International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

An Efficient Sequential Data Embedded Image Steganographic Approach

P. Jothimani, A. Nagarajan

Department of Computer Applications, Alagappa University, Karaikudi, Tamil Nadu, India

ABSTRACT

Steganography, the art of hiding the data from human perception. The usages have been increased more in the present decade. Many techniques and algorithms were evolved to improvise the process. It concerns more about the secure transmission of the data in the communication spectrum. The data may be in any format such as the text, image, audio and even video files. Steganography more deeply uses the image as a medium to cover the original information. In the proposed method, uses the modified form of Least Significant Bit (LSB) insertion technique. The original text file is first converted into binary form. The cover image is converting regarding the input data's corresponding pixel arrangement. The replacement takes place in such a way that, one pixel value will be modified and replaced in every block. As a result, the intruder cannot find out the changes taken place within the image. This method uses the LSB technique in a modified way with pixel replacement. The experimental results show that the proposed method remains secure and also, fast to process.

Keywords: Insertion Technique, Communication Network, Steganography, Digital Image.

I. INTRODUCTION

A cryptographic algorithm with all possible keys and protocols is known as a cryptosystem. Each security system must supply some security process that guarantees the secrecy of the system. Some of the goals that can be achieved by cryptography are as follows: Authentication, Confidentiality, Access Control, Integrity, Non-repudiation, Availability and Accountability. In the cryptographic process encryption and decryption demands a key. Some cryptosystems uses the same key together for encryption and decryption called as symmetric key or private key cryptography and asymmetric key or public key cryptography may use different keys together [4].

Steganography and Cryptography are two important methods to transmit secret information in a secured way. Digital technology in communication has become a crucial part of any infrastructure in which many applications were developed on the basis of Internet and it is desired that the communication be made secrecy [16]. Steganography covers the original data within the stego medium, which is in the form of an image. It hides the data within the image. Hence, it states that unauthorized entity cannot reveal the original information what is embedded inside the image.

Data hidden covered image is send to the receiver side. An intended receiver can retrieve the secret information by using extraction algorithm and key which is given by the sender. Steganography is the art and science of technique which is utilized to send out a secret message from a dispatcher to a recipient in which potential impostor does not suspect the subsistence of the secret message. This can be done through the way of embedding the secret message within another cover medium such as text, image, audio or video. [1]. The word Steganography is from Greek origin and it defines concealed writing" steganos meaning "covered or protected", and graphie meaning "writing" [6].

Steganography acts as a solution which makes it possible to send information without the fear of the messages being intercepted and mapped out. It can be paired with existing communication methods, and it

can be improvised to carry out hidden exchanges. The haulage of sensitive data is another key use of steganography. The paper is constructed as follows. Section 2 comprises of related arenas to the proposed technique. Section 3 consists of the existing methods and the proposed methodology to be implemented. Section 4 comprises of the experimental results and their scope. Section 5 followed by the conclusion of the proposed technique.

II. Literature Survey

Masud et al. [8] has been suggested improvisation of LSB method for color image to improve the security level of secret information. Mohmmad A.Ahmed et al. [9] has been proposed LSB method using MD5 technique in which with the help of MD5 , a cover image is passing to hash function to obtained hashing value.

Soumyendu Das et al. [13] have suggested various methods on steganography which is focusing the secure of secrecy information. They implement the proposed method using multimedia file and Network IP datagram as cover media. Existing method produced stego output which is less or more susceptible to various attacks media formatting and compression. In this way, they clear that proposed method is not vulnerable to various attacks.

Sachdeva S et al. [11] used Vector Quantization table for embed the original information and also improving the size of capacity and stego. Mandal, J.K et al. [7] has been implemented minimum deviation of fidelity method on the basis of data hiding technique. Hemalatha et.al [3] has made comparison on color image in both RGB and YCbCr domains. From the comparison of PSNR values, it is clear that the resultant stego image quality in RGB domain is good than YCbCr.

Bhavana et.al,[2] has been designed algorithm using LSB with Chaos theory concepts and promotes security as well as keep the secret information in secure way. Moreover, performance of proposed method has been analyzed and PSNR values also computed. Shilpa et.al.[12] has been analyzed the existing LSB algorithm and determined excess of distortion and so author enhanced the LSB (ELSB) algorithm for image. In this enhanced method, secret message is embedded in blue color of the cover image. This way performance of enhanced method has been improvised and obtained the less amount of distortion.

The proposed method of Prabakaran et al. [10] has described the image steganography using the Dual Wavelet and Blending Model. This method helps to hiding the size 256×256 of gray level secret image inside the size 512×512 of gray level carrier image with various combinations of DWT and IWT. Moreover, pixel values of original image have been scrambled takes place with the help of Arnold transform. This robust method proves the high level of security for secret image sharing.

Juan José Roque et al.[5] have been enhanced the LSB algorithm naming SLSB which is the terms of Selected Least Significant Bits. This improved version of algorithm is basis on spatial domain and it process LSBs of one of pixel components in image and changing them regarding the secret information bits to embed.

III. Proposed Work and Methodology

Today it has turned into an approach to transmit interactive multimedia information by means of the all-pervasive Internet. By means of the imminent electronic trade, it has ended up amazingly vital to handle the delicate issue of bearing information security, particularly in the perpetually zooming open system upbringing of the present day generation[15]. This Section briefly discusses the various steganographic methods and techniques used, various algorithms used to hide the data and the proposed technique with the experimental results.

IV. Types of Steganography

Steganography using different kinds of media as the cover object as well as for the retrieval of the stego object. Some of them are the text, Image file, Audio file, Video File and the IP protocol. The text file uses the digital files that do not contain the redundant data. Audio and Video Steganography is more complex to use. Generally Image Steganography is used for hiding the secret data. It remains as the most secure way to transfer the data over the communication network.

Because the intensity of image changes by 1 or 0, after the process have taken place. This image Steganography technique can be used and applied to the bitmap file images and the JPEG images. In JPEG format files, each pixel is coded using the Discrete Cosine Transformation function (DCT).

3.2 Steganographic Methods

In the Least Significant Bit Encoding the sampling technique is followed by the quantization methods. Before converting the digital data will be modified to the binary sequential format. The Human Perception does not recognize the Noise of the phase coding at the audio signals. The phase coding Steganography uses for this method. This technique encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of Peak - signal-to- noise ratio.

The next approach of Steganography, that hides the data in network datagram, is the protocol method. The main aim of this novel method is to make the stego object undetectable by the network watchers. The information is placed in the IP header of the datagram. In this method information to be conceal is located in the IP header of a TCP/IP datagram.

3.3 Least Significant Bit (LSB) Technique

LSB is the one of the classical and efficient steganography method; it is also called as substitution method. The process of this method is to cover media LSB pixel values are substituted. It is a simple way to hide the secret data inside the cover image. LSB insertion technique changing regarding the no. of bits in image.

For 24-bit image, Red Green Blue component of image would be change. In this basic approach, bits of secret data embed in least significant bits of the cover image which is not revealed easily by potential intruders.

3.4 Proposed Technique

The proposed method is developed with the least significant Bit substitution technique in a modified way. The following algorithm clearly states how the embedding will be taking place to make the message more secure.

3.4.1 Insertion Algorithm

Step 1: Read the text message that has to be embedded.
Step 2: Convert the given text message to the corresponding binary sequence.
Step 3: Choose the cover image in which the secret data to be hidden.
Step 4: Find the Red, Green, Blue components of the image along with the pixel arrangement.
Step 5: Find two LSBs of each Red, Green and Blue pixel from carrier image.
Step 6: Apply a function on the LSB of the carrier image to obtain the position in such a way that, in the first block the least two Red pixel value is substituted with the first two bits of corresponding binary sequence.
Step 7: In the second block, the two bits of Green pixel are replaced with next two bits of the original text message.
Step 8: Finally, the blue components of the next block are replaced with a sequence of binary value.
Step 9: Iterate the process to insert two bits sequentially with every RGB component until the final pixel is inserted.
Step 10: Transfer the stego image obtained as a result of the above steps over the transmission medium.

3.4.2 Retrieval Algorithm

Step 1: Retrieve a stego image as an input.
Step 2: Find two LSB bits of each Red Green Blue pixel from the input stego image individually for each block.
Step 3: Apply a reverse function on the LSB to obtain the position of LSB's with hidden data.
Step 4: With help of these obtained positions, recollect the bits in order of two bits respectively.
Step 5: Finally, the original information will be retrieved.

V. Experimental Results

Our proposed approach has been validated by experimenting with variations of the images. The proposed system has been implemented in Visual Studio 2010, with .NET Framework Version 4.0 using the language of C# windows application.

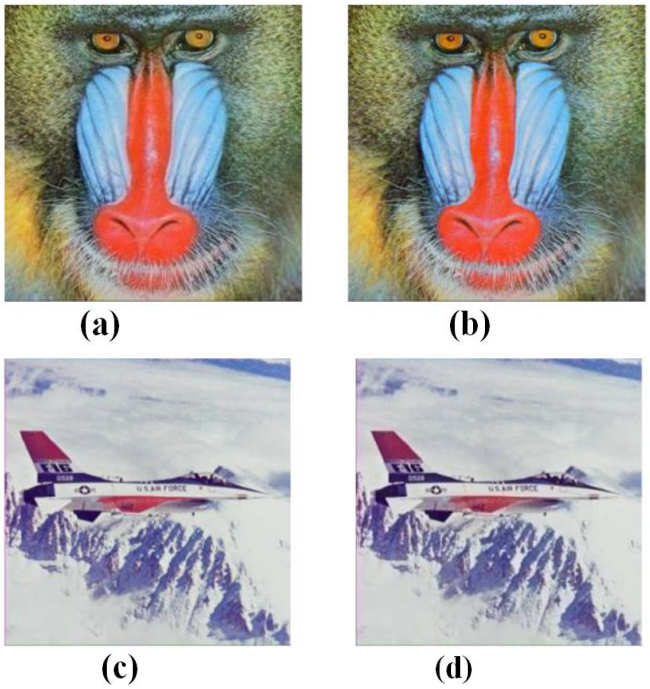

Figure 3: Sample Baboon and Jet Input and Stego Image results

In the above-indicated figures, figure (3) shows the input image Baboon (a), Jet (c), and embedded image Baboon (b), Jet (d), shows the image with embedded text using the proposed method.

4.1. Performance Evaluation

The performance values the PSNR calculated from the output image is compared with the PSNR values provided in the existing techniques, in the following tables 1.

Input Image	LSB	DCT	DWT	Proposed Technique
Baboon	53.7558	58.3766	44.96	58.6673
Jet	52.7869	55.6473	44.76	53.9519

Table 1. Comparison of PSNR value between Existing method and proposed Technique

4.2 Comparative Analysis

The following chart shows various performance metrics such as the peak signal to noise ratio, were calculated for the two input image and compared with the existing method [14]. It comprises of the LSB, DCT, DWT technique and their comparative analysis. This value is compared with our proposed method.

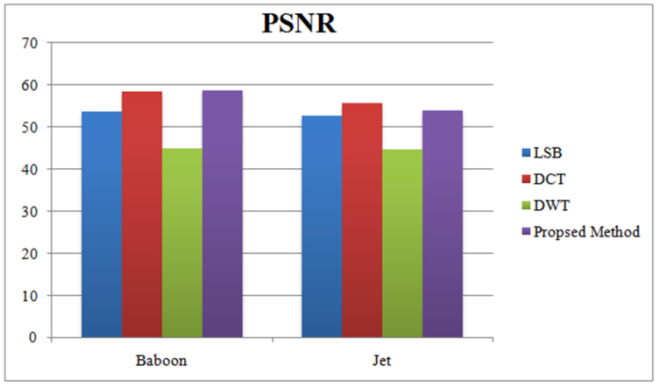

Chart 1 – PSNR Value of Baboon Image between existing and Proposed Technique

VI.CONCLUSION

To secure the image secrecy, a Modified form of LSB method has been proposed and well implemented. By the experimental results, we conclude that by using this proposed technique, there will be no major changes have been accomplished on the image, and it remains efficient. By replacing at least number of pixels, less variation is created in the cover image, which cannot find out by human visual perception. A specified enhanced embedded method made a secure and fast to transfer the information over any unsecure channel or internet. The performance of developed method has been analyzed and also made comparison on simple LSB method with proposed method in which obtained very good metric value for the stego image.

VII. REFERENCES

[1]. Ankit Chaudhary, J. Vasavada, J. L. Raheja, S. Kumar, M. Sharma, "A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images", in 22nd International Conference on Computer Graphics and Vision, 2012.

[2]. Bhavana.S, and K.L.Sudha, "Text Steganography Using Lsb Insertion Method Along With Chaos Theory".

[3]. Hemalatha S, U Dinesh Acharya, Renuka A, "Comparison Of Secure And High Capacity Color Image Steganography Techniques In Rgb And Ycbcr Domains", in International Journal of Advanced Information Technology (IJAIT) Vol. 3, No. 3, June 2013.

[4]. Shankar, K., and P. Eswaran. "An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm", Artificial Intelligence and

Evolutionary Computations in Engineering Systems. Springer India, 2016. 705-714.
[5]. Juan José Roque, Jesús María Minguet, "SLSB: Improving the Steganographic Algorithm LSB".
[6]. Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, "Hash Based Least Significant Bit Technique for Video Steganography (HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.
[7]. Mandal, J.K., Sengupta, M., (2011), "Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF).", Proceedings of Second International Conference on Emerging Applications of Information Technology, IEEE Conference Publications, pp 298 – 301.
[8]. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key", International Conference on omputer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.
[9]. Mohammad A. Ahmad, Dr. Imad Alshaikhli, Sondos O. Alhussainan, "Achieving Security for Images by LSB and MD5", Journal of Advanced Computer Science and Technology Research, Vol. 2, Issue No.3, Pages No. 127-139, Sept., 2012.
[10]. Prabakaran Ganesan and R. Bhavani, "A High Secure And Robust Image Steganography Using Dual Wavelet And Blending Model", in International Journal of computer Science, Vol 9, Issue 3, pp:277-284.
[11]. Sachdeva, S and Kumar, A., (2012), "Color Image Steganography Based on Modified Quantization Table., Proceedings of Second International Conference on Advanced Computing & Communication Technologies , IEEE Conference Publications, pp 309 – 313.
[12]. Shilpa Gupta, Geeta Gujral, and Neha Aggarwal, "Enhanced Least Significant Bit algorithm For Image Steganography", in International Journal of Computational Engineering & Management, Vol. 15 Issue 4, pp:- 40- 42, July 2012
[13]. Soumyendu Das,Subhendu Das, Bijoy Bandyopadhyay, sugata sanyal, "Steganography and Steganalysis: Different Approaches".
[14]. 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.
[15]. Shankar, K., and P. Eswaran. "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique", Journal of Circuits, Systems and Computers 25.11 (2016): 1650138.
[16]. József LENTI, "Steganographic Methods", in Periodica Polytechnica Ser. El. Eng. Vol. 44, No. 3–4, Pp. 249–258,2000.