A Review Of Multimodal Biometric Authentication Systems

Kunal Kumar, Mohammed Farik

Abstract: Authentication is the process of validating the identity of a person based on certain input that the person provides. Authentication has become a major topic of research due to the increasing number of attacks on computer networks around the globe. This review paper focuses on multimodal biometric authentication systems in use today. The aim is to elicit the best combination of authentication factors for multimodal use. We study the strengths and weakness of selected biometric mechanisms and recommend novel solutions to include in multimodal biometric systems to improve on the current biometric drawbacks. We believe this paper will provide security researchers some useful insight whilst designing better biometric systems.

Index Terms: Authentication, Biometrics, Face, Iris, Multimodal, Retina

1 Introduction

Authentication is a technique that a computer system uses to verify the identity of a person seeking to access resources of that system[1]. The term is common in computer science where access to any resources on a system normally requires verification of identity. Authentication technologies have gone through major improvements in recent years and new techniques are being introduced by researchers from around the world on a regular basis[2]. The improvements are warranted due to the heightened attacks on conventional authentication mechanisms. The mechanisms of authentication come in a wide variety utilizing a number of factors[3]. These mechanisms are mostly divided into three categories which are: “something you remember”, “something you possess”, and “something you are”. Our focus is on “something you are” type of authentication. “Something you are” is an upcoming mechanism for authentication. This type of authentication is more commonly known as biometrics and is considered one of the most secure forms of authentication[4]. Substantial amount of research is delved at this area and various technologies have been developed and advanced to improve this form of authentication. Biometrics simply means the utilization of biological traits or behavioral characteristics to authenticate a user[5]. For the purpose of this research we will use the term factor to refer to both biological trait and behavioral characteristics. Research in biometrics area has highlighted various factors of authentication, some of which are: fingerprint, face, iris, retina, gait, palm and many more[6]. Various technologies have been implemented to improve the performance of these authentication mechanisms such as use of heat waves to elicit patters and use of ridges and valley points[7] using various distance measures such as Euclidean, Manhattan, city block and so on[8].

- *Kunal Kumar is currently pursuing Masters Degree in Information Technology at The University of Fiji. Email: kunalk@unifiji.ac.fj*
- *Mohammed Farik is a Lecturer in Information Technology at The University of Fiji. Email: mohammedf@unifiji.ac.fj*

Biometrics systems have been divided into two categories which are: unimodal and multimodal biometrics system. The essential difference between the two is that a Unimodal system works with only one trait or behavior while a multimodal system combines the power of multiple traits and behaviors such as combining any number of traits such as fingerprint with face and voice, and etcetera. Our focus is specifically on multimodal biometrics system of authentication because it shows significant promise in terms of security and performance supplemented with providing convenience for users. The paper discusses the current trends in research of multimodal systems and identifies the strengths and weaknesses of this form of authentication. The next sections discuss history, strengths, challenges, and recommendations in regards to multimodal biometric systems.

2 Biometric Authentication Systems

2.1 History

Biometrics systems have been introduced in various aspects of the community. Biometrics is being used by the Justice system to record criminal data. The Federal Bureau of Investigation (FBI) of the US Department of Justice utilizes IAFIS, an automated 10-fingerprint matching system that captures rolled prints[9]. IAFIS started in 1999 and holds over 55 million subjects on file, making it the largest biometrics database in the world. The immigration sectors have also started use of biometrics. The US-VISIT system is another project launched by the United States Department of Homeland Security (DHS) collects, maintains, and shares information, including biometric identifiers, on selected foreign nationals applying for visas or entry into the country[10]. The banking and finance sector are actively engaged in biometrics authentication. The Royal Bank of Scotland (RBS) and NatWest pioneered the use of fingerprint technology via mobile phones to authenticate users[11]. The Citibank collected two Gartner Financial Services Cool Business Awards in 2015 for implementation of voice recognition for identification. Multimodal systems have recently got major attention due to the increased level of security it provides. Krawczyk proposed a multimodal system which uses online digital signature and voice recognition to secure medical records[12]. Shoaa Al-Hijaili has also proposed the use of face and iris to protect medical documents[13]. Catalin introduced a multimodal biometrics system to securing internet banking applications[14]. Biometrics will be used to open a token device and/or login to the internet banking application or

sign an order. While there are various multimodal system in play, these systems use various fusion techniques for decision making. Multimodal authentication systems have been implemented with a number of various techniques. The information extracted from various biometrics factors need to be pre-processed. Jain proposed score normalization techniques implemented at matching score level to produce a standard score[15]. Nandakumar developed a framework for fusion based on likelihood ratio test method. This method graphs the true and imposter distributions as finite Gaussian mixture model. Yan developed a class-dependence feature analysis method grounded on Correlation Filter Bank (CFB) method[16]. This method is implemented at feature level rather than matching or decision level. Monwar proposed a scheme for fusion that combines information provided by multiple domain experts based on the rank-level fusion integration method[17]. Data mining plays a vital role in driving the implementation and advancement of this system. Tor proposed a neural network model that generates different combinations of a hyperbolic functions to achieve approximation and classification properties[18]. The paper will now discuss multimodal systems.

2.2 Characteristics of Multimodal Systems

Biometric systems are proving to be more effective and secure. The systems are known to be difficult to manipulate and harder to hack or bypass. Like any other system, biometrics systems adhere to a set of characteristics which ensure authenticity and security of the system. Table 1 discusses these characteristics in detail.

TABLE 1
CHARACTERISTICS OF BIOMETRIC SYSTEMS

Characteristic	Description
Universality	Every individual should have this characteristic
Distinctness	Any two people should have discrete representation of the characteristic
Permanence	The characteristic should undergo no or very slight variance over time.
Collectability	There must be a way to convert the characteristic into data points.
Performance	Refers to standard expected rates of execution and accuracy.
Acceptability	Indicates the amount of support from people for using the system in their daily lives.
Circumvention	Refers to how easily the system can be compromised.

Multimodal systems aggregate two of more traits or behaviors to produce a more secure and robust system. This section will provide insight into the architecture and implementation of biometric systems. Multimodal system overlay on the architecture of the conventional unimodal systems, aggregating various traits or behaviors to work together. A unimodal biometrics system runs in three modes. These modes are: enrolment, verification and identification (Fig.1).

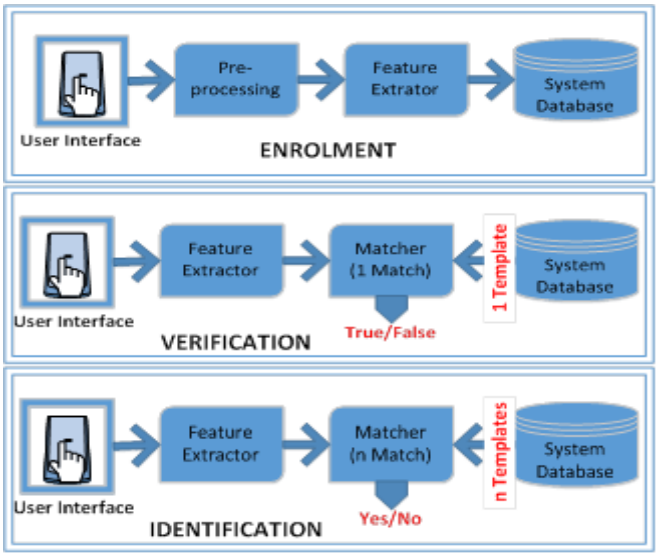

Fig. 1. *Unimodal Biometric System*

Enrolment is the initial process of registering an individual's template of the factor in the database. This process involves scanning of required factor and producing an image or signal. Directly scanned images are pre-processed to reduce noise in data and improve the efficiency of the procedure. The template registered contains vectors of data which if used in the matching phase of the system. Verification and identification is sometimes used interchangeably in literature but the two processes are distinct in nature. Verification simple means mapping an initially scanned factor with a previously scanned factor. Thus, having a one-to-one relationship system. Identification on the other hand lays on a one-to-many relationship whereby an initially scanned factor is run across a database of templates to find a match. Multimodal systems follow the same three modes of execution and the system architecture is identical to unimodal systems to some extent. Multimodal systems have an additional phase called fusion where the match scores of each factor in combined using a specific technique to produce a master score which will be used for decision making (Fig.2).

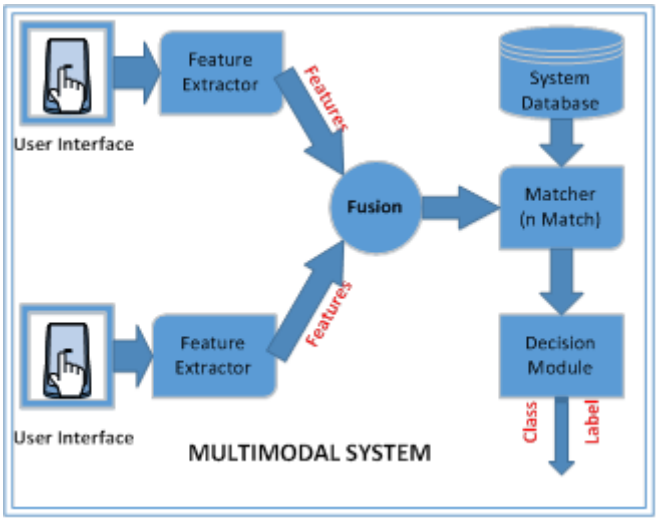

Fig. 2. *Multimodal Biometric System*

The National Institute of Standards and Technology (NIST) has been working on Biometrics research since the 1960's[19]. NIST has been involved in large scale studies of biometrics. NIST has classified Fingerprint, Face and Iris as the best traits to use in biometrics. Table 2 is illustrating the accuracy of fingerprint matching [20]. Table 2 takes in account the number of fingers as well as the side of the hand

TABLE 2
ACCURACY OF FINGERPRINT

	False Negative Identification Rate (FNIR)
Single-Right-Index Finger Identification	1.90%
Single-Left-Index Finger Identification	1.97%
Two-Index Finger Identification	0.27%
Four-finger identification	0.45%
Ten-Finger Identification (Right slaps)	0.45%
Ten-Finger Identification (Left slaps)	0.94%

Detailed information about participants has been outlines in Table 3.

TABLE 3
GENDER CLASSIFICATION PARTICIPANTS

Participant	Letter Code	Submissions		
		Aug. 2012	Mar. 2013	Oct. 2013
Cognitec	B	B10D	B20D	B30D, B31D
Neurotechnology	C			C30D
NEC	E	E10D		E30D, E31D, E32D
Tsinghua University	F	F10D		F30D
MITRE	K	K10D		
Zhuhai-Yisheng	P			P30D

Table 4 summarizes the accuracy of classification of face images by various algorithms. The algorithms presented have been submitted by participants[21].

TABLE 4
CLASSIFICATION ACCURACY OF FACE IMAGES

Algorithm	Accuracy (%)
B30D	93.2
B31D	93.3
C30D	91.9
E30D	94.2
E31D	94.5
E32D	96.5
F30D	88.6
K10D	90.8
P30D	88.1

Surveys have been conducted that evaluates the performance of Iris biometrics. Fig. 3 shows the recognition rates of iris using the principal component analysis method implemented at three levels. It is clear the feature level matching yields the best results. Research shows that feature level matching attains a False Reject Rate(FRR) of 0.1 providing 95% accuracy of recognition[22].

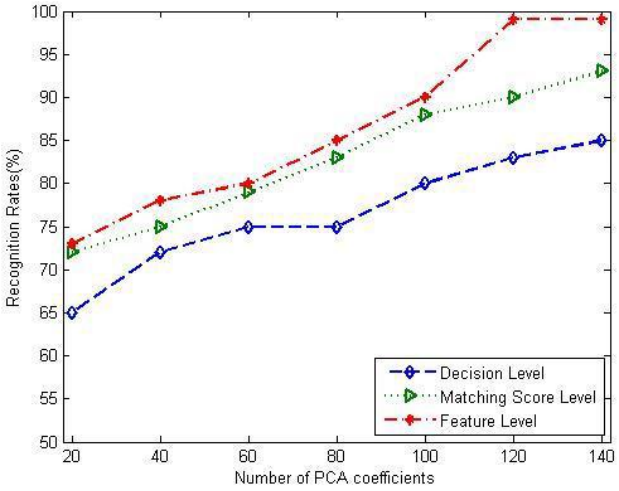

Fig. 3. *Recognition rate analysis of different number of PCA coefficients[22].*

It is clear that the combination of:

- two finger authentications
- E32D facial recognition algorithm
- Feature level recognition of Iris provide the best combination for a multimodal system.

The next sections will discuss the strengths and weakness of Multimodal biometrics.

2.3 Strength of Multimodal Biometrics

Multimodal biometrics systems have proven to solve some problems associated with unimodal systems. Unimodal systems suffer from problems of intra-class distinctions, noise, inflexibility, non-universality, spoof attacks and high error rates[23]. Multimodal systems are able to protect itself from these complications. Intra-class distinctions basically mean that data is spread over a large plane making it difficult to classify data. A multimodal system utilizes more than one biometrics factor and thus the fusion allows more data points to be initialized providing a better classification of data points. The fusion of factors also provides flexibility to the system and prevents noisy data to have substantial effects on the decision. Multimodal systems are generally more secure as there are multiple levels of authentication and it one factor is compromised the remaining factors will be able to secure the system. The system analyses patterns from various biometrics factors which solves the challenge on non-universality. Even if someone does not possess some required factor, the system will still be able to authenticate that person with other factors. While there are many advantages of implementing a multimodal biometrics system, they also face some major challenges.

2.4 Drawbacks of Multimodal Biometrics

Multimodal systems are also facing challenges in various aspects of its implementation. The research has identified the following challenges: (1) multimodal systems are difficult to

design[24], (2) user acceptance is quite low[25], (3) requires higher level of investment[26] and (4) the performance tradeoff[26]. Multimodal system design needs to consider various questions such as what number of factors to be used and which factors to be used. Design also needs to consider an acceptable architecture of the system that considers fusion of multiple biometric factors. Again, the level of fusion becomes a question of concern. Furthermore, appropriate threshold has to be initialized for all the factors to ensure acceptable levels of False Reject Rate(FRR) and False Accept Rate(FAR). Designing a multimodal system will require significant research and experimentation before it can be implemented which could become a costly endeavor. User acceptance is a concern to this emerging technology as success would depend on the acceptance of people. Generally, people do not prefer to pass through too many scans due to reasons such as inconvenience and discomfort. A multimodal system requires acquisition of multiple hardware scanners and Software Development Kits(SDK). While some hardware scanners such as for fingerprint are relatively inexpensive, some scanners are expensive requiring expertise in connection. Finally, as there is a significant upfront investment in the multimodal system, the system has to perform to a standard level of acceptance. Multiple layers of data aggregation and fusion does take its toll on the system. In addition, data generated from the factors can be huge, some ranging to hundreds of columns of data which needs to be preprocessed and normalized.

3 Proposed Solutions to the Challenges

The challenges facing multimodal systems need to be addressed to ensure growth of the technology. Design is one of the major issues of biometrics programming. While there are a number of programming languages and Integrated Development Environments (IDEs) that support image processing and biometrics programming, there is no suitable programming environment that provides easy design and implementation of biometrics applications. Applications currently need to be developed by importing various SDK's for different biometric factors. This task becomes cumbersome and time consuming. A specific IDE designed for developing biometrics application would ease the load of programmers allowing them to focus on better data structures and algorithms for implementation. This would allow for development of robust systems that are both efficient and effective for users. In additions, IDE should be able to handle most of the underlying architectural and technical details such as pre-processing and data management. It is important to work on developing IDEs supporting robust development of biometrics applications. If the systematic details can be handled by a system, then development and research will commence at a much faster rate allowing for greater advancements in significantly less time. The reduced time for development will allow for developers to focus on applications that are user-friendly. Thus, addresses the final issue of multimodal biometrics systems.

4 Conclusions and Future Works

It can be concluded that authentication come in various forms. The most popular among the authentication mechanisms is biometrics. While biometrics started off with simple unimodal systems which normally considered only one biometric factor for authentication, the higher need for security had given rise to a superior system known as multimodal biometric system. Multimodal systems utilize multiple biometric factors in a system allowing the system to be more secure and less stringent with variations in factors. Together with the advantages, multimodal systems also suffer from some major challenges such as difficult design and implementation, higher cost of implementation and lack of user acceptance. However, an IDE that can assist in the development and implementation phase will enable programmers to tackle the challenges faced by multimodal biometrics systems. The development of biometric IDEs will provide future directions for research. Multimodal biometrics systems are the future of authentication.

References

[1] Schneier, B., Walker, J., and Jorasch, J.: 'Remote-auditing of computer generated outcomes and authenticated biling and access control system using cryptographic and other protocols', in Editor (Ed.)^(Eds.): 'Book Remote-auditing of computer generated outcomes and authenticated biling and access control system using cryptographic and other protocols' (Google Patents, 1998, edn.).

[2] Aronowitz, H., Hoory, R., Pelecanos, J.W., and Nahamoo, D.: 'New Developments in Voice Biometrics for User Authentication', in Editor (Ed.)^(Eds.): 'Book New Developments in Voice Biometrics for User Authentication' (2011, edn.), pp. 17-20

[3] Brainard, J., Juels, A., Rivest, R.L., Szydlo, M., and Yung, M.: 'Fourth-factor authentication: somebody you know', in Editor (Ed.)^(Eds.): 'Book Fourth-factor authentication: somebody you know' (ACM, 2006, edn.), pp. 168-178

[4] Pankanti, S., Bolle, R.M., and Jain, A.: 'Biometrics: The future of identification [Guest Eeditors' Introduction]', Computer, 2000, 33, (2), pp. 46-49

[5] Jain, A.K., Ross, A., and Prabhakar, S.: 'An introduction to biometric recognition', IEEE Transactions on circuits and systems for video technology, 2004, 14, (1), pp. 4-20

[6] 6 Jain, A., Flynn, P., and Ross, A.A.: 'Handbook of biometrics' (Springer Science & Business Media, 2007. 2007)

[7] Adhami, R.: 'Peter Meenen and Reza Adhami', 1997

[8] Han, J., Pei, J., and Kamber, M.: 'Data mining: concepts and techniques' (Elsevier, 2011. 2011)

[9] Siskin, A.: 'Visa waiver program', Current Politics and Economics of the United States, Canada and Mexico, 2012, 14, (2/3), pp. 255

[10] Epstein, C.: 'Guilty bodies, productive bodies, destructive bodies: Crossing the biometric borders', International Political Sociology, 2007, 1, (2), pp. 149-164

[11] Bátiz-Lazo, B., and Reese, C.: 'Is the future of the ATM past?': 'Financial Markets and Organizational Technologies' (Springer, 2010), pp. 137-165

[12] Krawczyk, S., and Jain, A.K.: 'Securing electronic medical

records using biometric authentication', in Editor (Ed.)^(Eds.): 'Book Securing electronic medical records using biometric authentication' (Springer, 2005, edn.), pp. 1110-1119

[13] Al-Hijaili, S.: 'Multimodal biometrics fusion techniques', 2011

[14] Lupu, C., Găitan, V.-G., and Lupu, V.: 'Security enhancement of internet banking applications by using multimodal biometrics', in Editor (Ed.)^(Eds.): 'Book Security enhancement of internet banking applications by using multimodal biometrics' (IEEE, 2015, edn.), pp. 47-52

[15] Jain, A., Nandakumar, K., and Ross, A.: 'Score normalization in multimodal biometric systems', Pattern recognition, 2005, 38, (12), pp. 2270-2285

[16] Yan, Y., and Zhang, Y.-J.: 'Multimodal biometrics fusion using correlation filter bank', in Editor (Ed.)^(Eds.): 'Book Multimodal biometrics fusion using correlation filter bank' (IEEE, 2008, edn.), pp. 1-4

[17] Monwar, M.M., and Gavrilova, M.L.: 'Multimodal biometric system using rank-level fusion approach', IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2009, 39, (4), pp. 867-878

[18] Toh, K.-A., and Yau, W.-Y.: 'Combination of hyperbolic functions for multimodal biometrics data fusion', IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2004, 34, (2), pp. 1196-1209

[19] Xu, W.: 'Reference Materials: A Golden Criterion in Nucleic Acid Identification': 'Functional Nucleic Acids Detection in Food Safety' (Springer, 2016), pp. 63-84

[20] Flanagan, P.: 'Fingerprint Recognition', 2016

[21] Ngan, M., and Grother, P.: 'Face recognition vendor test (FRVT) performance of automated gender classification algorithms': 'Technical Report NIST IR 8052' (National Institute of Standards and Technology, 2015)

[22] Sallehuddin, A.F.H., Ahmad, M.I., Ngadiran, R., and Isa, M.N.M.: 'A Survey of Iris Recognition System', Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 2016, 8, (4), pp. 133-138

[23] Akhtar, Z.: 'Security of multimodal biometric systems against spoof attacks', Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy, 2012, 6

[24] Oviatt, S., Cohen, P., Wu, L., Duncan, L., Suhm, B., Bers, J., Holzman, T., Winograd, T., Landay, J., and Larson, J.: 'Designing the user interface for multimodal speech and pen-based gesture applications: state-of-the-art systems and future research directions', Human-computer interaction, 2000, 15, (4), pp. 263-322

[25] Ribaric, S., Ribaric, D., and Pavesic, N.: 'Multimodal biometric user-identification system for network-based applications', IEE Proceedings-Vision, Image and Signal Processing, 2003, 150, (6), pp. 409-416

[26] Ross, A., and Jain, A.K.: 'Multimodal biometrics: An overview', in Editor (Ed.)^(Eds.): 'Book Multimodal biometrics: An overview' (IEEE, 2004, edn.), pp. 1221-1224