EXECUTIVE BRIEF

Capture > Liveness > Matching:

Biometric Performance Metrics for "Real World" Commercial Applications

What is Multispectral Fingerprint Imaging?

Multispectral fingerprint imaging uses patented optical technology to reliably capture images of the finger using multiple colors of light from different angles. This unique approach consistently captures better fingerprint images than other optical or electrical fingerprint devices in "real world" conditions. Multispectral imaging captures both the "external print" on the skin's surface and the "internal print" or subsurface capillary information. Together, they significantly improve usability and confirm liveness.

In commercial biometric applications, customers want ease of use, availability, and convenience as well as high security.

Commercial organizations in today's challenging identity fraud landscape need proven biometric solutions that authenticate users in real situations, with convenience and security.

Challenge: Increased Identity Fraud Drives Demand for Security — and Intuitive User Experience

Despite significant efforts by global commercial organizations, identity fraud incidents and losses continue to grow:

- In 2017, Javelin Strategy and Research found that $16.8 billion was stolen from 16.7 million U.S. consumers. The same study confirmed that bank account takeovers losses reached $5.1 billion, a 120% increase from 2016. In the UK, CIFAS, a non-profit fraud prevention membership organization, estimated that identity fraud losses cost 5.4 billion £ per year.
- In 2017, ACI Worldwide concluded that 30 percent of consumers globally have experienced card fraud in the past five years. Mexico, Brazil and U.S. currently lead the world in consumer fraud incidents.
- A 2017 Ponemon Institute study found the average consolidated total cost of a data breach is $4 million. Each lost or stolen record containing sensitive and confidential information increased from a consolidated average of $154 to $158. In addition to cost data, the global study puts the likelihood of a material data breach involving 10,000 lost or stolen records in the next 24 months at 26 percent.

Despite these evolving security threats, consumers demand intuitive and easy-to-use interfaces from the organizations they entrust with their personal and financial data. In order to meet these two seemingly opposing goals—security and convenience—banks, healthcare providers and other businesses are turning to biometrics. This Executive Brief covers some of the most important factors to consider when evaluating the performance of commercial biometric solutions.

How to measure Biometric Performance for "Real World" Commercial Applications

Expectations for biometric solutions in commercial applications differ widely from those intended for law enforcement and other government uses. With biometric usage growing in banking, healthcare and enterprise access, government-oriented metrics for biometric performance don't fit these commercial needs. Commercial biometric authentication, while focused on preventing identity fraud, must first consider the customer experience,

Novetta, an advanced analytics company experienced with Biometrics and Identity Intelligence, recently developed a performance-based framework to assess fingerprint biometric technology in commercial applications. This framework focuses on the needs of commercial applications, where customer experience and identity fraud prevention are prioritized above biometric algorithm accuracy or complying with biometric device standards. Without an excellent customer experience, commercial organizations deploying biometric systems risk damaging their brand and reducing customer loyalty.

Considering a variety of requirements for public-facing commercial applications with traditional security-based evaluation methodologies, Novetta developed a new biometric performance criteria framework that takes into account the fundamental needs of commercial users. They evaluated the most common fingerprint technologies across three performance categories, listed here in order of importance:

- **Capture:** Metrics related to the ability to capture usable biometric data on the first attempt for every user. Ability to capture is the most essential performance consideration in commercial biometric applications. Consumers expect "100/100" capture performance, even in challenging environmental conditions and for diverse populations.
- **Liveness:** Metrics to determine that the captured biometric data is not fake, an increasingly common threat.
- **Matching:** Metrics related to the likelihood that an imposter fingerprint mistakenly matches a registered user.

After conducting extensive tests, it was determined that multispectral fingerprint technology has the strongest overall performance in regards to the metrics of capture, liveness, and matching.

A Deeper Look: How the new Biometric Performance Framework determined that Multispectral Imaging Achieves Superior Performance in Capture, Liveness and Matching

Capture >

Commercially deployed biometric devices must capture accurate, usable fingerprint data in real-world situations on each user's first attempt. As most biometric usage occurs in unattended environments, so devices must operate reliably and with a level of simplicity that requires no special training or assistance.

Figure 2. Multispectral fingerprint imaging is the only technology biometrics able to capture high quality external and internal fingerprint images for all skin tones in any condition—wet, dry, hot, cold, sanitized, dirty, elderly, damaged, in darkness or in bright light.

Figure 3. Common methods for attempting to "spoof" fingerprint scanners.

Liveness >

Liveness detection refers to the ability to confirm that the captured finger image is legitimate and from a live finger, by comparing complex optical characteristics of the material presented against known characteristics of living skin.

This unique ability of multispectral imaging provides accurate fingerprint liveness detection and eliminates the perception that fingerprint images must be kept secret to be trusted for user authentication. Fingerprint images are not secrets. We leave our fingerprint images in multiple places on any given day—on door handles, on countertops, on glasses at restaurants. Liveness detection ensures that fingerprints, even if stolen, are usable only by their legitimate owners.

How Important is Compliance with FIPS 201?

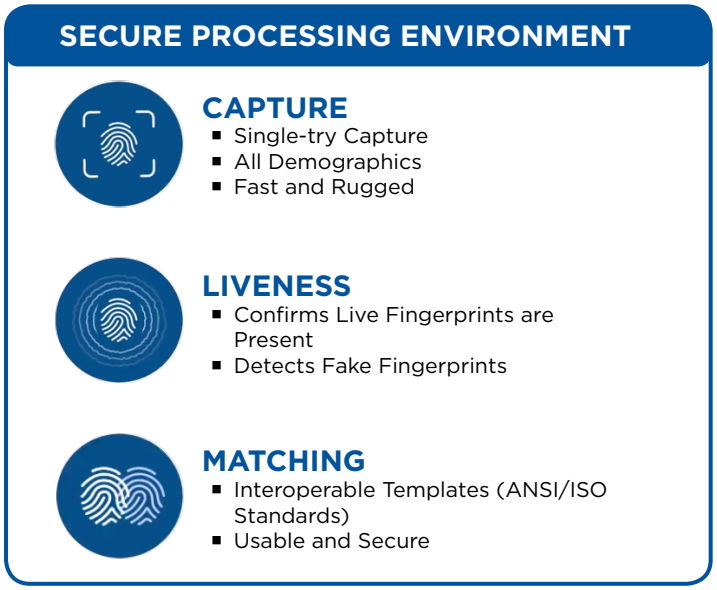
FIPS 201 (Federal Information Processing Standard Publication 201) is a U.S. Federal Government standard that defines requirements for fingerprint-capture devices including the PIV standard for Personal Identity Verification. This standard only applies to images captured from the surface of the skin. This standard does not measure biometric performance, and compliance does not guarantee good performance.

Multispectral imaging, however, uniquely captures fingerprint data from both the surface and the subsurface of the skin. While the subsurface data generally results in superior biometric performance, the resulting fingerprint image deviates from the FIPS 201 standard. Although multispectral imaging does not meet this standard, it provides significant capture reliability over FIPS 201 PIV-certified devices, which is more important to commercial organizations.

Fingerprint templates captured from multispectral imaging sensors, using MINEX III standard are fully interoperable with MINEX templates captured from PIV sensors, and this is a widely deployed solution today.

Matching >

To prevent vendor lock-in and to provide choice for users of commercial biometric systems, fingerprint authentication solutions should use interoperable and independently tested global fingerprint minutia standards. HID Global's fingerprint matching technology uses existing ISO 19794-2 templates supplied by a tier-1 MINEX III certified algorithm for fingerprint templates, including ANSI 378 and ISO 19794-2 MINEX templates supplied by a Tier-1 fingerprint algorithm partner, independently tested and validated by the U.S. National Institute of Standards and Technology (NIST).



Convenient / Reliable / Proven Biometric Authentication

When comparing fingerprint authentication technologies for "real-world" commercial applications in banking, healthcare, and enterprise access, organizations are advised to:

- Select proven biometric capture technology that will consistently work for diverse user populations in a wide range of environments.
- Ensure that the captured fingerprint image is from a living person, preventing identity fraudsters from using fake or stolen biometric data
- Choose independently validated, interoperable biometric matching algorithms, which provide choice to the deploying organization

For commercial organizations considering biometrics for customer or employee use, usability is essential for business success. Using a biometric evaluation framework aligned with their commercial needs rather than just complying with legacy, government-centric biometric standards can reduce identity fraud while ensuring a positive user experience.

To learn more about HID Global's Biometric solutions incorporating MSI, visit hidglobal.com/biometrics.

2018-05-25-hid-iam-capture-liveness-match-bio-eb-en

PLT-03867