LES Film Technology

Fingerprint Sensor Descriptions and Alternative Fingerprint Technologies

Absolute identification and authentication (verification of identity) through individual fingerprints, regardless of the technology used, requires three general steps: Image Generation/Image Capture, Feature Extraction, and Matching to an enrolled database. This document reviews Integrated Biometrics' patented light emitting sensor (LES) technology and the alternative technologies and processes for fingerprint image generation and image capture – their advantages and disadvantages, as well as a description of the features of fingerprint and matching – including a review of certification levels for legal identification.

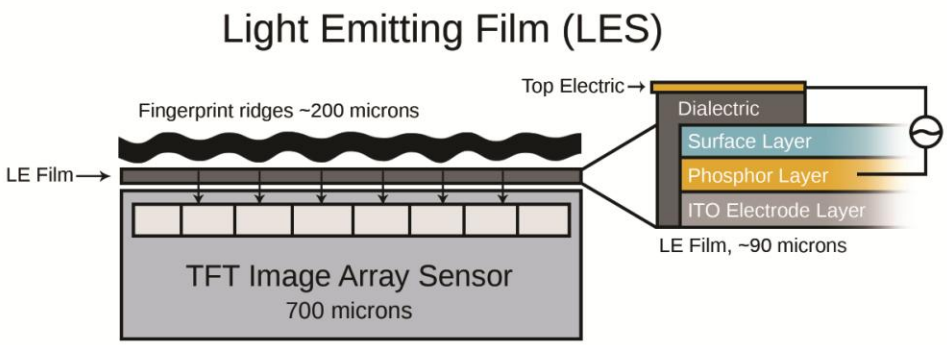
Sensing/Image Capture

There are many types of fingerprint sensors, both technologically and in form factor. Commonly used technologies include the original ink-on-paper technique, optical sensors, capacitive sensors, piezoelectric and ultrasound sensors, and electroluminescent film. In form factor, both area sensors and swipe sensors are in commercial use. The generated image quality, including the most detail of the unique features of the human fingerprint at the highest resolution, ultimately determines the performance of the fingerprint sensor/matching system. The size of the area sensor also has an effect on the accuracy and speed of the identification or authentication. Common fingerprint technologies and form factors, including their relative strengths and drawbacks are described below in the following sections (page number):

Electroluminescent Film (LES) Technology 2
Original Ink-on-Paper 7
Optical (TIR) Sensors 7
Capacitive Sensors 8
Piezoelectric Sensors 9
Ultrasound Sensors 9
Sensor Geometries (Swipe and Area) 10
Fingerprint Enrollment and Matching Algorithms 12
FBI Certification 13

Electroluminescent Film:

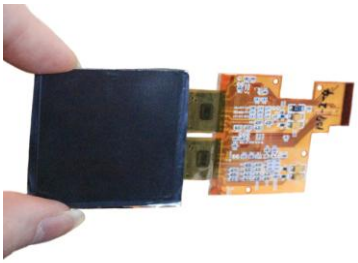
Integrated Biometrics produces a unique sensor based on an electroluminescent (LES) film to create the fingerprint image. The patented LES film is a multilayer, polymer composite. Dispersed within the film, at the nano-scale level, are particles that luminesce (give off light) in the presence of an electric field. When a finger is placed on the film, the live skin of the ridges of the fingerprint completes the low level electric circuit which causes the particles in the film to luminesce narrow wavelength light, producing a highly accurate, high resolution analog image of the fingerprint. The resolution of the fingerprint luminescence is between 1200 and 1500 ppi.

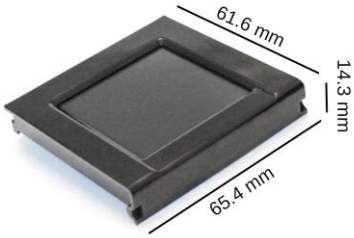


Shown below is the underside of the LES film showing the blue glow of the luminescent LES fingerprint image created when a finger is placed in contact with the top surface of the film.

The resultant high-resolution (1200 to 1500 ppi), narrow-wavelength optical image can be captured using a conventional lens and optical camera as used in traditional optical TIR systems or a using TFT (Thin Film Transistor like those used in digital radiography) or CMOS-based camera (like those used for cell phones). Regardless of the camera technology, the image is captured creating an Appendix F, FBI-quality image quality for flat or rolled fingerprints. The elegant combination of all these technologies has resulted in a technology that is truly a game changer for the mobile biometric marketplace.

Pictured below is the inner electronics of the Sherlock - the world's thinnest, lightest weight, FBI-certified fingerprint scanner.





The thickness of this unpackaged sensor is less than 1mm. Area dimensions for Sherlock are FAP45. (See Certified Section)

The LES sensor technology can be scaled up or down in size, from FAP 60 for multi-finger registration and identification to 4mmx4mm "button" size for mobile devices.

Image capture for Integrated Biometrics' TFT based sensors is 500 ppi with pixels that are exactly 50.8 microns in spacing. The image generation by the LES film is instantaneous and the image capture system records pictures at the rate of 10 to 15 frames per second.

The LES sensor system handles difficult to read fingerprints, such as dry, wet or dirty fingers by using adaptive circuitry and dynamic capture algorithms that quickly and automatically adjust to optimize the generated image. With a dry, wet or dirty finger, in the first few frames (less than one second), the system adjusts and captures a clear, full, and consistent high quality image.

Dry Fingers on Optical Scanner

Dry Fingers on LES

Black Mark on Finger
on Optical Scanner

Black Mark on Finger
on LES

The LES sensor system provides more spoof protection than conventional optical systems, as the fingerprint ridges and features touching the film must be human skin to activate the luminescence. Traditional optical sensors look at the surface topography of the subject matter presented to it and collect the print image via TIR (Total Internal Reflectance) technique, making them susceptible to spoofing. The LES sensor requires the ridge of the fingerprint touching the film to act as an electrical ground. Images of fingerprints will not create a fingerprint image with the LES system.

Latent prints or dirt left behind will not be seen by the LES sensor for the same reason. Oils left behind from previous users do not need to be cleaned away after each capture as is the case with other optical imaging sensors. This allows for high throughput (rapid enrollment and verification) of high quality fingerprints suitable for large population enrollments or verifications as well as the frequent, multiple authentications for mobile smart phones.

The LES sensor system using proprietary algorithms has extremely low FAR/FRR (False Acceptance and Reject Rates) for all fingerprint conditions which leads to less frustration for both rapid identification as well as authentication of valid users as they gain access with a single touch while still rejecting invalid users.

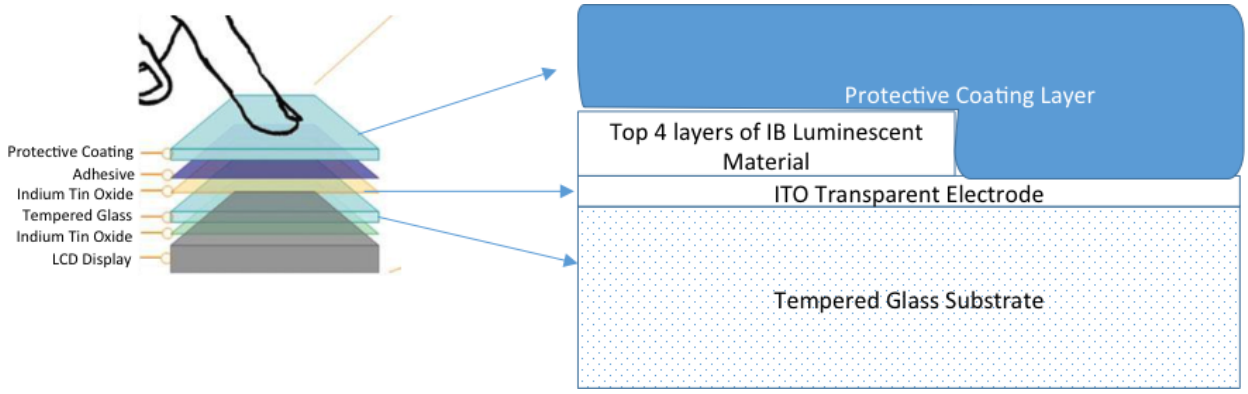
In addition to the features mentioned above, LES film is especially well suited for inclusion in devices used outdoors. Direct sunlight or bright light makes other optical sensors unusable. To be used outdoors, optical sensors require the fingerprint capture platens be shaded from the sun or bright lights. Sunlight or bright lighting has no effect on the Integrated Biometrics' sensor as external lighting has no effect on the luminescent image capture from the human fingerprint. Pictured below are images from a typical TIR optical scanner in sunlight contrasted with LES sensor system.

The LES system is environmentally rugged even at extreme temperatures. There are no fogging or condensation problems using LES film to generate the optical image. The LES film is

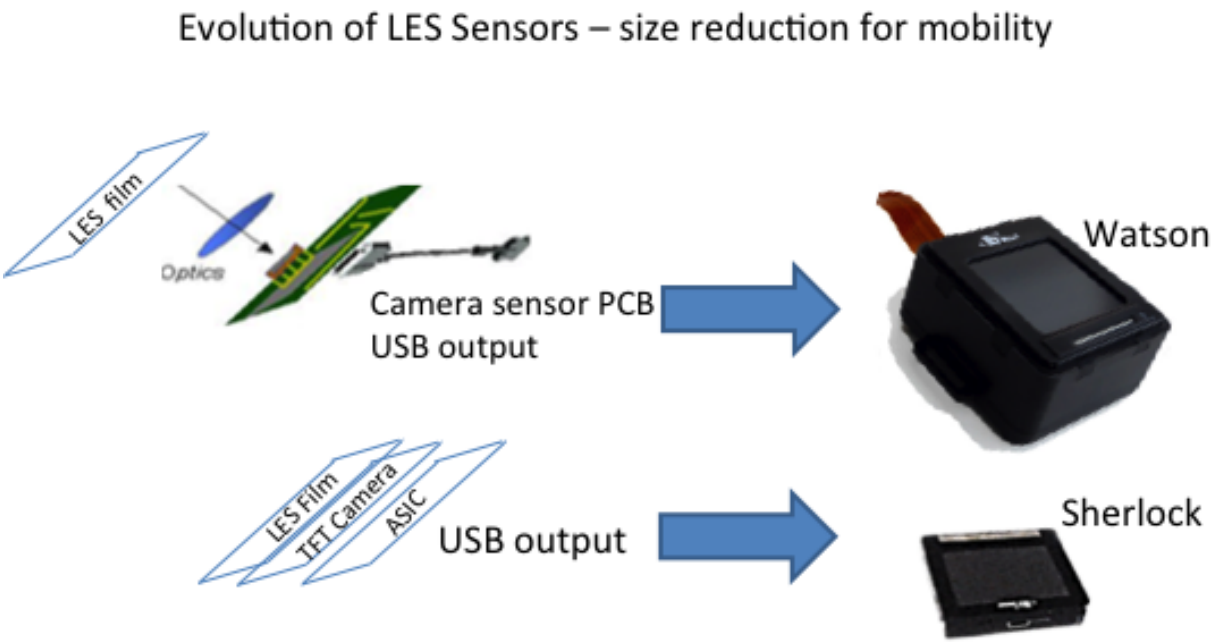
not easily damaged and resists abrasion. The LES sensor system has been used successfully for more than a decade in unprotected, outdoor, physical access control applications.

The LES film is flexible, allowing for sensors that are curved to fit the human finger. The flexible LES film allows for creation of sensors that are customizable to any shape or size.

The LES film is created by multi-layer screen printing. The layers of the film can also be printed onto substrates including glass allowing for fingerprint authentication/identification without a distinctly visible sensor or button. In the case of touch screen glass, the component layers of the LES film can incorporate the ITO and protective over-layer of the glass for a fully integrated sensor.



The LES Sensor System consists of 4 major functional elements to produce a digital image of a fingerprint: a proprietary and patented electro-luminescent film (LES), a digital image camera, an LES driver circuit and circuit board to control the system, and power source. Interface to host processor can be accomplished via USB or via parallel connection.



Integrated Biometrics continues to advance the integration of the LES film and sensors with innovation in camera/image capture and most recently screen printing of the film components into touch screen glass composites. In the evolution example above, the Watson product was reduced in size without compromise in quality or speed of performance by replacement of the traditional optical camera and lens with a TFT-based digital camera. The result is Sherlock, who sensor element is thinner than 1 mm and can be made to any area size or geometry.

Integrated Biometrics offers different sizes and form factors of "FBI certified" fingerprint capture technologies to meet the needs of mobile ID applications currently characterized by the FBI and other international standards organizations. In addition IB has developed smaller sensors for the consumer mobile market, where area sensor size is smaller than FBI standards. With smaller capture area, the quality of the image becomes even more critical for rapid, accurate ID. See the later discussion of sensor area

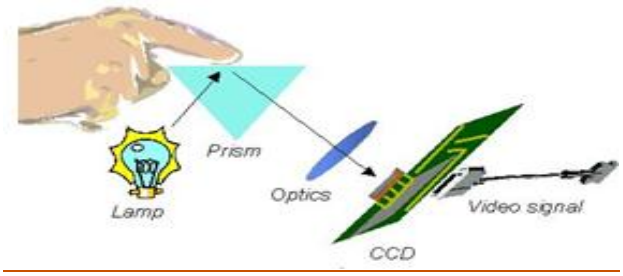
Integrated Biometrics' technology, including its LES sensor systems are patented under the following issued patents with several more pending: 6,326,644; 6,688,186; 6,952,490; 6,993,164; and 7,248,298.

Original Ink-on-Paper Technique: Before the creation of electronic fingerprint sensors, persons of interest were identified against an existing fingerprint card file or from latent prints recovered at crime scenes by collecting a set of all ten rolled (nail-to-nail) fingerprint images from the person. This required the person's fingers be covered with ink and pressed or rolled onto a paper card. The collected fingerprint images were then compared manually by trained fingerprint examiners against the stored record of fingerprint cards. To improve the speed of matching, today, the prints are converted into a digital format. These digitized images can then be analyzed and matched to an existing database by a high speed matching algorithm. To meet the certification requirements of the FBI, the scanned images must have a resolution of 500 +/- 1% ppi (pixels per inch).

Drawbacks of this technology include smearing of the fingerprint detail by the ink, requiring training and experience for the person taking the print, and the relatively slow speed for print capture.

Advantages of this technology are the ability to produce rolled fingerprint images, where the finger is rolled from nail-to-nail to capture a full finger image. These images are valuable to law enforcement when matching to partial, latent images left on objects that have been handled or touched. Generally, the original ink technique works adequately on all finger types as the entire process is monitored and managed manually.

Optical Sensors make use of TIR (Total Internal Reflection) technology to directly image the fingerprint of the finger placed on the top surface of a glass prism. Until recently, optical based sensors using TIR have been the only practical technology to achieve the level of image quality necessary to meet FBI standards for large surface (FAP20 and above) area sensors.



Using TIR, a light source provides light that bounces off the internal top surface of the prism and is focused through a lens on a CCD of a CMOS camera. When a finger is placed on the top surface of the prism, the ridges of the fingerprint make contact with the glass absorbing the light being reflected and resulting in a "negative" image of the fingerprint being collected by the camera. Multiple images may be captured and the matching algorithm may select the best image or combine images to achieve a high quality match.

This technology can produce FBI certifiable images of at least 500 ppi.

Drawbacks of this technology are the weight and size of the sensor/camera systems. The sensitivity of the camera can be "washed out" in the presence of bright light or sunlight. Latent prints left behind on the platen surface can be seen by the camera in subsequent readings, requiring constant cleaning. Cold temperature performance is challenging as the warm finger can cause condensation and fogging of the cold glass platen. These conditions severely impact minutiae and pattern recognition, and hence the ability to enroll or match accurately and quickly.

TIR based optical methods have difficulty with dry fingers that have low contrast between the fingerprint ridge and valleys. Dry finger performance is improved with silicone membranes that are installed over the glass surface. Maintenance of these membranes (tears and replacements) are an additional drawback. Conventional optical systems tend to be large, heavy and fragile in rough environments (mobile).

Current mobile versions of TIR optical technology are typically bulky, being several inches in dimension, weighing several pounds and as such, do not meet the full mobility needs of the users. As the TIR optical method requires direct visual imaging, the fingerprint must be clean and free of all dirt. The platen must be kept clean as well, as skin oils/sweat from previous users will remain on the surface, affecting subsequent images. Regularly cleaning and membrane replacement slows the rate of enrollment or verification readings for high volume scanning (border control, voting, etc.)

The TIR optical sensor can be readily fooled or spoofed with a latent print or rubber fingerprints.

Requirements to shine light on the fingerprint and then capture the reflected light also increase the size of the sensor and can be a disadvantage in situations where lighting is not managed or desired. For example, daylight use of an optical sensor requires that the sensor be shaded from sunlight or other bright light, so the camera can focus on light from the fingerprint. In military use, an optical fingerprint sensor can "leak" light from the sensor, providing a detrimental visible signal in dark operations. Power required to create the lighting is also be a detriment to mobile/battery powered devices.

Under ideal conditions, including human monitoring, optical TIR technology can provide high quality images and direct upload of the image to a digital database.

Capacitive Sensors consist of a two-dimensional array of individual micro-capacitor plates embedded in a chip. The other "plate" of each micro-capacitor is the finger skin itself. Small electrical charges are created between the surface of the finger and each of the silicon plates when a finger is placed on the chip. The magnitude of these electrical charges depends on the distance between the fingerprint surface and the capacitance plates. The resulting fingerprint "image" from a capacitive sensor is the two-dimensional array of relative electrical charge values that are used for matching, typically to one-to-few data based.

Disadvantages of capacitive sensor technology are quality and resolution of the image and the cost of the sensor (as it is based on semiconductor technology). Very few capacitance based sensors have ever passed FBI certification, and then only as the smallest size (FAP10). Costs do not scale linearly with size – leading this technology to be deployed more often as a swipe rather than area sensor. Also as a semiconductor, capacitive sensors can be fragile, sensitive to dirty or oily fingers, and prone to ESD (electrostatic discharge) failure. The quality of the images collected are reasonable and capable of meeting the FBI's PIV specification but their small surface area make them incapable of meeting the Appendix F FBI specifications required for one-to-many matching in large data bases. Current commercial capacitive sensors have false reject and false acceptance rates (FRR/FAR) that are much higher than acceptable for legal identification.

Capacitive sensors are subject to false readings from fingers that are dirty or wet, as these films on the fingerprint greatly affect their capacitance.

Advantages of capacitive sensors are due their natural, solid state, structure which is small, lightweight, thin, and less susceptible to breakage (than TIR optical). They are small and easy to use, leading to increasing consumer electronic adaptations. Capacitive sensors generate no stray light. Capacitive sensors use the conductance/resistance of skin to determine the locations of ridges and values and thus are inherently more spoof-resistant than TIR optical scanners.

Piezoelectric Sensors use a non-conducting dielectric (piezoelectric) material which generates a small electric current when pressure is applied from the fingerprint. Ridges and valleys in the fingerprint result in different pressures providing an electrical map of the fingerprint. This is a rather new technology and limited today to swipe sensor implementations

Piezoelectric sensors have not developed sufficiently in performance or cost for commercial viability.

Ultrasound sensing uses echography; sending acoustic signals toward the fingertip and capturing the echo signal. The echo signal is used to compute the range image of the fingerprint and, subsequently, the ridge structure itself. This method images the subsurface of the finger skin; therefore, it is resilient to dirt and oil accumulations that may visually mar the fingerprint.

While good quality images may be obtained by this technology, the scanner is large, expensive, not solid state, and challenging to deploy as a mobile sensor.

Sensor Geometry and Size

Swipe Sensors: In Sweeping or Swipe sensing the sensor surface is a small rectangle (e.g. 5mm x 10mm) whose width is typically larger than the finger, but whose height is just few pixels. As the user sweeps her finger on the sensor, the sensor delivers new image slices, which are combined into a two-dimensional image. Typically capacitive sensors are used in swipe mode but other technologies can be used in this form factor as well.

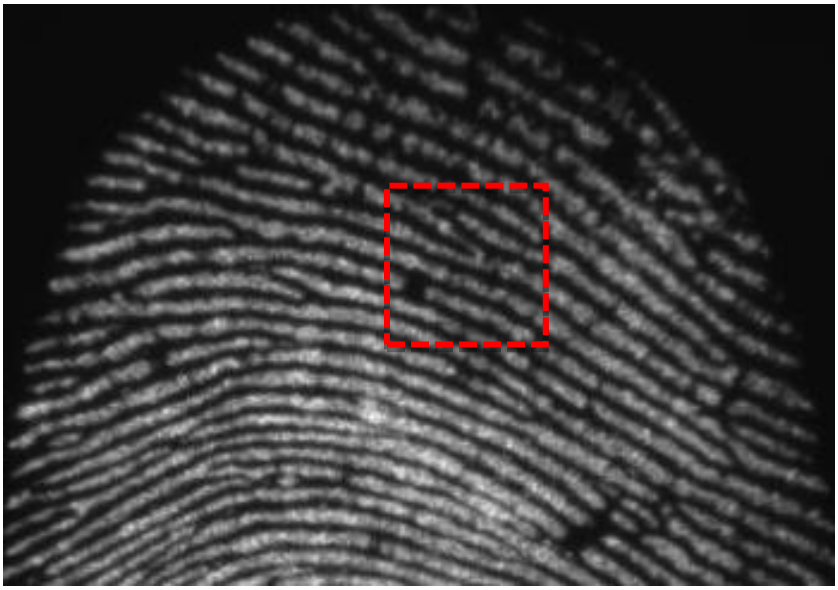
The advantage of this sensing geometry is that the sensor can be very small, allowing for a lower cost sensor. The sweeping motion tends to keep the sensor clean (if necessary) and no latent prints are left behind on the sensor surface.

The disadvantage of this geometry is that the very small sensor area may not repeatedly capture the enrolled fingerprint, requiring repeated swiping to confirm a fingerprint match. Combining swipe images requires a fast interface and computation. Reconstruction of the fingerprint by software can introduce errors. Swipe geometry does not improve the inherent technology's ability to read dry, dirty, oily or wet fingerprints. There are no FBI certified swipe sensors. Swipe sensor images contain random artifacts and do not pass FBI certification requirements.

Area Sensors are flat or curved surfaces where a finger is touched or rolled onto the surface. Multiple readings may be taken while the finger is touching the sensor. Area sensors come in a variety of sizes that may accommodate the width of a rolled fingerprint or even multiple finger or palm images – taken simultaneously. See the certification section for nomenclature of sensor area sizes.

An FAP10 (the smallest FBI certified sensor) is 10 times the area size of the Apple 5S sensor. FAP stands for Finger Acquisition Profile and it defines the specification for that size sensor. The active area of the sensor directly affects the accuracy of the identification or authentication and user experience.

The picture below shows an area of 4mmx4mm (currently the smallest commercial sensor) on larger fingerprint image. In order to gather enough unique detail from the fingerprint to allow authentication, the user must register their fingerprint multiple times in various orientations, so that a challenge reading can be identified as part of the composite fingerprint. Area sensors that are smaller than the fingerprint limit the size of the identification or authentication data base. A 4mm x 4mm sensor is limited to one-to-thousands authentication. For comparison an FAP10 provides one- to-millions identification.



One-to-One (1:1) vs One-to-Few (1:n) vs One-to-Many/Millions (1:N)

Integrated Biometrics LLC, from Spartanburg South Carolina, USA, is the first and only provider of an optical FAP 45, appendix F fingerprint sensor not based on TIR (Total Internal Reflectance) optics. The industry changing advantages of this technology over conventional optical sensors is significant.

The IB fingerprint technology is specifically designed for mobile and hand held tablet markets requiring the collection of high quality, standards based, “certified” fingerprints for large scale programs such as National ID, Military, Public Safety, Law Enforcement, Immigration and Border Patrol applications. In this segment, IB has no serious competition with comparable size, weight, low profile, power requirements, accuracy and of ease of use.

The use of our key enabling fingerprint capture technology gives a system integrator the benefits of the smallest, lightest, highest quality, easiest to use fingerprint collection solution for “certified” large scale applications in the world today.

For markets requiring FBI certified mobile solutions capable of rapid and accurate identification of an individual from databases of millions, Integrated Biometrics is the only technology suitable for the stringent needs of pocket sized devices.

For consumer markets, such as smart phones, fingerprint sensing is used to authenticate the user (not necessarily to uniquely identify). Matching is typically to a data base of a less than 1000. High quality imaging is still important as the size of the area sensor used is considerably smaller than the full surface of the fingerprint. With the advantages of excellent image generation (regardless of fingerprint condition) and image capture, Integrated Biometrics' LES technology also satisfies the extreme requirements of smart phone and tablet authentication. In spite of the LES technological advantages, consumer applications remain price competitive with other technologies.

Regardless of the need for 1-to-few or 1-to-millions matching, Integrated Biometrics LES technology is readily scale-able to any size area sensor from 4mm x 4mm to the large live-scan ten-print of 3in x 3 in.

Fingerprint Enrollment and Matching

Generally the science of fingerprint recognition has 3 levels of details. The first level is called Cahtterjee's scheme or classification of ridge shape. One can also count ridge frequency and look at distances between ridges. The first level requires a resolution at least 200 ppi (pixels per inch) but 250 ppi is better for seeing the fingerprint type at this resolution. There are 7 types and several subcategories under each, e.g. swirl left, swirl right, bull's eye, arch, tinted arch, etc.

The second level of detail is minutia points. This is the most common scheme for fingerprint recognition. This is where special ridge landmarks can be seen such as ridge bifurcation, ridge endings, ridge lone islands, etc. Everyone has about 60 or 70 of these landmarks on their fingers from the first joint out. Each ridge is called a ridge unit with its own shape. These minutia can start to be seen around 300 ppi but to see them clearly you need about 350-400 ppi. Depending on the country, 8-12 of these points are required to <u>legally</u> identify you. Lower than about 380 ppi, you can easily have false minutia and high levels of FRR (false reject rates).

Level three uses the detail of the ridge as identifying points. Also, incipient ridges are considered a level three detail. About 10-15% of a fingerprint is made of these ridges (although some people do not have them). These are immature small ridges between the normal ridge. The ridge itself is composed mostly of sweat pores. Level 3 detail provides no more identification value than level two in most systems where the print in question is whole. However, it is very valuable in forensic science where only a small or partial print is being identified.

Level three detail can start to be seen in low noise systems at 500 ppi. The Integrated Biometrics product, Sherlock, for example, can see these quite well. However, with most systems generating noisy images and artifacts, 800-1000 ppi is required.

Certifications – what does it mean to be "certified"

The United States has a fingerprint image quality specification called PIV which is Personal Identity Verification. There is a certain set of standards that applies to the quality of the image that you must meet to be certified. Those standards are very important to ensure consistency of quality, of usability, and of inter-operability. These standards are managed by the FBI and their testing body, The MITRE Corporation. Most PIV sensors today are either capacitive (silicone chips that have capacitive sensors) or they are smaller optical devices. There is only one capacitive sensor that meets PIV standards. Because of their size and technical accuracy, they are limited in the level of matching. They are primarily meant to do 1 to 1 verification.

The certified-for-searching or the certified-for-enrollment sensor, requires a sensor that is large enough to collect the roll fingerprint and that meets the FBI's highest image quality requirements, called Appendix F. There are two standards that apply to mobile ID in the United States: PIV and the FBI Appendix F. Appendix F certified devices are capable of 1:1 matching but can also handle 1:n and 1:N identification. Experience from the US Government has shown that large databases (N) require the larger size sensors (FAP 30, 45, 60) and multiple finger enrollment in order to accomplish the objective of rapid, post-enrollment matching.

Why is certification important?

Certification provides assurance to users of biometric collection systems that certified products meet or exceed minimum FBI interoperability standards and will work with the Integrated Automated Fingerprint Information System (IAFIS) or other back end AFIS systems used around the world. These standards ensure that the images used in the system are high quality and support all phases of identification for both fingerprint experts and the IAFIS.

What are the standards?

There are two standards currently in use for fingerprints: Appendix F and PIV-071006.

- *Appendix F* has stringent image quality conditions, focusing on the human fingerprint comparison and facilitating large scale machine many-to-many matching operation.
- *PIV-071006* is a lower-level standard designed to support one-to-one fingerprint verification. Certification is available for devices intended for use in the FIPS 201 PIV program.

What device categories are certified?

Fingerprint printers, card scanners, and live-scan devices of multiple types can be certified, based upon the appropriate standards. In all cases, a certified unit is a configuration of specific hardware and driver/support software optimized for usage with fingerprints.

Fingerprint Card Print Systems: Including software that generates 10-print cards of fingerprints, with sufficient image quality to support fingerprint identification/matching. Typical laser writer printing software does not meet the requirements.

Fingerprint Card Scanner. Certification is performed either with or without automatic document feed (ADF). Output resolution is within strict limits of either 500 ppi or 1000 ppi and the high image quality standards imposed by Appendix F apply. There are multiple livescan categories,

which differ in the required collection capabilities (single or multiple fingers, rollscan or flat, and dimensions of capture area) and the image quality required. All optical livescan devices are certified with or without a membrane, where "membrane" refers to a deformable substrate covering the finger platen.

- *'Live-Scan' (Tenprint) System*: Includes capability to collect all elements on a tenprint card, i.e. rollscans, plain thumb scans and 4-finger flats.
- *Identification Flats System*: Includes capability to collect 4-finger and 2-thumb flat impressions in a 3.2 x 3.0 inch area.
- *PIV Single Finger*: Includes capability to collect a single finger flat impression, with a minimum size limitation.
- *Mobile ID*: Devices that can operate in a mobile environment. Only flat impressions are required. The category is sub-divided into several levels by fingerprint acquisition profile (FAP) number, based upon device capture dimensions, the image quality specification applied, and the number of simultaneous fingers that can be captured. Additionally, MITRE has outlined a series of Stress Imagery tests related to the Mobile ID requirements that are used to define the performance of certified scanners. These Stress Imagery tests include working in direct lighting or sunlight and working with dirty fingers.

The following table summarizes the basic categories with overview information on the specification applied and types of images involved. See the specification documents themselves for exact details.

Certification Category	Specification	Capture Dimension (WxH inches)
Fingerprint Printer	Appendix F	
Fingerprint Card Scanner	Appendix F	8 x 5
Live-Scan (Tenprint) System	Appendix F	1.6 x 1.5 roll 3.2 x 2.0 flat
Identification Flats	Appendix F	3.2 x 3.0
PIV Single Finger	PIV-071006	0.5 x 0.65
Mobile ID (see below)		
FAP 10	PIV-071006	0.5 x 0.65
FAP 20	PIV-071006	0.6 x 0.8
FAP 30	PIV-071006	0.8 x 1.0
FAP 40	PIV-071006	1.6 x 1.5
FAP 45	Appendix F	1.6 x 1.5
FAP 50	Appendix F	2.5 x 1.5
FAP 60	Appendix F	3.2 x 3.0

Extra capabilities such as palm capture require larger capture areas, but are only tested in conjunction with another category already on the list (e.g. Live-Scan, ID Flats or FAP 60).

What device configurations are eligible for Mobile ID certification?

Mobile ID devices operate in a mobile environment. Mobile ID devices operating in that environment may exhibit functionalities beyond those specified by their own set of requirements (Appendix F or PIV) based upon the Captured Dimensions referred to in the above table.

The following examples are currently found on the Certified Product List (CPL):

- Mobile ID devices of FAP 45 and above which have been tested as capable of capturing optional rolled as well as plain fingerprints are labeled as such in the CPL with the wording “roll/plain” or “plain/roll”.
- Mobile ID devices of FAP 45 and above can also be, upon request, tested for PIV certification (if they will be used in the FIPS 201 program). When successful, such devices meet both Appendix F (under the Mobile ID certification category) and PIV specifications. Requesting both certifications at the same time shortens the duration of the dual assessment when compared to two sequential requests.
- Mobile ID devices of FAP 40 and below can request an independent PIV certification.
- Mobile ID devices which are capable of transmitting minutia points in addition to transmitting images, but which offer a choice in sending either one, are only certified when the image transmission mode is selected, whereby the mention “when used for [fingerprint] image transmission.”
- Mobile ID devices whose designs produce adequate images of impressions under the lighting conditions encountered in a windowless laboratory or office (approximately 500 lux), but whose quality drastically degrades below the point of usefulness under intense lighting conditions (at least 90,000 lux), are likely to receive the mention “not appropriate for use in direct sunlight.”

What else should be considered when choosing a device from the Certified Product List (CPL)?

A certified unit corresponds to a specific combination of hardware and software configured together to deliver images of impressions that are palatable to both examiners and IAFIS/NGI. The conditions under which such images are generated during certification tests are almost ideal because it would be both onerous and costly for vendors to replicate all conditions under which end users may use their products. Therefore, end users are encouraged to consider the following discussion topics with vendors, topics that are among those not covered by IQS certification (this list is by no means comprehensive):

- Research the hardware and software architecture into which the device would be integrated, including connectivity (in addition to electrical compatibility, one should ask vendors about device drivers, especially with aging architectures).
- Research the security rules (Information Assurance) that are applicable to the architecture, including devices which communicate with and/or connect to it.
- Articulate a range of intended operating conditions under which the device would be used (for instance: outdoor environmental conditions for Mobile ID devices; livescanners placed behind a window exposed southward; inmates with tattoos over their fingers/palms; or that end users should have at least one hand available during the entire capture process).

What is the difference between the specifications?

- *Appendix F* has the most stringent image quality specifications, focusing on the human fingerprint comparison and facilitating large scale machine many-to-many matching operation.
- *PIV-071006* is a lower-level specification designed to support one-to-one fingerprint verification.
- *Appendix G* is a deprecated standard that has not been tested against since 1999. It is of lower quality than Appendix F, and is missing some requirements present in PIV-071006.

About Integrated Biometrics

Integrated Biometrics provides enrollment and verification fingerprint sensors to hardware integrators, software and database providers, and contractors serving government agencies and commercial markets worldwide. More ideal for mobile environments than traditional silicon or optical sensors, Integrated Biometrics FBI-certified fingerprint sensors utilize our durable, patented light emitting sensor (LES) film and work in direct sunlight on dry or moist fingers, resist abrasion, and are 90-95% smaller and lighter than optical scanners. Integrated Biometrics offers the only Appendix F FBI-certified sensor that meets mobility requirements demanded by end users, solving the major problems of size, speed, accuracy and durability. Find out more online at www.integratedbiometrics.com.