Chapter 15

A Wrapper–Based Classification Approach for Personal Identification through Keystroke Dynamics Using Soft Computing Techniques

Shanmugapriya D.
Avinashilingam Institute for Home Science and Higher Education for Women, India

Padmavathi Ganapathi
Avinashilingam Institute for Home Science and Higher Education for Women, India

ABSTRACT

The password is the most widely used identity verification method in computer security domain. However, due to its simplicity, it is vulnerable to imposters. A way to strengthen the password is to combine Biometric technology with password. Keystroke dynamics is one of the behavioural biometric approaches which is cheaper and does not require any sophisticated hardware other than the keyboard. The chapter uses a new feature called Virtual Key Force along with the commonly extracted timing features. Features are normalized using Z-Score method. For feature subset selection, Particle Swarm Optimization wrapped with Extreme Learning Machine is proposed. Classification is done with wrapper based PSO-ELM approach. The proposed methodology is tested with publically available benchmark dataset and real time dataset. The proposed method yields the average accuracy of 97.92% and takes less training and testing time when compared with the traditional Back Propagation Neural Network.

INTRODUCTION

The confidential information can be secured from unauthorized users by providing authentication. User authentication is defined as the process of verifying the identity claimed by an individual. User Authentication is normally classified into three categories namely, Knowledge based Authentication, Object based Authentication, and Biometric based Authentication (Lawrence O’Gorman, 2003) which is shown in Figure 1.

DOI: 10.4018/978-1-5225-0703-1.ch015
Knowledge based Authentication is based on “something the user knows”. User name and passwords come under this category. However, passwords are vulnerable to password hackers because the users sometimes can’t remember the strong passwords and they write them down. Something the user has or possesses is called Object based authentication. Tokens or Personal Identification Numbers (PINs) are the widely used examples of this type of authentication. Tokens are easy to misplace or damage and PINs are vulnerable to shoulder surfing and systematic trial-and-error attacks (Seong-seob Hwang, Cho and Park, 2009). Biometric based authentication provides a very reliable method of authenticating a
Related Content

The Case for Privacy Awareness Requirements
www.igi-global.com/chapter/the-case-for-privacy-awareness-requirements/213828?camid=4v1a

A Framework for Protecting Users' Privacy in Cloud
www.igi-global.com/chapter/a-framework-for-protecting-users-privacy-in-cloud/213812?camid=4v1a

Collective Event Detection by a Distributed Low-Cost Smart Camera Network
www.igi-global.com/chapter/collective-event-detection-by-a-distributed-low-cost-smart-camera-network/213838?camid=4v1a
Border Security and Cooperative Initiatives to Counter Illicit Drug Trafficking: The Case of Jamaica and the USA
www.igi-global.com/chapter/border-security-and-cooperative-initiatives-to-counter-illicit-drug-trafficking/164719?camid=4v1a