

Theme Tracking

Secrets of Never-Failing Key

Common physical biometrics includes fingerprints; hand or palm geometry; and retina, iris, or facial characteristics, whereas behavioural characteristics include signature, voice (which also has a physical component), keystroke pattern, and gait. While some technologies have gained more acceptance than others, it is beyond doubt that the field of access control biometrics has gained a measure of acceptance.

Biometric products provide improved security over traditional electronic access control methods such as RFID tags, electronic keypads and some mechanical locks. They ensure that the authorized user is present in order for access to take place. The user's authorized card or password pin cannot be stolen or lost to gain access.

By Miha Lederer



GROWING NEEDS

In order for the biometrics to be ultra-secure and to provide more-than-average accuracy, more than one form of biometric identification is required. Hence, the need arises for the use of multimodal biometrics. This uses a combination of different biometric recognition technologies. In certain situations, the user might find one form of biometric identification is not exact enough for identification. This can be the case with fingerprints, where at least 10% of the population have worn, cut or unrecognizable prints. Multimodal biometric technology uses more than one biometric identifier to compare the identity of the person. Therefore, in the case of a system using, say, three technologies, i.e., face mimic and voice. If one of the technologies is unable to identify, the system can still use the other two to accurately identify against. Multimodal technologies have been in use commercially since 1998.

1:1 AND 1:N MATCHING

A biometric recognition system can be used in two different modes: identification (1:N matching) or verification (1:1 matching).

Identification is the process of trying to find out a person's identity by comparing the person who is present against a biometric pattern/template database. The system would have been pre-programmed with biometric pattern or template of multiple individuals. During the enrolment stage, a biometric would have been processed, stored and encrypted, for each individual.

A pattern/template that is going to be identified is going to be matched against every known template, yielding either a score or distance describing the similarity between the pattern and the template. The system assigns the pattern to the person with the most similar biometric template. To prevent impostor patterns (in this case all patterns of persons not known by the system) from being correctly identified, the similarity has to exceed a certain level. If this level is not reached, the pattern is rejected. With verification, a person's identity is known and therefore claimed a priority to search against. The pattern that is being verified is compared with the person's individual template only. Similar to identification, it is checked whether the similarity between pattern and template is sufficient enough to provide access to the secured system or area.

FAR & FRR

Biometric systems use scores (also called weights) to express the similarity between a pattern and a biometric template. The higher the score, the higher the similarity is between them. As described in the previous section, access to the system is granted only, if the score for an authorized individual (identification) or the person that the pattern is verified against (verification) is higher than a certain threshold. In theory, authorized user scores (scores of patterns from persons known by the system) should always be higher than the scores of impostors. If this would be true, a single threshold, that separates the two groups of scores, could be used to differ between clients and impostors. This unfortunately is not the reality for real world biometric systems. In some cases, impostor patterns can generate scores that are higher than the scores of an authorized user's patterns (FAR or false acceptance rate). For this reason it is a fact that, however, the classification threshold is chosen some classification errors may occur. For example, you may configure the threshold with a high setting, which will reject all impostor patterns that exceed this limit. As a result no patterns are falsely accepted by the system. But on the other hand the authorised user patterns with scores lower than the highest impostor scores are also falsely rejected. The opposite scenario would be to configure a low threshold that ensures no client patterns are falsely rejected. However, this would then allow a certain percentage of impostor patterns to be falsely accepted.

If you choose the threshold somewhere between those two points, both false rejections and rejections false acceptances occur. This creates an access control environment which is obviously not ideal for high security installations.

WHY MULTIMODAL?

By using more than one means of biometric identification, the multimodal biometric identifier can retain high threshold recognition settings. The system administrator can then decide the level of security he/she requires. For a high security site, they might require all three biometric identifiers to recognise the person or for a lower security site, only one or two of the three. With this methodology, the probability of accepting an impostor is greatly reduced.

Multimodal Biometric Access Control System

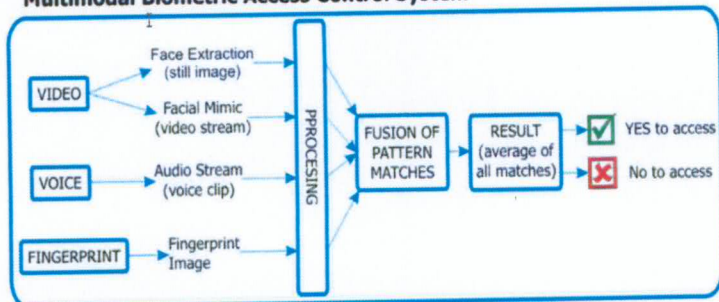


Figure 1. Multimodal biometric access control system (Photo by TAB Systems)

Traditional Unimodal Biometric Access Control System

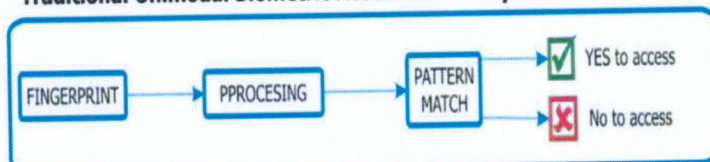


Figure 2. Traditional unimodal biometric access control system (Source: TAB Systems)

Miha Lederer is Product Manager of TAB Systems (www.tab-systems.com).

For more information, please send your e-mails to swm@infothe.com.
(c)2007 www.SecurityWorldMag.com. All rights reserved.

Close