IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 5, Issue 1, Feb - Mar, 2017
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Secure Communication Method Based On Steganography In Color Images

Uqba bn Naffa
Computer Science Department, University of Mustansiriyah, Baghdad, Iraq

Abstract: Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. For hiding secret information in images, there exists a large variety of Steganography techniques some are more complex than others and all of them have respective strong and weak points. The aim of this paper is to provide secure transmission of message by hiding them in image to prevent the detection of a secret message with no visual difference between the stego image and the cover image. The results of proposed method are given high PSNR values and reflect the Steganography techniques are more suitable for secure communication applications.

Keywords- Digital image steganography; spatial domain; frequency domain; adaptive steganography; security.

1. Introduction

Information security is essential for confidential data transfer. Steganography is one of the ways used for secure transmission of confidential information. It contains two main branches: digital watermarking and steganography. The former is mainly used for copyright protection of electronic products while, the latter is a way of covert communication. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit. Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file [1].

The main purpose of steganography is to convey the information secretly by concealing the very existence of information in some other medium such as image, audio or video. The content used to embed information is called as cover object. The cover along with the hidden information is called as stego-object [2]. In this paper color image is taken as cover and secret message is considered as secret information. Secret message and stego keys are embedded in the cover image to get stego image. The major objective of steganography is to prevent some unintended observer from stealing or destroying the confidential information [3].

The Steganography has been categorized into (i) Spatial domain Steganography: It mainly includes LSB Steganography and Bit Plane Complexity Slicing (BPS) algorithm. Spatial domain is frequently used because of high capability of hidden information and

easy realization. (ii) Transform domain Steganography: The secret information is embedded in the transform coefficients of the cover image. Examples of transform domain Steganography are Discrete Cosine Transform, Discrete Fourier Transform and Discrete Wavelet Transform. Steganography used for wide range of applications such as defiance organizations for safe circulation of secret data, intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials, medical imaging where patient's details are embedded within image providing protection of information and reducing transmission time [4].
A general scheme of steganography is given in Fig.(1) [5].

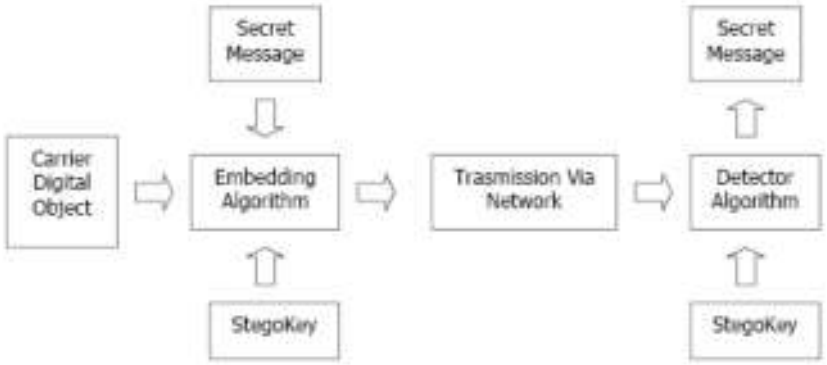

Figure (1): General scheme of steganography.

It shows the basic process involved in Steganography which consists of Carrier, Message and Key. Carrier is also known as cover-object, in which message is embedded and serves to hide the presence of the message. The data can be any type of data (plain text, cipher text or other image) that the sender wishes to remain confidential. Key is known as stego-key, which ensures that only recipient who knows the key, corresponding decoding key will be able to recover the message from a cover-object. The cover-object with the object secretly embedded message is then called the stego-object [4].
Some of related works are presented as follow: S. M. Masud Karim, et al., [5] proposed a new approach based on LSB using secret key. The secret key encrypts the hidden information and then it is stored into different position of LSB of image. This provides very good security. XIE Qing et al.,[6] proposed a method in which the information is hidden in all RGB planes based on HVS (Human Visual System). This degrades the quality of the stego image. In the method proposed by Sunny Sachdeva et al., [7] the Vector Quantization (VQ) table is used to hide the secret message which increases the capacity and also stego size. The method proposed by Rong-Jian Chen et al [8], presents the novel multi-bit bitwise adaptive embedding algorithm for data hiding by evaluating the most similar value to replace the original one. Sankar Roy et al., [9] proposed an improved steganography approach for hiding text messages within lossless RGB images which will suffer from withstanding the signal processing operations.

2. Proposed Method

The proposed method is designed to achieve the main aim of this paper. It is designed to hide secret message in color image to guarantee the secure communication between sender and recipient. The secret message is textual form which will be stored in colored cover image. In the proposed method, the cover is 256x256 color image. The main functions of the proposed system are: First, the Hiding Algorithm, which incorporates the secret message data into the host image. Second, the Extracting Algorithm, which recovers the secret message data from the received stego image. Fig.2 shows the main steps of proposed method.

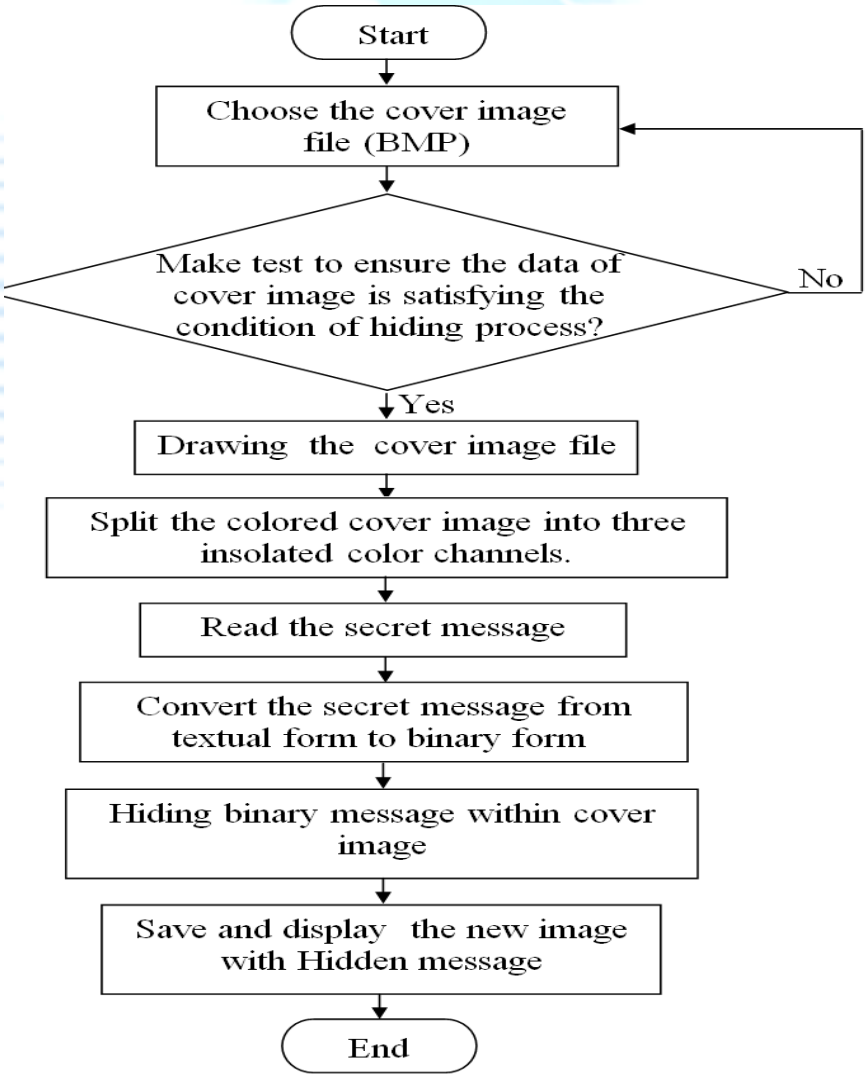

Figure (2): The Block Diagram of the proposed method.

This Algorithm is consisting of the following stages:

Stage 1: Loading Cover Image.
The input of the proposed method is a 24-BMP (true color) image
Stage 2: Split the colored cover image into three insolated color channels.
Stage 3: Read the secret message.
Stage 4: Convert the secret message from textual form to binary form. By using ASCII code method.
Stage 5: Hiding binary message within cover image.
In this stage the proposed method will be embed the entered message in cover image. This system, deals with bitmap (BMP) images, which utilize RGB (24-bit) color model. The BMP image file format consists of two parts, first is the header part which contains bits per pixel, size of image…etc, the second part is the image pixel values. (BMP) image is described in chapter two.
In this proposed method the hiding technique is the LSB technique, this is accomplished by replacing the least significant bit in the pixel bytes with the data to be hidden. Since the least significant pixel bits contribute very little to the overall appearance of the pixel, replacing these bits often has no perceptible effect on the cover image. The LSB technique is described in [10].
The secret key will use in the hiding operation to selection the hiding locations in cover image.
Stage 6: Save and display the new image with Hidden message.

3. Experimental Results

The algorithm is tested in MATLAB. The results with different cover images are shown. Original cover and stego images are shown in Fig. 3.

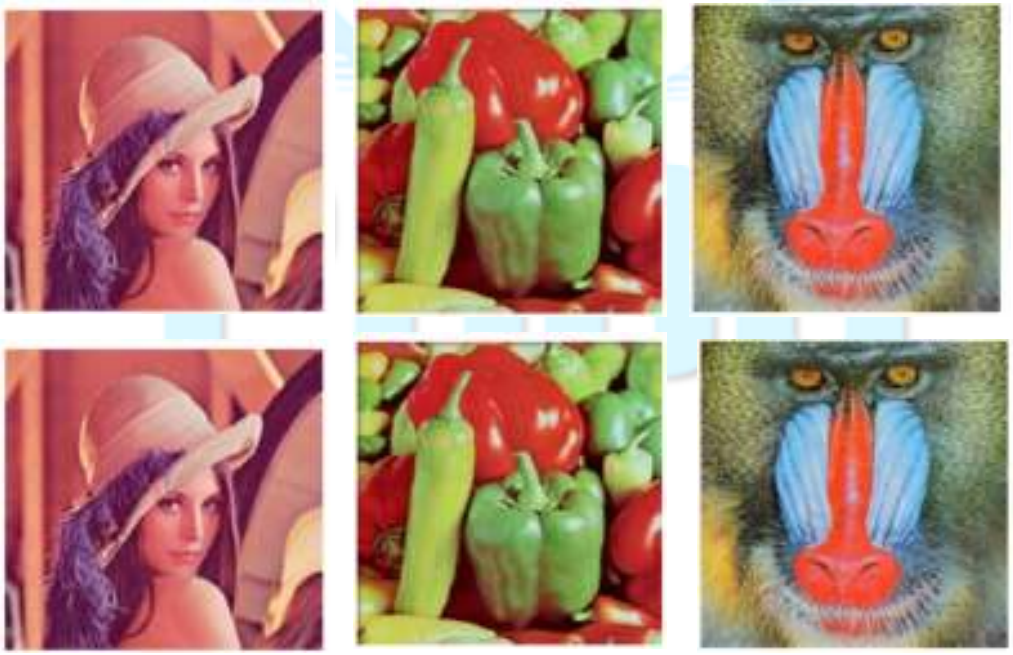

Figure (3): The results of proposed method; first row represents the original image, and second row represents the stego images.

Three cover images "Lena", "baboon" and "peppers", each of size 256X256, are considered for testing the algorithm. In all cases the average PSNR value of stego images is 44.7dB. Table 3 shows the PSNR value of the stego images in the proposed method.

Table (1): Results of proposed method

Stego Images	Quality indexes	
	PSNR(dB)	MAS
Lena	43.91	0.634
baboon	44.26	0.601
peppers	45.21	0.572

4. Conclusions

In this paper, we observe that secret message can be hidden in color image without significant distortion. This approach results in high quality of the stego image having high PSNR values compared to other methods. However the disadvantage of the approach is that it is susceptible to noise if spatial domain techniques are used to hide the key.

This can be improved if transform domain techniques are used to hide the key. The approach is very simple and the security level can be increased by using standard encryption techniques to encrypt the keys.

REFERENCES

[1]. Katzenbeisser, S. and Petitcolas, F.A.P., (2000) Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Boston, London.

[2]. Shejul, A. A., Kulkarni, U.L., (2011) "A Secure Skin Tone based Steganography (SSTS) using Wavelet Transform", International Journal of Computer Theory and Engineering, Vol.3, No.1, pp. 16-22.

[3]. Masud, Karim S.M., Rahman, M.S., Hossain, M.I., (2011) "A New Approach for LSB Based Image Steganography using Secret Key.", Proceedings of 14th International Conference on Computer and Information Technology, IEEE Conference Publications, pp 286 – 291.

[4]. Jagvinder Kaur and Sanjeev Kumar, " Study and Analysis of Various Image Steganography Techniques" IJCST Vol. 2, Issue 3, September 2011.

[5]. Masud, Karim S.M., Rahman, M.S., Hossain, M.I., (2011) "A New Approach for LSB Based Image Steganography using Secret Key.", Proceedings of 14th International Conference on Computer and Information Technology, IEEE Conference Publications, pp 286 – 291.

[6]. Xie, Qing., Xie, Jianquan., Xiao, Yunhua., (2010) "A High Capacity Information Hiding Algorithm in Color Image.", Proceedings of 2nd International Conference

on E-Business and Information System Security, IEEE Conference Publications, pp 1-4.

[7]. Sachdeva, S and Kumar, A., (2012) "Colour Image Steganography Based on Modified Quantization Table.", Proceedings of Second International Conference on Advanced Computing & Communication Technologies , IEEE Conference Publications, pp 309 – 313.

[8]. Chen, R. J., Peng, Y. C., Lin, J. J., Lai, J. L., Horng, S. J. Novel Multi-bit Bitwise Adaptive Embedding Algorithms with Minimum Error for Data Hiding. In Proceedings of 2010 Fourth International Conference on Network and System Security (NSS 2010), (Melbourne, Australia, 1-3 September 2010), IEEE Conference Publications, 306 – 311.

[9]. Roy, S., Parekh, R., (2011) "A Secure Keyless Image Steganography Approach for Lossless RGB Images.", Proceedings of International Conference on Communication, Computing & Security, ACM Publications, 573-576.

[10]. Jagvinder Kaur and Sanjeev Kumar, " Study and Analysis of Various Image Steganography Techniques" IJCST Vol. 2, Issue 3, September 2011