Global Information Assurance Certification Paper

Facial Recognition Technology

Karen J. Petrauskas
December 29, 2003

ABSTRACT

This paper gives an overview of biometrics: the process of and use in a security setting. After a definition of biometrics and a summary list of the different types of biometrics, the paper moves forward to discuss the pros and cons of using this technology. A brief overview of how biometrics works leads into a description of some of the test of this technology for practical uses. The summary discusses the use of biometrics in a casino environment. Given the information contained within the paper, this environment seems fitted for the use of this technology.

BIOMETRICS DEFINED

Biometrics is the use of an individual's physical or behavioral characteristics to uniquely identify them for authentication purposes. Biometric features include fingerprints, iris scans, veins, keystrokes, palm geometry, speaker verification, dynamic signature analysis, and facial characteristics. The biometric that deals with facial characteristics is called Facial Recognition Technology (FRT). Biometric devices cannot determine name, age, race, birthplace, health, citizenship, gender or income. These are common defining attributes of demographic classes.

According to Wayman, some of the issues that impact biometric measures such as FRT include the following:

- hard to obtain and cannot be continuously tracked
- private, but not secret
- can be stolen, but supervised use of stolen measure requires mechanical assistance
- cannot be revoked
- contain limited additional information
- contain limited additional information
- can be used (with difficulty) to link records
- weak identifier compared to SSN, phone or CC#

USES FOR BIOMETRICS

National ID Cards
INS
Banking/ATM
Point of Sale
Airport Security/Tickets
Surveillance
Site Access
Security: Identify or Verify
Legal/Financial Documents
Medical Information Cards

WHY BIOMETRICS: ADVANTAGES TO OTHER METHODS OF AUTHENTICATION

For security purposes biometrics is the most secure and convenient form of authentication. Security has three levels of authentication: What you know (a PIN #) which can be forgotten or stolen and therefore is a low level of security. What you have (smart card) which can be stolen or duplicated. What you are (a unique biometric). The biometric is the most secure of these three levels because it cannot be lost, stolen, forgotten, or easily forged. Biometric use can provide the most positive

identification/verification system available. The biometric chosen should match the intended use in terms of parameters such as ease of use, willingness to enroll, speed, ect.

For business purposes, biometrics promise to speed service through automation, reduce costs, and increase security of transactions. Establishing a person's identity is important as technology advances toward enabling electronic access to money and information. Biometric systems can function either to recognize or authenticate individuals. Recognition establishes a person's identity and authentication verifies the individual is who is says he is.

ERRORS: THE TECHNICAL DISADVANTAGES OF BIOMETRICS

Facial recognition technology is not yet a perfect science and is therefore subject to errors. The two most common errors discussed are the False Acceptance Rate and the False Rejection Rate. These errors are connected by a performance measure called the Crossover Rate.

False Acceptance Rate (FAR): The authorization of a non-authorized person – generally a measure more relevant for security purposes as it defines the probability of unauthorized people gaining access to secure areas/data. FAR can be lowered by raising the threshold. The threshold is the level of significance (similarity) required between the template and the current image. The template is a stored image captured and normalized during the enrollment process. It is the baseline image against which future authentications are compared. However, raising the threshold to create a lower FAR increases the False Rejection Rate (FRR).

False Rejection Rate (FRR): The rejection of an authorized person - generally thought of as a comfort criterion because a false rejection is annoying but not a breech of security. FRR is impacted by factors such as lighting, age, facial hair and glasses.

Crossover Rate (CER): The error rate at which FAR = FRR. A lower rate indicates a better system where both FAR, a security parameter, and FRR, a comfort parameter, are both improved versus systems with higher CERs.

Factors impacting FAR given constant FRR include: the characteristics of the biometric used, the quality of the camera/sensors, user behavior, software performance, and the amount of templates in the system, the type of authentication method used. These factors impact FAR and FRR differently as shown below:

	FAR	FRR
Biometric Characteristics		
uniqueness	X	
permanence		X
measurability		X

Quality of camera/sensors			X
User behavior			X
Software performance	X		X
Authentication Method	X		X

Failure To Acquire (FTA): The repeated false rejection of attempts to authenticate subjects. Factors negatively impacting authentication under FTA are usually temporary and can be attributed to “bandages”, poor sensors, and poor conditions. FTA is a class of FRR.

Failure To Enroll Rate (FTE, also FER): The FER is the proportion of people who fail to be enrolled successfully – have a facial image converted into a template by the software.

False Identification Rate (FIR): The False Identification Rate is the probability in an identification that the biometric feature is falsely assigned to a reference.

AN INTRA-BIOMETRIC COMPARISON OF FEATURES

Generally biometric features should have the following three characteristics:

Uniqueness: the biometric feature used has to be person specific – it is this uniqueness that provides the highest security

Universality: the type of feature used has to be shared amongst everyone – distance between eyes

Permanence: the biometric feature use has to be consistent over time – unaffected by age, growth, injury, or scarring (http://home.t-online.de/home/manfred.bromba/biofage.htm#Biometrie.

The permanence of different type of biometrics is illustrated in the chart below. The chart does not take into effect easily changed conditions such as dirt and cuts. The level of x’s corresponds directly to the level of permanence where more x’s = more permanence.

Biometric trait	**Permanence over time**
Fingerprint	xxxxxx
Signature	xxxx
Facial Structure	xxxxx
Iris pattern	xxxxxxxxx
Retina	xxxxxxxx
Hand geometry	xxxxxxx
Finger geometry	xxxxxxx
Vein structure of the back of the hand	xxxxxx

Ear form	xxxxxx
Voice (tone)	xxx
DNA	xxxxxxxxx
Odor	xxxxxx
Keyboard strokes	xxxx
Comparison Password	xxxxx

Source: http://home.t-online.de/home/manfred.bromba/biofage.htm#Biometrie.

Clearly not all biometric features are created equal. The two charts below list the best and worst biometric for varying parameters and factors that impact their performance. In the first chart FRT scores highest in comfort and availability. Its accuracy is par at best being beaten by eye biometrics, DNA, and hand biometrics.

In the second chart FRT only scores high in accuracy. For all other parameters FRT is a medium at best. Additionally, lighting, age, glasses, and hair impact FRT negatively.

Biometric trait	**Comfort**	**Exactness**	**Availability**	**Cost**
Fingerprint	xxxxxxx	xxxxxxx	Xxxx	xxx
Signature	xxx	xxxx	Xxxx	xxxx
Facial Structure	xxxxxxxxx	xxxx	Xxxxxxx	xxxxx
Iris pattern	xxxxxxxx	xxxxxxxxx	xxxxxxxx	xxxxxxxx
Retina	xxxxxx	xxxxxxxx	xxxxx	xxxxxxx
Hand geometry	xxxxxx	xxxxx	xxxxxx	xxxxx
Finger geometry	xxxxxxx	xxx	xxxxxxx	xxxx
Vein structure - back of the hand	xxxxxx	xxxxxx	xxxxxx	xxxxx
Ear form	xxxxx	xxxx	xxxxxxx	xxxxx
Voice (tone)	xxxx	xx	xxx	xx
DNA	x	xxxxxxx	xxxxxxxxx	xxxxxxxxx
Odor	?	xx	xxxxxxx	?
Keyboard strokes	xxxx	x	xx	x
Comparison Password	xxxxx	xx	xxxxxxx	x

Source: http://home.t-online.de/home/manfred.bromba/biofage.htm#Biometrie.

Characteristic	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very High	Very High	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Medium	High

Required security level	High	Medium	High	Very High	Medium	Medium	Medium
Long-term stability	High	Medium	High	High	Medium	Medium	Medium

Source: http://www.computer.org/itpro/homepage/jan_feb01/security3b.htm

Device	Mean Time (Sec)	Median Time (Sec)	Min. Time (Sec)	PIN (Y/N)
Face	15	14	10	N
Hand	10	8	4	Y
Iris	12	10	4	Y
Vein	18	16	11	Y
Voice	12	11	10	N

Source: http://www.usenix.org/events/sec02/wayman.pdf

The conflicting performance grades for FRT as well as for the other biometric measures support the concept that there is no one best biometric feature. Therefore, in classic fashion, form follows function and the biometric feature used should be applicable to the need. For example, unless DNA authentication could be done quickly and cheaply it would not be used to gain access to the door at the gym. More importantly, the discrepancies between performances of the varying biometric features are evidence of a technology absent of standards and still emerging.

THE BIOMETRIC PROCESS: As simple as 1, 2, 3

In it's simplest form, facial recognition technology is all about matching up stored data about a person's facial characteristics to current data to determine if the data is the same or different. Facial recognition technology measures the characteristics of the face using its peaks and valleys, distances and size between and of facial features and extrapolations of how these relationships will change due to changes in facial expressions. "The human face contains approximately 80 of these nodal points; only 14 to 22 nodal points are needed for facial recognition" (http://www.ceet.niu.edu/faculty/vohra/tech497/present/securitysys.doc). Facial mapping, conducted with a digital camera, focuses on the inner region of the face, which runs from temple to temple and just over the lip.

The biometric process is a three (3) step process. The first step in using facial biometrics is to capture a baseline image of the subject during the enrollment process using a camera or video. The second step is the normalization of the baseline image. The baseline image is a digital image of a face, which is converted by software using the nodal characteristics of the subject's face, and adjusted for lighting, expression, and camera angle into a template. Nodal points are the defined, for example, as the distance between the eyes, tip of the nose, edge of the mouth, and chin. This area is also known as the "golden triangle" because it represents the area of a face least likely to be effective by changes in weight or age. At the time of authentication, the third step, the template is compared current image and the software decides, based upon

statistical comparisons of similarities and differences, whether or not the two images are the same. This process is detailed in the following discussion.

Enrollment Process:
Several pictures are taken from slightly different angles and using several different expressions. The same camera should be used to capture the authentication image if possible.

According to Wayman, the following operating conditions maximize the utility of the face recognition system.

- looking directly into the cameras
- diffuse frontal lighting
- interocular distance of at least 50 pixels
- high quality search or watch list images of the target surveillance watch lists restricted in number to reflect system performance.

Conversion Process:

Normalize the images captured during the enrollment process
Store the captured data as a template (The template will be smaller than the image from which it was conceived. Quality facial images require 150 – 300kb. Templates are approximately 1300 bytes – less than 1/100th the size of the facial image.

Authentication Process:

The authentication process is the event where a second image is compared to the base image to determine likeness. The authentication process is done on one of two bases: One-to-many (identification) or one-to-one (verification).

In a “one-to-many” or identification authentication (1:n) the live template is compared to all templates saved in the system to answer the question “Who Am I?” For example, if 15 people are authorized access to a restricted system the one-to-many authentication will compare the live template with each of the saved templates. If the software finds a match to any of the 15 saved templates the person is granted access. For small databases the strain on the system is not too severe but as databases grow so too does the strain on the system. Additionally, the False Acceptance error is increased with this type of comparison because several stored images may have similar characteristics as a presented image. In the case of large databases where multiple templates are matched it may require human assistance to grant the final authentication.

In “one-to-one” or verification (1:1), the user enters his identity, a requirement, into the system using a keypad or memory card then a biometric feature is scanned. The biometric feature must only be compared to the template assigned to that person. If a match occurs, verification is successful. If a system has only one template identification is similar to verification, but the user need not first enter his identity.

Verification is faster than identification when the database of templates is large because the system only has to match the live image to a specific template. Verification is more secure than identification because the user must enter an ID and the live image must match a specific stored template. With identification using a large database it is possible for the live image to match several stored templates.

APPROACHES TO BIOMETRICS

Neural Networks: Use algorithms to create a global map of a face.

Local Feature Analysis: The mostly widely used technology and closely related to Eigenface. It has the ability to recognize faces that have changed appearance or aspect. Local Feature Analysis records 15 -40 very small 2D blocks of a face and their relative location to each other. It also predicts how these relationships will change with a change in the appearance of the face. Because of this predictive ability, this approach can identify faces from perspectives other than straight ahead. It can adjust to changes 25 degrees in the horizontal and 15 degrees in the vertical planes.

Automatic Face Processing: uses distances between and ratios of distances between key facial features such as eyes, end of nose, and tip of mouth. AFP is the least advanced of the four approaches it may have an edge in frontal views with dimly lit environments.

Eigenface "one's own face": developed and patented at MIT uses global 2D grayscale (light and dark) images identifying distinctive characteristics of a face. Most faces can be reconstructed by combining the features of 100 – 125 different eigenfaces.

SYSTEM REQUIREMENTS

Camera: Facial recognition can work reasonably well at normal distances using standard off-the-shelf cameras with a minimum resolution of 320x240 and a speed of 3-5 frames per second. For recognition at a distance better quality cameras result in a proportionately better capability.

Software: Face recognition software is available through a multitude of commercial and academic sources. The software is the primary factor in the performance of FRT given a controlled environment.

PC: Generally, computation speeds adequate for pattern recognition are required. This is about 100 million operations per second, which have only recently been attained by affordable hardware (PC, DSP).

STANDARDIZATION

An issue that FRT needs to overcome in its efforts to gain greater usability is the creation of a set of technical standards. Technical standards relate to the integration of systems and long-term product support. The key issue in current FRT technology standards regards the use of proprietary algorithms, which create the eigenfaces. Until standards are developed the integration of systems is unlikely.

The most commonly cited biometric standard is BioAPI, which provides a biometric application programming interface. The BioAPI Specification defines an open system standard API that allows software applications to communicate with a broad range of biometric technologies in a common way. BioAPI was approved as an official ANSI standard in February 2002, and has been submitted as an international standard through SC37 (http://www.ibgweb.com/reports/public/biometrics_standards.html).

At the moment, biometric standards are still in progress or have been submitted for standardization to ISO. Among the topics treated are:

Biometric data formats

Biometric interface formats

Biometric evaluations

PROMISE vs. PRACTICALITY

The promise of increased security is outweighed by the problems of practicality. In college laboratories and numerous businesses across the globe people are racing to develop a FRT that reduces the CER to levels, which promote tight security and ease of access to authorized users. However, practical applications of these technologies have mostly failed. Whenever the technology is removed from its ideal conditions its performance suffers to the point of being near useless.

"Facial scan technologies are much more capable of identifying cooperative subjects, and are almost entirely incapable of identifying uncooperative subjects." (http://www.facial-scan.com/facial-scan_technology.htm).

DOD TEST

DOD Feret Test: "The results in Table 1 show that illumination and time between acquisitions of each image can significantly affect face recognition performance" (http://www.dodcounterdrug.com/facialrecognition/DLs/Feret7.pdf).

Category	False Alarm Rate	False Rejection Rate
Same day, same illumination	2%	.4%
Same day, different illumination	2%	9%
Different days	2%	11%
Different days over 1.5 years	2%	43%

This test dates to March 1997 and the results presented are for "best cases." While not impressive, they are better than the result of the previous test performed between 1994 and 1996. In addition to time and lighting, camera angle had a negative impact on

performance. According to Feret, a 15-degree change in angle will result in materially poor results and a 45-degree change in angle will negate the results. Note: this test is still running and accumulating results.

TAMPA TEST

An example of FRT not living up to the hype it is made out to be was performance of a FRT system employed by the Tampa, Florida Police Department. The system identified zero (0) bad guys. "Facial recognition technology on the streets of Tampa, Florida is an over hyped failure that has been seemingly abandoned by police officials, according to a report released today by the American Civil Liberties Union". The logs showed that the system never identified a single individual contained in the department's database of photographs. It was marked with errors such as, mismatching male and female subjects and subjects with significant age difference. "Several government agencies have already abandoned facial-recognition systems after finding they did not work as advertised, including the Immigration and Naturalization Service, which experimented with using the technology to identify people in cars at the Mexico-U.S. border" (http://archive.aclu.org/news/2001/n010302a.html).

CASINO TEST

There is however a place where FRT does work and that is in Casinos. Over 100 casinos in the United States have used FRT for years, mainly to catch cheaters. "When used in conjunction with casino surveillance cameras and databases on cheaters, the system can quickly recognize a known cheater, list his modus operandi and call up photographs of associates or co-conspirators -- all in a matter of seconds" (http://www.crimelynx.com/casino.html).

There are several reasons why FRT works well for casinos. It is a controlled environment where the lighting is constant, the subjects are stationary, and the camera angle is acceptable. For example, a person playing blackjack sits at a table a measured distance from the dealer looking mostly ahead at the cards. These conditions most closely approximate laboratory conditions therefore the results most closely match expectations.

SUMMARY

Face Recognition Technology is promised to be the lock that cannot be picked. The only key for this lock is a person's unique biometric feature. Additionally, active scanning of public places will help authorities capture more criminals, as they will now have no place to hide. They will no longer be anonymous.

The developers of biometric products hype these wonderful and comforting ideals. It is their business to do so and the market has responded. Recent events and global threats are the motivations that allow easy acceptance of this hype by the uneducated public. However, before everyone stands in a line at their local police department to be photographed, this technology and these ideals have a few more hurdles to clear.

Without a discussion concerning the right of privacy vs. the interest of security, I just want to bring to light that technical hurdles may be the easier hurdles to overcome. While the Supreme Court ruled that a face is a public object and therefore is not protected by the right of privacy, unwilling subjects of this technology, such as at the Super Bowl, hold this technology in distaste. The unwillingness of a subject be enrolled is a dual problem for FRT as it encroaches upon both the expectation of a right to privacy and impacts the capture rate during the enrollment process.

The more immediate hurdle to overcome is the technical hurdle. In the most publicized real life test the technology was a bust. In Tampa, not one bad guy was nabbed over the course of the test resulting in a statement from the manufacturer that maybe there were no bad guys in the area at that time.

The Feret tests of the DOD also show poor results mostly attributed to lighting and time but also including camera angle. These tests were performed in controlled conditions albeit five years ago and the technology surely have improved since then.

Where FRT works in real life is in the casino industry. If we look at conditions it becomes easily seen why. FRT works best in well-lit, steady subject, small distance environments. This is exactly what the casino environment provides.

Given the information presented in this paper is seems that iris or retina scans offer the same or better level of security than FRT. However, FRT is the biometric with the momentum behind it. A key difference is that FRT may enable surveillance at a distance where iris/retina scans can only be used for individual security. The obvious question then becomes, Why FRT?

References

1. "A Practical Guide to Biometric Security Technology. Selecting a Biometric Technology." URL: http://www.computer.org/itpro/homepage/jan_feb01/security3b.htm (8 November 2003).

2. "Bioidentification." URL: http://home.t-online.de/home/manfred.bromba/biofage.htm#Biometrie (8 November 2003).

3. "Biometrics: Face Recognition." URL: http://www-users.cs.york.ac.uk/~tomh/Biometrics.html (8 November 2003).

4. Curran, John. 26 February 2001. "Casinos Using Facial Surveillance." URL: http://www.crimelynx.com/casino.html (8 November 2003).

5. "Facial Scan Technology: How does it Work." URL: http://www.facial-scan.com/facial-scan_technology.htm (28 December 2003).

6. Philips, P. Jonathon, Martin, Alvin, Przbocki, Mark. "An Introduction to Evaluating Biometric Systems." URL: http://www.dodcounterdrug.com/facialrecognition/DLs/Feret7.pdf (9 November 2003).

7. Wayman, Jim. "Biometric Authentication Technologies: Hype Meets The Test Results." URL: http://www.usenix.org/events/sec02/wayman.pdf (26 December 2003).

8. January 3, 2002. "Drawing a Blank: Tampa Police Records Reveal Poor Performance of Face-Recognition Technology." URL: http://archive.aclu.org/news/2001/n010302a.html (9 November 2003).

9. URL: http://www.ibgweb.com/reports/public/biometrics_standards.html (22 December 2003).

10. 9 December 2002. Special Project: "Impact of Information Technology on Security Systems." URL: http://www.ceet.niu.edu/faculty/vohra/tech497/present/securitysys.doc (22 December 2003.