BERKELEY PUBLICATION
AND RESEARCH INTERNATIONAL
03.31.2020
Journal of Pure and Applied Science Vol. 12 No. 9

INFORMATION FUSION SCHEMES FOR RELIABLE BIOMETRIC SYSTEM

ARANUWA, F.O.
Department of Computer Science, Adekunle Ajasin University, Akungba – Akoko, Ondo State, Nigeria

ABSTRACT

Authentication by biometric system is becoming increasingly more popular in corporate and public security systems for monitoring, identification, investigation, access control and many more due to its performance and basic premise that every person can be accurately identified by his or her intrinsic physiological or behavioral traits. In any biometric system, 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

Introduction:

Biometric can be described as a technology that uses the biological characteristics of a person to identify an individual. 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 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 pattern of

ISSN: 1399-8466

accuracy achieved by integrating the evidences presented by 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*

behavior of a person, including but not limited to typing rhythm, gait, and voice [3].

The basic premise of biometric authentication is that every person can be accurately identified these intrinsic physical or behavioral traits. 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. The choice and sources of evidence used in biometric system are strongly dependent on the application scenario and the design decisions. When a single trait is used in an 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 or multimodal biometrics [5].

Combination of multiple modalities in biometric becomes 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 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 four different classifier fusion schemes and six design scenarios viable for reliable biometric recognition system.

LITERATURE REVIEW

Biometric Processing Modes

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

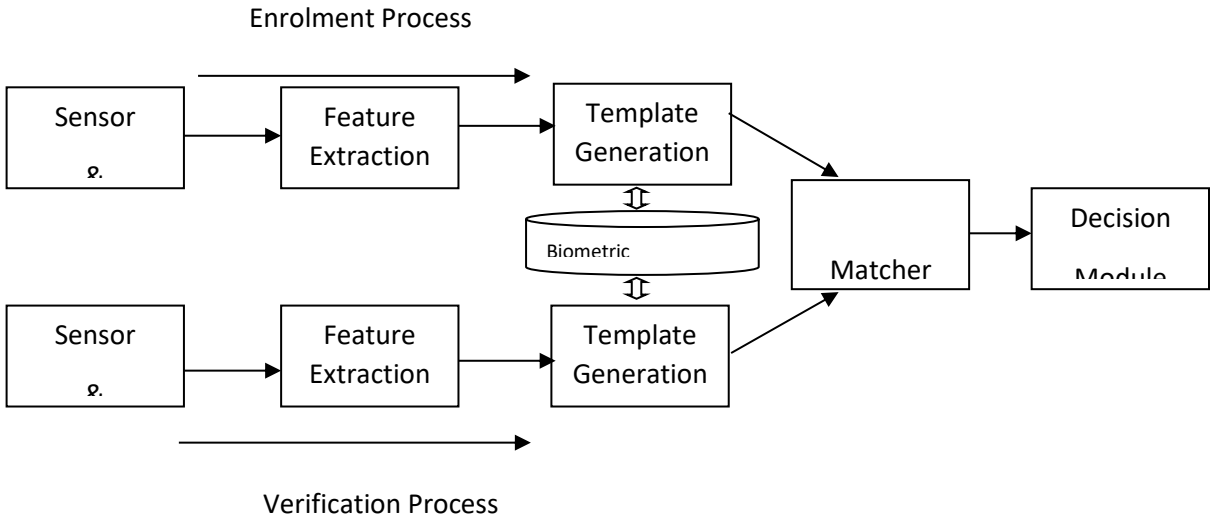

Figure 1: Generic Biometric Processing Modes and Stages

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 they 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.

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.

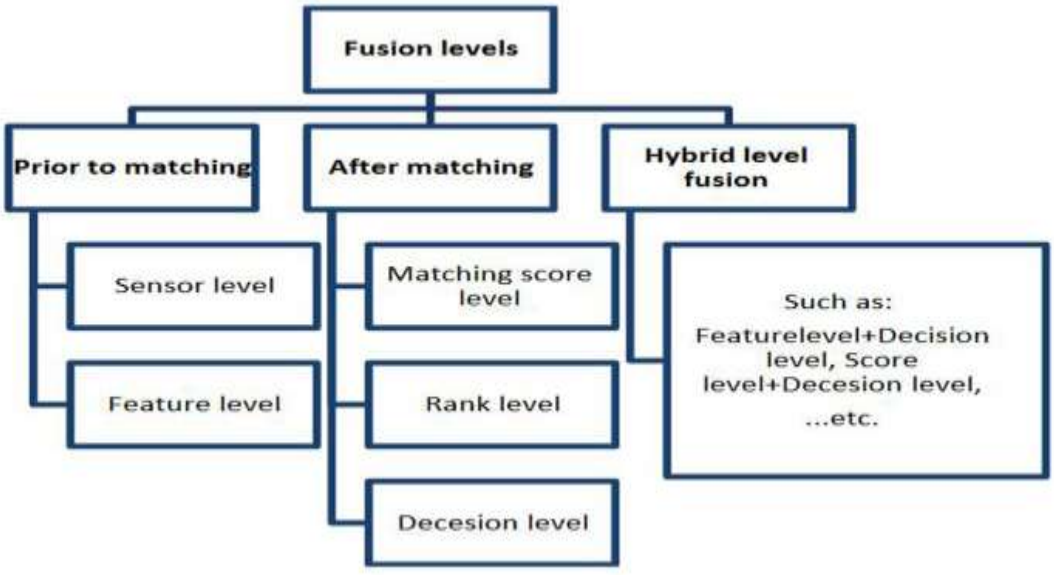

Figure 2: Categories of fusion levels Source: [5]

Analysis of the Fusion Levels

(a). Fusion prior to matching (Pre-classification)

Fusion levels in this category consolidate evidences before matching. The fusion levels that fall in this category are the following:

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.

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, forming a composite feature set.

(b). Fusion after matching (Post- classification)

The fusion scheme integrates evidences after matching. The following fusion levels are included in this category:

Match-Score level fusion:

In this level of fusion, match scores generated by multiple 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.

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 .

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 called abstract level fusion as it uses decision from individually processed biometric modality. Fusion at this levels is assumed to have loosed its rich contents before final decision is taken.

(c). **Hybrid level fusion**

Hybrid category consists of fusion levels in which more than one fusion levels 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.

In all, 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].

Biometric Information Fusion Methodologies

Since multi-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. The four fusion techniques as reported in [11] are presented as follows:

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 standandized. The standandaization 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]. 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 Si is the score from the ith classifier, assuming N classifiers.

Logistic Regression

Another linear combination technique is the Logistic Regression, this technique assigns weights to each classifier's score. In this method, the weight ωi given to the i-th classifier correspond to the means difference of the distributions for client and impostor scores for the i−th classifier. The

system performs better when the distributions relative to the clients and impostors are more separated and when their variance is smaller. In this case, the combination of two classifiers, S'^j for the test j, can be defined as a weighted sum rule as presented in equation 2:

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

Multi Layer Perceptron

Multi Layer Perceptrons (MLP), a non-linear method can also be used to fuse the scores from two sources or traits. The scores are considered as input features for the MLP classifier which are trained with client and impostor score samples on the development set. The MLPs used may have one input layer, one hidden layer with neurons, and one output layer. Hidden and output layers (the computational layers) are used with a double sigmoid as activation function as presented 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)

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) [13]. 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 [14]. 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 [15].

The traditional interpretation of Dempster's rule is that it fuses separate argument beliefs from independent sources into a single belief [16]. 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 [17]. If A and B are used here for computing new belief function for the focal element C. Their bel_1 and bel_2 can then be defined through its related bba m_1 and m_2 as follows:

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

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

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

In all the four techniques presented, Dempster Shafer's rule of combination is considered pragmatic enough particularly in high security applications.

CONCLUSION

A biometric system that consolidates evidences from multiple biometric sources or traits are considered intrinsically robust against noisy data and spoof attacks. The new paradigm promises matching accuracy, reliability with reasonably overall performance in many applications. The quest for a viable fusion scheme to combine the evidences obtained from multiple sources and traits motivated this research work. Therefore, 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.

ACKNOWLEDGMENT

Special acknowledgement goes to TETFUND and Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria for the financial supports towards the carrying out of this research study.

REFERENCE

Rouse, M. (2019). Biometric authentication. TechTarget's IT encyclopedia and learning center. techtarget.com. Retrieved online on 24th January 2020.

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

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

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

Thakkar D (2019). Multi-biometric Fusion Techniques Improving Identification. Senior Product Manager at Bayometric. www.bayometric.com

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

Jain, A. K. (2008), Microsoft ® Encarta ® 2008 ©, 1993-2007-Microsoft Corporation.

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

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

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

Aranuwa, F.O., Olabiyisi, S.O. & Omidiora, E.O (2013): "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). Baton rouge, USA, 4(1), 1-8.

Walley, P., (1991): "Statistical Reasoning with Imprecise Probabilities", Chapman and Hall, London, pp. 278-281.

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

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

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.

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

Dempster, A. P., (2010): Workshop on Theory of Belief Function. (http://bfas,iutlan.univrennes1.fr/belief2010.