Biometrics: Trading Privacy for Security

Chris Werner

April 23, 2006

Biometric identification has been around for many years, but due to the recent need of tightened security, and the price drop in the technology, biometric installations are rapidly becoming more common. Biometrics can offer excellent security solutions, but along with new technologies that can change our way of life, there is always a debate. And this one is a debate over privacy. This paper will discuss biometric technology, the social controversy, and privacy implications of implementing this technology.

The term biometrics comes from ancient Greek; bios meaning life, and metrikos or metron meaning measure. Biometrics is the science of using biological characteristics or traits to identify humans. One of the earliest uses of biometrics was recorded by explorer Joao de Barros. He reported that Chinese merchants in the 14th century were recording children's palm prints and footprints on paper to identify them later. Later in Europe they started using body measurements to identify criminals until the late 1800s but later reverted to the Chinese methods of fingerprinting when they found that some body measurements could identify more than one person. Today, the technology of biometrics has grown from this single method of fingerprinting to various methods, such as: fingerprinting, voice verification, hand-geometry, iris scanning, retina scanning, face recognition, palm printing signature recognition, and keystroke dynamics.

There are certain things that are required in order to use a biological measurement for biometrics. To be usable it must be a characteristic everyone has, there must be a difference in the characteristic from person to person (such as a

fingerprint), the characteristic should not change over a period of time, and the characteristic needs to be measurable quantitatively.

> However, for a practical biometric system, we must also consider issues of performance, acceptability, and circumvention. In other words, a practical system must meet accuracy, speed, and resource requirements, and it must be harmless to the users, accepted by the intended population, and sufficiently robust to various fraudulent methods and attacks. (Prabhakar)

A biometric system is a computer system that uses biometric authentication as a source of security and grants or denies access based upon biometrics. Biometric authentication refers to the study of automating the methods of human recognition using one or more physical or behavioral traits.

There are two main application types of biometric systems: identification and verification. In both types there is a database of acquired characteristic data, usually encrypted by an algorithm. The difference between the two types is how the database is searched. In identification mode, the system answers the general question: who is this person? It records a biometric characteristic of the person in question, whether it's a fingerprint, or iris scan, uses an algorithm to compute data the system can use, then compares that data to every record in the database. In this system there is no identity claim made by the person in question. An example of this would be in airport security, where they have a database filled with terrorist profiles. A biometric characteristic would then be recorded from everyone entering the airport and compared to this database, and if a match is made, security apprehends the suspected terrorist.

In verification mode, it answers the question: is this Bob? In this type of system, an individual will claim to be someone, usually by inputting a PIN or login name. Then a biometric characteristic is recorded from the person, and compared to the one on record for that PIN or login information. An example of this type of biometric system might be in the business world, where only certain employees have access to the server room. An employee would walk up to the door, input their PIN, and then perhaps a hand scan is used to verify the PIN to the person in question. If the hand scan matches the one on record for that PIN, and if the employee with that PIN is allowed in the server room, the door will open.

When a person is entered into the database it is called the enrollment phase. During this phase a biometric reader such as a fingerprint scanner, or iris scanner will acquire an individual's biometric characteristic. This biometric reader produces a digital representation of the characteristic. It does this by sending the data through a numerical algorithm. This data is then entered into the database and called a template. The first time an authorized user uses the system, they will need to go through the enrollment phase. In the case of the verification system, the next time the user tries to access the system, they will need to provide the reader their biometric characteristic, it will then create a template from this, and compare it to the template in the database and give it a score or match value. In the identification system the same thing will take place, but it will compare it to all of the templates in the database and it will receive many match values. The final step in the verification process is the decision to either accept the user or reject them. It bases the decision on the system threshold.

> This threshold value is either a parameter of the comparison process itself, or the system compares the resulting match value with the threshold value. If, for example, in a system performing identity verification, the match value is equal to or higher than the threshold value, the user is accepted. In an identification system, acceptance might require a match value that is both higher than the threshold value and higher than the second-best match by a specific amount. (Matyas)

Again the purpose of a biometric authentication system is to automate the decision making of granting access or not. But the systems are not perfect; therefore it cannot give definitive answers. That is why biometric systems work on scales. Two samples from the same person like a fingerprint might not produce the same digital representation every time, which could be caused by a few factors such as sensor noise, dry fingers, cuts and bruises, temperature and humidity, or finger placement or pressure.

The errors that biometric systems make fall into two categories: false match or false non-match. A false match error occurs when the system determines that a sample matches a template of someone different. It sees the biometric data from two different people to be from the same person. This error could result in an acceptance of an impostor. A false non-match error occurs when the system determines that a sample does not match a template that it should. The system does not accept a legitimate user that it should.

When biometric systems are set up, they decide the security level needed based on the application. This in turn will require them to make trade offs between the false

match rate (FMR) and false non-match rate (FNMR). The FMR and FNMR are functions of what is called the system threshold. For a system application that requires very high security, the FMR will need to be as small as possible. This is called raising the threshold. Doing this will also raise the FNMR; meaning that sometimes it will not accept legitimate users. For a less secure system, perhaps general building admission, where more secure systems are found later, they would not require the FMR to be that small. This is lowering the threshold. As the threshold is lowered, FMR increases, and FNMR decreases. Here is an excellent illustration of these functions found in "Biometric Recognition: Security and Privacy Concerns" an article written by Prabhakar, Pankanti, and Jain.

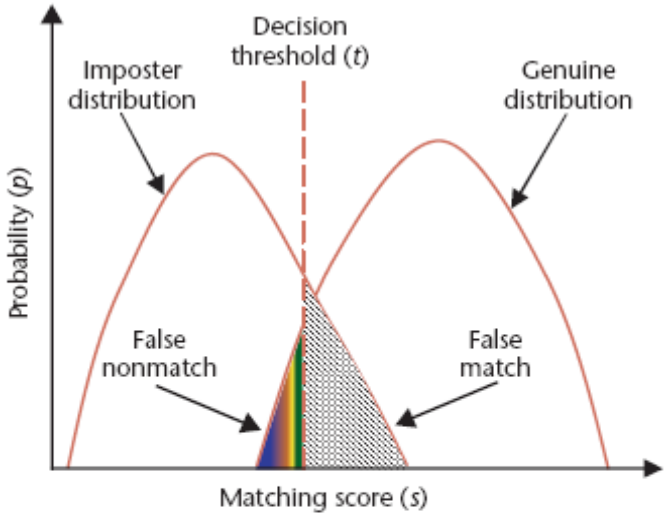

Figure 2. Biometric system error rates: The curves show false match rate (FMR) and false nonmatch (FNMR) rate for a given threshold *t* over the genuine and impostor score distributions. FMR is the percentage of nonmate pairs whose matching scores are greater than or equal to *t*, and FNMR is the percentage of mate pairs whose matching scores are less than *t*.

There are many applications of this new technology all over the world. They can be found in areas such as criminal identification, border control, background checks,

building security and many others. The West Virginia Department of Motor Vehicles uses face recognition to search for duplicate and fraudulent license applications. Georgia state drivers' licenses have a digital thumbprint incorporated into it. New York City uses a system that allows probation officers to check in with low-risk probationers on set dates using video screens and biometric authentication. Correction facilities across the nation have ID cards with biometric data saved on them, and when leaving, it is compared with a hand scan captured from the card carrier. Some bank accounts require voice authentication to perform over the phone bank transfers. There are even automated border control systems already in place to the north.

With all of these biometric systems in charge of such important systems, the technology must be secure. Biometric systems are different from regular password systems, and much more secure. Biometric systems can actually authenticate a user, whereas a username and password doesn't really tell the system who is on it, because passwords are easy to steal. "It is significantly more difficult to copy, share, or distribute biometrics. Biometrics cannot be lost or forgotten, and online biometrics-based recognition systems require the person being recognized to be present at the point of recognition" (Prabhakar). With password systems, the system is only as secure as the least secure password. But with biometrics, all of the templates are all equally secure. Some arguments about biometric system security is that attackers that are motivated enough to get into a system, could cut off limbs to authorized users and use them. But the new biometric systems are able to tell if the sample is from a living person or not. The sensors are able to look for pulses in fingers or hands, and the retina and iris scans are able sense small dilations and constrictions that happen without us even knowing.

Tsutomu Matsumoto, a Japanese cryptographer from Yokohama National University, and some of his colleagues reported that they successfully made fake fingers that were accepted by fingerprint readers on a surprisingly high rate. The defense against this claim though is that the fake fingers used in their study were made from molds of fingers that wanted to be used. It will be very hard to make a mold of someone's finger without them knowing.

Further action can be taken to secure these biometric systems in the way that the templates are stored, whether it be in a database or in a personal ID card. When the biometric data is collected at enrollment time, it will be sent through some method of cryptography. This method should be non-invertible, such as a hashing function. Then, when the person tries to enter the system, the same hashing function will be used to convert the collected biometric from the sensor, then the templates are matched. This is very useful in the event that a hacker actually achieves compromising a biometric. If a hacker somehow acquires a biometric template, such as hacking into the database and stealing the template, or intercepting it in transmission from the sensor to the database, the system can change the hashing function to use for that user, rendering the stolen template useless. IBM has come up with one solution that is similar to this; they use algorithms which stretch, twist, and squeeze the fingerprint and save this transformed template. This way "if someone steals your fingerprint, you're just issued a new one, like a replacement credit card number" (Talbot). The ideal biometric system setup was described by a writer for the EFF, William Abernathy, who is actually against the implementation of biometric systems. Abernathy said that biometric systems should only be implemented if the system is "built to the highest levels of data security,

including transmission that prevents interception, storage that prevents theft, and system-wide architecture to prevent both intrusion and compromise by corrupt or deceitful agents within the organization". And most new biometric systems are able to achieve all of these aspects of security, but it's up to the installer to implement and configure these correctly. In any event, biometric systems are more secure than present day password/ PIN based systems.

There are many people who are skeptical and against biometric systems. They believe that they are unreliable and impede on our civil liberties and right to privacy. To address the unreliability issue, the technology is new and quickly improving. But that doesn't go to say that the technology isn't reliable now. There have been tests done on facial recognition systems in airports in Florida and Boston and a few others, and these studies have found that the systems were about 50% effective. This low efficiency rate was due to a few factors such as inadequate lighting, non-frontal images, or disguises were worn. All of these could be addressed by installing the cameras at better locations. They could install them on the top and both sides of all of the metal detectors, and add lighting as needed. That way, there is a much better chance of getting a clear, frontal image that is usable to the system. There already has to be personnel there to man the metal detectors, why not let them have a preview screen right there to make sure a clear picture was taken? Even if a facial recognition system has a 50% chance of detecting a terrorist in a crowd, isn't that better than not having the system? That could be good enough to keep them from trying to enter that airport all together. I do not believe that the argument against the efficiency of the systems justifies the abandonment of the technology.

The next issue of concern is privacy. With the recent explosion of biometric system implementation, many privacy advocates have been getting nervous. Not so much for simple fingerprint systems, even though they don't like the idea of our biometrics stored on a database. They are more nervous about a kind of biometrics called covert biometrics. This is more evident in biometric technologies where it is possible to capture the biometric without the person knowing, such as face recognition systems. We can use our airport example again here. Along with the cameras that are visible to the passengers in an airport, there are also many hidden cameras capturing facial images.

This type of system is expected to not only be in airports and private buildings, but spread to public streets. Video surveillance systems have been installed in parts of London where there was a drop in crime in those areas by as much as 40%. This wasn't an ordinary video surveillance system though, we have those installed in cities here in the US, the one in London was connected to a face recognition system as well.

We are all familiar with our fundamental right to privacy and protection from unreasonable searches. But does a public surveillance system with face recognition capabilities invade our right to privacy? Some groups such as the American Civil Liberties Union compare these systems to police lineups. They used this analogy when commenting about the use of a facial recognition system at Super Bowl XXXV. First of all we need to remember that the constitution only limits the government. If the court system found face recognition systems of this nature to be in violation of our right to privacy, that would not prevent private buildings such as banks, stores, or even your workplace from using this technology. But it is my belief that it would not be

unconstitutional for the government to use this face recognition video surveillance in a public place. The fourth amendment right to privacy is based upon our expected level of privacy. It is reasonable to say that you expect to have more privacy in your house with all of your blinds shut then when you are in a shopping mall. Therefore, the expectation of privacy cannot be high in public places. Another matter to point out is that the fourth amendment protects against unreasonable searches, inferring that reasonable ones are legal. This brings up two points. Firstly, if you happen to be identified by one of these face recognition systems because you match the biometrics of a criminal on a watch list, and then a human confirms this belief; that alone is reasonable enough. The system finds you in a crowd, but it is a human that finally determines if they will apprehend you or not. Secondly, the simple use of a video camera to watch a crowd is not searching. It has been decided before in the past by the Supreme Court that a search by a government official is when they invade an individual's reasonable expectation of privacy. No one is being searched when the camera focuses on their face; the crowd is being observed.

When arguing about the privacy issue of these systems one must also remember that it is simply comparing a picture of an individuals face to a known database of terrorists or known criminals. I believe that these systems do not cause any privacy concerns as long as these systems do not record any information on the individual whose picture was taken, or link to any other systems or databases. There is no expected privacy in public or physical features, such as your face, that are exposed to the public all the time.

I believe that the current systems that are being used, such as the one used for the Super Bowl, did not invade peoples' privacy. These systems do have the capability to infringe on our privacy if they are abused. But many things can invade our privacy if they are abused. I believe that there should be some legislation made to prevent an Orwellian government biometric surveillance system, such as ones depicted in sci-fi movies of the future. Limitations must be set as to the enrollment in databases in systems used to sniff out criminals; some issues need to be addressed. What crimes allow enrollment into the database? How long do they remain in the database? And, who has the authority to enroll individuals into the database? But the government should be allowed to use them to automate already legal procedures. Using a face recognition surveillance system isn't any different than a police officer standing on a busy sidewalk holding a photograph of a suspected criminal, looking for him in the passing crowds (Ciensky). The system only automates this process and allows many more comparisons to be made.

The potential of this new technology is incredible, as long as it is used responsibly. These systems could save lives. Imagine if these were in place before the 9-11 attacks. Many of the terrorists who got onto the planes used in the attacks were already known terrorists, and on the governments watch list, with photographs available of them. This doesn't mean that the system would have caught them, but statistically not all of them would have made it past the system; maybe enough to prevent the attacks.

If the necessary issues are addressed, and the systems are implemented correctly, there will not be any trade off between security and privacy. People who

aren’t in the database don’t need to worry about their rights being infringed, and the people already in the database, gave up their rights when they committed their crimes. Benjamin Franklin once said, “they that can give up essential liberty to obtain a little temporary security deserve neither liberty nor security”. Biometrics could bring us privacy and security, with no sacrifices.

Bibliography

Abernathy, William, and Lee Tien. “Biometrics: Who’s watching you.” EFF.org. Ed. Sarah Granger. 26 Apr. 2006. <http://www.eff.org/Privacy/Surveillance/biometrics/>.

“Biometrics.” Wikipedia. 12 Apr 2006. 20 Apr 2006. <http://en.wikipedia.org/w/index.php?title=Biometrics&oldid=49630571>.

Bowyer, Kevin W. “Face Recognition Technology: Security versus Privacy.” IEEE Technology and Seciety (Spring 2004): 9-20.

Ciensky, J. “Police cameras denounced as threat to privacy.” National Post Online. 12 July 2001. 20 Apr. 2006. <www.nationapost.com>.

Coleman, Stephen. “Biometrics: Solving cases of mistaken identity and more.” FBI Law Enforcement Bulletin 69.6 (June 2000): 9-16.

Matsumoto, Tsutomu, et al., “Impact of Artificial Gummy Fingers on Fingerprint Systems.” Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677, Int’l Soc. for Optical Engineering, 2002: pp. 275–289.

Matyas Jr., Vaclav, and Zdenek Riha, "Toward Reliable User Authentication through Biometrics.” IEEE Security and Privacy 01.3 (2003): 45-49.

McCullagh, D. “Call It Super Bowl Face Scan I,” Wired News. 2 Feb. 2001. 20 Apr 2006. <http://www.wired.com/news/politics/ 0,1283,41571,00.html>.

Prabhakar, Salil, Sharath Pankanti, and Anil K. Jain, "Biometric Recognition: Security and Privacy Concerns.” IEEE Security and Privacy 01.2 (2003): 33-42.

Talbot, David. “Changeable Fingerprint.” Technology Review 108.11 (Dec2005/ Jan2006): 34-34, 1/3p.