Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 - 3915

A New Method in Image Steganography with Improved Image Quality

Atallah M. Al-Shatnawi

Department of Information Systems
Al-albayt University , Mafraq, Jordan
atallah@aabu.edu.jo

Abstract

"Steganography" is a Greek origin word which means "hidden writing". Steganography word is classified into two parts: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text). In this paper, a new Steganography technique is presented, implemented and analyzed. The proposed method hides the secret message based on searching about the identical bits between the secret messages and image pixels values. The proposed method is compared with the LSB benchmarking method. It is implemented to hide the secret message "I will come to see you on the first of June" on two Bmp images, with size (24 x 502 x 333) and (24 x 646 x 165) respectively. The results of the proposed and LSB hiding methods are discussed and analyzed based on the ratio between the number of the identical and the non identical bits between the pixel color values and the secret message values. The proposed method is efficient, simple and fast it robust to attack and improve the image quality, hence it obtained an accuracy ratio of 83%.

Keywords: Steganography, Least Significant Bit, Bmp Image, Secret Information

1 INTRODUCTION

Steganography" is a Greek origin word which means "hidden writing". Steganography word is classified into two parts: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text). However, in the hiding information the meaning of Steganography is hiding text or secret messages into another media file such as image, text, sound ,video. [1][2][7]

Steganography ancient origins traced back to 440 BC. It was started by the Greeks by shaving the slaves hair heads and writing the message on their heads,

after the hair had been grown, they were sent to their allies in order to communicate with them without the enemies knowledge [7]. As well as, the invisible ink used for hiding the secret messages by the American revolutionaries during the USA Revolution. Also it was used in both World Wars by German army [9]. Another Steganography technique is the Spam Mimic software which developed by Wayner in (2003), this software was developed to detect and hide the secret messages in text file based on set of protocols [10] [11].

The motivation behind developing image Steganography methods according to its use in various organizations to communicate between its members, as well as, it can be used for communication between members of the military or intelligence operatives or agents of companies to hide secret messages or in the field of espionage. The main goal of using the Steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this goal that has been planned to achieve the security of the secret messages, because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message.[3][4]

The main terminologies used in the Steganography systems are: the cover message, secret message, secret key and embedding algorithm [5]. The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The secret message is the information which is needed to be hidden in the suitable 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 embed the secret information in the cover message. [7][11]

In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e image, video, audio, text) and select the effective secret messages as well as the robust password (which suppose to be known by the receiver). The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other modern techniques. The Stego file is the carried message with the secret information. After receiving the message by the receiver, he can decode it using the extracting algorithm and the same password used by the sender [7][11]. The Steganography system scenario is shown in the Figure 1.

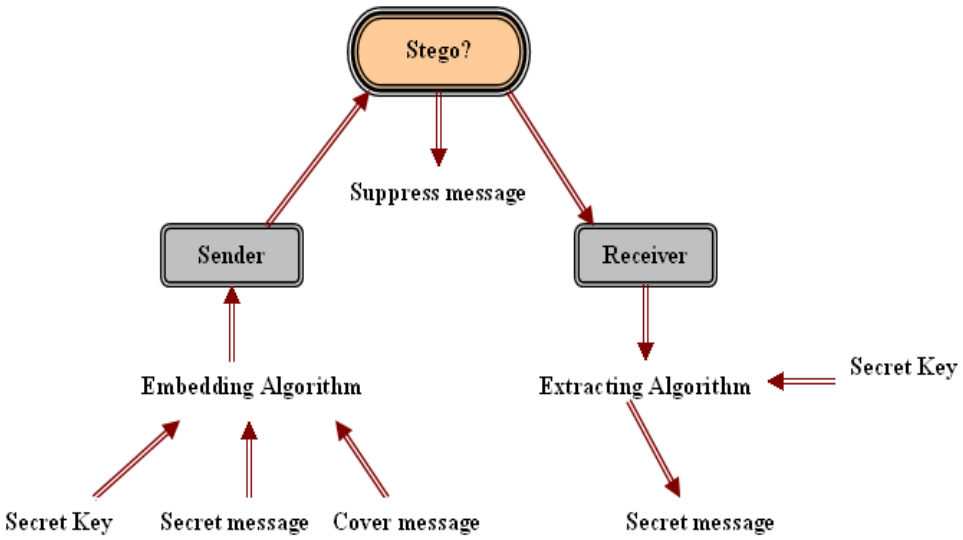


Figure 1: Steganography System Scenario

Many carrier messages can be used in the recent technologies, such as Image, text video and many others. The image file is the most popular used for this purpose because it easy to send during the communication between the sender and receiver. The images are divided into three types: binary (Black- White), Gray scale and Red-Green-Blue (RGB) images. The binary image has one bit value per pixel represent by 0 for black and 1 for white pixels. While the gray scale image has 8 bits value per pixel represent from 00000000 for black and 11111111 for white pixels. The RGB image has 24 bits values per pixel represent by (00000000, 00000000 and 00000000) for black and (11111111, 1111111 and 11111111) for white pixels. The RGB image is the most suitable because it contains a lot of information that help in hiding the secret information with a bit change in the image resolution which does not affect the image quality and make the message more secure. In this research paper the RGB images are used as a carrier message to hide the secret messages by the Least Significant Bit hiding method (LSB) as well as the proposed method. [6][5]

2 Least Significant Bit Hiding Technique (LSB)

LSB is the most popular Steganography technique. It hides the secret message in the RGB image based on it its binary coding. Figure 2 presents an example about pixel values and shows the secret message. LSB algorithm is used to hide the secret messages by using algorithm 1. LSB makes the changes in the image resolution quite clear as well as it is easy to attack. [8][9]

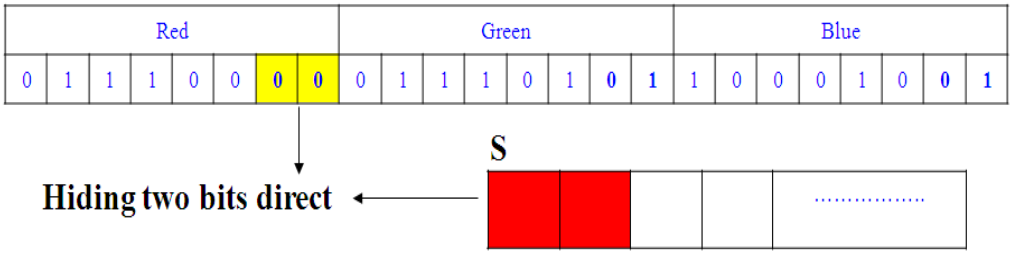


Figure (2) Least Significant Bit Hiding Technique

Algorithm (1) Least Significant Bit Hiding Algorithm.
Inputs: RGB image, secret message and the password.
Output: Stego image.

Begin
scan the image row by row and encode it in binary.
encode the secret message in binary.
check the size of the image and the size of the secret message.
start sub-iteration 1:
choose one pixel of the image randomly
divide the image into three parts (Red, Green and Blue parts)
hide two by two bits of the secret message in each part of the pixel in the two least significant bits.
set the image with the new values.
end sub-iteration 1.
set the image with the new values and save it.
End

3 The proposed method

LSB hiding technique hide the secret message directly in the least two significant bits in the image pixels, hence that affect the image resolution, which reduce the image quality and make the image easy to attack. As well as this method is already has been attacked and broken. Therefore a new technique that able to make the secret message more secure and enhance the quality of the image is proposed. The proposed method hides the secret message based on searching about the identical values between the secret messages and image pixels, see Figure 3. The proposed method is used to hide the secret messages by using algorithm 2.

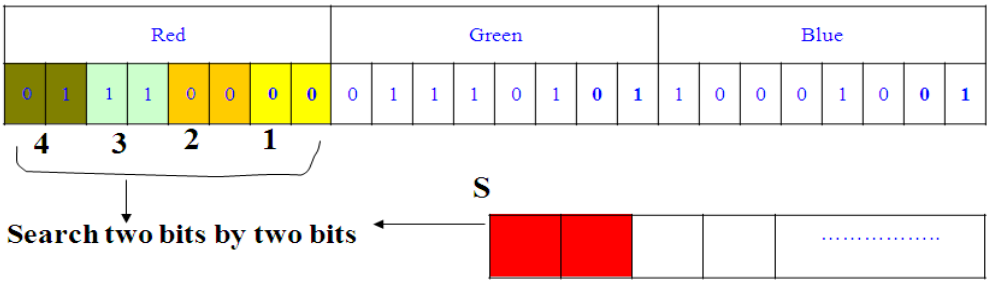


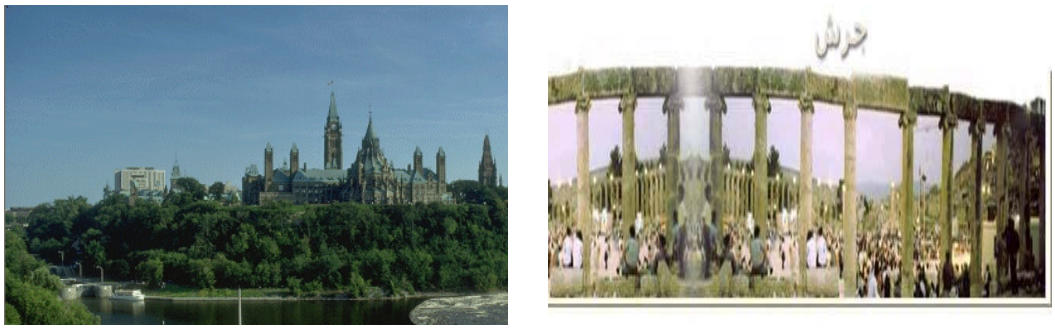
Figure (3) Least Significant Bit Hiding Technique

Algorithm (2) The Proposed Hiding Algorithm.
Inputs: RGB image, secret message and the password.
Output: Stego image.

Begin
scan the image row by row and encode it in binary.
encode the secret message in binary.
check the size of the image and the size of the secret message.
start sub-iteration 1:
choose one pixel of the image randomly
divide the image into three parts (Red, Green and Blue parts)
hide two by two bits of the secret message in each part of the pixel by searching about the identical.
if the identical is satisfied then set the image with the new values.
otherwise hide in the two least significant bits and set the image with the new values
save the location of the hiding bits in binary table.
end sub-iteration 1.
set the image with the new values and save it.
End

4 Experiment Results

The LSB and the proposed hiding algorithms have been implemented in the VB6 programming language on duo core 2.0 GHZ in 2012 The two methods are applied to hide the secret message "I will come to see you on the first of June" on two Bmp images, the first with size (24 x 502 x 333) and called "The nature image" which is considered as a darken image see Figure 4a, while the second one with size (24 x 646 x 165) and called "The Jerash image" which is considered as a light image, see Figure 4b.

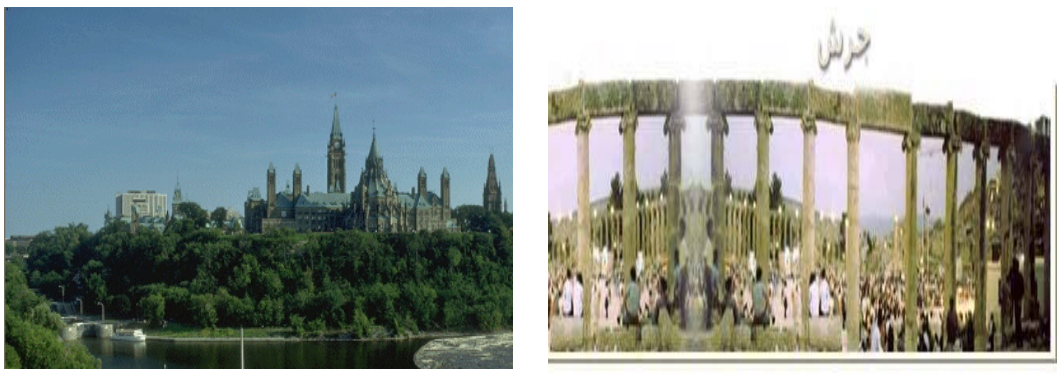


(a) (b)

Figure (4) Two Bmp images: (a) The Dark Image (the nature image) (b) The Light Image (the Jerash image).

5 Discussion and Analyses

The proposed method and the LSB hiding methods, hiding every 6 bits of the secret message in one pixel of the image which usually chosen randomly therefore the secret message used in this paper has 43 characters which are 344 bits, to hide those bits 58 pixels are needed. In this paper, the results of the proposed and LSB hiding methods are analyzed based on the ratio between the number of the identical and the non identical bits between the pixel color values and the secret message values. Figure 5 shows the resultant images and the analysis table which present the ratio success obtained by the proposed hiding method when applied on the 4a and 4b images respectively. On the other hand Figure 6 shows the resultant images and the analysis table which present the ratio success obtained by the LSB hiding method when applied on the 4a and 4b images respectively



	Identical	No IDT	Ratio IDT	Ratio no ID1	Net Ratio
CLR RED	46	12	79%	20%	99%
CLR GREEN	45	13	77%	22%	99%
CLR BLUE	49	9	84%	15%	99%
SUM	140	34			

(a)

	Identical	No IDT	Ratio IDT	Ratio no ID1	Net Ratio
CLR RED	35	23	60%	39%	99%
CLR GREEN	46	12	79%	20%	99%
CLR BLUE	31	27	53%	46%	99%
SUM	112	62			

(b)

Figure 5 The resultant images and the analysis table obtained by the proposed hiding method when applied on the (a) 4a and (b) 4b images.

	Identical	No IDT	Ratio IDT	Ratio no ID1	Net Ratio
CLR RED	18	40	30%	69%	99%
CLR GREEN	12	46	20%	79%	99%
CLR BLUE	16	42	27%	72%	99%
SUM	46	128			

(a)

	Identical	No IDT	Ratio IDT	Ratio no ID1	Net Ratio
CLR RED	12	46	21%	78%	99%
CLR GREEN	14	44	25%	74%	99%
CLR BLUE	13	45	23%	76%	99%
SUM	39	135			

(b)

Figure 6 The resultant images and the analysis table obtained by the LSB hiding method when applied on the (a) 4a and (b) 4b images.

Figure 7 shows the differences between the proposed and the LSB hiding methods in the dark and the light images. Based on that Figure, it is clear that the proposed method is more efficient than LSB method because it search about the identical then start hiding. As well as the change in the bits is quite low and doesn't affect the image resolution.

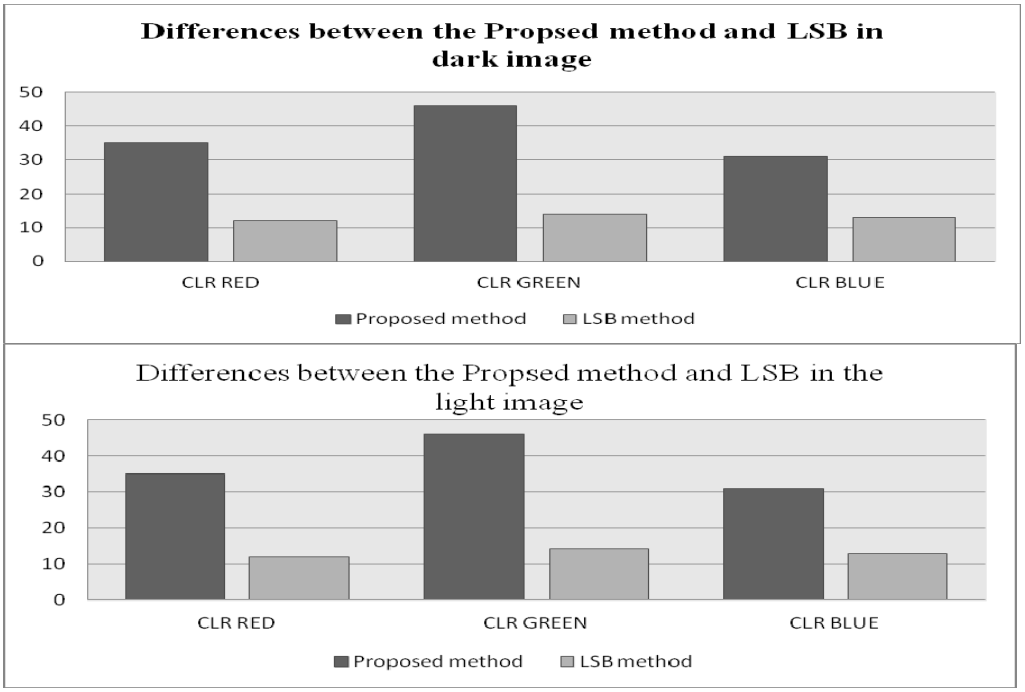


Figure 7 the differences between the proposed and the LSB hiding methods in the dark and the light images.

6 Conclusion

In this paper, a new Steganography technique was presented, implemented and analyzed. The proposed method 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 proposed and the LSB hiding methods were implemented to hide the secret message "I will come to see you on the first of June" on two Bmp images, with size (24 x 502 x 333) and (24 x 646 x 165) respectively.The results of the proposed and LSB hiding methods were discussed and analyzed based on the ratio between the number of the identical and the non identical bits between the pixel color values and the secret message values. This paper conclude that the proposed method is more efficient, simple, appropriate and accurate than LSB method, it search about the identical then start hiding, hence the change in the image resolution is quite low, as well as it makes the secret message more secure. This paper concluded that the LSB hiding method is the worst case of the proposed method. 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.

References

[1] B. Dunbar. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment, Sans Institute, 1(2002).
[2] C. Christian. An Information-Theoretic Model for Steganography, Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science. 1998.
[3] H. Wu, H. Wang, C. Tsai and C. Wang, Reversible image steganographic scheme via predictive coding. 1 (2010), ISSN: 01419382, 35-43.
[4] J, Corporation, Steganography. http://www.webopedia.com/ TERM/S/steganography.html. 2005.
[5] M. D. Swanson, B. Zhu and A. H. Tewfik, Robust Data Hiding for Images, IEEE Digital Signal Processing Workshop, University of Minnesota, September 1996 (37-40).
[6] N Ghoshal, J K Mandal .A steganographic scheme for colour image authentication (SSCIA), Recent Trends in Information Technology ICRTIT 2011 International Conference on (2011), 826-831.
[7] N. Johnson, Survey of Steganography Software, Technical Report, January 2002.
[8] N. Johnson, Digital Watermarking and Steganography: Fundamentals and Techniques , The Computer Journal. (2009)
[9] P. Fabien, J. Ross. Anderson, and Markus G. Kuhn. "Information Hiding – A Survey." Proceedings of the IEEE, 87:7. 1062-1078. 1999.
[10] Spam Mimic." http://www.spammimic.com.
[11] W, Peter. Disappearing Cryptography: Information Hiding: Steganography & Watermarking (second edition). San Francisco: Morgan Kaufmann. 3(1992) 192-213.

Received: March, 2012