Chapter 19
User Authentication Based on Dynamic Keystroke Recognition

Khaled Mohammed Fouad
Benha University, Egypt

Basma Mohammed Hassan
Benha University, Egypt

Mahmoud F. Hassan
Benha University, Egypt

ABSTRACT

Biometric identification is a very good candidate technology, which can facilitate a trusted user authentication with minimum constraints on the security of the access point. However, most of the biometric identification techniques require special hardware, thus complicate the access point and make it costly. Keystroke recognition is a biometric identification technique which relies on the user behavior while typing on the keyboard. It is a more secure and does not need any additional hardware to the access point. This paper presents a developed behavioral biometric authentication method which enables to identify the user based on his Keystroke Static Authentication (KSA) and describes an authentication system that explains the ability of keystroke technique to authenticate the user based on his template profile saved in the database. Also, an algorithm based on dynamic keystroke analysis has been presented, synthesized, simulated and implemented on Field Programmable Gate Array (FPGA). The proposed algorithm is tested on 25 individuals, achieving a False Rejection Rate (FRR) about 4% and a False Acceptance Rate (FAR) about 0%. This performance is reached using the same sampling text for all the individuals. In this paper, two methods are used to implement the proposed approach: method one (H/W based Sorter) and method two (S/W based Sorter) are achieved execution time about 50.653 ns and 9.650 ns, respectively. Method two achieved a lower execution time; the time in which the proposed algorithm is executed on FPGA board, compared to some published results. As the second method achieved a small execution time and area utilization so it is the preferred method to be implemented on FPGA.

DOI: 10.4018/978-1-5225-0808-3.ch019
1. INTRODUCTION

The word “Biometric” is an ancient Greek word which refers to bio means “life” and metric means “measure” (Babaeizadeh et al., 2015). Biometric authentication supports three important factors of information security system. These factors are authentication, identification, and non-repudiation (Smith et al., 2013). Authorization and Authentication (Emam, 2013) are kind of security and privacy issues of biometric authentication system. However, a lot of research discussed this problem and tried to introduce many solutions to decrease the gap among security, authentication and security environment which prevents the spread of that technology. Biometrics (Jaiswal et al., 2011) is a set of technologies based on the measurement of unique behavioral or physical characteristics for the purpose of identifying or authentication an individual (Bandara et al., 2015).

Biometric authentication systems (BAS) are believed to be the effective technologies compared to the traditional authentication methods such as passwords, tokens and PINs (Tin, 2015) that failed to keep up with the challenges presented because they can be stolen or lost (Babaeizadeh et al., 2015), this means infirm security system. Authentication types can be classified under three different security field (Liu et al., 2001) such as Table 1 shows an overview of different authentication approaches:

- **Something you Know**: Something only you remember like password, PIN, or a piece of personal information such as (where are you born?) and knowledge approaches.
- **Something you Have**: Something only you possess such as a Smart card, Card key or a token approaches like a secure – ID card.
- **Something you Are**: Some biometric property.
- **Combinations**: (Multiple factors)

Biometric authentication classifications consist of two types Physical and behavioral biometrics (Jaiswal et al., 2011) as shown in Figure 1

- **Physiological Biometrics**: Based on data derived from direct measurement of a part of the human body and relies on something the users are such as fingerprint (Cao, 2013), iris (LI, 2015), face (ACO, 2015; Ghanavati, 2015), hand geometry (Guo, 2012), retina (Kochetkov, 2013; Javier et al., 2013) as well as Palm prints (Lee, 2012; Wu et al., 2013) recognitions.
- **Behavioral Biometrics**: Based on the user’s behavior such as signature (Shah et al., 2015), voice (Rudrapal, 2012) and keystroke dynamics (Babich, 2012).

<table>
<thead>
<tr>
<th>Approach</th>
<th>Advantage</th>
<th>Disadvantage</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge</td>
<td>Effortless High acceptance</td>
<td>Forgotten Shoulder spoofing</td>
<td>Password, PIN</td>
</tr>
<tr>
<td>Token</td>
<td>Cheap Simple deployment</td>
<td>Lost, theft</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Biometrics</td>
<td>Deter sharing Unique Unforgettable</td>
<td>Cost Invasive</td>
<td>Fingerprint, Voice, Keystroke</td>
</tr>
</tbody>
</table>

**Table 1. Overview of different authentication approaches**
33 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:
www.igi-global.com/chapter/user-authentication-based-on-dynamic-keystroke-recognition/167237?camid=4v1

www.igi-global.com/e-resources/library-recommendation/?id=1

Related Content

Web Service Security: Authentication and Authorization Technologies
www.igi-global.com/chapter/web-service-security/105805?camid=4v1a

Risk Assessment Using AHP in a Petrochemical Engineering Case Study
www.igi-global.com/article/risk-assessment-using-ahp-petrochemical/77905?camid=4v1a

The Impact of the Sarbanes-Oxley (SOX) Act on Information Security
www.igi-global.com/chapter/impact-sarbanes-oxley-sox-act/23240?camid=4v1a

Information Technology Security Concerns in Global Financial Services Institutions: Do Socio-Economic Factors Differentiate Perceptions?
www.igi-global.com/article/information-technology-security-concerns-global/34059?camid=4v1a