion for multimodal biometric system; he used this approach for Face & Palm print biometrics. In Correlation Filter Bank, the unconstrained correlation filter trained for a specific modality is designed by optimizing the overall original correlation outputs. Therefore, the differences between Face & Palm print modalities have been taken into account and useful information in various modalities is fully exploited. PCA was used to reduce the dimensionality of feature set and then the designed correlation filter bank (CFB) was used for fusion. Fig. III shows the fusion network architecture proposed by them, the recognition rates achieved are in the range 0.9765 to 0.9964 with the proposed **method**

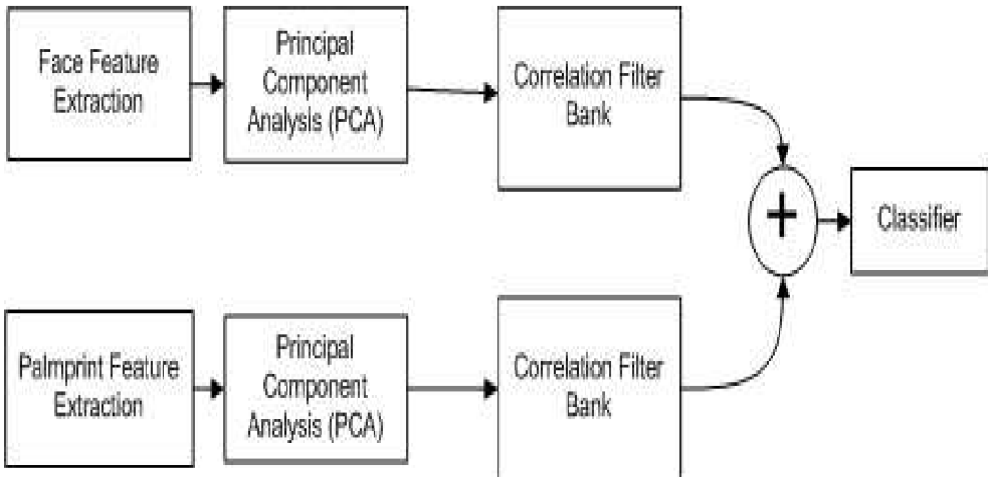


Figure III: Correlation Filter bank based fusion

3.2. Normalization

In this section, we present well-known normalization methods. We denote a raw matching score as s, from the set S of all scores for that matcher, and the corresponding normalized score as s'.

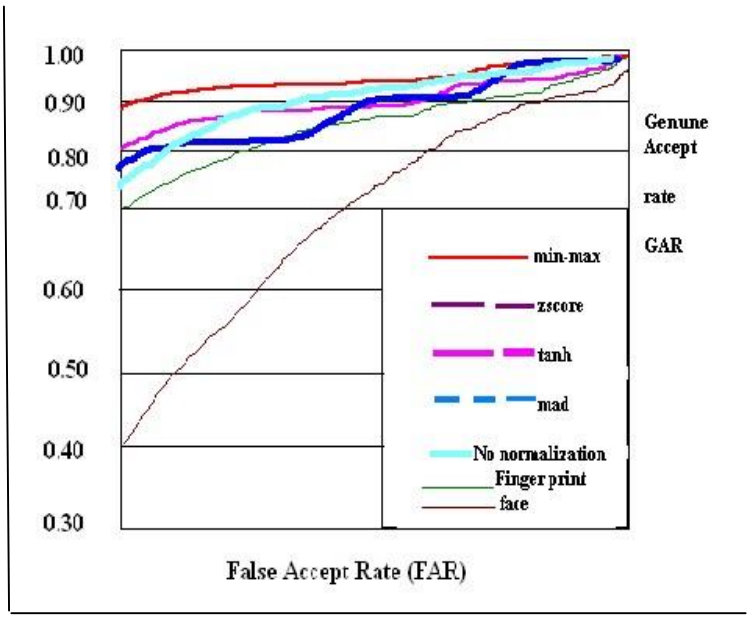
Min-Max : $s' = (s - min) / (max-min)$

Zscore : $s' = (s - mean)/(standard\ deviation)$

MAD : $s' = (s - median)/constant\ (median\ |\ -\ median|)$

tanh : $s' = .5[\ tanh\ (\ .01(s - mean)/(standard\ deviation))+1]$

Normalization addresses the problem of incomparable classifier output scores in different combination classification systems.



. Figure 4: simple sum rule with different normalizations

4. EXPERIMENTS

ROC (Receiver Operating Characteristic) curve implementation:

Performance statistics are computed from the real and fraud scores. Real scores are those that result from comparing elements in the target and query sets of the same subject. Fraud scores are those resulting from comparisons of different subjects. Use each fusion score as a threshold and compute the false-accept rate (FAR) and false-reject rate (FRR) by selecting those fraud scores and genuine scores, respectively, on the wrong side of this threshold and divide by the total number of scores used in the test. A mapping table of the threshold values and the corresponding error rates (FAR and FRR) are stored. The complement of the FRR (1 – FRR) is the Genuine accept-rate (GAR). The GAR and the FAR are plotted against each other to yield a ROC curve, a common system performance measure. We choose a desired operational point on the ROC curve and uses the FAR of that point to determine the corresponding threshold from the mapping table. Figure 4 shows a ROC (Receiver Operating Characteristic) curve for the simple sum fusion rule with various normalization techniques. Clearly the use of these fusion and normalization techniques enhances the performance significantly over the single-modal face or fingerprint classifiers. For example, at a FAR of 0.1% the simple sum fusion with the minmax normalization has a GAR of 94.9%, which is considerably better than that of face, 75.3%, and fingerprint, 83.0%. Also, using any of the normalization techniques in lieu of not normalizing the data proves beneficial. The simplest normalization technique, the min-max, yields the best performance in this example.

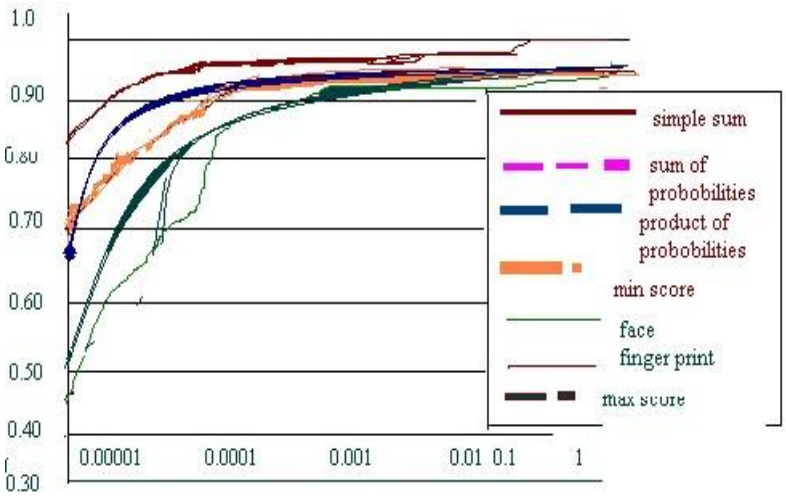


Figure 5 Min-Max Normalization with different fusions

Figure 5 illustrates the results of Min-Max normalization for a spectrum of fusion methods. The simple sum fusion method yields the best performance over the range of FARs. Interestingly, the Genuine-Accept Rate for sum and product probability rules falls off dramatically at a lower FAR. GAR for the spectrum of normalization and fusion techniques at FARs of 1% and 0.1% respectively. At 1% FAR, the sum of probabilities fusion works the best. However, these results do not hold true at a FAR of 0.1%. The simple sum rule generally performs well over the range of normalization techniques. These results demonstrate the utility of using multimodal biometric systems for achieving better matching performance. They also indicate that the method chosen for fusion has a significant impact on the resulting performance. In operational biometric systems, application requirements drive the selection of tolerable error rates and in both single modal and multimodal biometric systems, implementers are forced to make a trade-off between usability and security. In operational biometric systems, application requirements drive the selection of tolerable error rates and in both single-modal and multimodal biometric systems, implementers are forced to make a trade-off between usability and security.

5. CONCLUSION

In the context of Nigeria's circumstances, a comprehensive framework shall be established to evaluate the effectiveness of multimodal biometric systems. Extensive analysis was conducted using substantial datasets containing facial and fingerprint information, encompassing a variety of normalization and fusion techniques. The findings derived from this investigation indicate that multimodal biometric systems exhibit superior performance when compared to their unimodal counterparts.

An added advantage of implementing fusion at this level is its compatibility with existing proprietary biometric systems, eliminating the need for extensive modifications. This approach allows for the utilization of a standardized middleware layer to manage multimodal applications, requiring only minimal shared information.

In the upcoming phases, the focus will shift towards exploring alternative normalization and fusion methods, especially relevant within Nigeria's context. Notably, evaluations of single-mode biometrics have underscored the necessity of conducting tests on datasets comprising tens of thousands of subjects for accurate performance assessment. It's emphasized that drawing conclusions from tests conducted on small subject groups can't reliably predict system scalability. To address this, future plans involve expanding test databases to achieve these larger scales.

Furthermore, as part of evaluating the feasibility of implementing such systems on a larger scale, these tests will be conducted using Commercial Off-The-Shelf (COTS) products, aligning with practical deployment scenarios in Nigeria.

REFERENCES

"Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and interoperability," NIST Report to the United States Congress, Nov.2002.

A. Ross and A.K. Jain, "Information Fusion in Biometrics," Pattern Recognition Letters, vol. 24, no. 13, pp. 2115-2125, 2003.

A.K. Jain and A. Ross, "Learning User-Specific Parameters in a Multibiometric System," Proc. IEEE Int'l Conf. Image Processing, pp. 57-60, Sept. 2002.

Biometrics: Personal Identification in networked Society, A.K. Jain, R. Bolle, and S. Pankanti, eds., Kluwer Academic, 1999.

C. Lupu, V Lupu, "Multimodal Biometrics for Access Control in an Intelligent Car", 3rd International Symposium on Computational. Intelligence and Intelligent Informatics - ISCIII 2007 - Agadir, Morocco, March 28-30, 2007.

D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer,2003.

G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds, "Sheeps, Goats, Lambs and Wolves: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation," Proc. ICSLD 98, Nov. 1998.

G.Feng, K. Dong, D. Hu and David Zhang, "When Faces Are Combined with Palmprints: "A

J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas, "On Combining Classifiers," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 3, pp. 226- 239, Mar. 1998.

L. Hong and A.K. Jain, "Integrating Faces and Fingerprints for Personal Identification," IEEE Trans. Pattern Analysis and Machine Intelligence,

vol. 20, no. 12, pp. 1295-1307, Dec. 1998.

M. Indovina, U. Uludag, R. Snelick, A. Mink, and A. Jain, "Multimodal Biometric Authentication Methods: A COTS Approach,"

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

Novel Biometric Fusion Strategy, Proceedings of First International Conference, ICBA 2004, (2004), Springer, 701-707

P.J. Huber, Robust Statistics. Wiley, 1981.

R. Auckenthaler, M. Carey, and H. Lloyd-Thomas, "Score Normalization for Text-Independent Speaker Verification Systems," Digital Signal Processing, vol. 10, pp. 42-54, 2000.

R. Brunelli and D. Falavigna, "Person Identification Using Multiple Cues," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 17, no. 10, pp. 955- 966, Oct. 1995.

R.M. Bolle, S. Pankanti, and N.K. Ratha, "Evaluation Techniques for Biometrics-Based Authentication Systems (FRR)," Proc. 15th Int'l Conf. Pattern Recognition, vol. 2, pp. 831-837, Sept. 2000.

S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of Face and Speech Data for Person Identity Verification," IEEE Trans. Neural Networks, vol. 10, no. 5, pp. 1065-1075, 1999.

Teddy Ko , "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.