Chapter 24
Watermarking of Data Using Biometrics

Swanirbhar Majumder
Deemed University, India

Tirtha Sankar Das
RCC Institute of Information Technology, India

ABSTRACT

These days, for the copyright protection and security of multimedia data in this age of the tech-savvy world, watermarking is a very important technique. Moreover, with the inclusion of biometrics for the watermarking schemes, the concept of "something you are" is included in the watermark and/or cover image. This thereby increases the security intensity in the multimedia data. And to give a glimpse of the technique the concepts of Watermarking, biometric and watermarking using biometrics is discussed. Finally, a particular case of real time watermarking of data using biometric is discussed by specifying a practical example.

INTRODUCTION

The practice of hiding a message about an image, audio clip, video clip, or other work of multimedia within that work itself is called watermarking. It is mainly of two basic types; visible and invisible. Visible ones are commonly available in currency notes, stamp papers, etc. The invisible or the imperceptible variant is the one that will be discussed here. Alternately, watermarking can be considered as the practice of imperceptibly altering a work to embed a message about that work. Watermarking has been practiced and has existed for quite long, at least several centuries, if not the millennia—the field of digital watermarking only gained widespread popularity as a research topic in the latter half of the 1990s as per the earlier books that have devoted substantial space to the subject of digital watermarking. However, here in this chapter the watermarking involves a special data type which is related to us the biological beings as our individualistic traits, either characteristic wise or behavioral, i.e., the biometric.

DOI: 10.4018/978-1-4666-2518-1.ch024

Watermarking, information hiding and steganography are the three fields that have a great deal of overlapping but there are fundamental philosophical differences affecting the requirements. Information or data hiding encompasses a wide range of problems beyond that of embedding messages in content, referring to make the information imperceptible or keeping the existence of the information secret or even maintaining anonymity while using a network and keeping part of a database secret from unauthorized users unlike watermarking. Steganography is derived from the Greek words "steganos" and "graphia," which mean "covered," and "writing." It thus indicates the art of concealed communication where the very existence of a message is secret. Thereby these three techniques are not to be confused among each other.

Other than embedding of watermark in image and video formats of multimedia, watermarking has been done on the speech and audio signals as well. The audio signal watermarking is normally done with the pre-requisite that it does not degrade the audibility of the signal. Some of the popular audio watermarking methods are least significant bit (LSB) coding, echo hiding scheme and spread spectrum watermarking.

The word "biometrics" comes from the Greek words bio (life). It may be a characteristic which is a measurable biological and behavioral characteristic that can be used for automated recognition or a process that encompasses automated methods of recognizing an individual based on some measurable biological and behavioral characteristic. Biometric identification is generally preferred over traditional methods (e.g. passwords, smart-cards) because its information is virtually impossible to steal as it is "something you are." A number of biometric characteristics are being used in various applications as Universality, Uniqueness, Measurability, Performance, Acceptability, and Circumvention. When we say watermarking of biometric data, it may be in either way. That is, it might be a biometric image template being watermarked for its authenticity or a host/carrier image being watermarked by the user's or author's biometric for copyright issues. We hereby discuss a few different techniques of either type that have been employed concerning a few established works.

Rao (2009) have discussed a method for copyright protection of digital images by watermarking the images with the fingerprint features of the author/owner. Here the minutiae points were extracted from the fingerprint, and their coordinates are represented as a matrix to utilize them as the watermark. The transform domain used is a hybrid form of the discrete cosine transform and the singular value decomposition. This type of watermarking is done mainly to solve cases of any ownership dispute on the image. This is done by extracting the coordinates of the minutiae points from the watermarked image and compared with those extracted from the fingerprint of the person claiming the ownership. Thereby the biometric feature is utilized along with the watermarking scheme to ascertain that the digital image information is authenticated and secure.

Similarly for the issues on privacy, security and legal significance of text documents, Lam (2009) proposed a similar scheme as above with fingerprint as the secret key. Their scheme ensures the genuineness and integrity of the text document by encrypting the digital biometric fingerprint of the signatories. This encryption of the encrypted biometric in binary into a binary text document is done by a spatial domain method of watermarking called 'Flipping'. In this biometric watermark embedding process, text document to be watermarked, according to the number of biometric watermark bits, had to be adaptively partitioned into blocks with fixed size pixels. The flipping technique is applied for watermark embedding. The fingerprint watermark message was extracted after decryption, based on 'odd' and 'even' pixels in each block of the embedded document. They tested this system for both Chinese as well as Portuguese languages to validate.