Biometrics: Fingerprint Authentication

By

Kareem Sumner

For
Information Security

Instructor
Jerome Alston

April 25, 2001
# Table of Contents

Introduction pg. 2  
What is Biometrics? pg. 2  
Fingerprint Verification pg. 3  
  Optical technology pg. 3  
  Silicon technology pg. 3  
  Ultrasound technology pg. 3  
Three methods of storing a fingerprint template pg. 4  
  Within the device pg. 4  
  In a central Database pg. 4  
  On a token pg. 5  
Authentication and Identification pg. 5  
Issues and Concerns pg. 6  
  Privacy pg. 6  
  Inadequate Standards pg. 6  
  Performance Measures pg. 6  
  Accuracy pg. 7  
Benefits of Fingerprint Technology pg. 7  
Current Applications deploying Biometrics pg. 8  
Conclusion pg. 9  
Diagrams pg. 10  
  Figure 1: Graph of FRR, FAR and EEP pg. 10  
  Figure 2: Damaged Fingerprints pg. 10  
  Figure 3: General Biometric System pg. 11  
References pg. 12
INTRODUCTION

Technology is growing exponentially and is linking countries, industries, and individuals like never before. Globalization is becoming more of a realization and borders are becoming non-existent. Security is always a concern when implementing new systems, accessing corporate intranets or networks, gain access to sensitive information or even secure buildings or rooms.

In lieu of the tragic events that occurred on September 11th, 2001, the sense of security, and not just national security, has been heightened. There is a lot of buzz about implementing biometric security systems in various types of applications (i.e. driver’s license, airport security, national ID cards, borders and immigration etc.). Biometric systems have been in use for some time now, but many forms of biometric technology have come under heavy dispute from the public. People complain that the technology is too invasive and fear that their privacy will be compromised.

This paper will briefly describe the various biometric technologies that exist, but the primary focus will be on the fingerprint technology.

WHAT IS BIOMETRICS?

There are three conventional methods of identification in use today. One is something a person has, such as a card. The second is something that the person knows, such as a password or PIN code. The third is something a person is, such as a fingerprint; or something a person does, such as writing or speaking. Biometrics is the third form of identification and is described as a technology that identifies persons based on their unique physical and biological qualities. The technology ranges from fingerprints, retinal and iris scan, voice and facial recognition, hand geometry, signature verification and others. Biometrics can be divided into two classifications: physiological characteristics and behavioral characteristics. Physiological biometrics includes fingerprints, hand geometry, eye patterns, and facial features. Behavioral biometrics is the voice and signature recognition.

Retinal scanning scans the patterns of the retina using a low intensity light source via an optical coupler. It is rather accurate, but it inconveniences the user if they are wearing glasses. It can be intrusive to the user because something as sensitive as their eyes must make contact with the device.

Iris scanning uses a camera to photograph the iris in front of the eye. It is not intrusive as retinal scanning since a user can stand as far as three feet away from the camera. It can also work with the user wearing glasses.
Voice recognition has been integrated into telephone headsets and also devices that are mounted on walls to gain security access. Facial recognition scans the characteristics of the face. It can measure the distance between each pupil or the width of the mouth.

Hand geometry measures the physical characteristics of a person's hand and fingers using a video camera and compression algorithms.

The fingerprint verification is a more popular technology than all of the other technologies mentioned.

FINGERPRINT VERIFICATION

Fingerprinting has been around for a long period of time. Police departments have been using fingerprinting to identify criminals. The advancement in technology has allowed for the digitizing of fingerprints. There are devices that emulate the methods of the police by matching minutiae – the ridges and swirls on the bottom of a person's finger. The other approach is using global pattern matching – where the flow of the ridges is compared at all locations between a pair of fingerprint images. It is the capture of these distinctive characteristics of the human fingerprint that finger-scan biometrics is based.

There are three methods in use today to capture the fingerprint image with sufficient resolution and detail. The technologies are optical, silicon, and ultrasound.

**Optical** technology has been in use for a long period of time and is the most widely used. The device, usually a charged coupled device, converts the fingerprint image of dark ridges and light valleys, into a digital signal. The brightness of the image can be adjusted to enhance the image quality. These optical devices are relatively inexpensive, have been proven over time and can provide resolutions up to 500 dpi (there may be systems that have higher resolutions). Its biggest drawback however, is the underlying fingerprints that are left over from previous users. This may cause image degradation as the fingerprints may merge together.

**Silicon** (or chip) technology was introduced in the early 90’s and is based on DC capacitance. Silicon usually produces a better image quality using less surface area than optical. The sizes of the chips are getting smaller and less expensive so they can be implemented in many devices. Its resilience in sub-par conditions though, is yet to be proven.

**Ultrasound** technology is probably the most accurate of the three technologies, but is not yet widely used. It uses acoustic waves to measure the distance based on the impedance of the finger, the platen and air. It is capable of penetrating dirt and residue on the platen and finger.
When scanning a fingerprint, features are extracted from the image by a process known as feature extraction and a compact template is created. The full fingerprint image however, is not stored; only a small amount of calculated, mathematical data based on the minutiae (fine details concerning the ridges in a fingerprint pattern) is stored. Therefore, the full fingerprint cannot be reconstructed from the template. This phase/process is called enrollment. The fingerprint template is enhanced by the scanning device to reduce any distortion of the fingerprint caused by dirt, cuts, scars, sweat, burns and dry skin. The template is then converted into a usable format and stored in a database that can be searched and compared using an Automated Fingerprint Identification System (AFIS). AFIS compares the person’s fingerprint with the template in the database and determines if there is a match. This is known as the verification process (see figure 3 on page 10).

THREE METHODS OF STORING A FINGERPRINT TEMPLATE

There are three alternative ways, depending on the system being implemented, to store a template.

I. Storing the template within the device

   A. Advantages
      1. Allows for fast operation
      2. Holds a relatively small amount of templates
      3. More efficient in the verification process
      4. No external process is needed to access the template

   B. Disadvantages
      1. Device is vulnerable to physical abuse and power loss etc.
      2. Device must be present and functioning properly
II. Storing the template in a central database

A. Advantages
   1. Secure network environment
   2. Quick template retrieval depending on network throughput
   3. Backup procedures or systems in place

B. Disadvantages
   1. Large databases can slow down retrieval process
   2. Data traffic or bottlenecks can slow down verification process
   3. Network failure

III. Storing the template on a token (card)

A. Advantages
   1. Requires no local/central storage of templates
   2. Users have effective control over their templates
   3. Use other ID for backup purposes

B. Disadvantages
   1. User must re-enroll if token/card is stolen, lost or damaged
   2. Cost and complexity of system

AUTHENTICATION AND IDENTIFICATION

During the authentication process a user’s identity is verified. This usually occurs during the initial enrollment of a user and he may have to provide another characteristic, such as a password, social security number, driver license etc., along with his fingerprint to authenticate his identity. This is known as a one-to-one matching process because the user’s fingerprint does not exist in the database and it is only verifying the user.

The identification process occurs after a user’s fingerprint has already been enrolled into a system and a search is done on the database to find the matching fingerprint.
This is a one to many matching process because a search is done against a database filled with relevant data.

ISSUES AND CONCERNS OF FINGERPRINT AUTHENTICATION

Even though fingerprint scanning maintains a high level of security, there are still some public concerns about the technology. Aside from the psychological effect of being fingerprinted like a criminal, many people think it can be too invasive.

Privacy

Privacy is a major subject when it comes to any biometric technology. People want a higher degree of security but at the same time not have their privacy compromised. Since fingerprint templates are usually stored in large databases, people question whether their information (or the entire database for that matter) can be sold, modified, or manipulated by authorized (or unauthorized) persons. It is quite possible that the Federal government or private organizations will collect bio-information for one purpose and use it for another (much like a Trojan horse virus). Disclosing personal information is indeed a sensitive matter and should be safeguarded by trusted persons who scan and store the images with the individual’s consent. People also fear that each enrollment of their fingerprint will be audited and the information stored in a database.

There is also the issue of using one biometric technology for many applications – making it more centralized, or use multiple biometrics (a term referred to as balkanization). What may seem as a minor security risk may only need voice recognition (i.e. starting certain programs on a home PC). An application with a higher security may use fingerprint or iris scan (to gain access to buildings or secure rooms etc.). Will the general population be willing to sacrifice more than one body part for different application for even greater security?

Inadequate Standards

There are a wide variety of scanners and software to capture and store fingerprint images. The lack of standards makes it difficult to use fingerprint templates across different systems and application. This means that for every application that requires a fingerprint, an individual must enroll into each and every system.

Performance Measures

With any type of biometric there is a chance that an individual is unidentified, intentionally or worse yet unintentionally. A False Rejection Rate (FRR) occurs when an authorized individual is not allowed access to a system, building or any other application. This person has been falsely rejected and can cause an inconvenience for the person which is the opposite of what biometrics is supposed to provide. Also a False Acceptance Rate (FAR) allows unauthorized person’s gain access to secure
applications. These imposters or intruders are no different from crackers, hackers or even cryptanalysts. Depending on the type of application and its security level, the threshold can be adjusted. It can be manipulated by setting the biometric device to accept a larger number of false accepts but smaller number of false rejects (ideal in a less secure environment), or a larger number of false rejects but smaller number of false accepts (ideal in a more secure environments).

Many developers of finger-scan devices use these performance measures to sell their devices. The lower the error rate (which is usually around 0.1% - 0.3% depending on the accuracy of the device and the size of the database) of the FRR or the FAR, the more accurate the device is. A more realistic measure of performance although, is somewhere in between, called the Equal Error Rate (EEP) (see figure 1 on page 9).

Accuracy

Accuracy of fingerprint images that have been scanned by devices is also questionable. Even though an individual's fingerprints are unique, there may be cases where the scanning of the fingerprint has been distorted. This can occur from dirt, scars, sweat and dry skin. Bad prints can come from a person with skin infections, those who have been exposed to chemicals and also mechanical abrasion (see figure 2 on page 9). Depending on the job or hobby, someone who constantly uses their hands (i.e. construction workers, cleaners and even guitarists etc.) may have extremely cracked fingerprints. This can increase the FRR and possibly the FAR error rate.

BENEFITS OF FINGERPRINT BIOMETRICS

With all of the issues surrounding fingerprint biometrics and biometrics in general, it still has some strong advantages. First of all, fingerprint scans are usually fast, accurate, reliable and convenient. The current security methods of using passwords, PIN codes, keys and cards are all unreliable (or as reliable as the user) because they can be forgotten, lost or stolen. People have to remember so many passwords and PIN codes to gain access to different applications from company networks to ATM's, that they sometimes write their passwords down (usually in places visible by onlookers) so they are not forgotten. These passwords can be compromised by seamlessly 'innocent' onlookers or decrypted by hackers. With biometrics a person can never forget their password – it is a living part of them. It increases the integrity and authenticity of identifying a person.

Secondly, there cannot be multiple, different enrollments of a single fingerprint. There is one person, one identity. As mentioned earlier, the full characteristics of a fingerprint is not stored in a database, only a template that cannot reproduce the full fingerprint image. For additional security, the template is encrypted and can only be broken by an exact match. Fingerprint biometrics is possibly the most cost-efficient, convenient and widely used method for verifying a person's identity. It is convenient for quicker access
to certain applications that would ordinarily be time consuming. Further advances in the technology will reduce the costs of scanning devices and systems.

Thirdly, biometrics can decrease the credit card fraud rate. Credit cards are either lost or stolen and used by unauthorized persons to make unauthorized purchases via the Internet or over the phone. These transactions do not require the person to be present or to provide and identification accept maybe a billing address. This smart credit card will not only decrease fraud, but will be able to contain more value, information and functionality. Finger-scans can increase the security and privacy in the medical area by controlling access to medical records and procedures for both patients and doctors. Audit trails can be used on persons who viewed or modified certain data.

As far as standardization being an issue, NIST and the Biometric Consortium have established the Biometric Interoperability, Performance, and Assurance Working group to expand the deployment and acceptance of biometric technology. Its purpose is to support the advancement, compatibility and interoperability of biometric solutions nationally and globally.

APPLICATIONS CURRENTLY ADOPTING BIOMETRICS

Biometric systems are more recognized in the public domain than the private domain. Private organization have adopted some type of biometric system to gain access to buildings, secure rooms, networks etc., but they are mostly known to people that belong to those organizations.

Prisoner visitor systems use fingerprint scans to verify visitors so that inmates and visitors cannot be switched.

Biometric driver licenses are being adopted in some states. Truck drivers especially have been issued these licenses to cross state lines. In lieu of the 9/11 attack, the government is pushing to adopt a nationwide, standardized biometric driver license incorporating an individual’s fingerprint for verification.

Benefit payment systems are using various biometric techniques to decrease the number of person’s falsely claiming benefits.

Border control and Immigration (in the US) use a system called INPASS which is a card that has a person’s fingerprint embedded into the card. This improves the ‘filtering’ of illegal immigrants and reduces long waiting lines.

ATM’s in Europe and Australia are making use of portable finger-scanning devices that can be plugged into the ATM and have users access their accounts using their fingerprints.

Airline agencies, such as British Airways, are using a biometric travel smart card for more convenient immigration processes.
Workstations and network access are becoming more popular using finger-scan devices for employees to access systems and the company’s network.

There are other numerous applications that use some sort of biometric technology; the army for enrollment and the purchasing of goods, voting systems, banks, high schools and universities for meal plans and other snack vending machines. Future applications may consist of internet transactions, international identification cards, and automobile and home access just to name a few.

CONCLUSION

There are many reasons why biometric technology is met with great opposition. Privacy, identity theft, mistrust and misuse of collected data are the major factors that people fear in deploying biometrics. Since the tragedy of 9/11 however, people have been swayed to utilize the technology for increased security and peace of mind. Even though there is a negative connotation and an aura of criminality using the finger-scan technology, it is still the popular choice due to its cost-effectiveness and non-invasiveness. As long as people are informed of what data is collected and why, a minimum amount of data is collected and used only for the original purpose, users are allowed to correct their records, then people will be more receptive of fingerprint biometrics.

Biometric devices are the future technologies since traditional technologies of passwords and PIN codes are insufficient to reduce fraud and protect our computer systems, networks, and even our own identities. It is imperative to use these technologies in various applications where security is the highest priority, i.e. Law enforcement, physical access control and banking. Securing sensitive data on the Internet is a popular concern and will be a part of the future applications for biometrics. Internet banking and electronic commerce will be sectors where biometric technologies will provide a natural and logical solution.
Figure 1: Graph of FRR, FAR and EEP

Figure 2: Damaged Fingerprints
This is the general process of enrolling and identifying a user using various biometric methods. The devices and body parts that are used may be different, but the basic process is the same.
References


