Impersonation Attacks on Biometric Recognition Systems

Marta Gomez-Barrero*[1]

[1]Universität der Bundeswehr München [Neubiberg] – Werner-Heisenberg-Weg 39, 85577 Neubiberg, Allemagne

Résumé

With the widespread use of biometric recognition, several issues related to the privacy and security provided by this technology have been raised and analysed. Starting with the classification of attack points published by Ratha et al. in 2001, recent works have analysed the vulnerability of biometric systems from different perspectives, including inverse biometrics or morphing attacks. The former constitutes a severe threat for biometric systems from two different angles: sensitive personal data (i.e., biometric data) can be derived from compromised unprotected templates, and other powerful attacks can be launched building upon synthetic reconstructed samples. Morphing attacks, on the other hand, can severely decrease the security of identity documents or processes, in which morphed images matching two or more identities are injected. The present talk will describe these attack forms under the umbrella term of impersonation attacks, and discuss their impact on biometric technologies, including standardised evaluation metrics.

*Intervenant