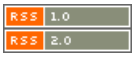
New Articles

- Opinion: Processing Burglary Scenes for DNA
- The Evidence is in the Bag
- Forensic Imaging and RAW Files
- Shooting-Incident Reconstruction Within a Room
- Mobile Biometrics

Latest News

- WANTED: Story Ideas
- Find ETM on Facebook
- ETM Now on Your iPhone or iPad
- How To: Logging In to ETM Online
- Welcome to the new Evidence Technology Online!

RSS Feed



Mobile Biometrics

Written by Kristi Mayo

MOBILE BIOMETRICS:
The potential for real-time identification in the field

IN RECENT YEARS, increased computing power and carefully crafted algorithms have made it possible to automate the quick and accurate detection of patterns of similarity in many different things—from fingerprints, faces, and irises, to foot-wear, license plates, and even tattoos and scars. This technology is continually evolving and offers promising potential to the law-enforcement and identification community.

Additionally, as technology and hardware becomes smaller and more portable, companies that specialize in biometric identification have brought a powerful breed of tools to the law-enforcement and military markets: mobile multi-modal biometric devices. These gadgets capture ten fingerprints, the face, and the irises of both eyes and then use that data to confirm an individual's identity. Mobile multi-modal biometric devices are proving themselves highly useful at booking stations, in prisons, in the cars of patrol officers, and on the battlefield.

Those applications primarily deal with verifying an individual's identity. But can that same mobile biometric technology be utilized in a way that would be useful to the crime-scene officer or investigator?

To answer that question, it is helpful to look at what the current technology offers. All of the multi-modal biometric devices feature the gold standard in human identification: fingerprints. They can capture ten prints from a subject and then transmit those prints to an automated fingerprint identification system (AFIS) for real-time identity verification, and some can perform real-time comparisons using a database contained within the mobile device.

Facial recognition is another feature offered on many of these mobile biometric devices. A cooperative subject is photographed using the mobile device, and that image is compared to a database of mug shots located either in the mobile device's onboard memory, or can be transmitted back to the agency's database for comparison. Results of facial-recognition procedures can be used secondarily or complimentary to conventional finger-print identification.

Some mobile biometric devices also allow the capture of a photographic image of the iris to aid in identification. Overall, iris recognition has proven to be highly accurate. However, very few agencies in the United States currently have large, searchable iris databases. The technology is being used more extensively internationally—particularly at border crossings and airports—and the use of iris-scan technology is expected to continue to grow as a way to verify identity.

In addition to these three forms of biometrics for identity verification, mobile multi-modal biometric devices also utilize secure wireless connections with the law-enforcement agencies' servers. This established communications infrastructure is important to note, since any forensic applications of these mobile devices would demand absolute security when transmitting data to and from the agency's server.

Moving from verification to identification

When you take a critical look at the three major forms of biometrics available on mobile devices—fingerprint, face, and iris—it does not take long to figure out which one is the best candidate for forensic applications.

Iris recognition has proven itself to be remarkably efficient and accurate. But for forensic applications, it has one major and obvious flaw: "A criminal does not leave 'iris prints' behind them at the crime scene," said Teresa Wu, marketing director for Cogent, Inc. "They leave traces of DNA. They leave latent prints. But iris I have not heard of yet."

Facial recognition falls short in forensic applications because of the limitations of the technology.

"Law enforcement has noted in the past that facial images can change so drastically over relatively short periods of time," said Mike Oehler, vice president of mobile-biometrics product management for CrossMatch Technologies. "Facial matching is a good tool for use in certain situations. Law enforcement can use it successfully because they can control the circumstances around mug shots—enabling them to take an image of a live, cooperative subject and match it against the database. But for evidence purposes, typically it is difficult to get good, quality facial images from security cameras—unless you get lucky."

Product News

Six interchangeable LED lamps highlight the features of the OPTIMAX Multi-Lite Forensic Inspection Kit from Spectronics Corporation. This portable kit is designed for crime-scene investigation, gathering evidence, and work in the forensic

The last available mobile biometric technology remaining is fingerprint comparison. And there, experts say, lies some definite potential for further development. Specifically: mobile latent capture.

“We are at the point of stepping forward with this technology to enable a crime-scene investigator to capture latent prints at the crime scene with a mobile device and then launch a latent search on the AFIS,” said Wu with Cogent. That company currently offers the Fusion device, a handheld biometric tool that can capture an image of a latent print at 500 or 1,000 ppi (depending on the model).

Although the ability exists to capture an image of the print, the ability of the Cogent Fusion to launch a 360° latent search is still in the field-testing phase. This capability will soon be available to crime investigation teams.

“This is cutting-edge technology, because it requires an AFIS on the backend to be able to process it, with an algorithm robust enough to do lights-out processing on the latent with limited expert intervention,” said Wu.

“Plus,” she added, “not all latent prints can be captured at the scene. Sometimes you need to bring the evidence object back to the laboratory to develop the print.”

Tony Misslin, product manager in L-1 Identity Solutions’ biometric division, expressed similar concerns for the quality of latent images captured in the field. “L-1 has demonstrated that it is feasible to capture a latent print using the cameras on a mobile device. However, we have yet to prove the image quality will be equivalent to those captured with the forensics equipment currently used by criminal investigation service (CIS) agents,” he said. “One potential concept is to use the current CIS process, but add the capability to transfer the latent prints using mobile identification systems. The L-1 IBIS mobile identification system can transmit the image by scanning the latent after it has been transferred to a plate, or by using the digital image captured by forensic cameras.”

The potential benefit of capturing a latent at the crime scene and immediately launching a mobile latent search from the field is the amount of time it would save in the investigation.

“Latent searches do take longer than a fingerprint search. Total search time, of course, is dependent on the database size and the wireless transmission bandwidth you are using,” said Juan Martinez, product manager for MorphoTrak. “But that is the goal: to get the results back, while the case is hot, and see if you can identify and start looking for suspects right away.”

MorphoTrak currently offers the RapID, a mobile biometric identification terminal that allows real-time AFIS searches for identification verification. Martinez said the company is currently working with government agencies to develop a way to capture latents in the field, building upon the infrastructure that is currently in place for law-enforcement agencies.

As with many other technologies, mobile latent capture is likely to see its first successes on the battlefield. Oehler with CrossMatch said the United States military expressed a strong interest in enabling their personnel to capture latent prints in the field. The company responded by repurposing the iris camera on the SEEK (Secure Electronic Enrollment Kit) mobile device to take forensic-quality images of latent prints at resolutions above 500 ppi.

“The military wanted the ability for personnel in Iraq or Afghanistan to capture latent images off unexploded ordinance, improvised explosive devices (IEDs), or the equipment used to trigger IEDs. When they take people into custody, they want to use the SEEK to capture latent prints off of PCs, cell phones, or any other kind of equipment they confiscate out in the field,” said Oehler. “The latents they capture can be entered into any AFIS, or they can be stored on the SEEK. That way, if a local is being vetted—for working on the military base, for example—even if they do not have a history, their fingerprints can be checked against that latent database.

“That ability to capture latents and match latents in the field for identification purposes is exactly what we are currently rolling out to the military right now.”

Using the fixed focal-length camera already equipped on the SEEK, military personnel can take an image of a print that has been developed with dark powder on a light surface, or light powder on a dark surface. Images are captured using full ambient light. Oehler said that the hood used to block bright light from the iris camera also works well to block harsh light when photographing prints.

Oehler added that correct orientation of the latent fingerprint will produce better results in most AFIS searches. “If you have a print patch that you have captured as a latent and you really have no clue as to how it was orientated, it takes a large amount of computing power to match every finger of a suspect against that latent patch,” said Oehler. “It really is a matter of the skill of the operator—not so much to capture the latent image, but to orient the latent image. With some control over that orientation, we are able to get some results that are meaningful.”

To further help in orientation and sizing, CrossMatch is beginning to equip their SEEK kits with adhesive scales that can be put down next to the latent for more accurate sizing. MorphoTrak is working on a similar concept for their latent-capture solution currently under development.

As manufacturers work to make the mobile devices increasingly user-friendly and accurate in the capture of latent images, one hurdle remains: true “lights-out” AFIS searching capabilities. Currently, those searches are growing more robust, requiring

laboratory. The LEDs provide six single-wavelength light sources, each useful for specific applications, from bodily fluids to fingerprints. The wavelengths are: UV-A (365 nm), blue (450 nm), green (525 nm), amber (590 nm), red (630 nm), and white light (400-700 nm). The cordless flashlight weighs only 15 oz. To learn more, go to: www.spectroline.com

Read more...

less effort from latent-print examiners in actions such as orienting the print and marking distinguishing features of a latent print. Advanced versions of these technologies undergo continued examination and validation. In the meantime, the results of these searches launched from the field remain under the watchful eyes of experienced latent-print examiners.

Kristi Mayo can be reached by e-mail at
kmayo@evidencemagazine.com

ORIGINALLY PUBLISHED:
"Mobile Biometrics: The potential for real-time identification in the field," written by Kristi Mayo
July-August 2010 (Volume 8, Number 4)
Evidence Technology Magazine
Buy Back Issue

Return to the August 2010 Featured Products & Services Main Page

< Prev **Next >**

[Back]