Chapter 12
Gaze Based Personal Identification

Clinton Fookes
Queensland University of Technology, Australia

Anthony Maeder
CSIRO ICT Centre, Australia

Sridha Sridharan
Queensland University of Technology, Australia

George Mamic
Queensland University of Technology, Australia

ABSTRACT

This chapter describes the use of visual attention characteristics as a biometric for authentication or identification of individual viewers. The visual attention characteristics of a person can be easily monitored by tracking the gaze of a viewer during the presentation of a known or unknown visual scene. The positions and sequences of gaze locations during viewing may be determined by overt (conscious) or covert (subconscious) viewing behaviour. Methods to quantify the spatial and temporal patterns established by the viewer for both overt and covert behaviours are proposed. The former behaviour entails a simple PIN-like approach to develop an independent signature while the latter behaviour is captured through three proposed techniques: a principal component analysis technique ('eigenGaze'); a linear discriminant analysis technique; and a fusion of distance measures. Experimental results suggest that both types of gaze behaviours can provide simple and effective biometrics for this application.

INTRODUCTION

The ability to recognise or authenticate an individual is an important capability required in many security solutions and is employed in a range of diverse sectors including finance, healthcare, transportation, entertainment, law enforcement, access control and border control. Traditional modes for person authentication including knowledge-based and token-based systems have obvious disadvantages due to the likelihood of theft, forgotten information and fraudulent reproduction. Biometric person recognition, however, has the ability to identify or

DOI: 10.4018/978-1-60566-725-6.ch012

authenticate an individual with much stronger certainty and relies on a person's physiological or behavioural traits (Ratha et. al 2003). Current biometric systems may make use of fingerprint, iris, retina, face, hand geometry, and palmprint (all which can be classed as physiological traits), signature, typing style and gait (which are behavioural traits) as well as voice (which is a combination of both physiological and behavioural traits) (Alexandre 1997, Ashbourn 2000, Crowley 1997).

Despite the enormous promise and potential capability of biometric technology, the uptake within industry and the community has not been as prolific as expected. This is likely due to a number of reasons:

1. There are challenges with the human interface, supporting ICT systems, and business process models that must be addressed with a practical implementation of any biometric system.
2. There are still several problems which are limiting the technology including problems such as noise in the sensed data (eg: acquired voice may be corrupted by background noise in a voice-based biometric system), intra-class variation (eg: testing lighting conditions may be different to enrolment lighting conditions in face biometrics), distinctiveness (eg: two people may have very similar hand geometry), and non-universality (eg: certain people have very faint fingerprints which cannot be used to extract suitable features) (Jain 2007).
3. Finally, most biometrics are not secret – they are often freely available and easy to acquire and this makes them prone to spoof attacks (for example, a photo of a person's face, or a copy of their fingerprint can be used to foil a biometric system).

While biometrics are harder to violate than pure knowledge-based or token-based systems, it is not impossible. Ideally, safer forms of biometrics would be based on non-visible and non-physiological information hidden deep within the person. Such a biometric could be based on behaviour or even thought processes. Gait recognition is an example of a behavioural biometric which is particularly hard to reproduce even though it is still visible. The downside for such biometrics is generally an increase in the intra-class variability, making the recognition process significantly harder and thus reducing recognition accuracies.

This chapter proposes to exploit the personal aspects of an individual's visual attention processes as a unique behavioural biometric which can be used for authentication or identification applications. The visual attention process of a person can easily be inferred through capturing their gaze (i.e. monitoring their viewing behaviour through measuring their eye movements). The approach relies on the principle that the human visual system requires the eye to rest motionless for short periods during its traversal of the viewing space, to assimilate detail at a given location in a visual scene. The assumption behind this biometric is that the viewing behaviour a person employs to gather information from a visual scene is inherently unique to that person. By detecting how and when the viewer looks at certain features in a presented scene, a signature for personal identification can be established and this is completely independent of other physiological measures of the viewer. The advantage of this approach is that it does not require physical contact between the viewer and a device, and at the same time it is difficult to detect by surveillance due to the close range nature of the monitoring required.

The viewing process can be directed overtly (consciously) or covertly (unconsciously). The later covert process is heavily related to the higher cognitive, psychological and neurological processes of that person. Thus, the process of utilising this information within a biometric system becomes one of identifying appropriate