Chapter 4

Biometrics for Forensic Identification in Web Applications and Social Platforms Using Deep Learning

Shefali Arora
Netaji Subhas Institute of Technology, India

M. P. S. Bhatia
Netaji Subhas Institute of Technology, India

ABSTRACT

Biometric authentication is being increasingly used in various applications to identify people using various traits. This can be of use in various applications like forensics, passport control, etc. In the rapidly growing era of internet, it is necessary to restrict access to data on the web. Security and customer usage are some of the essential parameters which should be taken care of in a web biometric system. Also, biometric technology has been implemented on social media platforms so as to save users from cyber-attacks and breach of privacy. This chapter provides an overview of how a web biometric system works, with an approach to use deep learning algorithms to identify traits like face, iris, and fingerprints. Such techniques can also be used to authenticate people in e-commerce applications. Further, the authors discuss the implementation of biometric verification techniques on social networking platforms like Facebook, Twitter, etc.

DOI: 10.4018/978-1-5225-9554-0.ch004
INTRODUCTION

As the popularity of the Internet has increased, there is a growing need to identify people who access sensitive content on the Web. Most of the web applications ensure the security of their services by using passwords (Duic, Cvrtila & Ivanjko, 2017). However, it is easy to intercept passwords of people. Moreover, intrusion into personal accounts has become common, thus leading to cybercrimes. Therefore, the concept of using biometric authentication is gaining popularity in web systems because biometric authentication is reliable and is an important technique (Saini & Kumar Kapoor, 2016) to identify criminals by using physical traits (such as fingerprints, facial patterns and iris scans) and behavioural traits (such as signature and voice).

The choice of a biometric trait depends on the following factors:

- **Universality**: Every individual should possess the biometric trait.
- **Uniqueness**: Each should have a unique trait.
- **Permanence**: The trait should not change over time.
- **Performance**: Given the limitations of an individual, the traits should be recognized with high accuracy.

Thus, a biometric system acquires data from an individual, extracts features from the available data, and compares these features with a set of templates that are already input in the system database (Mayron 2015). Biometric systems can be divided into two categories based on the mode of application:

- **Identification**: A biometric system searches among all the existing templates stored in its database and compares the features to prove a person’s identity. Thus, the system performs a 1:N comparison, and this process is slower than verification because the template is matched with all other templates in the database. The response validates the identity of the individual.
- **Verification**: This is a one-to-one comparison technique in which an individual's information is compared with his template in the database. For example, an individual's fingerprint is captured digitally through an application. The system then compares the fingerprints to verify if the fingerprint belongs to this individual.

Figure 1 displays the working of a biometric matcher in a web application. In a biometric matcher, features are either extracted and identified or verified through templates that are already stored in the database to allow access to a user.
Communiqué Issues in MANET and VANET Protocols With Network Security Disquiet