Chapter 2
Cognitive-Based Cover Image Selection in Image Steganography

Sangeetha K. N.
JSS Academy of Technical Education Bangalore, India

Usha B. Ajay
BMS Institute of Technology and Management, India

ABSTRACT

The chances of data getting lost while it is being transferred between the sender and receiver is very high these days. Since these data are very sensitive whose security cannot be compromised, there is a need for highly secure systems to transfer the data without compromising the content and the quality. Steganography techniques help us to achieve these objectives. In the present time, various organizations and industries are using cover image arbitrarily. In such cases, it does not provide personalized approach to the whole process of data hiding. Thus, as a result of this limitation, there is motivation to build such an application in which the system selects which image is most suitable for hiding data accordingly. The main algorithm being used here is the regression algorithm which consists of other algorithms like linear regression, decision tree regression. This application also extracts the hidden data from the generated stego image.

INTRODUCTION

Information hiding in digital images in the form of text, audio or video can be done using Image Steganography technique. In comparison with cryptography, steganography is not used to hide information from others but it is used to make others believe that the information does not even exist. Using steganography, the user can conceal/hide information in ways which will prevent the hidden message to be detected. In steganography, the information or encrypted information is hidden inside a digital host before being transferred through a network, thus existence of the hidden information is scarce. Image Steganography can be used for a wider number of applications such as copyright protection for digital media such as audio, video and images.

DOI: 10.4018/978-1-5225-9902-9.ch002

Steganography essentially cheats human perception, human senses have not been trained to keep an eye for files that may have hidden information inside them, there are a variety of available programs that can do Steganalysis (Detecting the use of Steganography.) Steganography is regularly used to hide one file into another file. When this hiding of files is performed, the hidden data is usually protected by a password.

A cognitive system performs the work of knowing, understanding, planning, deciding, problem solving, analyzing, synthesizing, assessing, and judging as it is fully integrated with perceiving and acting. In cognitive inspired image steganography, the algorithms employed are used to find the similarity ratio between the image before and after steganography is used. This is measured based on the SSIM ratios for each of the various images.

The main objective of using image steganography is to choose a suitable image for hiding the information so that any person trying to find encrypted information is unable to do so. The image that has been selected to hide the data should have a small SNR after steganography is performed on the image. Thus, the user gets an image which hides the encrypted data.

LITERATURE SURVEY

Khandare et al. (1996) discuss about data hiding technique called Steganography. Their paper presents a survey on various data hiding techniques in steganography along with the comparative analysis of these techniques. Their paper presents both traditional and novel techniques for addressing the data-hiding process and evaluates these techniques in light of three applications: copyright protection, tamper proofing, and augmentation data embedding. The authors have discussed about steganography and presented some notable differences between steganography and cryptography. They also surveyed various data hiding techniques in steganography and provided a comparative analysis of these techniques.

Goel et al. (2013) attempted to work on most of the prominent algorithms. Their work was mostly related to finding out the parameters that steganography can be based on and their comparison. Their paper deals with hiding information using LSB, DCT and DWT techniques. These algorithms are measured based on their MSE and PSNR values. Along with these, two other parameters are used to measure the effectiveness of these algorithms. They are Robustness and Capacity payload. The authors have successfully implemented the algorithms proposed in this paper and the results have been documented. From their results, they came to the conclusion that DCT having higher PSNR provides best quality of images.

Chen Ming et al. (2006) made a comparative study on different steganalysis techniques. They have implemented Markov Chains to try and test various techniques and made their conclusions.

Zöllner et al. (1998) studied SVM and its variation RBF to achieve the best possible results. According to his findings, the best result obtained was the usage of RBF as it was automatic and very versatile.

Joachims et al. (2000) has studied the effect steganography has on certain image features after the data has been embedded. They found out that certain statistical measures are different for cover images and stego images.

Fridrich et al. (2001) proposed a steganalysis method using the Histogram Characteristic Function (HCF) as a feature to distinguish the cover and stego images. This method is efficient in detecting the LSB replacement for RGB color bitmaps, but ineffective in detecting the LSB matching for grayscale images.