


Chapter 17

Implementing Information Security Using Multimodal Biometrics

Vinita Jindal

 <https://orcid.org/0000-0002-0481-4840>

Keshav Mahavidyalaya, University of Delhi, India

Divya Singhal

 <https://orcid.org/0000-0003-3223-7451>

Keshav Mahavidyalaya, University of Delhi, India

ABSTRACT

With the exponential growth of smart devices and dependency on the internet and wireless networks, the security of information is a major challenge in the recent years. Biometrics have been widely used for information security. It plays a crucial role in minimizing the probability of inappropriate access. Human biometrics are characterized into physical and behavioral features. In this chapter, the authors propose to use fingerprint and online signature for information security. Though biometric provides more security and integrity, it is also threatened by various attacks. Digital watermarking is the answer to the above problems. Initially, the features of the human biometric images are extracted and act as watermarks for other biometric image. It is assumed that fingerprints act as a host and a signature as watermark. This chapter presents a survey of various biometric and watermarking techniques. The chapter also reviewed the work done by different researchers in the area, algorithms employed by them with their literature to utilize them for biometric protection.

INTRODUCTION

The increasing usage of internet access and digital media has grown tremendously in the past few years. The advancement in technology and electronics media have put the protection of Information Security at risk due to the fact that digital data can be copied without any degradations to the quality of content.

DOI: 10.4018/978-1-7998-5728-0.ch017

Information security can be defined as the process of preservation of confidentiality, integrity and availability of information that can be either in printed or in written form. It not only protects the information, but also its associated elements such as hardware and software that stores and transmits the information. Intellectual Property Rights (IPR), Copyright protection and authentication are the types of Information Security. IPR prevents others from using, dealing, or tampering with his/her product without prior permission. Copyright protection generally applies to a range of creative, artistic, or intellectual works such as novels, poetry, songs, movies, software, and architecture. It does not protect the information or ideas, but, it protects the original expression of ideas and information. The researchers in their work used a SHA-1 160 bits hash function rather than MD5 to prevent the tampering of web resources (He, 2016). The Authentication access of such systems is controlled by recognizing passwords or personal identification numbers. The problem with this system is that an unauthorized user can access the password and numbers quite easily. Thus, it is necessary to add a security check to the data to protect its true ownership.

There are many solutions to the prevention of IPR problem and among these, biometric methods seem to be the most promising ones. The growing demand for reducing the instances of fraud and data breaches as well as the need for physical access control and logical access control have made biometrics a very strong authentication technique. Token based and knowledge-based identification systems are easily associated to being stolen or damaged. In legacy systems such as passwords and PINs, weak passwords are raising security issues, even the strongest password cannot resist sophisticated hacker attacks. The advancement in digital transactions necessitates the utilization of reliable factors such as human biometric features which are an intrinsic part of each person and are impossible to lose or forget. The primary objective of biometric is to provide non- repudiation which ensures that the person who uses the resources can not deny later of practicing it.

Both governments and private organizations worldwide, choosing biometric technology to fight against fraudulent users, leak of confidential data, security breaches, reduce costs, flexibility and to improve the overall user experience. Hence, Biometrics technology is requisite for today's personal identification and verification systems. Mostly, the requirement of imperceptibility is satisfied by using human physiological features such as Human Audible System, Human Visual System, and Biometric Authentication System. Even though the biometrics offer a reliable method for personal identification, security of the biometric authentication systems are a matter of concern. Passwords can be kept secret and stored in a safe location, however biometrics are public in nature and can be found easily by the hackers. All body characteristics that are used in biometrics are exposed to the public wherever the person goes. Fingerprints are left on anything a person touches, and eyes are given away when the person uses them to see things. A person's voice can be recorded easily using a smartphone by a bystander. There is also no way for a user to simply reset their biometric marker like getting a new password. If a fingerprint or facial image is stolen, the user cannot be simply given a new one. Passwords can be changed, but biometric markers are basically fixed for an individual's life span.

It should also be noted that biometric systems work with accuracy only when it is confirmed that the data is entered from some legitimate source and that data has not been changed or tampered. Gaata et al. in their paper reviewed that watermarking techniques have the potential to safeguard the authenticity of the biometric data (Gaata & Refah, 2016). Digital watermarking helps to embed the information into some multimedia file without presenting any visible deviation in the original file. The purpose of using this technique is to introduce a high level of protection. Inserting information at random locations without harming the actual features of biometric data helps in claiming the identity of an authorized user. As a result, a watermarking technique is imperceptible and robust to unauthorized persons.

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/implementing-information-security-using-multimodal-biometrics/261737

Related Content

SecBrain: A Framework to Detect Cyberattacks Revealing Sensitive Data in Brain-Computer Interfaces

Enrique Tomás Martínez Beltrán, Mario Quiles Pérez, Sergio López Bernal, Alberto Huertas Celdrán and Gregorio Martínez Pérez (2022). *Advances in Malware and Data-Driven Network Security* (pp. 176-198). www.irma-international.org/chapter/secbrain/292237

Automated Formal Methods for Security Protocol Engineering

Alfredo Pironti, Davide Pozza and Riccardo Sisto (2012). *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies* (pp. 138-166). www.irma-international.org/chapter/automated-formal-methods-security-protocol/56300

A Policy-Based Authorization Framework for Web Services: Integrating X-GTRBAC and WS-Policy

Rafae Bhatti, Daniel Sanz, Elisa Bertino and Arif Ghafoor (2008). *Securing Web Services: Practical Usage of Standards and Specifications* (pp. 138-161). www.irma-international.org/chapter/policy-based-authorization-framework-web/28517

Identification of Vulnerabilities in Web Services using Model-Based Security

Sebastian Höhn, Lutz Lowis, Jan Jürjens and Rafael Accorsi (2010). *Web Services Security Development and Architecture: Theoretical and Practical Issues* (pp. 1-32). www.irma-international.org/chapter/identification-vulnerabilities-web-services-using/40584

Trust and Voice Biometrics Authentication for Internet of Things

Alec Wells and Aminu Bello Usman (2023). *International Journal of Information Security and Privacy* (pp. 1-28). www.irma-international.org/article/trust-and-voice-biometrics-authentication-for-internet-of-things/322102