Information Fusion Schemes for Reliable Biometric System

Aranuwa, F. O[1*], Oriola. O[2] and Orimoloye, S.M[3]
[1,2,3]Department of Computer Science,
Adekunle Ajasin University
Akungba – Akoko, Ondo State, Nigeria
***E-mail**: felix.aranuwa@aaua.edu.ng
Phone: +2347031341911

ABSTRACT

Globally, biometric system is becoming increasingly more popular in many authentication applications due to its performance and the basic premise that every person can be identified by his or her intrinsic physiological or behavioral traits. The technology is largely used for identification, access control and surveillance system application. In many biometric systems, the choice and sources of evidence used are strongly dependent on the application scenario and the design decisions. Meanwhile, studies have revealed that a biometric system that uses a single biometric source or trait for authentication has this tendency to face with problems related to noise in sensed data, non-universality, susceptibility to spoof attacks and large intra-class variations. Therefore, it is believed that some of the shortcomings of uni-biometric systems can be overcome and much higher accuracy achieved by integrating the evidences from multiple biometric sources or traits for establishing identity. Researchers at different levels have proposed and combined the outputs of two or more classifiers in the domain. Yet, the issue of efficient information fusion of these evidences remains an obvious concept that attract research attention. Hence, this work investigated and presents different classifier fusion techniques and design level scenarios that are viable for reliable biometric recognition system. Based on the research investigation, Dempster Shafer's rule of combination and fusion at the match-score level were considered the preferred information fusion technique and design scheme respectively due to their pragmatic and performance physiognomies.

Keywords: Information fusion, Spoof attacks, Multiple Biometrics, Authentication, Security systems

24th iSTEAMS GoingGlobal Multidisciplinary Conference Proceedings Reference Format
Aranuwa, F. O, Oriola. O. & Orimoloye, S.M. (2020): Information Fusion Schemes for Reliable Biometric System. Proceedings of the 24th iSTEAMS GoingGlobal Multidisciplinary Conference Proceedings. The University of Ghana/Council for Scientific & Industrial Research Ghana – Vitually Stationed in June, 2020. Pp 87-96. www.isteams.net/ghana2020

1. BACKGROUND TO THE STUDY

Biometric can be described as a technology that uses the biological characteristics of a person to identify him or her. The term biometrics is derived from the Greek words' bio meaning life and metric meaning to measure [1]. Biometric identifiers are often categorized as physiological and behavioral characteristics [2]. The physiological characteristics are related to the shape or the structural pattern of the body. Examples include, but not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent, while behavioral characteristics are related to the behavioral pattern of a person, example include, but not limited to typing rhythm, gait, and voice [3].

According to [4], the technology globally has emerged as a reliable and highly secure identification and personal verification solutions in our environment today because of its performance, uniqueness and consistency over time. Notable application areas include: access control, authentication, forensic investigation and so on. In many biometric systems, the choice and sources of evidence to be used are strongly dependent on the application scenario and the design decisions. By application strategy, when a single trait is used in any application it is referred to as uni-biometric system, while combination of two or more sources or traits in an application is referred to as multiple biometrics [5].

1.1 Research Problem

Combination of multiple modalities in biometric is considered a good strategy to improve its performance and reliability as it is considered to be intrinsically robust against noisy data and spoof attacks [6]. However, the issue of efficient information integration/fusion of these evidences obtained from multiple traits or sources remains an obvious concept that attract research attention. Hence, this research work investigated and presents different classifier fusion schemes and design scenarios viable for reliable biometric recognition system.

1.2 Research Objective

The goal of this work is to investigate and presents different classifier fusion techniques and design scenarios that are viable for reliable multimodal biometric recognition system

2. BIOMETRIC PROCESSING FRAMEWORKS

2.1 Biometric Processing Modes

Generally, biometric system involves two basic biometric processing modes namely, the enrolment and verification modes. The two basic modes involve sub stages for its processes as depicted in Figure1.

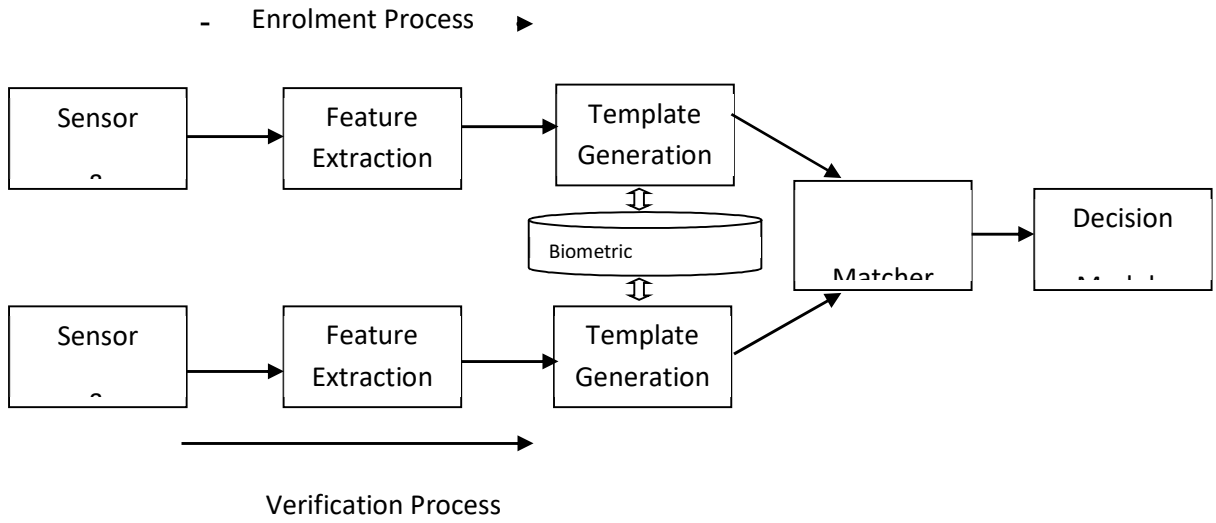

Figure 1: Generic Biometric Processing Modes and Stages

During enrolment process, biometric information from an individual is captured and stored in the biometric repository. In subsequent uses, biometric information is retrieved and compared with the information stored at the time of enrolment to validate or confirm whether the individual is the person claim to be during verification. According to [7], five modules are involved in each mode, the first is the sensor module which involves the capturing of biometric data from an individual using an appropriate device, the second is the feature extraction responsible for the processing and extraction of salient features from the data acquired.

The third module is the biometric repository that house the reference models called (template) for all the users in the model database. The template for each user is labelled with its confidence score for confirmation during the verification process. The fourth is the matching module, this module compares a claimed identity with the reference models stored in the database to generate match scores. The fifth is the decision module which uses the match scores generated in the match module to validate a claimed identity and determine whether to reject or accept the claim.

2.2 Information Fusion Schemes in Multiple-Biometric

Systems Sources and fusion scenario in multiple biometric systems can be classified into one of the following six categories: multiple sensors, multiple representations, multiple samples, multiple instances, multiple traits and hybrid [4]. The fusion of evidences from these sources generally can take place at four major levels, namely: the sensor level, feature level, score level and decision level. These levels are broadly categorized into: pre-classification scheme or fusion before matching and post-classification scheme or fusion after matching [8;5]. Figure 2 shows the broad classification of fusion levels.

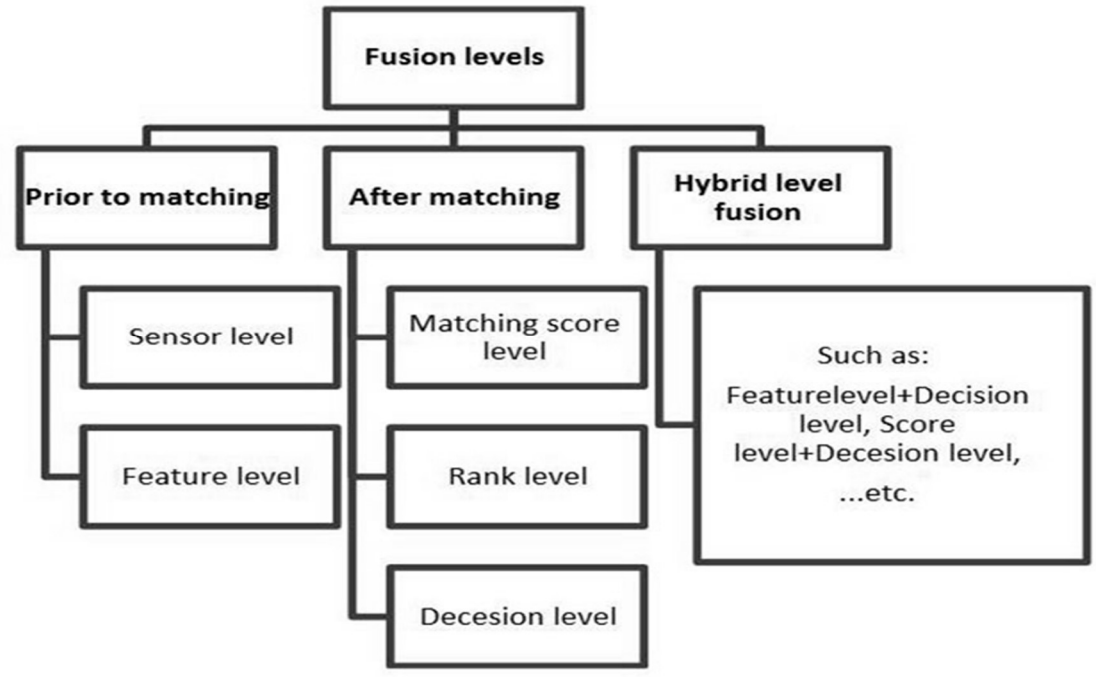

Figure 2: Categories of fusion levels
Source: [5]

2.3 Fusion Level Classifications

The fusion level classifications considered are discussed below

2.3.1 Fusion prior to matching (Pre-classification)

Fusion levels in this category consolidate evidences before matching. They are:

(a). The sensor level fusion: In this level, biometric data are consolidated at sensor level and new biometric data generated out of this merger. The data may be sampled from a single sensor or multiple compatible sensors. This level of fusion is also known as data level fusion or image level fusion. Fusion at this level may not be possible if the data instances and resolution are incompatible. For example: Fusion of infrared (IR) and visible face Images for face recognition.

(b). Feature level fusion: In feature level fusion, feature sets originating from multiple information sources are integrated into a new feature set. Feature set from this level contains richer information about the input biometric data than any other levels. However, integration at this level is difficult to achieve in practice because concatenating two features at this level may lead to dimensionality problem thereby required specific fusion algorithm to form a composite feature set.

2.3.2 Fusion after matching (Post- classification)

This fusion scheme integrates evidences after matching. The following fusion levels belongs to this category:

(a). Match-Score level fusion: In this level of fusion, match scores generated by ultiple classifiers pertaining to different modalities indicating degree of similarity (differences) between the input and enrolled templates are consolidated to reach the final decision. Integration of information at the matching score level is preferred in many applications as it offers the best tradeoff between information content and the ease in fusion.

(b). Rank level fusion: In rank level fusion, each biometric sub-system assigns a rank to each enrolled identity and the ranks from the subsystems are combined to obtain a new rank for each identity. Ties are broken randomly in this level to arrive at a strict ranking order and the final decision is made based on the combined ranks leading to computational complexity.

(c). Decision level fusion: Decision level fusion is performed using the decisions output by the biometric matching components. Final Boolean result from every biometric subsystem is combined to obtain final recognition decision. In multi-modal biometric systems, final decision is made by obtaining individual decision of different processed biometric characteristics. The final results of multiple classifiers are combined via techniques such as majority voting. This level fusion is also called abstract level fusion as it uses decision from individually processed biometric modality. Fusion at this level is assumed to have loosed its rich contents before final decision is taken. Hence, it may not yield good result.

2.3.3 Hybrid Level Fusion

Hybrid category consists of fusion levels in which more than one fusion level are included. This can occur when different levels of fusion take place in different levels of system. For example, an arrangement in which two speaker recognition algorithms are combined with three face recognition algorithms at the match and rank levels. Thus, the system having multi-algorithmic as well as multiple modalities in its design.

From the investigation, integration at the feature level should have be more effective and provide better recognition results than other levels of fusion because the feature set contains richer information about the input biometric data than any other levels. However, integration at this level is difficult to achieve in practice because concatenating two features at this level may result in a feature vector with very large dimensionality leading to dimensionality problem. Very few researchers used fusion at feature level due to its complexity in mapping the compatibility of computation of different biometric character and larger dimensions in fused features. Consequently, integration of information at the matching score level is preferred as it offers the best tradeoff between information content and the ease in fusion [9;10].

3. BIOMETRIC INFORMATION FUSION METHODOLOGIES

Since multiple biometric systems are designed to use more than one source or trait of biometric characteristics, fusion methodology that will effectively and efficiently consolidates these evidences cannot be over emphasized. In this section, four different information fusion techniques based on their pragmatic characteristics, robustness and reliability were comparatively presented as follows:

(a). Linear summation Rule:

Linear summation rule also known as the simple summation rule is the most common combination scheme for combining score values from multiple systems. The scores from different systems is however required to be standardized. The standardization is learned from development dataset by estimating distributions score values from each system. The scores are then translated and scaled to have zero mean and unit variance [12;13;14]. The simple sum rule adds the scores of each classifier to calculate the fused score. This can be expressed in the equation stated below:

$$S = \sum_{i=1}^{N} si \quad \text{.....Equation (1)}$$

Where S*i* is the score from the i*th* classifier, assuming N classifiers.

(b). Logistic Regression

Another linear combination technique is the Logistic Regression. The generally adopted method of this technique is the ordinary least squares (OLS) because of its tradition and ease of computation [15]. Practically, the technique usually assigns weights ωi to each classifier's score considered in an experiment. For instance, the weight ωi given to the i-th classifier correspond to the means difference of the distributions for client and impostor scores for i-th classifier. The system normally performs better when the distributions relative to the clients and impostors are more separated and when their variance is smaller. The combination of such two classifiers, S'j for the test j, can be defined as a weighted sum rule as presented in equation 2:

$$S'^{j} = \sum_{i=1}^{j=2} \omega_i S'^{j} \quad \text{..... Equation (2)}$$

Meanwhile, OLS estimation of regression weights in the multiple regression are affected by the occurrence of outliers, non-normality, multicollinearity, and missing data. Additionally, the methods are difficult to interpret.

(c). Multi Layer Perceptron

Multi-layer Perceptron (MLP) is a supervised learning algorithm capable to learn non-linear models. It is a class of feedforward artificial neural network (ANN) that utilizes a supervised learning technique called backpropagation for training. They composed of an input layer, an output layer that makes a decision about the input, and in between those two, an arbitrary number of hidden layers that are the true computational engine of the MLP [11;16]. MLP is different from logistic regression, in that between the input and the output layer, there can be one or more non-linear layers, called hidden layers. Figure 3 shows example of MLP with scalar output.

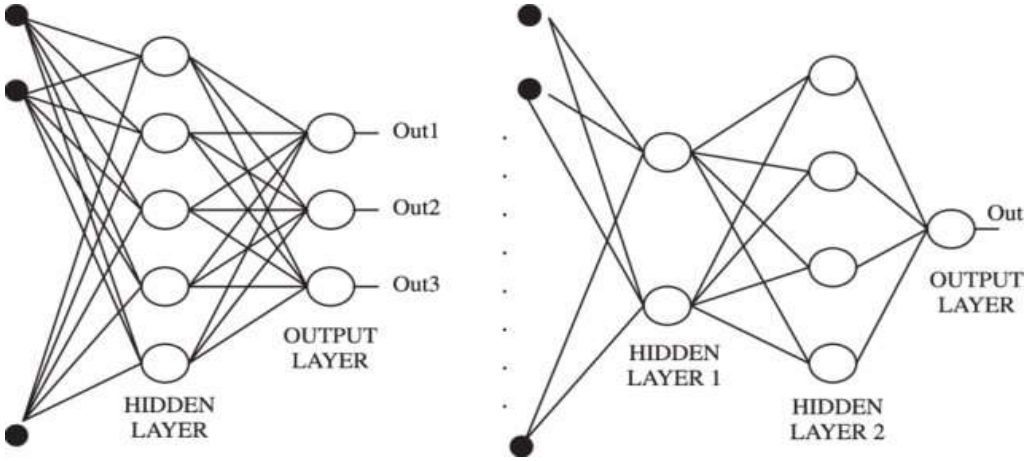

Figure 3: Examples of multi-layer perceptron
Sources: [16]

The perceptron rule is proven to converge on a solution from a finite number of iterations. In this case, MLP can be used to fuse the scores from two sources conveniently. The scores from these sources are considered as input features for the MLP classifier which are trained with client and impostor score samples on the development set. The hidden and output layers (the computational layers) are used with a double sigmoid as activation function as represented in equation 3.

$$s' = \frac{1}{1+\exp\left(-2\left(\frac{s-t}{r}\right)\right)}$$

$r = r_1$, if $s < t$

$r = r_2$, otherwise

.....Equation (3)

MLP is actually a popular machine learning solution, finding applications in diverse fields such as speech recognition, image recognition, and machine translation software, but this technique is usually faced with strong competition. For instance, the perceptron can only learn simple problems. Although, it can place a hyperplane in pattern space and move the plane until the error is reduced. But, uunfortunately this is only useful if the problem is linearly separable. This complexity has weakened this technique.

(d). Dempster's Shafer rule of combination

Another technique which is widely studied in classical classifier fusion but less applied in biometrics is the Dempster's rule of combination from the original conception of Dempster-Shafer theory (DST) [17]. Dempster–Shafer Rule of combination as proposed in Dempster Shafer Theory (DST) is a mathematical theory of evidence that provides a useful computational scheme for combining information from multiple sources [18]. It is a powerful tool for combining accumulative evidences and can update its priors regularly with the presence of new evidences in the database [6]. The evidence theory has been successfully applied in artificial intelligence systems, data fusion and pattern recognition [19].

The traditional interpretation of Dempster's rule is that it fuses separate argument beliefs from independent sources into a single belief [20]. It is an associative and commutative operation that maps a pair of belief functions defined both on the same space say Ω into a new belief function on Ω'. For instance, let bel_1 and bel_2 be two belief functions on Ω, with m_1 and m_2 as their related basic belief assignments (bba's). The combination (called the joint $m_{1,2}$) is calculated from the aggregation of two bba's m_1 and m_2 [20]. If A and B are used here for computing new belief function for the focal element C. Then their bel_1 and bel_2 can then be defined through its related bba m_1 and m_2 as follows:

$$m1,2(\,)\,C = \sum m1(\,)A \; Xm2(\,)B \;, \forall C \in \Omega$$
$$\frac{A \cap B = C}{1 - K} \qquad \text{.....Equation (4)}$$

The same result in equation (4) above can be conveniently represented with the commonality function as stated in equation (5):

$$\sum m1(A)\; Xm2\,(B) \qquad \text{..... Equation (5)}$$
$$A \cap B = \theta$$

In all the four techniques presented, Dempster Shafer's rule of combination is considered pragmatic enough particularly in high security applications. The evidence theory has been successfully applied in artificial intelligence systems, data fusion and pattern recognition systems, practically in [11; 18; 22] with good upshoot. Table 1 shows the summary of the fusion techniques considered and their performance physiognomies.

Table1: Summary of the fusion techniques considered and their performance physiognomies

S/N	Fusion Techniques	Efficiency	Robustness
1	Linear Summation	Yes	No
2	Logistic Regression	Yes	No
3	Multilayer Perceptron	Yes	No
4	Dempster's Shafer Rule of Combination	Yes	Yes

4. CONCLUSION

The quest for a viable fusion scheme to combine the evidences obtained from multiple sources and traits (Multiple Biometric) motivated this research work. The work investigated different classifier fusion schemes and design scenarios that are viable for reliable biometric recognition system. Based on the investigation on performance characteristics and application scenario, Dempster Shafer's rule of combination and fusion at the match-score level were considered the preferred information fusion technique and design scheme respectively.

6. ACKNOWLEDGMENT

Special acknowledgement to Tertiary Education Trust Fund (TETfund) and Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria for sponsoring this research work.

REFERENCES

[1] Ashok, J, Shivashankar, V and Mudiraj P.V.G.S.An Overview of Biometrics. International Journal on Computer Science and Engineering (IJCSE) 2(7). 2010, 2402-2408.

[2] Jain, A. K. and Ross, A. Introduction to Biometrics 2008. In Jain, AK; Flynn; Ross, A (eds.). Handbook of Biometrics. Springer. 1–22. ISBN 978-0-387-71040-2. Archived from the original on 9 March 2011.

[3] Poddar, A; Sahidullah, M and Saha, G. Speaker Verification with Short Utterances: A Review of Challenges, Trends and Opportunities. IET Biometrics 2018. 7:2: 91–101. doi:10.1049/iet-bmt.2017.0065.

[4] Aranuwa, F. O. Multiple Biometric Systems: Design Approach and Application Scenario. Elixir International Journal for Computer Science and Engineering. Roma, Italy 2014: 73:1, 26015-26019.

[5] Thakkar, D. Multi-biometric Fusion Techniques Improving Identification. Senior Product Manager at Bayometric 2019. www.bayometric.com

[6] Soliman, H., Mohammed, A. S and Atwan, A. Feature Level Fusion of Palm Veins and Signature Biometrics, International Journal of Video & Image processing and Network Security IJVIPNS-IJENS 2012: 12:01: 28- 39.

[7] Jain, A. K. Microsoft ® Encarta ® 2008 ©, 1993-2007-Microsoft Corporation.

[8] Sanderson, C and Paliwal, K.K. Information fusion and person verification using speech and face information", Research Paper IDIAP-RR (2002): 02-33, IDIAP, September, 2002.

[9] Alsaade,F. Rahmoun, A. and Zahrani, M. On Improving Multimodal Biometrics Verification Using Genetic Algorithms In E-MEDISYS 2010: 10 Conference Programmme

[10] Haghighat, M. Abdel-Mottaleb, M. and Alhalabi W. Discriminant Correlation Analysis: Real-Time Feature Level Fusion for Multimodal Biometric Recognition. IEEE Transactions on Information Forensics and Security 2016. 11:9: 1984–1996.

[11] Aranuwa, F.O, Olabiyisi, S.O. & Omidiora, E.O. An Intelligent Classifier Fusion Technique for Improved Multimodal Biometric Authentication using Modified Dempster-Shafer Rule of Combination".Computing, Information Systems and Development Informatics (CISDI) Journal) (2013). Baton rouge, USA, 4:1: 1-8.

[12] Jiang, H, Xu-dong, W, Yang, D, Mu-ming, P, and Xiao-hui, Z. An arithmetic rule for spatial summation of excitatory and inhibitory inputs in pyramidal neurons. PNAS December 22, 2009 106 (51) 21906-21911; https://doi.org/10.1073/pnas.0912022106

[13] Bradley, S. A counterexample to three imprecise decision theories, *Theoria (*2019). 85:1 18–30.

[14] Bradley, S. How to choose among choice functions. *Proceedings of the Ninth International Symposium on Imprecise Probability: Theories and Applications (2015)*, 57–66 URL = <http://www.sipta.org/isipta15/data/paper/9.pdf>.

[15] Ho, K. Naugher, J. Outliers lie: An illustrative example of identifying outliers and applying robust models. *Multiple linear regression viewpoints*, 26(2) (2000), 2-6

[16] Wei H, Kin K Lai -Yoshiteru N, Shouyang W. Forecasting Foreign Exchange Rates with Artificial Neural Networks: A Review. International Journal of Information Technology and Decision Making 3(1):145-165 March 2004. DOI: 10.1142/S0219622004000969

[17] Smets, P. Data fusion in the Transferable Belief Model. Universite Libre deBruxelles, Belgium (2000). Retrieved from http://iridia.ulb.ac.be/psmets 7/1/2020.

[18] Brest, B. Workshop on Theory of Belief Functions (http:/bafas.iutlan.univrennes1.fr/belief2010/) 2010: (Brest, 1 April 2010).

[19] Guan, X., YI, X., and HE, Y (2005): An Improved Dempster-Shafer Algorithm for Resolving the Conflicting Evidences. International Journal of Information Technology 11:12: 200 -205.

[20] Josang, A., and Pope, S., Dempster's Rule as Seen by Little Coloured Balls University of Oslo (2012). Willey Publications, Inc.

[21] Dempster, A. P. Workshop on Theory of Belief Function. (http://bfas,iutlan.univrennes1.fr/belief 2010.

[22]. Aranuwa, F.O. Multilevel decision threshold authentication mechanism for efficient Multimodal Biometric Systems. Elixir International Journal for Computer Science and Engineering. Roma, Italy (2016):6 92(1), 38702-38705.