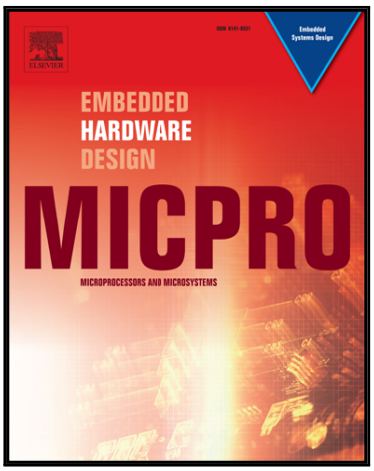

Continuous Face Authentication Scheme for Mobile Devices with Tracking and Liveness Detection

Max Smith-Creasey, Fatema A. Albalooshi, Muttukrishnan Rajarajan

PII: S0141-9331(17)30523-9
DOI: 10.1016/j.micpro.2018.07.008
Reference: MICPRO 2724

To appear in: *Microprocessors and Microsystems*

Received date: 28 November 2017
Accepted date: 19 July 2018

Please cite this article as: Max Smith-Creasey, Fatema A. Albalooshi, Muttukrishnan Rajarajan, Continuous Face Authentication Scheme for Mobile Devices with Tracking and Liveness Detection, *Microprocessors and Microsystems* (2018), doi: 10.1016/j.micpro.2018.07.008

Continuous Face Authentication Scheme for Mobile Devices with Tracking and Liveness Detection

Max Smith-Creasey*, Fatema A. Albalooshi†, and Muttukrishnan Rajarajan*
*School of Mathematics, Computer Science and Engineering, City, University of London, London, UK
{Max.Smith-Creasey, R.Muttukrishnan}@city.ac.uk
†College of Information Technology, University of Bahrain, Sakheer, Kingdom of Bahrain
Falbalooshi@uob.edu.bh

Abstract—We present a novel scheme for continuous face authentication using mobile device cameras that addresses the issue of spoof attacks and attack windows in state-of-the-art approaches. Our scheme authenticates a user based on extracted facial features. However, unlike other schemes that periodically re-authenticate a user, our scheme tracks the authenticated face and only attempts re-authentication when the authenticated face is lost. This allows our scheme to eliminate attack windows that exist in schemes authenticating periodically and immediately recognise impostor usage. We also introduce a robust liveness detection component to our scheme that can detect printed faces and face videos. We describe how the addition of liveness detection enhances the robustness of our scheme against spoof attacks, improving on state-of-the-art approaches that lack this capability. Furthermore, we create the first dataset of facial videos collected from mobile devices during different real-world activities (walking, sitting and standing) such that our results reflect realistic scenarios. Our dataset therefore allows us to give new insight into the impact of user activity on facial recognition. Our dataset also includes spoofed facial videos for liveness testing. We use our dataset alongside two benchmark datasets for our experiments. We show and discuss how our scheme improves on existing continuous face authentication approaches and efficiently enhances device security.

Index Terms—continuous authentication, face recognition, face tracking, liveness detection, biometrics

1 Introduction

Mobile devices are one of the most widely used technologies of our time, requiring users to store private and personal information to use features and applications. Whilst many devices incorporate a variety of security mechanisms such as a PIN, password, or pattern, recent research has shown that such security mechanisms are susceptible to a variety of forgery attacks, such as the smudge attack [1]. Additionally, such mechanisms are intrinsically limited in that they provide only inconvenient and one-time authentication; the user explicitly authenticates once for entire device access. These mechanisms for authentication leave the device vulnerable to attacks if it is left unlocked by the genuine user.

Recent research in mobile device security has sought to alleviate the issues with traditional security mechanisms by proposing continuous authentication (also known as active authentication) techniques [2]. These techniques typically collect biometric data from the device during use and compares the data to a user profile. Collected biometrics are either behavioural (e.g.: touch-screen gestures) or physiological (e.g.: fingerprint) [3]. Physiological biometrics often yield better results because they are not as susceptible to change. For this reason, facial recognition in continuous authentication schemes is an active research area.

Using transparently captured faces from mobile devices to authenticate was first proposed in studies such as [4] and [5]. Since then, however, the quality of cameras and computational power in devices has made facial recognition more feasible. Industry also has an interest in mobile face recognition with Google incorporating *Smart Lock*[1] into Android and Apple announcing *FaceID* for iPhone[2]. These approaches, however, use facial recognition in a one-time authentication process.

State-of-the-art research into continuous facial authentication sees schemes proposed that periodically (e.g.: every 30 seconds) capture facial images and authenticate them [6]. Such schemes leave windows of attack and can be seen as more periodic than continuous. Conversely, schemes that authenticate each available frame are computationally inefficient. Furthermore, state-of-the-art studies achieve results for robustness against attacks by testing the system using impostor faces only [7] and do not account for the possibility of facial spoof attacks [8]. We also find that such schemes do not account for variety in user activity during face recognition; a crucial area of exploration for real-world systems.

The main focus of this paper is producing novel components that form a facial authentication scheme that mitigates spoof attacks, properly continuously authenticates (rather than periodically) and provides insight into facial recognition in real-world scenarios. Our approach uses features extracted from a detected face to verify the liveness. We show the results of our face recognition approach on faces collected from different illumination conditions and different activities. We mitigate attack windows and improve efficiency by tracking authenticated faces rather than re-authenticating in subsequent video frames. The contributions of this paper are therefore threefold:

- We create a liveness detection component for use in continuous authentication schemes. It provides mitigation against 2D spoof attacks using printed faces or videos played in front of a mobile device camera. We test our liveness detection on different facial attributes.

Corresponding author: Max Smith-Creasey (email: Max.Smith-Creasey@city.ac.uk).

1. https://support.google.com/nexus/answer/6093922
2. https://www.apple.com/iphone-x/