Multimodal Biometric Authentication System - MBAS

Dr. Salah M. Rahal
Computer Technology Dept. College of Computer and Information Sciences, King Saud University, P.O. Box 51178, Riyadh11543, KS.A
Tel: +966(1) 4675421
Fax: +966(1) 4675630
Rahal@ccis.ksu.edu.sa

Dr. Hatim A. Aboalsamah
Computer Sciences Dept. College of Computer and Information Sciences, King Saud University, P.O. Box 51178, Riyadh11543, KS.A.
Tel: +966(1) 4678565
Fax: +966(1) 4675630
Hatim@ccis.ksu.edu.sa

Dr. Khaled N. Muteb
Computer Technology Dept. College of Computer and Information Sciences, King Saud University, P.O. Box 51178, Riyadh11543, KS.A.
Tel: +966(1) 4676178
Fax: +966(1) 4675630
Kmutib@digi.net.sa

Abstract

Most biometric systems deployed in real-world applications are unimodal, such as they use a single source of information for authentication (e.g., single fingerprint, face, voice,..). Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity.

In this paper, it is shown that fingerprint and face recognition can form a good combination for a multimodal biometric system and they are used in our work; where the system design in its hardware and software parts is done. The hardware part involves the capture devices, fingerprint signal processing unit, & PC. The software part includes the system software, databases, and face recognition module. The implementation of the system prototype as "Access Control System" with the suitable features was done.

Keywords: Biometrics, Identifier, Minutiae, Fingerprint, Face Recognition, Authentication, and Features.

1- Review

Biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. This technology acts as a front end to a system that requires precise identification before it can be accessed or used.

Utilizing biometrics for personal authentication is becoming more accurate than current methods (such as the utilization of passwords or Personal Identification Number - PINs) and more convenient (nothing to carry or remember). Thus, Biometrics is not just about *security*, it's also about *convenience.*

The need for biometrics can be found in a wide range of commercial and military applications. Thus, biometrics is set to pervade nearly all aspects of the economy and our daily lives.

2- Types of Biometrics

They involve two categories: *Physiological Biometrics & Behavioral Biometrics.*

2-1 Physiological Biometrics

In this category the recognition is based upon physiological characteristics. Some examples are: Fingerprint, Hand Geometry, Iris Recognition, Retinal Scanning, and Facial Recognition [1-7,10,11].

2-1-1 Fingerprint Recognition

Fingerprint is a unique feature to an individual. The lines that create fingerprint pattern are called *ridges* and the spaces between the ridges are called *valleys* or *furrows*. It is through the pattern of these *ridges* and *valleys* that the unique fingerprint is matched for authentication and authorization.

2-1-2 Hand Geometry Recognition

This technology verifies a person’s identity by the size and shape of the hand. The front part of the hand is used for hand geometry measurements. A set of

features have been identified that could be used to represent a person's hand. These features include the finger thickness, length, and width, the distances between finger joints, the hand's overall bone structure.

2-1-3 Iris Recognition

The iris as physical feature of a human being can be used for biometric verification or identification through the process of iris recognition. It is not genetically determined (which means that genetically identical eyes, e.g. the right and left eye of any given individual, have unrelated iris patterns) and it is believed to be stable throughout life. Iris recognition technology is known for it's extreme accuracy: The probability of two individuals having the same iris pattern is 1 in 10^{78}; while The current population of the earth is not more than 10^{10} [4].

2-1-4 Retinal Scanning

Retinal scanning technology is used to measure the unique configuration of blood vessels located at the back of the eye. The retinal image is difficult to capture, and during enrollment the user must focus on a point while holding very still so the camera can perform the capture properly.

As the iris retinal recognition, is generally considered to offer the best security, because of the distinctiveness of the patterns and the quality of the capture devices [5].

2-1-5 Facial Recognition

The "passive" nature* of face recognition makes it more suitable for wide range surveillance and security applications. In particular, an automated face

---

* In contrast, fingerprint, hand and iris recognition are examples of "active" biometric tasks. They require people's cooperation to place hands on a fingerprint or hand reader, or to look into iris scanner.

recognition system is capable of capturing face images from a distance using video camera, and the face recognition algorithms can process the data captured: detect, track and do the recognition. Face recognition focuses on recognizing the identity of a person from a database of known individuals.

Face recognition has several advantages over other biometric technologies: it is natural, non-intrusive, and easy to use.

To prevent a fake face or mold from faking out the system, many systems now require the user to smile, blink, or otherwise move in a way that is human before verifying.

2-2 Behavioral Biometric

Behavioral biometrics is traits that is learned or acquired over time as differentiated from physiological characteristics. Some examples are: Voice Recognition, Signature Recognition and Keystroke Recognition [2,4-6].

2-2-1 Voice Recognition

Voice is a behavioral biometrics. The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound.

These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions (such as common cold), emotional state, etc.

2-2-2 Signature Recognition

The way a person signs his name is known to be a characteristic of that individual. Signature requires contact with the writing instrument and an effort on the part of the user. Signature recognition systems, also called dynamic signature verification systems, measure both the distinguishing features of the signature and the distinguishing features of the process of signing. These features include pen pressure, speed, and the points at which the pen is lifted from the paper. These behavioral patterns are captured through a specially designed pen or tablet (or both) and compared with a template of process patterns.

2-2-3 Keystroke Recognition

It is hypothesized that each person types on a keyboard in a characteristic way. This behavioral biometric is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity *verification*. Keystroke dynamics is a behavioral biometric; for some individuals, one may expect to observe large variations in typical typing patterns. Further, the keystrokes of a person using a system could be monitored unobtrusively as that person is keying in information.

3- Limitations of Unimodal Biometric Systems

Most biometric systems deployed in real-world applications are unimodal, so they rely on the evidence of a single source of information for authentication (e.g., single fingerprint, face, voice,…). These systems have to contend with a

variety of problems such as noise in sensed data, intra-class variations, inter-class similarities, non-universality*, and spoof attacks. It leads, as shown in table –1, to a no neglected false acceptation and reject rates in such systems [8].

Table-1

Biometric	FAR*[1]	FRR*[2]
Fingerprint	**2%**	**2%**
Face	**10%**	**1%**
Voice	**10-20%**	**2-5%**

*[1] False Acceptance Rate *[2] False Reject Rate

Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. These systems allow the integration of two or more types of biometric systems.

4- Selection of adequate identifiers

Based on the following main requirements that biometric identifier to recognize a person should satisfy (i. e. Universality (1), Distinctiveness (2), Permanence (3), Collectability (4), Performance (5), Acceptability (6) and Circumvention (7), *it is shown that fingerprint and face recognition have a very good balance of all desirable properties (Table-2]*.

Table-2

Biometric identifier	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Face	H	L	M	H	L	H	H
Hand geometry	M	M	M	H	M	M	M
Fingerprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Retina	H	H	M	L	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

H: High M: Medium L: Low

* It is estimated that 5% of the population does not have legible fingerprints [9].

On the other hand, as shown in figure-1, Facial and fingerprint features scored very good compatibility in Machine Readable Travel Documents (MRTD) system based on a number of evaluation factors, such as enrollment, renewal, machine requirements, and public perception [7].

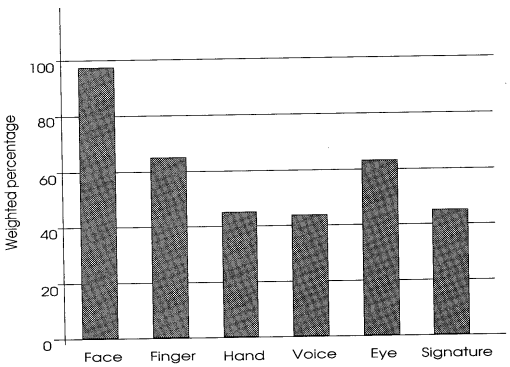

Figure -1

Thus, ***the fingerprint and face identifiers can form a good combination for a multimodal biometric system.***

The fusion of this combination in such systems demonstrates substantial improvement in recognition performance as shown in figure -2 [3]. It is due to the fact that the sources are (fairly) independent. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a 'live' user is indeed present at the point of data acquisition.

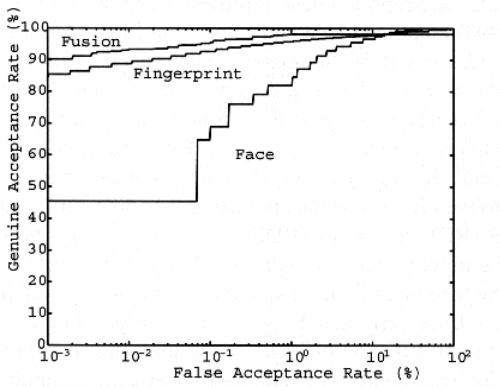

Figure -2

5- Features of selected identifiers

5-1 Fingerprint Features

Fingerprints basically consist of ridges (raised skin) and furrows (lowered skin) that twist to form a distinct pattern (Figure -3).

Although the manner in which the ridges flow is distinctive, other characteristics of the fingerprint called "minutiae" are what is most unique to the individual. These features are particular patterns consisting of terminations or bifurcations of the ridges.

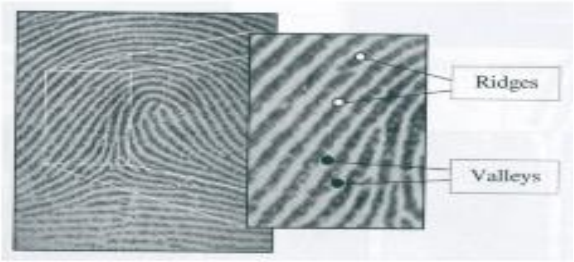

Figure -3

Minutiae features (Figure -4) are particular patterns consisting of [3]:

- ***Ridge ending (Termination)***- a ridge that ends abruptly;
- ***Bifurcation*** - a single ridge that divides into two ridges;
- ***Lake or enclosure*** - a single ridge that bifurcates and reunites shortly afterwards to continue as a single ridge;
- ***Short ridge (independent ridge)*** - a ridge that commences, travels a short distance and then ends;

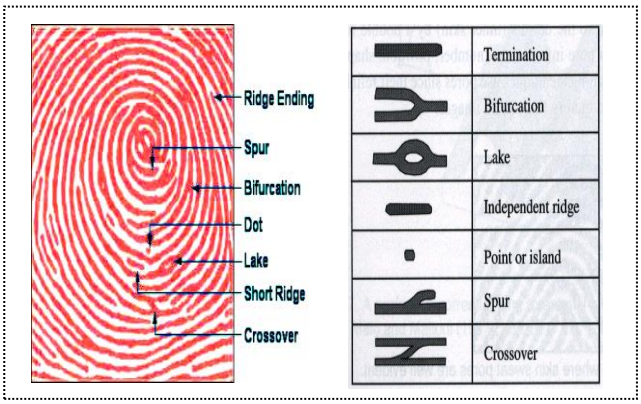

Figure -4

- ***Dot (point or island)*** - an independent ridge with approximately equal length and width;
- ***Spur*** - a bifurcation with a short ridge branching off a longer ridge; and
- ***Crossover or bridge*** - a short ridge that runs between two parallel ridges.

It is these features that are extracted and compared for determining a match in an automatic fingerprint authentication.

5-2 Face Features

Facial recognition analyzes the characteristics of a person's face images. It measures the overall facial structure. Measured features are retained in a database and used as a comparison when a user stands before the camera. In feature-based recognition, these features are of two orders (Figure -5) [10]:

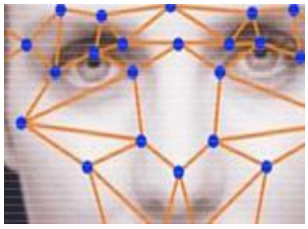

Figure -5

- ***First-order features*** that are individual organs located on a face. They include the following:
  - *Distances* such as length of face. Height of face. Length of mouth. Length of each eye. Length of each eyebrow,…
  - *Area, Angle* such as mouth. Each eyebrow. Each eye,…
- ***Second-order features*** that are the spatial relationships of the individual organs. They include the following:
  - *Distances* such as Right eye-mouth. Left eye-mouth. Left eyebrow-right eyebrow. Left eye- right eye. Left eyebrow-left eye…
  - *Angle* such as left eye-mouth-right eye. Left eyebrow-mouth-right eyebrow…

6- System Design & Implementation

The major issues in designing a fingerprint authentication system include: defining the system identifiers, working mode for each identifiers, selecting hardware and choosing software components for each, making them work together, and defining effective administration and optimization policy.

As shown in paragraph – 4, the fingerprint and face identifiers can form a good combination for a multimodal biometric system and they are used in our work.

The system designer should take into account several factors: Proven technology, system interoperability and standards, cost/performance tradeoff, available documentation, and support.

Based on these factors, the proposed system shown in figure –6 is designed. It consists of the following parts:

- Fingerprint part functioning in "verification mode" and consisting mainly of sensor unit and fingerprint recognition unit.
- Face Recognition part functioning in "verification mode" also. It consists of the camera and a Face Recognition Algorithm.
- PC that is mainly used as administrator PC, processor for face rrrrrr recognition part
    - As PC Administrator.
    - As processor for face recognition part, and for providing the database – 2 of enrolled users.
    - For providing database –3 where all users info (entering time, leaving time, break time,…) are stored.
-

.

PC that is used as administrator PC, processor for face recognition part and For providing database –3

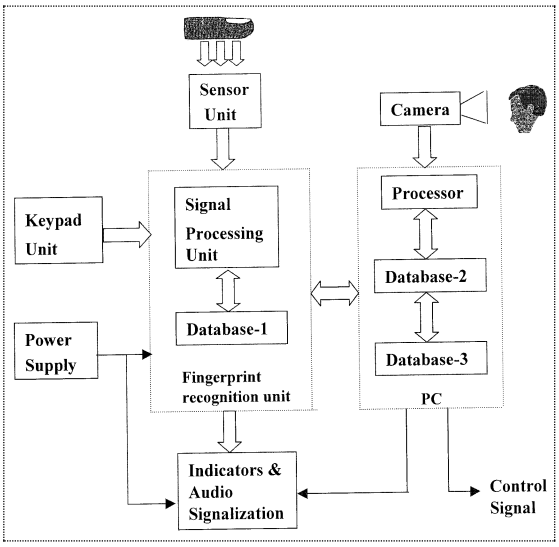

Figure –6

recognition part and for providing database-3.

- Common Units: Keypad, Indicators and power supply unit.

System usage: There are two phases:

1- **Enrollment phase:** The user fingerprint and face features are, for the first time, stored using the sensor and camera, in the database-1 and database-2 accordingly as "user templates". They are assigned with Personal Identification Number, which is entered by the keypad unit.

2- Normal usage: The user enters his PIN by the keypad; the sensor and the camera capture his fingerprint and face; the finger recognition unit compares the fingerprint features with the stored, in database-1, user fingerprint template; the face recognition algorithm extracts the user face features and compares them with the stored, in database-2, user template. The possible cases are:

- **Match (of Fingerprint and face):** Captured user fingerprint and face features are matched with stored fingerprint and face templates: The user is allowed to enter/to go out to/from the establishment. The pass indicator will be lighted for short delay. A control signal (for opening /closing a virtual door will be formed. In case of match of one identifier (fingerprint or face), the user will be temporarily accepted.
- **Non-match (of Fingerprint and face):** The user is not accepted. The fail indicator will be lighted for short delay.

In all these cases the user data will be stored in the database-3 for reference. They will be used for issuing different reports: daily, weekly, monthly,..

7- Conclusion

In the first phase of this research work, we focused on the design of a biometric system using two identifiers. The selection of the used ones was justified. The system is working in the mode 1:1 i.e. in the verification mode. The selection of adequate hardware and software subcomponents was achieved.

The second phase involves the system software coding permitting to issue different reports in Arabic, system assembly, system test and fulfillment of the aimed specifications.

Acknowledgement: The authors thank Mr. Abdullaziz Ahmed Assiri & Mr. Abdulrhman M. AL Hothaily for their valuable efforts.

References:

[1] S. Rahal
Authentication Fingerprint System, First National Information Technology Symposium (NITS 2006): Bridging the digital Divide: Challenges and Solutions, College of Computer & Information Sciences, King Saud University – 2006.

[2] Java Card Special Interest Group – JCSIG: Introduction to Biometrics, 2002
http://www. javacard. org/others/ biometrics_intro.htm

[3] D. Maltoni, D. Maio, A. K. Jain, S. Prabahakar
Handbook of Fingerprint Recognition, Springer, 2003.

[4] Anil K. Jain, Arun Ross and Salil Prabhakar, An Introduction to Biometric Recognition, IEEE, Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004. (Section 8. Multimodal Biometric Systems); http://www.tiresias.org/guidelines/biometric_systems.htm

[5] An Overview of Biometrics, E-Court Conference 2002
http://ctl.ncsc.dni.us/biomet%20web/definition

[6] J. Wayman, A. Jain, D. Maltoni, D. Maio
Biometric Systems, Technology, Design and Performance Evaluation, Springer – 2005.

[7] Stan Z. Li, Anil K. Jain
Handbook of Face Recognition, Springer – 2005.

[8] A. Ross, A.K. Jain
Mulimodal Biometrics: An Overview
12th European Signal Processing Conference (EUSIPCO), Vienna, Austria, pp 1221-1224, 9/2004.

[9] Components of biometrics, Technews, 12/2004

http://securitysa.com/Article.ASP?pklArticleID=3316&pklIssueID=487

[10] Ilker Atalay
Brief Introduction to Pattern Recognition; Face Recognition; Face Recognition Using EigenFace.

[11] Retica Systems Inc. Eye Biometrics, 2005
http://www.retica.com/site/biometrics/index.html