Cassie Migani
Programming Fundamentals
So Teach Me Something Part 5
December 7, 2005

Is Biometrics "Big Brother" Watching You?

Eye Catcher

"But be careful what you touch, because you are leaving your identity behind every time you take a drink" ~ Paul Saffro, 2005, in an article discussing the implications of the use of DNA in a biometric system.

"The public needs to learn that biometrics could be one of the most effective, and in the long run, more profitable means for protecting individual privacy." ~Anil Jain, 2000, in an article explaining a biometric system and the uses it has in society.

Summary

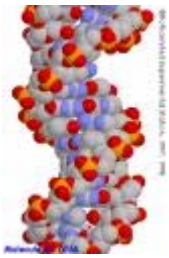
Biometrics is a method of identifying a person by biological traits. The most common forms of biometric identifiers include fingerprints, retinas, iris, voice patterns, facial patterns, and hand measurements (Orr, 2005). These traits are unique to each individual, and do not change over time, making them ideal for use in identification. The goal for biometrics is to be able to correctly identify a person in a manner so that it is accurate and foolproof. This system could be used to verify age for certain purchases or could be taken to more extremes, such as identifying people every time they go out in public, like in the 2002 movie *Minority Report*.

Biometrics is a hot topic in today's society for several reasons. Among these reasons is the fact that Americans are very protective of their privacy and many feel that the use of this technology could result in their lives being closely monitored. The main argument against the

use of biometrics is that information will be stored on a computer system that would make it accessible to users, but potentially open it up to more unauthorized people that could lead to identity theft. If this system becomes as widespread as hoped, this would also allow a given person's whereabouts and daily habits to be looked up at a moments notice, compromising their privacy. A good example of potential public fear comes from the 2002 move *Minority Report*. In this fictional movie, all citizens had to get a retinal scan every time they went out in public, even if it was just entering a store. This allowed the government to track anyone at given time, reminiscent of George Orwell's fictional novel, *1984*. The arguments in favor of biometrics include that it is very accurate, it is an easy way to store medical alerts and other important information, and allows data to be recalled as needed. Many companies in the industry of manufacturing biometric scanners claim that "a false acceptance rate (FAR) and false rejection rate (FRR) is 0.01% or less" (Alterman, 2003) which means that less than one out of 10,000 people would match with someone else's fingerprint, or not match with their own. A biometric system could replace ID cards and could assist in identifying underage people trying to buy alcohol or cigarettes. Biometrics is also being considered for use in speeding up "law-abiding travelers through checkpoints and to search for domestic terrorists" (Lipton, 2005). This idea was initialized after the September 11th terrorist attacks and is already being used in some airports.

One of the major deterrents from using a biometric system is also one of the main advantages. Once you have this identifying system in place, it is all you need. In the traditional

identification systems, such as knowledge based identification or token-based identification, you are given an item or a piece of knowledge to access a system. If something happens and you forget your PIN number, you can just get a new number issued. However, with biometrics, if someone gets hold of



your identity, nothing can be done. You cannot get new DNA (Jain, 2000). Combining that with the idea that DNA in "its architecture is designed for duplication" (Saffo, 2005), if a person steals your DNA, they can do whatever they want with your personal information. Another problem is that if a programmer for any reason makes an error, or another act of terrorism occurs, "a technical error could cause the release of decrypted ID's and the personal data associated with them on a corporate internet or extranet" (Alterman, 2003) allowing anyone to see your personal information. This could happen by honest mistake, or an outsider could gain access and change something within the system in hopes to destroy the United States. If your personal information is leaked abroad in addition to within the United States, the possibility of negative things happening seems infinite.

Biometrics is already being used in some areas of the United States. The government is trying out a program called Registered Traveler to do background checks and speed up wait time in some airports (Frank, 2005). This system uses images of traveler's fingerprints and irises "on a highly secure, government-approved biometric card" (Frank, 2005). In Albertson's supermarket near Portland, Oregon, customers can pay using their fingerprints in a manner similar to that of a debit card (Walker, 2005). This technology is called Pay By Touch, and while convenience is the driving force behind people using such a system, many people are hesitant because they are not sure what is happening to their information (Walker, 2005). In 2003, *Information Week* reported that soon in some locations, MacDonald's customers also would be able to pay using a credit card linked to their fingerprint (Alterman, 2003). Even family-orientated places such as Disney World are using finger scans linked to their season passes (Alterman, 2003).

Educational Importance

Biometrics is becoming more relevant as technology becomes more advanced. The items that were part of science fiction movies of the past are becoming closer to reality. If people are uneducated about what biometrics is and how their information will be used, people may not be fully aware of the ramifications of their decisions when it is their turn to enter the system.

There are many different ways that a biometric scanner could be utilized in the United States. The eventual hope would be to tie money and credit to a scan as already used in some Albertson's grocery stores in Oregon (Walker, 2005). If this system is to be used in such a widespread manner as promoters hope, then everyone will need to know exactly what they are committing to by entering into such a program. The importance for the American public to be 100% aware of what they are doing is so imperative in this technologically advancing era, that an uninformed decision should never be made, especially concerning something as important as their identity.

If the public is unaware of exactly what is going to be done with the system, than they could sign away their privacy without fully understanding the consequences. A biometric system is coming closer to being implemented in the United States as technology improves. If people think that the system will do one thing and then find out that the system will be used to do more than what they expected, their privacy could have been given away because of making uninformed decisions. Keeping informed about technology in an ever-changing society may seem daunting, but it is an important aspect in a society where technology plays such a large role.

My Opinion

My own feelings about using a biometric system are mixed. I feel that the idea for a national identification system in the United States would be beneficial, especially after the

September 11th attacks. An identification system such as this could help in preventing any future acts of terror simply by putting a red flag on any people that are deemed suspicious. However, I would feel very skeptical being included in this system if I knew that there was a way for someone to hack into a mainframe and steal my identity. If the government issued a statement saying that this system to be utilized and it worked only 95% of the time, I would not feel safe trusting my identity and defining characteristics to something that does not work perfectly. As mentioned, you can reissue a credit card, or get a new PIN number, but if someone got a hold of the information being stored in this system, I would be worried. With technology continuing to advance, the possibilities for what could be done with an individuals DNA are frightening. As soon as I heard that this was a 100% safe way to identify people, I would sign up right away, but not until then.

Other Materials

Case Studies

"Lab's Errors in '82 Killing Force Review of Virginia DNA Cases"

In 1982 Rebecca Williams was raped and fatally stabbed by Earl Washington Jr. Under most circumstances, this case would end after the conviction of Mr. Washington and his death sentence earned for this crime would be carried out. However, Mr. Washington was convicted of this particular crime without using DNA, and in 2000 was pardoned for this crime by the governor because DNA evidence had arisen that questioned the validity of Mr. Washington's guilt.

The lawyers for Mr. Washington had tried in the past to get a DNA analysis performed on the semen found at the crime scene, but there mistakes made in the DNA lab which resulted in Mr. Washington remaining on death row for an additional seven years. While Mr. Washington

has not been completely exonerated, he is expected to be in the near future. The defense for Mr. Washington has performed a separate test on the semen found at the crime scene, which points to the actual guilty party, a convicted serial rapist.

If this case had occurred during the time where an accurate DNA based identification was in place, like the biometric system, this could have prevented Mr. Washington's stay on death row. It could also expedite the court process and make the time inmates spend on death row, or even awaiting trial, much less than is currently the case.

There are other cases that are appearing where men have been put to death based on DNA evidence that has been later found to be incorrect. If innocent men are being put to death, then perhaps there should be a more tangible way of identifying people, such as a biometric scanner. If a system such as this is in place, then it could prevent people who are innocent from being incarcerated.

"For '73 Rape Victim, DNA Revives Horror, Too"

Rape can be harsh for victims who are forced to relive the events years after it happened. In 1973, a woman was raped in Manhattan, and thirty-two years later, she was forced to experience again the traumatic experience when her attacker was put on trial. Fletcher Anderson Worrell raped Kathleen Ham in New York and in 2004, when Mr. Worrell attempted to purchase a handgun in Atlanta; his background check indicated two warrants for his arrest back in New York for sexual assault. Back in New York, Ms. Ham's case was opened back up and a DNA sample was compared indicating that he had raped not only Ms. Ham, but in addition there were twenty-two other rapes in a similar pattern in the New York area, that are being attributed to Mr. Worrell, but have yet to be conclusively proven. Thanks to this DNA test, Mr. Worrell's DNA

profile was sent to the FBI databank and was matched to at least nine rape and two sexual assault cases.

Using DNA can alleviate much of the guesswork that law enforcement must rely on to catch a perpetrator. The use of a system such as biometrics would make DNA matches much simpler and faster to obtain, instead of waiting thirty-two years and forcing the victim to experience again memories that were painful and difficult to suppress. The FBI already maintains a national database of DNA for use in nationwide cases and has helped prosecute 27,806 criminals as of November 2005. If a biometric system was in place, it could help catch perpetrators sooner, and prevent the victims from having to go through painful emotions a second time.

Keywords

- **Biometrics**- the method of identifying a person by biological traits. (Allan, 2005)
- **Biometric system**- a pattern recognition system that makes a personal identification by establishing the authenticity of a specific physiological or behavioral characteristic possessed by the user (Jain, 2000)
- **DNA**- Deoxyribonucleic acid; nucleic acids, usually the molecular basis of heredity; a chain that carries the traits of heredity, in the form of a double helix. (dictionary.com)
- **Facial Thermogram**- the underlying vascular system in the human face, produced by heat passing through the facial tissue and is emitted through the skin. (Jain, 2000)
- **Identification**- the act of identifying; the state of being identified; a person's association with the qualities, characteristics, or views of another person or group.(dictionary.com)

- **Knowledge based identification**- using private knowledge to prove your identity. For example, using a PIN number. (Jain, 2000)
- **Recognition**- another term used instead of identification (Jain, 2000)
- **Retinal scan**- a technology for the identification of individuals that depends on the uniqueness of the pattern of blood vessels in the retinas of people's eyes.(Orr, 2005)
- **Thermal-swipe sensing**- measuring the temperature differences between ambient conditions and a fingerprint's valleys and ridges. (Allan, 2005)
- **Token based identification**- using something you have to make a personal identification. For example, a driver's license or ID (Jain, 2000)

Hot Quotes

- "Customers at the Edeka German supermarket chain soon will be able to pay for their shopping by placing their fingerprints on a scanner at the checkout counters", Roger Allen, *Electronic Design*, June 30, 2005 discussing the future for biometrics.

- "By 2010, fingerprint scans will no longer be the predominant biometric technology", Roseanne Gerin, *Government Computer News*, Aug. 29, 2005 discussing the potential for biometrics in the United States.

- "Unlike a credit card number, DNA can't be retired and swapped for a new sequence if it falls into the hands of crooks or snoops", Paul Saffro, *The Washington Post*, April 3, 2005 discussing problems with DNA.

- “At least 2 per cent of the population have fingerprints unsuitable for biometric scanners”, Duncan Graham-Rowe, *New Scientist,* September 17, 2005 discussing statistics for using biometrics.

- “It is expected that more and more information systems and computer-networks will be secured with biometrics with the rapid expansion of the Internet and intranet”, Anil Jain, *Communications of the ACM*, February 2000 discussing the future for biometrics.

References

Allan, Roger (2005). "Biometrics wields a double-edged sword." (Megatrends: Tomorrow's Winners Biometrics)." *Electronic Design* 53.12 (June 30, 2005): 77(3). *Expanded Academic ASAP*. Thomson Gale. Wheaton College, 15 September 2005 http://find.galegroup.com.

Alterman, Anton (2003). "'A piece of yourself': Ethical Issues in Biometric Identification." *Communications of the ACM*, Issue 5, pg 139.

Arnott, Sarah. "Biometric Flaws Mar Start of ID Card Plan." *Computing*, 18 August 2005. Lexis-Nexis, accessed 2 October 2005.

"Biometrics." Wikipedia. Wikipedia, the free encyclopedia. 6 September 2005 http://en.wikipedia.org/wiki/Biometrics

"Biometric security and business ethics." TechNovelgy.com. 6 September 2005 http://www.technology.com/ct/Technology-Article.asp?ArtNum=15

Dao, James. "Lab's Errors in '82 Killing Force Review of Virginia DNA Cases". *The New York* Times 7 May 2005. ProQuest, accessed 10 November 2005.

Frank, Thomas. "Biometric IDs could see massive growth." *USA Today*, 15 August 2005. Lexis-Nexis, accessed 2 October 2005.

Gerrin, Roseanne. "DOD plans to recognize more than just fingerprints. (Biometrics). "Government *Computer News* 24.25 (August 29, 2005):12(1). *Expanded Academic ASAP*. Thomson Gale. Wheaton College, 15 September 2005 http://find.galegroup.com.

Graham-Rowe, Duncan. "Privacy and Prejudice; whose ID is it anyway?" *New Scientist*, 17 September 2005. Lexis-Nexis, accessed 2 October 2005.

Jain, Anil, Lin Hong, and Sharath Pankanti. (2000). "Biometric Identification." *Communications of the ACM*, Volume 43, Number 2, p 90-98.

Lipton, Eric (2005). "Hurdles for Technology in U.S. Security Efforts." *The New York Times*, 10 August 2005. Lexis-Nexis, accessed 6 October 2005.

Orr, Bill (2005). "A new /old biometric method fingers users by their typing rhythms. (Tech topics: Webnotes)(BioPassword Inc.)." *ABA Banking Journal* 97.7 (July 2005): 52(1) *Expanded Academic ASAP*. Thomson Gale. Wheaton College, 15 September 2005 http://find.galegroup.com.

Preston, Julia. "For '73 Rape Victim, DNA Revives Horror, Too" *The New York Times*, 3 November 2005. http://www.nytimes.com/2005/11/03/nyregion/03rape.html.

Saffo, Paul. “A Trail of DNA and Data.” *The Washington Post* 3 April 2005. Lexis-Nexis, accessed 2 October 2005.

Schineier, Bruce. (1999). “The Uses and Abuses of Biometrics.” *Communications of the ACM*, Volume 42, Number 8, p136.

Travis, Alan. “Identity cards: memory chips, fingerprints, iris scans… but will it work?” *The Guardian*, 26 May 2005. Lexis-Nexis accessed 6 October 2005.

Walker, Andrea K. “Making purchases at your fingers ends; Biometrics can eliminate wallet, credit card, checkbook and cash.” *The Baltimore Sun*, 24 July 2005. Lexis-Nexis, accessed 2 October 2005.