

MARCH 28-30, 2007 | SANDS EXPO AND CONVENTION CENTER | LAS VEGAS, NV

Search

**ISC EXPO**  
INTERNATIONAL SECURITY  
CONFERENCE & EXPOSITION  
**2007**

**ISCWEST**  
We've got you covered.

SPONSORED BY:  
**SIA**

↓ **What's New** ↓

Featured Product

The only camera system ready to go wherever the future takes you

**BOSCH**

Register Now

HOME | WHO'S EXHIBITING | TRAVEL | CONTACT

- ATTENDEE →
- ISC EDUCATION →
- PRESS →
- EXHIBITOR →

ISC WEST Partners:



THE INDUSTRY'S  
NEWEST INNOVATIONS



## TAB Systems

Booth : 60066

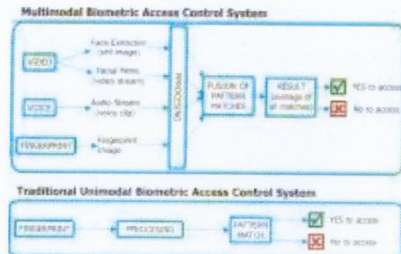
Trzic,  
Slovenia  
[www.tab-systems.com](http://www.tab-systems.com)

[Exhibitor Details](#) | [Product Gallery](#) | [Press Releases](#) |

### Press Releases

**Title:** smarti®- Multimodal biometrics

**Date:** 17 January 2007



## Introduction

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.

### The use of multimodal biometrics

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.

#### 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.



[Privacy Policy](#) | [Copyright Statement](#) | [Reed Jobs](#) | [Reed Corporate Site](#) | [Reed Elsevier](#)