Available online at www.elixirpublishers.com (Elixir International Journal)

Bio Technology

Elixir Bio Tech. 92 (2016) 38702-38705

ISSN: 2229-712X

Multilevel decision threshold authentication mechanism for efficient Multimodal Biometric Systems

Aranuwa Felix Ola

Adekunle Ajasin University, Akungba Akoko, Ondo State, Nigeria.

ARTICLE INFO

Article history:

Received: 12 December 2015;

Received in revised form:

29 February 2016;

Accepted: 2 March 2016;

Keywords

Multilevel,

Decision threshold

Recognitionand authentication,

Multimodalbiometrics,

Computational Complexity.

ABSTRACT

The human body has the privilege of possessing features that are unique and exclusive to each individual. This exclusivity and unique characteristic has led to the field of biometrics and its application in ensuring security in various fields. Today, the technology has emerged as a reliable and effective method for establishing the identity of a person and controlling access to both physical and spaces, more importantly in the wake of heightened concern about security and rapid advancements in communication and mobility in our environments. Meanwhile, experimental studies have shown that a biometric system that uses a single biometric trait for recognition has this propensity to contend with challenges related to non-universality of trait, spoof attacks, large intra-class variability, and noisy data. Besides, no single biometric trait can meet all the requirements of every possible application. Therefore, it is believed that some of the limitations imposed by unimodal biometric systems can be overcome and much higher accuracy achieved by integrating the evidence of multiple biometric traits for establishing identity. However, the time and computational complexity of combining the evidences from different traits during application processes remains an overt concept that attracts research attention. In this research work, a multilevel decision threshold authentication mechanism is presented for efficient multimodal biometric system. This kind of level-based strategy allows data fusion at three different levels to gradually improve the performance of any biometric authentication system.

Introduction

By definition, biometrics has been described as the science and technology of recognizing an individual based on his or her physiological or behavioural traits (Akhtar and Affrarid, 2011). Stanley, Jeberson, and Klinsega (2009) described biometrics as the most secured and convenient authentication tool that cannot be stolen, forgotten, borrowed or forged. Their study identified a number of features that make biometrics a reliable authentication tools. These include: universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention.

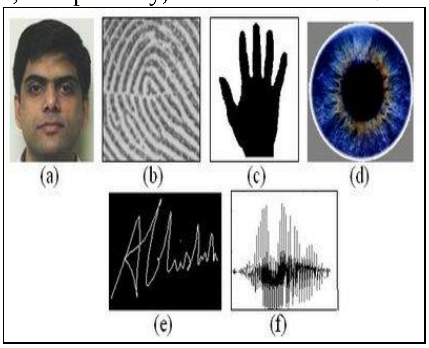

Figure 1. Examples of commonly used biometric characteristics are: (a) face,(b) fingerprint, (c) hand geometry, (d) iris, (e) signature, and (f) voice (Jain,2008a).

This technology has become an underpinning of highly secured identification and personal verification solutions, more importantly in the wake of heightened concern about security challenges in our world today. Notable application areas of biometric systems include border control and immigration, security monitoring and surveillance, forensic investigation, access control and authentication system to mention but few. A number of biometric characteristics that are being used in various applications are illustrated in Figure 1.

According to Damousis and Argyropoulos (2012), further classification of common physical biometrics includes fingerprints, hand or palm geometry, and retina, iris, or facial characteristics. On the other hand, behavioural characteristics include signature, voice (which also has a physical component), keystroke pattern, and gait and so on. When a single trait is used in an application it is called unimodal biometric, while combination of two or more traits in an application is referred to as multimodal biometrics (Ross and Jain, 2006). Studies however have shown that a biometric system that uses a single biometric trait (unimodal) for recognition has this proclivity to contend with issues related to non-universality of the trait, spoof attacks and large intra-class variability. Besides, no single biometric trait can meet all the requirements of every possible application, hence the need for multiple biometric system to overcome the limitation of unimodal biometric system (Soliman et al, 2012; Aranuwa 2014). The new paradigm integrates evidences from multiple biometric sources for establishing identity such as fingerprint, face, signature, hand geometry and so on. (See Figure 2). The paradigm offers considerable improvements in reliability with

Tele: +234703131911

E-mail address: felix.aranuwa@aaua.edu.ng

reasonably overall performance in many applications. However, the issue of efficient and effective integration of the evidences obtained from different traits and its computational complexity remains an overt concept that attracts research attention. In this research paper, a classical multilevel decision threshold authentication mechanism for efficient multimodal biometric system is presented.

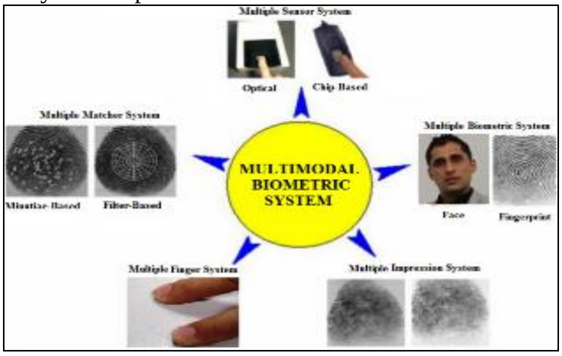

Figure 2. Multiple Biometric Systems (Khan, 2014)

Recognition and Authentication process in Biometric System

In any biometric system application, the users are first known to the system through an enrolment or training process. In the process, a user provides a biometric sample and reference information that will be stored in a database. During authentication or verification, an individual who desires to be recognized claims an identity and the system validates a user identity by comparing the captured biometric data at point of presence with his biometric template stored in the system database. The two distinct mode of process in an authentication system is sketched in Figure 3.

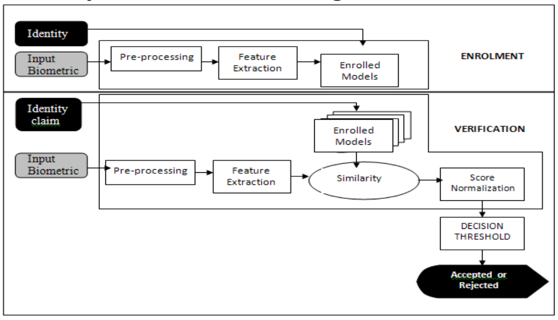

Figure 3. Schematic process of Enrolment and Verification in an Authentication System (Jain et al, 2004)

Integration Techniques in Biometric System

Several different fusion techniques such as rule based, statistical methods and machine learning algorithms have been proposed for biometric information fusion at different levels such as, feature level, match score level, and decision level. Earliest efforts in combining multiple biometrics for person recognition or authentication can be traced back to mid nineties (Brunelli and Falavigna, 1995; Bigun *et al.*, 1997a; Hong and Jain 1998; Kitler *et al.*, 1998 ; Ben-Yacoub, 1999). In all these works, the common practice was to combine biometric evidences at the matching score level. This is also known as fusion at the measurement level or confidence level. At this level the biometric matchers output a set of possible matches along with the quality of each match (matching score) and it is relatively easy to access and combine the scores generated by these different matchers. Figure 4 illustrates level of data fusion possibilities. With respect to biometric authentication, two early theoretical frameworks for combining different machine experts are described by Bigun et al, (1997) and Kitler et al, (1998), the former from a risk analysis perspective (Bigun, 1995), and the later from statistical pattern recognition point of view (Duda et al, 2001). Both of them concluded under some mild conditions that may not hold in practice that weighted average of all the different opinions provided by the systems in the form of similarity scores is a good way of conciliating these evidences from different sources. The approach certainly improves performance of multiple biometric systems but reduces the system's throughput because of its time and computational complexity.

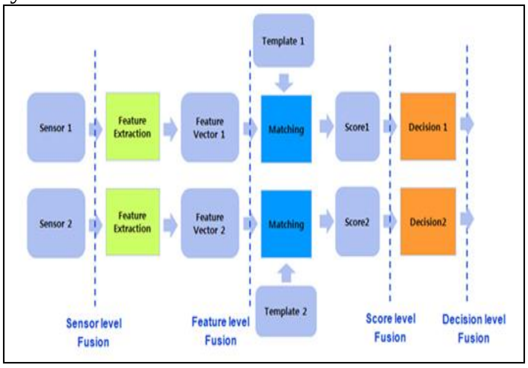

Figure 4. Level of data fusion.

The Architecture of the Proposed Multilevel Decision Threshold Authentication System – (MDTAS)

This architecture of the proposed system – (MDTAS) is composed of three stages as shown in Figure 5.

The first stage is the acquisition of the data pertaining to the three traits proposed in this work, employing applicable sensors and feature vectors created independently. This stage defines the human machine interface and it is pivotal to the performance of the biometric system. The feature acquired is processed and a salient feature is extracted to represent underlying trait. The acquired data will be subjected to a signal enhancement algorithm in order to improve its quality. During enrolment, this feature set will be stored in the database in templates form. Feature extracted from an identity claim will be compared against the stored template to generate match scores. The number of matching features between the input and the template feature sets is determined, and a match score is reported.

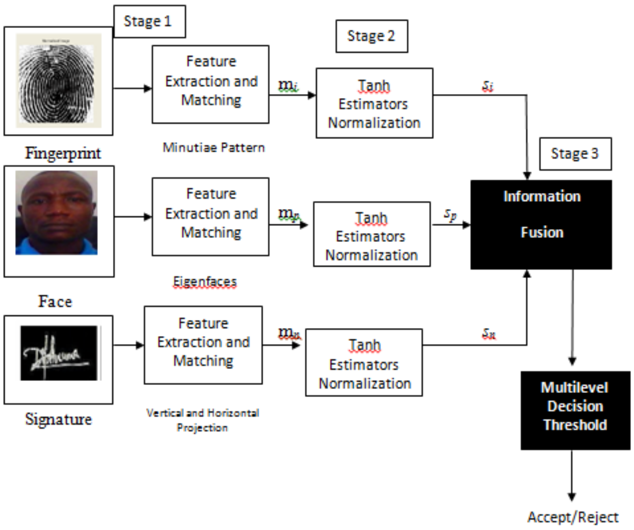

Figure 5. The structure of the Proposed Multilevel Decision Threshold Authentication System – (MDTAS)

The second stage is the deployment of a modified Dempster's rule of combination, which was achieved by inbreeding a *tanh* estimator normalization algorithm into the original Dempster's rule as presented in (Aranuwa, Olabiyisi & Omidiora, 2013).The third phase is the computation of multi-level decision threshold for final decision of authentication.

Analysis of the Multilevel Decision Threshold Authentication System

The mass of each evidence or classifier is combined recursively using the equation stated below in equation 1-4: In the work, the author employed the Dempster–Shafer Theory (DST), a mathematical theory of evidence that provides a useful computational scheme for combining information from multiple sources. It is a powerful tool for combining accumulative evidences and changing priors in the presence of new evidences (Brest, 2010).

$$m_{1,2}(C) = \frac{\sum_{A \cap B = C} m1(A)\ X\ m2(B), \quad \forall\, C \in \Omega}{1 - K} \quad \text{................}eqn\ 1$$

Where,m_1 represent basic belief assignment (bba) of evidence A and,m_2 represent basic belief assignment (bba) of evidence B,Ω represent the belief function and where:

K is defined as,

$$\sum_{A \cap B = \theta} m1(A), X\ m2(B) \quad \text{...................}eqn\ 2$$

Specifically, the combination (called the joint $m_{1,2}$) is calculated from the aggregation of two bba's m_1 and m_2. A and B are used for computing new belief function for the focal element C. The mass final is represented as:

$$mfinal = m_1 \oplus m_2 \oplus m_3 \quad \text{..................}eqn\ 3$$

Where $\oplus$ shows the rule of combination and final result is obtained by applying the threshold t to *mfinal*. The upshot is expressed as follows:

$$Result = \begin{cases} Accept, \text{ if } \quad mfinal \geq t_1 \text{ OR } t_2 \text{ OR } t_3 \\ Otherwise \quad Reject, \end{cases} \quad \text{..................}eqn\ 4$$

where t_1 = threshold value for Fingerprint, t_2 = threshold value for Fingerprint + Face and, t_3 = threshold value for Fingerprint + Face + Signature. With this approach, problem of time and computational complexity can be circumvented. The method is believed to improve reliability, accuracy and reduce error rate.

Performance Metrics for reliability of the Biometric System

An important issue for the adoption of biometric technologies is to establish the performance of individual biometric modalities and overall systems in a credible and objective way. One performance parameter is the measure of the errors in biometric system which is usually tested in terms of false acceptance rate (FAR), false rejection rate (FRR), failure to enroll rate (FER), during enrollment and verification time. False Acceptance Rate (FAR) is defined as the ratio of impostors that were falsely accepted over the total number of impostors tested described as a percentage**.** (i.e FAR = Number of accepted imposter claims / Total number of imposter accesses x 100%).

This indicates the likelihood that an impostor may be falsely accepted and this must be minimized in high-security applications. False Reject Rate (FRR) is defined as the ratio of genuine clients that are falsely rejected to the total number of genuine clients tested described as a percentage. (i.e FRR = Number of rejected genuine claims / Total number of genuine accesses x 100%). This indicates the probability that a valid user may be rejected by the system. Ideally this should also be minimized especially when the user community may be put-off from using the system if they are wrongly denied access.

In this type of application, a number of 'clients' may be enrolled onto the system, both genuine and impostor. The impostor may be someone who is not enrolled at all or someone who tries to claim the identity of someone else either intentionally or otherwise. When being verified the genuine clients should be recognized as themselves and impostors should be rejected. In order to estimate FAR and FRR, a set of genuine and impostor matching scores have to be generated. The decision to accept or reject is based on a pre-defined threshold. If the distance is less than this threshold then we can accept the sample.

A unique measure however, can be obtained by combining these two errors into the Total Error Rate (TER) or Total Success Rate (TSR) where:

TER = FAR + FRR / Total number of accesses x 100 and,

TSR = 1 – TER.

Another important performance parameter is the verification time defined as the average time taken for the verification process. This may include the time taken to present the live sample. The actual verification time will critically depend on user training, operating environment and psychological conditions.

Conclussion

Multimodal biometric system certainly offers considerable improvements in reliability, accuracy and reduce error rate with reasonably overall performance in many applications over the unimodal biometric system. The new paradigm has become an underpinning of highly secured identification and personal verification solutions, more importantly in the wake of heightened concern about security challenges in our world today. However, the issue of efficient and effective integration of the evidences obtained from different traits and its computational complexity remains an overt concept that attracts research attention. Several different fusion techniques such as rule based, statistical methods and machine learning algorithms have been proposed for biometric information fusion at different levels such as, feature level, match score level, and decision level. In this research paper, we have proposed multilevel decision threshold authentication mechanism using modified Dempster-Shafer Rule of Combination, a powerful tool for combining accumulative evidences and changing priors in the presence of new evidences to profer solutions to the fusion challenges in multiple biometric systems and in turns produce an efficient multimodal biometric authentication system. Currently, we are working on the implementation of the proposed architecture, but this work can be improved upon in several ways, especially for the case of multiple classes.

References

[1] Akhtar, Z and Affrarid, N (2011): "Secure learning Algorithm for Multimodal Biometric Systems against Spoof Attacks". International Conference on Information and network technology IPCSIT vol.4 (2011) © (2011) IACSIT Press. Singapore.

[2] Stanley, P., Jeberson, W., and Klinsega V.V. 2009. Biometric Authentication: A Trustworthy Technology for Improved Authentication. 2009 International Conference on Future Networks, , pp. 171-175.

[3] Jain, A. K. (2008a), Microsoft ® Encarta ® 2008 ©, 1993-

2007-Microsoft Corporation.
[4] Damousis I. G. and Argyropoulos S (2012) : "Four Machine Learning Algorithms for Biometrics Fusion": A Comparative Study. Applied Computational Intelligence and Soft Computing Volume 2012, Article ID 242401, 7 pages. Hindawi Publishing Corporation doi:10.1155/2012/242401
[5] Ross, A. and Jain, A.K. (2006): "Multimodal Biometrics: An Overview", Proceedings of 12th European Signal Processing Conference (EUSIPCO), (Viena Austra), pp.1221-1224, Sept., 2006**.**
[6] 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 Vol. 12No 01,pg 28-39, February, 2012.
[7] Aranuwa, F. O (2014): Multiple Biometric Systems: Design Approach and Application Scenario. *Elixir International Journal for Computer Science and Engineering.* Roma, Italy. Volume 73, pg 26015-26019, July 2014. ISSN 2229-712X. Available online at: *www.elixirpublishers.com.*
[8] Khan, T. M (2014). VSLI Research Group, Macquqrie University, Sidney Australia
[9] Jain, A. K and Ross, A. (2004). "Multibiometric Systems". Communications of the ACM, Special Issue on Multimodal Interfaces, 47(1):34–40, January 2004.
[10] Brunelli, R. and Falavigna, D. (1995), "Personal Identification Using Multiple Cues". IEEE Trans. on Pattern Analysis and Machine Intelligence 17(10), 955-966.
[11] Bigun, E., Bigun, J., Duc, B. and Fisher, S. (1997), "Expert conciliation for multi modal person authentication systems by Bayesian statistics". Proceedings of the first international conference on Audio and Video-based Biometric Person Authentication 327–334.
[12] Hong, L, and Jain,A. K (1998). "Integrating faces and fingerprints for personal
identification," IEEE Transactions on *PAMI*, vol. 20, pp. 1295–1307, Dec 1998.
[13] Kittler, J., Hatef, M., Duin, R. P. W. and Matas, J. (1998), "On combining classifiers". IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(3): 226–239.
[14] Ben-Yacoub S.B, (1999). "Multi-modal Data Fusion for Person Authentication using SVM". Proceedings of the second International Conference on Audio and Video-based Biometric Person Authentication (AVBPA'99) pp.25-30.
[15] Duda, R. O. and Hart, P. E. (2001), "Pattern Classification and Scene Analysis. New York: John Wiley & Sons.
[16] 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, Volume 4: No 1, March, 2013 pg 1-8. ISBN 978-2257-44-7, ISSN 2167-1710. Available online at: *http://www.cisdijournal.net.*
[17] Brest B. (2010): Workshop on Theory of Belief Functions (http:/bafas.iutlan.univrennes1.fr/belief2010/) (Brest, 1 April 2010).