Solid-State Fingerprint Detection

An AuthenTec White Paper

INTRODUCTION

Acquisition is Everything

If instant fingerprint recognition is to become the widely-used and dependable tool for personal identification that it has promised to be, it must function properly (that is, transparently) for virtually everyone on the planet. This means that a useful system must acquire fingerprints at a level of reliability that is unprecedented. The situation demands near-perfect performance, and "success" is spelled a-c-q-u-i-s-i-t-i-o-n!

In other words, you've got to get an accurate image before anything else can happen. And if you can't acquire a usable fingerprint sample, it won't matter how sophisticated your application software is – you're not really in the personal identification business.

The world population offers a very broad range of finger and skin conditions. There are a wide variety of physical environments in which a fingerprint sensor must operate. Given these demanding conditions, successful implementation of a solution on this scale is not by any means a trivial problem.

Table of Contents

AuthenTec welcomes your input. We try to make our publications useful, interesting, and informative, and we hope you will take the time to help us improve them. Please send any comments or suggestions by mail or e-mail.

AuthenTec, Inc.
Post Office Box 2719
Melbourne, Florida 32902-2719
321-308-1300
www.authentec.com
apps@authentec.com

White Paper: Solid-State Fingerprint Detection
2065 Rev 1.1 (DRAFT)

ABSTRACT

A Comparison of Capacitive and Active Array Based
Human Fingerprint Readers

This paper addresses relative aspects of the two currently available all-solid-state technology solutions to the digital fingerprint identification problem. In the body of this report passing mention is made of some other approaches, and a very brief summary of the whole biometric technology set can be found in APPENDIX B: Biometric Technologies.

Fingerprint Acquisition

What is a FingerPrint?

The traction-producing skin of the palmar (hand) or plantar (foot) body surfaces, especially the fingertips, exhibit the familiar and characteristic ridges and valleys of the human fingerprint. Everyone has them, and their classification and identification are far and away the most widely-used of all of the various personal identification measurements, or “biometrics”. But the fingerprint that we can see by eye – that produces the detective’s “latent print” when we touch most surfaces, or that stamps the image when inked and pressed to paper, or that is detected when optically or capacitively scanned – is actually a structure composed mostly of dead epidermal skin.

The fingerprint is initially formed in the living subdermal tissue just below the visible outer layer. In a cycle of constant rejuvenation, the newly-formed skin cells, mostly *keratinocytes*, slowly migrate outward through five distinct epidermal regions[1], deteriorating as they go, yet retaining the unique anatomical patterns originally set in the live tissue. Arriving at the surface, they replace older cells, which are then worn away by friction or abrasion, or simply sloughed off as skin detritus in a process called *desquamation*. These new cells are discarded from the skin surface in their turn as they are replaced by yet newer cells from below.

In this way, the characteristic patterns of the epidermis are naturally and constantly renewed over time. Nevertheless, physiological processes such as dermatitis, disease, aging, and calluses can obscure them. They can be mechanically damaged – worn smooth, contaminated by dirt, etched by chemicals, or even burned or scarred – all without affecting the living cells beneath.

[1] The epidermis consists of a continuous mass of cells, usually differentiated into the following regions or *strata*: the **stratum corneum**, the uppermost layer, containing dry, dead cells, flattened to form a relatively continuous thin outer membrane skin that is highly *cornified* or *keratinized* (rendered horn-like); the **stratum lucidum**, the region where dying cells are located, which contain an oily substance that renders them translucent; the **stratum granulosum**, in which the cells contain large granules; the **stratum spinosum**, where the cells show marked spines or bridges between each other; the **stratum basale**, where the cells contain living basal cells called *keratinocytes* and *melanocytes*; and the lowest region, the **epidermal-dermal junction** (often called the basement membrane), which consists of a thin zone of ground substance, containing no fibers, lying between the basal cells and the dermal surface. – Adapted from Gray’s *Anatomy*, 38th edition. Williams, Peter L., et al. Churchill Livingston.

Fingerprints are anatomic features that are unique to the individual human. They are "phenotypic" (that is, produced by interaction with the environment – in this case *in utero*), not "genotypic" (meaning gene-coded). In other words, their conformation is not genetically determined. For this reason, even monozygotic (identical) twins, despite sharing a full set of genotypic characteristics such as gender, blood group, and DNA sequences, have fingerprints that differ from one another in the same degree that they differ from any other unrelated individuals.[2] Furthermore, there is no apparent correlation between the fingerprint configurations of ridge and valley, and the race or gender of their bearer. The fingerprint does not say anything general about its bearer, but it speaks quite clearly to specific identification.

Background

A very long time in the past, in fact more than two thousand years ago, the people of both India and China knew of the unique nature of fingerprints. They used finger impressions taken on wax (and sometimes clay) seals or tablets to identify individuals. With this method, merchants could validate the provenance, nature, or quality of their goods. Government agents could ensure the validity of official communications. By careful comparison it could be determined whether or not two fingerprint impressions matched and so verify their source. However, there was no codified system to this matching – they simply relied on the expert eye of the user. Such a fingerprint impression was often called a "chop", from the Hindi word *chap*, meaning "stamp".

The first generation of modern fingerprint acquisition technology was, of course, ink on paper. As we have seen, fingerprinting as an identification technology dates from antiquity, but modern, sophisticated methods have been with us as a science for little more than a century. In his seminal work *Finger Prints* (1892) Galton[3] defined the unique anatomical features called *minutiae* and generally described the rule-based method of fingerprint identification that remains in use today.

Throughout the world, considerable engineering effort has been expended over the last several decades to produce a small variety of skin-surface-oriented technologies for reading real-time (also called "live scan") fingerprint patterns.

[2] Daugman, John, "Biometric Decision Landscapes" 1999 University of Cambridge, UK.
[3] Galton, Sir Frances (1822-1911) British anthropologist and statistician; cousin to Charles Darwin; "the father of modern fingerprinting".

The fingerprint acquisition technologies that are currently important, and their relative generational positions are listed in the following table:

Table 1 – Fingerprint Acquisition Technologies

GENERATION	ACQUISITION TECHNOLOGY
Pre-technology	Impression on wax or clay token.
First	Ink-on-paper.
Second	General document scanning. Dedicated optical fingerprint scanning.
Third	Solid-state Capacitive Sensing. Direct Thermal-Optical Scanning. LCD Thermal-Optical Scanning.
Fourth	Solid-state Active Array Sensing.

The Acquisition Challenge

After more than 100 years, **ink-on-paper** is still by far the most widely used acquisition technology. Without considering the rest of the world's government agencies, the U.S. Federal Bureau of Investigation (FBI) alone has about 200 million fingerprint cards in its files, while continuing to collect 30 to 50 thousand more PER DAY![4] The resulting avalanche of paper artifacts can be evaluated by expert human analysts or digitized using any of a number of widely available general-purpose **document** scanners to create a searchable database. Further processing of the resulting digital images by sophisticated recognition software can greatly reduce the size of the database (the FBI is faced with a 200-terabyte storage problem) and render manageable the search and identification tasks. The ongoing trend is to bypass the tedious, time-consuming, and inaccurate mechanical front end of the process through the use of automated fingerprint capture devices.

Dedicated **optical** scanners, being inexpensive, currently dominate the live scan fingerprint market. Such units have substantial drawbacks, including relatively low durability. They are also rather large and cumbersome (the several-inch focal length of the optics is not easily reduced, even with (optically "noisy") Fresnel lenses) and so are not readily incorporated in the design of such size-sensitive equipment as consumer electronics (portable computers, cell phones, and the like). **Solid-state capacitive**, **thermal**, and **thermal-optical** sensors can be made small and robust

[4] Brislawn, Christopher; "Image Coding Standard" 1996 Federal Bureau of Investigation, USA.

enough, but share with optical scanning many of the same inherent performance limitations.

As indicated in the foregoing reference to the FBI, automated fingerprint identification has historically received a great deal of interest from the law enforcement sector. The existing technologies are often able to acquire useful fingerprint images from most of the criminal population (composed as it is almost entirely of youthful males). Nevertheless, all of these devices mentioned above suffer from a key weakness – they are limited in their ability to acquire usable fingerprint pattern data from substantial other segments of the population.

They often cannot acquire useful data from people with epidermal variances from the norm, such as skin that is dry, thickly callused, or worn smooth by mechanical abrasion or chemical agents. These devices are also ineffective in situations where finger traction surfaces are contaminated with dirt, oil, or other substances; or which exhibit contact dermatitis from exposure to chemicals, or are damaged by other environmental factors. The reduction of skin tone and elasticity because of collagen loss in the aging process also contributes to a general deterioration of the skin, adding to the difficulties of getting a good image at a resolution sufficient to enable reliable acquisition. Finally, several classes of people, notably children and small women, present acquisition problems simple due to the small physical size of the finger.

The simple fact is that a significant portion of the population does not have “normal” skin – even among office workers.

Active Array Sensing[5] is a fourth-generation solution to these many problems. It bypasses most of the difficulties and drawbacks of previous approaches by perceiving certain physiological characteristics of the subdermal layer of the skin. This technology actually “looks” under the outer surface to the living layer beneath where the fingerprint actually originates.

The Capacitive Sensor

Capacitive Sensing is a physical biometric technology for fingerprint acquisition which detects very small variations in skin surface capacitance as measured by a solid-state array of charged capacitor plates that transduces capacitance measurements into a gray-scaled bit map image.

Operation

The typical capacitance-measuring fingerprint sensor is an integrated circuit (IC) featuring an externally-accessible portion of the substrate called the detection area or platen, which receives the fingerprint contact. This platen is formed by a matrix of discrete conductor elements (sensor plates). Each element is a capacitor plate, the dielectric for which is the air gap formed by the ridges and valleys of the fingerprint. Depending on the “pitch” (the distance between centers) of the plates, such an array may have many thousands of elements in the detection area. Figure 1 below illustrates this configuration.

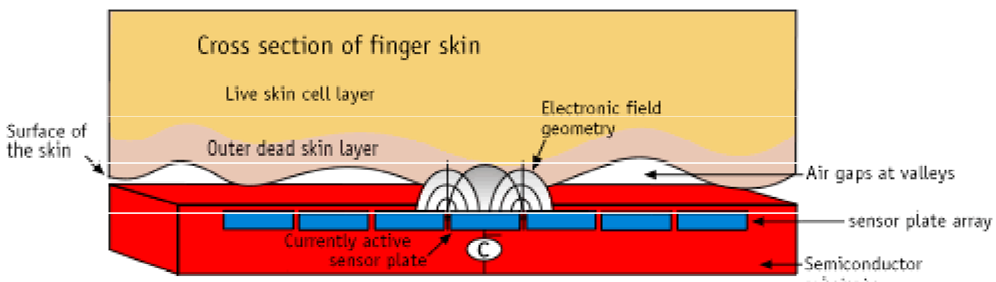
[5] Active Array Sensing is a trademark of AuthenTec, Inc.

When a fingerprint is presented on the platen, each sensor plate (which has received a known, fixed charge) interacts with its adjacent neighbors to produce a delta in the fixed charge that is expressed as a capacitance measurement. This value is interpreted as the gray-scale value of a bitmap image picture element (pixel) at that location.

The patterns generated by this structure are shown in the following illustration. The capacitive flux lines originate from an energized sensor plate and interact with the skin surface in closest proximity to the plate, terminating on adjacent sensor plates, or on the substrate of the integrated circuit.

Depending on the dielectric qualities of the tiny air gaps formed by the ridges and valleys of the fingerprint (influenced by the epidermal skin of the friction surface) the charge intensity will vary from plate to plate, and therefore from pixel to pixel in the resulting image.

Figure 1 - Capacitive Fingerprint Sensing



Discussion

A serious weakness in the capacitance-measurement approach to fingerprint imaging lies in the spherical field geometries that are generated around each sensor plate when energized. In a field of this shape the output of each element overlaps the sensing areas of its neighbors. This overlap can considerably exceed the size of the sensor plate, resulting in considerable cross-talk between adjacent or nearby plates. This phenomenon can reduce the device's real imaging resolution to about half the theoretical resolution of its actual matrix density.

A variation on the basic design uses two plates per sensor element to improve the spatial resolution and reduce cross-talk. This design limits the size of each sensing region by adding a second conductive plate to each element's sensing mechanism. Electronic circuitry, such as an operational amplifier feedback loop, measures the capacitance between the two plates while minimizing the effects of spurious capacitance between the sensing plates and their environment.

In both of the capacitive designs described here, the depth of penetration of the sensing field beyond the platen surface is very shallow. So much so, in fact, that those capacitance-sensing devices actually differentiate ridges from valleys by detecting the difference in the dielectric coefficient between the air gap in the valleys and the dead skin on the surface of the ridges.

For fingers that are clean, healthy, and above all, young, this approach can work adequately, but problems arise when less than optimal surface skin conditions occur. When the finger is dirty or worn, there is often little or no remaining air gap at all. When the finger surface is very dry, the difference in the dielectric qualities of the air gap and the skin itself is significantly reduced. In elderly people (as a class, the most difficult acquisition target), the typical loss of dermal collagen due to normal aging processes causes the skin to become flaccid and inelastic. Under these conditions, normal finger contact pressure on the reception surface readily flattens the surface ridges and valleys.

All this translates into an unpredictable and often inadequate ability to acquire useful fingerprint images, thus limiting the sensor's applications. At its very best, capacitive sensing cannot normally be expected to yield fingerprint recognition rates that are acceptable for high-volume commercial situations involving the general population. In some studies tests have shown that "failure-to-acquire" rates for this technology, that is, the rate at which candidate fingers cannot be enrolled at all, have been higher than 20% for "normal" skin conditions, and as high as 90% in certain specialized cases (see Appendix A:- An Acquisition Comparison Test).

This is not a very impressive or useful performance in the fault-intolerant world of commercial personal identification.

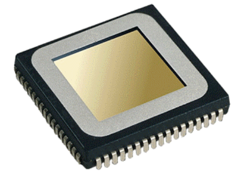
The Active Array Sensor

Active Array Sensing is a new technology. It was first introduced in May, 1997 by AuthenTec, Inc. of Melbourne, Florida, U.S.A. with its AF-S1 "FingerLoc[6]" integrated circuit. It is a physical biometric method for fingerprint acquisition, which detects very small changes in the parameters of transmitted signals, as the signals are modulated by interaction with the subdermal layer of the skin. The modulated signals are received by a solid-state antenna array that transduces the signal variations into a gray-scaled bit map image of the fingerprint.

Operation

The sensorium of an Active Array fingerprint-imaging device is comprised of a **drive ring** (an extremely short-range transmitter) and a **sensor matrix** (an active antenna array of thousands of elements, that receives the transmitted signal).
This illustration shows a standard implementation of this technology, a CMOS integrated circuit in the form of a standard JEDEC[7] 68-pin Plastic Leaded Chip Carrier (PLCC) package. The central rectangular area is the *sensor matrix*. The light-colored annular band is the *drive ring*. Altogether, the IC is only about the size of a postage stamp.

[6] FingerLoc is a trademark of AuthenTec, Inc.
[7] The JEDEC Solid State Technology Association, formerly the Joint Electronic Device Engineering Council, is the semiconductor engineering standardization body of the Electronic Industries Alliance (EIA).

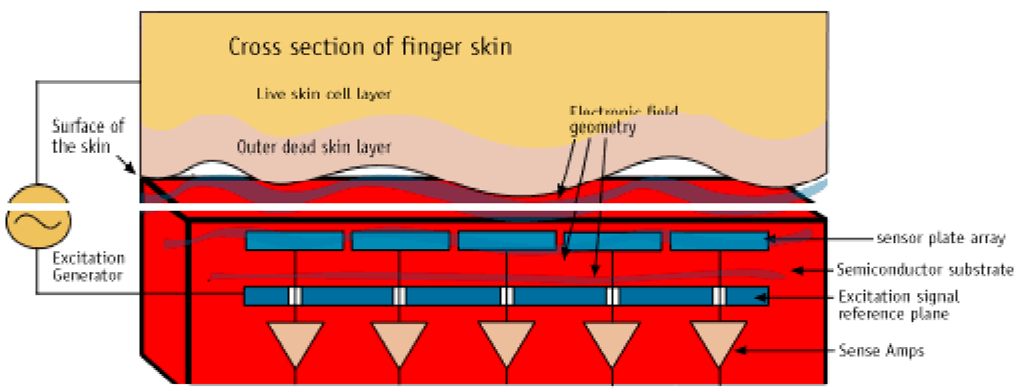


When a finger is placed on the platen of the sensor it makes physical contact with both the sensor matrix and the drive ring. The drive-ring couples a small signal onto the living subdermal layer of the finger. The signal on the live skin generates a quasi-static-electric field between the finger and a ground plane buried beneath the antenna array, under the surface of the integrated circuit.

The planar field geometries thus generated replicate the shapes of the ridges and valleys of the underlying live layer. The shape of this planar field structure is in marked contrast to the spherical geometries generated by simple capacitive sensors.

Each of the thousands of elements in the sensor matrix antenna array can generate a gray-scale dot and so can be thought of as a **pixel** in a **bitmap**. The signal from each element is read using an "under pixel" amplifier, then conditioned to a digital representation. The result is an accurate, undistorted digital image of the fingerprint.

Figure 2 - Active Array Sensing



Discussion

- Focused field
- Depth of penetration
- High Input impedance sensors
- Flexibility and adjustability
- Frequency and phase angle

- Complex skin impedance measurements

Active Array Sensing is a technology that lends itself very well to image acquisition improvement.

In the AuthenTec FingerLoc IC, the present imaging density (usually expressed as "dpi" or dots-per-inch) approximates the general capability of the marketplace.

The imaging matrix of the FingerLoc AF-S*x* fingerprint sensors is 250 physical pixels per inch. Because crosstalk between individual picture elements is extremely limited, a true 250 dot per inch (dpi) information content results.

More is not used simply because, with TruePrint Technology, the increased density is not necessary to accurately acquire fingerprint ridge and valley patterns. Some competing devices use 500 physical pixels per inch, but there is so much crosstalk between the sensing elements that the resulting images contain information that is even less than 250 dots per inch. In other words, the extra pixels add no new information, just digital noise and other unwanted artifacts.

Underscoring this observation is that most of the matching algorithms used in real-time fingerprint identification systems, when presented with a 500 dpi image, will down-sample the image to 250 dpi or less before processing. In other words they throw out three out of every four pixels in a 500 dpi image and process the resulting 250 dpi image.

This density yields sufficient resolution to reliably acquire the fingerprints of people that are about six years old or older. The fingerprints of younger children sometimes have ridges that are too delicate for this resolution. The Company anticipates that future versions of the sensor array will exhibit increased element densities suitable for the resolution and capture of features as small as skin pores. This will add a powerful tool to the present ability to detect and evaluate fingerprint data.

In addition, several rectangular variations on the present square format of the sensor array have been proposed and are currently under evaluation. Should these shapes become available, it will add breadth and flexibility to the mechanical design possibilities that can be served.

As discussed in the previous section, AuthenTec Active Array sensors operate on a technological principle that differs in a marked and fundamental way from the methods of various competitors. As a result, many types of fingers that are difficult or impossible to image adequately using optical or capacitive sensors (as discussed in a foregoing section of this report, <u>The Acquisition Challenge</u>), can be successfully acquired by Active Array Sensing.

For tabular data showing the performance of Active Array sensing technology versus several competitors, see <u>APPENDIX A: An Acquisition Comparison Test</u>.

This innovative technology has other important advantages as well:

- The nature of the penetrating linear flux fields permit Active Array devices to use a much thicker protective coating on their exposed substrate, without consequent loss of sensitivity, than is possible with capacitive sensors. The proprietary coating on the sensor matrix of the AuthenTec AF-S*x* family of integrated circuits is several times the thickness of that found in competing devices.

The coating material is considerably harder than glass, and during its development has passed a rigid series of abrasion and impact tests. Ongoing engineering effort in this important area continues, in an effort to improve still more the durability of the FingerLoc sensors.

- The Active Array sensing mechanism is very adaptable by nature and design. The sensor's operating points and parameters (such as operating frequencies, gain, phase shift, etc.) can be dynamically varied in real-time, to optimize detection of various types of fingerprint features and to reject noise and undesired artifacts.

  These adaptive features are referred to as Dynamic Optimization , an inherent software component of AuthenTec's TruePrint[8] Technology Suite.

[8] TruePrint is a trademark of AuthenTec, Inc.

APPENDIX A: An Acquisition Comparison Test

A test of acquisition rates between various fingerprint-sensing devices was conducted. An AuthenTec AF-S1 Sensor IC in a FingerLoc Module was compared to three competitive devices. Two of the competing devices used optical technology and one was capacitive. The following table shows the result of this test.

In the table, the fractions indicate the number of fingers successfully enrolled and verified for each device versus the number of fingers attempted for each skin condition. For example, "1/10" indicates one successful enrollment or verification was achieved in ten fingers tried. **Blue text** indicates the best performance for a test set and **red text** indicates the worst of the set.

In this test, up to three attempts were permitted for in each finger state versus the target acquisition technology. An important aspect of this test is that all initial enrollment failures were included with verification failures - most comparisons of this kind do not include enrollment discrepancies", but consider only verification performance after successful enrollment.

Table 2 – Technology Comparison

	Acquisition Technology			
Skin Condition or State	**Active Array**	**Optical 1**	**Optical 2**	**Capacitive**
Normal	12/12	12/12	10/12	9/12
Dry	10/10	10/10	8/10	8/10
Sweaty	10/10	8/10	8/10	3/10
Callused	12/12	12/12	10/12	11/12
Elderly	9/10	3/10	8/10	1/10
Worn Smooth	10/10	8/10	9/10	7/10
Totals	**63/64**	**53/64**	**51/64**	**39/64**
Acquired	**98%**	**83%**	**80%**	**61%**

APPENDIX B: Biometric Technologies

This section offers very brief definitions of the various biometric technologies currently in use. This material is for information only, and is not intended to be exhaustive or even authoritative.

Fingerprint Identification

Active Array Sensing

Active Array Sensing is a **physical biometric** technology for fingerprint acquisition. It detects very small changes in the parameters of transmitted signals, as the signals are modulated by passage through the subdermal layer of the skin. These modulated signals are received by a solid-state antenna array that transduces the signal variations into a gray-scaled bit map image of the fingerprint.

Active Array Sensing was formerly called **E-Field** technology and sometimes Linear Field technology.

Capacitive Sensing

Capacitive Sensing is a **physical biometric** technology for fingerprint acquisition. It detects very small variations in skin surface capacitance as measured by a solid-state array of charged capacitor plates that transduces the capacitance measurements into a gray-scaled bit map image.

Optical Scanning

General – There are several distinct variations on the theme of optical scanning for fingerprints. An optical scanning system can be nothing more than a computer-connected digital scanner reading inked fingerprint cards and creating from that stream the data artifacts necessary to build templates or perform verification.

A more sophisticated class of hybridized optical systems shares certain characteristics with true solid-state systems. Here, the actual fingertip is presented to a receiving platen, where it is scanned. The resulting image is optically transferred to a solid-state charge-coupled device (CCD or CMOS). The device transduces the image into a usable digital data stream.

Additionally, most optical scanners employ a soft coating on the platen to help overcome some of the limitations of the technology. This coating degrades rather rapidly because of accumulation of embedded dirt, UV discoloration of the coating material over time, and physical damage from scratches and impacts. Consequently, these coated platens must be replaced at regular intervals to avoid significant degradation of image quality.

Optical sensors often function erratically when the acquisition platen is flooded with light (especially sunlight or bright daylight), overloading the transducer within.

Opto-Electroluminescent Scanning – In this variation, a platen made of a specialized electroluminescent polymer selectively emits light when electrically stimulated by contact with a charged finger. The charge gradient between ridges (in contact with the platen) and valleys in the fingerprint creates the image. The postage-stamp-sized image is optically reduced about 100 times by a Fresnel lens and delivered to a solid-state imaging device that transduces it into digital data.

Edge-Lit Holography – In this variation on the optical theme, the topological details (ridges and valleys) of a fingerprint presented to the platen are illuminated by light diffracted by a volume hologram. The light thus modulated is passed to a CCD imaging device which transduces it directly into digital data.

Thermal Sensing

Thermal Sensing is a **physical biometric** technology that measures the temperature gradient between ridges (in contact with the platen) and valleys (cooler air gaps) in the fingerprint. The thermal data are collected by a solid-state device that transduces it directly into digital data.

Ultrasound Sensing

Ultrasound Sensing is a **physical biometric** technology that analyzes and compares the acoustic impedance of skin, air, and the fingerprint platen to build an image of the fingerprint.

Other Technologies

A number of other biometric identification technologies are available or in development. Some of these are well-known in the industry and some are not. In alphabetical order these include:

DNA Analysis

A **physical biometric** technology that analyzes the unique structure of repeating patterns in the millions of pairs of nucleotides found in the body's **d**eoxyribo**n**ucleic **a**cid. In the past, these patterns could not identify specific persons, but they could be used to determine whether two DNA samples were from the same person, from related people, or from non-related people. However, recent developments in analysis techniques have opened the possibility of reliable "DNA Fingerprinting" – the identification of an individual. This process is neither simple nor easy, and involves a complex and precise laboratory effort to clip the DNA strand into usable sections using "chemical scissors" called restriction enzymes.

Ear Geometry Recognition

Cochlear Geometry Recognition is a **physical biometric** technology that analyzes the unique convolutions of the pinna, the exterior structure of the human ear. Earlobe Capillary Pattern Recognition is a related methodology.

Face Recognition

Face Recognition is a **physical biometric** technology that analyzes anatomical "eigenface" characteristics of the human face, such as the distance between the eyes, and the shape and location of the cheekbones. Acquisition of the face image is by a digital camera – preferably two (or more) interacting cameras to give a depth-of-field stereo effect for three-dimensional analysis. Face recognition software can generally compensate for the presence or absence of glasses, hats, beards, and so on. This technology doesn't work reliably with identical twins.

Gait Recognition

Gait Recognition is a **physical biometric** that, like voice recognition, also exhibits characteristics of a behavioral biometric, because although the pattern of locomotion is largely determined by the articulation and physiology of the body, it can be readily altered by the subject. This biometric analyzes the presumably unique way in which a person moves and walks.

Hand/Finger Geometry Recognition

Hand and Finger Geometry Recognition are related **physical biometric** technologies that analyze the unique configurations of hand and/or finger shape. As many as 90 characteristics may be evaluated, including the dimensions of the hand, length and width of the fingers, and the shape of the knuckles. Hand geometry systems may analyze the whole hand, a single finger, or two fingers at a time.

Iris Pattern Recognition

Iris Pattern Recognition is a **physical biometric** technology that analyzes the unique patterns formed by various features in the iris (the colored portion) of the eye. This technology doesn't work in the presence of vanity contact lenses.

Keystroke Dynamics

Keystroke Dynamics is a **behavioral biometric** technology that analyzes the characteristic way in which an individual types on a computer keyboard. It works best with touch-typists. In a related and now obsolete technology, from the very earliest days of telegraphy, operators knew one another by their "fists" – the characteristic way that they used the telegraph key – rather cognate with recognizing a voice on the telephone and one of the very earliest technical identification biometrics.

Passwords, PINs, Keys, and Tokens

Passwords and personal identification numbers are alphanumeric strings that can be entered into a computer system and used to identify the user. A key, naturally, is a mechanical device used to open a lock.

A token is some physical object possessed by a person that serves to provide positive identification or some other proof-of-situation. For example, a token could be a marriage certificate, a letter of introduction, or a passport. It could also be an identification badge (with or without electronic encoding), a credit card, or an active electronic device that can be interrogated by an identification system.

Of course, these are not biometric technologies at all (no biological characteristics are measured), except insofar as a password or PIN may be a product of the imagination of an individual. However, these easily-defeated security measures are ubiquitous, and are very often used in conjunction with (or as a backup to) other biometrics (for example, the PIN that goes with your **ATM** card).

Retinal Pattern Recognition

Retinal Pattern Recognition is a **physical biometric** technology that analyzes the unique patterns formed by blood vessels in the retina of the eye. This technology doesn't work in the presence of vanity contact lenses.

Signature Dynamics

Signature Dynamics is a **behavioral biometric** technology that analyzes various aspects of the way in which an individual writes a signature. Such factors as pen and stroke speed, stroke order, and pressure variations are considered, as well as the actual appearance of the signature.

Vein-Pattern Recognition

Vein-Pattern Recognition is a **physical biometric** technology that analyzes the subcutaneous vascular network on the back of the human hand, using infrared illumination to produce a thermographic image of the unique vein pattern.

Voice Recognition

Voice Recognition is a **physical biometric** technology that analyzes speech cadence, pitch, and tone. It also exhibits some of the characteristics of a **behavioral biometric** because although the pattern of the voice is largely determined by the physiology of the throat, pharynx, and larynx, it can be readily altered by the subject. Health, fatigue, and stress are important conditioning factors. Background noise and other extraneous sounds greatly affect how well a voice recognition system operates.

APPENDIX C: Biometric Sources

Avanti
An international reference site, Avanti offers a considerable amount of background information about biometrics, their use in everyday business situations, and how to deploy them.
www.biometric.freeserve.co.uk

Biometric Consortium
The US Government's focal point for research, development, test, evaluation, and application of biometric-based personal identification/verification technology.
www.biometrics.org

For more information contact:

AuthenTec, Inc.
Post Office Box 2719
Melbourne, Florida 32902-2719
321-308-1300
www.authentec.com
apps@authentec.com