

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

A Novel Even Pixel Replacement (EPR) Steganography Technique

Aron Sylvester¹, Dr.T.Meyyapan²

¹Reserach Scholar, ²Professor

¹²Department of computer Science and Engg, Alagappa Unviersity,
Karaikudi, Pin no.630001

¹aronsylvester2014l@gmail.com, ²meyyappant@alagappauniversity.ac.in

Abstract - Security is one of the main concerns in the communication spectrum. To increase the security of the content there exist many methods and algorithms, which enhance more protection to the user-defined data. Steganography is the art of hiding information from the user's perception. In steganography, secret information is embedded in plain content. This will provide more protection to the data. The Steganography has the advantage that, the hidden object does not catch the attention of itself as an entity of analysis. Authors of this propose a new substitution method in Steganography, which can generate stronger cipher than the existing substitution algorithms. In this method, each letter in the plaintext is replaced by a letter in even numbered positions. In this paper we are discussing Existing image steganography techniques like Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT).The result of the paper shows our techniques provides increased level of security to the data and also increases quality of stego image.

Keywords — Steganography, LSB, Hash-LSB, Data Hiding, Substitution Ciphers.

1. INTRODUCTION

The art of hiding the information is so called as "Steganography". Its main goal is to provide and secure the data from unauthorized user's perception. Steganography today, however, is significantly more sophisticated that, allows a user to hide large amounts of information within image and audio files. These forms of Steganography often are used in conjunction with cryptography so that the information is doubly protected.

The main difference between cryptography and Steganography is that cryptography scrambles the message so that it becomes difficult to understand whereas Steganography hides the very existence of a message. Steganography plays the central role in secret message communication. Several message hiding techniques have been developed and implemented in the past using digital images, audio/video files and other media [6].

Digital communication has become an essential part of infrastructure nowadays, it is desired that the communication be made secret. Two techniques are available to achieve this goal: one is cryptography, where the sender uses an encryption key to scramble the message. The second method is Steganography, where the secret message is embedded in another message. Using this technology even the fact that a secret is being transmitted has to be secret.[2] The following is the basic Steganography methodology,

$$\text{covermedium} + \text{hiddendata} + \text{stegokey} = \text{stegomedium}$$

In this context, the cover medium is the files in which the users will hide the data, which may also be encrypted using the stegokey. The resultant file is the stego medium. The cover medium is typically image or audio files. An image file is merely a binary file containing a binary representation of the color or light intensity of each picture element (pixel) comprising the image. Images typically use either 8-bit or 24-bit color. When using 8-bit color, there is a definition of up to 256 colors forming a palette for this image, each color denoted by an 8-bit value. In this case, each pixel is represented by three bytes, each byte representing the intensity of the three primary colors red, green, and blue (RGB), respectively.

Choosing the hiding medium as the criteria, the steganographic techniques are classified as (i) Text- or linguistic based Steganography , (ii) Audio Steganography , (iii) Image Steganography hide the secret message in the images which is nearly impossible to differentiate by human eyes. Spatial domain technique approaches embeds the message in intensity of image pixel directly. In transform domain technique the images are transformed into frequency coefficients and messages are embedded in transformed coefficients[9].

The rest of the paper is organized as follows. Section 2 describes various related work that have been contributed in this research area. Section 3 embraces various existing methods and techniques for the Steganography process and their merits. Section 4 discusses the proposed method for the information

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

hiding. It is then followed, by the experimental results and their Conclusions. Finally, the section 5 concludes and interpretes the outcome of the experimental results.

2. LITERATURE REVIEW

Soumyendu Das, Subhendu das, Bijoy et.al [10] have shown different approaches on Steganography and steganalysis. They elucidate the different approaches towards implementation of steganography using 'multimedia' file (text, static image, audio and video) and Network IP datagram as cover medium. The stego multimedia produced by existing methods for in a steganography is more or less vulnerable to attacks like media formatting, compression etc. In this respect, IP datagram steganography technique is not susceptible to different type of attacks.

Arvind Kumar and KM.Pooja [2] in their work, discusses about the data hiding techniques. They discusses how digital images can be used as a carrier to hide messages. Performance Analyses of some of the steganography tools are also elucidated. Steganography is a useful tool that allows covert transmission of information over the communications channel. Combining secret image with the carrier image gives the hidden image. The hidden image is difficult to detect without retrieval.

Anil Kumar and Rohini Sharma [1]. embrace the secure image Steganography using the RSA algorithm and LSB hash technique. They have proposed a new technique of image steganography i.e. Hash-LSB with RSA algorithm for providing more security to data. Their proposed technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. This technique makes sure that the message has been encrypted before hiding it into a cover image. If in any case the cipher text got revealed from the cover image, the intermediate person other than receiver can't access the message as it is in encrypted form

Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dughav, [4] thrash out the steganography using Least Significant Bit method. They give a brief idea about the image steganography that make use of Least Significant Bit (LSB) algorithm for hiding the data into image. Their work creates a stego image in which the personal data is embedded and is protected with a password which is highly secured.

The main intention of the project is to develop a steganographic application that provides good security. The proposed approach provides higher security and can protect the message from stego attacks. By using the Least Significant Bit algorithm the algorithm becomes faster and reliable and compression ratio is moderate compared to other

algorithms.

Prabakaran Ganesan and R.Bhavani, [9] shows a high secure and robust image steganography using dual wavelet and blending model. A high secure steganography scheme hiding a 256×256 size gray secret image into a 512×512 size gray cover image with different combination of Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT). Pixel Value Adjustment (PVA) is first performed on cover image. The secret image values are scrambled by using Arnold transform. The DWT /IWT is applied on both cover and scrambled secret image. Blending process is applied to both images and compute Inverse DWT/IWT on the same to get the stego image. The extraction model is actually the reverse process of the embedding model. Different combination of DWT/IWT transform is performed on the scrambled secret image and cover image to achieved high security and robustness.

Neil F. Johnson and Sushil Jajodia in [6,7] discuss three popular methods for message concealment in digital images. These methods are LSB insertion, masking and filtering and algorithmic transformations. Marvel and Retter in [5] introduced a new method of image steganography. The method embeds the hidden information within white Gaussian noise (WGN) which is subsequently added to the digital image to form the stego-image. The hidden information is encoded by an error control code before it is embedded into the WGN signal. The WGN signal with the embedded data, the stego-signal, is then added to the image. At the receiver, the embedded stego-signal is estimated as the difference between the stego-image and the denoised version of the stego-image. The embedded information is extracted from the estimated stego-signal and any remaining errors are corrected by the error-control decoder [6].

3. EXISTING METHODS AND ALGORITHMS

This section briefly discuss about the techniques already exists for the steganographic process such as Substitution system, Transform Domain techniques, statistical Steganography, Distortion technique used.

A Substitution System

In substitution system, the data substitutes with redundant parts of a cover with a secret message. Basic substitution systems try to encode secret information by substituting insignificant parts of the cover by secret message bits. The most important substitution technique is the LSB (Least Significant Bit) Substitution Method.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

B Least Significant Technique

The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the coverimage. If user is using 24-bit color, the amount of change will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

Table 1. RGB Encoding

10010101	00001101	11001001
10010110	00001111	11001010
10011111	00010000	11001011

Now suppose the user want to "hide" the following 9 bits of data (the hidden data is usually compressed prior to being hidden): 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in **bold** have been changed):

Table 2. LSB Technique

10010101	000011 0	11001001
100101 1	000011 1	110010 1
10011111	00010000	11001011

C Pixel Value Adjustment (PVA)

The gray scale cover image and payload pixel intensity values vary from zero to 255. During the payload embedding process the intensity values of cover image may exceed lower and higher levels which results in difficulty to retrieve the payload at the destination. Hence the cover image pixel intensity values are limited to lower 15 and upper 240 instead of zero and 255 [9].

D Haar-DWT

Haar wavelet operates on data by calculating the sums and differences of adjacent elements. A 2-D Haar-DWT operates first on adjacent horizontal operation and the other is the vertical one. One nice feature of Haar wavelet transform is that the transform is equal to its inverse[9].

E Arnold Transform

The first mathematical Arnold transform is proposed By Arnold and Avez (1968). It's improved chaotic map Introduced by Mishra et al. (2012) which is applied to a Digital image that randomizes the original organization Of its pixels and the image becomes imperceptible or Noisy. However, it has a period and if iterated number of times, the original image reappears [9].

F Integer Wavelet Transform

Integer Wavelet Transform is a Nonlinear transform Having a structure of lifting scheme and as its

rate Distortion. Performance similar to DWT, Wavelet Transforms that map integers to integers allow faultless reconstruction of the original image. The algorithm employs the wavelet transform coefficients to Insert messages into four subbands of two dimensional Wavelet transform. To avoid problems with floating point Precision of the wavelet filters, the Integer Wavelet Transform is used.

G Steganalysis

Steganalysis is the process of identifying steganography by inspecting various parameter of a stego media. The primary step of this process is to identify a suspected stego media. After that steganalysis process determines whether that media contains hidden message or not and then try to recover the message from it.

In the cryptanalysis it is clear that the intercepted message is encrypted and it certainly contains the hidden message because the message is scrambled.

H SteganalysisTechniques

The properties of electronic media are being changed after hiding any object into that. This can result in the form of degradation in terms of quality or unusual characteristics of the media: Steganalysis techniques based on unusual pattern in the media or Visual Detection of the same.

I SteganographyAttacks

Steganographic attacks consist of detecting, extracting and destroying hidden object of the stego media. Steganography attack is followed by steganalysis. There are several types of attacks based on the information available for analysis. Some of them are as follows:-

- Known carrier attack: The original cover media and stego media both are available for analysis.
- Steganography only attack: In this type of attacks, only stego media is available for analysis.
- Known message attack: The hidden message is known in this case.
- Known steganography attack: The cover media, stego media as well as the steganography tool or algorithm.

4. PROPOSED METHODOLOGY

In this section the detailed proposed methodology is presented. Steganography substitution technique uses the Least Bit Significant replacement. Our proposed work instead of replacing LSB, the pixels in the even place of block transmission is replaced with the user

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

provided data ASCII value. Thus, for the normal user perception there will be no change in the cover media. The procedure for the bit replacement is as follows:

A Data Insertion using Even Pixel replacement and substitution policy

- Step 1: Read the plain text.
- Step 2: Read the Image, The image is used as the cover media.
- Step 3: Get each pixel from the input image.
- Step 4: Convert the user provided plain text into several blocks. Each block will comprise of 3 characters.
- Step 5: Read the even number place value of the pixel. Remove that pixel for the replacement of the text.
- Step 6: Convert the each block's character into corresponding ASCII value and Substitute each block value instead of the already replaced pixel.
- Step 7: Repeat the steps until last block of the input text is reached.

B Data Retrieval

- Step 1: Read the Replaced Image.
- Step 2: Read the even number place value pixel, so as to get the Red, Green, and Blue Values.
- Step 3: Convert each pixel number in to ASCII character.
- Step 4: Convert each pixel number in to ASCII character until last pixel is reached.
- Step 5: Combine all the character which is converted pixel value to ASCII character (Result of step 3), save it in a text file.

The following table shows various performance metrics such as the peak- signal- noise- ratio, Mean Square Error, were calculated for the two inputted image and compared with the existing method [11]. It comprises of the LSB, DCT, DWT technique and their comparative analysis. This value is compared with our proposed method.



Figure 1: Input Baboon



Figure 2: Embedded Output Image



Figure 3: Input Jet



Figure 4: Embedded Output Image

In the above indicated figures, figure (1,3) shows the input image , and figure (2,4) shows the image with embedded text using the proposed method. The performance of the proposed method is compared with existing methods in terms of PSNR and MSE values. The results are tabulated and plotted, in the following tables 3, 4.

Input Image	PSNR value of Existing Technique			PSNR value of Proposed Technique
	LSB	DCT	DWT	
Baboon	53.7558	58.3766	44.96	68.3959
Jet	52.7869	55.6473	44.76	67.6352

Table 3. Comparison of PSNR value between Existing method and proposed Technique.

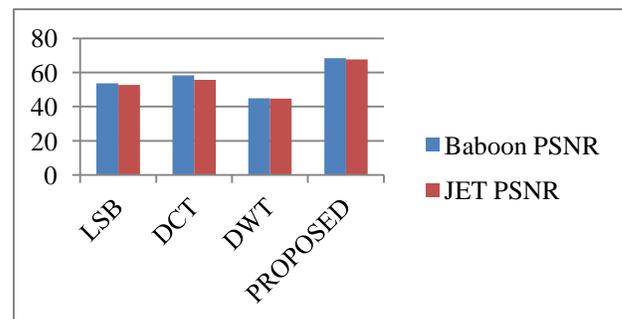


Figure 5: Comparison of PSNR Value of Baboon and Jet Image between Existing and Proposed Technique

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Table 4. Comparison of MSE value between Existing method and proposed Technique.

Input Image	MSE value of Existing Technique			Proposed Technique
	LSB	DCT	DWT	
Baboon	0.5232	0.3074	1.4401	0.0941
Jet	0.5850	0.4208	1.4741	0.1121

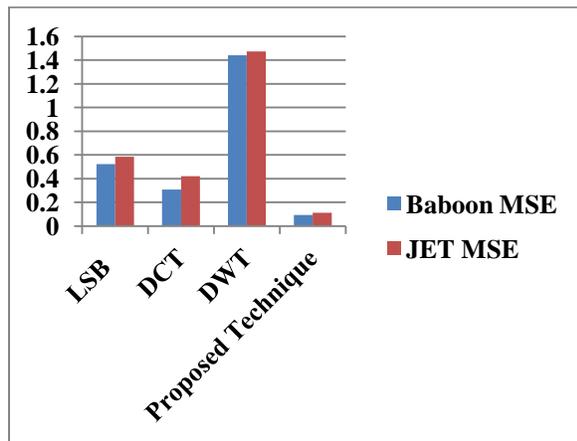


Figure 6: Comparison of MSE Value of Baboon and Jet Image between existing and Proposed Technique

5. CONCLUSION

In this paper, the authors proposed a novel method for image steganography. It employs an effective substitution technique. The secret message is being hidden in even numbered pixels of the cover image. The Proposed method is very simple and robust. It increases the embedding capacity as well as PSNR value. The quality of the image is not affected in any way, as it uses only even numbered pixels. The proposed technique is implemented with C# coding in .NET. The PSNR and MSE value of the image quality is measured with Mat Lab coding. Performance of the proposed technique is compared with LSB, DCT and DWT techniques and found to be encouraging. Sample images are subjected to the proposed technique and the results are tabulated and plotted. It proves to be a secure method since only the even numbered pixels in bit block are changed. It secures the hidden messages are against unauthorized access

References

[1] Anil Kumar and Rohini Sharma, "A Secure Image Steganography based on RSA Algorithm and Hash – LSB Technique", in *International Journal of Advanced Research in*

Computer Science and Software Engineering, Volume 3, Issue7, July 2013, pp.- 363 – 372.

[2] Arvind Kumar and KM.Pooja, "Steganography – A data Hiding Technique", in *International Journal of computer Applications*, Volume 9, Issue 7, November 2010, pp.-19-23.

[3] Battacharya, T. N. Dey and S.R.B. Chauduri, "a session based multiple image hiding technique using DWT and DCT", *International Journal of Computer Applications*, vol- 38, 2012, pp-18-21.

[4] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Significant Bit Algorithm", in *International Journal of Engineering Research and Applications*, Vol. 2, Issue 3, May-Jun 2012, pp. 338-341.

[5] Lisa M. Marvel, and Charles T. Retter, "The Use of Side Information in Image Steganography," in *Proceedings of IEEE International Symposium on Information Theory and Its Applications*, Honolulu, Hawaii, USA, November 5-8, 2000.

[6] Mamta Juneja, and Dr. Parvinder S. Sandhu, "An Improved LSB based Steganography Technique for RGB Color Images", in *2nd International Conference on Latest Computational Technologies (ICLCT'2013)* June 17-18, 2013 London (UK), pp.-10-14.

[7] Neil F. Johnson, and Sushil Jajodia, "Exploring Steganography, Seeing the Unseen," in *IEEE Computer Magazine*, pp. 26-34, February 1998.

[8] P. Nithyanandam, T. Ravichandran, N. M.Santron, E. Priyadarshini, "A Spatial Domain Image Steganography Technique Based on Matrix Embedding and Huffman Encoding", *International Journal of Computer Science and Security (IJCSS)*, Vol. 5, Issue No. 5, 2011.

[9] Prabakaran Ganesan and R.Bhavani, "A High Secure and Robust Image Steganography Using Dual Wavelet And Blending Model", in *Journal of Computer Science*, Vol 9, Issue 3, 2013, pp.-277-284.

[10] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay, sugata sanyal, "Steganography and Steganalysis: Different Approaches".

[11] Stuti Goel, Arun Rana, Manpreet Kaur, "A Review of Comparison Techniques of Image Steganography", in *IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)* Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48.