Global Information Assurance Certification Paper

Biometric Technologies Overview

Author : Manoj Gupta

March 16, 2001

Purpose of this document

The objective of this document is to understand various biometric identification techniques and analyze them in terms of accuracy.

Audience

This document will be of help to Security administrators and Security solution designers to deploy the right Biometrics technology in their environment.

Scope of this document

The beauty of a biometrics trait is that it is as unique as the individual from whom it was created. Unlike a password or PIN, a biometric trait cannot be lost, stolen or recreated. This makes biometrics an obvious antidote to identify theft.

The various technologies in Biometrics are briefly described below:

Fingerprint Identification

Fingerprint identification is, perhaps, the oldest of the biometric sciences. Fingerprint comparisons, these days, is based on "minutiae", individual unique characteristics within the fingerprint pattern. With a typical fingerprint image obtained by a live scan device, there are an average of 30-40 minutiae. The Federal Bureau of Investigation (FBI) has shown that no two individuals can have more than 8 common minutiae.

Fingerprint technology is believed to have the greatest potential to produce the highest accuracy rate for identification purposes. Fingerprint images contain large amount of data. Because of the high level of data present in the image, it is possible to eliminate false matches and quickly reduce the number of possible matches to a small number, even with large database sizes. Because of the fact that Fingerprint Imaging Systems use more than one finger image in the match process, the match discrimination process is geometrically increased.

Fingerprint identification technology has undergone an extensive research and development effort over time and as a result today, in the criminal justice Automated Fingerprint Identification System (AFIS) has a 98%+ identification rate and the false positive identification rate is less than 1%.

Facial Recognition

Facial recognition is the most natural means of biometric identification; this method of distinguishing one individual from another is an inherent ability of virtually every human. However, until recently, facial recognition has never been treated as a "science" and has been largely subjective in nature.

Facial recognition technology has recently developed into two areas of study: facial metrics and eigenfaces.

Facial metrics technology relies on the measurement of specific facial features (e.g. the distance between the inside corners of the eyes, the distance between the outside corners of the eyes and the outside corners of the mouth, etc.) and the relationship between these measurements.

Within the past two years, an investigation has been made into categorizing faces according to the degree of fit with a set of "eigenfaces". It has been postulated that every face can be assigned a "degree of fit" to each of 150 eigenfaces; further, the template eigenfaces with the 40 highest "degree of fit" scores are necessary to reconstruct a face with over 99% accuracy. The difference between the eigenface method of facial categorization and the police artist method of building a face from template parts is that the eigenface method is based upon an actual photo of the individual and the "eigenface" information is derived from a computer based analysis of the digital image of the photo.

Eigenface technology has some promise, but it is a technique that is just in the infancy stage of development. Very little data regarding eigenface error rates (false, negative, false positive) exists currently.

Hand Geometry

Hand geometry is based on the fact that virtually every person's hand is shaped differently than another person's hand and that the shape of a person's hand (after a certain age) does not significantly change its shape. Various methods are used to measure the hand; these methods generally fall into one or two categories - mechanical or image-edge detection. Either method produces estimates of certain key measurements of the hand (length of fingers and thumb, widths etc.) this data is used to categorize a person.

Hand geometry, as compared to some other means of biometric identification, does not produce a large data set. Therefore, given a large number of records, hand geometry may not be able to distinguish one individual from another who has similar hand characteristics. As the size of the database grow, there must be an increase in the number of distinguishing characteristics of the biometric used in order to place the individual in order to place the individual into an increasingly narrow band of individuals who share similar biometric characteristics. With hand geometry, there is not enough data available, the individual is placed in a band within the database structure that contains many individuals.

Retinal Scan

Retinal Scan technology is based on the blood vessel pattern in the retina of the eye. An infrared light source is used to illuminate the retina of the eye: the infrared energy is absorbed faster by blood vessels in the retina than by surrounding tissue. The image of the enhanced blood vessel pattern of the retina is analyzed for characteristic points within pattern.

A retinal scan can produce almost the same volume of data as a fingerprint image analysis. Based on the fact that a high data volume equates to a high discrimination rate (identification rate), it would seem that retinal scan may be an alternative to fingerprint identification.

Retinal scan technology has several drawbacks that are not common to fingerprint imaging technology, like:
The retinal scan is more susceptible to disease (notably cataracts, etc) that can change the characteristics of the eye
The method of obtaining a retinal scan is personally invasive – a laser light (or other coherent light source) must be directed through the cornea of the eye
The method of obtaining a correct retinal scan depends heavily on the skill of the operator and the ability of the person being scanned to follow directions.

Iris Scan

Iris Scan technology is based on characteristics in the iris of the eye. A person must stand approximately 12-14 inches from a camera which frames-grabs an image of the iris for analysis. An iris scan produces a high data volume, which equates to a high discrimination rate (identification rate).

Iris scan technology may be more acceptable to user than retinal scans and as opposed to retinal scan, it does not use an infrared light source to highlight the biometric pattern in the iris.

Iris scan technology is not yet in production and is currently in prototype testing.

Vascular Patterns

Vascular pattern technology is very similar to Retinal Scan technology in that it used infrared light to produce an image of the vein pattern in the face, in the back of a hand, or on the wrist.

Vascular pattern technology is generally acceptable to users except that some users still object to any biometric method that uses infrared.

Signature Recognition

Signature recognition is based on the dynamics of making the signature, i.e., acceleration rates, directions, pressure, stroke length, etc., rather than a direct comparison of the signature after it has been written.

The problems with the signature recognition lie in the means of obtaining the measurements used in the recognition process and the repeatability of the signature. The instrumentation cannot consistently measure the dynamics of the signature. Also a person does not make a signature in a fixed manner; therefore the data obtained from any one signature from an individual has to allow for a range possibilities.

Signature recognition has the same problem with match discrimination (i.e., finding a match in a large database) as does hand geometry.

Voice Dynamics

Voice dynamics relies on the production of a " voice template" that is subsequently used to compare with a spoken phrase. A speaker must repeat a set phrase several times as the systems builds the template.

This biometrics technique relies on the behavior of the subject rather than the physical characteristics of the voice and is therefore, prone to inaccuracy.

The above mentioned biometric technologies can be evaluated on following parameters.

BIOMETRIC ACCURACY

Biometric accuracy is measured in two ways; the rate of false acceptance (an impostor is accepted as a match - Type 1 error) and the rate of false rejects (a legitimate match is denied - Type 2 error).

Every biometric technique has a different method of assigning a "score" to the biometric match; a "threshold value" is defined which determines when a match is declared. Scores above the threshold value are designated as a "Hit" and scores below the threshold are designated as "No-Hit." A Type 2 error occurs if a true match does not generate a score above the threshold. A Type 1 error is made when an impostor generates a match score above the threshold. If the Type 1 and Type 2 error rates are plotted as a function of threshold value, they will form curves which intersect at a given threshold value. The point of intersection (where Type 1 error equals Type 2 error) is called the crossover accuracy of the system. In general, the greater the value of the crossover accuracy, the greater the inherent accuracy of the biometric.

Biometric	**Crossover Accuracy**
Retinal Scan	1:10,000,000+
Iris Scan	1:131,000
Fingerprints	1:500
Hand Geometry	1:500
Signature Dynamics	1:50
Voice Dynamics	1:50
Facial Recognition	no data
Vascular Patterns	no data

Table -1

TYPES OF BIOMETRIC SEARCHES

Typically most systems use two types of biometric searches; CLOSED searches and OPEN searches. A CLOSED search will occur when the client claims to be already enrolled in the system; in this case, the client's biometric will be read and the biometric will be compared to the biometric data already on file for the client. An OPEN search will occur when the client

is (or claims to be) unknown to the system (i.e., not in the biometric database); in this case, the client's biometric will be searched against all biometric records in the database.

Of the two types of searches, the OPEN search is technically the most challenging and costly. OPEN search accuracy generally decreases as the size of the database increases; for this reason, biometric records must be categorized according to some broad characteristic within the biometric data. Records that fall into a like category are put into a fixed "partition" of the database. Subsequent searches for a particular record, or a record belonging to the given category, is searched within the small subset or partition of the total database. This technique lowers the relative size of the database per search and thereby increases the accuracy of the system.

In order to divide the biometric data into partitions, the per-record size of the biometric data must be considered. In general, the larger the per-record data size of the biometric, the easier it is to assign the biometric record to a particular partition within the database. Also, the database can be divided into a greater number of partitions as the per-record data size of the biometric grows larger (i.e., there are more possibilities for generating distinct partitions).

Biometric	Data Size Per Record (bytes)
Retinal Scan	35
Iris Scan	256
Fingerprints	512 - 1000
Hand Geometry	9

Table 2

DATA COLLECTION ERROR RATES

Data collection procedures differ according to the biometric used. Some biometric measurements are prone to error during the measurement while others produce consistent results from read to read.

Biometric collection procedures are listed as follows:

Retinal Scan - "The (Retinal Scan) reader contains an aperture where the user looks to align his eye with an optical target, which appears as a series of circles. As the user moves his eye around, the circles become more or less concentric. Proper alignment is achieved when the circles appear concentric and the user is looking at the contour of the circles." With the eye properly aligned with the reader device, an infrared light illuminates the retina (heating the blood vessels of the retina) and a camera captures an image of the infrared-enhanced blood vessel pattern.

Fingerprints - "The user places his or her finger on a small (flat) glass plate. The system captures a high-resolution optical image of the fingerprint, typically using a charge-coupled device (CCD) camera."

Data Collection Error Rate For:		
	Retinal Scan	Fingerprint
Test 1	3.41%	0.42%
Test 2	18.28%	6.01%
Test 3	9.16%	1.88%

Table 3

Conclusion

The choice of biometric technology deployment may depend on parameters like Accuracy, Search and Data Collection Error Rates, but limitations like cultural nuances cannot be omitted. The choice may further depend on the facts like Cost, Business Interest and Technology maturity.

References

Orla O'Sullivan. "Biometrics comes to life".
http://www.banking.com/aba/cover_0197.htm (10th March 2001)

Thomas Ruggles. " COMPARISON OF BIOMETRIC TECHNIQUES". February 11, 2001
URL: http://biometric-consulting.com/bio.htm (12th March 2001)

Dr. Despina Polemi. " Review and evaluation of Biometric Techniques for Identification and Authentication - Final Report"". 3 May 1999
URL: http://www.cordis.lu/infosec/src/stud5fr.htm (18th March 2001)

Roger Clarke. "Human Identification in Information Systems" 16 August 1997
URL: http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID (15th March 2001)

Simon G. Davies. "Information Technology & People", Vol 7, No. 4 1994
URL: http://www.privacy.org/pi/reports/biometric.html (8th March 2001)

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS