

Chapter 3

Performance Evaluation of Behavioral Biometric Systems

F. Cherifi

University of Caen, France

B. Hemery

University of Caen, France

R. Giot

University of Caen, France

M. Pasquet

University of Caen, France

C. Rosenberger

University of Caen, France

ABSTRACT

We present, in this chapter, an overview of techniques for the performance evaluation of behavioral biometric systems. The BioAPI standard that defines the architecture of a biometric system is presented in the first part of the chapter. The general methodology for the evaluation of biometric systems is given including statistical metrics, definition of benchmark databases, and subjective evaluation. These considerations rely with the ISO/IEC19795-1 standard describing the biometric performance testing and reporting. The specificity of behavioral biometric systems is detailed in the second part of the chapter in order to define some additional constraints for their evaluation. This chapter is dedicated to researchers and engineers who need to quantify the performance of such biometric systems.

INTRODUCTION

Biometrics is now a technology that is present in our daily life. It is used as for example in airports (passport verification), offices (access control,

biometric USB key...) and even in some places in the world for banking operations... Different biometric modalities can be used for the identification / verification of an individual (face recognition, keystroke dynamics recognition, DNA analysis...) (Mahier et al., 2008).

DOI: 10.4018/978-1-60566-725-6.ch003

The characterization of a human by considering its behavior in its daily life operations (gait, signature dynamics, voice...) (Han et al. 2006; Muramatsu & Matsumoto, 2007; Petrovska-Delacretaz et al., 2007) or through its interactions with a computer (mouse dynamics, keystroke dynamics...) represents an interesting and open area in research (Hwang et al., 2006; Orozco et al., 2006).

The performance evaluation of such biometric systems is very important for many reasons:

- To be used in a real (that is to say in an industrial) context, the quality of a biometric system must be precisely quantified. The context of use, the efficiency, the robustness of the algorithm must be defined to determine if it fulfills the requirements of a particular industrial application (logical access, physical access, e-commerce...);
- The comparison of different biometric modalities is essential to qualify their relative advantages and drawbacks;
- The performance evaluation is also necessary in order to facilitate the research in this field (Hemery et al., 2006). We need a reliable evaluation method in order to put into obviousness the benefit of a new biometric system.

The objective of this chapter is to make an overview on evaluation techniques that are used in the state of the art to quantify the performance of behavioral biometric systems. An engineer or a researcher will find in the proposed chapter, the different criteria or methods he can use to validate a biometric system he intends to use in a real context. A behavioral biometric system can be evaluated by considering the general approach to evaluate a biometric system while taking into account the specificity of this type of modality.

The plan of the chapter is given below. In the section 1, we present the general approaches for the evaluation of a biometric system. It necessitates generally to use a benchmark database (Hemery

et al., 2007) and a set of criteria (computation time, FAR...). The benchmark database can be composed of real biometric templates or synthetic ones. We present different solutions from the state of the art. Section 3 focuses on specificities of behavioral biometric systems. We present their specificities that must be taken into account for their evaluation. Section 4 concerns the future trends that must be achieved in order to facilitate research progress in this domain. We conclude this chapter in section 5.

GENERAL EVALUATION METHODOLOGIES

Introduction

A biometric system is composed of different steps (see Figure 1). There are mainly two processes in the use of a biometric system. The enrollment phase has for objective to determine a model of an individual given the characteristics acquired by the selected biometric sensor. The identification / verification phase uses this model to make a decision on an individual.

The international standards committee for biometrics within ISO (ISO/IEC JTC1 SC37) developed a complete specification and reference implementation for a standardized API (BioAPI Consortium, 2005). The purpose of the BioAPI Specification is to define an open system standard application program interface (API) which allows software applications to communicate with a broad range of biometric technologies in a common way.

Figure 2 shows the interaction between the three BioAPI 2.0 components: applications, BioAPI Framework, and BSPs (Biometric Service Providers). The BioAPI 2.0 specification implements two APIs. The first one is the API which is the interface between the BioAPI Framework which supports the functions in the API specification and application. The second is

16 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/performance-evaluation-behavioral-biometric-systems/36914

Related Content

Application of Artificial Neural Networks to Reliable Nuclear Data for Nonproliferation Modeling and Simulation

Pola Lydia Lagari, Vladimir Sobes, Miltiadis Alamaniotis and Lefteri H. Tsoukalas (2016). *International Journal of Monitoring and Surveillance Technologies Research* (pp. 54-64).

www.irma-international.org/article/application-of-artificial-neural-networks-to-reliable-nuclear-data-for-nonproliferation-modeling-and-simulation/180666

Evolutionary Methods for Analysis of Human Movement

Rahman Davoodi and Gerald E. Loeb (2006). *Computational Intelligence for Movement Sciences: Neural Networks and Other Emerging Techniques* (pp. 281-298).

www.irma-international.org/chapter/evolutionary-methods-analysis-human-movement/6815

Computer Architecture: A New Weapon to Secure Web Services From Bots

Amit Kumar Singha and Geeta Chhabra Gandhi (2020). *International Journal of Smart Security Technologies* (pp. 41-48).

www.irma-international.org/article/computer-architecture/251909

Extended Automata for Temporal Planning of Interacting Agents

Christine Largouët, Omar Krichen and Yulong Zhao (2017). *International Journal of Monitoring and Surveillance Technologies Research* (pp. 30-48).

www.irma-international.org/article/extended-automata-for-temporal-planning-of-interacting-agents/182505

Intention-Based Decision Making via Intention Recognition and its Applications

The Anh Han and Luis Moniz Pereira (2013). *Human Behavior Recognition Technologies: Intelligent Applications for Monitoring and Security* (pp. 174-211).

www.irma-international.org/chapter/intention-based-decision-making-via/75291