Steganography in Image Segments using Genetic Algorithm

Masoud Nosrati *
Young Researchers and Elite Club,
Kermanshah Branch,
Islamic Azad University,
Kermanshah, Iran.
minibigs_m@yahoo.co.uk

Ali Hanani
Department of Computer Engineering,
Songhor and Koliaei Branch,
Islamic Azad University,
Songhor and Koliaei, Iran.
ali_hanani@yahoo.com

Ronak Karimi
Young Researchers and Elite Club,
Kermanshah Branch,
Islamic Azad University,
Kermanshah, Iran.
rk_respina_67@yahoo.com

***Abstract*— This study offers a heuristic genetic algorithm based method for message hiding in a carrier image. This approach focuses on the "before embedding hiding techniques" by trying to find appropriate places in carrier image to embed the message with the least changes of bits. Due to it, segmentation is done in order to convert the LSBs and message strings to the sets of blocks for participation in genetic algorithm. After finding the right places, secret message blocks are embedded and a key file is created to make the message extraction available by providing the data addresses. Experimental results with the least changes in image histogram (by the policy of setting an appropriate amount for the length of block bits) show the efficiency of current method.**

Keywords- Steganography; Genetic Algorithm (GA); data hiding; secure communication

I. INTRODUCTION

Secure communication is one of the most challenging topics in now-a-days digital world. It is hard to find a secure channel for communication all the times. So, some sciences and techniques came to existence in order to alternate the security, such as cryptography (converting ordinary information into unintelligible gibberish [1]), watermarking (a pattern of bits inserted into a digital media file that commonly identifies the file's copyright information [2]), Reversible Data Hiding (RDH) (it has ability of extraction of both hidden data and carries media [3]) and steganography.

Steganography is the art and science to hide data in a cover media such as text, audio, image, video, etc. [4] In other words, steganography is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message [5].

Steganography will hide the message so there is no knowledge of the existence of the message in the place [6]. The term Steganography is forked from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing" [7]. The notion of data hiding or steganography was first introduced with the example of prisoners' secret message by Simmons in 1983 [8].

There are several media for covering the secret message. This paper will introduce a new method for hiding data in 24-bit RGB image files. Also, genetic algorithm is utilized for securing stego-data against stego-analysis methods ("stego-analysis" also called "steganalysis" means detection of covered data in media [9][10][11]). The most important existing method for steganalysis is RS analysis [12], which investigates the statistical features of image to detect the message. Statistical analysis looks for the different blocks of pixels in image that aren't match with the context. In this way, it can understand about the existence of covered data.

It is clear that spirit of steganography is embedding message in a cover media. It can be done in different phases like runtime, or through preprocessing [13]. Regarding the process of embedding, applying steganography techniques for increasing the robustness is largely done in two phases:

1. Techniques before embedding
2. Techniques after embedding

First phase generally includes some activities like increase the statistical irregularity of image. For example, by adding impulse noise to carrier image before embedding, RS analysis results will fail to show the truth.

In related previous studies, it is seen that GA is largely employed to increase the robustness of secret messages against steganalysis [14] in second phase. It means, after embedding the data in special places of image, some techniques are hired to change the statistical features of pixels' blocks, so that RS get unable to detect the existence of message.

The method that is presented in this study focuses on the before embedding techniques. It aims finding suitable places in carrier image that causes fewer changes in original image. In this way, changes in color histogram are less and detecting the existence of stego-text will become harder. Finding the suitable places is a process which is implemented by genetic algorithm. System in whole, takes an RGB 24-bit color image and a secret message as input, and gives the modified image that contains the secret message in its least significant bits and a key string for extraction of message from modified image as output.

1.1 Related works

Generally, there are two types of data hiding techniques using images: spatial and frequency domain [15]. The first group is based on embedding message in the least significant bit (LSB) of image pixel. The basic LSB method has a simple implementation and high capacity [16]. However it has low robustness versus some attacks such as low-pass filtering and compression [16].

2327-0659/15 $31.00 © 2015 IEEE
DOI 10.1109/ACCT.2015.57