Chapter 10
A Review on Spatial and Transform Domain-Based Image Steganography

Divya Singla
Panipat Institute of engineering and technology, India

Neetu Verma
Deenbandhu Chhotu Ram University of Science and Technology, India

Sakshi Patni
Panipat Institute of Engineering & Technology, Panipat, India

ABSTRACT

Steganography is a secret way of communicating, hiding the existence of information. It hides the message secretly without letting anyone know about its existence. This chapter gives a brief of various image steganography techniques in the spatial domain and transforms domain with their advantages and disadvantages. The characteristics to measure the performance of an image steganography technique are given as well. It also introduces the idea of drawing out the embedded data from the cover object called steganalysis.

INTRODUCTION

Digital image steganography contains two words: digital image and steganography. The term digital image is described as an image containing a finite number of elements, generally called pixels, each of which has a digital value of one or more bits at a particular location. The term steganography refers to the art of concealing

DOI: 10.4018/978-1-6684-6864-7.ch010

a message in any medium. It originates from two different Greek words, which are *steganos,* meaning covered, and *graphia,* which means calligraphy. Digital Image steganography refers to concealing the message in a digital image to hide its presence from the unwanted user. Steganography aims to prevent the very existence of the news away from inquisitive eyes. We can use any digital media as cover media like images, text files, audio, video, etc., which is required to hide and carry information from one place to another. It allows two or more people to silently communicate with each other leading to the protection of secure data.

Usually, images are preferred as cover media because the human eye cannot be able to differentiate between the pixel value of two adjacent pixels (244, 245). Both pixel intensities appear to be the same. The Gray image consists of the pixel having an intensity value ranging from 0 to 255. This variation in pixel intensity can be exploited to insert secure data without providing any clue to the person's eye. The human eye can't able to differentiate between the original image and the message-encrypted steganographic image. In this chapter, we will cover the History of steganography, how steganography differs from the term cryptography, the role of steganography, and various techniques used to hide data in an image.

Steganography is a prehistoric practice used in several forms for past thousands of years to keep Information hidden and Secure. For example:

1. The steganographic technique was first used around 440 B.C in Greece. Histaeus, the ruler of Greek, used steganography to send secret messages through an enslaved person. They shave the head of the deprived and tattoo the message on scalp and then wait for the hair to come, so that message will get hidden. The receiver of the message reverses the process by shaving the enslaved person's head to get the hidden message and then replies in the same or different form of steganography.
2. During the Revolutionary War of America, both the British and American forces used invisible ink to pass secret communication. They form invisible ink with familiar sources, like vinegar, fruit juices, milk, and urine, for the hidden text. Heat or light is required to decipher these hidden messages.
3. In secret message communication, null ciphers were also used. They were unencrypted messages containing real messages embedded in the current text. Hidden messages were hard to interpret explicitly. For example, basically freshwater bonus and salt awash reward anyone feeding agreed. Resourceful anglers usually find masterful leapers' buns and admit above-rank tweaking any day.

By taking the third letter in each word, the following message emerges: