CHAPTER

1

Introduction

Secure data transmission has been and always will be a significant problem where through past, present and also in the future our main concern will be how to have a secure communication. Another emerging need is to secure personal information that became an important issue due to the rise of the digital era where we deal with secret data almost everywhere in our daily life such as email passwords, bank accounts, credit cards numbers, etc. This led to the development of several techniques to maintain the security of this information. Cryptography was used many years ago as an efficient way to provide secrecy to information but on the other hand cryptography attracts attention to that information since it appears as scrambled and meaningless information.

As an alternative to cryptography a variety of information hiding techniques can be used to hide the existence of the secret information; in this way the secret information will not draw any suspicion.

1.1 Information Hiding Classification

Information hiding techniques is not a new idea; it was used many years ago by Romans and Greeks especially for diplomacy and military purposes. The interest in researching information hiding techniques started at the mid nineties derived by the need to provide a way of copyright protection of digital media [1].

Information hiding has different requirements and specifications of robustness and the volume of hiding capacity. Most applications, however, require near-perfect perceptual transparency [2]. Each application has its own set of different design requirements which includes maintaining statistical transparency to conceal the presence of embedded data, or improving the quality of recovered signature data after being attacked. Each of these applications (classes) must be treated differently. We shall explain these issues in the next chapter. The classification of information hiding is shown in Figure 1.1 [3].

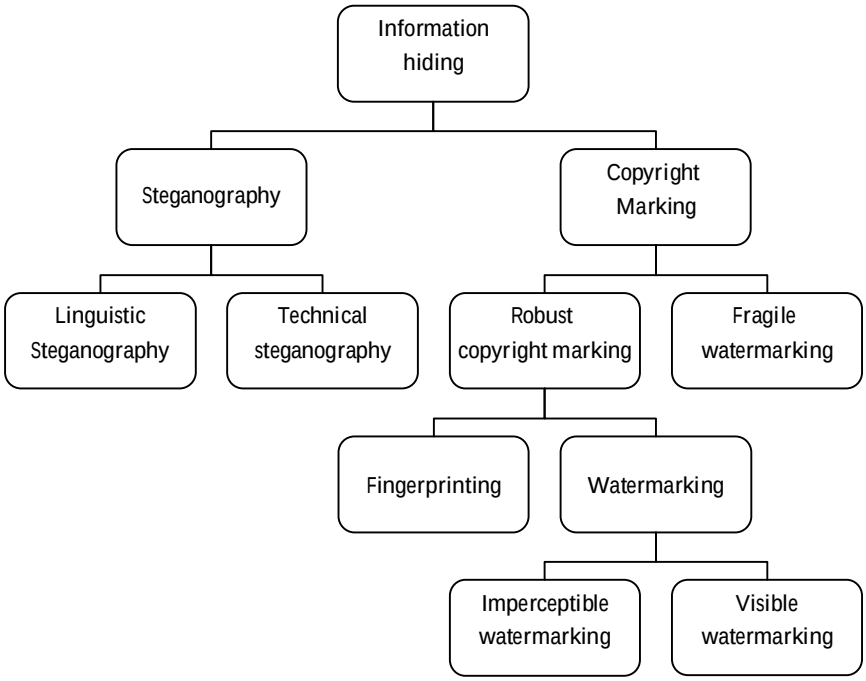

Figure 1.1 Classification of Information Hiding [3]

Information hiding has two major areas, the first is Steganography which is used to secure communication by hiding communicated information or protect personal data. The aim here is to prevent the detection of such an information or message. While the other major area of information hiding is copyright marking; it is used to assert copyright in order to protect the ownership of a certain product. Copyright marking is divided into fragile watermarking that is used for data authentication and robust watermarking used for copyright protection; it can be further divided into fingerprinting and watermarking. Fingerprinting is used to trace the copyright distribution [3].

1.1.1 Steganography

In computer age, steganography is a strategy for hiding information in some form of digital media [5]. The interest in modern digital Steganography started by Simmons in 1983 [6], when he presented the problem of two prisoners wishing to escape and being watched by the warden that blocks any suspicious data communicated between them and passes only normal looking one. Any digital file such as image, video, audio, text or IP packets can be used to hide secret messages. Among all digital file formats available nowadays image files are the most popular cover objects because they are easy to find and have higher degree of distortion tolerance over other types of files with high hiding capacity due to the redundancy of digital information representation of an image data.

Our main concern in this research is steganography in digital images which have three main conflicting requirements; perceptual transparency, robustness, and hiding capacity. For steganography applications it is very important to embed as many bits into the host as possible of the secret message without causing any perceptual

distortion to the host, in other words, the capacity of the embedding system should be as high as possible.

According to figure 1.1 steganography is divided into linguistic stegangraphy which is using linguistic skills to embed a code ideogram into a dispatch that can't be sensed. The other type is technical steganography in which, the secret data is embedded imperceptibly into a multimedia host using image and signal processing techniques [3].

1.1.2 Watermarking

Unlike the idea of steganography which hides the message secretly and the message itself is secret, in watermarking, the embedding process is known and the embedded data does not have to be a secret. Watermarking is the direct embedding of additional information into the original content or host image. Watermarking preserves the content of the cover in its original form allowing the user to listen, view, examine or manipulate the content. Ideally a watermark should be difficult to remove or alter without the degradation of the host signal [3].

1.1.3 Fingerprinting

Fingerprinting is a secret watermark embedded into the multimedia product for point-to-point distribution environments information about authenticated customers before the secret delivery of the data. The goal of fingerprinting is to identify which customer broke his license agreement by supplying the property to third parties using a hidden serial number, which enables the intellectual property owner to take any proper action against that customer [3].

1.2 Thesis Contribution

The work presented in this thesis is mainly focused on embedding information into images, however, several of the proposed approaches and analyses are general, and can be easily applied for other media data, such as audio and video.

The objective of this thesis is to develop a novel steganographic technique based on images as cover objects in order to achieve higher embedding capacity more than the ones recorded by previous techniques while maintaining good robustness and undetectability measures. The system will be adapted to the local characteristics of the image in order to make use of all possible space that can be used in hiding data. An evaluation criterion will be established to compare the proposed technique with other related techniques in order to show the superiority of the proposed system.

1.3 Thesis Organization

The organization of the thesis will be as follows:

Chapter 1: Gives a general overview of data hiding problem, the contributions and the organization of the thesis.

Chapter 2: Introduces essential concepts of steganography and steganalysis, modern and ancient steganographic techniques and how these techniques can be classified and used in different applications. We will also overview the basic measures that must be considered in designing a steganographic system.

Chapter 3: Presents an introduction to the wavelet transform and the integer wavelet transform, and then explain the steps made that led us to the final structure of the proposed system

Chapter 4: Presents a summary of the experiments performed using the proposed system in order to test its robustness and undetectability. These experiments include

different image analysis techniques to the transparency of the proposed algorithm output. It also discusses the hiding capacity obtained by the proposed algorithm and compares it with other systems; also comparing the results of the experiments and how they have affected the robustness and undetectability of the stego image.

Chapter 5: Presents the final conclusion of the proposed algorithm by discussing the results and suggest possible directions for future research.