Getting Started - Mobile Biometrics

David Benini

Vice President, Marketing I Aware, Inc.

September 2013 Update

planet
biometrics

Welcome to Planet Biometrics' In Focus page on mobile biometrics. While use of mobile biometric solutions has evolved in step with the larger biometrics market for some time, the growing ubiquity of smart phones and the rapid and dramatic improvements in their features and performance are accelerating the trend. As a result, mobility is becoming an increasingly important part of the biometrics landscape. The time is right to take a closer look at mobile biometrics, and to investigate in greater depth how they can be used to their full potential.

The purpose of this article is to initiate a dialog that ultimately establishes a useful and up-to-date source of information about mobile biometrics. We'll continue to add new content, with particular interest in learning about new technologies and products, and how they are faring in the field. Hopefully in the process, we as an industry can educate potential users about what's possible and also learn about what users are looking for.

Getting us started on the topic, we'll take a quick review of biometrics, and get squared away on our technology fundamentals and terminology. We'll then discuss the current state of the mobile biometrics market: applications, form factors, workflows, and products. We'll finish up with a look at what's on the horizon in mobile biometrics and speculate on what might be headed our way. Please feel free to contact me with ideas and material that can help educate the market with fresh information.

September 2013 Update

In the months since this white paper was first posted, there have been several developments that suggest we are on the cusp of a surge in mobile biometric technology adoption. In July 2012, Apple acquired fingerprint sensor manufacturer Authentec. As we approach the anticipated iPhone launch date, rumours abound, but consensus seems to be that the iPhone will in fact include a sensor. There is further consensus that if Apple can successfully integrate a fingerprint sensor into a smart phone, we can expect to see rapid growth in use of biometric-based smart phone applications that did not follow their broad integration into laptops several years ago. We can also anticipate that application developers to quickly find fresh and innovative ways to make use of the sensors towards improved security.

On another important front, the US Government has provided seed funding to private industry towards improved cyber security; to essentially find alternatives to passwords to better secure our online interactions. This comes in the form of "NSTIC", created and administrated by NIST to launch an open industry working group "IDESG" tasked with envisioning a new "identity ecosystem". The goal is to specify models for secure online transactions for a wide range of applications in several verticals. Mobile solutions are on the forefront, and biometrics will play a role. On a similar mission, the FIDO Alliance has defined a model utilizing existing security standards that proposes to eliminate passwords altogether.

It's expected that over the course of the next year, we will see these market dynamics converge to drive the introduction and adoption of biometrics–based applications and solutions for smart phones. We can only imagine what people will come up with, but it promises to make 2014 an interesting year for mobile biometric solution providers.

Why go mobile?

Mobile biometrics are about achieving biometric functionality with portability. Achieving portability means trading one set of physical constraints for another; we trade the power of computer workstations, reliability of power outlets and Ethernet jacks, and predictability of an office-like environment for portable, miniaturized capture and computing hardware in convenient but potentially non-ideal, unpredictable environments.

Why is mobility important for biometrics? Biometric tasks can't always be performed in a controlled environment. Biometrics need to go where people go... outside or in public spaces, for example, and they might be needed somewhere different each day. Achieving mobility while maintaining sufficient biometric performance is difficult, but the challenges are not unlike those associated with other familiar mobile technologies (laptops and cell phones): power consumption, security, durability, reliability, portability, ergonomics, processing power, and connectivity.

Biometric Applications

The first application of biometrics was for criminal investigation and law enforcement: to use "latent" fingerprints found in a crime scene to help identify who might have left them behind. Today this application remains an extremely important one, but with the help of modern digital computing we've also learned to use biometrics for another very useful purpose: to establish trust in a person's identity. Modern biometrics, at their core, are about using an individual's physical characteristics or behaviour to generate a set of numbers that can be used (with the help of a computer) to uniquely identify them consistently over time. Establishing trust in identity—proving we are the person we say we are—is useful. Being able to do so with mobility is even more so, and this is the focus of our article.

The biometrics pie can be sliced in many ways, but here we'll divide the space by application into three parts: 1) access control, 2) watchlist checking, and 3) duplicate checking:

Access control involves securing access to either a physical asset, such as a room or building, or to a digital asset, such as a computer application or database. Biometrics can be used to enhance access control by performing a mathematical comparison of a person's live biometric sample to a trusted stored sample. This stored sample might reside either in a central database or on a credential such as a smart card ID. This process can be called a "one-to-one verification" of an individual's biometrics. In this way, we can "authenticate" the assertion of a person's identity, answering the question "are you really who you claim to be?" and using the comparison result to either grant or deny their access to a particular asset. Use of biometrics for access control is of particular interest for commercial or personal security applications. Mobility is useful for some access control applications; perhaps most notably physical access control to a secure perimeter such as a nuclear plant or corporate research facility.

Watchlist checking is a very different process that serves to assess whether an individual's biometrics are stored in a database of "persons of interest". In this process, an individual's live biometrics are submitted to a biometric search system for "one-to-many identification." The system mathematically compares the live "probe" sample to many samples in a "gallery" of persons-of-interest in a watchlist. In doing so, we can identify an individual even if they are not truthfully identifying themselves. Watchlist checking is performed most often by governments for a variety of purposes where trusted identity is important, including criminal investigation and law enforcement, visa issuance and border management, employment screening, and defence. Again, mobility is potentially useful for these applications, such as when potential persons-of-interest are encountered outdoors.

Duplicate checking is yet another biometric process performed to determine whether there are individuals represented more than once in a database. This might be performed to detect fraud, such as in the case where an individual has enrolled multiple times in a social benefits program. This process involves matching every biometric sample in the database to every other, and could be called a "many-to-many duplicate search." Duplicate searching is a centralized function that does not require mobility.

Biometric Processes

Enrolment

Biometric systems rely on two distinct processes: enrolment and comparison. The purpose of enrolment is to capture and store the biometric samples (e.g. on a smart card or in a watchlist) that will be used for future comparisons with live samples. Enrolment of high-quality samples can contribute to enabling a sufficient level of matching performance, which is particularly important for one-to-many identification tasks. Enrolment may be performed on a mobile device if necessary, but is typically done on a stationary workstation if possible.

Comparison: extraction and matching, interoperability and performance

Comparison of biometric samples involves two computations: template extraction and algorithmic matching. First, a numeric representation of the biometric sample called a 'template' is generated. This template is then algorithmically compared to other templates, yielding a match score. In most cases, these templates are proprietary and can't be used with comparison algorithms from different vendors. This can be important in mobile systems where the extraction and matching processes take place in different locations. For example, templates can be stored on a smart card, and then matched later on a mobile device. MINEX-certified minutiae-based fingerprint template generators and matching algorithms were designed for this application; they have been tested and verified to be interoperable between different vendors for one-to-one verification applications.

A high-performance biometric system is characterized by a low rate of false matches and false non-matches. Generally speaking, higher quantities of data (e.g. more fingerprints) and higher-quality samples are required for one-to-many and many-to-many processes than for one-to-one verification. It is helpful to understand that a mobile one-to-one verification solution will not have as stringent biometrics sample quality requirements as a one-to-many identification. In some cases, the enrolment might take place at a stationary workstation, with only the verification or identification process requiring mobility. For example, an access control application might require a new employee to submit biometrics in a controlled environment as part of a new-hire introduction process, but then need to submit biometrics using a mobile device when attempting access at a control point somewhere on the property perimeter.

Modalities, Hardware and Software

Much is made about the breadth of biometric modalities, and indeed some of the research into new, more exotic biometrics (ear, gait, odor, etc.) is compelling. But the “big three” modalities that are field-proven and currently in use are fingerprint, face, and iris. Each is currently used extensively in mobile applications. In a mobile context, voice is also important, given the inherent audio capture and playback capabilities of a smart phone. There is no perfect biometric; each has advantages and disadvantages, such as having more reliable matching performance, or being easier to capture. Some mobile approaches are multi-modal, incorporating more than one modality and utilizing “fused” match results.

All biometric solutions include hardware and software components, and many include both client- and server-based components. Mobile biometric hardware includes capture peripherals, power source, network interface, and computing platforms. Mobile biometric software includes a user interface, peripheral interface, biographic data capture and validation, biometric image capture and processing workflow, and biometric template extraction and matching. Mobile capture solutions vary in the degree of required miniaturization and portability, and as such sometimes use the same hardware and software components as for stationary solutions.

Hardware

Fingerprint sensors are currently designed upon either one of two technologies: optical and capacitive. Capacitive sensors can be either full-finger or swipe. It is important for fingerprints to be of sufficient resolution (500 ppi) and contrast, and be free of distortion. An optical sensor uses a prism, light source, and light sensor to capture images of fingerprints. Capacitive sensors are based on a silicon chip that detects electrical currents when the finger ridges make contact. Optical sensors generally provide higher-quality images than capacitive sensors but are also larger and consume more power. Full-image capacitive sensors generate higher-quality images than swipe sensors but are also larger. Swipe sensors do not generate image quality sufficient for one-to-many identification.

Capture of facial images has traditionally been performed using off-the-shelf consumer-grade digital cameras such as a Canon PowerShot. But camera technology has changed dramatically in only the last several years, making facial capture with mobile devices far more viable. We have all seen the vast improvements in image quality of web cams and smart phone cameras, many of which are now capable of eight megapixels or more. This is compelling, considering that the best digital cameras on the market were on the order of four megapixels only five years ago. Digital facial images traditionally require an interocular resolution of about 60 pixels for one-to-one matching and 90 pixels for one-to-many matching. But resolution is not the only factor affecting facial matcher performance; perhaps even more important are the distortion, brightness, contrast, sharpness, and background clutter of the image. Improvements in these areas have not been as dramatic with smart phone cameras as resolution, but improvements are nevertheless compelling. But the challenge here is less with the camera performance and more with the fact that with mobile solutions, the capture conditions are highly variable as compared to stationary environments; lighting, background, and distance to the subject can change from photo to photo, and have a substantial impact on matching performance. In mobile facial image matching systems, it is helpful to keep photo capture conditions as consistent as possible.

Iris is probably the fastest growing biometric modality, and has also benefitted from the dramatic changes in the camera and sensor arena. But iris differs from face in that it requires an infrared image of the iris. The degree to which a pure infrared image can be captured (with minimal "pollution" from visible light), the better the matching performance. This is why off-the-shelf cameras aren't used for iris image capture, and a special camera is required; a system must illuminate the iris with infrared light and then filter out other wavelengths.

Voice biometrics are a particularly viable means of one-to-one verification using a smart phone, given its obvious audio capabilities. But in this application mobile voice biometrics suffer from the same challenges as other biometrics in that the environment is unpredictable; background noise can interfere with the matching process just as the background of a facial image can. Voice samples (such as those collected from a surveillance device) can be used as a "latent" like fingerprints, and the background of voice signals can also have forensic value for law enforcement and military applications.

A different take on mobile biometrics is "biometrics in motion," where biometrics are taken of an individual in motion using stationary equipment. There are several systems available for this application and are desirable for their speed and low degree of interference with a person's activity. Facial and iris biometric systems are available, and fingerprint systems are currently in advanced research stage.

Hardware challenges: durability, ergonomics, power consumption

Capture hardware must be designed to accommodate a wide variety of environmental and ergonomic factors particular to mobile devices used outside an office environment. They must operate in direct sunlight, temperature and humidity extremes, and by operators with gloved fingers. They must be sufficiently durable to withstand moisture, dust, dirt, and impact. Power consumption is a significant factor and is very use-case specific, but typically a device must operate reliably by battery power for at least one work-day. A consideration is whether batteries can be replaced on-the-fly, or whether the entire device must be offline during a battery charge. Biometric capture peripherals often require lighting, and one-to-many search software can consume processing. They must be ergonomically designed such that an operator can quickly and reliably collect high-quality biometric samples from inexperienced or even uncooperative individuals.

Software

Software for mobile capture is functionally similar to stationary biometric solutions, but with meaningful differences. Mobile devices typically run operating systems designed for smaller devices, such as Windows CE, Windows Mobile, Apple iOS, Blackberry, and Android, so biometric software libraries need to be ported to these operating systems. Processors are less powerful, and there is less memory and RAM, so processing-intensive operations such as compression and template extraction must be optimized appropriately. Video screens are smaller and utilize touch screens and gestures, so the user interface must be designed to accommodate these. Special software is applied to help make up for shortcomings of the hardware, such as by providing more advanced image processing and quality control. Some more powerful mobile devices such as those used in the military run Windows XP but still need software that accommodates a small touch screen and less processing power.

Device independence is a particularly important consideration in implementing a mobile system. Ideally, an owner of a system can support different kinds of mobile devices in their system so that they are not reliant on a single vendor for devices. This can be achieved by requiring that an open, standards-compliant interface be implemented between the device and wherever the trusted sample is stored (i.e. a smart card or central server). Another approach is to operate a hardware-agnostic software application on the mobile device. The advantage here is that different hardware devices can be used in the system and can be procured separately, but the software, user interface, workflow, etc. are the same.

Security

Security is of particular concern in mobile biometric solutions because physically securing access to the device is much more challenging. Biometric data on a device needs to be protected for purposes of personal privacy, because it is possible though not trivial for a stolen biometric to be used to generate a false identity and spoof the system. Biometrics may also be accompanied by sensitive, private biographic data. It is typically desirable to keep confidential the individuals listed on a watchlist, so this data must also be kept private; a compromised mobile device could be used by an adversary to learn whose biometrics are on the watchlist, or to enroll false information. Storage of templates as opposed to images can be effective in helping secure biometric data because it is difficult but not impossible to spoof a live sample from template data.

For these reasons, particular care is given to securing mobile biometric capture solutions by securing 1) data at rest on the device, 2) data in motion on a communication network between the device and central system, and 3) data in system, such as stored on a central server and accessible by the device. Enhanced security is achieved through traditional means, such as password- or biometric-controlled access to the software application, encryption of data at rest and in motion, and firewalls. Watchlists stored on mobile devices can be encrypted, but will reduce the speed with which identifications can be performed, a factor for particularly large watchlists stored on the mobile device.

Match Modes and Networks

Owner-based, permission-based, operator-based, kiosk-based

An “owner-based” biometric application is one by which a single person (or a few) is using a mobile biometric device to secure access to their own assets, such as the device itself. A “permission-based” system involves the controller of an asset to grant self-access to an asset, (e.g., a company using biometrics to grant employees access to their data). “Operator-based” applications require an authorized, trained operator of the device to collect biometrics from the individual providing the biometric sample. “Kiosk-based” applications can be semi-mobile and require capture to be performed without any training or experience and minimal instruction. These are important distinctions in designing a mobile solution because they have an impact on its ergonomics and workflow, and users of the device will not necessarily be located where assistance is readily available. Will one person or two require simultaneous access to the device? Must a person be trained to use it?

Match onboard, match-to-chip, match-to-code, match-to-server

One-to-one and one-to-many biometric matching can be performed onboard the mobile device in any of several modes; security, watchlist size, and required response time are often the considerations in their design and selection. A live sample must be compared to a trusted sample stored either on the device itself, in memory on a smart card, or encoded in a bar code. Each approach presents different pros and cons and depends on the application; importantly it must be feasible to securely enroll, encode, and store the trusted sample in the location of choice, and then retrieve the sample upon matching, whether it be on the device, card, code, or server. Bar codes can be used to store biometric templates, such as specified by the ILO Seafarers' identity document technical report ILO SID-0002. Biometrics can also be stored in a smart card (e.g. PIV card) and retrieved by the mobile device via the contact interface. Ideally, interoperability is facilitated by using standards-compliant products. FIPS 201 for Personal Identity Verification (PIV) is a standard that specifies biometric smart cards and systems and is in broad use.

Mobile biometric devices are often equipped with mobile connectivity via Bluetooth, Wi-Fi, or GSM/CDMA network. With connectivity, mobile biometric matching can be performed between live samples and trusted samples or watchlists stored somewhere else in a network. The feasibility of such an architecture is determined by the reliability, speed, security of the network, and sensitivity of the application. Image-based biometric samples can be somewhat cumbersome to transport in a mobile system; compressed samples are typically on the order of 10 to 20 Kbytes each and vary widely between modality and vendor, so it's an important consideration in system design. If matching to a watchlist residing on a mobile device, a mechanism must be implemented that is capable of updating the watchlist on the device. This can be done over a wireless network, but depending on its size can be prohibitively time consuming. Another option is to update the watchlist while the device is connected to a wired network, such as during a battery recharge.

Mobile Biometrics Form Factors

As discussed, mobile biometric devices take many forms and are designed to facilitate a wide range of applications and usage environments. Following are some product categories and a list of products that is by no means exhaustive. A summary is provided at the end of the paper.

Integrated. This form factor is comprised of a traditional mobile device that is equipped with one or more integrated capture devices. Examples are laptops or mobile phones equipped with Authentec Mobile Smart Sensors, and web cameras.

Handheld. This is a device that is custom designed specifically for biometric capture. It will incorporate capture peripherals for one or more modalities, a CPU, network connectivity functionality, and human interface devices such as touch screen and/or keyboard. They have custom software applications that enable the user to operate the device. Examples are the Iris ID iCAM H100, 3M Cogent BlueCheck II, and MorphoIDent.

Suitcase. This form factor utilizes a laptop and traditional biometric hardware peripherals that are organized into a compact, hardened, portable suitcase. They are generally somewhat configurable, enabling the selection of either one or several modalities; e.g. single finger optical scanner or slap scan device. An example is the Cross Match Guardian Jump Kit.

Kiosk. A kiosk is generally semi-portable, with integrated biometric capture components, document readers, and other peripherals; they are often designed to enable self-enrolment and verification. Examples are Speed Identity G3 and SmartMatic PARmobile.

Ruggedized. A ruggedized mobile solution is designed specifically for military and law enforcement applications, and is thus designed to capture high-quality data suitable for identification while being extremely durable and reliable. Examples are the Cross Match SEEK II, MorphoTrust HIIDE 5, and Northrop Grumman BioTRAC.

Smart Phone and Tablets. Modern smart phones and tablets are equipped with powerful processors, multiple high-quality cameras, network connectivity, and intuitive user interfaces. They can be equipped with biometric capture peripherals and integrate with server-based systems to provide an advanced mobile biometric solution. Examples are the Apple iPod Touch equipped with the Fulcrum Biometrics mobileOne, and the Apple iPad equipped with the SIC iFMID 500 .

Mobile Applications and SDKs. Some solutions are hardware-independent software programs or software development kits designed to operate on different hardware devices. An example is Aware URC Mobile, designed for ruggedized devices.

Mobile Infrastructure. An infrastructure solution is designed to support use of mobile devices to achieve authentication or other biometric functions. They typically include both device- and server-based software and are largely hardware-independent. Examples include Daon IdentityX and Aware Biometric Services Platform (BioSP).

Biometrics in Motion. “Biometrics in motion” are enabled by stationary systems that enable biometric capture from subjects who are themselves mobile, such as when they walk through a gateway. An example is SRI/Sarnoff Iris on the Move.

On the Horizon - Emerging Trends

What does the future hold for mobile biometrics? It is fairly clear that smart phones and tablets will be the most fertile area of biometric innovation for the next several years. The devices will continue to become more powerful, and the market will likely have on the order of 100 biometric solutions designed around smart phones and tablets within 18 months.

Smart phones will be able to communicate with smart cards via near field communication, which will enable them to authenticate a live biometric sample with a template stored on a smart card. Standards compliance will be a key driver of adoption of this technology.

But general-purpose mobile devices will never be able to fulfil all requirements for all biometric applications. Identification of a biometric sample within a large gallery will require capture of a lot of high-quality biometric data, and this won't ever be practical on a device designed to perform such a breadth of consumer-based applications. There will be a role for these devices in defence and military applications, but it will likely be limited to one-to-one verification for access control or humanitarian missions. Durability will remain a critical factor for many applications where reliability is required.

Following is a product summary; feel free to contact me to add your product to the Mobile Biometrics In Focus web page.

Product Name	Product Vendor
Integrated	
Sherlock	Integrated Biometrics
VFS	Validity
FPC	Fingerprint Cards
OEM Modules	Digital Persona
Handheld	
iCAM H100	Iris ID
3M Cogent BlueCheck II	3M Cogent
MorphoIDent	MorphoTrust
Stratus	AOptix
Suitcase	
Guardian Jump Kit	Cross Match
Kiosk	
G3	Speed Identity
PARmobile	SmartMatic
Ruggedized	
SEEK II	Cross Match
SEEK Avenger	Cross Match
HIIDE 5	MorphoTrust
BioTRAC	Northrop Grumman
Smart Phones and Tablets	
mobileOne	Fulcrum Biometrics
iFMID	SIC
Tactivo	Precise Biometrics
Mobile Applications and SDKs	
URC Mobile	Aware
Onyx	Diamond Fortress
Mobile Infrastructure	
Biometric Services Platform (BioSP)	Aware
IdentityX	Daon
Biometrics in Motion	
Iris on the Move	SRI/Sarnoff