Steganography Using Segmenting Mosaic Images with Embedding Data by 3 LSB S-Type Scanning

Abhinav Tripathi
Department of Computer Science and Engineering
Oriental Institute of Science and Technology, Bhopal, MP, India

Jijo S Nair
Department of Computer Science and Engineering
Oriental Institute of Science and Technology, Bhopal, MP, India

Abstract- In any communication, security of the information is the most important issue in today's world. In this research paper "Steganography using segmenting mosaic images with embedding data by 3 LSB S-type scanning" the data is embedded into a particular sort of image i.e. Mosaic image by using 3 LSB (Least Significant Bit) in a special pattern i.e. S-type. The embedded data is unearthed from, the steno image by using the reverse method i.e how data was embedded. The proposed approach is based on the 3 LSB insertion technique applied on maximum color used in histogram of the mosaic image. The key idea is to split the image into four segments and apply s-type scanning along with the data embedding for each segment.

Keywords – ***Steganography, LSB, Histogram, Mosaic images.***

I. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Data hiding is referred to as a process to hide data into cover media. The stegnography links two sets of data, a set of the embedded data and stego image. In stegnography it is taken care that hidden data should not be easily traceable to human eyes. In the majority cases of data hiding, the stego image will experience some alteration due to data. That is, some permanent distortion has occurred to the cover media even after the hidden data have been extracted out. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Images, audio and video files are the most popular cover objects used for steganography. For instance to a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its color. These pixels are displayed horizontally row by row. The main terminologies used in the steganography systems are: the cover message, secret message, secret key and embedding algorithm. Image, video, audio, text, protocol are used by the encrypting algorithm to send the secret message. The secret message is the data which is wanted to be hidden in the suitable furtive digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually use to encrypt the secret data in the stego image. This paper presents a 3 LSB approach for the data embedding in mosaic images. The rest of the paper is arranged as follows the second section presents a brief review of the some recent work in this field. The third section presents an overview of the steganography and the proposed approach is presented in fourth section. Finally the conclusion is presented in fifth section and references in the last section.

II. LITERATURE REVIEW

Due to the crucial demand of data hiding in images many approaches have been already published some of them are presented in this section.

In the research paper "Reversible Data Hiding" by Zhicheng Ni et al [1]. Proposed reversible data hiding algorithm has been applied to many different types of images, including some commonly used images, medical images, texture images, aerial images, and all of the 1096 images in the Corel DRAW database, has always achieved satisfactory results, thus demonstrating its general applicability.
In the research paper "An overview of Image Steganography" by T. Morkel et al [2]. Some of the main image steganographic techniques are discussed in which all the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness.
In the research paper "A New Method in Image Steganography with Improved Image Quality" by Atallah M. Al-Shatnawi [3]. In this method, it hides the secret message based on searching about the identical bits between the secret messages and image pixels values. The proposed method was compared with the LSB benchmarking method for hiding the secret message which hide the secret message directly in the least two significant bits of the image pixels. The result obtained by the proposed method and the LSB hiding method in terms of ratio of accuracy in improving the image quality were 83% and 43% respectively.
In the research paper "An introduction to steganography methods" by Masoud Nosrati et al [4] explained the working of steganography and its types.
In the research paper "Practical Data Hiding in TCP/IP" by Kamran Ahsan et al [5]. Two practical data hiding approaches in the TCP/IP protocol suite is analyzed in this paper. It is demonstrated how IPv4 header manipulation can be used to pass supplementary information over the Internet. It presents two practical data hiding techniques for TCP/IP based on fragmentation strategies and the identification field.
In the research paper "A Novel Approach for Hiding Messages in Images" by Hassan Mathkour et al [6]. A spiral-based LSB approach for hiding messages in images was presented in this paper. The proposed approach was based on the LSB substitution technique applied on RGB color components of BMP images.

III. STEGANOGRAPHY

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient even knows that a message has been sent. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" [2] defining it as "covered writing". Figure 1 shows the Steganography system scenario. However, in the hiding information the meaning of steganography is hiding text or secret messages into another media file. In image steganography the information is hidden solely in image. An effective and appropriate steganography algorithm must be selected which can encode the message in more secure form. The sender may send the stego file by using modern engineering techniques. Steganography works in two stages, Encryption and Decryption. During the encryption stage, a key is used to encrypt a message in a cover medium resulting in a stego-object. The stego-object is then transmitted along with the modern engineering communication systems. When the stego-object is acknowledged by the receiver, the encrypted message is extracted from stego-object using the known stego-key and the decryption algorithm. Image, video, audio, text and protocol formats can be used for steganography. The least significant bits (LSB) of an image are those bits that can be altered without the alteration being detected easily.

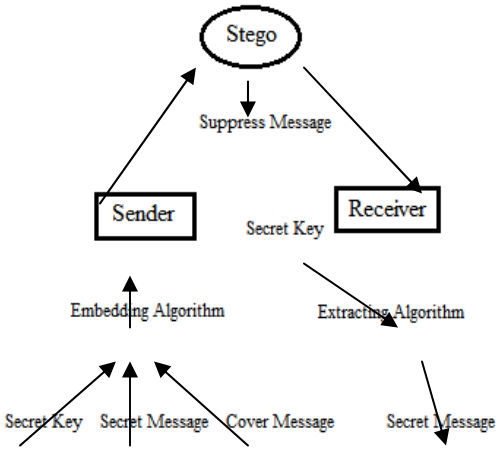

Figure 1: Steganography System Scenario

A. LSB INSERTION

Digital images usually use 24-bit or 8-bit to store its pixels, for colored images each pixel has red, green and blue color components [6]. The basic idea of LSB insertion is to embed (hide) information in the LSB of the image pixels. A digital image consists of a matrix of color and intensity values. In a typical gray scale image, 8 bits/pixel are used. In a typical full-color image, there are 24 bits/pixel, 8 bits assigned to each color components. The simplest steganographic techniques embed the bits of the message directly into the least significant bit plane of the cover image in a deterministic sequence. Modulating the least-significant bit does not result in a human-perceptible difference because the amplitude of the change is small. Other techniques "process" the message with a pseudorandom noise sequence before or during insertion into the cover image. The advantage of LSB embedding is its simplicity and many techniques use these methods.
LSB embedding also allows high perceptual transparency. However, there are many weaknesses when robustness, tamper resistance, and other security issues are considered. LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image. A part of 3 LSB insertion, Watermarking and Fingerprinting and Transform Domain-Based Steganography are the main categories of steganography.

IV. PROPOSED ALGORITHM

The proposed algorithms for encryption and decryption can be explained in the following steps:

Steps for Encryption:

Step 1: Take the mosaic image (as a cover media).

Step 2: Histogram generation:-
2.1 Generate the Histogram of the image.
2.2 In generated histogram, find the maximum color used.
Step 3: Splitting & Numbering:-
3.1 Split the image into 4 parts i.e. (x_1,y_1) value is to be entered by the user where (x_1,y_1) lies between

$$0< x_1 < x$$
$$0< y_1 < y$$

where value of (x, y) = maximum value of x and y co-ordinate. *Key 1= (x_1,y_1)*
3.2 Number these 4 parts sequentially, i.e. part 1, part 2, part 3 and part 4.

Step 4: Scanning & Data Embedding:-

4.1 Start S-type scanning from part 1.

4.2 As soon as it gets the maximum color point (it can be in any of defined part), immediately start data embedding, using 3 LSB insertion method (applied on 2 columns of each part).

4.3 Continue both scanning and embedding process to the next parts.
4.4 During the scanning process, if two adjacent pixels of different colors are found, do not embed the data into those pixels. Only embed data on those pixels whose adjacent pixel colors are same.
4.5 Similarly then embed the data in descending order of the color, according to the generated histogram (repeat steps 4.1 to 4.4).
4.6 If at any particular point, any two colors in the image has the same histogram value, then choose the nearest color from the origin (0,0) and then next color.
4.7 As soon as embedding process in a part is completed, immediately start in the next one respectively.

Step 5: Note the point (x_n,y_n) along with the Part number of image (P_n), where embedding process is completed.

Key 2= (x_n,y_n) && (P_n)

Step 6: Join all these 4 parts together of the image and now Stego image is prepared.

Steps for Decryption:

Step 1: Take the Stego image.

Step 2: Histogram generation:-
2.1 Generate the Histogram of the image.
2.2 In generated histogram, find the maximum color used.

Step 3: Splitting & Numbering:-
3.1 Split the image into 4 parts i.e. (x_1,y_1) value is to be entered by the user where (x_1,y_1) lies between

$$0< x_1 < x$$
$$0< y_1 < y$$

where value of (x, y) = maximum value of x and y co-ordinate. *Key 1= (x_1,y_1)*
3.2 Number these 4 parts sequentially, i.e. part 1, part 2, part 3 and part 4.

Step 4: Scanning & Data Extraction:-
4.1 Start S-type scanning from part 1.
4.2 As soon as it gets the maximum color point (it can be in any of defined part), immediately start data extraction, using 3 LSB method (applied on 2 columns of each part).
4.3 Continue both scanning and extraction process to the next parts.
4.4 During the scanning process, if two adjacent pixels of different colors are found, do not extract the data into those pixels. Only extract data on those pixels whose adjacent pixel colors are same.
4.5 Similarly then extract the data in descending order of the color, according to the generated histogram (repeat steps 4.1 to 4.4).
4.6 If at any particular point, any two colors in the image has the same histogram value, then choose the nearest color from the origin (0,0) and then next color.
4.7 As soon as extraction process in a part is completed, immediately start in the next one respectively.
4.8 Do the extraction process till the point (x_n,y_n) & part (P_n) and stop.

Step 5: Collect the extracted data sequentially.

Generated Keys during Proposed Algorithm:

Key 1: The point (x_1,y_1) which is defined by the user.
Key2: Point (x_n,y_n) && Part (P_n), where embedding process is completed.
So, Data Encryption KEY = Key1 + Key2

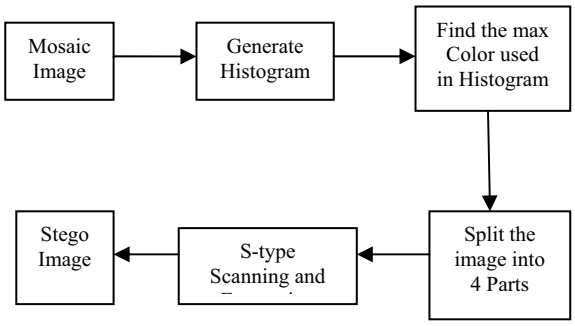

Figure 2. Block diagram of Proposed Algorithm

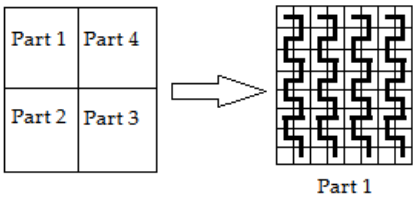

Figure 3. Elaborated concept of figure 2

The concept of proposed algorithm is represented above in figure 2. Sequentially figure 3 shows the elaborated concept of figure 2 i.e. the segmentation of the image in four parts along with S-type scanning and data embedding in a part of the image.

V. CONCLUSION

In this paper, Steganography algorithm using segmenting mosaic images with embedding data by 3 LSB insertion methods along with S-type scanning is presented. The proposed approach is based on the 3 LSB insertion technique applied on maximum color used in histogram of the mosaic images. The key idea is to split the image into four segments and apply S-type scanning along with the data embedding for each segment. The reason behind using the mosaic images, as cover media is that mosaic images has various colors, where occurrence of colors presents in a very random and unconventional form, so that normal human eyes cannot detect the changes occurred, due to secret data hiding in them. In proposed algorithm, two keys are generated during encryption, Key 1 and Key 2, which helps the user to decrypt the data from the image without any distortion and it reduce the time complexity of the algorithm.

REFERENCES

[1] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su "Reversible Data Hiding", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 16, NO. 3, MARCH 2006.

[2] T. Morkel, J.H.P. Eloff, M.S. Olivier "AN OVERVIEW OF IMAGE STEGANOGRAPHY", in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005

[3] Atallah M. Al-Shatnawi "A New Method in Image Steganography with Improved Image Quality" Applied Mathematical Sciences, Vol. 6, March 2012, no. 79, 3907 - 3915.

[4] Masoud Nosrati, Ronak Karimi, Mehdi Hariri "An introduction to steganography methods", World Applied Programming, Vol (1), No (3), August 2011. 191-195 ISSN: 2222-2510 ©2011 WAP journal. www.waprogramming.com

[5] Kamran Ahsan, Deepa Kundur, "Practical Data Hiding in TCP/IP" Proceedings of the Workshop on Multimedia Securityat ACM Multimedia, 2002.

[6] Hassan Mathkour, Ghazy M.R. Assassa, Abdulaziz Al Muharib, Ibrahim Kiady, "A Novel Approach for Hiding Messages in Images", 2009 2 IEEE International Conference on Signal Acquisition and Processing.

[7] Hsiang-Cheh Huang, Yueh-Hong Chen, I-Hung Wang, "Reversible Data Hiding with Improved Histogram Alteration Method", 2010 IEEE Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

[8] Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang "Reversible Data Hiding Based on Histogram Modification of Pixel Differences", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 19, NO. 6, JUNE 2009.

[9] Hyoung Joong Kim*, Member, IEEE*, Vasiliy Sachnev, Yun Qing Shi*, Fellow, IEEE*, Jeho Nam*, Senior Member, IEEE*, "A Novel Difference Expansion Transform for Reversible Data Embedding", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 3, NO. 3, SEPTEMBER 2008.

[10] Yongjian Hu, Heung-Kyu Lee, and Jianwei Li "DE-Based Reversible Data Hiding With Improved Overflow Location Map", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 19, NO. 2, FEBRUARY 2009.

[11] Chin-Chen Chang*, Fellow, IEEE*, and Chih-Yang Lin, "Reversible Steganography for VQ-Compressed Images Using Side Matching and Relocation", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 1, NO. 4, DECEMBER 2006.

[12] Jun Tian, "Reversible Data Embedding Using a Difference Expansion", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 13, NO. 8, AUGUST 2003.