EUROPEAN ACADEMIC RESEARCH
Vol. II, Issue 6/ September 2014

Impact Factor: 3.1 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Image Steganography

ZEINA H. AL- HADAD
INAS FADHIL ABDULLAH
Department of Computer Science
Kufa University
Iraq

Abstract:

Steganography can be defined as a science and art of invisible communication for secret purpose, as well as steganography is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer. The paper describes the novel method for hiding information within an image depending on information discovered indirectly from the image. there are two important factors in any algorithm which must be decided before hiding step, that are the number of bits will be used in hiding step and the positions of pixels that will be altered to contains the hiding information. Hiding information is not free process and the capacity of hiding information is mostly limited and restricted by the size of cover images in addition, there is a tradeoff between both steganography capacity and stego image quality.

Key words: image steganography, hiding step, Sobel image, edges.

1. Introduction

Steganography is the art of invisible communication. Its purpose is to hide the presence of communication by embedding messages into cover objects. Each steganography system consists of an hiding algorithm and an extracting algorithm.

There are five elements in each steganography algorithm which are:

1- Cover file**:-** (may be text, audio, image or video file) this file used to hide information in it and the file size must be selected carefully to be enough to contain the secret information, this file also called carrier.
2- Message file:- also called secret file (may be text, audio, image or video file) this file contains information that must be hiding.
3- Hiding algorithm:- is the deterministic sequence to hide the message in the cover.
4- Stego file:- is the file produced after embedding the message in the cover file.
5- Extracting algorithm**:-** to extract the message from stego file.

To accommodate a secret message in a digital cover, the original cover is slightly modified by the embedding algorithm. The result is modified cover object that contains the secret message and it is called stego object**.**

Steganography can be split into two types of algorithms generally

a) Fragile:- involves embedding information which is destroyed if the file is modified.

b) Robust:- aims to embed information into a file which cannot easily be destroyed.

Steganography involves hiding data in a message in such a way that it is difficult for an adversary to detect and difficult for an adversary to remove. Based on this goal, three main principles can be used to measure the effectiveness of a given steganography technique:

1- Amount of data: the better technique that capable to hide more information within a suitable cover file size.
2- Difficulty of detection: relates to how it is easy for somebody to discover and detect the message that has

been hidden. There is usually a direct relationship between how much data can be hidden and how it is easy for someone to detect it.

3- Difficulty of removal: if someone intercepting the stego file, he would not be able to remove the hidden information easily.

There are four types of steganography according to cover file type which are

1- Text steganography.
2- Image steganography.
3- Audio steganography.
4- Video steganography.

To hide a message inside an image without changing its visible properties, the cover file is altered in (noisy) areas, these alterations involve the usage of the (LSB), masking, and transformations on the cover image. A simple approach for embedding information in cover image is uses the Least Significant Bits (LSB).

There are four algorithms currently implemented, each use least significant bit steganography and some filter the image first

1- The blind hide algorithm is the simplest way to hide information in an image, it blindly hide information by starts from the top left corner of the image and works its way across the image (then down in scan lines) pixel by pixel. It isn't very secure; it also isn't very smart.
2- This algorithm randomly distributes the message across the image. It uses a password to generate a random seed, then uses this seed to pick the first position to hide in. It continues to randomly generate positions until it has finished hiding the message.
3- This algorithm filters the image using one of the inbuilt filters and then hides in the highest filter values first. It is essentially a fancier version of Blind Hide as it doesn't

require a password to retrieve the message. Because we are changing the pixels we need to be careful about filtering the picture because we don't want to use information for filtering that might change. If we do, then it may be difficult (if not impossible) to retrieve the message again.

4- The battle steg algorithm is the best of all which performs (Battleship Steganography). It first filters the image then uses the highest filter values as a (ships) the (h %) of highest filter values is designated as (ships). The algorithm then randomly (shoots) at the image (like in Hide Seek), (Shots) are randomly picked the pixel positions on the cover image, until a ship is found (known as a "hit"), and when it finds a (ship) it clusters its shots around that hit.

2. The proposed system

In general, the proposed system consists of two stages; each stage consists of many steps as illustrated in figure (1) and (2).

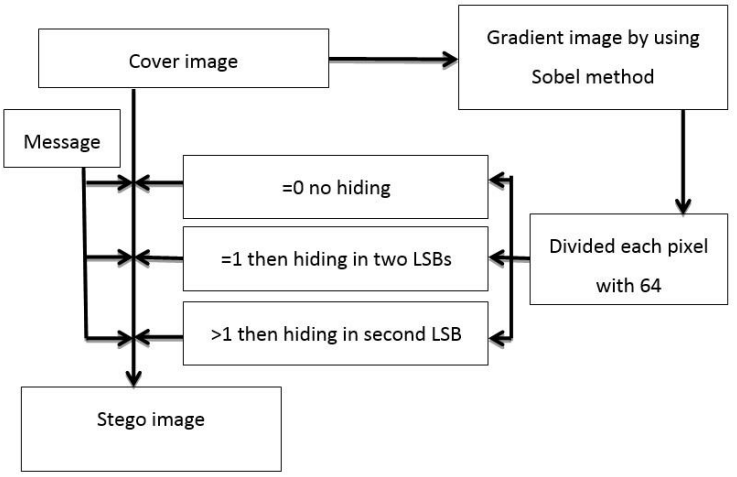


Figure (1) Hiding stage of the proposed system

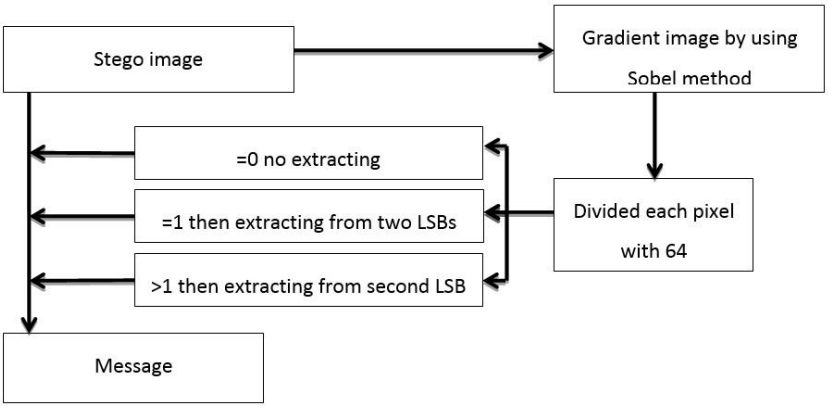


Figure (2) Extracting stage of the proposed system

2.1. Hiding stage

To explain the hiding stage of the proposed system we will take an example for a piece of image as illustrated in figure (3)

110	220	120	210	20
100	200	110	250	10
110	220	100	200	0
150	240	120	200	250
110	220	100	200	0

Figure (3) piece of image

The proposed system start by repairing the guide image for hiding information, we will used Sobel image as a guide image that will be calculated by applying the masks in figure (4), then the gradient image will be illustrated in figure (5)

-1	-2	-1
0	0	0
1	2	1

-1	0	1
-2	0	2
-1	0	1

Figure (4) horizontal and vertical Sobel masks

$$G = \sqrt{(G_x)^2 + (G_y)^2} \quad \ldots(1)$$

A	B	C
D	E	F
G	H	I

28	86	255
143	31	226
80	120	60

Figure (4) Sobel image

$G_x(A)$ = -110-440-120+110+440+100=-20
$G_y(A)$ = -110-200-110+120+220+100=20
G(A) = sqrt(800) = 28
$G_x(B)$ = -220-240-210+220+200+200= 50
$G_y(B)$ = -220-400-220+210+500+200= 70
G(B) = 86

And soon for other pixels as illustrated in figure (4), if the message that we want to hide is 110100101…. Then we will divided each pixel in gradient image by (64) as illustrated in figure (5)

0	1	3
2	0	3
1	1	0

Figure (5) Sobel image divided by (64)

Then, according to hiding algorithm we don't hide in pixel (A), and hide in least significant two bits in pixel(B) as follows

0	1	1	0	1	1	1	0	become	0	1	1	0	1	1	1	1

While we will hide in second bit in pixel(C) as follows

1	1	1	1	1	0	1	0	become	1	1	1	1	1	0	0	0

And so on for other pixels and message bits until hiding the message then the modified stego image will be illustrated in figure (6)

200	111	248
222	100	200
241	121	200

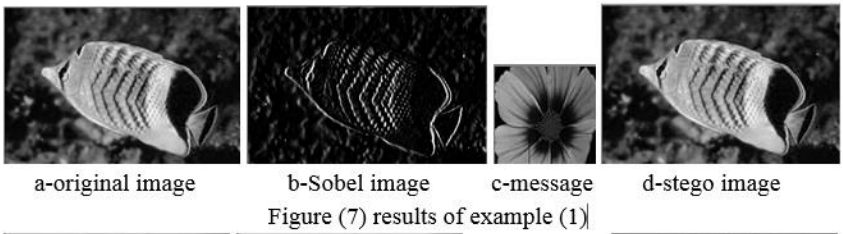
Figure (6) stego image

2.2. Extracting stage

The extracting stage work in the same way but in opposite direction with hiding stage and start with stego image until reached to the secure message.

3. Results

The proposed system will be applied on three image examples as follows:



a-original image b-Sobel image c-message d-stego image

Figure (7) results of example (1)

a-original image b-Sobel image c-message d-stego image

Figure (8) results of example (2)

a-original image b-Sobel image c-message d-stego image

Figure (9) results of example (3)

4. Conclusions

1- Each steganography algorithm hides information in LSBs, but these algorithms differ in the techniques that will be used in hiding process , the mechanism used in deciding the number of bits used in hiding message bits and the image that will be used in hiding process (DCT image, Gradient image, wavelet image, or original image)
2- Our proposed system used a key to decide the number and position of bits that will be used for hiding information and this key discover from cover image without help needing from sender.
3- Hiding in second or third bit is useful for keeping information secure if attacker change LSB or apply lossy compression algorithm.

REFERENCES

[Samir 2008] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjeeand Poulami Das "A Tutorial Review on Steganography", University of Calcutta, 2008.

[Vinay 2009] Vinay Kumar, and S. K. Muttoo "Principle of Graph Theoretic Approach to Digital Steganography", Institute of Computer Applications and Management, New Delhi, 2009.

[Dr.Umamaheswari 2010] dr.M.Umamaheswari, Prof.S. Sivasubramanian, and S.Pandiarajan "Analysis of Different Steganographic Algorithms for Secured Data Hiding", IJCSNS International Journal of Computer Science and Network Security, 2010.

[Gandharba 2010] Gandharba Swain, Dodda Ravi Kumar, Anita Pradhan, and Saroj Kumar Lenka "A Technique

for Secure Communication Using Message Dependent Steganography", International Conference ICCT, 2010.

[Masoud 2011] Masoud Nosrati, Ronak Karimi, and Mehdi Hariri "An introduction to steganography methods", World Applied Programming, 2011.