New technique prevents identity theft in smartphones and tablets

21/01/2020

Research news

> **The new system, designed by researchers from the University of Granada, is based on deep neural networks and enables users to discern whether the incoming voice belongs to a legitimate person or is an identity theft attack carried out by a fraudster**

Researchers at the University of Granada (UGR), from the Department of Signal Theory, Telematics and Communications, have designed a new technique based on neural networks that prevents identity theft in the automatic voice recognition systems of electronic devices, such as smartphones or tablets.

Access to information portals via electronic devices requires secure authentication mechanisms that guarantee that the identity of the user is genuine. Unlike the traditional use of mechanisms based on user–password matching, in recent years the use of biometric authentication methods, such as facial or voice recognition, has witnessed significant growth.

Biometric authentication methods offer the advantage of freeing the user from having to remember passwords to access these systems, as the authentication is conducted using the biometric characteristics of the user, for example by fingerprint, iris, or facial recognition.

In an article published in the prestigious journal IEEE/ACM Transactions on Audio, Speech, and Language Processing, the UGR researchers explain their study into a

particular type of biometric authentication that is generating interest both in the scientific community and in the business field: voice biometrics.

“The voice is a unique personal characteristic, different for each of us. In just a single word we can distinguish without any difficulty the voice of a family member or friends. This is due to the unique anatomical characteristics of each person, which are related to the organs involved in voice production. Voice biometrics, therefore, enables a person to be identified by their voice,” explains Alejandro Gómez Alanís, one of the researchers at the UGR’s Department of Signal Theory, Telematics and Communications and the main author of the work.

Malicious attacks

In recent years, however, it has been demonstrated that automatic voice verification systems are susceptible to malicious attacks by intruders seeking fraudulent access to the information system. These intruders could use voice samples from a legitimate user to fraudulently access the system. The voice samples could be obtained, for example, by making undercover recordings of legitimate users or employing state-of-the-art speech synthesis and conversion software, which enables a person’s voice to be cloned in just a few minutes.

“In our research, we address this problem by proposing a new intrusion-detection technique for voice biometrics. Specifically, we propose a technique based on deep neural networks to discern whether the incoming voice belongs to a legitimate user or is an identity theft attack carried out by a fraudster,” says Gómez.

The new technique for detecting security attacks on voice biometrics systems (known as Gated Recurrent Convolutional Neural Network, or GRCNN) was submitted by the UGR research group to the 2019 ASVspoof anti-spoofing challenge (www.asvspoof.org). It was ranked among the top 10 systems out of a total of 63 research groups and participating companies at international level, both in the detection of physical-access attacks (recording and repetition) and also logical access (voice synthesis or conversion).

Gómez concludes: “In this study, we have addressed the problem of detecting identity theft attacks via the voice—commonly known as anti-spoofing—where the main challenge is to develop systems capable of spotting attacks not detected during the training stage. In our proposed approach, we combine the discriminatory capacity of neural networks with classic signal processing methods to impregnate signal knowledge in the network, and thus help detect identity theft attacks under different acoustic conditions.”

Bibliography:

Gómez-Alanis, A., Peinado, A.M., Gonzalez, J.A., and Gómez, A.M. (2019), ‘A Gated Recurrent Convolutional Neural Network for Robust Spoofing Detection’, IEEE/ACM Transactions on Audio, Speech, and Language Processing, 27(12), 1985-1999. IF: 3,531

Media enquiries:

Alejandro Gómez Alanís

Department of Signal Theory, Telematics and Communications, UGR

Email: agomezalanis@ugr.es

Compartir en