Chapter 4
High Efficient Data Embedding in Image Steganography Using Parallel Programming

Usha B. A.
R V College of Engineering, India

ABSTRACT

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points.. As embedding data in an image, is independent of one another. Parallelism can be used to achieve considerable time gain. nography, although it has made communication safe, it has its own drawbacks. One among it is time required to embed data in pixels of the image. This problem is bugging computer scientists from long time. This paper discusses a method which makes OpenMP parallel library to parallelize embedding of data, which basically reduces the time by almost fifty percent and to achieve PSNR ranging from 30 to 50 after embedding data in the pixels of the image.

INTRODUCTION

In today's generation, hackers are intelligent enough to crack the normal encrypting algorithms. So there exists a need for a better way to communicate the critical data between the two ends, without being exposed to the hackers. Steganography is one such technique, which really helps to achieve this, by embedding the data in pixels of an image. Although it is not an entirely different way of communication, it helps us to embed the critical data and helps us to achieve better security.

Digital information hiding was inherent with the advent of digital technology. These days, steganography systems use distinctive sorts of computerized media like text, image, audio, video, binary, or html files. Modern steganography techniques rely on data hiding techniques using current media. Steganography varies from cryptography; cryptography focuses on keeping the substance of a message riddle and safe

DOI: 10.4018/978-1-5225-4044-1.ch004

while steganography deals with keeping the vicinity of a message mystery. Cryptography provides data security by applying encryption/decryption techniques.

An encrypted message is susceptible to eavesdroppers' attacks, if they know of its presence. The superlative resolution is to hide the message reality by implanting it into cover media. Therefore, the role of steganography is clear and strong with use of cryptography. Both techniques provide more secure communication between sending and receiving ends.

Embedding data is independent of all other things; this gave us motivation to exploit parallelism concepts and achieve significant time difference. With parallel embedding of data, high volume data embedding is promising.

Over the last decade, novel techniques have been applied and developed for Image Steganography. Image steganography is a very upcoming hiding technique since the robustness offered by the algorithms to the steganalytic attack is appealing high and, therefore, ensures secure data transmission both when data hidden is critical and sensitive. Text, images, audio data have been tried as secret messages to be hidden in the Image. Some of the latest developments in the field of Image Steganography have used artificial intelligence techniques, sudoku puzzle, hybrid fusion techniques, cognitive science and many more.

There are two main objectives for this application. They are as below:

- Ensuring secured communication between any two ends, using steganographic techniques.
- Exploiting parallelism concepts in data embedding and extraction, this gives us significant time gain in processing.

The common requirements to rate the performances of steganographic techniques are as follows.

- **Invisibility:** The invisibility of a steganographic algorithm is the first and foremost requirement, while the strength of steganography lies in its capability to be unobserved by the human eye. The moment that one can see that a picture has been messed with, the algorithm is compromised.
- **Payload Capacity:** As opposed to watermarking, which in turn would need to introduce merely a bit of copyright data, steganography is aimed at undetectable connection and for that reason demands adequate embedding ability.
- **Robustness Against Statistical Attacks:** Measurable steganalysis is the act of identifying hidden data through applying factual tests on image information. Numerous steganographic calculations leave a "mark" while installing data that can be effectively distinguished through measurable investigation. To have the capacity to go by a supervisor without being recognized, a steganographic algorithm must not leave such an imprint in the picture that is measurably large.
- **Robustness Against Image Manipulation**b In the correspondence of a stego picture by trusted frameworks, the picture may experience changes by a dynamic supervisor trying to uproot concealed data. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. According to the manner in which the information will be inlayed, these types of manipulations may eliminate the concealed information. It is ideal for steganographic algorithms to be vigorous against either malicious or accidental changes to the image.
- **Independence of File Format:** With a wide range of picture record arrangements utilized on the Internet, it may appear to be suspicious that one and only kind of document configuration is consistently conveyed between two gatherings. The most intense steganographic calculations in this way have the capacity to implant data in a document. This additionally takes care of the issue