Finger PIN

21-022

Integrated Knowledge & Biometrics-Based Authentication factors Create a Fingerprint-Based PIN (FingerPIN)

Background

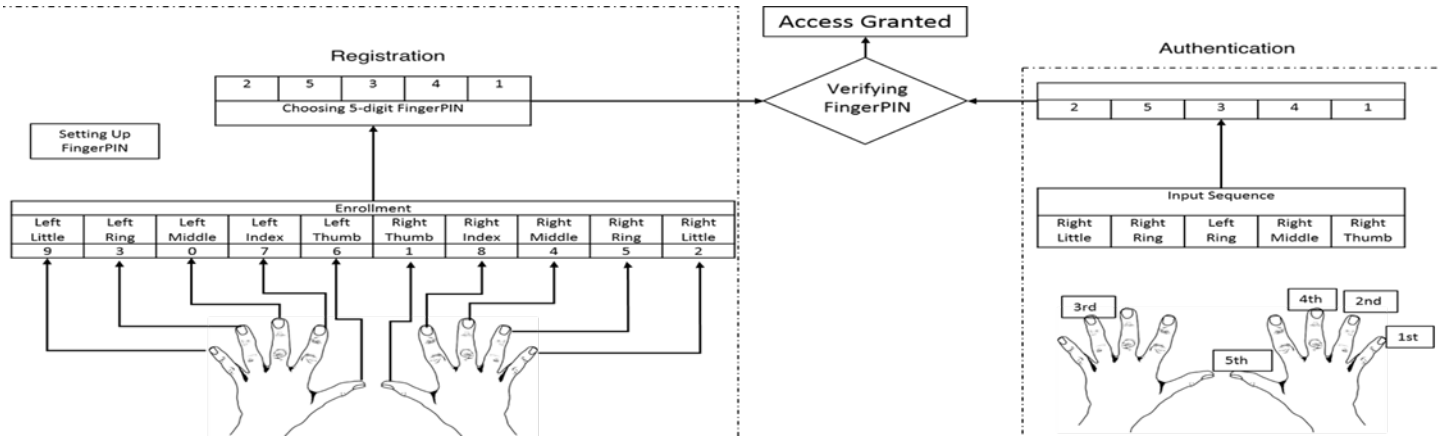
Type 1 (knowledge-based) is still the most widely adopted form of authentication, despite its many weaknesses. Most user created passwords are easy to remember and therefore easy to guess or crack through a variety of means including social engineering and dictionary attacks. When longer or difficult-to-remember passwords are chosen, users tend to write them down in easily accessible places, effectively defeating the purpose of using authentication. To provide more security, Type 3 (biometric-based) authentication, such as fingerprint-based, has been successfully adopted in many applications. Potential breaches of biometrics security represent a significant concern as biometrics are unique and do not change over an individual's lifetime. Once compromised, they cannot be replaced.

Innovation

The subject technology integrates Type 1 and Type 3 factors into a single fingerprint-based identification number (FingerPIN). To authenticate, a subject is required to present a sequence of fingerprints corresponding to the digits of a PIN based on a previous mapping of numbers and fingers. Where traditional multi-factor authentications require users to present multiple factors sequentially, FingerPIN integrates multiple elements into a single composite factor, and users need only to present their fingerprints in the correct order. One key advantage of this technology is it accommodates the compromise of one or more fingerprints.

Advantages

- More security than password-based authentication
- Avoids compromise of a biometric factor
- Significantly increases user-friendliness



Development Stage

Research Prototype

For More Information contact:
George Mason University, Office of Technology Transfer
703-993-8933 ott@gmu.edu https://ott.gmu.edu/