A Biometric System Resistant to Spoof Attacks

A working model for developing a biometric system that is resistant to spoof attacks has been developed by researchers at the National Institute of Technology, Raipur and TCS Innovation Labs, Mumbai in their recent study.

Read more

A large number of organizations presently use biometric systems for person authentication, in an easy and reliable manner to manage data from a large number of users. However, biometric systems that use fingerprint matching as the sole strategy to authenticate person are prone to spoof attacks. During a spoof attack, an imposter uses the fingerprint of a genuine user that may be obtained by unethical means for obtaining unduly authentication.

Researchers at the National Institute of Technology, Raipur and TCS Innovation Labs, Mumbai have developed a new model that uses fingerprint matching and fingerprint dynamics for authentication in biometric machines. Fingerprint dynamics requires the users to scan fingers multiple times. It uses parameters such as the sequence of fingers used for scan, repeated use of a finger, the length of finger area used during scan, time taken between consecutive scans to add another dimension during person authentication.

Since, this model uses software-based intervention, it is cost effective, convenient, reliable and automated. Fusion of these two parameters, fingerprint matching and fingerprint dynamics improved the overall efficiency and performance of biometric system remarkably. The researchers proclaim, " (their system)… provides commendable spoof resistance while minimizing the error rates. The increased spoof resistance of the proposed system is because of the use of behavioral characteristic, fingerprint dynamics".

The new proposed model can be used to devise spoof-resistant biometric systems thereby enabling more security to organizations and their data.

Bhavya Khullar
December 15th, 2016.
Reference: *Pattern Recognition* **62**: 214-22.