Texila International Journal of Academic Research
Volume 4, Issue 2, Dec 2017

Intricacies of Secured Multi-Biometric System

Article by Emmanuel Chinweuba Nwani
Department of Computer Science, Federal Polytechnic Oko Nigeria
E-mail: emuban@yahoo.com

Abstract

The Multi-biometrics system is designed as a measure for security purposes to recognize individuals using all available features. It is a thrilling research domain carried out to boost the security level of a country or of an organization. The integration of muti-modal biometrics in real time application resolves the limitations of the uni-modal applications. Although, the design and assessment of the multi-biometrics systems raises much issues, this paper tends to unravel the clumsiness and trade-offs in its applications, the benefits of fusion level, integration strategies and check to spoofing. In conclusion, a thorough reviewing of multi-modal secured biometrics techniques and approaches was carried out to ensure data identification integrity. Some points were suggested for consideration as subjects of interest for future research.

Keywords: *Multi-Biometrics; Multimodal application; Unimodal application; Secured Biometrics; fusion levels Spoofing.*

Introduction

Verification is an authentication method of identifying a person in a biometric security system. It is a very essential and challenging practical and secured authentication technology. The customary techniques of user authentication is categorized into two; the Token Techniques (use of key and smart cards) and the Knowledge-based Techniques (use of text and picture passwords) [13]. These techniques are vulnerable and the authentication tools can be easily lost, wear-off or forgotten. These customary techniques are considered not secured or reliable in a contemporary security checks and hence, are not sufficient to be applied in the global security challenges. The basic benefit of biometrics authentication over the traditional techniques is that the biometrics cannot be stolen, forgotten, wear-off, misplaced or spoof biometric traits [11]. Considering the larger accuracy and higher recognition of biometric authentication, it becomes imperative and preferred technique to analyze individual traits for security identification purposes. The system is free from spoofing, misused or counterfeited.

Basically, biometrics information considered most secure method is used in areas such as; security system, surveillance systems, access control, physical buildings, verification and authentication, forensic investigations, border control, e-commerce, parenthood determination, online banking, medical records management and security monitoring. Its application has cut across diverse fields of endevour.

Generally, Biometric technology is defined as the computerized technique of verifying and recognizing the identity of a human being, a living individual using the following traits: (a) *the Physiological biometrics*, which includes facial, ear, hand and hand vein infrared thermogram, hand and finger geometry, retina, fingerprint, Iris, Voice, DNA and palm print. (b) *the Behavioral biometrics* such as gait, signature and Keystroke, which is the traits that measure human actions [10].

The biometric systems operate in two modes depending on application context – the verification mode and the identification mode. In the verification mode, the biometric system verifies the identity comparing the registered biometric traits with the biometric model stored in the system [5]. This mode used for positive recognition is aimed at preventing multiple users from using the same identity.

The enrolled sample in the identification mode is compared with existing templates stored in the central database to identify the user. The identification mode is important in negative recognition

DOI: 10.21522/TIJAR.2014.04.02.Art024
ISSN: 2520-3088

applications that aim to avert a single user from using multiple identities during enrollment [18]. The negative identification can be known as screening. Apparently, the verification is less expensive and more encompassing, while identification is more expedient and less obtrusive [22].

Multi-biometric systems address the issue of noisy data, non-universality and expedite the indexing of large-scale biometric database, unlike the out-of-date uni-biometric systems. In addition, it is very difficult for an impostor to carryout spoof attack on all the biometric traits of an individual enrolled in the database and also essential to fraudulent technologies, which is difficult to forge multiple biometric features. The multi-biometric recognition systems have the benefits especially in the continuous monitoring of a user in treat situations when a single trait is not enough to track him. The system continues to function even when any part of the biometric sources (such as software malfunction, sensor malfunction or deliberate user manipulations) fails or become unavailable [30].

General idea of biometric technologies

The term "Biometric technologies" can be defined as a programmed method of verifying and recognizing the identity of an enrolled individual based on these two categories: (1) Physiological Biometrics, which includes (fingerprints, retina, facial, hand and hand vein infrared thermogram, ear, finger geometry, DNA, voice and palm print) [15], and (2) the Behavioral biometrics, which includes (keystroke, gait and signature) that measures human actions [15]. The human electrocardiogram (ECG) signal is also considered as one of the biometric traits used in an individual recognition and authentication [29].

The reliability of a biometric system depend on the following characteristics

Availability – (Universality): Indicates that an individual should have distinct characteristics. Availability or universality is measured by FTER ("failure to enroll" Rate).

Distinctiveness: This asserts that two individuals should adequately have different characteristics. Distinctiveness is measured by FMR (False Match Rate), which is also called ‘Type (II) Error’.

Robustness – (Permanence): It declares that characteristics should be constant over a period of time with respect to matching characteristics; hence, the traits should be stable over age. The Robustness or Permanence is measured by FNMR (False Non-Match Rate, which is also called ‘Type (I) Error’.

Accessible – (Collectability): It asserts that the features can be measured using quantitative method, and can also be easy to image with electronic sensors [14].

Resistance to Bypass tests and verify how the system resists spoofing and fraudulent methods easily.

All the biometrics traits can be used to verify and authenticate an individual enrolled in the database. Each trait is characterized by FRR (false reject rate) and FAR (false accept rate).

Limitations of unimodal biometric systems

The vulnerability of biometric sensor to bad or noisy data as a result of distorted and imperfect acquisition of captured biometric trait. This limitation can be generally seen in the applications that use facial recognition, where the quality of the enrolled facial images could be affected by illumination and facial conditions, and hence results to False Reject Rate (FRR). A similar scenario is the fingerprint recognition, where an image scanner fails to read dirty fingerprints obviously and hence, leads to a false database match. In unimodal biometrics system, an enrolled individual can be erroneously rejected and however, an impostor can be falsely accepted [12].

Certainly, unimodal system cannot work perfectly with definite groups of population. For instance, fingerprint images might not be accurately captured from much younger children and elderly people because of underdeveloped fingerprint ridges and faded fingerprints respectively [17]. Although, biometric traits are likely to exist among every person, there could be some exemptions where a person is unable to make available a particular biometric trait due to pathological conditions. For example, iris images might not be acquired from an individual with pathological eye condition. All these stated limitations might not provide accurate match in a unimodal biometrics system because there is no other biometric trait of the same individual to fuse and determine the identity of the enrolled user.

With large population to enroll, the unimodal biometrics is susceptible to inter-class similarities of biometric features. Facial recognition may not perfectly work for identical twins, even as it could be difficult for the camera to make a distinction between the two subjects that could lead to erroneous matching. The unimodal biometric systems are relatively exposed to spoof attacks, where enrolled data can be easily forged or imitated. For example, rubber fingerprints can be used to spoof fingerprint recognition systems.

Unimodal biometric which rely on evident single source of data for authentication may not achieve the preferred performance requirements because it has plenty of error rates [22]. The error rates the system contends with are:

1. Noise in sensed data due to faulty or inappropriately maintained sensors from buildup of dirt on fingerprint sensor. In addition, voice could be distorted by cold, iris recognition performance can be altered by wearing glasses and light variations cold distort face recognition system.
2. Uniqueness (Inter-class similarities and Intra-class variations) – Biometric trait is expected to vary considerably across two individuals. When an individual interacts with the sensor erroneously, the intra-class variations occur, while the individual characteristics form the inter-class similarities.
3. Spoof attack – with single source of biometrics data, a fake trait of an enrolled user can be introduced and saved as template in the database. In this case, an impostor might attempt to use artificial fingerprint to spoof the sensed data when the trait is used

Multimodal biometric systems

A Multimodal biometric system fuses multiple biometric technologies such as fingerprint, facial recognition, iris scanning, voice recognition and hand geometry. The multimodal system measures two or more different biometric characteristics by taking input from single or multiple sensors [10]. The system that combines iris and face characteristics for biometric identification is known as a multimodal system, notwithstanding whether the iris and face images were captured by same or dissimilar biometric imaging devices. For instance, a biometric system that combines face and fingerprint recognition and permits users to be verified and identified using either of the modality.

Multimodal systems

Given below is the block diagram of multimodal systems.

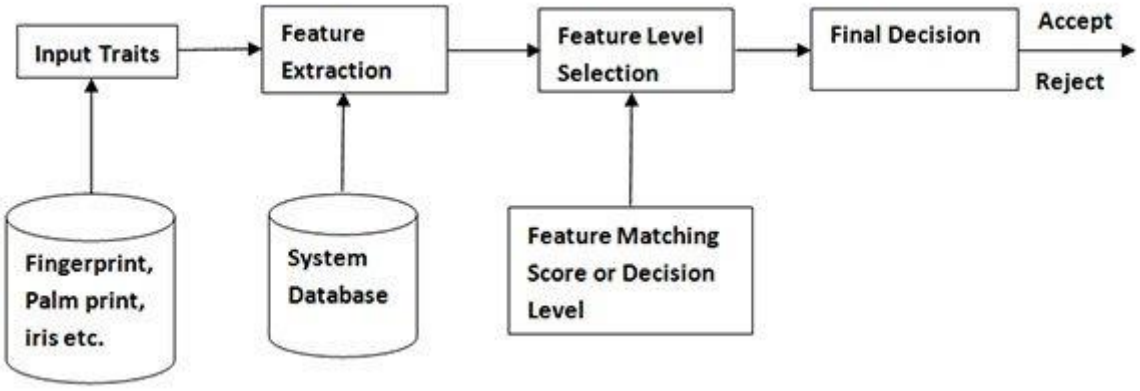

Figure 1. A diagram of multimodal system

The multimodal biometric system is made up of four modules

i. Sensor
ii. Feature Extraction
iii. Matching and

DOI: 10.21522/TIJAR.2014.04.02.Art024
ISSN: 2520-3088

iv. Decision-Making modules

Fusion in multimodal biometric system is achieved by combining two or more biometric traits alongside two or more different algorithms that is used to work out a decision. The technique is extremely useful in a large scale, where the identity of millions of individuals have to be authenticated at a time [23].

Types of multimodal biometric systems

1. **Multi-Algorithmic Biometric System:** This biometric system takes a single biometric trait from a single sensor, analyze and process it using different algorithmic procedures.
2. **Multi-instance biometric system:** This biometric system uses one or more sensors to capture two or more various samples of the same biometric trait. For instance, the system that captures images of multiple fingers is an example.
3. **Multi-sensorial Biometric System:** This biometric system uses two or more different sensors to capture the same example of a biometric trait. A single or a combination of algorithms is used to process the captured samples. Example of multi-sensorial biometric systems is where the same facial image is captured using a visible light camera and an infrared camera fixed with a particular frequency.

Multimodal biometric systems fusion

More biometric modality is used in multimodal biometric systems, to give more than one channels of decision. This system designs a mechanism that can combine the classification result from each of the biometric channel; hence this mechanism is called biometric fusion [16]. Fusion strengthens authentication accuracy by combining the measurements from different biometric traits and reduces the weaknesses of the singular measurements.

Fusion addresses lots of challenges in implementation of biometric systems. These issues include efficiency, accuracy, applicability, robustness, and universality. Sensor, feature, matching score level fusion and the decision level fusion are different levels of fusing (combining) biometric traits that can be used to increase the strength of multimodal biometric system [31].

The figure below shows the fusion levels of a multimodal biometric system.

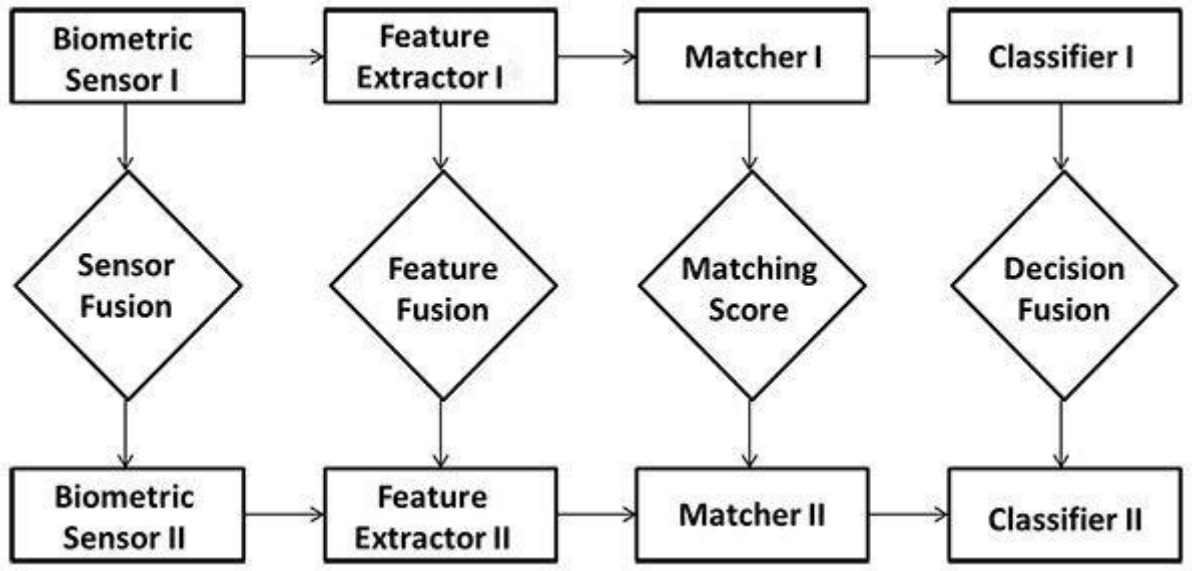

Figure 2.1. Showing different levels of fusion in multimodal biometric systems

Sensor level fusion

The biometric traits captured by different sensors like iris scanner, fingerprint scanner, video camera etc. are fused in sensor level fusion to form a merged biometric trait and then the processes.

Feature level fusion

The signals emanating from different biometric channels in feature level fusion are first processed and thereafter, the feature vectors are taken out individually from every biometric trait. The extracted feature vectors are then fused (combined) to form a merged feature vector using a particular fusion algorithm. Only the useful feature vectors are selected and used, using some reduction techniques. It is evidence that that the feature level fusion provides more significant accuracy when the features of various biometric modalities are well-matched with each other.

Matching score level fusion

The feature vectors in matching score level fusion are processed independently rather than combining the vectors, and then a separate matching score is found. We fuse the matching level to find a multiple matching score that can be used for classification based on the accuracy of every biometric channel. We can use different techniques like logistic regression, Bayes rule, mean fusion and highest rank to combine match scores [27]. We can also use different techniques like Min-max, piecewise linear and z-score to realize normalization of match scores gotten from different modalities.

Decision level fusion

Every biometric trait in decision level fusion is pre-classified individually and the separate biometric trait is firstly captured, and the feature vectors are extracted from the traits captured. Based on the extracted features, the traits are categorized as either ‘accept’ or ‘reject’. The final classification is achieved by combining the results of different modalities.

Benefits of multimodal biometric systems as the best solution

1. The unimodal biometric systems encounter image acquisition errors, which include failure-to-enroll (FTE) and failure-to-acquire (FTA) rate, and also the matching errors consisting of false match rate (FMR), which makes and intruder to be granted access and the false non-match rates (FNMR) where an enrolled individual can be rejected. Multimodal biometric system accuracy is measured by matching the biometric traits and the errors in image acquisition. The Multimodal systems have nearly zero FTE, FTA, FMR and FNMR rates [15].
2. In some situations where millions of people will be enrolled in the system and some individuals are facing challenges with a particular biometric trait, the multimodal systems can best be applied to overcome the limitations of FTE and FTA rates by using different biometric capture for the segment of that population. The multimodal system will certainly ensure almost zero failure-to-enroll (FTE) and failure to acquire (FTA) rate.
3. Multimodal biometrics system reduces data distortion algorithm. In a scenario where the quality of a biometric sample is rejected, the other biometric sample can be used to determine accuracy. For instance, if the fingerprint scanner rejects fingerprint image as a result of poor quality, the use of another biometric modality like facial or iris will reduce the false rejection rates.
4. Multimodal systems are difficult to spoof because it is very hard to imitate all the biometric templates captured in the database, unlike the unimodal systems where a single biometric template can be imitated. Even when one biometric modality is spoofed, the user can be authenticated by using the other biometric identifiers.

DOI: 10.21522/TIJAR.2014.04.02.Art024
ISSN: 2520-3088

Limitation of multimodal biometrics system

Some deficiencies are still found in multimodal system such as noise. Deficiencies such as scratches in the fingerprint and facial marks can lead to the increase in FRR. In some instances, the failure of one biometrics trait will make the entire multi-biometric system to fail [22]. However, the setting up of multimodal biometric systems incurs more expensive and complex due to the requisite of additional hardware, software, storage facilities and matching algorithms [13]. In addition, in some instances, all the biometric traits may be required for authentication, and if any of the biometric templates is rejected, authentication might be difficult.

Conclusion

Multi-biometrics system gives more accurate result compared to unimodal biometric system and this topic has attracted greater interest in today's research. It is often used to identify the physiological and behavioral characteristics of an individual specifically for security purposes. The limitations of singular (unimodal) biometric system, especially spoofing necessitated the recent clamour for multimodal biometric implementation suitable for all applications, administration policies, technologies and populations to accomplish higher performance. The enormous benefits of multi-biometrics, different levels of fusion and matching process were highly discussed as a solution to security lapses. Finally, some interesting points were suggested to be considered in a future research to enhance applications.

References

[1]. Amirthalingam, "A Multimodal Approach for Face and Ear Biometric System," International Journal of Computer Science Issues (IJCSI), vol. 10, no. 5, pp. 234-241, 2013.
[2]. Ahuja M. S. and S. Chabbra, "A Survey of Multimodal Biometrics," International Journal of Computer Science and its Applications, vol. 1, no. pp. 157-160, 2011.
[3]. Anwar, M. A. Rahman, and S. Azad, "Multibiometric Systems Based Verification Technique," European J. Scientific Research, vol. 34, no. 2, pp. 260-270, 2009.
[4]. Asha S. and C. Chellappan, "Authentication of E-Learners Using Multimodal Biometric Technology," presented at the Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on, Islamabad, 2008. pp. 1-6.
[5]. AlMahafzah and M. Z. AlRwashdeh, "A Survey of Multibiometric Systems," International Journal of Computer Applications vol. 43, no. 15, pp. 36-43, 2012.
[6]. Bhatia R., "Biometrics and Face Recognition Techniques," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, pp. 93-99, 2013.
[7]. Bhargava and R. S. Ochawar, "Biometrics in Access Control System," International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 2, pp. 269-273, 2013.
[8]. Deriche, "Trends and Challenges in Mono and Multi biometrics," presented at the Image Processing Theory, Tools and Applications, 2008. IPTA 2008. First Workshops on, Sousse, 2008. pp. 1-9.
[9]. Delac and M. Grgic, "A Survey of Biometric Recognition Methods," in Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium, ELMAR-2004, Zadar, Croatia, 2004, pp. 184-193.
[10]. Elumalai and M. Kannan, "Multimodal Authentication for High End Security," International Journal on Computer Science and Engineering, vol. 3, no. 2, pp. 687-692, 2011.
[11]. Feng, K. Dong, D. Hu, and D. Zhang, "When Faces are Combined With Palmprints: A novel Biometric Fusion Strategy," presented at the In proc. of 1st Int. Conf. on Biometric authentication, Hong Kong, China, 2004. pp. 701-707.
[12]. Gad R., M. Mohamed, and N. El-Fishawy, "Iris Recognition Based on Log-Gabor and Discrete Cosine Transform Coding," Journal of Computer Science and Engineering, vol. 5, no. 2, pp. 19-26, 2011.
[13]. Gavrilova L. and M. M. Monwar, "Current Trends in Multimodal Biometric System Rank Level Fusion," in Pattern Recognition, Machine Intelligence and Biometrics, ed: Springer, 2011, pp. 657-673.

[14]. Geethanjali and K. Thamaraiselvi, "Feature Level Fusion of Multimodal Biometrics and Two Tier Security in ATM System," International Journal of Computer Applications, vol. 70, no. 14, pp. 17-23, 2013.Karray, J. A. Saleh, M. N. Arab, and M. Alemzadeh, "Multi Modal Biometric Systems: A State of the Art Survey," Pattern Analysis and Machine Intelligence Laboratory, University of Waterloo, Waterloo, Canada, no. 2007.
[15]. Jain K., A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, 2004.
[16]. Kalra S. and A. Lamba, "A Survey on Multimodal Biometric," International journal of computer science and information technologies, vol. 5, no. 2, pp. 2148-2151, 2014.
[17]. Meraoumia, S. Chitroub, and A. Bouridane, "Multimodal Biometric Person Recognition System based on Iris and Palmprint Using Correlation Filter Classifier," in Proc. of the Second International Conference on Communications and Information Technology, Hammamet, Tunisia, June 26-28, 2012, pp. 782-787.
[18]. Manjunath M. and K. B. Raja, "A Novel Approach for Iris Recognition using DWT&PCA," Int. J. Advanced Networking and Applications, vol. 5, no. 1, pp. 1830-1836, 2013.
[19]. Mr. Rupesh Wagh A. P. C., "Analysis of Mutlimodal Biometrics with Security Key," International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE). vol. 3, no. 8, pp. 1363-1365, 2013.
[20]. Malhotra S. and D. C. Kant, "A Novel Approach for Securing Biometric Template," Internal Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol. 3, no. 5, pp. 397-403, 2013.
[21]. Matsumoto T., H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems," in Electronic Imaging 2002, Proceedings of SPIE, San Joes, USA, 2002, pp. 275-289.
[22]. Meva T. and C. K. Kumbharana, "Comparative Study of Different fusion techniques in multimodal biometric authentication," International Journal of Computer Applications, vol. 66, no. 19, 2013.
[23]. Monwar M. and M. L. Gavrilova, "Multimodal Biometric System Using Rank-Level Fusion Approach," IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics,, vol. 39, no. 4, pp. 867-878, 2009.
[24]. Ross A., K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics vol. 6. New York: Springer Science & Business Media, 2006.
[25]. Ross A., A. K. Jain, and K. Nandakumar, "Information Fusion in Biometrics," in Handbook of Multibiometrics, ed, 2006, pp. 37-58.
[26]. Radha N. and A. Kavitha, "Rank Level Fusion Using Fingerprint and Iris Biometrics," Indian Journal of Computer Science and Engineering (IJCSE), vol. 2, no. 6, pp. 917-923, 2011.
[27]. Sathish G., S. V. Saravanan, S. Narmadha, and S. U. Maheswari, "Multi-Algorithmic Iris Recognition," International Journal of Computer Applications, vol. 38, no. 11, pp. 13-21, 2012.
[28]. Singh Y. S. a. S., "Evaluation of Electrocardiogram for Biometric Authentication," Journal of Information Security, vol. 3, no. 1, pp. 39-48, 2012.
[29]. Singhal R., N. Singh, and P. Jain, "Towards. An Integrated Biometric Technique," International Journal of Computer Applications, vol. 42, no. 13, pp. 20-23, 2012.
[30]. Siddiqui M., R. Telgad, and P. D. Deshmukh, "Multimodal Biometric Systems: Study to Improve Accuracy and Performance," International Journal of Current Engineering and Technology, vol. 4, no. 1, pp. 165-171, 2014.
[31]. Schouten and B. Jacobs, "Biometrics and Their Use in E-Passports," Image and Vision Computing, vol. 27, no. 3, pp. 305-312, 2009.
[32]. Satyarthi, Y. P. S. Maravi, P. Sharma, and R. K. Gupta, "Comparative Study of Offline Signature Verification Techniques," International Journal of Advancements in Research & Technology, vol. 2, no. 2, pp. 1-6, 2013
[33]. Sharma S., "An Improved Iris Recognition System Based on 2-D DCT and Hamming Distance Technique," ICRTEDC-2014, GV/ICRTEDC/08, vol. 1, no. 2, pp. 32-34, 2014.Soltane M., N. Doghmane, and N. Guersi, "Face and Speech Based Multi-Modal Biometric Authentication," International Journal of Advanced Science and Technology, vol. 21, no. 6, pp. 41-56, 2010.