Chapter 18

Multimodal Biometric Hand-Off for Robust Unobtrusive Continuous Biometric Authentication

P. Daphne Tsatsoulis
Carnegie Mellon University, USA

Robert Batie
Raytheon Company, USA

Aaron Jaech
Carnegie Mellon University, USA

Marios Savvides
Carnegie Mellon University, USA

ABSTRACT

Conventional access control solutions rely on a single authentication to verify a user's identity but do nothing to ensure the authenticated user is indeed the same person using the system afterwards. Without continuous monitoring, unauthorized individuals have an opportunity to "hijack" or "tailgate" the original user's session. Continuous authentication attempts to remedy this security loophole. Biometrics is an attractive solution for continuous authentication as it is unobtrusive yet still highly accurate. This allows the authorized user to continue about his routine but quickly detects and blocks intruders. This chapter outlines the components of a multi-biometric based continuous authentication system. Our application employs a biometric hand-off strategy where in the first authentication step a strong biometric robustly identifies the user and then hands control to a less computationally intensive face recognition and tracking system that continuously monitors the presence of the user. Using multiple biometrics allows the system to benefit from the strengths of each modality. Since face verification accuracy degrades as more time elapses between the training stage and operation time, our proposed hand-off strategy permits continuous robust face verification with relatively simple and computationally efficient classifiers. We provide a detailed evaluation of verification performance using different pattern classification algorithms and show that the final multi-modal biometric hand-off scheme yields high verification performance.

DOI: 10.4018/978-1-4666-2919-6.ch018

INTRODUCTION

The goal of continuous authentication is to prevent intruders from hijacking the user session of an authorized individual who may momentarily step away from his terminal. Access control has traditionally been achieved through means such as passwords and pass-cards. Passwords suffer from a variety of vulnerabilities including brute-force and dictionary based attacks. Pass-cards or other physical tokens used for authentication can be lost or stolen. Biometric systems identify a user based on characteristics such as face, iris or fingerprint which are tightly coupled with physical identity (Klosterman & Ganger, 2000). Biometrics can be continuously monitored which makes them an ideal solution for continuous authentication systems. This work focuses primarily on computer workstations, however, continuous authentication systems have been proposed for other environments. For example, Carillo (2003) outlines a design for continuous biometric authentication in airplane cockpits to prevent an unauthorized takeover of the aircraft.

The ideal continuous authentication system is fully transparent to the user who need not alter his routine to allow himself to be monitored continuously. Robust biometric modalities such as iris and fingerprint require cooperation from the user, usually in the form of touching some kind of biometric sensor or being at a fixed distance for suitable quality iris acquisition. These two modalities are not suitable for continuous and transparent monitoring. On the other hand, facial images can be used to identify an individual but not to the same degree of accuracy as iris and fingerprint especially when a longer interval has elapsed between testing and training.

A system that combines multiple biometrics benefits from the advantages of each modality. Typically, the stronger biometric will be used for the initial verification to establish the subject's identity. This modality can then hand control of the authentication system to another less intrusive biometric, such as facial modality, which begins to continuously take readings and has the ability to quickly train on the appearance of the authenticated user. This second biometric modality, although weaker when used as a stand-alone authentication solution, has an easier task to perform: it only needs to solve the following problem, "Is the user I see now the same as the one I just saw a moment ago?". It can incorporate temporal data from the recent past when making this decision. This strategy allows for continual and unobtrusive identity management.

During the last decade, new developments in hardware, such as the rapid increase in CPU clock speeds, the proliferation of multi-core CPUs and larger memory available in retail desktop machines, combined with computationally efficient face detection algorithms like the one developed by Viola and Jones (2004) have made it possible to design a real-time continuous authentication system that runs as a background process on a typical computer. Many laptops now ship with built-in web-cams convenient for the collection of application-relevant face image data, making them ideal mobile continuous authentication stations. This chapter gives an overview of a real continuous authentication system, which employs the aforementioned multi-biometric hand-off strategy. The application is light-weight in CPU and memory usage, so the typical user will not notice any reduction in performance while using the computer for his work as a result of our continuous system application running in the background. In our system, the initial static log-on uses a Daugman-style iris recognition approach (Daugman, 2004), followed by biometric hand-off to the face recognition component. We use the Viola-Jones face detection algorithm to detect faces, pre-process and crop them for different types of face recognition classifiers. Later in this chapter, we give a detailed background of the algorithms used in our application.

The verification accuracy of an authentication system designed in this manner can be experimen-