Skysong Innovations
Advancing the Arizona State University Knowledge Enterprise

1475 N. Scottsdale Road, Suite 200
Scottsdale, AZ 85287-3538
Phone: 480 884 1996 Fax: 480 884 1984

Case ID:M18-217P^
Published: 2/27/2023

Inventors

Yimin Chen

Yanchao Zhang

Contact

Shen Yan
shen.yan@skysonginnovations.com

Authenticating a User on a Mobile Device

Protecting mobile devices from unauthorized access is becoming more than indispensable these days. In particular, mobile devices such as smartphones and tablets are pervasive and store increasingly highly sensitive information about a user (e.g., contacts, usernames, passwords, emails, browser histories, business secrets, health conditions, etc.). User authentication is widely adopted to protect mobile devices from unauthorized access and has two forms: (1) user is authenticated to unlock device and (2) user is authenticated to use apps or password managers. A popular method for authenticating a user is face authentication by verifying/identifying a user by validating selected facial features from an image or video. However, face authentication can be vulnerable to both photo-based forgery attacks (PFA) and video-based forgery attacks (VFA). In PFA or VFA, an adversary uses a photo or video containing the user's face to bypass the authentication system.

Current defenses against PFA and/or VFA aim at liveness detection, which seeks to find a live indicator that the submitted photo or video of the user is indeed captured in real time. Current methods for liveness detection include detecting a nose angle change as an indication of a live user or checking the consistency between two movement traces as an indication of a live user. However, these methods have been proven vulnerable to attack. What is needed is a liveness detection method that is easy-to-use for the mobile device user and improves security of face authentication.

Researchers at Arizona State University (ASU) have developed a liveness detection scheme based on comparing two photoplethysmograms extracted from two video sequences for user authentication on a mobile device. Unlike other liveness detection schemes for face authentication, ASU's scheme uses heart biometrics for liveness detection which is impossible for an attacker to fake. The scheme checks the consistency of two concurrent and independently extracted photoplethysmograms of a user as the live indicator. In one example, a video of the user's face is taken by a front-facing camera and a video of the user's fingertip is taken by a rear-facing camera at the same time. Photoplethysmography is applied to extract two underlying photoplethysmograms from the face and fingertip videos. If the two photoplethysmograms are from the same live person and measured at the same time, they must be highly consistent and vice versa. As photoplethysmograms are closely tied to human cardiac activity and almost impossible for the adversary to forge or control, the consistency level of two extracted photoplethysmograms can well indicate the confidence level in the liveness of a face authentication request.

Related publication: Your face your heart: Secure mobile face authentication with photoplethysmograms

Potential Applications:

- Mobile device security
- Defense against photo-based and/or video-based attacks on mobile devices

Benefits and Advantages:

- Can be implemented in any scenario deploying face authentication (e.g., mobile device unlocking, user verification for online services, etc.)
- Can defend against 3D face attack which compromise most existing liveness detection methods