Chapter 26
Steganography Using Biometrics

Manashee Kalita
NERIST, India

Swanirbhar Majumder
NERIST, India

ABSTRACT

In this smart age, smart gadgets with internet connectivity have become a necessity. While enjoying these facilities, one must count the security of their private or confidential information. With due time, a lot of cryptographic methods have been developed for enforcing security. On the other hand, with the advancement of technologies, the intruders and hackers have also developed their skills and tools. Therefore, many times we fail to protect our information. To get rid of this situation, the developers have to focus on some other method besides cryptography. Steganography can be considered as the solution to overcome this problem, as it is the technique which conceals the existence of any secret information in a usual media file. Moreover, inclusion of biometric with steganography enhances the security level, as biometric systems are dominating the field of authentication. Here, various techniques of steganography, biometrics, and steganography using biometrics will be discussed. Finally, the present scenario of steganography using biometrics will be demonstrated.

INTRODUCTION

Steganography is one of the techniques which is used to provide security to the information. There are many other techniques available to do so. Those are cryptography, steganography and watermarking. Cryptography scrambles the message using some encryption algorithm with some secret key. When the receiver receives the scrambled message (cipher), he/she decrypt the message using the proper key (same or different). Last two methods, steganography and watermarking are very much similar to both the methods come from the set of data hiding techniques, but with a different objective. Watermarking is a technique where the cover image is digitally marked using some data hiding technique. The method has some way to logically extract the mark without destroying or harming the cover image. On the other hand, for steganography, the matter of concern is the hidden message only, not the cover image. Steganography pay attention to the degree of imperceptibility where watermarking concentrates on the

DOI: 10.4018/978-1-5225-7492-7.ch026

number robustness of the method. Application of watermarking are copy control, authentication, device control, proof of ownership, etc. Steganography mainly aims to provide the security to the information.

The word steganography is derived from Greek. The Greek word **"**stego**"** means cover and "grafia" means writing. The goal of steganography is to conceal the very existence of any secret information in the cover media file. The cover media is any media which usually doesn't come under suspicion. Selection of cover media has being changed with the change of technology. In the ancient time, the cover was different, such as messenger's body part, some natural picture, usual greeting letter, etc.

BACKGROUND

Steganography is a prehistorical practice. From the ancient times, steganography has been using to provide security to the confidential information. Italian mathematician Jerome Cardan reinvented Chinese ancient secret writing method. In that method two parties share a paper mask with holes and after that fill up the blank spaces. The final message appears as an innocuous text. Many secret writing techniques were invented during World War II, such as null cipher, microdot, invisible ink, etc. In the5th century, BC Hiatus wanted to send some message to his friend secretly. He shaved one of the trusted slave's head and tattooed a message on it. The slave was sent after his hair grew back. During World War II, Morse codes were encoded in pictures, like long Blades of grass indicate dashes and dots were indicated by short blade.

The word biometrics is also originated from Greek word "Bio" which means life and "metric" means measure. Biometric define the measurement of statistical analysis of people's physical and behavioral characteristics. This is mainly used for authentication, access control, identification. Nowadays, authentication tool/machine developers start to prefer biometrics characteristics as identification or authentication measure rather than passwords, smart card, etc. Because biometrics is a property which can defines or identify "who are you." Various biometric characteristics are being used by different authentication machine such as palm geometry, fingerprints, iris, face, skin, etc.

Physical characteristics are related to the feature of the body, such as palm veins, retina, face recognition, DNA, fingerprint, hand geometry, etc. On the other hand, the behavioral characteristic is related to the behavior of a person. It includes signature, voice, gait, typing speed, handwriting, etc. Biometric gets the preference to be a reliable authentication measure than a password, smart card, etc. because biometric characteristics are virtually impossible to steal. Therefore, biometric starts dominating the field of authentication. We can observe the large application of biometric in regular life, e.g. Bank employees use Thumbprint to login into their system, in many universities, offices use biometric punching machine where the biometric feature of employees is used to keep the attendance.

Now, if we focus on the steganography using biometrics, it can be done in two ways, one hides your biometric information in some cover file, and another is the reserve one, i.e., biometric information will carry some secret information. Here a brief discussion related to these two mentioned types are presented.

LITERATURE SURVEY

Anil K. Jain et al. (2003) proposes another method to hide biometric information using steganography. They discuss two scenarios. In the first one, the authors embed the fingerprint information (minutiae) into another fingerprint image, so that attackers do not suspect that the visible fingerprint image is not