# Research on avoiding fraud in biometric identification

October 25 2010

This is a biometric iris image taken in the research laboratory. Credit: UC3M

Spanish scientists from Carlos III University of Madrid are analyzing possible attempts at fraud in various biometric identification systems in order to improve the security of facial, iris, fingerprint or vascular recognition, among other types.

The field that these researchers are working in is known by its nickname, "anti-spoofing", and basically consists in trying to detect all of the possible attempts at fraud that a biometric system might suffer, especially with regard to an action in which the user presents the biometric proof to the system. "What we are trying to do is detect those attempts so that the system can then act accordingly", explains the head of UC3M's Grupo Universitario de Tecnologías de Identificación (GUTI)(University Identification Technology Group), Raúl Sánchez Reíllo, who is leading this research. This way, if someone used a colored contact lens to recreate a specific iris at an access control point, the system would detect this possible fraud attempt and would indicate to this user that s/he could not use the automatic system and would have to use the manual identification system, with a security agent, for example.

These scientists work on "anti-spoofing" related to most of the forms of biometric identification. In addition, they evaluate the strength of current biometric systems in the face of various types of attacks, and they also create algorithms, devices and collateral techniques and usage policies that avoid and detect these attempts at fraud. " Currently, we are working very intensely on the ocular iris as well as written signatures, although previously we have worked on fingerprints, and in the near future we will be working on facial recognition", comments this professor from UC3M's Electronic Technology Department (Departamento de Tecnología Electrónica de la UC3M), pointing out that the challenges in this field are enormous. The reason: there is a constant struggle between "good" and "evil", in which the latter is constantly trying to find new ways to attack the security of the system. "Let's say that the good guys work to stay a step ahead of those attempts, introducing anti-fraud measures in advance of what the bad guys might come up with ", he reveals.

At a recent scientific conference, the scientists of the GUTI group presented part of their research on sources of noise and the most common falsifications in recognition systems based on iris identification. The article, titled "Estudio de la Casuística de la Muestras de Entrada en los Sistemas de Reconocimiento mediante Iris Ocular" ("A Case Study of the Entrance Samples in Recognition Systems Based on the Ocular Iris") presented at the V Jornadas de Reconocimiento Biométrico de Personas JRBP2010 (Fifth Conference on Biometric

Recognition of Individuals JRBP2010) held in Huesca in early September, concluded that the robustness of the recognition algorithm and the inclusion of antifraud mechanisms in it are essential to keeping falsifications such as impressions of photographs of the iris, prostheses, or contact lenses from successfully violating the security of the systems.

## Different types of fraud

Many of the attempts at fraud in biometric identification can be seen in films, although some of these definitely belong to world of science fiction. One that is actually feasible, according to the researchers, is the reproduction of fingerprints using silicone or other plastics, while cutting off a person's finger or hand in order to use his/her fingerprint or hand geometry for identification purposes would only work with systems that are in the lowest range. In contrast, using contact lenses with the iris painted on them is usually detectable, and removing someone's eyeball is useless, as the eye deteriorates very quickly, according to the scientists. In the case of facial recognition, using make-up to take on the appearance of another does not usually work, while the use of masks or plastic surgery is sometimes successful.

The university's GUTI research group also carries out periodic, independent evaluations of these systems, in order to identify the strengths and weaknesses of new developments to the manufacturers, as well as to analyze the usability of the systems, to see if users feel comfortable with them. This is because, according the researchers, systems for identifying people, whether they use documents, biometrics or both, should not be seen as simple security tools, but as a way to bring technology closer to the user, so that the user can work more easily with automatic services.

Currently, biometric systems are being used with greater frequency in both banking and commercial applications. The biometric identification system par excellence, and the most widely used, is the fingerprint system, although techniques such as vascular identification are starting to be used in hospitals and automatic teller machines, where they could substitute or complement intelligent cards or fingerprints. In fact, in Japan, a large number of automatic teller machines have already been adapted to use this type of identification, although their current rate of use is still below ten percent, as the process introduction process is still in progress, explains Sánchez Reillo. Another important biometric technique uses the iris. This system offers a very low rate of 'false rejections' (that is, when the system does not recognize you although you are the correct person) and, at the same time, its rate of 'false acceptance' (when you are not the correct person, but the system accepts you) is practically zero. However, both the computational costs and the economic costs of this system are high compared to other techniques such as vascular or fingerprint.

There are other interesting biometric applications in existence, such as multimodal systems, in which various different techniques are used– fingerprints and the vascular system, for example – the data are merged and, based on the results obtained so far, the rate of success is even higher. Hybrid systems can also be developed by combining technologies, and can then be used in automatic teller machines depending on the amount of money to be withdrawn. For example, if the user wishes to withdraw three hundred euros, s/he can use a PIN number for identification; however, if s/he wants to withdraw a greater amount of money, the system may require the user to identify him/herself using the veins in his/her hands.

Provided by Carlos III University of Madrid

Citation: Research on avoiding fraud in biometric identification (2010, October 25) retrieved 3 May 2024 from https://phys.org/news/2010-10-fraud-biometric-identification.html