BIZCOMMUNITY

The wrong technology in the wrong environment can actually increase risk

By Marius Coetzee

31 May 2018

Biometrics certainly presents a compelling use case across fraud and risk management, security and access control, so major enterprises are looking to harness biometrics in a broader way.

In light of FNB's recent introduction of a mini-ATM that uses biometrics as a means of validation for consumers, it`s important to highlight the risks of using inferior fingerprint readers. Not all biometrics technologies are equal, and some may 'come back to bite' the enterprises rolling them out.

It is therefore important that the appropriate sensors are used, backed by the right algorithms.

Key fingerprint sensors

There are a number of key fingerprint sensors in the market today, with use cases and some pros and cons around most of them.

Capacitive sensors, which in some markets are appropriate and fit for use. However, South Africa's environment is conducive to creating static electricity, which can quickly blow the sensor.

Optical sensors, which typically use light to illuminate the fingerprint tip and so read light and dark areas, are which are more appropriate to South African conditions, can be categorised by:

- A unique, patented light emitting sensor technology certified by the FBI and manufactured primarily for use in criminal investigations, civil applications and embedded solutions such as Ideco's BIMS terminal.
- True reflective imaging (TRI) delivering crisp, good quality images with obvious contrast. Most fingerprint identification systems will be able to easily assign the matching points on these images with a high level of accuracy, especially when the technology is certified by the FBI for its image quality.
- Multi-spectral imaging (MSI) designed to use various wavelengths of light during fingerprint capture. This allows the scanner to both read the fingerprint surface information, as well as the sub-dermal information. This technology claims the advantage of being capable of "seeing" through dirt or moisture on the fingerprint. But collating information from multiple wavelengths lowers the resulting image quality and fails to reach the minimum FBI certification.

Algorithms

Supporting the scanner technology is the algorithms ‘reading’ and matching the fingerprint information. Advanced systems will correctly match the fingerprint patterns, or minutiae, and identify the difference between fingerprint minutiae and wear and cuts due to manual labour, or wrinkles due to ageing.

While the new Home Affairs automated biometric identification system (ABIS) system will seamlessly process TRI sensors images, others in South Africa are rolling out MSI scanners.

Comparing TRI and MSI scanners

We set out to compare the accuracy of the two technologies and achieved the following results when scanning the same fingerprint.

The picture on the left was obtained using a conventional TRI fingerprint scanner. Any experienced fingerprint expert will agree with me that this is a good quality print. The fingerprint ridges, core and delta are clearly visible. The contrast is obvious and even the sweat pores are noticeable. Most fingerprint identification systems will be able to easily assign the matching points with a high level of accuracy.

The picture on the right is of the same finger but was obtained using an MSI scanner. Besides the obvious difference in capture size, this image seems to be out of focus and smudged, with many artefacts. In many areas, the fingerprint ridges look inverted and all the crisp detail is missing. One can even argue that there is another picture superimposed on this image.

Research carried out by the University of Colorado at Colorado Springs found that spatial processing of fingerprints (looking beyond the two-dimensional surface image) will produce different artefacts on different measurements. It is therefore impossible to produce a consistent image over time and customers may have to be re-enrolled on a regular basis.

According to a senior fingerprint expert, with years of experience in the criminal justice system, it would be impossible to use these fingerprint images as evidence in a court of law.

High risk of false acceptance

In addition, if the fingerprint images do not meet the international image quality standards there is a high risk of false acceptance or failing to identify the person; while fingerprints obtained from these devices are not suitable for processing against their criminal database as part of the criminal investigation process.

We tested the strength of various algorithms and it’s frightening to see how bad some are. We’ve seen up to 25% false

minutiae added by flawed or weak algorithms.

Basically, with inadequate scanner technology and weak algorithms, the risks of fraud and of criminals illegally accessing areas are increased, rather than decreased.

ABOUT THE AUTHOR

Marius Coetzee is the CEO of [[www.ideco.co.za Ideco]], a pioneer in identity management solutions.