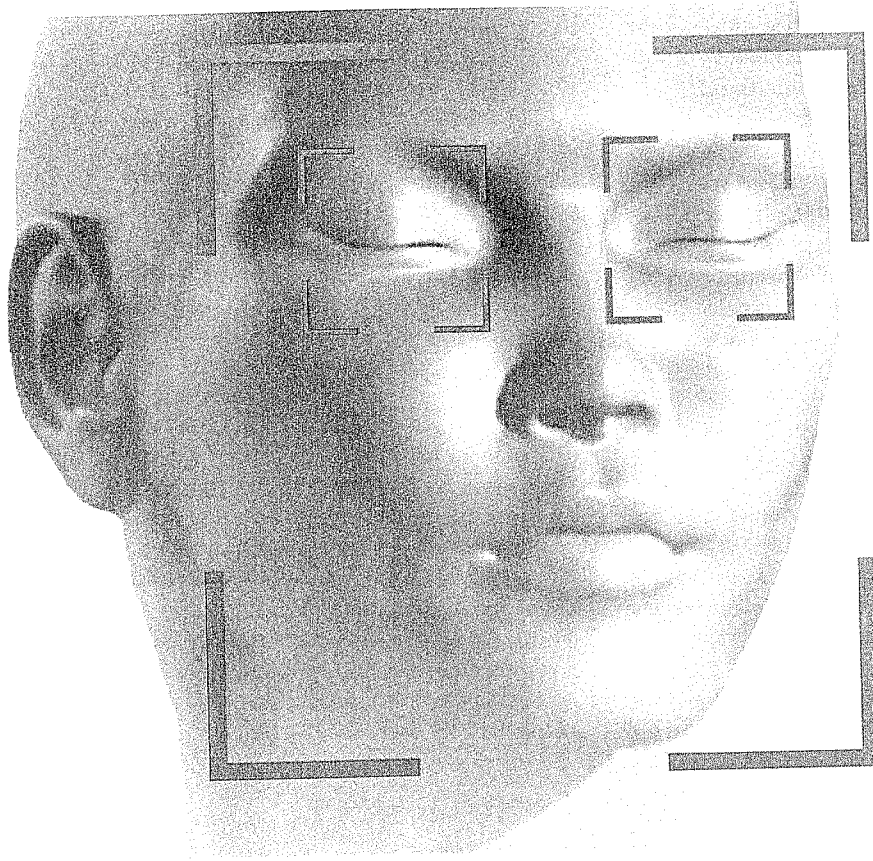


Multimodal Biometrics in Access and Presence Control



There are many features of a person that can be useful for biometric feature extraction. A single feature, however, sometimes fails to be exact enough for identification. (Photo by TAB System)

While there is increased sensitivity to the potential advantages of biometrics, there have been a number of technological hurdles to be overcome. With respect to technological diversity, the biometrics industry includes more than 150 separate hardware and software vendors, each with their own proprietary interfaces, algorithms, and data structures. So, among many technological issues, one of the most important ones is the development of integratable solutions. The most secure systems use multimodal biometrics (combination of different biometric recognition technologies).

By Tomaz Bergant

Biometrics measures individuals' unique physical or behavioral characteristics, as a means to recognize or authenticate their identity. Common physical biometrics includes fingerprints; hand or palm geometry; and retina, iris, or facial characteristics, whereas behavioral characteristics in-

clude 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 and biometrics as a whole shows great potential for use in end user segments.

Biometrics can be used for a number of security purposes -- for virtual or physical access, for covert surveillance, etc. Many of these biometric techniques have been used for a number of years by banks, the immigration services, and law enforcement, among others. While there is increased sensitivity to the potential advantages of biometrics, there have been a number of technological hurdles to be overcome. With respect to technological diversity, the biometrics industry includes more than 150 separate hardware and software vendors, each with their own proprietary interfaces, algorithms, and data structures. So, among many technological issues, one of the most important ones is the development of integratable solutions. The most secure systems use multimodal biometrics (combination of different biometric recognition technologies).

About FAR, FRR and EER

Here are some general principles of biometric recognition systems, description about different classification errors and explanation of how the quality of two systems can be compared objectively.

Identification and Verification

A biometric recognition system can run in two different modes: identification or verification. Identification is the process of trying to find out a person's identity by examining a biometric pattern calculated from the person's biometric features.

In the identification case, the system is trained with the patterns of multiple persons. For each person, a biometric template is calculated in this enrolment stage. A pattern that is going to be identified is matched against every known template, yielding either a score or a 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.

In the verification case, a person's identity is claimed a priority. 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.

Thresholding (False Acceptance/ False Rejection)

Biometric systems use scores (also called weights) to express the similarity between a pattern and a biometric template. The higher the score is, the higher the similarity is between them. As described in the preceding section, access to the system is granted only, if the score for a claimed person (identification) or the person that the pattern is verified against (verification) is higher than a certain threshold.

In theory, client 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.

Due to several reasons, this assumption isn't true for real world biometric systems. In some cases impostor patterns can generate scores that are higher than the scores of some client patterns. For that reason it is a fact that, however, the classification threshold is chosen, some classification errors may occur.

For example, you can choose the threshold such high, that really no impostor score will exceed this limit. As a result, no patterns are falsely accepted by the system. On the other hand the client patterns with scores lower than the highest impostor scores are falsely rejected. In opposition to this, you can choose the threshold such low, that no client patterns are falsely rejected. Then, on the other hand, some impostor patterns are falsely accepted. If you choose the threshold somewhere between those two points, both false rejections and false acceptances occur.

The following figures should help to achieve a better understanding of this topic. Think of a biometric verification system, which is tested with a large amount of test data. The test data consists of both impostor and client patterns. Let's first take a look at the impostor patterns. The belonging scores would be somehow distributed around a certain mean score. This can be seen in the first image on the left side.

Depending on the choice of the classification threshold, between all and none of the impostor patterns are falsely accepted by the system. The threshold depending fraction of the falsely accepted patterns divided by the number of all impostor patterns called False Acceptance Rate (FAR). Its value is one, if all impostor patterns are falsely accepted and zero, if none of the impostor patterns is accepted. Look on the graphic on the right to see the values of the FAR for the score distribution of the left image for varying threshold.

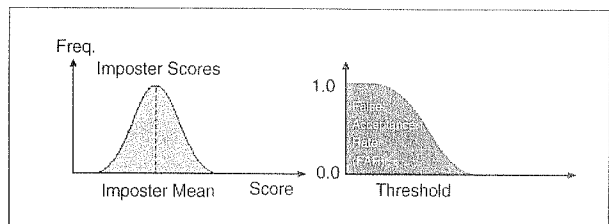


Figure 1. False Acceptance Rate (FAR)
(Source: TAB Systems)

Similar to the impostor scores, the client pattern's scores vary around a certain mean value. The mean score of the client patterns is higher than the mean value of the impostor patterns, as shown in the left of the following two images. If a classification threshold that is too high is applied to the classification scores, some of the client patterns are falsely rejected. Depending on the value of the threshold, between none and all of the client patterns will be falsely rejected. The fraction of the number of rejected client patterns divided by the total number of

client patterns is called False Rejection Rate (FRR). According to the FAR, its value lies in between zero and one. The image on the right shows the FAR for a varying threshold for the score distribution shown in the image on the left.

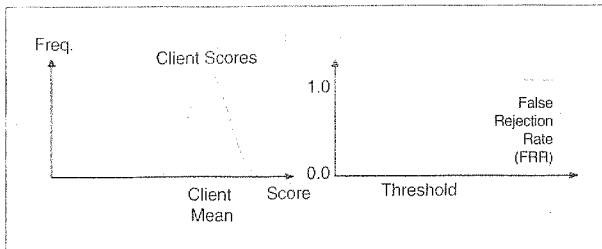


Figure 2. False Rejection Rate (FRR) (Source: TAB Systems)

The choice of the threshold value becomes a problem if the distributions of the client and the impostor scores overlap, as shown in the next image on the left. On the right, the corresponding false acceptance and false rejection rates are displayed.

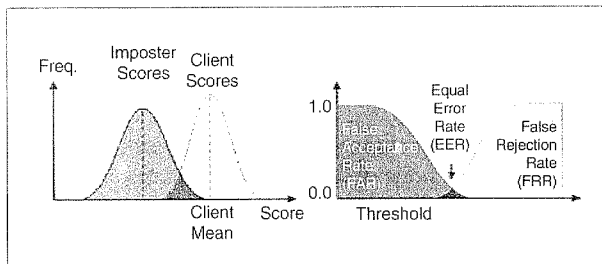


Figure 3. Equal Error Rate (EER) (Source: TAB Systems)

Note that if the score distributions overlap, the FAR and FRR intersect at a certain point. The value of the FAR and the FRR at this point, which is of course the same for both of them, is called the Equal Error Rate (EER). Lower the EER is, more secure is the biometric system.

Multimodal Biometrics

There are many features of a person that can be useful for biometric feature extraction. The face, the voice, the eye, the movement, amongst many others, can be used to distinguish a person from another. Many research activities have proven the principle usefulness of those features.

A single feature, however, sometimes fails to be exact enough for identification. Consider twins, for example. The face feature alone will not be able to distinguish them. If additional features, like voice or movement, are taken into account, the system can distinguish those individuals more accurately. Another disadvantage of using only one feature is the "readability" of the chosen biometric feature. For example, 5% of the human beings do not have fingerprints that can be recorded.

By using different modalities, however, a much higher accuracy can be achieved. Even when one modality is somehow disturbed, e.g. voice recognition in a noisy environment, the other two modalities still lead to an accurate decision. Nevertheless, a multimodal system offers the full flexibility to choose any of the modalities in any combination: applications like a face recognition system, or a voice identifier, or a combined face/voice recognizer can therefore easily be created.

There is an access control and presence tracking system, which is based on multimodal biometric person recognition -- smarti® which is supposed to be the only device of this kind in the world: It recognizes person using multiple biometric parameters -- by face/mimic recognition and voice recognition. As similar devices it allows connection with other technical systems, e.g. locks, lights, alarms, machines, etc. One of its main characteristics is "high security level", which makes it usable for government, public, companies, home automation, high security facilities, etc. What exactly will it do depend mainly on the settings. It can register an event with a digital photo of an individual, unlock the door, turn on the light send an SMS or e-mail to someone (administrator, manager, chief security officer...), etc. It also takes care of presence tracking. It can record and calculate regular and overtime presence and take care of reports.

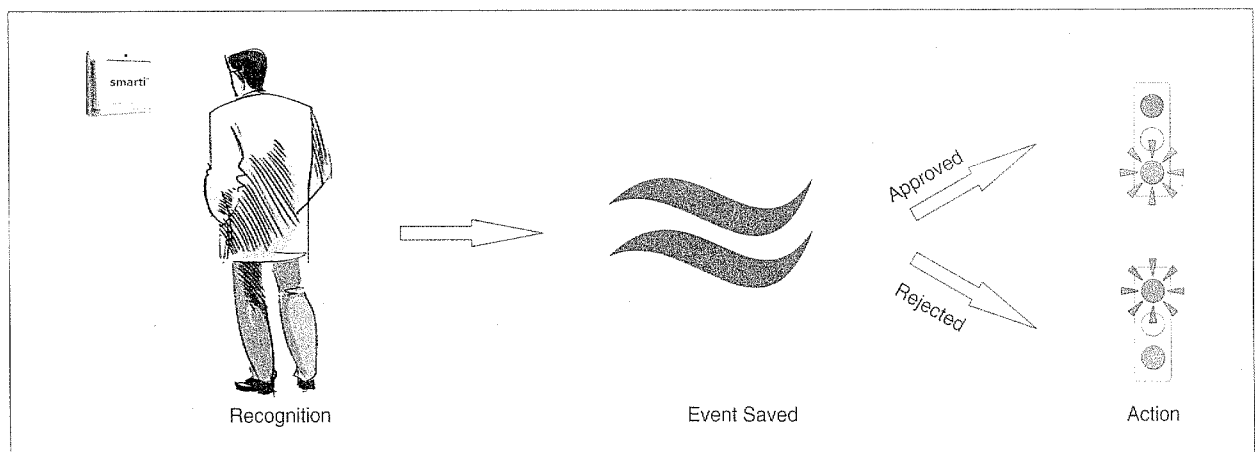


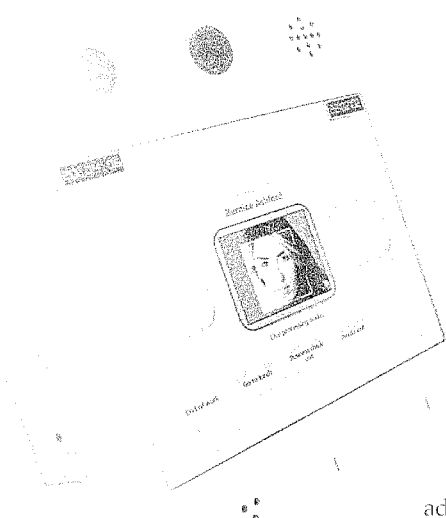
Figure 4. Procedure Schematics of Multimodal Biometric Person Recognition (Source: TAB Systems)

How Does it Work?

What does an access control/presence tracking system like this mean to the employees and visitor? Every person can be treated differently, in other words, different employees and other persons (visitors, part-time workers, intruders, etc.) can have different access rights with or without a time limitation. Everything is recorded; prior events in the database (with an exact date, hour and a photo) can be easily overviewed by an authorized administrator or human relations officer.

Cost Vs. Functionality

Best practices for information technology investment dictate that prior to making any significant project investment, the benefit and cost information of the system should be analyzed and assessed in detail. A business case should be developed that identifies the organizational needs for the project and a clear statement of high-level system goals should be developed. The high-level goals should address the system's expected outcomes such as the binding of a biometric feature to an identity or the identification of undesirable individuals on a watch list. Certain performance parameters should also be specified such as the time required to verify a person's identity or the maximum population that the system must handle. Once the system parameters are developed, a cost estimate can be developed. Not only must the costs of the technology be considered, but also the costs of the effects on people and processes. Both initial costs and recurring costs need to be estimated. Initial costs need to account



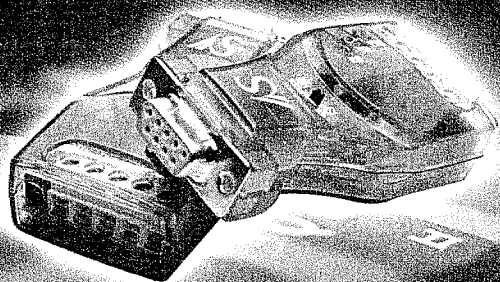
smarti is an access control and presence tracking system based on multimodal biometric person recognition: face, mimic and voice recognition (Photo by TAB Systems)

for the engineering efforts to design, develop, test, and implement the system; training of personnel; hardware and software costs; network infrastructure improvements; and additional facilities required to enroll people into the biometric system.

Recurring cost elements include program management costs, hardware and software maintenance, hardware replacement costs, training of personnel, additional personnel to enroll or verify the identities of people in the biometric system, and possibly the issuance of token cards for the storage of biometrics.

The main advantage of the smarti[®] system, besides its price, is that "whenever you come to the door, you are recognized by multiple parameters -- voice and face/mimic", and it's integration of multiple additional features like presence tracking, access control, external device control, video messaging, video intercom, video surveillance into one compact device for a reasonable price. "We haven't found the kind of system like smarti[®] anywhere in the world -- a system which has everything integrated in one small box -- a touch screen, video camera, configurable options, unlimited features, etc.," said Mr. Matej Stefancic, R&D Manager of TAB Systems, man-

RS-232 to RS-422 / RS-485 Converter



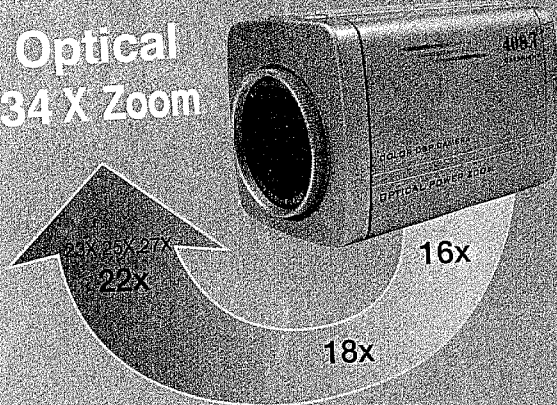
- RS-232 to RS-422, RS-485 Conversion
- Up to 115.2 Kbps
- No external power required
- Automatic toggling
- 15 kV surge Protection
- Built-in termination resistors
- Power, TX, RX LEDs

SystemBase
Since 1987

16F, Daerung Post Tower 1, 212-9, Guro-Dong, Seoul, Korea.
Tel.: +82-2-855 0501 Fax: +82-2-855 0506
E-mail: sales@sysbas.com www.sysbas.com

Digital World digital leader in CCTV!
Nothing is better than This!
No one did, but we did it!

**Optical
 34 X Zoom**



We do not say New but most Stability!
 We do not say Leading but most Reliability!
 We do not say First but do efforts to be #1!

We do not make money so much, to be a most leading in market, but we would like to be a most reliable manufacturer and supplier at any where.



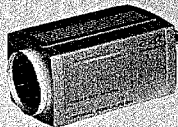
10X PTZ Dome



22X AF Zoom Dual Day & Night



22X AF Zoom Day & Night



22X AF Zoom



10X AF Mini Zoom



3X Digital Zoom

DIPEL Electronics Co., Ltd
 TG Win Co., Ltd

www.dipelcctv.net cctv@dipecctv.net

manufacturer of smarti®. "If you wanted to achieve the same result with a classical access control system combined with a CCTV system, and a video intercom system, it would be much more expensive. You would have to buy cameras, video recorders, video intercom devices, etc. If you use a classical card access control system, which are still most common, there are no extra features included. Here you get an 'all-in-one' deal. It's today's solution for tomorrow's needs."

Ethical Issues

The future of the biometrics industry however, to a large extent, depends on the resolution of technological and ethical issues. With safety and accountability receiving an increased emphasis in organizations, biometric technologies will become more prevalent and more socially acceptable in the coming decade. However, privacy concerns could hinder the acceptance rates for biometrics. In today's world companies, organizations and institutions already possess a wide variety of sensitive personal data such as social security numbers and special needs information. With the addition of biometrics, they can suddenly find themselves with extra information along with the responsibility of protecting that information. With the continued implementation of biometric systems, the fear of the identifying information misuse will be offset by the benefits found with the biometric system, such as enhanced accountability and taking the proper precautions to ensure the sensitive data is not used inappropriately or is not disclosed to third parties. Each type of biometric application can have a different impact on various privacy issues. People will see biometrics differently with different threats or risks and will view it at different levels of severity. Some of the privacy threats people will see are privacy of person, privacy of personal data, privacy of personal behavior. Like all change, the introduction of biometrics is likely to be met with great resistance. The security of the data is only as good as the administrator or system responsible to maintain the database. Biometrics can be used to centralize all the data in a more secure manner. In order for the use of biometrics in general to be successful and accepted, companies and organizations need to focus on the maintenance of the controlled environment and work to ensure the public and staff of the integrity of the system. The International Biometric Industry Association (IBIA), which is a nonprofit trade association in Washington, D.C., has been formed to educate the public as well as convincing opinion leaders, and government officials that we can trust biometric technologies to protect privacy. One thing is certain, the growing need for biometrics and a price drop for devices, which use such technology, caused the global breakthrough in acceptance of such devices and certainly promise a much brighter future.

Tomaz Bergant is CEO of TAB Systems (www.tab-systems.com).