Did I Do That?

A Current Analysis of Biometric Technologies

by Jalaynea A. Cooper

Introduction

Have you ever wondered about a bank transaction that you don't remember doing or losing your bank credit card and hoping that no one will use it? There are several security authentication options that can be taken in order to assure that no one else claims to be you. One in particular is Biometrics.

What is Biometrics? Biometrics are automated methods of recognizing a person based on physiological or behavioral characteristics.[2] Physiological characteristics are those that we are born with such as fingerprint, hand geometry, or iris. The way a person speaks or a person's signature is classified as behavioral characteristics. We will explore some of the man types of physiological and behavioral biometrics below.

Physiological Characteristics

Fingerprint

Figure 1

Fingerprints like the one in Figure 1 can be used by matching the minutiae or emulating a traditional police method.[3] *No two fingers are alike due to not having the same dermal ridge.*

The fingerprint biometric identification scheme is the analysis of an individual's unique fingerprints.[13] It is the oldest and most widely recognized biometric marker. [18] More biometric devices for fingerprints are available to use than any other biometric system.[3]

- How does the *fingerprint* technology work?

Fingerprints are made up of ridges and valleys on the surface of the finger. Segments on the upper skin layer are the ridges and the lower skin layers are the valleys. Minutia points are formed by ridges. The fingerprint is determined unique by the pattern of the ridges and minutiae points. A fingerprint pattern can be split into 5 categories: arch, tented arch, left loop, right loop, and whorl. In order of percentages, the loops make up most of the fingerprint with 60%, whorls make up 30%, and arches make up 10%. [1]

Minutia matching and patter matching are two methods used to recognize fingerprints: During the minutia matching method, the ridges in the fingerprint are compared by unique details. Minutia points on the individual's finger are located and processed to extract these points. They are then compared with a registered template. [1]

In comparison to the minutia matching method, the pattern matching method compares all of the finger's characteristics. Sub-areas of the ridge thickness, curves, or density are some of the finger's characteristics. The area around the minutia, with low curvature, or combination of ridges is taken from the fingerprint. The extracted area is then processed and compared with a registered template. [1]

The user places his/her finger against a reader. The reader then scans the fingerprint and it is sent into a database. Once in the database, the fingerprint is compared, verified, and identified. [8]

- **Table 1:** Advantages/Disadvantages for Fingerprint Biometrics

Advantages	**Disadvantages**
Can be placed on a smart card for an added degree of authentication	Higher risk of false rejection (a rate that authentic users are denied or prevented access to authorized areas, as a result of a failure in the biometric device)[17]
Low instances of false acceptance (a rate that fraudulent users or non –users are allowed access to systems or areas,	The degradation of the fingerprint caused by occupation,

as a result of failure in the biometric device)[17]	age or even trauma.
Low cost	
Integration is easier	
Fingerprint readers are small in size.	

- Current Uses

Fingerprint biometrics can currently be seen used with computers and flash drives

Figure 2: This fingerprint reader made by Microsoft© is small in size and can be easily connected to your computer by a USB drive.

Law enforcement use fingerprint biometrics to identify a suspect. Another current use is that of background searches by job employers. Banks have begun using fingerprint technology at the ATM. Some grocery stores are even evaluating how using fingerprint technology to speed up the checkout process will work.

Hand Geometry

The hand geometry biometric identification scheme is the analysis of the edge of the hand and the length of the fingers. [13] "This is the second most widely used biometric marker." [18] Hand geometry is scanned by a three-dimensional perspective.

- How does the *hand geometry* technology work?

The geometry of the hand is analyzed overall by the shape, length, thickness, width, fingers, or joints. The skin surface can also be used to analyze. As many as 90 parameters can be measured.

An individual uses the hand biometric device by placing his/her hand on it. The device is provided with pegs where the person's hand is supposed to be laid. Once the hand is in place, the hand geometry device checks it against the database for verification that the user is who he/she says they are.

In order to prevent false acceptance, some hand geometry devices require the person to wiggle his/her fingers. Other precautions can be provided through hand thermography, (heat of the hand), or skin conductivity. [1]

- **Table 2:** Advantages/Disadvantages for Hand Geometry Biometrics

Advantages	**Disadvantages**
Easy to use	Injury or trauma degradation can make the print hard to read.
Easy to integrate	The hand itself is not unique. It is the parameters that make it unique.
Does not significantly change after ageing	Does not work well for people with arthritis
Used to improve security, accuracy, and convenience for access control, time, and attendance. [18]	Accuracy is low
Can work with dirty hands	Fairly expensive

- Current Uses

Hand geometry is currently used to access restricted areas of a company or any building in general. Airports use hand geometry biometrics is verify the correct passenger. Immigration facilities use hand geometry for the INSPASS system that is used for frequent international travelers.[11]

Vein

The analysis of the pattern of veins in the back of the hand and the wrist makes up the scheme of this particular biometric identification. [13] Each person has a unique set of blood veins in his/her hand. Veins are very complicated therefore contain lots of different features that help to identify a person.

Figure 3: Vein Biometrics

How does the *vein* technology work?

This certain biometrics scheme works by a person's vein image getting scanned with near-infrared rays. The light that is given after diffusion is then captured. The vein vessels appear to be black when the infrared ray is absorbed by the deoxidized hemoglobin in the veins. [1] Once the vein pattern is captured; it is verified against a pattern that was already registered. When the person has been verified, the individual is authenticated.

- **Table 3**: Advantages/Disadvantages for Vein Biometrics

Advantages	**Disadvantages**
Veins do not change during a person's life.	Fairly new- so the effect by a person's heart attack or medical problems is not clear
Highly secure due to being hard to copy or even read.	

It maybe a question as to can this system be effective even when a person is deceased. Vein biometrics can only be used if the person is living. The device that is used for vein biometrics can only recognize a pattern if the deoxidized hemoglobin is actually flowing in the veins. [1]

- Current Uses

Security systems, log-in control, healthcare, and banking and financial services currently use the vein biometric system. An example is in the Bank of Tokyo-Mitsubishi in Japan, the palm vein biometrics system is already being used. [1] Vein biometrics are also used in the testing of major military installations.[16]

Iris

This certain biometric identification scheme uses the analysis of the colored ring that is around the eye's pupil.[13] More than 200 points can be used for comparison.

- How does the *iris* technology work?

This technology can be used up to 2 feet away. The user places him or herself so that the person can see his/her eye reflection in the iris biometric device. Afterwards, the user has to look into the device for a few minutes in order to capture the features of the iris. [14] The unique code provided by the iris relies on very high-quality images provided by the software and the user. [10]

Some iris biometric devices provide measures that assist with preventing false acceptance. These devices may be capable of shining a light and looking for dilation of the eye.

- **Table 4:** Advantages/Disadvantages for Iris Biometrics

Advantages	**Disadvantages**
Does not require intimate contact with the reader	Not easy to use
Higher average for matching performance	Not easy to integrate with other systems
Convenient for people who wear glasses	The position of the eye can be problematic
Chances of a false positive are very low	Require specialized devices, so can be expensive
Almost unaffected by environment sue to being protected by the cornea and the aqueous humor. [10]	
Left and right iris patterns a certain person are different, including those of identical twins. [10]	

- Current Uses

US law enforcement has recently begun using the iris biometric technology in 1994 when the Lancaster County Prison in Pennsylvania first began using it. This technology is used to identify prisoners and to do security checks. Another specific current use is at the Charlotte Douglas International Airport in North Carolina. [14]

Figure 4: A person's eye can be used for Iris or Retina Biometrics

Retina

The capillary vessels that are located in the back of the eye are analyzed for the retina biometric identification scheme.

- How does the *retina* technology work?

In order for the retina biometric technology to work, the user has to place his/her eye very close to the scanner. During the scan, the individual has to stare and focus at a certain point while remaining still until the scan is complete. The time for a retina scan usually lasts about 10-15 seconds. A light is projected into the eye retina and a photograph is then taken of the blood vessels and analyzed. [1]

- **Table 5**: Advantages/Disadvantages for Retina Biometrics

Advantages	**Disadvantages**
Accurate	Not very convenient for people who wear glasses
Impossible to forge a human retina	Uncomfortable for users
Lower error rate of 1 in 10,000,000 compared to fingerprint identification (1 in 500) [1]	Fairly new, so not many are using retina biometric devices
Low false acceptance rate and low false rejection rate	

- Current Uses

Retina biometric technology is usually used in high-security areas to control access. These areas can include power plants and military buildings.[7]

Face

Figure 5: Face Biometrics are easy to use

The face biometric identification scheme consists of the analysis of facial characteristics.[13] It uses geometrical characteristics of the face.

- How does the *face* technology work?

  Face biometrics analyze the overall structure of a person's face. Features such as the distance between the eyes, nose, mouth, eye sockets, location of the nose and eyes, and cheekbones are analyzed. To begin the enrollment process for face biometrics, several pictures are taken featuring different angles and facial expressions. In order for the individual to be verified and identified, he/she has to stand in front of a camera. The camera then scans the person's face and compares with a previously recorded template.[1]

  Certain face biometrics also provide false acceptance prevention by using facial thermography, (heat of the face), or making the user perform a facial expression,(smile, nod, blink).

- **Table 6**: Advantages/Disadvantages for Face Biometrics

Advantages	**Disadvantages**
Can be placed on a smart card for an added degree of authentication	A person's face can be scanned without his/her knowledge
More suited for authentication	If the background contrasts, an error can be caused.
Highly desirable	Less suited for identification due to a person being able to change his/her face by wearing a mask or any attachment.

	Factors such as make-up, hairdressing, and artifacts can cause degradation. [10]

- Current Uses

Law enforcement agencies currently use facial biometrics. It is also used in banks by bank tellers in the form of verification.[7] Humans use face biometrics as a way to identify and authenticate other humans.

Voice

Figure 6: Voice biometrics can be classified as either physiological or behavioral

Voice biometric identification schemes are used to analyze the tone or pitch of a person's voice. Cadence and frequency of a person's voice is also analyzed. [13] Voice biometrics can also be classified as behavioral, (accent). The physiological part is the voice tract.

- How does the *voice* technology work?

Voice biometrics can be split into two categories: speech recognition and voice recognition. Speech recognition interprets what a person is saying. Voice recognition looks at the quality of the person's voice that is unique to them.

To begin the enrollment process, the user has to repeat a phrase or a few numbers into a microphone, telephone, and/or PC microphone. Once the phrase or set of numbers is captured by any of the audio devices, it is then analyzed. By the user repeating phrases, unauthorized access can be prevented.

- **Table 7:** Advantages/Disadvantages for Voice Biometrics

Advantages	**Disadvantages**
Vocal tract is not affected by a cold.	Local acoustics can throw off the biometric system
Can be used with telephones	Illness and age can be some of the factors that effect voice biometrics.
Low invasiveness	High false non-matching rates

- Current Uses

A wall mounted reader is currently a use of voice biometrics. They are also used to authenticate e-commerce transaction.

Dental

Dental biometric schemes analyze dental radiographs for human identification.[5]

- How does the *dental* technology work?

Postmortem radiographs, (PM), are those radiographs that are acquired after a person's death. Antemortem radiographs, (AM), are acquired while a person is alive. Dental biometrics can be broken into two categories: feature extraction and matching.

Images are enhanced and dental work is segmented in the feature extraction stage. The matching stage can be further broken into three steps: tooth-level matching, computation of image distances, and subject identification. [5]

- Tooth-level matching – Using a shape registration method, the tooth contours are matched. Dental work is also matched on overlapping areas in this stage.
- Computations of image distances – Distance between the two radiographs is measured based on the corresponding teeth.
- Subject identification – All of the distances between the given PM and the AM are combined to establish the identity of the person.

The database containing both AM and PM radiographs are used to analyze one of the radiographs against the other.

- **Table 8**: Advantages/Disadvantages for Dental Biometrics

Advantages	**Disadvantages**
Radiographs can be used on living and non-living people	Not an automated method
	Variation of dental structure between AM and PM

- Current Uses

Dental biometrics are used to identify people through dental records.

DNA

Figure 7: DNA strand

Each person has 23 pairs of chromosomes that contain their DNA blueprint. Each pair has one member from the individual's mother and one from the father. [1]

- How does the *DNA* technology work?

In some cases DNA is not quite considered a biometric technology. There are different ways of gaining a person's DNA. Some are by gaining a strand of hair, a mouth swab, or blood work. Five percent of a person's DNA is made up of the coding portion, (genes).[12] The genes are analyzed to help identify a person.

DNA is currently being evaluated more in order to make the biometric process of gaining and analyzing DNA much easier and faster.

- **Table 9**: Advantages/Disadvantages for Dental Biometrics

Advantages	**Disadvantages**
The genome is unique to each person.	Not fast and automated
Accurate	Matching not done in real-time
	Intrusive

- Current Uses

  The DNA technology is used to compare DNA between suspects 1 and suspect 2 against DNA found at a crime scene, in law enforcement and court. DNA is also used in paternity testing, and identification of a missing person.

Behavioral Characteristics

Signature

Signature biometric identification schemes analyze the way a person signs his or her name. [2]

- How does the *signature* technology work?

  Signature biometrics work by analyzing the stroke order, the pressure applied and the speed. The signature image is also analyzed. [1] A scanner is used to record the way a person writes on tablet, and even with a sensored pen. Another way of capturing a signature biometric is by using ultrasonic sensing. Once the signature is captured, it is verified against the database.

- **Table 10:** Advantages/Disadvantages for Signature Biometrics

Advantages	**Disadvantages**
Reasonably accurate	Systems can be fooled by imitation signatures
Easy to user	

- Current Uses

Online signature verification is currently used by IBM to verify an accurate signature from a false one. Camera verification is another current use of signature biometrics. People use signature biometrics everyday when he/she signs their name to make a purchase. Contract execution, access to controlled documents, and acknowledgement of services are some of the more popular and current uses of signature biometrics.

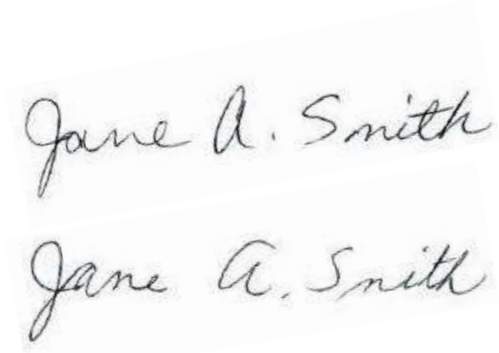

***Figure 8*: Signature Biometrics are analyzed to assist with the identification of a person. As displayed above, two people can try to copy the same signature, but there is always something different to determine that it is not the same person.**

Keystroke

This particular biometric identification analyses the way a person types.

- How does the *keystroke* technology work?

While the user is typing a phrase with the keyboard, the biometric system records the timing of the typing. This usually has to be done a number of times in order to verify that the keystrokes are distinctive.[4] It is compared against the database to verify and identify the user.

- **Table 11:** Advantages/Disadvantages for Keystroke Biometrics

Advantages	**Disadvantages**
User friendly	A person may hack in and get the users password.
Fairly unique between people	Less suitable for identification
More suitable for verification	
Low cost	

- Current Uses

Keystroke biometrics can be used to control access to company documents. This technology is used widely as a security measure for password, pass-phrases, and IDs.

Gait

Gait is the biometric identification scheme that analyses the way a person walks.

- How does the *gait* technology work?

Gait technology works by analyzing the way a person walks and that individual's surroundings.[9] Photographs and camera can be used to capture images of the person walking. The images then are compared and verified against a database.

- **Table 12:** Advantages/Disadvantages for Gait Biometrics

Advantages	**Disadvantages**
Can be obtained from a distance	Can be obtained from a distance – invasion of privacy
Can be used to determine medical illnesses	

- Current Uses

This technology is currently used in hospitals to determine medical issues. Athletes use gait technology to optimize and improve their performance. [9]

Identification vs Verification

There are two categories of Biometric Systems. They are identification and verification. Identification is known as the process that compares a present person to a biometric pattern or database. Verification is a process that validates a person's ID by comparing his/her biometric data with already captured biometric data that is stored in a system. Identification is more complex than the verification process. Identification may generate a *one to many matches*, where verification generates a *one to one match*. [3]

An example is a person using biometrics at an airport. During the verification process the passenger would provide a smart card, (already programmed with his/her biometric data). When it is time for the passenger to be scanned, authorization would be verified against both the person and the smart card. This process is extremely straightforward and more easy to use.

The identification process is more complicated. Let's take this same passenger, but this time he/she does not have a smart card. Upon being scanned by the biometric system, the identification process can generate a large number of results based on similar aspects. The results of the database can then be filtered down based on sex, ethnic origin, and other facts.[3.]

How does Biometrics work?

No matter what type of biometric scheme is used, all have to go through the same process. The steps of the process are capture, process, and comparison.

- Capture – A biometric scheme is used to capture a behavioral or physiological feature.
- Process – The captured feature is then processed to extract the unique element(s) that corresponds to that certain person
- Comparison – The individual is then enrolled into a system as an authorized user. During this step of the process, the image captured is checked against existing unique elements. This verifies that the element is a newly authorized user. Once everything is done, the element can be used for future comparisons.

How do I choose the right biometric system? [6]

Certain questions need to be asked and answered when choosing a biometric system. Below are some of these questions:

1. What level of security is needed?
2. Will the system be attended or unattended?
3. Do you want the system to be resistant to spoofing?
4. What reliability level is wanted?
5. Should this system work 24 hours a day?
6. Does the system require backups?
7. What is the acceptable time for enrollment?
8. Is privacy an issue for your system?
9. What about the storage of the signature?

10. Cost? Reliability? Security?

Table 13: Myths about Biometrics [15]

(From "*Myths of biometrics")*

Biometrics is absolute security	Absolute security does not exist, nearly any security system can be compromised. Biometrics is not 100% secure. It would say that you are able to give exactly the same image and same pixels at each presentation (think of facial recognition) which is impossible in the real world, so a threshold is mandatory. It is possible to authenticate with an accuracy of 99.999%, but never 100%. Even DNA does not allow 100%, because of the technology (not all bases are sequenced), but also because of twins...
Biometric systems are able to detect diseases	It is generally just impossible to detect diseases with a biometric systems, but it is also true that in some cases, the sensors are reading some information that may be seen as related to a disease, but one must decide to use this information, and how. □ Fingerprint: there is no information related to diseases in fingerprints □ Retina: it is likely that some retina diseases are visible on the retina image, but well, you need to be a specialist to diagnose such thing.

	□ Gait: sure, if you are disabled, it is likely that gait recognition will recognize this fact..
Stolen body parts can be reused	This is an extension of spoof detection. If a fake is difficult to make, it seems simpler to directly use the original biometric trait, success rate should be higher. This is the case most of the time, and biometric systems must add what is called aliveness detection.
Twins have identical biometric traits (identical fingerprints, irises…)	This is not true, excepted for DNA. Almost all biometric types are different to a certain degree and most of the time, biometric systems are able to make the difference, and much more better than human. In some cases, there is the same difference between twins as two unrelated individuals! □ Fingerprints: fine details are different as different as two unrelated individuals. □ Iris: genetically identical eyes have uncorrelated Iriscode □ Face recognition: Delean Vision has demonstrated that their face recognition technology is able to recognize twins. □ Retinal scan: not two retina are identical, even twins. This will be the same for a clone: fingerprints are not a genetic trait written in DNA.
Making a fake finger is easy	It is true that we can make fake finger using "gummy bears", But using gummy bear to make a fake is only a very small part of

	the process, which requires several skills, and being a very smart guy. The most difficult thing is to get the fingerprint image, and the good one! Making a fake with cooperation helps a lot, as the owner just need to apply his/her finger in a soft material which becomes the negative when becoming hard. Once you get the latent fingerprint image, you will need to process it, as the latent prints are not good enough to make a mold, generally using the printed board technique. .
Iris recognition is extremely accurate and much better than fingerprints.	At the moment, there are no equivalent tests for the iris -but this will happen in the future.
It is possible to know the gender from the fingerprint	NO. There is no correlation between the fingerprints and the gender. And this is already very clever to say that there are only two individuals on a crime scene, as you need to make the link between the fingers, which is not so easy...

Conclusion

Biometrics are used for identification purposes. They are usually classified as physiological or behavioral. Sometimes a certain biometric can be classified as both. As we continue to progress into the future, more and more biometric schemes will become available. Also, more of the existing biometric schemes will advance further for a higher level of security.

Identification and verification classify biometrics even further. The identification process matches 1:N and the verification process is 1:1. All biometrics have to go through a process which is capture, process, and comparison.

As the need for security increases, so will the need for biometrics! It will definitely be interesting to see what the future holds for BIOMETRICS.

Resources

1. (n.d.). Retrieved July 12, 2007, from BIOMETRIC NEWSPORTAL.COM: www.biometricnewsportal.com

2. Biometrics. (n.d.). Retrieved from Webopedia: http://www.webopedia.com/TERM/B/biometrics.html

3. Biometrics. (n.d.). Retrieved July 3, 2007, from Biometrics: http://ewh.ieee.org/r10/bombay/news5/Biometrics.htm

4. Biometrics. (n.d.). Retrieved July 14, 2007, from Keystroke Dynamics: http://perso.orange.fr/fingerchip/biometrics/types/keystroke.htm

*5. Chen, H., & Jain, A. K. (August 2005). Dental Biometrics: Alignment and Matching of Dental Radiographs. *IEEE Transactions on Pattern Analysis and Machine Intelligence* , 1319-1326.

6. Choosing a biometric system. (n.d.). Retrieved July 8, 2007, from Biometrics: http://perso.orange.fr/fingerchip/biometrics/issues.htm

7. Facial Recognition. (n.d.). Retrieved June 28, 2007, from Individual Biometrics: http://ctl.ncsc.dni.us/biomet%20web/BMFacial.html

8. Fingerprint. (n.d.). Retrieved June 28, 2007, from Individual Biometrics: http://ctl.ncsc.dni.us/biomet%20web/BMFingerprint.html

9. Gait analysis. (n.d.). Retrieved July 14, 2007, from Wikipedia: http//:en.wikipedia.org/wiki/Gait_analysis

10. Garcia, J. O., Bigun, J., Reynolds, D., & Gonzalez-Rodriguez, J. (March 2004). Authentication Gets Personal with Biometrics. *Increasing security in DRM systems through biometric authentication.* , 50-62.

**11. Hand Geometry*. (n.d.). Retrieved June 28, 2007, from Individual Biometrics: http://ctl.ncsc.dni.us/biomet%20web/BMHand.html

12. How DNA Evidence Works. (n.d.). Retrieved July 14, 2007, from how stuffworks: http://science.howstuffworks.com/dna-evidence1.htm

13. Introduction to Biometrics. (n.d.). Retrieved from The Biometric Consortium: http://www.biometrics.org/intro.htm

**14. Iris Scan*. (n.d.). Retrieved June 28, 2007, from Individual Biometrics: http://ctl.ncsc.dni.us/biomet%20web/BMIris.html

15. Myths of biometrics. (n.d.). Retrieved July 8, 2007, from Biometrics: http://perso.orange.fr/fingerchip/biometrics/myths.htm

16. Vascular Patterns. (n.d.). Retrieved June 28, 2007, from Individual Biometrics: http://ctl.ncsc.dni.us/biomet%20web/BMVascular.html

17. (2004). In M. E. Whitman, & H. J. Mattord, *Management of Information Security* (p. 372). Boston, MA: Thompson Course Technology.

18. Woodard, J. D., Orlans, N. M., & Higgins, P. T. (2003). *Biometrics (electronic book)*. New York: McGraw-Hill/Osborne.