Chapter 77
Advances in Biometrics for Secure Human Authentication System:
Biometric Authentication System

Jagannath Mohan
VIT University, India

Adalarasu Kanagasabai
PSNA College of Engineering and Technology, India

Vetrivelan Pandu
VIT University, India

ABSTRACT

In the recent decade, one of our major concerns in the global technological society of information security is confirmation that a person accessing confidential information is authorized to perform so. Such mode of access is generally accomplished by a person's confirming their identity by the use of some method of authentication system. In present days, the requirement for safe security in storing individual information has been developing rapidly and among the potential alternative is implementing innovative biometric identification techniques. This chapter discusses how the advent of the 20th century has brought forth the security principles of identification and authentication in the field of biometric analysis. The chapter reviews vulnerabilities in biometric authentication and issues in system implementation. The chapter also proposes the multifactor authentication and the use of multimodal biometrics, i.e., the combination of Electrocardiogram (ECG) and Phonocardiogram (PCG) signals to enhance reliability in the authentication process.

DOI: 10.4018/978-1-5225-0983-7.ch077

INTRODUCTION

Security plays an important part in contemporary day situation where identity fake and radicalism possesses biggest risk. These continually increasing criminal and terrorist acts in government/private properties, public places resulted in chaotic scenarios thereby making the existing security systems questionable – "How effective is the security system to prevent unlawful activities?", "Does the existing system guarantee the required level of security?", "Is the system user friendly?". In early stages, the identity management systems relied on cryptographic methods (knowledge based) requiring the users to remember a secret text (password) or keep something with them (token, card) or a combination of both to prove their identity. Consequently, the population is flooded with passwords and tokens to gain access to required resources for instance; access control, computer logins, e-mail checking, making internet banking, conflict zones etc. However, the users challenged the efficacy of such systems through the queries such as, "What happens, if I forget/lost my password/token?", "How many passwords/cards I have to remember/keep?". As an answer, from the middle of the 20th century, the rise of new technologies in order to assess bodily or behavioural features of human has given the word, Biometry, a newer connotation for security applications. The idea of human identification and authentication based on bodily (physiological) or behavioural attributes of individuals is proposed and very often termed as Biometrics. Biometrics is described as programmed recognition of persons based on their unique bodily (iris, face, fingerprint, etc.) or behavioural (voice, signature, gait, etc.) characteristics (Jain et al., 2004; Jain & Kumar, 2012). In modern decade, the need for improvement in security for personal information storage has grown steeply and among the expedient alternatives is one which employs inventive biometric system. Although biometrics is not the perfect solution but it offers several advantages over knowledge and possession based approaches in the way that there is no need to remember anything, biometric attributes cannot be lost, transferred or stolen, offer better security due to fact that these attributes are very challenging to falsify and involve the manifestation of honest user while permitting access to specific resources. Inspired from the development of Bertillon's system in 1883 to Sir John Galton's elementary fingerprint recognition system in 1903, the research community devoted their efforts to discover several biometric modalities.

Any physiological or behavioral attribute can qualify for being a biometric trait unless it satisfies the criteria such as:

1. **Universality:** Possessed by all humans,
2. **Distinctiveness:** Discriminative amongst the population,
3. **Invariance:** The selected biometric attribute must exhibit invariance against time,
4. **Collectability:** Easily collectible in terms of acquisition, digitization and feature extraction from the population,
5. **Performance:** Pertains to the availability of resources and imposition of real constraints in terms of data collection and guarantee to achieve high accuracy,
6. **Acceptability:** Willingness of population to submit that attribute to recognition system, and
7. **Circumvention**: Prone to imitation or mimicry in case of fraudulent attacks against the recognition system (Jain et al., 2004).

Based on the criteria, several distinctive human characteristics are identified and tested. Instead of the broad categories (physiological, behavioral and soft attributes), for convenience the physiological