

Gradiant gets the best score in the IJCB 2017 international competition

The goal was to evaluate the best biometric facial recognition technologies in mobility scenarios for detection of anti-spoofing attacks

The competition was held in the framework of the IJCB 2017 conference, to be held in Denver (USA) next October

Gradiant has achieved **the highest score in all tests** of the international competition that evaluate the performance of **biometric facial systems for anti-spoofing attacks detection in mobility scenarios**. As **Esteban Vázquez, head of biometrics at Gradiant** explains, “anti-spoofing systems have been gaining interest in recent years. As biometric recognition technologies have begun to hit the market, the need for robust systems has been growing up. But until quite recently, most of these systems were being evaluated in academic settings, with the limitations that this entails in real scenarios, which is why competitions like this are very important for the advance of technology”.

The competition, held in the framework of the **International Joint Conference on Biometrics - IJCB 2017**, to be held in Denver (USA) next October, has focused on assessing and comparing the skills of the technologies developed by participants with several tests for the detection of anti-spoofing attacks in biometric facial recognition tools for mobility scenarios. Among the **teams participating in this international competition**, in which **Gradiant’s facial recognition system developed has obtained the best score in all tests**, were companies such as **FUIJTSU Laboratories LTD** (Japan), **CpqD** and **University of Campinas** (Brazil), **Idiap Research Institute** (Switzerland), **Universisty of Oulu** (Finland) and the **Indian Institute of Technology Indore** (India), among others representatives from France, Russia, China and Algeria.

The tests, the technologies presented to this competition are submitted to, focused on four scenarios, using a **database developed by OULU-NPU**. The first one, evaluated the performance of the systems under different lighting conditions. The second scenario evaluated the behaviour of the systems with different mobile devices or different sensors; the third one, analysed how the systems designed generalized to unknown attacks, for example videos recorded with different devices, on a support, with variations of movement, different types of screens, etc. The last of the scenarios presented integrates all three previous scenarios to determine the strength of the designed system. “When you design multibiometrics tools like this, you need to make sure that you can not only detect the attacks you have trained the system for, but also that you can deal with scenarios that are unfamiliar because, as a developer, you never know what environment or under what conditions the customer will use the system in”, says Vázquez.

Combined Multibiometric Technologies

Nowadays, we can find different options to reduce the risk of spoofing, using systems much more sophisticated and expensive; combining collaborative and automatic mechanisms (such as the one used in the IJCB 2017 competition) that require the user's interaction, such as moving the head or making some gesture; or thanks to complementary biometric recognition systems, also called **multi-factor authentication**, such as combining facial recognition systems with handwritten signature recognition systems or speaker recognition systems.

Given the **increasing demand in market** (banking, health, fintech, insurtech, among others) for tools that guarantee security and privacy in mobility environments, Gradiant has developed a solution that combines **facial recognition biometrics, life detection and dynamic signature**. Thus, with this system it is possible to identify that the user is a real person and alive (not a photo) and that the image that the system captures of that user agrees with the signature saved in the profile of the same one. The novelty of the system is that it is a **simultaneous process**, that is, both the identification of the user's image and the signature are done at the same time. "Combining life detection and dynamic signature mechanisms, the system we have developed puts a stronger and more effective solution to potential spoofing attacks" said Esteban Vázquez, head of biometrics at Gradiant.

With more than ten years of experience in biometric research, Gradiant has been able to transfer secure technologies to sectors such as banking, health and security. Following this philosophy, we make available our biometric technologies for mobile devices in three complementary modalities: face, voice and signature recognition.