Chapter 13
Transform Domain Techniques for Image Steganography

Siddharth Singh
University of Allahabad, India

Tanveer J. Siddiqui
University of Allahabad, India

ABSTRACT
Recent advancement of multimedia technology has posed serious challenges to copyright protection, ownership, and integrity of digital data. This has made information security techniques a vital issue. Cryptography, Steganography, and Watermarking are three major techniques for securing information and ensuring copyright ownership. This chapter presents an overview of transform domain techniques for image steganography. The authors discuss the characteristics and applications of image steganography and briefly review Discrete Cosine and Wavelet transform-based image steganography techniques. They also discuss the various metrics that have been used to assess the performance of steganography techniques and shed light on the future of steganography.

INTRODUCTION
Steganography techniques were invented as a quest of human desire for communicating secret information. The term steganography refers to covered communication. Secret communication plays an important role in diplomacy and wars. Hence devising ways for secret communication has ever been fascinating. Codes and ciphers, invisible inks, wax coated wooden tablets, physical objects have been used thousands of years ago to communicate secret information. The oldest example of steganography is traced back to around 400 BC in the Greek history. The word steganography has been derived from the Greek words steganos (covered or secret) and graphein (writing) which literally means “covered writing”. In the “Histories of Herodotus” (1996), Herodotus reports an interesting story of Greek ruler Histiaeus. In order to inform his friends that it was time to begin a revolt against Mededs and Persians he tattooed a message on the shaved head of a slave. He waited till his hair grew back, and then sent him. The message reached to the intended recipients and the revolt was successful. Of course it took longer time, unlike emails, to grow hair back and to travel to the destination. Since then revolutionary changes have been occurred in the world of communication. We are now living in the digital era leading to enormous amount of digital content of various modalities. This has added new dimensions and brought new challenges to information security.

DOI: 10.4018/978-1-4666-6158-5.ch013
In particular, this poses serious challenges to copyright protection, ownership and integrity of digital data. This has made information security an emerging area of research. New applications have been emerged, new techniques have been invented and old techniques have undergone a sea change.

Cryptography, Steganography and Watermarking are the three main techniques used for securing information and ensuring copyright ownership. These techniques are closely related, have a great deal of overlap and share many technical approaches (Fridrich, 2010). However, there are fundamental differences. Cryptography secures data by scrambling it that it can not be understood by unintended recipient even if it is detected. The message is encrypted but its existence is not hidden.

Steganography is an art of hidden communication in which a secret message is communicated by hiding it in a cover file so that the very existence of the secret message is not detectable.

Watermarking is closely related to steganography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication. Unlike steganography, watermarks do not always need to be hidden. Both visible and invisible watermarks are in use. In steganography the hidden data is important whereas in watermarking there is no problem even if an invisible watermark is detected. However, watermarking system requires resistance against removal. The fundamental difference between steganography and watermarking is that “the information hidden by a watermarking system is always associated to the digital object to be protected or to its owner while steganographic systems just hide any information (Katzenbeisser et al., 2000)”. However, the use of invisible watermarking is blurring the distinction between steganography and watermarking at least at the level of technique. In invisible watermarking, watermark may be in the form of steganography where a party communicates secret message to another party. Like steganography, invisible watermarking requires that it should be nearly impossible for someone to guess that an image has been watermarked. Despite of obvious differences between watermarking and steganography techniques there are a lot of commonality and many of the watermarking techniques can be applied in steganography and vice versa. It is not possible to cover all these techniques in a single chapter. In this chapter, we limit our discussion to steganographic techniques. However, due to inherent commonalities between steganography and watermarking we will refer watermarking techniques as well.

As noted earlier steganography was in existence from ancient time. With newer development the slaves head and carved messages have been replaced by the digital content (cover media and embedded message). The cover media can be image, audio or video; the most commonly being the image files because of many reasons: (1) Digital images are being used quite frequently on the internet. (2) The size of image is large. (3) Digital images usually contain redundant bits. So, we can hide large amount of data in a digital image without being suspected by human visual system. The commonly used image file formats which are used for steganography are graphic interchange format (GIF), Joint Photographic Expert Group (JPEG) and bitmap format (BMP). We restrict the scope of this chapter to transform domain image steganography techniques only.

The message can be embedded directly in the cover image or in the transform domain. In this chapter, we will review transform domain techniques of digital image steganography. An extensive survey of digital image steganography can be found in (Cheddad et al., 2010).

The rest of the chapter is organized as follows:

In the next section, we introduce the basic concepts and major issues involved in steganography and discuss some of its applications. We then discuss various steganography techniques and classify them. We will focus on discrete cosine transform and wavelet transform based techniques. In the next section, we shed light on future of steganography. Finally, the chapter closes with conclusion.