Journal of Advanced Computing and Communication Technologies ***(ISSN:* 2347 - 2804*)***
Volume No.2 Issue No. 3, June 2014

A New Method for Image Steganography With Enhanced Confidentiality

By

[1]Aparajita, [2]Prof Ajay Rana
Assistant Professor, Dept. of MCA
Galgotias Institute of Management and Technology. Greater Noida (UP), India.
Program Director, Dept. of CSE
Amity School of Engineering and Technology, Amity University, Noida (UP), India.
aparajitagupta2000@gmail.com

ABSTRACT
Steganography is the art of hiding information within other information in such a way that it is hard or even impossible to identify that it is there. As the demand of more secure yet efficient image steganography techniques has increased, there are many different steganography and encoding techniques have been proposed. The aim of this paper is to propose a new approach for the steganography with improved confidentiality. In this manuscript we are also presenting a new table for encoding the characters.

Keywords
Steganography, steganalysis, cover-image, stego-image, cryptography, watermarking.

1. INTRODUCTION
We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material.

Cyber Crime is a term used broadly to describe criminal activity in which computers or networks are a tool, a target, or a place of criminal activity. Telemarketing and Internet fraud, identity theft, and credit card account thefts etc are considered to be cyber crimes. It is one of the world's costliest problems, but one which many organizations fail to secure themselves properly against. Steganography and Cryptography techniques can be employed to hide and encrypt the information from the attackers. An unhidden coded message, no matter how unbreakable it is, will arouse suspicion and may in itself be incriminating, as in some countries encryption is illegal [1].

Steganography derives from the Greek word, “Steganos”, meaning covered or secret and “graphy” means writing or drawing. Steganography is the technique which provides secrecy of a secret message it could be text or image to prevent them from third parties. Generally in steganography secret information is stored into the particular position of Least Significant Bit of a cover image which is can be understood as the carrier to embed messages [2, 3, 4, and 5]. No one can notice the embedded message in the stegoimage, by the human eye or by computer analysis without access to the original image [6]. A great deal of attention is paid to ensuring that the secret message goes unnoticed if a third party were to intercept the cover Work. The extracting process is traditionally a much simpler process as it is simply an inverse of the embedding process, where the secret message is revealed at the end [7].

The entire process of steganography for images can be presented graphically as shown in figure 1. The system shown in the figure 1 is probably the most common system of image steganography today. Inputs are required for the embedding process are secret message which is usually a text file that contains the secret message that you want to transfer and cover image which is used to construct a stegogramme that contains a hidden secret message. We can see the functioning entities, the processing functions and their input and output. In the next step pass the inputs from the Encoder, which will be designed to embed the secret message within an exact copy of the cover Work which requires a key to operate, such that minimum distortion is made. The lower is distortion; the better will be chances of undetectability. Without using the key it would be possible for someone to correctly extract the message if they managed to get hold of the embedding or extracting algorithms and read the secret message. By the application of key it is possible to randomise the way the stegosystem encoder operates, and the same key will need to be used when extracting the message so that the stegosystem decoder knows which process to use.

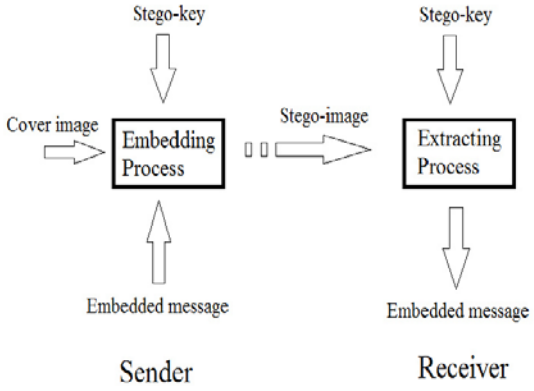

Fig. 1 Process of Steganography for Images

This means that if the algorithm falls into the attacker's hands, it is very difficult that they will be able to extract and encode the message successfully. The result from the encoder is the stegogramme, which is designed to be as similar to the cover Work as possible, except it will contain the secret hidden message. This stegogramme is then sent over network along with the key that was used to embed the message. When message is received at receiver end both the stegogramme and the key are then fed into the decoder where an estimate of the secret message is extracted. When stegogramme is send over the network through various communication channels, stegogramme may be subjected to noise that will change some values and distort the original image or message. So we can have only estimation of the output message which is extracted from decoder. Therefore, we can never be sure that the message extracted is an exact representation of the original.

2. LITERATURE SURVEY

All material on each page should fit within a rectangle of 18 x 23.5 cm (7" x 9.25"), centered on the page, beginning 2.54 cm (1") from the top of the page and ending with 2.54 cm (1") from the bottom. The right and left margins should be 1.9 cm (.75"). The text should be in two 8.45 cm (3.33") columns with a .83 cm (.33") gutter.

In this section we will discuss the main principles of steganography and steganalysis by firstly discussing where we currently stand in both fields, and then introducing the necessary background knowledge that is required to properly understand the proposed method.

There are many techniques developed by researchers. El Safy, R.O, Zayed. H. H, EI Dessouki. A [7], used an adaptive steganographic technique based on IWT, which improves the hiding capacity and PSNR compared to DWT technique which was proposed by B. Lai and L. Chang [8]. The hiding capacity and PSNR were further improved by Elham Ghasemi, Jamshid Shanbehzadeh and Bahram ZahirAzami [9], who use a steganographic method based on IWT and Genetic Algorithm. Silvia Torres-Maya, Mariko Nakano-Miyatake and Héctor Perez-Meana [10] propose an image steganography system based on Bit Plane Complexity Segmentation (BPCS) and IWT, in which the data is hidden in bit planes of subband wavelets coefficients obtained by using the IWT. To increase data hiding capacity the replaceable IWT coefficient are defined by a complexity measure using BPCS. Guorong Xuan et al, [11] propose a watermarking technique using IWT in which the watermark is embedded in the middle bit planes of the IWT coefficients in the middle and high frequency subbands. Several steganography methods based on LSB have been proposed and implemented [12][13][14].

As described above all the available techniques used in early tools are old and follow some specified process with some improvements to previously proposed techniques. This makes the intruders work easy. The intruder may try a counter attack by making some changes to counter existing techniques. None of the existing techniques offers protection through multiple levels. That is one of the reasons why an intruder is able to view/obtain hidden data with just one or two attacks.

Currently many cryptography and steganography techniques have come into existence. Encoding of plaintext is achieved using DES, AES, Triple DES, RSA and many other algorithms. Any individual can use one's own approach as encryption method. Traditional methods of securing communication were based on cryptography which means secret writing, which encrypts plain text to generate cipher text. However, the transmission of cipher text may easily arouse attackers' suspicion, and the cipher text may be attacked or decrypted violently. Steganography's goal is to keep its mere presence undetectable, but steganographic systems because of their invasive nature-leave behind detectable traces in the cover medium. Even if secret content is not revealed, the existence of it is: modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called statistical steganalysis. Steganography gets a role on the stage of information security [16, 17].

Many algorithms such as JSteg, JPHide and JPSeek, OutGuess, F3, F4 and F5 were invented for the purpose of embedding images. These algorithms follow a certain principle to embed and retrieve hidden contents. All the existing approaches have their own disadvantages as they can easily be compromised using steganalysis. It means that one way or another, an intruder can figure out the existence of hidden data which results in him/her compromise of sensitive data. Currently, no integration of cryptography and steganography approach in one application exists for image based information security. There are encryption and embedding approaches present that work with plaintext only.

3. PROPOSED STEGANOGRAPHIC SYSTEM

In this Working Architecture shown in Figure 2, we may use One Bit Stego, Two Bit Stego or Three Bit Stego as per user requirements and we will use new encryption/decryption

method to make more secure our transmitted data on communication channel.

Steps involved in proposed technique:

1. Encrypt text file which is containing secret message by using new encryption algorithm. By encrypting the text file it will be converted into cipher text file.

2. Cipher text file will be merging in to jpeg Plain Image file also called as cover-image. After the merging the whole image will be called as stego image.

3. Stego Image having secret hidden cipher text will be transfer via communication channel.

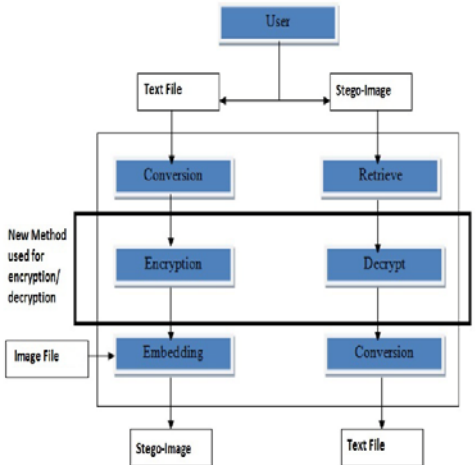

Fig. 2 Working System Architecture

4. At the receiver side the file will be received and receiver will retrieve Cipher Text File from Stego Image and regenerate Plain Image.

5. Decrypt Cipher text file using new developed method by applying reverse algorithm for encoding.

For the above steganographic system we will use new encryption/decryption method described in next section for text file encryption/decryption for increasing data confidentiality.

Proposed Steganography Algorithm

Firstly we encrypt text file by using new encryption method proposed in this manuscript.

Encoding

To reduce the number of character, 8-bit are reduced to 7-bit by considering 7 character at a time. The actual translation follows mapping of values from 0 to 127 characters (A-Z, a-z, 0-9 etc). New Designed Table (Confidential):

TABLE I. mapping of values from 0 to 127 characters

Values	Character
	A
1.	B
2.	C
- - - - -	- - - - -
- - - - -	- - - - -
- - - - -	- - - - -
125	Û
126	Ü
127	Ý

For example, consider string “Hello Sandy”. Base 128 (7-bit code) interpretation for given string is as follows.

1. Convert the character to binary.

2. “Hello S” is

01001000 01100101 01101100 01101100 01101111 00100000 01010011

3. Convert the 56 bit from 8 bit group to 7 bit group

0100100 0011001 0101101 1000110 1100011 0111100 1000000 1010011

4. Convert each of 7-bit into decimal

0100100 = 36

0011001 =25

0101101 =45

1000110 =70

1100011 =99

0111100 =64

1010011 =83

5. Use of the 8 bit decimals to lookup the base 128 (7 bit code) character code (table generated).

36 =K

25 =Z

45 =t

70 = +

99 = Ú

60 =8

64 = %

83 =?

6. You now have first 7 ASCCII character (“Hello S”) encoded as 7 bit code.

(“KZt+ Ú 8% ? “)

Decoding

Decrypt Cipher text file using reverse steps of encoding by new proposed method.

1. You now have first encoded 7 bit code.

(“KZt+ Ú 8% ? “).

2. Use of the 8 bit decimals to lookup the base 128 (7 bit code) character code (table generated).

K=36

Z =25

t =45

+ =70

Ú =99

8 =60

% =64

? =83

3. Convert each of decimal into 7 bit

36 = 0100100

25 = 0011001

45 = 0101101

70 = 1000110

99 = 1100011

64 = 0111100

83 = 1010011

4. Convert the 56 bit from 8 bit group to 7 bit group

0100100 0011001 0101101 1000110 1100011 0111100 1000000 1010011

5. Base 128 (7-bit code) interpretation for given string is as follows.

01001000 01100101 01101100 01101100 01101111 00100000 01010011

6. Convert the binary to character.

7. Decoded String “Hello S”.

4. PERFORMANCE SPECIFICATION

The primary idea behind developing this technique is to protect confidential data from an intruder’s counter-attacks and to block the intruder through various levels in his/her attacks. A new tool has been developed with a combination of cryptographic encryption and stegangraphic encryption for its implementation .The developed steganographic tool has a sender’s segment that can take a message, a password and a cover image as input and give a stego-image as output that has message embedded in it. On the other hand, it also has a receiver’s segment where the receiver inputs the stego-image and the same password is used by the sender as input to get the sender’s message as output. The project is tested with various inputs and made sure that the generated stego-image has no noise are data loss.

The developed steganographic tool is a very useful to any user who shares confidential data through a network .The developed model has a customized access that gives more freedom to users. An interface has been developed that helps the user to interact with the tool. The interface is very user-friendly with different modules implemented to encode and decode the secret message. The developed tool was tested for various input conditions.

The system was designed using an image of size 200x150 (30000) pixels. The message text was converted into cipher text using the proposed encryption algorithm. Then we have to take 128 color GIF image to hide the message. The cipher text was then embedded into the image.The image containing message data was found to have no visible distortion as shown in figure 3.

(a) (b)

Fig. 3 Experimental result from the proposed method on an image: (a) Original image, (b) Stego image

For decryption the cipher was extracted by checking the pixel variations and inverse function was applied to retrieve the message. To retrieve the cipher from the image, after this the encrypted message was retrieved from the image. The inverse of proposed encryption algorithm was applied to this encrypted message in order to retrieve the original message text.

Proposed steganocryptic algorithm combines the features of cryptography and steganography and hence provides improved confidentiality of the message. The algorithm also is more secure than a normal cryptographic system as the data is encrypted and mapped by new designed table. The image bits are used not to store the message but a slight deviation which correspond to a unique character. This deviation is then retrieved from the image and used to decrypt the original message.

5. CONCLUSION

This paper proposes a novel approach for steganography in which only a mapping of the secret information with the cover is embedded rather than the actual secret information, minimizing the risk of the secret information exposure even if the payload is revealed to an adversary. The major objectives of any steganography system include maximizing the hiding capacity and imperceptibility. In this paper a secure image steganography technique is proposed to hide images, which also tells how to hide data bits. The experimental results show that the technique produces good quality stego images with good PSNR values with reasonable execution time In the process of embedding information into the cover image, a successful threshold strategy is used. All the operations are done with user-friendly interface.

6. REFERENCES

[1] An Overview of Steganography for the Computer Forensics Examiner - http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm.

[2] F. Hartung and M. Kutte "Information hiding-a survey, "Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Content, Volume: 87 Issue: 7, pp. I062-I078, July 1999.

[3] M. Hossain, S.A. Haque, F. Sharmin, "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Iriformation", Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December 2009, Dhaka, Bangladesh.

[4] Na-I Wu, "A Study on Data Hiding/or Gray-Level and Binary Images ", http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=OCBwQFjAA&url=http%3A%2F%2Fethesys.lib.cyut.edu.tw%2FETD-db%2FETDsearch%2Fgetfile%3FURN%3Detd-0707104144705%26filename%3Detd-0707104-144705.pdf&ei=yMavTr7LOoSBhQet3pHRAg&usg=AFQjCNFztbb-TMOJ3fg_ Qvv8DsUDY8qwA ,Accessed on March 2009.

[5] GJ. Simmons, "The Prisoners' problem and the subliminal channel," in proc. CRYPTO'83, pp. 51-67, 1983.

[6] L. M. Marvel, C. G. Boncelet, C. T. Retter, "Spread Spectrum Image Steganography," IEEE Transactions on Image Processing, vol. 8, no. 8, August 1999.

[7] Abdelmgeid Amin Ali, Al-Hussien Seddik Saad, New Text Steganography Technique by using Mixed-Case Font.

[8] El Safy, R.O, Zayed. H. H, El Dessouki. A "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", IEEE conference, 2009, pp 111-117.

[9] Lai and L. Chang, "Adaptive Data Hiding for images Based on Harr Discrete Wavelet transform," Lecture Notes in Computer Science, Volume 4319, 2006.

[10] Elham Ghasemi, Jamshid Shanbehzadeh and Bahram ZahirAzami, "A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm", IEEE conference 2011, pp 42-45.

[11] Silvia Torres-Maya, Mariko Nakano-Miyatake and Héctor Perez-Meana, "An Image Steganography Systems Based on BPCS and IWT", 16th IEEE International Conference on Electronics, Communications and Computers, 2006.

[12] Guorong Xuan, Jiang Zhu, Jidong Chen, Yun Q. Shi, Zhicheng Ni and Wei Su, "Distortionless data hiding based on integer wavelet transform", IEEE Electronic letters, December 2002 Vol. 38 No. 25, pp. 1646-1648.

[13] C. K. Chan, L. M. Cheng, "Hiding data in image by simple LSB Subst itution", pattern recognition, Vol. 37, No. 3, 2004, pp. 469-474.

[14] R. Z. Wang, C. F. Lin and I. C. Lin, "Image Hiding by LSB substitution and genetic algorithm", Pattern Recognition, Vol. 34, No. 3, pp. 671-683, 2001.

[15] D. Sandipan, A. Ajith, S. Sugata, An LSB Data Hiding Technique Using Prime Numbers, The Third International Symposium on Information Assurance and Security, Manchester, UK, IEEE CS press, 2007.

[16] A. Nag, S. Biswas, D. Sarkar, P. P. Sarkar, "A Novel Technique for Image Steganography Based on Block-OCT and Huffman Encoding". International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010.

[17] Neil F. Jhonson, Sushil Jajodia. "Exploring Steganography: Seeing the Unseen". IEEE paper of February 1998.