

# Security Requirements for Multimodal Biometric Systems

Kevin Daimi and Katherine Snyder  
Department of Mathematics and Computer Science  
University of Detroit Mercy, Detroit, Michigan 48219, USA  
{daimikj, snyderke}@udmercy.edu

## ABSTRACT

Biometrics systems are automated systems that recognize a person based on physical or behavioral characteristics. There are a number of primary biometric disciplines including fingerprint, facial recognition, voice recognition, iris scan, and retina scan. A multimodal biometric system refers to a combination of the above physiological and behavioral human characteristics. There are many crucial biometric applications, such as passport control, benefit payments, medical insurance fraud reduction, identification of missing children, home banking, secure access to buildings, securing medical records, restriction to access sensitive equipment, and access control to defense forces, government agencies, and restricted areas of an airport. Any vulnerabilities or security breach in these systems will either be very costly or disastrous. In this paper, we will investigate the security requirements for Multimodal Biometric Systems that will help to prevent compromising them.

## Keywords

*Biometrics Systems, Requirements Engineering, Security Requirements, Multimodal Biometrics Systems, Biometric Technology, Security Requirements Process.*

## I. INTRODUCTION

Biometrics systems are automated systems capable of accurately recognizing individuals based on their physiological or behavioral characteristics. The characteristics used may be fingerprints, hand geometry, facial geometry, retina pattern, iris pattern, voice recognition, handwriting recognition, or any other distinguishable available characteristics [1, 6, 14, 22].

There is currently substantial interest and pursuit associated with the use of biometrics in many different areas due to the increased performance of computers,

the reduced cost of biometric technology, the improvements in the internet technology, and the higher level of security awareness. These areas include banking, transportation, healthcare, education, public justice and safety, security, and government. As a result of the advances in biometric technology, computer hardware and software, and based on the many applications of biometrics in the above areas, it is anticipated that a substantial growth will take place in the years ahead. The current status of biometric applications in addition to future growth demand standardization. A number of biometric standards have been or are being developed to support the industry and the technology. Those standards enable high-level interoperability of the data collection and storage processes, and provide a common approach to securing a biometric system regardless of the technology used [18, 21, 22].

The deployment of biometric-based technologies carries with it new terms, techniques, and concepts. The major biometric-based technologies include finger-scanning, hand geometry, facial recognition, iris scanning, retinal scanning, finger geometry, voice recognition and dynamic signature verification. In addition, there are also other more obscure biometric-based technologies such as ear geometry, body odor, keystroke dynamics, and gait recognition. Some experts in the field add DNA-based technology to the above list of technologies [1, 2, 11, 13, 22].

There are many biometrics applications currently available. Examples of these include, easing and securing the passage of people between countries when visas are not required, verifying the legal recipients and holders of social security benefits and food stamps, ensuring a person has not voted twice, identification of criminals, identification of missing children, automated teller machines, home banking, ensuring the security of credit cards, securing medical records and patient records, monitoring plant condition, securing access to

buildings, securing access to a university's labs, verifying people picking up children in a kindergarten, granting access to restricted areas in airports, and defense and government agencies applications.

All biometric systems, regardless of the technology used, operate in essentially the same manner. They follow two characteristics traits: *identification* and *verification*. A biometric sample is captured when the sensor reads some physiological or behavioral characteristics unique to an individual. This is followed by feature extraction resulting in a biometric template. A template is a representation of the captured measurement that retains all the relevant information but with less space. Then this template is compared to the records in the biometric database using a one-to-one search for verification, and a one-to-many search in case of identification. However, a number of metrics are useful in the comparison of biometric-based technologies and may provide some sense of objectivity in the choice of specific technologies. Among these metrics are: False Reject Rate (FRR), False Acceptance Rate (FAR), and the Crossover Error Rate (CER). There are additional factors such as throughput, cost, easiness of use, user acceptance and transparency, while not primary indicators of biometric system performance, are key to the success of any biometric system implementation [1].

A biometric system that relies on a single biometric characteristic in making a personal identification is often not able to meet the desired performance requirements. A multimodal biometric system uses multiple applications to capture different types of biometrics. This allows the integration of two or more types of biometric recognition and verification systems in order to meet stringent performance requirements. A multimodal system could be, for instance, a combination of fingerprint verification, face recognition, voice verification, or any other combination of biometrics. This enhanced structure takes advantage of the proficiency of each individual biometric and can be used to overcome some of the limitations of a single biometric [9, 15, 16, 17, 19].

A security requirement is a manifestation of high-level organizational policy into the detailed requirements of a specific system. Most security requirements are introduced only after functional requirements have been completed [4]. Biometric systems requirements and design processes must be refined to bring an earlier focus on security issues.

Security requirements aim at preventing abuse cases [12]. Other kinds of requirements aim at supporting use

cases. Security requirements are needed to ensure four things: data is used only for authorized purposes (confidentiality), data is correct (integrity), data and processing are available to authorized users (availability), and a person is who claims to be (authenticity).

According to Firesmith [5], most requirements engineers are poorly trained to elicit, analyze, and specify security requirements, often confusing them with the architectural security mechanism that are traditionally used to fulfill them. Instead of specifying security requirements, they end up specifying architecture and design constraints.

Traditionally, security is incorporated in a software system after all the functional requirements have been addressed. Due to its criticality, security should be integrated in the software life cycle [7]. There should be a need for security requirements to be an integral part of the entire software development life cycle. Conventional software requirements engineering methodologies rarely mention information security aspects. They try to avoid system security methodologies to save projects from running late and over budget [10]. The security needs of a given system are often not determined until well into the implementation, resulting in late and expensive attempts to shoehorn security into the work in progress [8]. Security requirements should not be specified in terms of the types of security architecture mechanisms that are typically used to implement them [5].

In this paper, we will investigate the security requirements for Multimodal Biometrics Systems. As biometric systems are security systems, it is extremely essential to ensure that they are absolutely secured themselves.

## **2. OVERVIEW OF BIOMETRICS TECHNIQUES**

To better understand the security requirements, a brief introduction to some of the biometric techniques will be presented. Details of these techniques are beyond the scope of this paper. They could be found in the various biometric references below.

### **2.1 Fingerprint Recognition**

Fingerprinting is one of the oldest and certainly the most widespread means of identification in use today. An individual's fingerprints are defined by a complex combination of patterns: lines, arches, loops, and whorls. An image of a fingerprint is acquired either by optical scanning, or capacitance sensing. Biometric

templates are generated by matching intricate fingerprint features.

## 2.2 Hand Geometry

A hand scanner is a fairly simple device that measures hand geometry to obtain a template of the user's hand. The user places his/her hand in a small device, and positions his or her fingers according to a set of pins on the device. A solid-state digital camera captures the side and top views of the hand, and sends the data to a microprocessor for analysis and comparison against a stored template. Scanners generate templates based on various features of an individual's hand, including finger length. The information used to generate this type of template is often perceived by users to be less reliable than other types of biometric devices.

## 2.3 Eye (Iris/Retina) Recognition

The iris is the colorful part of the eye between the white (sclera) and the pupil. The properties of the iris that enhance its suitability for use in automatic identification include: protection from the external environment, impossibility of surgical modification without risking the vision, and physiological response to light which provides a natural test. Iris recognition is fast, and non-invasive.

The retina, the backside of the eyeball, has unique patterns of blood vessels. In the retinal scan, a biometric template is formed by scanning the retina and recording the patterns of capillary blood vessels at the back of the eye. Once the retina is scanned, special software creates a digital profile of the user's unique pattern of blood vessels. The image is processed and saved in the templates, and these templates are stored in user's identification card or in a central database.

## 2.4 Facial Recognition

Facial recognition can take the form of thermal scanning, or the matching of key facial characteristics. Thermal facial images are unique from person to person. The variation of branching blood vessels throughout one's face creates a different 'thermal' image for each person; even identical twins have different facial thermograms. Facial thermograms apparently do not change during a person's lifetime and are not affected by surface or cosmetic changes to the face; even plastic surgery won't change the thermogram unless it goes so deep as to redirect the flow of blood. Facial recognition by key characteristics involves extracting information such as relative position of eyes, nose, mouth and ears

from photographs of an individual's head or face. Authentication of facial features is quite sensitive to variations in the environment (camera position, lighting, etc.) at enrollment.

## 2.5 Voice Recognition

A person's voice is determined somewhat by behavior patterns, but also by many physical attributes that differ from person to person. Vocal cords vibrate at about 80 times per second for men, 400 times per second for women. These vibrations are modified by the size of the jaw opening and by tongue and lip shape and position — factors that make each person's voice unique. In the voice recognition, the user speaks a specific word into a microphone attached to the system. Software analyzes his or her voice and abstracts significant measures on roughly about twenty parameters (pitch, speech, energy density, waveforms, etc.). This live profile is compared against a profile stored on a central database or the user's card. A good match authenticates the user. An advantage of voiceprint techniques over other forms of biometric is the potential to detect coercion through the analysis of stress patterns in the sample voiceprint.

## 2.6 Signature

Signature is not new as it has long been the means by which we validate all our legal documents. However, absolute validation of signatures is a different matter, and is much more difficult. Some systems use pens with motion-sensing and pressure-sensing devices inside. In this case, a special pen is used that contains a bi-axial accelerometer to measure changes in force in the x and y direction. A force sensor measures the variations in downward (z-axis) force. A person enrolls into the system by signing his or her name a number of times. The computer reads and analyzes the dynamic motions produced by the signer during each signature. Software senses the pen's movements and extracts significant templates. These may include signing speed, sharpness of loops, and changes in pressure. These templates form a profile that is compared to a profile stored on the user's card or in a central database. A good match validates the user. Other biometric signature systems use a magnetic tip pen with a sensitive tablet. These systems analyze only the dynamic changes in the x and y directions, and as a result the hardware required is much simpler. As more and more of the same signature is entered into the system, the system 'learns' the more consistent and more varying parts of the signature. The user's template data can be stored in a database or on a smartcard.

### 3. SECURITY REQUIREMENTS

As mentioned above, we will be dealing with Multimodal Biometric Systems. In Mathematical terms, we will be dealing with systems of the form:

$$T = \sum W_i \cdot S_i, \text{ for } i = 1, \dots, n$$

In this formula, T is the total matching score, W is the weight given to each biometric characteristic such that  $\sum W_i = 1$ , S is the score for an individual characteristic such as finger-scanning, hand geometry, facial recognition, iris scanning, retinal scanning, etc., and n represents the number of characteristics. Any unused characteristic will have a weight of zero.

Security requirements researchers introduced a number of categorizations for security requirements. The aim of these categorizations is to allow a better understanding of the requirements and their important role in the software analysis process, ensure security is achieved, and address the different threats faced by a system. Daimi et al [3] introduced a classification based on the severity/urgency and criticality of the requirements. A security requirement is *critical* if its absence will produce a disastrous impact on the system. A security requirement is *urgent* if it needs to be incorporated immediately into the functional requirements. Firesmith [5] suggested twelve kinds of security requirements, ten of which were addressed in Sommerville [20]. In this paper, we follow the classification of Firesmith [5].

#### 3.1 Authentication Requirements

- The biometric application should verify all the clients that it will serve, before granting them any access to the system
- The system should lock after a certain number of unsuccessful verification attempts
- The biometric application should verify that only enrollment administrators are allowed to create user biometric templates
- The biometric application should verify that only security administrators are allowed to update the configuration parameters
- The biometric application should verify that only audit administrators are allowed to delete or modify records in the audit log
- The system should validate that the captured sample is coming from a live human being

#### 3.2 Identification Requirements

- The biometric application should identify all of its clients that it will serve, before granting them any access to the Multimodal Biometric System
- The biometric application should identify the enrollment (verifying the identity of new users and guiding them through the process), security (managing the configuration parameters), and audit (reviewing audit logs) administrators
- The application should not require an administrator to identify herself/himself a multiple number of times during any session
- All personnel associated with the system should be identified by the biometrics data center before granting them access
- The system should prevent individuals, in general, from enrolling themselves without the presence of an enrollment administrator

#### 3.3 Authorization Requirements

- The system should allow the security administrator to set the False Acceptance Rate (FAR) to a level that assures the verification process, for example, 1 in 50,000.
- The system should not allow an administrator to have access to other administrators' data or functions to ensure independent rolls
- The system should not allow the combination of the rolls of the enrollment, security, and audit administrators to ensure no administrator can create, modify, or delete data without detection
- The system should ensure only the enrollment administrator can re-create a template whenever an indication of improper biometric characteristic capturing is evident
- The biometric database, and the templates are only available to trusted people and programs

#### 3.4 Physical Requirements

- The biometric data center should identify each biometrics device including its type, model number, its configuration and any other relevant information
- All personnel associated with the system should have their identity verified by the biometrics data center before granting them access

- The biometric data center should protect all the computers, biometric measuring devices, and communication equipments from any damage
- The physical connection between the biometric devices used should be properly secured
- The biometric data center should provide personal protection for their enrollment, security, and audit administrators in addition to all other important individuals
- The biometric data center should verify the type, model number, configuration and any other relevant information for each biometrics device to ensure no device has been replaced/modified

### **3.5 Immunity Requirements**

- The system should scan any template presented to it for known viruses and other harmful programs
- The system should ensure all client application that it serves are free of infectious programs
- The system should have disinfection capabilities available in case of emergency
- The system should inform the Security Administrator about any harmful program/data it detects

### **3.6 Privacy Requirements**

- The system should indicate what parts of it are allowed to be accessed by authenticated applications
- All captured data should be deleted or moved to a secure storage after the template is created
- The system should allow the security administrator to ensure data is properly encrypted
- No other personal information apart from the biometric data should be stored
- The system should not disclose to a user any information regarding the matching score of the captured sample

### **3.7 Intrusion Detection Requirements**

- The system should prevent an identical captured characteristic from being used in repeated manner
- The system should reject all exact matches
- Any attempt to access the system should be prevented or at least detected
- The system should have access to intrusion detection and prevention software

### **3.8 Auditing Requirements**

- Unauthorized access to the biometric database should be reported to the Security Administrator
- The system should ensure all the relevant information regarding the unauthorized access are recorded
- The system should collect, store, and organize all the necessary information for auditing purposes including identification, authorization, and authentication information
- Audit trails and audit event logs should be kept and protected by the system

### **3.9 Integrity Requirements**

- The system should ensure the confidentiality and integrity of biometric templates and live samples
- The application should prevent the unauthorized corruption of templates captured from various biometric devices
- The system should ensure the security of all biometric data before it is transmitted from one device to another

### **3.10 Survivability Requirements**

- The system should ensure that all external communication channels are protected against any corruption
- If one of the biometric characteristics failed to identify a user, others should be able to work properly

### **3.11 System Maintenance Requirements**

- The system should ensure that security is enhanced or at least maintained whenever a hardware or biometric device is repaired or replaced
- The system should ensure that security is enhanced or at least maintained whenever a biometric software or communication software is either updated or replaced

### **3.12 Nonrepudiation Requirements**

- The system should require the signature, or any other means, to be added to the modified record prior to granting the modification privilege

## 4. CONCLUSIONS

To ensure more reliable verification and identification security checks, traits that really characterize a given person should be employed. Biometrics furnish this purpose as they offer automated methods for identification and verification based on measurable physiological or behavioral characteristics such as fingerprint, iris, and retina recognition.

Security is a necessity due to the nature of today's society. Security requirements play a crucial role in all software systems. This is particularly true when the software system is a security system itself. If a security system, such as a biometric system, is compromised, disastrous consequences are to be expected.

In this paper, we have attempted to overcome the vulnerabilities that could exist in Multimodal Biometrics Systems. We believe that compromising such systems will be prevented by enforcing the security requirements stated above.

## 5. References

- [1] A. Cavoukian, (1999, September 1). Consumer Biometric Applications: A Discussion Paper [Online]. Available: <http://www.ipc.on.ca/docs/cons-bio.pdf>
- [2] J. Chirillo, and S. Blaul, Implementing Biometric Security, New Jersey: Wiley, 2003.
- [3] K. Daimi, and C. Wilson, "Electronic Voting System Security requirements Engineering," in Proc. The International Conference on Software Engineering Research and Practice, Las Vegas, USA, 2005, pp. 230-235.
- [4] P. T. Devanbu, and S. G. Stubblebine, "Software Engineering for Security: A Roadmap," in Proc. 22<sup>nd</sup> International Conference on Software Engineering, 2000, pp. 227-239.
- [5] D. G. Firesmith, "Engineering Security Requirements," Journal of Object Technology, vol. 2, pp. 53-68, Jan. 2003.
- [6] M. C. Frye, "The Body As a Password: Considerations, Uses, and Concerns of Biometric Technologies," MS Thesis, Graduate School of Arts and Sciences, Georgetown University, Washington DC, 2001.
- [7] D. P. Gilliam, T. L. Wolfe, J. S. Sherif, and M. Bishop, "Software Security Checklist for the Software Life Cycle," in Proc. WETICE'03, 2003, pp. 243-248.
- [8] C. B. Haley, R. C. Laney, and B. Nuseibeh, "Deriving Security Requirements from Crosscutting Threat Descriptions," in Proc. The International Conference on Aspect-Oriented Software Development, 2004, Lancaster, UK, pp. 112-121.
- [9] M. Indovina, U. Uludag, R. Snelick, A. Mink, and A. Jain, "Multimodal Biometric Authentication Methods: A COTS Approach," in Proc. Workshop on Multimodal User Authentication, Santa Barbara, CA, 2003, pp. 99-106.
- [10] M. Kis, "Information Security Antipatterns in Software Requirements Engineering," in Proc. PLoP 2002, 2002, pp. 1-7.
- [11] S. Kung, M. Mak, and S. Lin, Biometric Authentication: A Machine Learning approach, New Jersey: Prentice Hall, 2005.
- [12] S. Lauesen, Software Requirements Styles and Techniques, Guilford: Addison Wesley, 2002, pp. 266-278.
- [13] S. Nanavati, M. Thieme, and R. Nanavati, Biometrics: Identity Verification in a Networked World, New Jersey: Wiley, 2002.
- [14] Z. Riha and V. Matyas, "Biometric Authentication Systems," Faculty of Informatics, Masaryk University, Brno, Czech Republic, Rep. FIMU-RS-2000-08, 2000.
- [15] A. Ross, A. Jain, and K. Nandakumar, Multimodal Biometrics: Human Recognition Systems, London: Springer, 2006.
- [16] A. Ross, and A. Jain, "Information Fusion in Biometrics," in Proc. AVBPA, Halmstad, Sweden, 2001, pp. 354-359.
- [17] A. Ross, and A. Jain, "Learning User-Specific Parameters in Multibiometric System," in Proc. The 5th international conference on Multimodal interfaces (IEEE ICIP), Rochester, NY, 2002, pp. 68-72.
- [18] A. Sasse, "Assessing the Biometrics Enterprise: The present Situation and Future Challenges," IEE Seminar on the Challenge of Biometrics, 2004, London, UK.
- [19] R. Snelick, M. Indovina, J. Yen, and A. Mink, "Multimodal Biometrics: Issues in Design and Testing", in Proc. The 5th International Conference on Multimodal Interfaces (ICMI 2003), Vancouver, Canada, 2003, pp. 68-72.
- [20] I. Sommerville, Software Engineering, New York, NY: Addison Wesley, 2004, pp. 204-207.
- [21] C. Tilton (2003). Biometric Industry Standards: A White Paper [online]. Available: [http://www.saflink.com/pdf/Bio\\_Stds\\_CTilton.pdf](http://www.saflink.com/pdf/Bio_Stds_CTilton.pdf)
- [22] J. Woodward, N. Orleans, and P. Higgins, Biometrics, New York, NY: McGraw Hill, 2003, pp. 25-41.