Security Issues in Biometric Identification

Anthony Delehanty
University of Minnesota, Morris
dele0064@morris.umn.edu

ABSTRACT

In this paper, we provide a brief overview of biometric identification including the processes used and the types of attacks that are possible. in order to provide a better idea of the technical challenges we delve into more detail on the intricacies of hashing and watermarking. We outline several security flaws present when using biometric identification including problems with the nature of biometrics, and summarize a few methods to deal with these security issues. These methods include hashing in different ways, introducing additional biometric identifiers, and creating effective watermarks to make the systems more secure.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Authentication*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Physical Security*; K.6.m [**Management of Computing and Information Systems**]: Miscellaneous—*Security*

General Terms

Security, Verification

Keywords

Integrity Verification Scheme, Watermarking, Biometrics

1. INTRODUCTION

Biometric data is data inherent to one's body, and almost always is unique to an individual. There are many forms of biometric identifiers. These include, but are not limited to: fingerprints, retinal scans, DNA, voice, gait, hand shape, signatures (not only the shape, but also the pressure used and the speed it takes to sign), and facial scans [6]. Unfortunately, some biometric identifiers, such as siblings' facial scans and identical twins' DNA are not unique. In addition, some forms of biometric data do not work well in large groups, such as facial scans, palm shape scans, and a person's gait, but these data are easy to gather, and work very well for a small group.

Biometric data's uniqueness makes it an effective form of identification, as the user does not need to remember a password, Personal Identification Number (PIN), or carry an identification card. All the user needs to do is scan a fingerprint, retina, or use another unique identifier.

However, just like any other identification system, there are security issues inherent to biometric identification. Not only are standard security issues such as insecure databases present, but the presence of a biometric scanner invites other forms of manipulation, such as mimicking a person's gait, or providing a copied fingerprint.

Furthermore, if someone were to gain access to a database of biometric identifiers, the intruder could potentially access a person's fingerprint, retinal scan, or other information which a user would like to keep secret [9].

In addition to these issues, biometric identification carries risks which are unique to it. In a traditional password or other authentication system, the user wants the information to be private. This privacy is what makes the authentication system work. Biometric information is not at all private. People leave their fingerprints everywhere; a retinal match could be made with a high-resolution photo; and anyone who would like to mimic someone's gait simply needs to observe him or her for a period of time.

Additionally, if someone gains access to a biometric identifier, that identifier is permanently compromised. If someone guesses your password, it is usually trivial to change that password. However if someone gains a copy of your fingerprint scan, you can only change this identifier nine more times, by switching fingers. In the cases of retinal and palm scans, you can change this information once, and in the cases of DNA and facial scans, once someone obtains your identifier, you need to change the authentication system in order to keep them out. Similarly, if someone guesses a password that you use for multiple systems, it is usually trivial to change it across all of the systems. However, if someone obtains your biometric identifier, they can use it to access anything which you use that identifier for.

The manner in which biometric data is stored is also relevant. Some forms of biometric data, such as a fingerprint, can change based on how much oil the skin has, or cuts on the finger. Because of this, precise matching is often impossible, so the traditional method of hashing (reducing a large segment of data into a smaller one which is based on the larger segment) does not work, as the differences can cause

UMM CSci Senior Seminar Conference, April 2011 Morris, MN.

a different hash to be developed.

2. BACKGROUND

2.1 Usage

Typically, the first time someone uses a biometric scanner, the scanner performs an *enrollment* [9]. During enrollment, the system will store the user's biometric information to be matched on future uses. During authentication, the system checks the user's information and then compares it to the information on file for that user. If a match is found, the user is approved, if no match is found, the user is rejected.

2.2 Modern Uses

In the modern world, there are numerous uses for biometric identification, and all of them have their own strengths and weaknesses in terms of security.

Smart-card Security

People use cards for everything from payment (credit and debit cards) to unlocking doors. If an individual loses a smart-card, it would be trivial for someone else to gain access to that person's bank account, place of work, or other information stored on the cards.

In order to prevent this security breach, some cards have fingerprint scanners on them. The cards use these scanners by either employing fingerprint *matching* or fingerprint *mapping* [1].

In fingerprint matching, the smart-card stores a copy of the owner's fingerprint, and the user must provide a matching fingerprint in order to get the card to transmit its information whenever the information is accessed. In fingerprint mapping, when a valid fingerprint is scanned the card temporarily deactivates a lock on the information stored in the card. This information can then be accessed as many times as the user desires without a further scan. When the user would like to stop the information from being accessed, he or she simply rescans his or her fingerprint, and the data cannot be accessed until the user scans a fingerprint once again.

Identification

Biometric identification is used in many other places throughout the world as well. In February 2011, India started their Universal ID program. The goal of the program is to provide each of India's 1.2 billion residents with a unique identification number. Each number will be based on the person's fingerprint scans from all ten fingers, iris scans from both eyes, and a facial scan [5]. In addition, the United States uses fingerprints to identify immigrants and many hospitals uses some form of biometrics to validate that a patient is who he or she claim to be.

3. SYSTEM VULNERABILITY

There are two basic types of failures in a biometric system [2]. The first group, *intrinsic failures*, deal with limitations in the hardware or software, and are not caused by an outside attack. As such, they will not be discussed in this paper. The second, *failures due to an adversary attack* are caused by an outside agent directly manipulating, either intentionally or accidentally, the hardware or software used in the biometric system. Attacks on the system can further be classified as physical attacks if they are aimed at hardware, or system attacks if they are aimed at software.

3.1 Types of Adversary Attacks

There are many types of adversary attacks, the most basic of which involves directly manipulating the biometric scanner. However, these attacks can be attacks on the software as well.

Insider Attacks

This form of attack includes any failure or manipulation of the biometric system by those who directly oversee or operate it. Such attacks may be accidental, for instance the owner of the system neglecting to validate credentials a potential user provides and failing to authenticate that users are, in fact, who they say they are. However, insider attacks can also be caused by the owner or operator of the system intentionally allowing an unauthenticated person to authenticate, or an authorized user of the system allowing an unauthorized person access to the system.

Such attacks are outside the scope of this paper, as they deal with personnel management instead of software or hardware solutions.

Biometric Overtness

This method of attacking involves tricking the biometric scanner itself into incorrectly identifying the user as an authorized person. Examples of these include using lifted finger prints, making a gummy eyeball, or attempting to mimic someone's gait.

While this is the most basic security issue in biometric passwords, it is also one of the most easily solved, as will be discussed in Section 4.1.

Non-secure Infrastructure

This kind of attack includes any attack which involves manipulating the data being passed at any point in the authentication process after the scan has been made. These attacks usually involve finding security breaches in either the database where the users' authentication data is stored or security breaches in the data itself, such as poor data encryption.

4. A FEW POTENTIAL SOLUTIONS

4.1 Securing Hardware

There are several things that one can do in order to combat physical attacks on a biometric scanner.

Physical Security

One method of protecting a scanner is to increase the physical security present. This can include adding a person or camera watching the scanner, or requiring a password to access the scanner. This however would defeat the purpose of biometric identification, and is not recommended. Because these methods do not involve the biometric system itself, they will not be further discussed in this paper. However, it is oftentimes trivial to get around these methods, so while the use of them can help, a determined attacker should not have any difficulty bypassing them.

Securing Your Scanner

One of the simplest methods of preventing a physical attack is to add complexity to your scanner. In order to protect against false fingerprints or retinal scans, a heat sensor could be used to ensure that a real finger or eyeball is being used [3]. A signature scanner could include a pressure pad to ensure that a user is not trying to trace a copy of someone's signature.

4.2 Securely Matching Fingerprints

Shenlin Yang and Ingrid M. Verbauwhede of UCLA proposed a method of securely matching fingerprints [12]. Commonly used methods include image-based matching, graph-based matching and minutiae-based matching. Minutiae-based matching compares the differences in the details of the fingerprints instead of the fingerprints themselves for a match. Such details include the types of minutiae present, and their distance from each other [4]. Fingerprint minutiae are minor details in the fingerprint which set it apart from other fingerprints. Major types of minutiae include ridge endings, ridge bifurcations, ridge enclosures, short ridges, islands, spurs, crossovers, deltas, and cores [8].

Image-based matching uses the entire gray scale fingerprint as a template to match against other fingerprints. This method is very inconsistent, as it is difficult to account for minor variation. Graph-based matching represents the minutiae in the fingerprint in the form of graphs. However, this method has a very high computational complexity, which limits its practical use. Because a minutiae-based matching system uses more discriminating and reliable features, and provides higher processing speed and a much lower template size of biometric information, Yang and Verbauwhede decided to base their system on minutiae matching.

The authentication algorithm works by comparing a minutia's neighbors to the neighbors of the corresponding minutia in the database. See Figure 1 for examples of minutiae, the neighbors of the lower circled island would be the circled bifurcation and enclosure.

As stated earlier, the security of the biometric data itself is important, not only the scanner. To address this concern, some biometric systems try to move the signal processing and matching engines from the server to the embedded device (in this case, the biometric scanner). In this type of system, the biometric data is processed and matched within the scanner itself, and the result of the processing and matching is sent to the server, instead of the full fingerprint. This approach avoids many attacks on the communication between the scanner and the server, and on the server itself. Unfortunately, it is relatively simple to compromise the biometric templates which are stored in the scanner. As a result, the template is often encrypted.

When a request comes in, the encryption key is used to decode the template, which is then used to process the input. However, this key is able to be extracted by analysis of external effects such as timing, electromagnetic radiation, and power consumption. This type of attack is called a Side Channel Attack (SCA), and the most common form of SCAs is a Differential Power Analysis (DPA). A DPA is an attack which monitors the power usage of the device, and can tell a match by the different power consumptions. SCAs are most effective against a portable device, as there is often not enough room to add excess processing to be used as noise to trick the attacker.

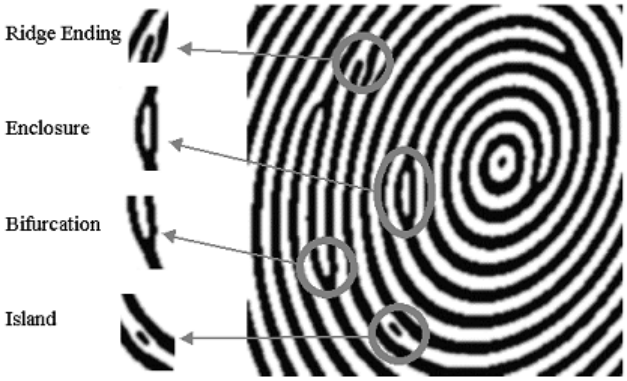

Figure 1: Several types of fingerprint minutiae.

Yang and Verbauwhede's system counters this problem by splitting the process into two sections: a non-secure section, and a secure section which runs on a DPA-proof platform. Everything in gray in Figure 2 is inside the secure portion, while everything out of the gray area is in the non-secure portion. To counter information leak from the secure portion, Sense Amplifier Based Logic (SABL) is used to handle the storage and processing of the above. SABL is designed with a constant power consumption and other methods to stop the emission of side channel information.

As technology has developed, SCAs, and DPAs especially have begun to become outdated. The method which Yang and Verbauwhede utilized to deal with them is still relevant, however. As many others did, Yang and Verbauwhede utilized a hashing method in addition to the SABL to further reduce the effectiveness of DPAs. However, hashing is very risky in biometrics, because some biometric data fingerprints can change based on oil present or other cosmetic changes, hashing the entire fingerprint does not work. To combat this, Yang and Verbauwhede proposed a hashing algorithm which hashes the fingerprint's minutiae, instead of the fingerprints themselves. As a result, the hash can recognize the minutiae of each fingerprint even after the fingerprint itself has changed.

Each minutia M's details are available as a result of gathering information on the M's surroundings with the following equation ,which holds for each neighboring minutia $n \in \{1, 2, \ldots, N\}$:

$$\begin{cases} d_n = \sqrt{(x_n - x_o)^2 + (y_n - y_0)^2} \\ \phi_n = \text{diff}(\psi_n, \psi) \\ \theta_n = \text{diff}(\arctan((y_n - y_0)/(x_n - x_0)), \psi), \end{cases} \quad (1)$$

where d_n describes the distance between minutia M and its n^{th} neighbor, ψ_n is the related radial angle between M and its n^{th} nearest neighbor, and θ_n is the related position angle of the n^{th} nearest neighbor. A position angle is the angular offset of the neighbor n and minutia M if a line were to be drawn from the viewpoint [11]. The function diff() calculates the difference between two angles, and then converts the result to the range $[0, 2\pi]$. X and y describe the position of the minutia on a standard coordinate scale.

The algorithm which Yang and Verbauwhede proposed first compares the direction of the ridges the minutiae are

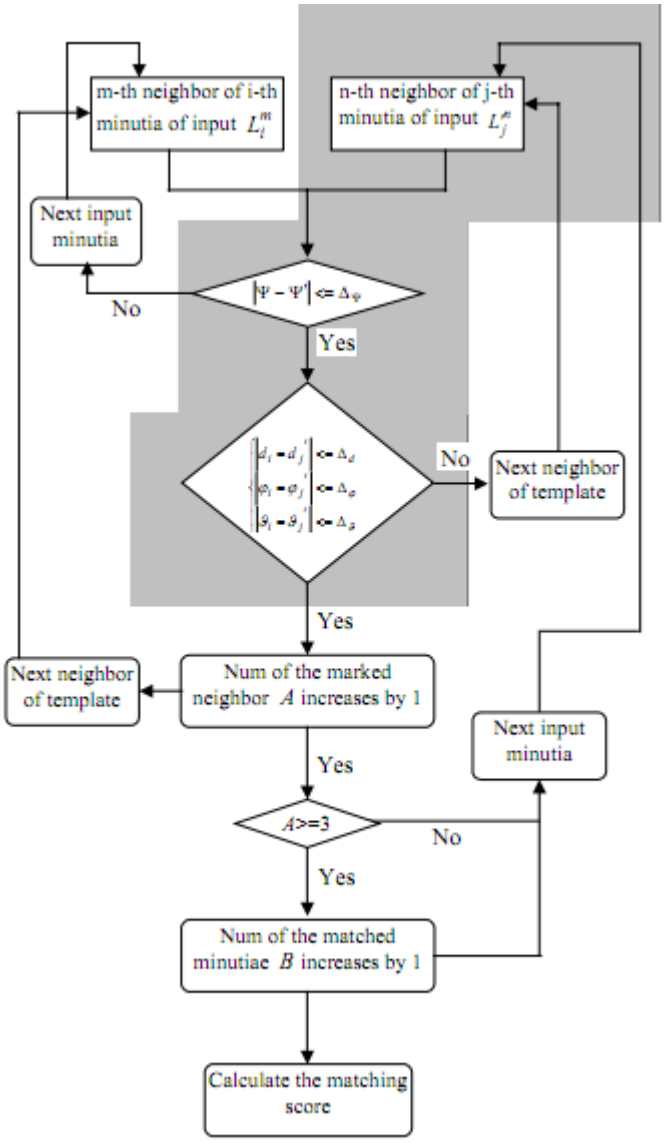

Figure 2: Flowchart of Yang and Verbauwhede's matching system.

based on according to the following equation:

$$|\psi - \psi'| > \Delta_\psi, \tag{2}$$

where ψ has the same meaning as it does in Equation 1, and Δ_ψ is the threshold for the direction of the ridge the minutia is based on. If the result is lower than the threshold, the pair is rejected.

The algorithm then compares the neighborhood of the minutiae in the input fingerprint to the neighborhood of the same minutiae in the corresponding fingerprint in the template. If the minutiae are similar enough, as determined by Equation 3, they are taken as a matched minutiae pair.

$$\begin{cases} |d_i - d_j'| <= \Delta_d \\ |\phi_i - \phi_j'| <= \Delta_\phi \\ |\theta_i - \theta_j'| <= \Delta_\theta, \end{cases} \tag{3}$$

where Δ_d is the threshold for distance, Δ_ϕ is the threshold for the radial angle, and Δ_θ is the threshold for the position angle.

The total number of matched pairs a fingerprint has after repeating this process on every minutia is used to calculate the fingerprint's score as follows:

$$Score = B/(max(K_{input}, K_{temp}), \tag{4}$$

where K_{input} is the number of minutiae in the input fingerprint, and K_{temp} is the number of minutiae in the template fingerprint. Two fingerprints are verified as being from the same finger if their score is higher than a pre-set threshold.

4.3 Multimodal Systems

A multimodal biometric identification system is a system which uses multiple forms of biometric identification in order to provide additional security. Increasing the number of identifiers used makes it more difficult for an attacker to gain access. Not only would the attacker need to acquire additional information for a physical attack, but the systems can combine the different identifiers in clever ways to make the data more complex, thus harder to imitate.

4.3.1 Using Palm and Knuckleprints

Sun et al. proposed a system which uses both palmprints and knuckleprints [7]. Sun et al. suggest using the palmprint as the main identifier, but also discretely taking a knuckleprint scan, which would be used not only as another identifier, but it would also be used to provide a watermark for the palmprint. A watermark is data hidden in an image in order to ensure legitimacy. A common example is the red and blue threads in American currency.

The system begins by scanning the knuckleprint, and using that scan to extract feature data. This feature data is then used to create a watermark, which is embedded into the palmprint image. During the authentication phase, the watermark is extracted from the palmprint, providing the original knuckleprint feature data. This data, in addition to the palmprint, is scanned against the database to validate whether the person is an authorized user. This process is displayed in Figure 3.

In addition to the watermark, the knuckleprint provides a layer of physical security. The knuckleprint scanner is built into the palmprint scanner, so an unauthorized user may not notice that they need to provide both the knuckleprint and

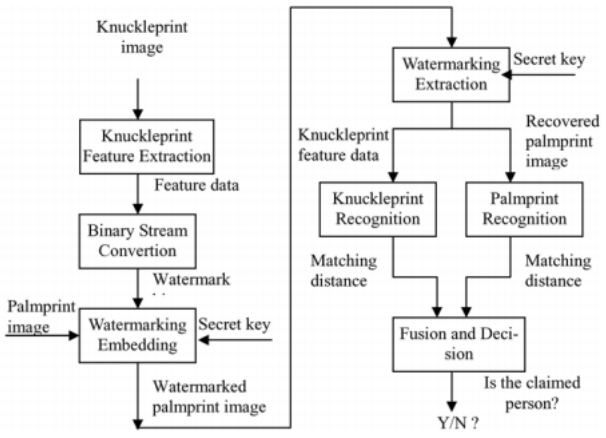

Figure 3: The flow of Sun et al.'s verification scheme

the palmprint. This practice is often referred to as security through obscurity and is usually discouraged, since a security system should not rely on an attacker not knowing its details, only on his inability to forge a required identification. However, the benefits provided by watermarking still makes the second identifier useful, since forging two identifiers is more difficult than forging one.

4.3.2 Multimodal Systems and Integrity Verification

Won-gyum Kim of the Copyright Protection Center in South Korea and HeungKyu Lee of Korea University Department of Visual Information Processing proposed an integrity verification scheme, a system which makes sure the input has not been tampered with, which uses a robust watermarking system [3].

Watermarking

Kim and Lee's solution starts by taking both a fingerprint and a facial scan. The fingerprint is then watermarked as follows:

$$TN(k,l) = SS(l_{SP}(i+m, j+n))), \quad (5)$$

where $TN(k,l)$ denotes a thumbnail image (of a facial image) with size $M \times N$ pixels; k = 0,1,...,M; l = 0,1,...,N (both M and N were set to 10); $l_p(i,j)$ is the face image of size $I \times J$, and is divided into sub-regions $l_{sp}(m,n), m = 0,1,...I/M-1, n = 0,1,...,J/N-1$ which do not overlap. Finally, $I_{SP}((i+m, j+n)$ denotes a luminance value of a subregion where i and j describe the location in the original face image. SS() is a function which chooses the first pixel in the area of the fingerprint which receives the watermark.

This watermark is then embedded into the fingerprint image through means of a two-dimensional pseudorandom sequence array with 256 different sequences of length 256.

Integrity Verification

The first portion of the integrity verification phase begins by extracting the thumbnail feature vectors from the estimated watermark signal. To do this, a two-dimensional random sequence created using the original watermark is used to describe the pixel values of a specific location in the thumbnail feature vectors of the face image. This array is then converted into a one-dimensional form. Because the extracted watermark might not be identical to the original

Figure 4: Biometric image watermarking: (a) face image, (b) fingerprint image, (c) thumbnail image (resized for display), and (d) watermarked fingerprint image.

watermark, the similarity between the extracted watermark and random sequences is computed using cross-correlation. Cross-correlation is a method used to calculate the difference between two functions which differ only by a shift on the x-axis, y-axis, or both [10]. By using this similarity, it is possible to find the forged region in an attack.

The second portion of the integrity verification phase regards verifying the integrity of the face image. By using the thumbnail feature vectors, the integrity of the face image is verified by comparing it with the thumbnail feature vectors from the fingerprint image. If the thumbnail feature vector is different, then the face image region representing the thumbnail feature vector is forged, thus, it is an unauthorized attempt. If the thumbnail feature vectors are the same, then the attempt is verified as a secure attempt.

5. CONCLUSION

In this paper, we provided a brief overview on biometric identification including its uses in the modern world as well as several security issues present. We then identified methods of dealing with these issues: hashing the minutiae instead of the fingerprints enables hashing to be effective when dealing with fingerprints, and using additional biometric identifiers in the same system increases security by increasing the information needed in a physical attack and allows one to increase security by using watermarks.

Acknowledgments

The author thanks Elena Machkasova, Rob Jansen, Peter Dolan, James Delehanty, and Ryan Klawitter for their help in writing this paper.

6. REFERENCES

[1] Clancy, T. C., Kiyavash, N., and Lin, D. J. Secure smartcardbased fingerprint authentication. In

Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications (New York, NY, USA, 2003), WBMA '03, ACM, pp. 45–52.

[2] Jain, A. K., Nandakumar, K., and Nagar, A. Biometric template security. *EURASIP J. Adv. Signal Process 2008* (January 2008), 113:1–113:17.

[3] Kim, W., and Lee, H. Multimodal biometric image watermarking using two-stage integrity verification. *Signal Processing 89*, 2 (2009), 2385 – 2399.

[4] Liu, L., Yang, J., Chaozhe, Z., and Jiang, T. Information theory based fingerprint matching. *IEEE Transactions on Pattern Analysis and Machine Intelligence* (2011, to appear).

[5] Saenz, A. India launches universal id system with biometrics. `http://singularityhub.com/2010/09/13/india-launches-universal-id-system-with-biometrics/`, September 2010.

[6] Schneier, B. Inside risks: the uses and abuses of biometrics. *Commun. ACM 42* (August 1999), 136–.

[7] Sun, D., Li, Q., Liu, T., He, B., and Qiu, Z. A secure multimodal biometric verification scheme. In *Advances in Biometric Person Authentication*, S. Z. Li, Z. Sun, T. Tan, S. Pankanti, G. Chollet, and D. Zhang, Eds., vol. 3781 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2005, pp. 233–240.

[8] Wikipedia. Minutiae — wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Minutiae&oldid=359363333`, 2010.

[9] Wikipedia. Biometrics — wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Biometrics&oldid=419298116`, 2011.

[10] Wikipedia. Cross-correlation — wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Cross-correlation&oldid=423926531`, 2011.

[11] Wikipedia. Position angle — wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Position_angle&oldid=421760573`, 2011.

[12] Yang, S., and Verbauwhede, I. M. A secure fingerprint matching technique. In *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications* (New York, NY, USA, 2003), WBMA '03, ACM, pp. 89–94.