Biometrics

Ihssan Alkadi, University of Louisiana at Lafayette
Ghassan Alkadi, Southeastern Louisiana University

ABSTRACT

People can change the way they look by changing their hair color, hair style, eye color, and even general appearance now-a-days with the advancement of technology. Because of plastic surgery, people can completely change their appearance to where no one would recognize them. It is also easy for people to steal other's identities with the improvement of technology. For some people, it is hard to keep up with credit cards and passwords and other identity-safe substances. The development of biometrics would solve all of these problems. You can change the way you look but you cannot change the structure of your body. In the world today there are many ways to gain access to someone's identity. Through the use of biometrics, such as fingerprinting, facial recognition and retinal scanning, identity fraud can be reduced and hopefully one day stopped. The information technology age today that we are all accustomed to is an ever changing scene. New means of quicker, more reliable, and more versatile applications are appearing so fast that they become obsolete not long after they hit the market. Biometrics involved in applications is the one exception. It offers security, reliability, convenience, identification, and verification to the market where the various amounts of information in networks, and security operations that have to be protected. In a quickly growing global economy, fraudulent claims grow at equal pace and the technology is here to prevent it. However, with growing technology comes, concerns to be addressed.

The term biometrics refers to the measurements of "certain physical or behavioral characteristics of an individual used to create a unique identifier which can be electronically stored, retrieved and compared for positive identity purposes"(Gershon). Through the use of computers as well as other electronic devices, the world is becoming more computer literate. This has done wonders for many fields as far as advancement and understanding, but it has also created problems in privacy. It is now extremely easy for someone to get into a computer and access numerous files on themselves as well as other individuals. Through the use and education of how and why biometrics is used, the chance of identity fraud as well as unauthorized access into files can be reduced.

There are many different uses and forms of how biometrics is used. Some forms most people are familiar with are the use of a signature or hand geometry to gain access to personal files. There is also iris scan and smart cards. The three forms of biometrics this paper will explain are the uses of fingerprinting, retinal scans and facial recognition.

Fingerprinting "is the oldest method which has been successfully used in numerous applications" (Jain, Prabhacker). Every person is born with a different fingerprint, even identical twins, so it is almost impossible for some one to have their fingerprint misread. Fingerprinting was first used in the 14th century in China so that parents could distinguish their own children from other people's children. The English then began to use this process in 1858. The way this technique is done today is that the user "presses his finger gently against a small reader surface usually of about 2 inch square size" (NCSC). Then the reader is hooked up to a computer and is scanned and sent to the database. Sometimes there is a threat of fake fingerprints, so to prevent this; some of the systems measure blood flow. Today, fingerprinting is not only used for criminal investigations, it is also used as verification at ATMs, some grocery stores and for driver's license registration. Some of the main reasons that fingerprinting is still used so widely today is that it is easy and fast and its longtime use has proven that it is effective.

Retinal scanning is another use in biometrics being used today. Although people are familiar with this technique, it “is used almost exclusively in high-end security applications” (NCSC). The military and power plants are two examples of institutions that might use this kind of technology. Research of retina scanning began in the 1930s and suggested that the use of the patterns of the blood vessels on the back of the eye were unique to each person. The way this process works is that the person who is getting scanned must look through a small opening of the device that takes the scan. The user must keep their head still and allow the device to take a scan of the retina and verify it, which takes about 10-15 seconds. This technique works well because the human retina is impossible to replicate. There is no known way to do this, and the retina of a dead person deteriorates too fast for it to be replicated or used. The retina is “difficult to spoof” and for this reason as well as the “minimal alignment and focus problems” retina scans are another way to keep your identity your own.

The last use of biometrics this paper will explain is facial recognition. Research for this technique began in the 1980s and was not available for commercial use until the 1990s. Most people were not really familiar with this until after September 11, 2001. People who attended Super Bowl XXXV, were “part of the largest police lineup ever conducted” (Bonsor). As the crowd walked in, a camera took pictures of their faces and plugged them into a database of criminal mug shots. The way facial recognition works is that the user “faces the camera, standing about two feet from it. The system will locate the user’s face and perform matches against the claimed identity” (NCSC). This process takes about 5 seconds. Currently this technique is being used to help protect against terrorist crimes. It is also being used by some bank tellers that use facial recognition for some verification purposes. This technique has been embraced because of the acceptability of it. Facial recognition can be utilized using standard video output and can be used with “previously compiled photo databases” (Gershon).

There are many different uses for biometrics in this technology-based world that we are living in today. Even though it seems as though more people’s private lives are being invaded, biometrics is continuing to use the ever evolving technologies to create fool proof ways of keeping personal information out of reach of unauthorized persons. Through research and dedication the world of biometrics is becoming more and more accessible to the public. Banks as well as other institutions have tested the use of different biometric techniques and have found that “anything that saves the information-overloaded citizens from having to remember another password of personal id number comes as a welcome respite” (O’Sullivan). And as this happens the goal of having and keeping one’s privacy seems more obtainable than ever. The terms “Biometrics” and “Biometry” have been used since early in the 20th century to refer to the field of development of statistical and mathematical methods related to data analysis problems in the biological sciences. These methods are used for the analysis of data from agricultural field experiments to compare the different varieties of wheat. The analysis of data from human clinical trials assess the comparative usefulness of competing therapies for disease. These methods are also used for the analysis of data from environmental studies on the effects of air or water pollution on the appearance of human disease in a region or country. These are all examples of problems that would fall under the umbrella of “Biometrics” as the term has been historically used.

Lately, the term “Biometrics” has also been used to refer to the up-and-coming field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition.

Biometrics was popularized by the movie “Mission Impossible.” Years ago when the movie came out people thought “Wow! That would be neat and easy if our lives were like that.” To be able to use your fingerprint or your eyes (a retinal scan) to maintain access would be a wonderful thing. You would never need to bring anything with you or remember any codes to be able to do anything. From the business aspect, this would also lessen the possibility for information getting into the wrong hands.

Everyone has definitive and unchanging physical attributes that can always be used to identify oneself. Security systems are increasingly using these attributes to its advantage. Biometrics relies on certain physiological characteristics that can be measured and utilized to distinguish people with a reasonably high degree of precision. The physical attributes, mentioned before, are facial and hand geometries, voice, fingerprints, handwriting, and skin texture and iris patterns. The key to making Biometrics accepted is to perform it in a respectful and non-invasive manner.

One main concern with Biometrics is that the databases are very large and expensive to maintain. When a database is so large, you must have very unique entries so that the computer can process an exact match. Examples of a unique entry would be fingerprints and iris patterns. These are the only details precise enough to make a one-to-many match. A problem that plagues large databases is the problem of creating a false negative, or even worse a false positive, reading. For example, an authorized person could be denied access into a secure place or a secure database because the computer could not achieve a match. The worst case scenario is a false positive. This is when an unauthorized person is given access into these secure places because the computer matched something incorrectly in the database.

To reduce errors, one needs to choose the correct type of Biometric method of identification for their business. Choosing the right Biometric method depends on a number of details. Some of these details are the monetary constraints, the height of security that is needed, the size of the database that is needed, and the speed needed to access and operate your database. For example, iris scanning equipment was installed in schools in the Plumsted Township in New Jersey. The teachers and staff have been using swipe cards to gain access into their classrooms and into the school. The students have been using an iris scan to enter into the school and to exit from the school. This has helped the school to keep track of the flow of traffic coming on and off of the premises at all times and keeping record of these activities. This has created a sense of well-being for the community of Plumstead, New Jersey.

Being able to use Biometrics in any situation could be greatly beneficial. Not only would it lessen the responsibilities of the everyday person, it would also make people feel more comfortable knowing that “someone” is watching over them and making sure that the right people are where they need to be and also knowing that the wrong people are kept away from things that they should not have. For prisons, schools, and institutions with ever changing populations, research shows that iris scanning should be used because it is the most flexible and accurate Biometric method available. It will produce the least amount of errors.

With everything new that comes out, especially when it involves technology, there are possible errors that could occur. The problem is not always a technical problem. Likewise, the solution is not always technical. Bad people will always figure out a way around new ideas to security. They will also always have an easy time when good people place too much faith in technology. A Biometric program will always be run by some trusted, authorized human being. In being a human being, mistakes can happen and corruption can occur. If Biometrics is a solution for your business, make sure that there are a multiple number of defenses that go along with it.

Traditional business networks in the past have relied on passwords or pins to gain access to their systems. Although the previous access methods are effective, they are effective for one thing and only one thing which is “accessibility.” The implementation of biometrics rather than pins or passwords is designed for accessibility, but also allows for systems to use identification, verification, and security. The biometric applications consist of scanning a person based on physiological and behavioral characteristics. This simply means data derived from directly analyzing or measuring parts of the human body for verification. Examples of these are retina scans, face recognition, fingerprints, voice recognition, and handwriting. As the global economy increases every year so does the risk of fraud through our electronic transmissions in our business and our homes. The applications where biometrics is implemented include network, workstations, remote access to resources, single sign on, domain access, transaction security, and Internet security (biometric info).

To understand the growing demand for biometrics it is only logical to understand it from its early intentions. The field of biometric study began with an anthropologist named Alphonse Bertillion in the 1880's. The problem he faced was with identifying convicted criminals. He sought to fix the problem with repeating offenders who would always change their names to various aliases or reshaped their normal appearance in some way. However, Bertillion figured out that regardless of what appearance the criminals presented certain features of the human body remained unchanged. Examples included the size of their skull or the length of their fingers. The method he developed was called “Bertillonage.” His method was used by authorities for quite a while until they discovered that some people shared the same measurements. Moreover, two people could be treated as the same person. The next step in advancing the concept of measuring a person's physical traits was realized by Richard Henry of Scotland Yard. Where

he came up with using fingerprinting for verification. After this the police adopted the fingerprinting system and is still used today (ganges).

Although technological advances were sparse in the past, today we have the availability and the know how to implement these concepts to insure the accuracy of biometric identification and make it a reliable field. The problem with the use of biometrics today and its potential growth is that its use and applications available have not been fully realized by the public. The most popular means of use in recent years is institutions like bank's ATM's and government programs. These applications are mainly for entry control and security. The main authentication scheme for these has been iris recognition (techrepublic). The main drawback to biometric growth is acceptance and public concerns about new application use. The *onClick Corporation*, a manufacturer of fingerprint and signature biometrics enclosed a report on there website from *TMC Research* entitled: *A Comprehensive Report On Technologies, Vendors, Products and Applications (2000-2010)*. This report basically summarizes the concerns gathered from surveys about further implementation of biometrics. A few of the concerns addressed were, "I am worried about privacy and confidentiality," "If biometrics fade in time then we're left in the dark!" The key answer to these concerns is what biometrics is trying to address. In dealing with privacy and confidentiality, fingerprints, and signatures are superior to previous passwords to databases, which can be copied for fraudulent authentication. The biometric applications are stored in a database and a copy of the fingerprint or signature verification will not work for fraudulent attempts. To address the concern about biometrics "fading in time," onClick gives multiple facts showing it is here to stay. Facts like the concept of biometrics is only new to the private entities, it has shown a wide variety of use since the 1980's in government welfare programs. "The biometric industry, once worth \$601 million in 2002, is expected to grow into a \$4 billion industry by 2007." There are numerous amounts of markets that have already put biometrics to use that the public may not realize such as government, medical, military, aviation, transportation (airports), engineering manufacturing, data centers, etc. Credit card companies are also adopting biometrics for there cards called smartcards. Companies like *MasterCard* say that it will reduce fraud by 80%. *IBC* (international Biometric Group) which is also a biometric research firm enclosed on their site actual charts showing projected revenues and usage rates in the market share of biometrics (on next page). The downside of new "high-tech" advances is always welcoming criticism and insecurity. The real truth lies in analyzing the benefits that such implementations like biometrics can offer. Various beneficial aspects can be seen in the business setting. Consumers for example have the availability of privacy, security, and convenience. This will offer anonymous transaction abilities, safer online purchases, e-mail and private files will be secured, also the convenience of not having to remember or reset your password. Employers will also notice more flexibility with increased security to detect fraudulent account access, reduced cost from password maintenance, and competitive advantage because of familiarity with advanced technology. And last but not least, the public sector usage will benefit from increased trust in reducing entitlement abuse and reduce costs because it will be the strongest way to deter benefits fraud (biometric info).

In closing, I would like to add that I was interested in this topic because I use biometric fingerprint scans at the restaurant were I work everyday and I find that it has added such convenience and quick reliable access whenever I need it. Any business entity is missing out if they haven't adopted some form of biometrics in their environment. The truth is the use of biometrics is gaining momentum. However the widespread use and acceptance of biometrics is, at this current time, still young in development.

REFERENCES

1. Ahead of the Annual General Meeting is Precise Biometrics AB. Precise Biometrics. http://biz.yahoo.com/prnews/050323/lnw025_2.html. March 23, 2005.
2. Chakraborty, B. Identix Slides; Worries Biometrics Programs May Slow Down. *Associated Press*.
3. Consortium, C. Biometrics Not a Silver Bullet for Security Strategies. *Analyst Firm*. Tekrati, Inc. 2000-2005.
4. Definition of Biometrics. International Biometric Society. <http://www.tibs.org/DefinitionofBiometrics.htm>. March 23, 2005.
5. TSA should assess... *National Journal's Technology Daily*. <http://www.govexec.com/dailyfed/0305/032105tdpml.htm>. March 22, 2005.

6. Bonsor, Kevin. How Facial Recognition Systems Work. <http://howstuffworks.xom>
7. Gershon, Christine. Biometrics Authentication & Smart Cards.
http://www.fts.gsa.gov/2003_network_conference/5-1_biometric_smartcards/index.htm April 14, 2003.
8. Jain, Anil & Salil Prabhakar. Fingerprint Identification. <http://biometrics.cse.msu.edu/fingerprint.html>
9. National Center for State Courts. <http://www.ncsconline.org/>
10. O'Sullivan, Orla. Biometrics Comes To Life. http://www.banking.com/aba/caver_0197.htm. 1997.
11. <http://ganges.cs.tcd.ie.html>. Team B.A.N.A.N.A
12. <http://www.biometricsinfo.org>. Biometrics Information Resource
13. <http://www.onclickcorporation.com>. TMC Research Report. The Biometric Industry: A Comprehensive Report on Technologies, Vendors, Products, and Applications (2000-2010).
14. <http://www.biometricgroup.com>. International Biometric Group: Biometrics Market and Industry Report 2004-2008.
15. <http://www.techrepublic.com>. Case study reveals the pros and Cons of Biometrics

NOTES