Chapter 11
An Effective Combination of Pattern Recognition and Encryption Scheme for Biometric Authentication Systems

Vijayalakshmi G. V. Mahesh
https://orcid.org/0000-0002-1917-7506
BMS Institute of Technology and Management, India

ABSTRACT

Authentication based on biometric technology is largely preferred in providing access control to the systems. This technology has gained wider attention due to the rise in data generation and the need of data security. The authentication depends upon the physiological traits of human such as face, fingerprint, hand geometry, iris scan, retinal scan, and voice. Depending upon the level of security required, a single trait or multiple traits could be utilized. The key features or patterns extracted from the biometric data play a significant role during authentication process that involves pattern recognition. That is, the patterns that exist in the database are matched with the patterns provided during log on. The access is provided based on complete match. Though biometry-based authentication systems provide an effective way of accessing the system, still it is affected by attacks that try to get unauthorized entry into the system. Thus, this chapter focuses on working with the methodologies that provide additional security to the biometric authentication system by utilizing encryption algorithm.

1. INTRODUCTION

The process of authentication is significant related to any system's security as it verifies the user before providing access to the system. Authentication is a part of three step procedure for obtaining access to a resource or system ie., identification, authentication and authorization. Authentication falls into the following types:

DOI: 10.4018/979-8-3693-1642-9.ch011

Copyright © 2024, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

(i) Knowledge based or password based authentication: this is the most frequently used method for gaining access. But passwords are reused by the users, they are easy to guess and break. The user accounts here are vulnerable to brute force and phishing attacks.

(ii) Two factor authentication: Most commonly known as 2FA. This method is improved version of the knowledge based method as the user has to provide an additional authentication feature apart from the password. The additional feature can be rather like One time password which is shared to the user through email or SMS. The 2FA is more secured as the attacker needs additional information along with login credentials to break in to the system but there is also a possibility of SMS and email breach.

(iii) Single sign on authentication: Here identity provider is used by the user to have an account and the user is verified by identity provider. User with single set of credentials can access multi resources. The benefit of the method lies in reduction of the credentials a user needs to remember. With this method, the attackers can gain access to the systems if identity provider is data breached.

(iv) Token based authentication: In this method user uses token that verifies the identity of the user. Token based authentication relies on physical token such as physical devices: Smart card, Smart key, Smart phone and Computer system or web token to gain access to a system. Tokens need to be kept track of if otherwise leads to locking of the user accounts.

(v) Certificate based authentication: In this authentication method, digital certificates which are the electronic documents with important details generated from public key cryptography are distributed by the certificate authority to identify the users before gaining access to the systems. They are resistant to phishing attacks, also are expensive and time consuming to establish.

(vi) Biometric authentication: In this method, a person's unique physical and behavioral traits that include: face, voice, iris/retina, palm, gait, voice, finger print, shape of ears, facial thermograms and physiological signals are used to gain access to the system. Unlike other methods it is easier to deploy, need not remember and recall and difficult to hack.

Though biometric authentication is proved to be more secure as the physical and behavioral traits of a person are distinct but still is affected by attacks such as spoofing where the attacker masquerades as the authenticated user. With the development of secure cryptographic algorithms one can provide privacy protection to the biometric template. Thus during enrolment, the biometric trait is encrypted to form encrypted-biometric template, further features/patterns are derived from the encrypted template and stored. During verification process, user presents the biometry to the system where the features or the patterns are compared with that of the stored patterns to find the match and thus grant the access while the non-match will result in the discard of the input trait. The chapter presents and discusses about the encryption of the biometric data for authentication in a pattern recognition(PR) approach.

The next section (section 2) presents a review of the literature survey on biometric authentication. Then it is followed by methodology section (section 3) that describes the overall framework and giving details about the biometric data used, encryption scheme, the feature extraction and selection methods. This section The performance metrics used for the evaluation are also presented here. The results and discussion is presented in section 4. The conclusion of the chapter is provided in section 5.

19 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/an-effective-combination-of-pattern-recognition-and-encryption-scheme-for-biometric-authentication-systems/340980

Related Content

A Survey of Cryptographic Data Protection and Machine Learning
V. R. Kanagavalliand A. Meenakshi (2024). *Machine Learning and Cryptographic Solutions for Data Protection and Network Security (pp. 1-11).*
www.irma-international.org/chapter/a-survey-of-cryptographic-data-protection-and-machine-learning/348598

Information Security-Based Nano- and Bio-Cryptography
W. K. Hamoudiand Nadia M. G. Al-Saidi (2014). *Multidisciplinary Perspectives in Cryptology and Information Security (pp. 179-199).*
www.irma-international.org/chapter/information-security-based-nano--and-bio-cryptography/108030

Efficient Energy Saving Cryptographic Techniques with Software Solution in Wireless Network
Alka Prasad Sawlikar, Zafar Jawed Khanand Sudhir Gangadharrao Akojwar (2020). *Cryptography: Breakthroughs in Research and Practice (pp. 159-179).*
www.irma-international.org/chapter/efficient-energy-saving-cryptographic-techniques-with-software-solution-in-wireless-network/244912

Secure Multi-Party Computation (SMPC) Protocols and Privacy
Mosiur Rahaman, Varsha Arya, Sheila Mae Orozcoand Princy Pappachan (2024). *Innovations in Modern Cryptography (pp. 190-214).*
www.irma-international.org/chapter/secure-multi-party-computation-smpc-protocols-and-privacy/354040

Zero Knowledge Proofs and Their Applications in Cryptography: Advancements, Challenges, and Future Aspects
Tanish Aggarwal, Sudhakar Kumar, Sunil K. Singh, Brij B. Gupta, Nadia Nedjahand Arcangelo Castiglione (2024). *Innovations in Modern Cryptography (pp. 55-74).*
www.irma-international.org/chapter/zero-knowledge-proofs-and-their-applications-in-cryptography/354035