INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

EFFICIENT ADAPTIVE STEGANOGRAPHY ALGORITHM

Dr. THAMIR RASHED SAEED,

SHAYMAA ABD-ELGHANY

IJPRET-QR CODE

PAPER-QR CODE

Department of Electrical Eng. - Unv. Of Technology/ Iraq, Electronic Design for Signal Processing Research Group, Ciphering Research Group

Accepted Date:

20/07/2013

Publish Date:

01/08/2013

Keywords

Steganography,

LSB,

Probability of Detection

Corresponding Author

Dr. Thamir Rashed Saeed

Abstract

With the emergence of the Internet and its explosive growth as a communication medium and, due to advances in Internate technology(IT), most of the information is kept electronically, as well, the development of network techniques, the problem of network security becomes more and more important. Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse the eaves-dropper's suspicion. Three different aspects information-hiding systems contend with one other: capacity, security, and robustness. The proposed algorithm based on the assumption that the enemy has full knowledge of the design. The steganographic system is also known as adaptive steganographic (as hidden data is adapted according to give size & statistics of image before, and after hiding the data) .Then, by using our proposed algorithm, probability of detection is reduced from 6.56% to 0.431% , and the false-negative rate was0.564%, while the hiding improvement was 15.2%. The algorithm presented in this paper reduces the distortion by hiding information in LSB of the image pixels. Also, the detection rate weakness was overcome, by non-repeating which means the probability of detection nearly equal to zero. The two strength points in the proposed algorithm are inversely related and depend on the text (massage) size.

1. INTRODUCTION

With the emergence of the Internet and its explosive growth as a communication medium and in content distribution capabilities, the need to protect ourselves and our property is greater than it has ever been [1].

Also, due to advances in IT, most of the information is kept electronically, and with the development of network techniques the problem of network security becomes more and more important, and, It is necessary to protect this information specially while communicating over insecure channels like internet [2].Security means protection from unauthorized users of hackers, and, providing high security to prevent data modification.

Cryptography and Steganography are ways of secure data transfer over the Internet [4], while, increasing at the data transfer rate over the internet. This area of data security has gained more attention over the recent period of time [3].

Cryptography scrambles messages so they cannot be understood. Steganography has enjoyed a lot of importance since last decade. The Art of steganography has attracted human attention for many years, on the other hand, It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists [1, 3, 4, 5]. If a steganography method causes someone to suspect the carrier medium, then the method has failed [6]. In some situations, sending an encrypted message will arouse suspisuspicion while invisible message will not do so. Both sciences can be combined to produce better protection of the message. Here, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques [4, 7].

2. STEGANOGRAPHY

Because Steganography is a technique of hiding information in digital media, therefore, this approach of information hiding technique has recently become important in several application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly[6].

In steganography, the text to be concealed is called embedded data. An innocuous medium, such as text, image, audio, or video file; which is used to hide embedded data is called cover. The key (optional) used in embedding process is called a stage - key.

A stego-key is used to control the hiding process to restrict detection and/or recovery of embedded data to the parties who know it. The stego object is an object we get after hiding the embedded data in a cover medium as shown in figure (1)[4], where;

Cover medium + embedded message + stegokey = stego-medium [3]

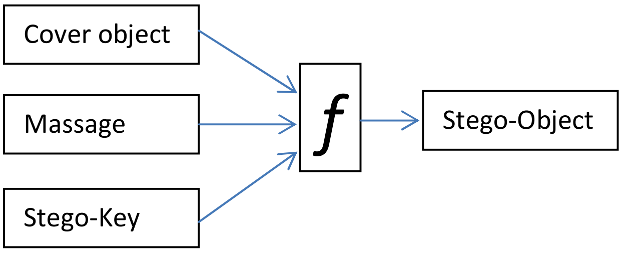


Figure (1) Stego-system

Three different aspects of information-hiding systems contend with one nother: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to the eaves-dropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [8].

In order to embed secret data in a cover message, the cover must contain a sufficient amount of redundant data or noise. This is because in the embedding process Steganography actually replaces redundant data with the secret message.

Spatial domain steganography is a technique in which secret message is encoded in the LSBs of carrier image. More the number of LSBs used for hiding the secret message more will be the capacity of carrier image but also more will be the distortion in the stego image.

There are basically three types of steganographic protocols used. They are Pure Steganography, Secret Key Steganography, and Public Key Steganography [1].

There are many applications for digital steganography of image, including copyright protection, feature tagging, and secret communication. Copyright notice or watermark can embed in an image to identify it as intellectual property. If someone attempts to use this image without permission, we can prove by extracting the watermark.[6]

3. **DESCRIPTION OF THE STEGANOGRAPHY ALGORITHM**[3]

In the Steganography algorithm, two parts (data hiding at the sender side and data extracting at the receiver side). These parts are constructed and implemented to satisfy the following requirements:

1. The algorithm must reduce the chances of statistical detection.

2. The algorithm must provide robustness against a variety of image manipulation attacks.

3. The stego-image must not have any distortion artifacts.

4. The algorithm must not sacrifice embedding capacity in order to achieve the above requirements.

Review of Steganography Techniques:

Monika,[4], presents three novel approaches of text steganography. The first approach uses the theme of missing letters puzzle and hides each character of secret message in a word by missing one or two letters in that word depending on the ASCII value of the embedded character. The second approach works by hiding messages in a list of words where the starting letter of word and word length is determined by the ASCII value of the character to be hidden. In the third approach, the cover comprising of paragraphs can be drawn from any source like newspaper/book. The approach conceals secret bits using start and end letter of words of cover file. Unlike the first two proposed approaches in which cover comprising of a collection of words.

Manish and Navdeep [1], dealt with adaptive steganography which take care of the important characteristics & statistics on the cover image well in advance to the embedding of secret data, so that the disturbance of image statistics, which attracts the forgery or unauthorized access, can be minimized.

Phad and et al [2], have developed a high security model by combining Cryptography and Steganographic security. In cryptography was used advanced encryption standard (AES) algorithm to encrypt secret messages by pixel value differencing (PVD) with K-bit least-significant-bit (LSB) substitution to hide encrypted message into true color RGB image.

Amin and Ali [5], have embedded the massage in non-uniform region in a uniform image areas make attack visual in uniform areas to prevent attacks. They examine the complexity of each block, if there is complexity block, placing for half-tone; otherwise the blocks are going to next.

Nirmalya and Puspita[9], presented an efficient method for hiding data into an image and send to the destination in a safe manner. The technique does not need any key for embedding and extracting data. Also, it allows hiding four bits in a block of size 5×5 with minimal distortion. The proposed algorithm ensures the security and safety of the hidden information.

Saddaf and Younus [10], have devised a new algorithm to hide the text in any colored image of any size using wavelet transform. It improves the image quality and imperceptibility. His method sustains the security attacks. Extensive testing is performed using different sizes of images and presented his results in payload and PSNR values.

4. PROPOSED ALGORITHM

The proposed algorithm as shown in Figure (3) is based on the assumption that the enemy has full knowledge of the design and implementation details of the steganographic system. The steganographic system is also known as adaptive steganographic (as hidden data is adapted according to given size& statistical of image before and after hiding the data) , also, the size of the imagewhich selected to covered depend on the size of the information (massage). The algorithm steps are;

1. The image size Mz= 209 X 270 =56430 pixels
2. Splitting the image matrix into two matrices Mz1 and Mz0 according to the LSB of each pixel before hiding the message;Where:

Mz1=28221 pixels , and

Mz0=28209 pixels.

3. Text (massage) size Tz =463 bytes (3707 bits).
4. The massage bits hidden distribution by non-repeated randomly to the LSB of image pixels as ;

Pixel No. which hides the bit of massage in LSB of it is;

$PHB = a^i \mod p$ (1)

Where;

a- Primitive root of prime p and

$0 \leq i \leq p\text{-}1$

P- Prime number which has primitive root equal to the image size.

5. Then splitting the image matrix as in step 2, where Mz1=28237 pixels, and Mz0=28193 pixels. At this step its clear the number of pixels which have LSB equal one and zero are different from that before the hidden a text. This means the distortion can be detected.
6. To overcome the above weakness, determine the difference of the number of pixels which have a one and zero at LSB from the pixels which not have a text.
7. Add one's and zero's to that pixel to satisfy the numbers in step 2, where Mz1=28221 pixels and Mz0=28209 pixels.

The true-positive ratethe probability that an image detected by Stegdetect really has steganographic contentas follows [8];

$$p(S|D) = \frac{p(S)\times P(D|S)}{P(D)} = \frac{P(S)\times\ P(D|S)}{P(S).P(D|S)+P(\neg S).P(D|\neg S)} (2)$$

Where

P(S) - Probability of steganographic content in images, P(¬S) - complement of P(S)

P(D|S) - probability that we'll detect an image that has steganographic content,

P(D|¬ S) is the false-positive rate. Conversely,

$p(\neg D|S) = 1 - P(D|S)$
(3)

Where;

$p(\neg D|S)$ – false-negative rate.

Then, by using our proposed algorithm, probability of detection before adding one's and zero's(step 6) P(D|S) =6.56% and after adding one's and zero's (step 7) P(D|S) =0.431% , and the false-negative rate $p(\neg D|S) = 0.564$, The hiding improvement Hi=15.2%

5. RESULTS

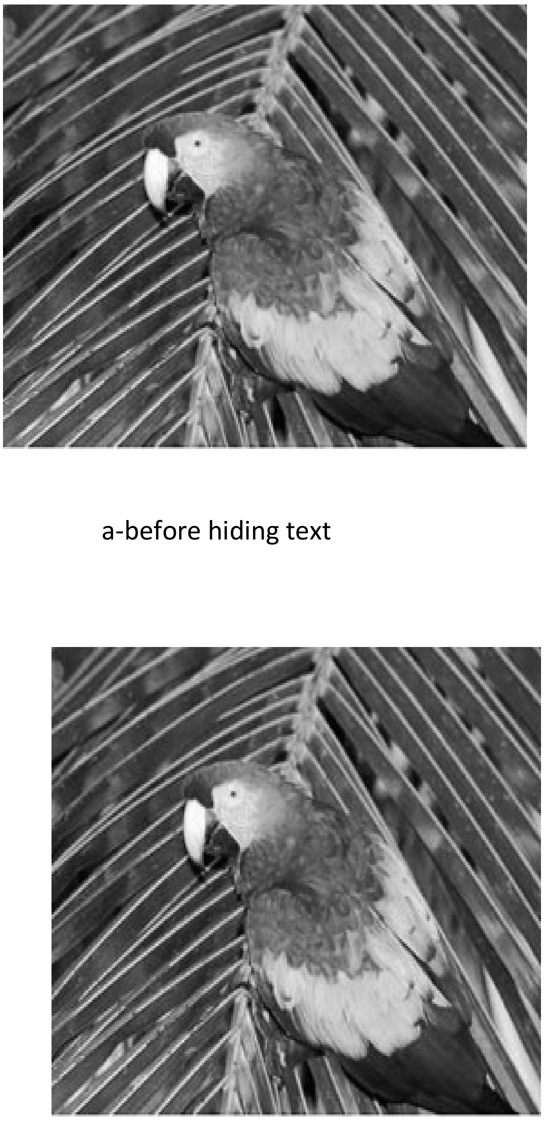
Three features of the proposed algorithm can be observed from the results, these are ;

No distortion of the image as shown in the Figure (2-a, 2-b) before, and after the hiding the teat (massage). As well as the probability of detection as set out in the form where it's less than it is without the use of the proposed algorithm as shown in Figure (4). Also, can be observed the number one's and zero's and how it has changed when hidden a text (massage) and, then, adding one's and zero's in other pixels for reducing the statistical detection as shown in Figure (5).

6. CONCLUSION

Often the statistical analyzed of stego-image which reflects or show the presence of certain hidden data in the image .In our proposed algorithm, we overcome this weakness of the steganographic system cause reduce the statistical detection, to reduce the distortion by use hidden in LSB of the image pixels. Also, the detection rate weakness was overcome it, by non-repeated which the probability of detection nearly equal to zero.

However the two power points in proposed algorithm are inversely related and depend on the text (massage) size. Where the text size decrease the non–repeated distribution factor affect on detection will reduce, and the adding noisy data to re-statistical of an original image factor affect will increase and the capacity will decrease, and vice versa. Nevertheless, the LSB distortion though it is little but exists. We examine our work by wifi internet network for many cases and get same results.



a-before hiding text

b-after hiding text

Figure (2) Cover-Image

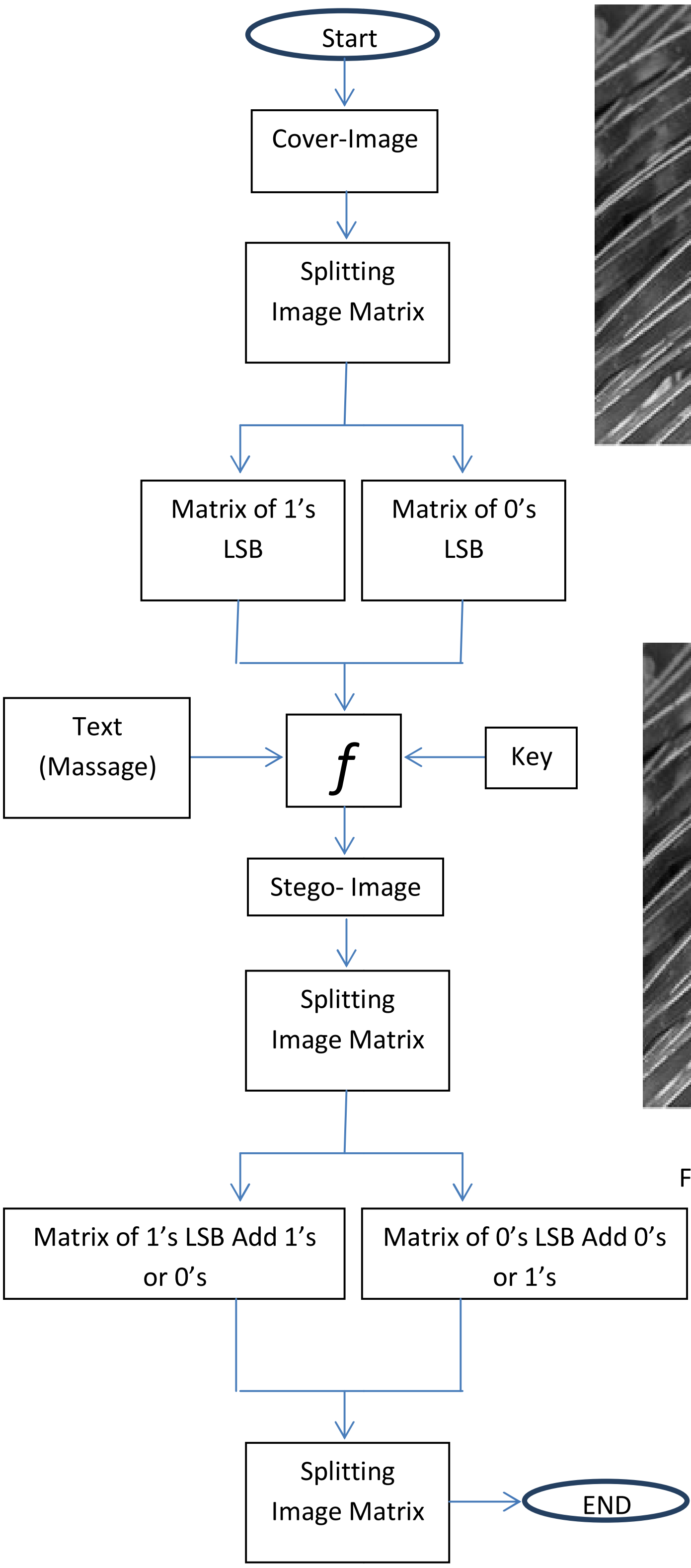


Figure (3) Flowchart of proposed algorithm

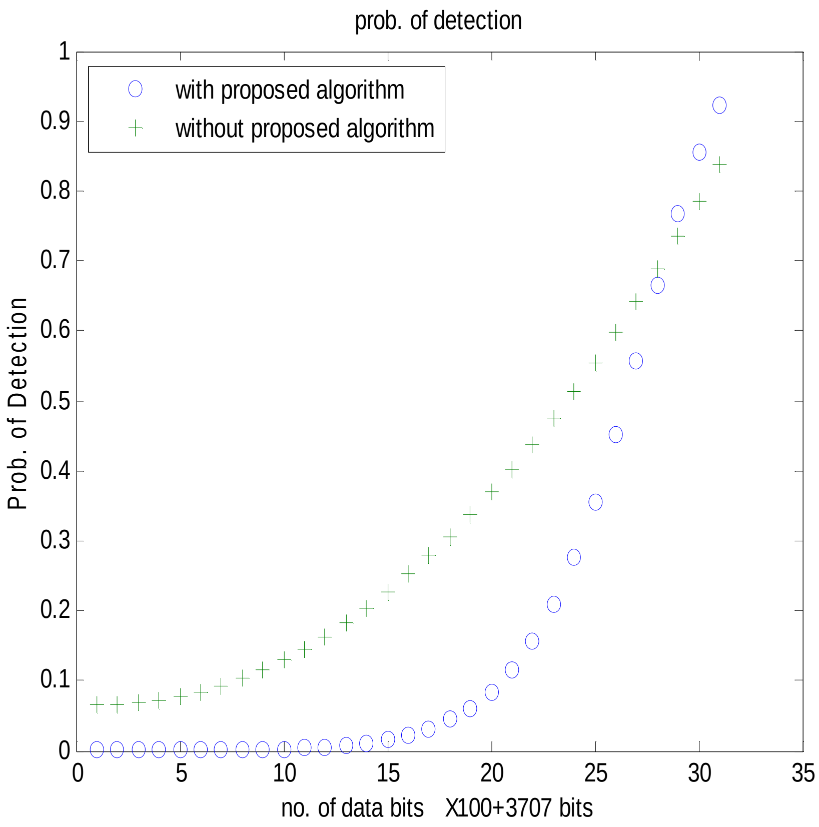
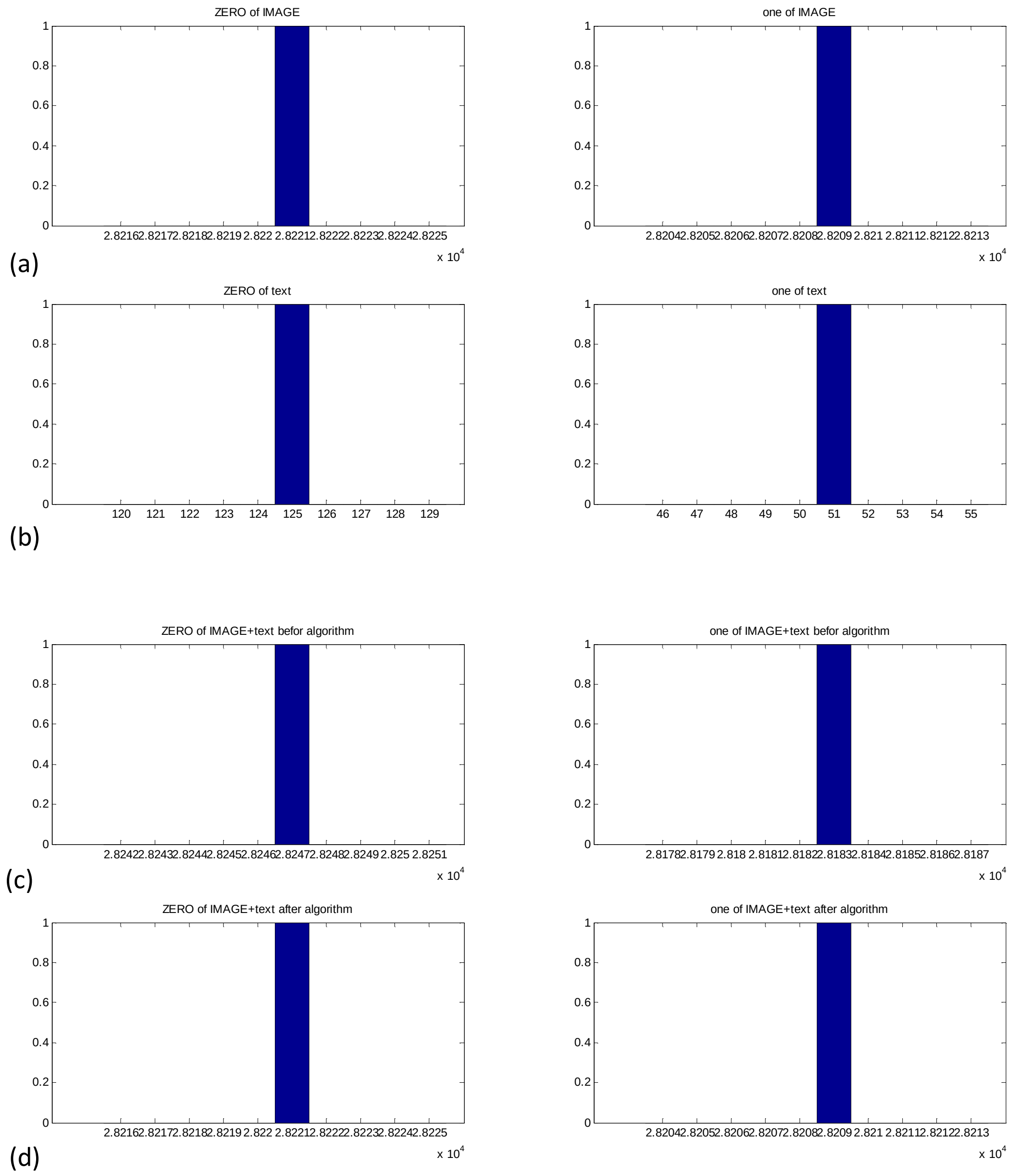


Figure (4) Prob. Of Detection with and without a proposed Algorithm



REFERENCES

1. M. Mahajan and N. Kaur, "Adaptive Steganography: A Survey of Recent Statistical Aware Steganography Techniques,", I. J. Compter Network and Information Security, 10, 76-92, 2012.

2. P. Vitthal, B. Rajkumar and P. Archana, " A Novel Security Scheme for Secret Data Using Cryptography and Steganography,", I. J. Compter Network and Information Security, 2, 36-42, 2012.

3. J. Majumder and S. Mangal, " An Overview of Image Steganography Using LSB Technique," National Conference on Advances n Computer Science and Applications with international Journal of Comuter Application (NCAVSA 2012).

4. M. Agarwal, "Text Steganographic Approches: A Comparison," International Journal of Network Security and Its Applications (IJNSA), Vol. 5 No. 1 Jan. 2013.

5. A. H. Pour and A. Payandeh, "A New Steganography Method Based on the Cmplex Pixels," Journal of Information Security, 3, 202-208, 2012.

6. MM Amin, "Information Hiding Using Steganography," Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on Pag. 21 - 25, 14-15 Jan. 2003.

7. J. R. Krenn, "Steganography and Steganalysis,"www.krenn.nl/univ/cry/steg/article.pdf.

8. N. Provos and P. Honeyman," Hid and Seek: An Introduction to Steganography," IEEE Security and Privacy, Vol. 1 Issue 3, Page. 32-44

9. N. Chowdhury and P. Manna, "An Efficient Method of Steganography Using Matrix Approch," I. J. Intelligent Systems and Applications, 1, 32-38, 2012.

10. S. Rubab and m. Younus, "Improved Image Steganography Technique for Colored Images Using Wavelet Yransform," International Journal of Computer Application, Vol. 39, No. 14 Feb. 2012.