Scientific Journal of Impact Factor (SJIF): 3.134

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 2, February -2016

Hiding Text Messages into Images using Adaptive Least Significant Approach

ROHIT KUMAR JAIN[1], Dr. RAHUL MALHOTRA[2], KULBUSHAN RASSEWATT[3]

[1]*M.Tech Student,* [2]*Director/Principal,* [3]*Assistant Professor (ECE)*
Guru Teg Bahadur Khalsa Institute of Engineering & Technology, Chhapianwali, Malout

Abstract: *In today's era of technology, digital images are used as a medium to transfer the data from one place to another place. This data can be a simple text as well as a complex multimedia file. While transferring the data with these digital images security must be main concern of the authors thus various data hiding algorithms which are also known as steganography techniques has been invented by the various researchers. In this paper, we have proposed a new technique based on least significant bit (LSB) of pixels of image. This technique is named as Adaptive Least Significant Bit technique in which data is text data is hidden into an image based on Fibonacci number. The proposed system is tested on various input images and results are obtained very well than that of existing techniques. Proposed system is also compared with the existing system on the basis of PSNR and accuracy of the system.*

Keywords: Information Hiding, Adaptive Least Significant Bit technique, Stegnography, Information Security.

I. INTRODUCTION

Digital steganography is the art and science of hiding communications; a steganographic system thus embeds secret data in public cover media so as not to arouse an eavesdropper's suspicion. A steganographic system has two main aspects: steganographic capacity and imperceptibility. However, these two characteristics are at odds with each other. Furthermore, it is quite difficult to increase the steganographic capacity and simultaneously maintain the imperceptibility of a steganographic system. Additionally, there are still very limited methods of steganography to be used with communication protocols, which represent unconventional but promising steganography mediums. Digital image steganography, as a method of secret communication, aims to convey a large amount of secret data, relatively to the size of cover image, between communicating parties. Additionally, it aims to avoid the suspicion of non-communicating parties to this kind of communication. Thus, this research addresses and proposes some methods to improve these fundamental aspects of digital image steganography. Hence, some characteristics and properties of digital images have been employed to increase the steganographic capacity and enhance the stego image quality (imperceptibility). This chapter provides a general introduction to the research by first explaining the research background. Then, the main motivations of this study and the research problem are defined and discussed. Next, the research aim is identified based on the established definition of the research problem and motivations.

Steganography and Cryptography

Cryptography and steganography achieve separate goals. Cryptography conceals only the meaning or contents of a secret message from an eavesdropper. However, steganography conceals even the existence of this message (Lou and Liu, 2002). Furthermore, steganography provides more confidentiality and information security than cryptography since it conceals the mere existence of secret message rather than only protecting the message contents. Therefore, one of the major weaknesses of cryptosystems is that even though the message has been encrypted, it still exists.

Even though both cryptographic and steganographic systems provide secret communications, they have different definitions in terms of system breaking. A cryptographic system is considered broken if an attacker can read the secret message. However, a steganographic system is considered broken if an attacker can detect the existence or read the contents of the hidden message. Moreover, a steganographic system will be considered to have failed if an attacker suspects a specific file or steganography method even without decoding the message. As a result, this consideration makes steganographic systems more fragile than cryptography systems in terms of system failure. Additionally, steganographic systems must avoid all kinds of suspicion in order to achieve security and not be considered failed systems. Since steganography adds an extra layer of protection to cryptography, combining steganography and encryption gives the ultimate in private communication. Therefore, the purpose of steganography is to complement cryptography and to avoid raising the suspicion of system attackers but not to replace cryptography.

Stegnography and Watermarking

Stegnography aims to hide the very existence of communication by embedding messages within other cover objects. However, watermarking aims to protect the rights of the owners of digital media such as images, music, video and software. Even if people copy or make minor modification to the watermarked file, the owner can still prove it is his or her file. Thus, both of stegnography and watermarking are forms of data hiding and share some common characteristics. Nevertheless, the goal of stegnography is the embedded message while the goal of watermarking is the cover object itself. Watermarking is a data hiding technique that protects digital documents, files, or images against removal of copyright information. Even if someone knows that a watermark is exist (i.e. visible watermarking) in a given object, it should be impossible to remove the watermark from the watermarked object without causing a distortion or destroying the original (watermarked) object. This

aspect or feature of watermarking is known as "robustness". According to the kind of embedded information, two techniques of document marking can be distinguished: watermarking and fingerprinting. Watermarking is the process of embedding a specific copyright mark into digital documents in the same way. On the other hand, in order to detect any break of licensing agreement, a serial number is embedded in every copy of this digital document. This process is known as "fingerprinting". Even if these markings are detected, it should be practically impossible to remove them.

II. LITERATURE SURVEY

K.Thangadurai and G.Sudha Devi (2014) Steganography refers to information or a file that has been concealed inside a digital picture, video or audio file. If a person views the object in which the information is hidden inside, he or she will have no indication that there is any hidden information. So the person will not try to decrypt the information. Steganography can be divided into Text Steganography, Image Steganography, Audio/Video Steganography. Image Steganography is one of the common methods used for hiding the information in the cover image. LSB is very efficient algorithm used to embed the information in a cover file. This paper presents the detail knowledge about the LSB based image steganography and its applications to various file formats. In this paper we also analyze the available image based steganography along with cryptography technique to achieve security.

Gurpreet Kaur and Kamaljeet Kaur (2013) In this paper author uses Least Significant Bit (LSB) Insertion, in which each 8-bit pixel's least significant bit is overwritten with a bit from the watermark. Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times. Authors do not test the proposed system on different types of images which is concluded as the future work.

Amit Singh et. al (2013) In this paper new algorithm proposed for digital watermarking using Least Significant Bit (LSB) .LSB already used but there is a slightly effect on the image. The above algorithm is using LSB & second LSB bit. Here they used binary value of watermark text in LSB, and in place of second LSB, the inverse of their corresponding LSB bit. The proposed algorithm is flexible depending on the length of watermark text. In this paper they compare their proposed algorithm with simple LSB method and other method, for example DCT & DWT.

Jayashri Deb Sinha and Subhabrata Barman (2012) This paper gives a brief idea about wireless sensor networks and energy efficient routing in wireless sensor networks. Sensor networks are deployed in an ad hoc fashion, with individual nodes remaining largely inactive for long periods of time, but then becoming suddenly active when something is detected. Sensor Networks are generally battery constrained. They are prone to failure, and therefore the sensor network topology changes frequently. In this paper, we propose a routing algorithm for Wireless Sensor Networks combining Energy Efficient and Hierarchical based routing techniques which minimize the energy consumption, increase the lifetime of the sensor nodes and saves battery power.

III. PROPOSED METHODOLOGY

The Proposed research aims to develop an improved steganography approach which is Adaptive LSB Method for color images with higher imperceptibility/quality, large capacity/payload and better in robustness/resistance to attacks. Text messages can be hide within the images using sequential and random methods. It will incorporate cryptography to achieve high security and random pixel embedding to attain high immunity to attacks. It would be highly immune to any environmental disturbances like noise due to hybrid filtering.

The proposed system comprises of two components:

1. Embedding Module
2. Extracting Module.

Embedding Module

Embedding is the process of hiding the embedded message generating the stego image. Hiding information may require a Stego key which is additional secret information, such as password, required for embedding the information.

Algorithm steps for embedding module are as below:

Step1: Input the input image.

Step 2: Input the text messages to hide.

Step 3: Covert the input message into binary format.

Step 4: Generate the Fibonacci number for the message obtained from step 3.

Step 5: if number % 3= 0 then XOR message 1^{st} bit to Red Color 2^{nd} bit to Green Color and 3^{rd} bit to blue color of Image pixel.

If number %3 = 1 then XOR message 1^{st} bit to Green color, 2^{nd} bit to Blue color and 3^{rd} bit to Red color of Image pixel.

If number %3 = 2 then XOR message 1^{st} bit to Blue color, 2^{nd} bit to Red color and 3^{rd} bit to Green Color of Image pixel.

Step 6: Go to next pixel of the image and go to next bit of the message.

Step 7: Repeat steps 5 and 6 until all bits of the message are embedded into Image.

Step 8: End.

Extracting Module

Extracting is the process of getting the embedded message from the stego image.

Algorithm steps for extraction module are as below:
Step 1: Input the stegano image.
Step 2: Generate the Fibonacci number for the message obtained from step 3
Step 3: if number % 3= 0 then extract LSB from1st bit from Red Color, 2nd bit from Green Color and 3rd bit from blue color of Image pixel and add it to the message.
If number %3 = 1 then extract LSB from 1st bit from Green color, 2nd bit from Blue color and 3rd bit from Red color of Image pixel and add it to the message.
If number %3 = 2 then extract LSB from 1st bit from Blue color, 2nd bit from Red color and 3rd bit from Green Color Blue Color of Image pixel and add it to the message.
Step 4: Go to next pixel of the image .
Step 7: Repeat steps 5 and 6 until all pixels of the stegano image are processed.
Step 8: Convert the binary message into text message.
Step 9: Display the message to the user.
Step 10: End

IV. RESULTS & DISCUSSION

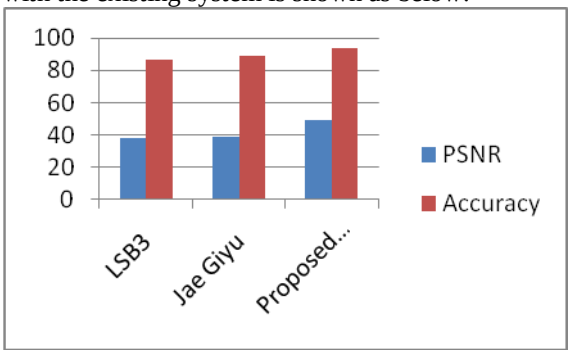
We have conducted several experiments to examine the effectiveness of proposed algorithm. We choose the cover image of buildings, people and vehicles and images to hide as logo images and various text. All the images are of different sizes and taken from real world data. Proposed system is tested on more than 50 images with different watermarks for data hiding. System is giving 94% accurate results.
The following table shows the statistics of the proposed system:

Parameter	Value
Total Images Tested	50
Text Messages	25

PSNR (Peak Signal to Noise Ratio) of the obtained stego-image can be computed by
PSNR worst =20 × log10 (255/MSE) dB (3.1)
The results are then compared with various steganography methods as shown in the following table. In current work more pixel values is change because the simple LSB replacement depends upon size of image. Comparative study of previous method and adaptive LSB substitution method is shown below:

Input Image	LSB3	Proposed System
PSNR	37.92	49.32

Comparison of the proposed system with the existing system is shown as below:



V. CONCLUSION AND FUTURE SCOPE

There are several types of algorithms for stegnography. Each type of algorithms has its own advantages and limitations. No method can provide fully perfect solution. Each type of solution has robustness to some type of attacks but is less resilient to some other types of attacks. Main focus of the current research in this field is to make the stegnography algorithms resilient to geometric transformations. In case of practical application, choice of solution type actually depends on the nature of application and requirements. The proposed method uses Modified LSB Method to optimize the strength of steganographic process. The imperceptibility and robustness of proposed method shows better performance in comparison to other approaches in practice. Accuracy of the system evaluated to be 94% which shows considerably good improvement over the existing approaches.

FUTURE SCOPE

Proposed system can embed the steganograph such as Text in the image of any format. We proposed two algorithms, one for embedding the stegano image into a cover image and second for decoding the message from the encoded image. Proposed system shows good results But it has one major limitation which is system cannot embed the image message larger than the image in which message to hide. Further the proposed system can also be extended to embed watermark in the video file.

References

[1]. K.Thangadurai and G.Sudha Devi, (2014), "An analysis of LSB Based Image stegnography", International Conference on Computer Communication and Informatics, IEEE.

[2]. Gurpreet Kaur, Kamaljeet Kaur , "Image Watermarking Using LSB (Least Significant Bit)"International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.

[3]Amit Singh, Susheel Jain, Anurag Jain, "Digital watermarking method using replacement of second Least significant Bit(LSB) with inverse of LSB", International Journal of Emerging Technology and Advanced Engineering, Vol. 3, Issue 2, February 2013,pp. 121-124.

[4] Lahouari Ghouti, Ahmed Bouridane, Mohammad K. Ibrahim, and Said Boussakta, "Digital Image Watermarking Using Balanced Multiwavelets" IEEE Transactions on Signal Processing, Vol.54, No.4, April 2006.

[5]Pratap Chandra Mandal, "Modern Steganographic technique: A Survey", Vol. 3 No. 9 Sept., 2012, pp. 444 – 448.

[6] H. B. Kekre, Dhirendra Mishra ,Rhea Khanna, Sakshi Khanna & Aadil Hussaini , " Comparison between the basic LSB Replacement Technique and Increased Capacity of Information Hiding in LSB's Method for Images", International Journal of Computer Applications, Vol.45, No.1, May 2012, pp. 33-38.

[7] Komal Patel, Sumit Utareja, Hitesh Gupta, " Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm", International Journal of Computer Applications, Vol. 63, No.13, February 2013,pp. 24-28.

[8] Deepesh Rawat, Vijaya Bhandari, "Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method", International Journal of Computer Applications ,Vol67,No.1, April 2013.

[9] Mr. Rohit Garg, Mr. Tarun Gulati, "Comparison Of Lsb & Msb Based Steganography In Gray-Scale Images", International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 8, October 2012,pp.1-6.

[10] Prashanti .G, Sandhya Rani.K, Deepthi.S, " LSB and MSB Based Steganography for Embedding Modified DES Encrypted Text", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 8, August 2013.

[11] Ravi kumar, Kavita Choudhary, Nishant Dubey, "An Introduction of Image Steganographic Techniques and Comparison", International Journal of Electronics and Computer Science Engineering, Vol.1, No. 3, pp.1000-1005.

[12] Gopika V Mane, G.G. Chiddarwar, "Video Watermarking Techniques", International Conference on Computational Intelligence and Computing Research, IEEE, 2013.

[13] Yonghong Chen, Jiancong Chen, "Digital Image Watermarking Based on Mixed Error Correcting Code" *Journal of Information Security*, 2012,pp. 156-161.

[14] Prabhishek Singh and R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, Issue 9, March 2013.

[15]Jaishri Guru, Hemant Damecha, "Digital Watermarking Classification: A Survey",International Journal of Computer Science Trends and Technology (IJCST), Vol. 2 Issue 5, Sep-Oct 2014.

[16] Ramanpreet Kaur, Baljit Singh, Ishpreet Singh,"A Comparative Study of Combination of Different Bit Positions In Image Steganography", International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.5, Sep-Oct. 2012 pp-3835-3840 ISSN: 2249-6645

