

Chapter 4

Individual Identification from Video Based on “Behavioural Biometrics”

Y. Pratheepan

University of Ulster, UK

J.V. Condell

University of Ulster, UK

G. Prasad

University of Ulster, UK

ABSTRACT

This chapter presents multiple methods for recognizing individuals from their “style of action/actions,” that is, “biometric behavioural characteristics.” Two forms of human recognition can be useful: the determination that an object is from the class of humans (which is called human detection), and the determination that an object is a particular individual from this class (which is called individual recognition). This chapter focuses on the latter problem. For individual recognition, this chapter considers two different categories. First, individual recognition using “style of single action,” that is, hand waving and partial gait, and second, individual recognition using “style of doing similar actions” in video sequences. The “style of single action” and “style of doing similar actions,” that is, behavioural biometric characteristics, are proposed as a cue to discriminate between two individuals. Nowadays, multibiometric security systems are available to recognise individuals from video sequences. Those multibiometric systems are combined with finger print, face, voice, and iris biometrics. This chapter reports multiple novel behavioural biometric techniques for individual recognition based on “style of single action” and “style of multiple actions” (i.e., analysing the pattern history of behavioural biometric motion), which can be additionally combined with finger print, face, voice, and iris biometrics as a complementary cue to intelligent security systems.

DOI: 10.4018/978-1-60566-725-6.ch004

INTRODUCTION

A biometric is a unique, measurable characteristic or trait of a human being for automatically recognizing or verifying their identity. There are two types of biometrics that can be used for the purposes of human identification or verification: physical biometrics and behavioural biometrics. Physical biometrics, such as fingerprint and iris, have already been widely acknowledged and used in many real applications. Behavioural biometric is based on an action taken by a person (source: <http://www.authentec.com/technology-biometrics-overview.html> -retrieved on 29/08/2008.) and is generally very hard to copy from one person to another. It is well known that humans intuitively use some behavioural characteristics such as “gait” or “style of action” to recognize each other.

A biometric system is essentially a pattern recognition system which recognizes a user by determining the authenticity of a specific physiological or behavioural characteristic possessed by the user. Several important issues must be considered in designing a practical biometric system. They have the principles of acquisition, feature extraction, matching and decision in common (see Figure 1).

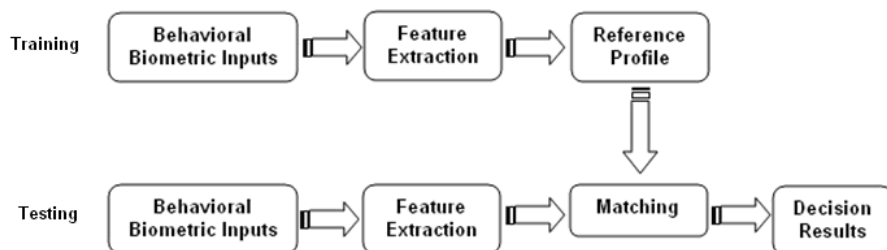
Depending on the context, a biometric system can operate either in a verification (authentication) or an identification mode. Verification (*Am I who I claim I am?*) involves confirming or denying a person’s *claimed identity*. On the other hand, in identification, the system has to recognize a person

(*Who am I?*) from a list of N users in the template database. Identification is a more challenging problem because it involves 1: N matching compared to 1:1 matching for verification. This chapter considers individual identification problem rather than individual verification problem.

In intelligent security systems, identification of humans and their activities is generally one of the most important tasks. Examples of such systems are intelligent security systems that detect unknown or suspicious people entering restricted door entrances or an interface robot that acts as an interface for taking known users’ commands and presenting results. Consider a scenario that if a person needs to go through a security enabled door then he/she may need to prove his/her identity. An intelligent security system should offer a natural and reliable solution to the problem of identifying a person based on “who is he/she” rather than “what he/she knows” (i.e. password) or “what he/she carries” (i.e. key or ID cards) (Jain, Bolle & Pankanti, 1999).

As a relatively new technology, behavioural biometrics help to identify a person’s identity through some measurable activity patterns, e.g., speaker recognition (i.e., analyzing vocal behaviour), signature recognition (i.e., analyzing signature dynamics), gait recognition (i.e., analyzing walking patterns), keystroke dynamics (i.e., analyzing keyboard typing patterns), mouse dynamics (i.e., analyzing mouse moving patterns), etc. Recently security systems operate using multi-biometric techniques, combined with anatomical

Figure 1. Basic structure of behavioural biometrics systems



24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/individual-identification-video-based-behavioural/36915

Related Content

An Enhanced Computational Fusion Technique for Security of Authentication of Electronic Voting System

Adewale Olumide Sunday, Boyinbode Olutayo and Salako E. Adekunle (2020). *International Journal of Smart Security Technologies* (pp. 22-37).

www.irma-international.org/article/an-enhanced-computational-fusion-technique-for-security-of-authentication-of-electronic-voting-system/259322

On Automated Generation of Keyboard Layout to Reduce Finger-Travel Distance

Amol D. Mali and Nan Yang (2017). *International Journal of Monitoring and Surveillance Technologies Research* (pp. 29-43).

www.irma-international.org/article/on-automated-generation-of-keyboard-layout-to-reduce-finger-travel-distance/185800

Tensor Space

David Zhang, Fengxi Song, Yong Xu and Zhizhen Liang (2009). *Advanced Pattern Recognition Technologies with Applications to Biometrics* (pp. 135-149).

www.irma-international.org/chapter/tensor-space/4279

A Novel Hybrid Cyber Range for Security Exercises on Cyber-Physical Systems

Bil Hallaq, Andrew Nicholson, Richard Smith, Leandros Maglaras, Allan Cook, Helge Janicke and Kevin Jones (2021). *International Journal of Smart Security Technologies* (pp. 16-34).

www.irma-international.org/article/a-novel-hybrid-cyber-range-for-security-exercises-on-cyber-physical-systems/272099

Brain-Computer Interfaces and Visual Activity

Carmen Vidaurre, Andrea Kübler, Michael Tangermann, Klaus-Robert Müller and José del R. Millán (2012). *Gaze Interaction and Applications of Eye Tracking: Advances in Assistive Technologies* (pp. 153-174).

www.irma-international.org/chapter/brain-computer-interfaces-visual-activity/60039