Volume 3, Issue 2, February 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis and Implementation of Algorithm to Hide Secret Message

Harvinder Singh(M.Tech)
AMITY University Noida
India

Anuj kumar
Lecturer, SIET Gr. Noida
India

Prateek Bansal
Lecturer, SIET Gr. Noida
India

Abstract- 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 analysed based on the ratio between the number of the identical and the non identical bits between the pixel colour values and the secret message values. As there are many techniques to perform steganography on electronic media, most notably audio and image files. The outcome of this paper is to generate a cross platform that can effectively hide a message inside a digital image file. An image is the combination of several pixels and each pixel has three colour numbers and an image consist of millions of numbers. So the change in few colour numbers resulting the picture which would probably look a lot likes the original image.

In this paper we are presenting the technique which works by changing a few pixel color value; we will use selected pixel value to represent characters instead of a color value. Obviously the resulting image will still look mostly like the original except that a few points seem little out of place if we look very closely.

Keywords— Steganography, Steganography Imaging System, Data hiding model, Steganographic attacks, Peak Signal to Noise Ratio

I. INTRODUCTION

Steganography" [1][2][11] 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. Steganography is the art of hiding the fact that communication is taking place, by hiding the information in or under information. There are different kinds of steganography used in communication channel but in digital file format the format that are more suitable are those with a high degree of redundancy. This can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily[1][2]. Hiding information in text is historically the most important method of steganography.an obvious method was to hide a secret message in every nth letter of every word of a text message text steganography using digital files is not used very often since text files have a very small amount of redundant data.

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[11].

Steganography Imaging System (SIS) is a system that is capable of hiding the data inside the image. The system is using 2 layers of security in order to maintain data privacy. Data security is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or corporate data. Privacy, on the other hand, is the ability of an individual or group to seclude them or information about themselves and thereby reveal them selectively. Data privacy or information privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal issues[15].

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).

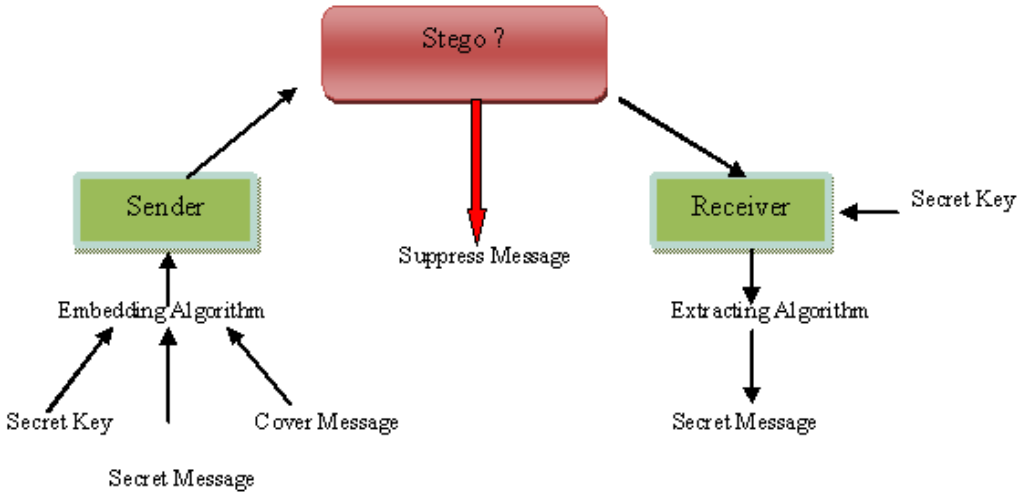
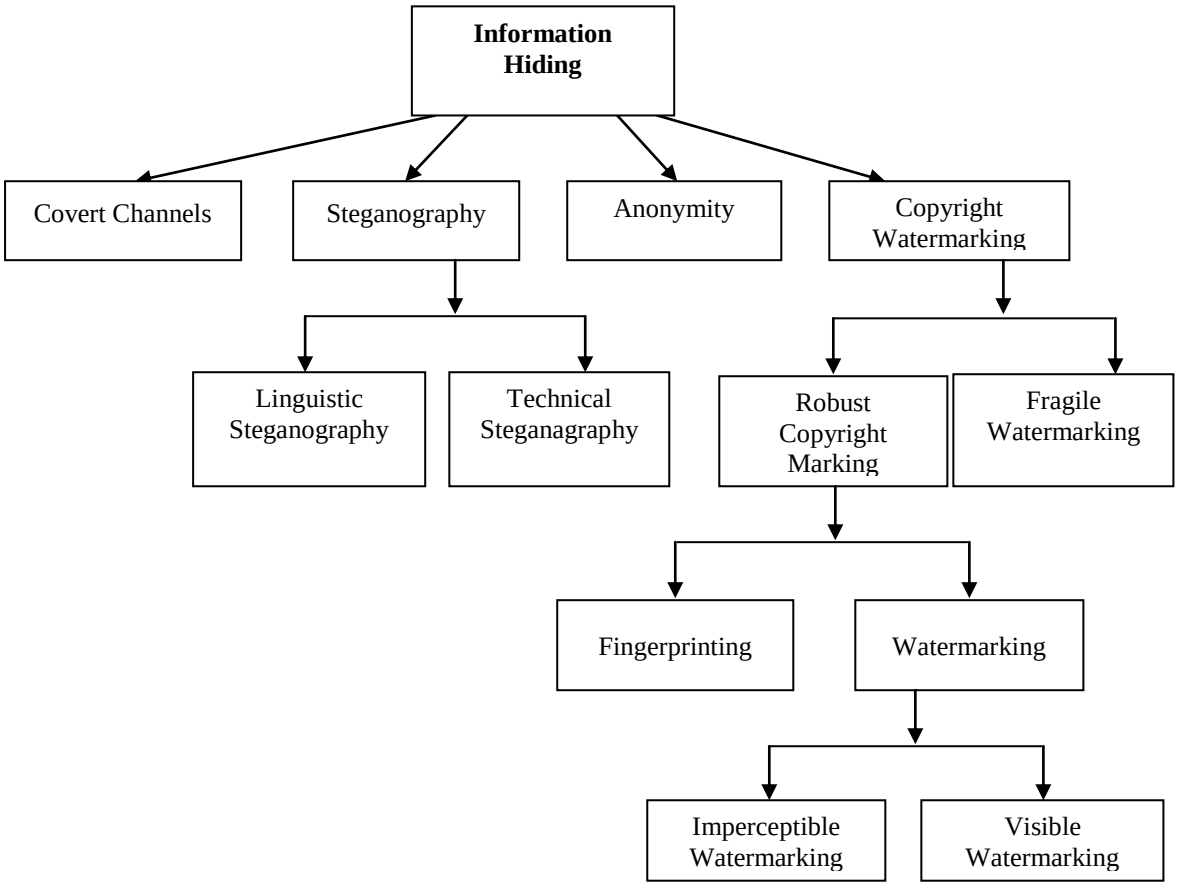


Figure1. General model of hiding data

The general model of hiding data in other data can be described as follows. The *embedded* data is the message that one wishes to send secretly. It is usually hidden in an innocuous message referred to as a *cover-text*, or *cover-image* or *cover-audio* as appropriate, producing the *stego-text* or other *stego-object*. A *stego-key* is used to control the hiding process so as to restrict detection and/or recovery of the embedded data to parties who know it



. *Figure 2. Classification of information hiding techniques*

II. RELATED WORK

Hiding data is the process of embedding information into digital content without causing perceptual degradation [8] . In data hiding, three famous techniques can be used. They are watermarking, steganography and cryptography. Steganography is defined as covering writing in Greek. It includes any process that deals with data or information within other data. According to Lou [9] et al., steganography is hiding the existence of a message by hiding information into various carriers. The major intent is to prevent the detection of hidden information. Research in steganography technique has been done back in ancient Greek where during that time the ancient Greek practice of tattooing a secret message on the shaved head of a messenger, and letting his hair grow back before sending him through enemy territory where the

latency of this communications system was measured in months[10]. The most famous method of traditional steganography technique around 440 B.C. is marking the document with invisible secret ink, like the juice of a lemon to hide information.

Another method is to mark selected characters within a document by pinholes and to generate a pattern or signature.However, the majority of the development and use of computerized steganography only occurred in year 2000. The main advantage of steganography algorithm is because of its simple security mechanism. Because the steganographic message is integrated invisibly and covered inside other harmless sources, it is very difficult to detect the message without knowing the existence and the appropriate encoding scheme[12]. There are several steganography techniques used for hiding data such as batch steganography, permutation steganography, least significant bits (LSB), bit-plane complexity segmentation (BPCS) and chaos based spread spectrum image steganography (CSSIS).

Algorithm for embedding data inside image.

Algorithm
Begin
Input: Cover_Image, Secret_Message, Secret_Key;
Transfer Secret_Message into Text_File;
Zip Text_File;
Convert Zip_Text_File to Binary_Codes;
Convert Secret_Key into Binary_Codes;
Set BitsPerUnit to Zero;
Encode Message to Binary_Codes;
Add by 2 unit for bitsPerUnit;
Output: Stego_Image;
End

Figure 3. Algorithm for embedding data inside image.

For the steganography algorithm, Figure 3 shows the algorithm for embedding the secret message inside the image[15]. During the process of embedding the message inside the image, a secret key is needed for the purpose of retrieving the message back from the image. From Figure 3, the secret message that is extracted from the system is transferred into text file first. Then the text file is compressed into the zip file. The zip text file then is used for converting it into the binary codes. The purpose of zipping the text file is because the zipped text file is more secured if compared with the file that is without the zipped. The contents in the zipped file will significantly hard to be detected and read. Furthermore, this series of binary codes of the zipped text file and the key is a long random codes in which they only consist of one and zero figures. A data hiding method is applied by using this series of binary codes. By applying the data hiding method, the last two binary codes from the series are encoded into a pixel in image, then, next two binary codes are encoded to the next pixel in image, the process is repeated until all the binary codes are encoded. The secret key in this proposed steganography algorithm is playing an essential role where the key is acts as a locker that used to lock or unlock the secret message. For the data hiding method, each last two bit is encoded into each pixel in image. This will ensure the original image will not be tempered with too many changes.

Algorithm for extracting data from stego image.

Begin
Input: Stego_Image, Secret_Key;
Compare Secret_Key;
Calculate BitsPerUnit;
Decode All_Binary_Codes;
Shift by 2 unit for bitsPerUnit;
Convert Binary_Codes to Text_File;
Unzip Text_File;
Output Secret_Message;
End

Figure 4. Algorithm for extracting data from stego image.

Once the message is hidden inside the image, this message can be extracted back from the stego image.
Figure 4 shows the algorithm for extracting the secret message from the stego image[15]. In order to retrieve a correct message from the image, a secret key is needed for the purpose of verification. From Figure 4, for the data extracting method, a secret key is needed to detect whether the key is match with the key that decodes from the series of binary code. Once the key is matched, the process continues by forming the binary code to a zipped text file, unzip the text file and transfer the secret message from the text file to retrieve the original secret message.

Limitations of some information hiding systems

A number of broad claims have been made about the `robustness' of various digital watermarking or fingerprinting methods. Unfortunately the robustness criteria and the sample pictures used to demonstrate it vary from one system to the

other, and recent attacks In some cases the watermark is simply said to be `robust against common signal processing algorithms and geometric distortions when used on some standard images'. This motivated the introduction of a fair benchmark for digital image watermarking.

Similarly, various steganographic systems have shown serious limitations. Craveretal. identify at least three kinds of attacks:

robustness attacks which aim to diminish or remove the presence of a digital watermark, *presentation attacks* which modify the content such that the detector cannot detect and the watermark anymore and the *interpretation attacks* whereby an attacker can devise a situation which prevents assertion of ownership. The separation between these groups is not always very clear though[4][5].

III. DISCUSSION AND ANALYSIS

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

Figure 5(a)

Figure.5(b)

Figure .5 Two Bmp images: (a) The Dark Image (the nature image) (b) The Light Image (the Jerash image).

	Identical	No IDT	Ratio IDT	Ratio no IDT	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			

	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			

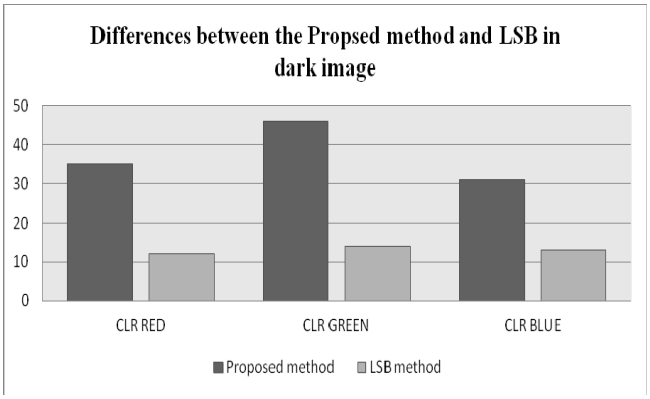
Figure 6 The resultant images and the analysis table obtained by the proposed hiding method when applied on the (i) 5(a) and 5(ii) 5(b) images.

	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			

	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			

Figure 7 The resultant images and the analysis table obtained by the LSB hiding method when applied on the (i) 5(a) and (ii 5(b) 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.



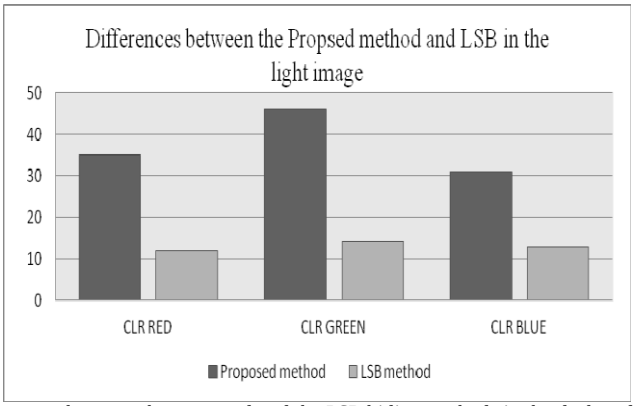


Figure 8 the differences between the proposed and the LSB hiding methods in the dark and the light images.

IV. CONCLUSIONS AND RESULTS

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.

Proposed approach gives satisfactory PSNR value to establish the robustness of the work. Since only selected high frequency components are modified for the hiding method, therefore there must be a constraint on the secret image size. Final results can be improved further by applying proper image filter.

Peak Signal to Noise Ratio (PSNR)

It measures the quality of a stego image. This is basically a performance metric and is used to determine perceptual transparency of the stego image with respect to host image:

$$PSNR = \frac{MN \max_{x,y} P_{x,y}^2}{\sum_{x,y} \left(P_{x,y} - \overline{P}_{x,y}\right)^2}$$

Where, M and N are number of rows and columns in the input image,

$P_{x,y}$ is the original image and

$\overline{P}_{x,y}$ is the Stego Image.

PSNR between Cover Image and Stego Image is 34.0240 shown in Table1.

Table 1

Cover Image vs. Stego Image	PSNR
	34.0240

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] M. Chen, N. Memon, E.K. Wong, Data hiding in
document images, in: H. Nemati (Ed.). Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.
[9] D.C. Lou, J.L. Liu, H.K. Tso, Evolution of information – hiding technology, in H. Nemati (Ed.), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.
[10] Schneider, Secrets & Lies, Indiana:Wiley Publishing, 2000.
[11] E. Cole, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Indianapolis: Wiley Publishing, 2003.
[12] T. Jahnke, J. Seitz, (2008). An introduction in digital watermarking applications, principles and problems, in: H. Nemati (Ed), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference,2008, pp. 554-569.
[13] M. Warkentin, M.B. Schmidt, E. Bekkering,
Steganography and steganalysis, Premier reference
Source–Intellectual Property Protection for Multimedia Information technology, Chapter XIX, 2008, pp. 374-380.
[14] N.N. El-Emam, Hiding a large amount of data with high security using steganography algorithm, Journal of Computer Science 3 (2007) 223-232.
[15] R. Ibrahim and T.S. Kuan, Steganography imaging system (SIS): hiding secret message inside an image, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2010, San Francisco, USA, 2010, pp. 144-148.

