International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-7)

Research Article

July 2015

Novel LSB Approach for Steganography

Gurwinder Kaur
Student of M.Tech
AIET, Faridkot, India

Navdeep Singh Sethi
Assistant Professor
AIET, Faridkot, India

Harinderpal Singh
Assistant Professor
AIET, Faridkot, India

Abstract-

Steganography is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. This paper purposed an image based steganography that uses Least Significant Bit (LSB) techniques and pseudo random encoding technique on images to enhance the security of the communication.

Keywords -Steganography, LSB, Random-key, Image, secret message, stego-key, cover image, Techniques.

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. .

II. 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. Steganography can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. If it is achieved successfully, the message does not attract attention from eavesdroppers and attackers. The main objectives of steganography are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data. These are the main factors which make it different from other techniques watermarking and cryptography. This paper includes the important steganography methods and the main focus is on the review of steganography in digital images.

III. 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. Images

as well as text messages can be hidden 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.

A. 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.
For example, when a secret message is hidden within a cover image, the resulting product is stego image (stego object).
The main algorithm for the embedded stage can be listed as follow:
1. Input the secret text/image files that to be hidden in the cover image.
2. Select the cover image (JPEG file) from list of stored Image files and the text files.
3. Calculate the size of the secret text.
4. Substitute the secret characters/Image from step 4 to cover image obtained from step 2 randomly as follows
a) Calculate the RGB values for every pixel of the cover image to embed the hidden text
b) Find the minimum value from these three values of Red, Green and Blue.
c) Choose this color to be target color to embed the secret message in it.
d) Embed the message and Repeat step 4 for complete secret message.

B. Extracting Module
Extracting is the process of getting the embedded message from the stego image.
The main algorithm for the embedded stage is as follow:
1. Extraction of secret text message from stego image is carried out from random pixels of cover image
2. For edge areas: Extract data from which has the highest value among the three color Red, Green and Blue.
3. For smooth areas: Extract data from adaptive no. of bits.

IV. RESULTS AND 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 Watermark	25
Image Watermark	25
System Accuracy	94%

Fig:-results of novel LSB approach

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:

Table 2. Comparison of Novel LSB Approach with other techniques

Input Image	**LSB3**	**Jae Giyu**	**Novel LSB**
PSNR	37.92	38.98	49.32
Accuracy	86.52	88.62	94.02

V. CONCLUSION
There are several types of algorithms for steganography. 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 steganography 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 Novel 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.

VI. FUTURE SCOPE

Proposed system can embed the steganograph such as images as well as text in the image of any format. We proposed two algorithms, one for embedding the stego 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 e hide. Further the proposed system can also be extended to embed watermark in the video file.

REFERENCES

[1] Vijay Kumar Sharma, Vishal Shrivastavaa "Steganography Algorithm For Hiding Image In Image By Improved LSB Substitution By Minimize Detection"
[2] Gurpreet Kaur, Kamaljeet Kaur, Image Watermarking Using LSB (Least Significant Bit)
[3] Amit Singh, Susheel Jain, Anurag Jain, Digital watermarking method using replacement of second Least significant Bit(LSB) with inverse of LSB
[4] Nayan K. Dey ,Suman K. Mitra ,Ashish N. Jadhav , Hybrid Scheme for Robust Digital Image Watermarking Using Dirty Paper Trellis Codes
[5] Lahouari Ghouti, Ahmed Bouridane, Mohammad K. Ibrahim, and Said Boussakta, Digital Image Watermarking Using Balanced Multiwavelets
[6] Amir Houmansadr, Shahrokh Ghaemmaghami, A Digital Image Watermarking Scheme Based on Visual Cryptography
[7] Neil F. Johnson2, Zoran Duric1, and Sushil Jajodia2 "Recovery of Watermarks from Distorted Images"
[8] Henri Bruno Razafindradina and Attoumani Mohamed Karim, BLIND AND ROBUST IMAGES WATERMARKING BASED ON WAVELET AND EDGE INSERTION
[9] Prabhishek Singh, R S Chadha, A Survey of Digital Watermarking Techniques, Applications and Attacks
[10] Vinita Gupta, Mr. Atul Barve, A Review on Image Watermarking and Its Techniques
[11] Chan-Il Woo and Seung-Dae Lee, Digital Watermarking for Image Tamper Detection using Block-Wise Technique
[12] Gopika V Mane, G. G. Chiddarwar, Review Paper on Video Watermarking Techniques
[13] Rajat Tiwari, Navneet Kaur, Manpreet Kaur, An Optimization Image Watermarking Technique Using Biogeography Based Optimization
[14] Yonghong Chen, Jiancong Chen, Digital Image Watermarking Based on Mixed Error Correcting Code
[15] Saeed AL-Mansoori and Alavi Kunhu, Robust Watermarking Technique based on DCT to Protect the Ownership of DubaiSat-1 Images against Attacks

