Privacy-Preserving Remote Biometric Authentication (#7885)

Balances deep learning and cryptographic methods

This biometric authentication system and method balances the deep learning (DL) inferences of face and voice biometrics with cryptographic privacy-preserving tools, resulting in a technology designed to be both accurate and practical. The technology combines in a novel way standard privacy-preserving tools such as reusable fuzzy extractors and locality-sensitive hashing with advanced DL systems for face and voice biometrics.

Using biometric samples that are cryptographically protected, the system authenticates a user's enrollment and authentication data to a remote server without revealing the user's biometric data to the server. This approach is intended to eliminate privacy risks associated with databases of people's faces. The technology also includes noise handling techniques that efficiently maintain accuracy of respective plaintext systems.

This Georgia Tech technology can be used with face- and voice-based authentication, a combination of the two, or potentially other biometric features associated with a client device, such as iris, fingerprint, and gait. The user-friendly system accommodates standard one-click, device-based authentication for daily use.

Benefits/Advantages

- **Protective:** Designed to eliminate privacy concerns associated with databases of people's faces
- **Flexible:** Supports various biometrics, including face, voice, iris, fingerprint, and gait
- **Remote authentication:** Eliminates the need to always possess the enrollment device
- **Improves usability:** Accommodates standard one-click, device-based authentication for daily use
- **Increases security:** Achieves ~25 bits and ~33 bits of security guarantees for face- and voice-based pipelines, respectively

Potential Commercial Applications

- Secure area technologies (governments and private)
- Banking
- eCommerce security
- National borders security technologies
- Consumer devices (computers and smartphones)
- Social media account authorization

Background/Context for This Invention

Biometric authentication is becoming increasingly popular due in part to the fact that biometric features are difficult to lose and easy to measure via sensor-rich smartphone technology.

Conventional biometric verification requires client enrollment data to be stored in a remote server—unprotected—for later comparison at authentication time. This data storage raises privacy concerns because if an adversary or the server itself gains access, harm can result through impersonation or by enabling unwarranted surveillance.

A current and popular solution involves locking an enrollment template in a client's device under hardware protection. However, this cumbersome approach permanently binds authentication to the device, meaning a user has to enroll each device separately and cannot authenticate without one. A preferred solution would allow the server to authenticate the user, thereby decoupling the user from the device.

Georgia Tech's Justitia technology achieves privacy-preserving face- and voice-based verification using samples that are cryptographically protected, while simultaneously maintaining the accuracy of off-the-shelf DL systems.

Simon Chung
Graduate Research Assistant – Georgia Tech College of Computing

Dr. Wenke Lee
John P. Imlay, Jr., Chair of Software - Professor - Georgia Tech College of Computing

Erkam Uzun
PhD Student - Georgia Tech Computer Science

Carter Yagemann
Phd Student - Computer Science Georgia Institute of Technology

More Information

International Application Filed - WO 2019/200264 A1

Publications

Cryptographic Key Derivation from Biometric Inferences for Remote Authentication, ACM Asia Conference on Computer and Communications Security (ACM ASIACCS 2021), June 2021

For more information about this technology, please visit:

https://licensing.research.gatech.edu/technology/privacy-preserving-remote-biometric-authentication

Images:

The automated sequential delivery of multiple fluids. A varying number of delay gates imprinted in the branches are shown in the figure.

COVID-19 and flu saliva test on paper: (A) The automatic sequential delivery of multiple reagents required for virus test; (B) Water pouring into the device triggers the virus assay, allowing the presence of SARS-CoV-2 and influenza A & B viruses to be visually identified by the color changes in the corresponding detection spot