BIOMETRIC TECHNOLOGIES - FINGERPRINTS

Chris Roberts
February 2006

Table of Contents

Key Words 3

Abstract 3

Introduction 4

Fingerprints 4
- Fingerprints Defined 4
- Henry Classification System 5

Automated Identification Systems 7
- Australia 7
- Europe 8
- New Zealand 8
- United Kingdom 8
- United States 8

Storage and Compression 9
- Example of Lossy Compression 9
- JPEG 9
- WSQ 10
- JPEG2000 vs WSQ 10
- Other Graphics Formats 10
- File Compression Tools 11
- Recent Developments 11
- Live Scan Systems 11

Biometric Fingerprint Standards 12
- Adoption of Standards 13

Fingerprint Readers 14
- Capacitive 14
- Optical 15
- Other Technologies 15

Security 16
- Biometric Attack Vectors 16
- Defences 18
- Randomising Data 18
- Retention of Data 18
- Liveness Detection 18
- Multiple Biometrics 19
- Multi-Factor Authentication 19
- Cryptography and Digital Signatures 19
- Network Hygiene 19
- Physical Security 19

In Conclusion 20

Endnotes 21

Key Words

Biometric, identification, security, fingerprint, fingerprint standards.

Abstract

A companion paper prepared in November 2005 provides an overview of biometrics, related standards, uses and concerns. This paper provides a background to fingerprint recognition, describes the biometric use of fingerprints, biometric standards and related security issues. It is one of a series of papers also covering iris and retinal scanning, facial recognition as well as several other biometric technologies.

Introduction

Some biometric techniques are still confined to the laboratory but as research continues and technology improves, these techniques may be developed into practical applications. Currently used for identity, authentication and forensic purposes, biometric technologies can be broadly grouped into four areas with several techniques in each:

1. Hands;
2. Heads and face;
3. Other physical characteristics; and
4. Behavioural characteristics.

The first three categories are physiological and are based on measurement of a physical characteristic. Except in the case of a serious accident or operation, these biometrics are generally unchanged over time. Examples include fingerprints, hand geometry, iris and retinal patterns and DNA.

Behavioural characteristics are more susceptible to change and can be affected by age, illness, disease, tiredness and can also be deliberately altered, for example gait or signature. These are, therefore, less reliable as authenticators or identifiers.

Fingerprints

Fingerprint analysis, also known in the US as dactylography, is the science of using fingerprints to identify a person. Fingerprints are the most commonly used biometric and have been used for identification since the 1890's.

In 1901, Sir Edward Henry introduced the Henry Classification System for fingerprints which is widely recognised, even today, in anglophone countries. In South American countries a system devised by Dr. Juan Vucetich in 1892 is widely used. These manual classification systems are, however, being replaced by other techniques which are more suitable for large scale electronic storage and analysis.

Fingerprint identification is well established and a mature science. It has also been extensively tested in various legal systems and is accepted as an international standard for identification. Although law enforcement agencies are principal users of fingerprints, various electronic readers are now commonly available and are used for authentication purposes, mainly in access control applications.

Fingerprints Defined

All digits (fingers, thumbs and toes) have epidermal ridges, furrows and patterns. Palms and the soles of feet also have distinctive epidermal patterns. These patterns are widely believed to provide a friction surface to assist in gripping and handling objects and for walking[1,2]. Fingerprints are formed in the third and fourth month of foetal development and are unique. Even identical twins will have differing fingerprint patterns. In the many years fingerprinting has been used by law enforcement agencies, no two individuals have been found to have identical prints.

The skin excretes oils and perspiration through sweat glands, flowing along the tops of the ridges. When a surface is touched the fingerprint is transferred. Smooth, clean surfaces record better quality fingerprints but fingerprints can also be found on irregular surfaces such as paper. There are three basic categories of fingerprint:

- visible prints (also called patent), such as those made in oil, ink or blood
- latent prints which are invisible under normal viewing conditions; and
- plastic prints which are left in soft surfaces such as new paint.

There are now over forty methods available for collecting prints including powders, use of chemicals such as iodine, ninhydrin, and silver nitrate, digital imaging, dye stains and fumes. Some are powders and chemicals are coloured to contrast with the background or to fluoresce or illuminate under alternative light sources. Lasers are also used. Generally the least destructive method is used first.

Henry Classification System[3]

As the Inspector General of Police for Bengal Province in India, Sir Edward Henry (1850 - 1931) developed a classification system which was officially adopted by British India in 1897. The British Association for the Advancement of Science heard of Henry's success in India and in 1900 he presented a paper entitled "Fingerprints and the Detection of Crime in India. Shortly after, Henry's book "The Classification and Uses of Finger Prints" was published.

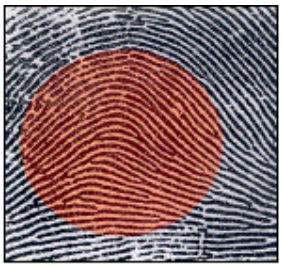
In December 1900, Britain's Belper Committee recommended that the fingerprints of criminals be taken and classified by the Indian System. In 1901, Henry was called back to England and given the post of Assistant Commissioner of Police in charge of Criminal Identification at New Scotland Yard. In 1903, Henry became Commissioner of Police.

The Henry Classification System organises ten-print fingerprint records by pattern type. Finger ridges and patterns can be continuous, interrupted, forked, and other formations. Fingerprints are classified and identified by the relationship of these formations, described as minutiae. These patterns are divided into five basic groups, with various subgroups[4]:

- Arch: a ridge that runs across the fingertip and curves up in the middle. Tented arches have a spiked effect.
- Whorl: an oval formation, often making a spiral pattern around a central point. Principal types are a plain whorl and a central pocket loop whorl.
- Loops: These have a stronger curve than arches, and they exit and enter the print on the same side. Radial loops slant toward the thumb and ulnar loops away from the thumb.
- "Composites" are a mix of other patterns;
- "Accidentals" form an irregular pattern that's not classifiable as an Arch, Loop or Whorl.

WHORL
In a whorl pattern, the ridges are usually circular.

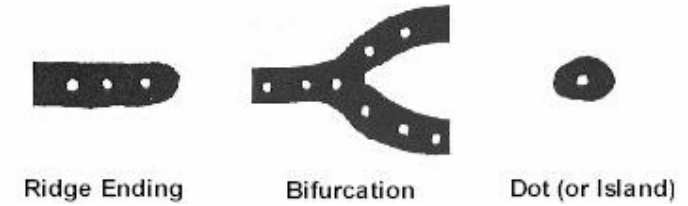
LOOP
In a loop pattern, the ridges enter from either side, re-curve and pass out or tend to pass out the same side they entered.



ARCH
In an arch pattern the ridges enter from one side, make a rise in the center and exit generally on the opposite side.

Source: FBI[5]

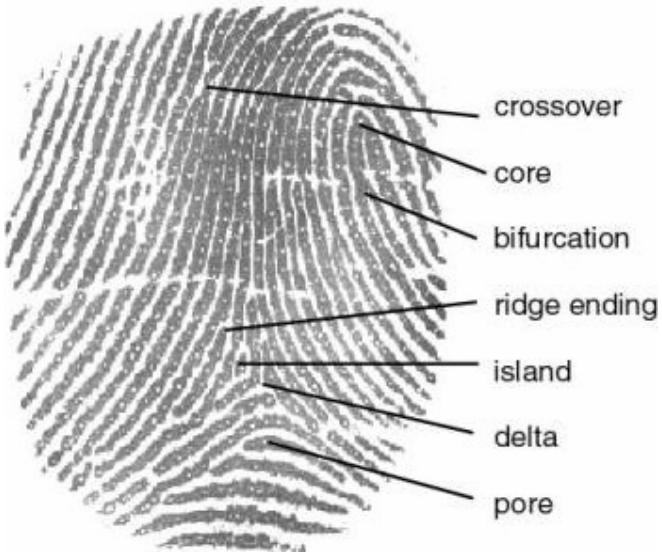
Several other characteristics can be present within fingerprint patterns. These are minutiae or interruptions to the smooth flow of ridges, and are the basis for most fingerprint identification. Codified in the late 1800's as Galton features, minutiae are at their most rudimentary ridge endings, the points at which a ridge stops, bifurcations, the point at which one ridge divides into two, and dots or small ridges.



Source: New Zealand Police[6]

Many types of minutiae are categorised and in addition to ridge endings, bifurcation and dots, include[7]:

- Islands (ridges slightly longer than dots, occupying space between two temporarily divergent ridges);
- Ponds or lakes (empty spaces between two temporarily divergent ridges);
- Spurs (a notch protruding from a ridge);
- Bridges (small ridges joining two longer adjacent ridges); and
- Crossovers (two ridges which cross each other).



Source: Rosistem, Romania

Automated Identification Systems

Automated Fingerprint Identification Systems, generally known as AFIS, were first introduced in the 1970's and are now well established and mature technologies. Most AFIS were originally based on the Henry Classification System and designed to speed the manual search process. The Henry Classification System is not, however, easily automated and works well only when all ten fingerprints are recorded. Partial print and incomplete fingerprint records could not be properly classified.

More recently automated classification of fingerprints is based on ridge flow analysis or ridgeline counting which generates a unique "map" of each fingerprint. These "maps" are stored as mathematical representations, occupy less storage space than the original image and are more suitable for computerised search and matching. This process is known as feature extraction.

Almost all police agencies around the world now use an AFIS. Unfortunately there is still a lack of commonly accepted standards by the manufacturers and vendors, poor interoperability between systems and poor compatibility with different types of scanner hardware. There is, however, considerable activity in establishing such standards with some aspects of fingerprint technology published by ISO and national standards bodies.

The use of fingerprints for authentication and identification in non-law enforcement application, such as welfare payment management or border control, has lead to the development of plain impression (also known as "live scan") AFIS applications.

Australia

The present Australian National Automated Fingerprint Identification System (NAFIS) was commissioned on April 31st 2001, utilising SAGEM technology. It currently contains approximately 2,6 million ten-print records. This includes records from all arrested persons since 1941 and other ten-print records such as police applicants or other occupations where probity checks are conducted.

The NAFIS can be accessed from any State or Territory in Australia from 39 metropolitan and remote locations. Each site can upload both ten-print and latent data and review AFIS search results. It also supports live-scan technology[8].

Europe

EU Ministers recently announced consideration of the creation of a European criminal Automated Fingerprints Identification System (AFIS)[9]. This AFIS could be either a centralised European AFIS or a de-centralised solution (linking the databases of exiting law enforcement agencies in European countries[10].

The Interpol European Expert Group on Fingerprint Identification (IEEGFI) was formed in 1998 and was tasked with formulating a European Fingerprint Identification Standard. The standard is to include standard fingerprint identification procedures, minutiae and other characteristics[11].

New Zealand

The New Zealand Police have used NEC's AFIS technology since 1991[12]. The system houses over four million fingerprints. In addition there are over 400,000 sets of fingerprints in physical form[13]. As with other AFIS systems, there is the ability to perform matches and searches using latent, ten-print or other crime scene marks.

United Kingdom

In the United Kingdom a National Automated Fingerprint Identification System (NAFIS) servicing 43 police forces, was introduced in September 2000. It holds over five million sets of prints, over half a million crime scene marks and interfaces with the national criminal history system[14]. Search times are now a few minutes, a significant reduction on the older, more manual processes where searches were performed centrally at New Scotland Yard and could take several weeks. NAFIS searches can be conducted in a number of ways including:

- Tenprint sets can be searched to establish if there is a criminal history;
- Latents or crime scene marks from crime scenes can be searched against the national database of tenprints from offenders.
- Tenprints from someone in custody can be compared against a database of latents and crime scene marks;
- Crime scene marks can be matched against the database of crime scene marks to help link crimes.

The improved search times resulted in a change in business processes with more speculative searching taking place. In one area, the police force had so many hits that they didn't have enough police to arrest all of the suspects. The system is processing approximately 1,500 latents per day with approximately 85% of latents resulting in an identification. Because of the success rates, police are able to reopen old cases.

In one instance, an individual in Wales was stopped for not wearing a seatbelt and fingerprinted. The NAFIS search revealed that the individual was using an alias and that he was wanted for an armed robbery of £5.5 million[15].

United States

The Integrated Automated Fingerprint Identification System (IAFIS), is the US national fingerprint and criminal history system maintained by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division. It records fingerprints (ten-print and latent print), subject search, and criminal history[16]. It is the largest biometric

database in the world, containing the fingerprints and corresponding criminal history information for more than 47 million subjects[17]. In 1995 it was estimated that the FBI archive, dating from the 1920's, contained over 200 million items and the archive was increasing at a rate of between 30,000 and 50,000 new items per day[18].

Storage and Compression

Image storage can consume significant computing resources. With the increased collection of fingerprint images, particularly in the US, the need to find efficient storage mechanisms that minimise data loss and file transfer times is imperative. Image compression is one technique used to conserve storage capacity and reduce file transfer times. Compression should not, however, introduce distortion which can limit usefulness and may compromise evidential integrity.

In a law enforcement environment, the preservation of the image is important and image quality degradation or distortion could create difficulties in fingerprint identification or possibly be challenged in court. Two basic types of compression are in use:

- Lossless, where the compression has no discernible effect on quality of the restored image; and
- Lossy, where some loss of image quality is expected, depending on the level of compression applied. Images can degrade with compression and/or decompression.

Lossless compression techniques generally have smaller compression ratios than lossy techniques. They also define maximum error rates between the original image and the reconstructed image. These are more properly described as "near lossless" as some degree of loss still occurs in the compression and reconstruction process. This has also been described as "visually indistinguishable from the original"[19]. A true lossless compression technique will reconstruct the image as a bit-for-bit match to the original image.

Lossy compression techniques are selected to remove components indiscernible to the human eye. Lossy compression can negatively affect the performance of automated systems when attempting to match fingerprints.

Example of Lossy Compression[20]

This is an industry standard test image. The image on the left is approximately 12Kb in size, the centre image has been compressed approximately 85% to 1.8 Kb with some loss of detail. The image on the right is compressed 96% to 0.56 Kb with a marked loss of detail and "compression artefacts" are pronounced.

JPEG

JPEG (Joint Photographic Experts Group) was formed in 1986 and developed a standard for the compression of photographic images, based on a discrete cosine transform. This is often coupled with the JPEG File Interchange Format (JFIF) developed by this group in 1992[21].

The JPEG standard is more formally known as the ISO standard - ISO/IEC IS 10918-1| ITU-T Recommendation T.81[22]. The JPEG standard is widely used for image compression but performs badly in compressing line drawings, textual or iconic graphics, for example fingerprints[23]. A newer standard, JPEG 2000, using a discrete wavelet transform, was developed to address some of the deficiencies of the earlier standard. JPEG 2000 has an architecture designed to accommodate a wide range of uses including medical imaging and digital cameras[24].

State of the art image compression is considered to be the use of Wavelet-based image coders. Wavelets are a mathematical tool that hierarchically represent and approximate functions[25] but are lossy. The choice of wavelets can be optimised for particular image types, such as photographic images but may not, however, perform satisfactorily on other image types[26].

WSQ

The FBI adopted Wavelet Scalar Quanitization (WSQ) in the early 1990's as a standard for 500dpi/8 bit grayscale fingerprint images. WSQ provides a higher compression ratio than the original JPEG standard, with less image degradation and distortion.

JPEG2000 vs WSQ

A study of the interoperability of JPEG 2000 and WSQ was conducted by MITRE Corporation in 2000/2001. This study resulted in some enhancements to JPEG 2000 Part 1 to accommodate elements present in WSQ but not in JPEG 2000 Part 1. Comparison of JPEG 2000 Part 2 and WSQ revealed some errors in trancoding from WSQ to JPEG although these errors were not usually detectable visually. This error, although small, was outside the tolerances of the FBI's specifications. The JPEG files were shown to be at least 10% smaller than the corresponding WSQ files[27].

Other Graphics Formats

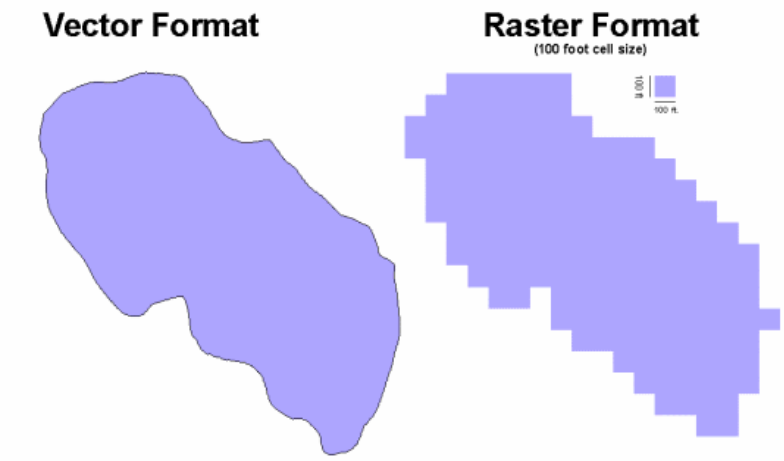
There are numerous other graphic formats. Some commonly used formats include:

- GIF, Graphics Interchange Format. It uses the proprietary LZW compression algorithm and dates from the late 1980s;
- PNG, Portable Network Graphics, an IETF and W3C recommended format. It was designed as a license free replacement for GIF and offers lossless compression;
- BMP, BitMapped graphic format used by Microsoft Windows systems. BMP files are generally uncompressed;
- TIFF, Tagged Image File Format. This is a lossless format but does offer a compression option through the use of the LZW compression algorithm.

GIF, BMP, PNG, TIFF and JPEG, are raster image formats. A raster format uses pixel grids (usually square or rectangular) to represent an image. Vector formats, by contrast use geometric primitives such as lines, points and curves to represent an image (see Figure 1 below).

There have been modifications and enhancements to the formats listed above over time but generally these earlier formats do not provide sufficient compression or resolution and are not considered suitable for evidential storage of fingerprints.

Figure 1: Representation of a lake



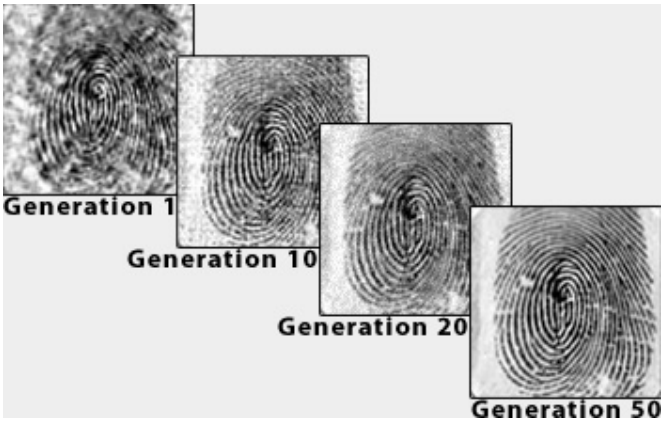
Source: University of Rhode Island[28]

File Compression Tools

A number of file compression tools are widely available, for example PKZip®, Winzip®, Stuffit® and a variety of UNIX and LINUX tools. These are designed as data compression tools and deal with a wide variety of data types. While they can compress image files, again they are not considered suitable for evidential storage of fingerprints.

Recent Developments

More recently, University of Texas researchers have developed a computer-generated algorithm which has superior performance to the FBI's WSQ. There are other human-developed and generated algorithms which also have superior performance but this development is reportedly unique in being entirely computer-generated[29].



Source: *Grasemann and Mikkulainen, Effective Image Compression using Evolved Wavelets, GECCO '05, (c) 2005 ACM, Inc.*

Live Scan Systems

In traditional law enforcement system, fingerprints are "rolled" to provide an impression of the entire print "nail to nail". These rolled impressions are usually recorded by inking the fingertips and then rolling the fingertip against paper. The inked impressions are then

scanned into an AFIS. Plain impressions are usually recorded by placing the finger on a scanner which records the impression from the part of the fingerprint in contact with the scanner. These are also described as "live scan" impressions[30].

These prints are typically 50% or less of the area of a rolled print and generally record only one or two fingerprints[31]. The small area recorded can limit the accuracy of matching and authentication. One technique used to try and overcome this limitation is the use of multiple, overlapping images of the same finger that are digitally composited into a complete fingerprint.

Live scan systems can also suffer from various image quality issues including image and geometric distortion and image break-up, often attributable to the quality of the scanner used. Poor quality images can also suffer image degradation and information loss when compression techniques for storage or archival purposes, are used. In addition, user co-operation is required to ensure good quality images are recorded.

Various studies have determined that the variables having the greatest effect on system accuracy were the number of fingers used and quality of the image recorded. The use of additional fingers greatly improved matching accuracy and the quality of the image was not entirely dependant on the type of device used to capture the fingerprint[32]. Testing included the FBI IAFIS system and the US-VISIT IDENT system.

In July 2005, Department of Homeland Security announced that visitors to the US will be required to submit all ten fingerprints on entry[33]. Approximately 36 million visitors have had two fingerprints recorded to date with 180,000 travellers a day. The ten fingerprint standard is intended to provide greater accuracy and better compatibility with the FBI's AFIS although no implementation date has yet been announced.

The conversion is likely to be complex, the technology will be expensive to implement and the system could cause delays and inconvenience for travellers. There will be a number of difficulties to overcomes including[34]:

- The requirement for increased processing power and greater data storage capacity;
- Programming and infrastructure changes;
- System integration between the US-VISIT INDENT and the FBI's IAFIS applications;
- The capacity of the IAFIS to accommodate the volume of new data; and
- The requirement for larger scanners and readers capable of enrolling and reading 10 fingerprints. These devices are presently around 10 to 20 times more expensive than the devices currently in use.

Biometric Fingerprint Standards

Most standards relating to fingerprints deal with the recording, classification, image quality, image compression techniques and data interchange. Much of the work has been undertaken in the US and includes[35]:

- ANSI/NIST ITL 1-2000, *Data Format for the Exchange of Fingerprint, Facial, and SMT Information*. Specifications for record formats and quality requirements for fingerprint images, facial photos, and SMT data. There is also an Interpol implementation of this standard[36].
- ANSI INCITS 377-2004, *Finger Pattern Based Interchange Format* This specifies the interchange format for the exchange of pattern-based fingerprint recognition data[37,38].

- ANSI/INCITS 378:2004, *Finger Minutiae Format for Data Interchange*. Specifications for representation of fingerprints using minutiae including a data format.
- ANSI INCITS 381-2004, *Finger Image-Based Data Interchange Format.*
- ANSI/INCITS 383-2004, *Interoperability and Data Interchange Biometrics-Based Verification and Identification of Transportation Workers*.
- CJIS/FBI IAFIS-IC-0110, FBI WSQ (Wavelet Scalar Quantization) standard for fingerprint image compression and decompression.
- CJIS-RS-0010(v)7 FBI *Electronic Fingerprint Transmission Standard* (EFTS). Message transmission requirements for submission of fingerprint data.
- AAMVA DL/ID-2000 *National Standard for the Drivers License/Identification Card*, issued by the American Association of Motor Vehicle Administrators and incorporating fingerprint image and minutiae, facial, and signature capture, quality, formatting, and compression requirements.
- *Products Certified For Compliance With The FBI's Integrated Automated Fingerprint Identification System Image Quality Specifications*, an FBI publication[39]
- NISTIR 6529, *Common Biometric Exchange File Format* [CBEFF , published by The (US) National Institute of Standards and Technology (NIST)][40].
- Internationally ISO has issued[41]:

    - ISO/IEC 19794-2:2005, *Biometric data interchange formats -- Part 2: Finger minutiae data.* This specifies data formats for representation of fingerprints using minutiae, including data elements, three data formats for interchange and storage of this data and extended data formats for including additional data such as ridge counts and core and delta location.
    - ISO/IEC 19794-4:2005, *Biometric data interchange formats—Part 4: Finger image data.* This specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas within the ISO/IEC 19785-1 CBEFF data structure.

- ISO also has a number of standards in development including:

    - Final Draft International Standard FDIS 19794-3, *Biometric Data Interchange Format - Part 3, Finger Pattern Spectral Status.*
    - Final Committee Draft FCD 19794-8, , *Biometric Data Interchange Format - Part 8, Finger Pattern Skeletal Data.*

Adoption of Standards

There are a number of examples of the adoption of the standards outlined above including[42]:

- The International Civil Aviation Organisation's (ICAO) Machine Readable Travel Document specifications include CBEFF and Finger Interchange format standards.
- International Labour Office of the UN, requirements for a seafarer's card includes finger minutiae, finger image and CBEFF standards.
- Department of Homeland Security Transportation Workers Identification Credential includes the INCITS 383 Standard.
- Department of Homeland Security Registered Traveller Programme includes INCITS 377-2004, INCITS 381-2004 and CBEFF standards.

The US Homeland Security Presidential Directive HSPD-12 called for secure credentials for US Federal employees and contractors to improve security of access to US Federal facilities and networks. Personal Identity Verification (PIV) standards were developed and have been

published by NIST as FIPS 201[43] and Special Publication 800-76[44], which references ANSI/INCITS 378:2004 and ANSI/INCITS 385:2004.

Under HSPD-21 information will be stored on a smartcard and will include the template data of two fingerprints. Originally images of the fingerprints were to be stored which raised a number of cost, logistical, security and privacy concerns[45]. Storing images would require a card with greater capacity than the 32Kb capacity of the most widely used smartcards. Vendors would have to produce a card with 64 or 128Kb capacity and reader equipment and supporting systems would have to be modified. Security and privacy concerns formed around the accessibility of personal data and fingerprint images if a card was lost or stolen.

Some of these concerns have been addressed with the standards issued by NIST which store the mathematical representation of the fingerprint, rather than the image itself. US Federal agencies are required to start issuing cards by 27 October 2006 and all US Federal credentials must be replaced by 2009. SP 800-76 also covers facial image biometrics requiring the use of the INCITS 385 standard[46].

Fingerprint Readers

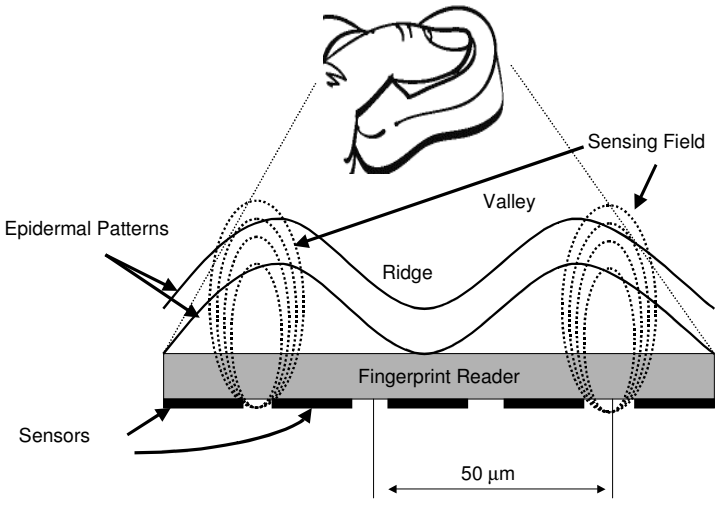
Fingerprint readers can employ several techniques. The principal methods are:

- Capacitive; and
- Optical.

Capacitive

Capacitive readers measure the differences in electrical signals generated by the valleys and ridges of fingerprints when presented to the reader. Capacitive readers use a sensor that measures conductivity of a large number of points over the surface of the sensor. Limited by the size of the human finger, sensors measure approximately 15 x 20mm. Grids embedded in the sensors create discrete points of measurement, sometimes described as pixels. For example, in a sensor 12.8 x 18.0 mm in size contains a grid of 256 x 360 pixels[47]

Active capacitive sensing is considered to have a high tolerance for parasitic effects compared to passive capacitive sensing, thus improving accuracy.



Adapted from Active Capacitive Sensing:UPEK[48].

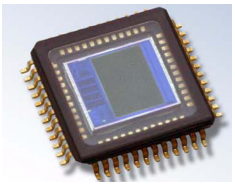
A key advantage of a capacitive reader is the requirement for a fingerprint-type shape, rather than an image. This can be a defence to spoofing. Based on semiconductor chips, capacitive readers can have a price advantage and be more compact than optical devices.

Optical

Optical readers use either a complementary metal oxide semiconductor (CMOS) device or, more commonly, a charge coupled device (CCD), similar to the devices used in digital cameras. A fingerprint scanner typically has its own light source, usually a light-emitting diode (LED) array.

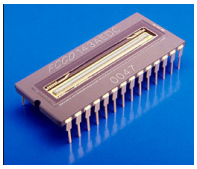
Currently, CMOS image sensors offer lower power consumption (up to a factor of 100) and more on-chip functionality. They are also often found in high volume, portable applications such as camera cellular phones, PDAs and some digital cameras[49].

CMOS Image Sensor



Source: OmniVision[50]

CCD



Source: Fairchild Imaging[51]

First invented in the 1960's by Bell Laboratories, CCD sensors are constructed with thousands of pixels grouped in linear or matrix arrays and register light intensity of each pixel[52], thus creating an image of a scanned fingerprint. CCDs generally provide higher quality images than CMOS devices

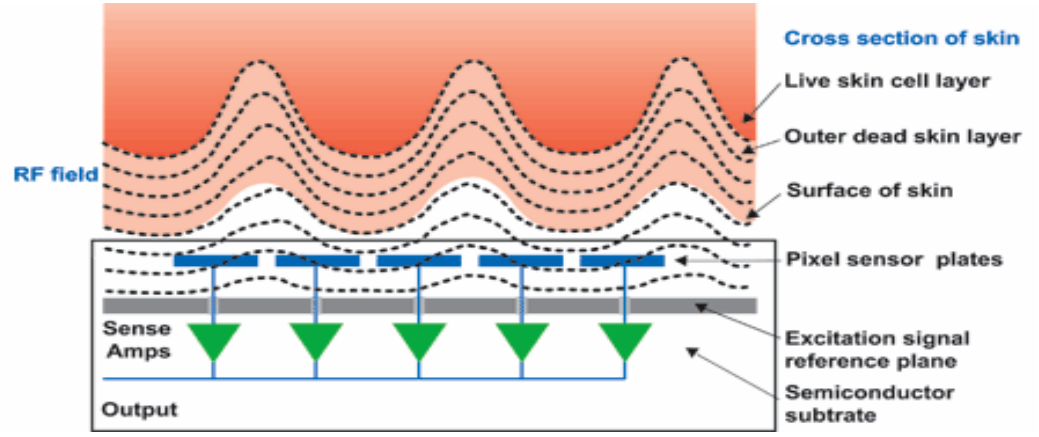
Other Technologies

Other sensing technologies include[53]:

- Radio Frequency (RF); which seeks a live skin layer thus incorporating a "liveness" test;
- Thermal; measuring temperature differences between the ridges and valleys on the fingerprint.
- Piezo-resistive; also known as piezo-electric and which detect finger pressure. More commonly used to detect tapping or key entry patterns;
- Ultrasonic; or acoustic sensors measuring differences in reflected sound when the fingertip is presented to the sensor. This is usually very high frequency such as 50 MHz; and
- Micro-Electrical Mechanical Systems (MEMS). These are devices that integrate electronic and mechanical components, usually onto a single substrate. Examples also include ink-jet printer heads, blood pressure sensors, accelerometers and pressure sensors. MEMS can include a variety of sensor technologies, including those outlined above.

The sensing technologies described above are being continually developed and may, in the future, take a place alongside capacitive and optical designs.

Figure 2: RF Sensing



Source: Authentec[54]

Security

There have been attempts to circumvent fingerprint security systems for many years. An early report into fingerprint devices and their susceptibility to acceptance of "lifted" fingerprints or fake fingers, was published by Network Computing in 1998[55]. They found that four out of six devices tested were susceptible to fake finger attacks.

Further research was undertaken by Tsutomu Matsumoto who published a paper on "gummy" fingers in 2002[56]. In this research fake fingers were made from gelatine and had a high acceptance rate from fingerprint readers using optical or capacitive sensors. In addition, fake fingers could be enrolled in the system with between 68 to 100% acceptance.

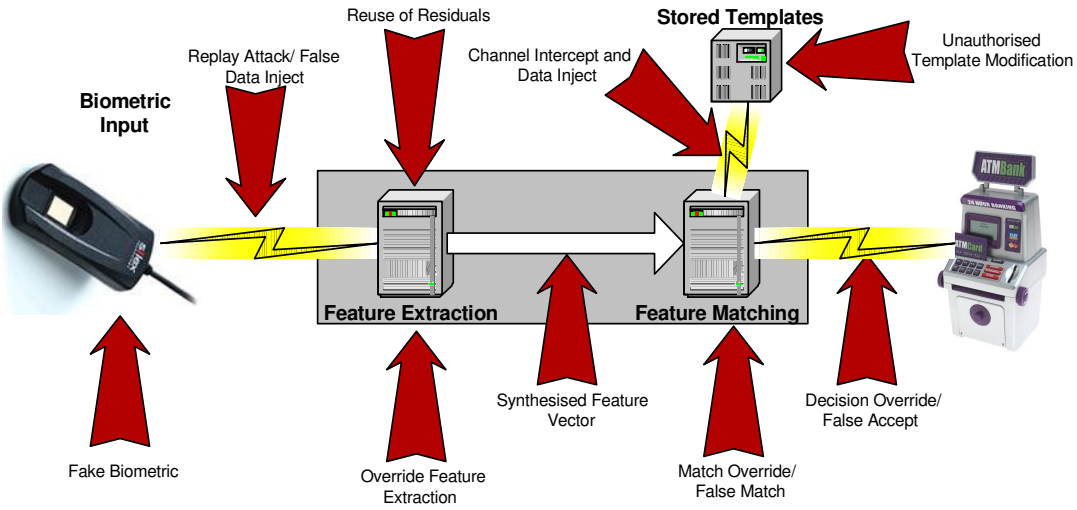
In November 2002 c't magazine[57] published the results of an investigation into testing of a variety of biometric devices. A number of spoofing attacks were successful as were "man-in-the-middle" attacks on datastreams.

More recently (December 2005) research undertaken at Clarkson University revealed that it was possible to demonstrate a 90% false verification rate in the laboratory[58]. This included testing with digits from cadavers, fake plastic fingers, gelatine and modelling compounds. However, when "liveness" detection was integrated into the fingerprint readers, the false verification rate fell to less than 10% of the spoofed samples.

From this and other related research, the presentation of a synthetic or dismembered finger or the use of a latent print are recognised methods of spoofing a fingerprint reader.

Biometric Attack Vectors

There are a number of points or vectors at which a biometric system can be attacked. While the fake biometric attack has attracted the greatest publicity, all other attacks require some form of access to the biometric processing systems and perhaps represent a more significant risk. The key attack vectors are illustrated below:



Adapted from: Biometrics: A Grand Challenge[59]

Fake Biometric

This may be any fake biometric, designed to circumvent the biometric system. It includes cadaver and false fingers make from silicone, gelatine, plastic, modelling clay or some other substance. Other techniques include the activation of a latent print by breathing on a print from a prior user, use of plastic bags filled with warm water, or spraying the latent print with a substance designed to make that print readable.

Replay Attacks/ False Data Inject

Here the data related to the presentation of biometric is captured and replayed. Alternatively a false data stream is injected between the sensor and the processing system.

Reuse of Residuals

Some systems may retain the last few biometrics extracted and templates used in memory. If an attacker gains access to this data, they may be able to reuse it to provide a valid biometric. Clearing memory and prohibition of an identical samples being used consecutively is an effective defence here.

Override Feature Extraction

This attack interferes with the feature extraction routines to provide false data for further processing. Alternatively, this attack can be used to disable a system and create a denial of service (DOS) attack.

Synthesised Feature Vector

A data stream representing a fake biometric is injected into the system.

Match Override/False Match

The matching decision is overridden or ignored and replaced with a match. Adjustments to the system tolerances in feature matching, in particular the false acceptance rate (FAR), can result in system acceptance of poor quality or incorrect data. The US Department of Defense recommends an FAR no greater than 1 in 100,000 and a False Rejection Rate (FRR) no greater than 5 in 100[60].

Storage Channel Intercept and Data Inject

Perhaps the attack with the most significant consequences, this attack can compromise both the processing system and any data stored.

Unauthorised Template Modification

Templates are modified, replaced or added to the system. Adding a template can circumvent any registration procedures and real (but unauthorised) biometrics can be presented and processed by the system alongside legitimate biometrics.

Decision Override/False Accept

This attack ignores any processing and overrides the decision data or injects a false acceptance between the system and the end device (for example a door lock or a cash dispenser).

Defences

There are a number of defensive measure that can be taken to minimise the risk of the attacks described above. As with many defensive measures, these are complementary and security should not rely on a single method. Relevant defensive measures include[61,62]:

- Randomising input biometric;
- Retention of data;
- Liveness detection;
- Use of multiple biometrics;
- Use of multi-factor authentication;
- Cryptography and digital signatures;
- Network hygiene; and
- Physical security.

Randomising Data

Where users are required to enroll multiple biometric samples, such as several fingerprints, verification can randomise the sample requested thus adding complexity to any attempt to circumvent the biometric authentication. Such systems may also require multiple fingerprints for verification, again adding complexity as any such attempt to circumvent the biometric system will have to prepare several "target" fingerprints. This will also defeat attempts to reuse latent fingerprints on the fingerprint reader.

Retention of Data

In most biometric systems, data is discarded after template generation. Retaining image data may provide a means of resolving spoof claims, although this adds system complexity in dealing with privacy and storage protection challenges. This defence against “man-in-the-middle” attacks forces an impostor to create data that appears as a biometric sample to the naked eye as well as to the system.

Liveness Detection

A key defence to spoofing is “liveness” detection to ensure the finger presented to the reader is attached to a live person and is not artificial or from a cadaver. Some liveness tests are based on autonomic responses and other can use a challenge-response construct such as blinking an eyelid on command. Liveness detection methods can be incorporated into the biometric reader or can be a separate device. Detection methods include:

- Measurement of perspiration patterns;
- Pulse oximetry where pulse and blood oxygenation are measured by shining a beam of light through the finger tissue;
- Skin spectroscopy, which measures the absorption of light by tissue, fat, and blood and melanin pigment; and
- Thermal measurement.

Multiple Biometrics

Similar to randomising biometric data requested, multiple biometrics add a level of complexity if more than one biometric is required, for example, fingerprint and iris scan. Clearly it is much more difficult to spoof multiple and different biometrics. The requirement for multiple biometrics, however, adds complexity to the authentication system.

Multi-Factor Authentication

Again similar in concept to randomising data and the use of multiple biometrics, the use of multi-factor authentication, such as a requirement for smart cards, tokens, PINS and passwords, can provide a powerful deterrent to spoofing. It can, however, increase processing time and may reduce the convenience of biometric systems. An attempt to circumvent the biometric system would need both the biometric and the second authentication factor. Multi-factor authentication can be combined with a challenge-response mechanism, further increasing the complexity for any attacker.

Cryptography and Digital Signatures

Encryption of data streams can be an effective defence against data interception and injects. Encryption of data "at rest", such as templates, can be an effective defence against data modification. Digital signatures also defend against data modification for both data in process and "at rest". Encryption keys should be secured, preferably not on the biometric system.

Network Hygiene

As with all technology, good network disciplines and hygiene are essential to the maintenance of system security. Many frameworks and best practice guides are available and apply equally to biometric as well as other technology systems. Examples include ITIL®[63], ISO 27005:2005[64] and COBIT®[65].

Physical Security

Physical security, as in many IT security systems, is often the cheapest and most effective deterrent to attempts to circumvent biometric systems. This ranges from physical restrictions to limit access to the biometric readers, to surveillance and guards and can defeat other attack types, such as coercion.

Regular inspection and cleaning of equipment is also important. Cleaning, for example, will not only sanitise the equipment for health reasons but, more importantly, minimises the persistence of latent prints and may also improve the performance of the sensor.

Many of the attack vectors described are more easily executed if the attacker has physical access to the biometric system. Physical security is also a key defence in managing access to biometric systems and stored data, such as templates.

In Conclusion

Fingerprints have been widely used as a form of identification for many years and are well-established in many cultures, countries and jurisdictions. The biometric use of fingerprints continues to grow as sensor technology improves, prices fall and supporting systems are enhanced.

While much publicity has been afforded to the spoofing of fingerprint sensors, this is only one of the security concerns with biometric identification and authentication systems. It is clear that most attack vectors relate to the supporting systems and networks. It is equally clear that properly architected and secured systems, together with physical security, good network hygiene and management, must play a key role in securing such biometric systems.

Endnotes

[1] Fingerprint, Wikipedia, http://wikipedia.org/wiki/Fingerprint, accessed 02 October 2005
[2] New Zealand Police Fingerprint Sections, http://www.police.govt.nz/service/fingerprint/, accessed 02 December 2005
[3] The Henry Classification System, International Biometric Group, 2003 http://www.biometricgroup.com/Henry%20Fingerprint%20Classification.pdf, accessed 02 December 2005
[4] All About Fingerprints, Chapter 4 - The Techniques, http://www.crimelibrary.com/criminal_mind/forensics/fingerprints/4.html, accessed 02 December 2005
[5] Taking Legible Fingerprints, Federal Bureau of Investigation, http://www.fbi.gov/hq/cjisd/takingfps.html, accessed 02 December 2005
[6] New Zealand Police Fingerprint Sections, http://www.police.govt.nz/service/fingerprint/, accessed 02 December 2005
[7] Biometric Education/Fingerprints, Rosistem Romania, http://www.barcode.ro/tutorials/biometrics/fingerprint.html, accessed 02 December 2005
[8] Australian NAFIS, The Thin Blue Line Information Section, NSW Police, http://www.policensw.com/info/fingerprints/finger15.html, accessed 04 December 2005
[9] EU ministers approve biometric ID, fingerprint data sharing, John Lettice, The Register, 01 December 2005, http://www.theregister.co.uk/2005/12/01/jahc_biometric_id_standards/, accessed 04 December 2005
[10] Communication From The Commission To The Council And The European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, Brussels, Commission Of The European Communities, 24 November 2005, http://www.europa-kommissionen.dk/upload/application/d7e26639/com_2005_0597_f_en_acte.pdf, accessed 04 December 2005
[11] Method For Fingerprint Identification, Interpol, http://www.interpol.int/public/Forensic/fingerprints/WorkingParties/IEEGFI/ieegfi.asp, accessed 04 December 2005
[12] What is AFIS?, NEC New Zealand, http://www.nec.co.nz/html/pro_afis.html, accessed 04 December 2005
[13] Wellington District , New Zealand Police, http://www.police.govt.nz/district/wellington/features.php, accessed 04 December 2005
[14] NAFIS, Police Information Technology Organisation (PITO), http://www.pito.org.uk/what_we_do/identification/nafis.htm, accessed 04 December 2005
[15] AFIS Committee Minutes 23 February 2001, International Association for Identification, http://onin.com/iaiafis/IAI_AFIS_Minutes_072400.pdf, accessed 04 December 2005
[16] IAFIS Incremental Builds, FBI, http://www.fbi.gov/hq/cjisd/iafis/iafisbuilds.htm, accessed 04 December 2005
[17] Integrated Automated Fingerprint Identification System, FBI Criminal Justice Information Services Division, http://www.fbi.gov/hq/cjisd/iafis.htm, accessed 02 December 2005
[18] Handbook of Fingerprint Recognition, Maltoni *et al*, Springer, New York, 2003, http://bias.csr.unibo.it/maltoni/handbook/Chapter_1.pdf, accessed 23 October 2005
[19] Isn't there a lossless JPEG?, http://www.faqs.org/faqs/jpeg-faq/part1/section-13.html, accessed 12 December 2005
[20] Lossy data compression, wikipedia, http://en.wikipedia.org/wiki/Lossy_compression, accessed 12 December 2005
[21] JPEG File Interchange Format Version 1.02, September 1992, http://www.jpeg.org/public/jfif.pdf, accessed 12 December 2005
[22] JPEG Homepage, http://www.jpeg.org/jpeg/index.html, accessed 12 December 2005
[23] JPEG, Wikipedia, http://en.wikipedia.org/wiki/JPEG, accessed 12 December 2005
[24] JPEG 2000 Homepage, http://www.jpeg.org/jpeg2000/index.html, accessed 12 December 2005
[25] Effective Image Compression using Evolved Wavelets, Grasemann and Miikkulainen, University of Texas at Austin, http://nn.cs.utexas.edu/downloads/papers/grasemann.geccoo5.pdf, accessed 12 December 2005

[26] Effective Image Compression using Evolved Wavelets, Grasemann and Miikkulainen, Department of Computer Sciences, The University of Texas at Austin, http://nn.cs.utexas.edu/downloads/papers/grasemann.gecco05.pdf, accessed 12 December 2005

[27] JPEG 2000 and WSQ Image Compression Interoperability, Margaret A Lepley, Mitre Corporation, February 2001, http://www.mitre.org/work/tech_papers/tech_papers_01/lepley_jpeg2000/lepley-jpeg2000.pdg, accessed 12 December 2005

[28] Natural Resources and Environmental Management, University of Rhode Island, http://www.edc.uri.edu/criticallands/raster.html, accessed 19 February 2006

[29] Man Against Machine, National Science Foundation, 01 September 2005, http://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=104378&org=IIS, accessed 11 December 2005

[30] Handbook of Fingerprint Recognition, Maltoni *et al*, Springer, New York, 2003, http://bias.csr.unibo.it/maltoni/handbook/Chapter_1.pdf, accessed 23 October 2005

[31] Fingerprint Interoperability, PAR Worldwide Group, http://www.bioidentix.net/solutions/finger_inter.html, accessed 04 December 2005

[32] Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report, NISTIR 7123, Wilson *et al*, National Institute of Standards and Technology, June 2004, http://fpvte.nist.gov/report/ir_7123_summary.pdf, accessed 04 December 2005

[33] Homeland Security to expand biometric visitor tracking system, Chris Strohm, Government Executive, 25 October 2005, http://www.govexec.com/dailyfed/1005/102505c1.htm, accessed 04 December 2005

[34] DHS to foreign visitors: Give me 10, Alice Lipowicz, Government Computer News, 15 August 2005; Vol. 24 No. 23, http://www.gcn.com/24_23/news/36665-1.html, accessed 04 December 2005

[35] Biometric Industry Standards, Catherine J. Tilton, SAFLINK Corporation, 2003, http://www.saflink.com/pdf/Bio_Stds_CTilton.pdf, accessed 04 December 2005

[36] Data format for the Interchange of Fingerprint, Facial & SMT information, Interpol Implementation (ANSI/NIST-ITL 1-2000), Version No. 4.22b - October 28, 2005, The Interpol AFIS Expert Group, http://www.interpol.int/Public/Forensic/fingerprints/RefDoc/default.asp, accessed 04 December 2005

[37] InterNational Committee for Information Technology Standards, http://www.ncits.org/list_INCITS.htm, accessed 29 January 2006

[38] American National Standards Institute, http://webstore.ansi.org/ansidocstore/product.asp?sku=ANSI+INCITS+378%2D2004, accessed 29 January 2006

[39] Products Certified For Compliance With The FBI's Integrated Automated Fingerprint Identification System Image Quality Specifications, FBI, http://www.fbi.gov/hq/cjisd/iafis/cert.htm, accessed 04 December 2005

[40] Common Biometric Exchange File Format, NIST, http://www.itl.nist.gov/div895/isis/bc/cbeff/, accessed 05 February 2006

[41] ISO, http://www.iso.org/iso/en/ISOOnline.frontpage, accessed 29 January 2006

[42] Biometric Standards Developers, Ferdando Podio, September 29 2005, http://public.ansi.org/ansionline/Documents/Standards%20Activities/Homeland%20Security%20Standards%20Panel/ANSI-HSSP%20Fourth%20Plenary/Breakout%20%232%20-%20BTS/Podio2.ppt, accessed 05 February 2006

[43] Federal Information Processing Standard (FIPS)201, Personal Identity Verification of Federal Employees and Contractors, http://csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf, accessed 29 January 2006

[44] NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification, 15 December 2005, http://csrc.nist.gov/publications/drafts.html#sp800-76, accessed 29 January 2006

[45] Feds to use faster, safer fingerprint standard, Michael Arnone, Federal Computer Week, 12 December 2005, http//www.fcw.com/ accessed 12 December 2005

[46] NIST chooses minutia for HSPD-12 biometric standard, Jason Miller, Government Computer News, http://www.gcn.com/vol1_no1/daily-updates/37790-1.html, accessed 20 December 2005

[47] Sensors, UPEK, Inc., http://www.upek.com/products/sensors.asp#Table2, accessed 19 February 2005

[48] Active Capacitive Sensing, UPEK, http://www.upek.com/products/technology/active.asp, accessed 12 February 2006

[49] Capturing an Image, Eastman Kodak Company, http://wwwdk.kodak.com/global/en/corp/historyOfKodak/capturingAnImage.jhtml, accessed 12 February 2006

[50] OmniVision Camera Chips ,http://www.ovt.com/p_cameraChips.html#5m, accessed 12 February 2006

[51] CCD143A Specification Sheet, Fairchild Imaging, http://www.fairchildimaging.com/main/ccd_linear_143a.htm, accessed 12 February 2006

[52] Technical Overview: CCD Technology, Technical Information Bulletin 4131, Eastman Kodak Company, http://wwwye.kodak.com/global/en/service/professional/tib/tib4131.jhtml?id=0.1.14.34.3.10&lc=en, accessed 12 February 2006

[53] Solid State Fingerprint Scanners - A Survey of Technologies, Philip D. Wasserman, NIST, 26 December 2005, http://www.itl.nist.gov/iad/894.03/pact/SSFS_113005.pdf, accessed 12 February 2006

[54] TruePrint Technology, Authentec, http://www.authentec.com, accessed 12 February 2006

[55] Six Biometric Devices Point The Finger At Security, David Wills and Mike Lees, Network Computing, June 1, 1998, http://www.networkcomputing.com/910/910r1.html, accessed 29 January 2006

[56] Impact of Artificial "Gummy" Fingers on Fingerprint Systems, Tsutomu Matsumoto *et al*, January 2002, http://cryptome.org/gummy.htm, accessed 29 September 2005

[57] Body Check, Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler, c't magazine, http://www.heise.de/ct/english/02/11/114/, accessed 05 February 2006

[58] Clarkson Universit Engineer Outwits High-Tech Fingerprint Fraud, Clarkson University, 10 December 2005, www.yubanet.com/artman/publish/printer_28878.shtml, accessed 19 December 2005

[59] Biometrics: A Grand Challange, Jain *et al,* Michigan State University, http://biometrics.cse.msu.edu/icprareareviewtalk.pdf, accessed 05 February 2006

[60] Biometrics Security Technical Implementation Guide Version 1, Release 2, Defense Information Systems Agency for the US Department of Defense, 23 August 2004, http://csrc.nist.gov/pcig/STIGs/biometrics-stig-v1r2.pdf, accessed 13 September 2005

[61] Liveness Detection in Biometric Systems, Biometrics Information Resource, http://www.biometricsinfo.org/whitepaper1.htm, accessed 05 February 2006

[62] Biometrics Security Technical Implementation Guide Version 1, Release 2, Defense Information Systems Agency for the US Department of Defense, 23 August 2004, http://csrc.nist.gov/pcig/STIGs/biometrics-stig-v1r2.pdf, accessed 13 September 2005

[63] IT Infrastructure Library, Hompage, http://www.itil.co.uk/, accessed 10 February 2006

[64] ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems – Requirements, http://www.iso.org, accessed 10 February 2006

[65] COBIT, Information Systems Audit and Control Association®, http://www.isaca.org/, accessed 10 February 2006