Edmund Spinella
SANS GSEC
Original Submission
San Francisco, CA Dec 2002
28 May 2003

Biometric Scanning Technologies: Finger, Facial and Retinal Scanning

Abstract

This paper discusses several Biometric scan technologies: finger-scan, facial-scan and retinal-scan. We discuss the recent history of Biometrics and how it has been influenced by such pseudo-sciences as Phrenology, the study of human skull characteristics and Anthropometry, the study of human body measurement. We discuss how finger-scan technology was influenced by French and British police advancements in the nineteenth century and still remain the most widely used Biometric technology today. Facial-scan technology is beset with privacy concerns especially when this technology is applied to unsuspecting crowds. Retinal-scan technology, is a relatively new entrant to the biometric field and offers significant promise. One of the continuing challenges for the biometric industry is to define the environment in which the technology provides the strongest benefit to individuals and institutions. For the security officer, the challenge will be to demonstrate to upper management that the costs associated with deployment outweigh the risks and costs.

Biometics: Recent History

The word “biometrics” comes from the Greek language and is derived from the words bio (life) and metric (to measure). This paper will refer to biometrics as the technologies used to measure and analyze personal characteristics, both physiological and behavioral. These characteristics include fingerprints, voice patterns, hand measurements, irises and others, all used to identify human characteristics and to verify identity. These biometrics or characteristics are tightly connected to an individual and cannot be forgotten, shared, stolen or easily hacked. These characteristics can uniquely identify a person, replacing or supplementing traditional security methods by providing two major improvements: personal biometrics cannot be easily stolen and an individual does not need to memorize passwords or codes. Since biometrics can better solve the problems of access control, fraud and theft, more and more organizations are considering biometrics a solution to their security problems. However, biometrics is not a panacea and has some hurdles to overcome before gaining widespread use. This paper will discuss the recent history of biometrics, benefits of biometrics over traditional authentication methods, some of the most widely used biometric technologies and the issues surrounding biometrics to include issues standing in the way of widespread biometric implementation.

The past development of two disciplines, Phrenology and Anthropometry, helped to pave the way for biometrics. Phrenology, the study of the structure of the skull to determine a person's character and mental capacity, was founded by Franz Joseph in early nineteenth century Germany. Gall believed that certain mental characteristics could be aligned with certain cranial shapes and features. This concept was further advanced by an Italian physician named Cesare Lombroso who linked the concepts of phrenology with specific regard to criminal behavior, trying to relate behavior patterns with physical and biological characteristics.[1] Although long considered a pseudoscience lacking real scientific merit, Phrenology remained popular, especially in the United States, throughout the 19th century and still has advocates today [2]. Alponse Bertillon, a late nineteenth French police Captain, advanced the idea of Anthropometrics, the study of human body measurement for use in anthropological classification and comparison. A pseudoscience like Phrenology, it was used mainly to classify potential criminals by facial characteristics. For example, Cesare Lombroso's *Criminal Anthropology* (1895) claimed that murderers have prominent jaws and pickpockets have long hands and scanty beards.[3] Bertillon developed a system of identifying criminals by multiple anatomical measurements, which was widely used in France at the time and named after him (Bertillonage)[4]. His system was used by police authorities throughout the world, but then faded when it was discovered that some people shared the same measurements and based on the measurements alone, could be treated as one.[5]

While developments in Phrenology and Anthropometry took place, interest was increasing in the areas of finger and hand geometry. In 1823, the Czech

Jan Evangelista Purkinje was studying sweat glands in the hand and realized the grooves and depressions that these sweat glands opened up into seemed to be unique to each individual.[6] An extremely reliable method of categorizing and identifying marks in fingerprints was developed by Richard Edward Henry of Scotland yard in the late nineteenth century. Henry made advancements on a fingerprinting method first brought forward by Francis Galton in 1892, and conducted experimental tests in the 1890's. In the early twentieth century, mainly due to the negative publicity from the Bertillionage failure in 1903, finger printing became the method of choice for police around the world. Today, fingerprinting is the biometric method most people associate when speaking of biometrics and will be discussed next.

Finger-Scan Technology

Fingerprinting or finger-scanning technologies is the oldest of the biometric sciences and utilizes distinctive features of the fingerprint to identify or verify the identity of individuals. Finger-scan technology is the most commonly deployed biometric technology, used in a broad range of physical access and logical access applications.[7] All fingerprints have unique characteristics and patterns. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. It is through the pattern of these ridges and valleys that a unique fingerprint is matched for verification and authorization.[8] These unique fingerprint traits are termed "minutiae" and comparisons are made based on these traits. On average, a typical live scan produces 40 "minutiae". The Federal Bureau of Investigation (FBI) has reported that no more than 8 common minutiae can be shared by two individuals.[9]

There are five stages involved in finger-scan verification and identification: fingerprint image acquisition, image processing, location of distinctive characteristics, template creation and template matching. A scanner takes a mathematical snapshot of a user's unique biological traits. This snapshot is saved in a fingerprint database as a minutiae file. The first challenge facing a finger-scanning system is to acquire high-quality image of a fingerprint. Image quality is measured in dots per inch (DPI) – more dots per inch means a higher-resolution image. Lower DPI found on the market are in the 300-350 DPI, but the standard for forensic-quality fingerprinting is images of 500 DPI.[10] Image acquisition can be a major challenge for finger-scan developers, since the quality of print differs from person to person and from finger to finger. Some populations are more likely than others to have faint or difficult-to-acquire fingerprints, whether due to wear or tear or physiological traits.[11] Taking an image in the cold weather can have an affect also. Oils in the finger help produce a better print. In cold weather, these oils naturally dry up. Pressing harder on the platen (the surface on which the finger is placed, also known as a scanner) can help in this case.

Image processing is the process of converting the finger image into a usable format. This results in a series of thick black ridges (the raised part of the fingerprint) contrasted to white valleys.[12] At this stage, image features are detected and enhanced for verification against the stored minutia file. Image enhancement is used to reduce any distortion of the fingerprint caused by dirt, cuts, scars, sweat and dry skin.[13] The next stage in the fingerprint process is to locate distinctive characteristics. There is a good deal of information on the average fingerprint and this information tends to remain stable throughout ones life. Fingerprint ridges and valleys form distinctive patterns, such as swirls, loops, and arches. Most fingerprints have a core, a central point around which swirls, loops, or arches are curved. These ridges and valleys are characterized by irregularities known as minutiae, the distinctive feature upon which finger-scanning technologies are based.[14] Many types of minutiae exits, a common one being ridge endings and bifurcation, which is the point at which one ridge divides into two. A typical finger-scan may produce between 15 and 20 minutiae. A template is then created. This is accomplished by mapping minutiae and filtering out distortions and false minutiae. For example, anomalies caused by scars, sweat, or dirt can appear as minutiae.[15] False minutiae must be filtered out before a template is created and is supported differently with vendor specific proprietary algorithms. The tricky part is comparing an enrollment template to a verification template. Positions of a minutia point may change by a few pixels, some minutiae will differ from the enrollment template, and false minutiae may be seen as real. [16] Many finger-scan systems use a smaller portion of the scanned image for matching purposes. One benefit of reducing the comparison area is that there is less chance of false minutiae information, which would confuse the matching process and create errors.[17] Most finger-scan technologies are based on minutiae. Samir Nanavati, author of Biometrics, Identity Verification in a Networked World states that 80 percent of finger-scan technologies are based on minutiae matching but that pattern matching is a leading alternative. This technology bases its feature extraction and template generation on a series of ridges, as opposed to discrete points. The use of multiple ridges reduces dependence on minutiae points, which tend to be affected by wear and tear.[18] The downside of pattern matching is the it is more sensitive to the placement of the finger during verification and the created template is several times larger in byte size—approximately 1,000 bytes versus 250 to 500 bytes.

Before we leave finger-scanning, lets discuss some of the advantages and disadvantages of this biometric technology. Finger-scans continue to be the primary means used by law enforcement agencies for positive identification and are used in the commercial and government sectors with a good deal of success. Finger-scan technology is proven and capable of high levels of accuracy. There is a long history of fingerprint identification, classification and analysis. This along with the distinctive features of fingerprints has set the finger-scan apart from other biometric technologies. There are physiological characteristics more distinctive than the fingerprint (the iris and retina, for example) but automated identification technology capable of leveraging these characteristics has been developed only over the past few years. [19] The technology has grown smaller, more capable and with many solutions available. Devices slightly thicker than a coin and an inch square in size are able to capture and process images. Additionally, some may see the large number of finger-scan solutions available today as a disadvantage, many see it as an advantage by ensuring marketplace competition which has resulted in a number of robust solutions for desktop, laptop, physical access, and point-of-sale environments.[20] Another advantage of finger-scan technology is accuracy. Identical matches are nearly impossible since fingerprints contain a large amount of information making it unlikely that two fingerprints would be identical. Even with large databases, it is possible to eliminate false matches and quickly reduce the number of possible matches to a small number because of the high level of data present. Because of the fact that some Fingerprint Imaging Systems use more than one finger image in the match process, the match discrimination process is geometrically increased.[21] Fingerprint technology has another advantage offered by technology; the size of the memory required to store the biometric template is fairly small.

There are some weaknesses to finger-scanning, most of which can be mitigated. There is a fraction of the population that is unable to be enrolled. There are certain ethnic groups that have lower quality fingerprints than the general populations. Testing has shown that elderly populations, manual laborers, and some Asian populations are more difficult to be enrolled in some finger-scanning systems.[22] Another problem is that over time, sometimes in as short a period as few months, the fingerprint characteristics of an individual can change, making identification and verification difficult. This problem is seen with manual workers who work extensively with their hands. There are also privacy issues attached to finger-scanning technologies. Some fear that finger-scans may be used to track a person's activities. Others fear that data collected may be improperly used for forensic purposes.

Finger-scan technology is deployed throughout the world and provides a capable solution. More commonly seen these days are computer network access and entry devices for building door locks utilizing fingerprint scanning technology. Fingerprint readers are being used by banks for ATM authorization and are becoming more common at grocery stores where they are utilized to automatically recognize a registered customer and bill their credit card or debit account. Finger-scanning technology is being used in a novel way at a middle school in Pennsylvania where some cafeteria purchases are supported by a federal subsidized meal program in which students receive federally subsidized meals and retain the ability to remain anonymous. Paying with a government meal card at checkout instead of with cash would identify the student as a program recipient. The solution was for the school to provide students the option of using a finger-scan peripheral to purchase meals. At the end of each month, a bill is sent to their parents for payment or to the free food program for reconciliation. This use of a finger-scan ensures that there is no way to determine whether their parents or government grants are paying for their meals.[22]

Facial-Scan Technology

Another biometric scan technology is facial recognition. This technology is considered a natural means of biometric identification since the ability to distinguish among individual appearances is possessed by humans. Facial-scan systems can range from software-only solutions that process images processed through existing closed-circuit television cameras to full fledged acquisition and processing systems, including cameras, workstations, and back-end processors.[23] With facial recognition technology, a digital video camera image is used to analyze facial characteristics such as the distance between eyes, mouth or nose. These measurements are stored in a database and used to compare with a subject standing before a camera.[24] Facial recognition systems are usually divided into two primary groups. First there is what is referred to as the 'controlled scene' group whereby the subject being tested is located in a known environment with a minimal amount of scene variation. In this case, a user might face the camera, standing about two feet from it. The system locates the user's face and perform matches against the claimed identity or the facial database. It is possible that the user may need to move and reattempt the verification based on his facial position. The system usually comes to a decision in less than 5 seconds. [25] The other group is known as the "random scene" group where the subject to be tested might appear anywhere within the camera scene. This situation might be encountered within a system attempting to identify the presence of an individual within a group or crowd. [26] This situation was evidenced since 11 Sept when security personnel stated that facial scan recognition technology would be used at a Super bowl game.

Facial-scan technology is based on the standard biometric sequence of image acquisition, image processing, distinctive characteristic location, template creation, and matching.[27] An optimal image is captured through a high-resolution camera, with moderate lighting and users directly facing a camera. The enrollment images define the facial characteristics to be used in all future verifications, thus a high-quality enrollment is essential.[28] Challenges that occur in the image acquisition process include distance from user, angled acquisition and lighting. Distance from the camera reduces facial size and thus image resolution. Users not looking directly at the camera, positioned more than 15 degrees either vertically or horizontally away from ideal positioning are less likely to have images acquired. [29] Lighting conditions, which cause an image to be underexposed or underexposed, can cause challenges. Additionally, users with a darker skin tone can be difficult to acquire. Select Hispanic, black and Asian individuals can be more difficult to enroll and verify in some facial-scan systems because acquisition devices are not always optimized to acquire darker faces.[30] After the issues with image acquisition are worked out, the process of image processing takes place. Color images are normally reduced to a black and white and images cropped to emphasize facial characteristics. Images are normalized to account for orientation and distance. Images can be enlarged or reoriented as long as a point between the eyes serves as a point of reference. The processes of characteristic location can then take place. There are several matching methods available for facial scans which attempt to match visible facial features in a fashion similar to the way people recognize one another. Areas of the face not apt to change over time such as sides of the mouth, nose shape and areas around the cheekbones, distinctive characteristics most often used in image matching. Areas likely to change over time, such as ones hairlines are not normally used for verification.

Facial-scan technology has its advantages and disadvantages. One major advantage is that facial-scan technology is the only biometric capable of identification at a distance without subject complicity or awareness. [31] This allows police to install facial-scan technology in public places to survey crowds and for security to accomplish the same at a casino house. This capability also quiets those who express concern about a biometric that physically touches them or about touching a device that others may have had contact with. Another advantage of facial-scan technology is the fact that static images can be used to enroll a subject. This can shorten the time to enroll a target population compared to an automated Fingerprint Identification system (AFIS), which can take years to accomplish. The disadvantages include acquisition environment and facial characteristic changes that effect matching accuracy and the potential for privacy abuse. Images are most accurate when taken facing the acquisition camera and not sharp angles. The users face must be lit evenly, preferably from the front.[32] Changes in hairstyle, makeup or the wearing of a hat or sunglasses may pose a problem during the verification process. Facial-scanning technology has a poor record in verifying a subject who has had plastic surgery to alter their appearance. The fact that a biometric facial scan can take place without the knowledge or consent of a subject, raises privacy concerns among many. Two facial-scan deployments in Florida have met with public objections: one aimed to prevent crime in a shopping district and one aimed to catch criminals at the 2001 Super Bowl. [33] Facial-scan technologies have unique advantages over all other biometrics in the areas of surveilling large groups and the ability to use pre-existing static images. Its disadvantages include the falsely non-matching folks when subject appearances change during verification. For implementations where the biometric system must verify users reliably over time, facial-scan can be a very difficult technology to implement successfully.

Retinal-Scan Technology

The last biometric technology to discuss is retinal scanning. Retina-scan technology makes use of the retina, which is the surface on the back of the eye that processes light entering through the pupil. Retinal Scan technology is based on the blood vessel pattern in the retina of the eye. The principle behind the technology is that the blood vessels at the retina provide a unique pattern, which may be used as a tamper-proof personal identifier.[34] Since infrared energy is absorbed faster by blood vessels in the retina than by surrounding tissue, it is used to illuminate the eye retina. Analysis of the enhanced retinal blood vessel image then takes place to find characteristic patterns. Retina-scan devices are used exclusively for physical access applications and are usually used in environments that require high degrees of security such as high-level government military needs. [35] Retina-scan technology was developed in the 1980's, is well known but probably the least deployed of all the biometric technologies. Additionally, retina-scan technology is still in a prototype development stage and still commercially unavailable.

Retina-scan technology image acquisition is difficult in that the retina is small and embedded, requiring specific hardware and software. The user positions his eye close to the unit's embedded lens, with the eye socket resting on the sight. In order for a retinal image to be acquired, the user must gaze directly into the lens and remain still, movement defeats the acquisition process requiring another attempt.[36] A low intensity light source is utilized in order to scan the vascular pattern at the retina. This involves a 360 degree circular scan of the area taking over 400 readings in order to establish the blood vessel pattern. This is then reduced to 192 reference points before being distilled into a digitized 96 byte template and stored in memory for subsequent verification purposes.[37] Normally it takes 3 to 5 acceptable images to ensure enrollment. Because of this, the enrollments process can be lengthy. Enrollments can take over 1 minute with some users not being able to be enrolled at all. It seems the more that a user is acclimated to the process, the faster the enrollment process works. After image acquisition, software is used to compile unique features of the retinal blood vessels into a template.

Retina-scan technology possesses robust matching capabilities and is usually configured to do one-to-many identification against a database of users, however, this technology requires a high quality image and will not enroll a user unless a good image is acquired. For this reason, there is a moderately high false reject rate due to the inability to provide adequate data to generate a match template. [38]

Retina-scan technology has its advantages and disadvantages. Among its advantages are its resistance to false matching or false positives and the fact that the pupil, like the fingerprint remains a stable physiological trait throughout ones life. The retina is located deep within ones eyes and is highly unlikely to be altered by any environmental or temporal condition.[39] Its resistance to false matching is due to the fact that retinal scans produce patterns that have highly distinctive characteristics, sufficient to enable identification. Well-trained users find retina scan capable of reliable identification. Like fingerprints, retina traits remain stable throughout life.

Disadvantages include the fact that the technology is difficult to use, users claim discomfort with eye-related technology in general and the fact that retina-scan technology has limited uses. Enrollments require prolonged concentration requiring a well-trained and motivated user. Retina-scan enrollments take longer than both iris-scan and fingerprinting. Users claim discomfort with the fact that they must position their eye very close to the device. Users commonly fear that the device itself or the light inside the device can harm their eyes in some way.[40] Many also feel that this retina scans are invasive in that the inability to use the retina can be linked to eye disease. Retina scan has limited uses normally deployed in high security, low volume physical access situations in which inconveniencing users is an acceptable cost of heightened security.[41] Retina-scan technology is not apt to become a widely deployed technology any time soon. Other biometrics can provide most if not all the benefits of this technology without the problems. But never discount technology and its advances over time. If future technology allows for retina scanning being easier to use and allow users to enroll from a greater distance from the imaging device, its future will be bright.

Conclusion

In summary, Biometrics allow for increased security, convenience and accountability while detecting and deterring fraud. Biometrics, however, are not suitable for every application and is some situations biometric identification may be the wrong solution. One of the continuing challenges for the biometric industry is to define the environment in which the technology provides the strongest benefit to individuals and institutions. For the security officer, the challenge will be to demonstrate to upper management that the costs associated with deployment outweigh the risks and costs.

Footnote References

[1] Julian Ashbourn. (2002), Biometrics: Advanced Identity Verification, London: Springer-Verlag, p. 5.

[2] Robert Todd Carroll, The Skeptics Dictionary:Phrenology, http://skepdic.com/phren.html.

[3] Robert Todd Carroll, The Skeptics Dictionary:Anthropometry, http://skepdic.com/anthropo.html.

[4] Julian Ashbourn. (2002), Biometrics: Advanced Identity Verification, London: Springer-Verlag, p. 5.

[5] Robert Todd Carroll, The Skeptics Dictionary:Anthropometry, http://skepdic.com/anthropo.html.

[6] Julian Ashbourn. (2002), Biometrics: Advanced Identity Verification, London: Springer-Verlag, p. 5.

[7] Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc.

[10] Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 48.

[11] Ibid. p. 50

[12] Ibid. p. 51.

[13] Zeena Marchant, Biometrics: Fingerprint Authentication, SANS Reading Room, http://rr.sans.org/authentic/fingerprint.php

[14] Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 51.

[15] Ibid. p. 52.

[16] Ibid. p. 53.

[17] Julian Ashbourn. (2002), Biometrics: Advanced Identity Verification, London: Springer-Verlag, p. 48.

[18] Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 56.

[19] Ibid. p. 58.

[20] Ibid. p. 59.

[21] Manoj Gupta, Biometric Technologies Overview, SANS Reading Room, http://rr.sans.org/authentic/biometric2.php

[22] Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 60.

[22] Ibid. p. 58.

[23] Ibid. p. 64.

[24] Manoj Gupta, Biometric Technologies Overview, SANS Reading Room, http://rr.sans.org/authentic/biometric2.php.

[25] Ibid.

[26] Julian Ashbourn. (2002), Biometrics: Advanced Identity Verification, London: Springer-Verlag, p. 56.

[27] Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 65.

[28] Ibid. p. 65.

[29] Ibid.

[30] Ibid. p. 66.

[31] Ibid. p. 73.

[32] Ibid. p. 74.

[33] Ibid. p. 75.

[34] Julian Ashbourn. (2002), Biometrics: Advanced Identity Verification, London: Springer-Verlag, p. 55.

[35] Samir Nanvati. (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc, page 106.

[36] Ibid. p. 108.

[37] Julian Ashbourn. (2002), Biometrics: Advanced Identity Verification, London: Springer-Verlag, p. 55.

[38] Ibid.

[39] Ibid. p. 111.

[40] Ibid. p. 112.

[41] Ibid.

Bibliography

1. Julian Ashbourn. (2002), Biometrics: Advanced Identity Verification, London: Springer-Verlag.

2. Robert Todd Carroll, The Skeptics Dictionary:Anthropometry, http://skepdic.com/anthropo.html.

3. Manoj Gupta, Biometric Technologies Overview, SANS Reading Room, http://rr.sans.org/authentic/biometric2.php.

4. Milteades Leonidou, (2002), Iris Recognition: Closer Than We Think? http://www.sans.org/rr/paper.php?id=143

5. Zeena Marchant, Biometrics: Fingerprint Authentication, SANS Reading Room, http://rr.sans.org/authentic/fingerprint.php

6. Ali Meraayan, (2001), Proximity Authentication, (2001), http://www.sans.org/rr/papers/6/102.pdf

7. Samir Nanvati, (2002), Biometrics: Identity Verification in a Networked World, New York: Wiley and Sons, Inc.

8. Wayne Penny, (2002), Biometrics, A Double-Edged Sword, http://www.sans.org/rr/paper.php?id=137