iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VI **Month of publication:** June 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Vol. 2 Issue VI, June 2014
ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

An improved mechanism of secret data hiding in an image and enhanced security by minimized detection

Ms.Deeksha Bharti[#1], Dr. Archana kumar[*2]

[#1]*M.Tech student ,Dept. of CSE ,Delhi Institute of Technology and Management, DCRUST ,Murthal ,Haryana*

[#2]*Associate Prof.,Dept of CSE, Delhi Institute of Technology and Management, DCRUST ,Murthal ,Haryana*

Abstract –Steganography is the art of hiding information and an effort to conceal the existence of the embedded information .In recent years many steganography methods have been challenge by steganalysis. Steganalysis algorithm which detects the stego - message by the static analysis of pixel values [1]. In the proposed method, the secret message is encoded by using vigenere encryption method which guarantees the protection of hidden message. Then hiding the secret text in an image by using first component alteration technique .In this technique, 8 bits of blue components are replaced with secret data bits , then that image can be hidden in cover image in non sequential pixel by using variable hope value power of 2 [2,4,8,16].The Proposed method aim not only to provide improved security and capacity problems of simple LSB method but also the increased visual quality of stegoimage.

Keywords- steganography , vigenere encryption , LSB embedding , extraction , first component alteration technique.

I.INTRODUCTION

Data protection and security of the personal information have become a critical issue in the digital world. Therefore, the demand of having a protected method to transfer the confidential data is dramatically increasing. Steganography is the art of passing information through original files in a manner that the existence of the message is unknown. The term steganography is arrived from Greek word means, "Covered Writing" [1]. In contrast to cryptography which make data unreadable for a third party by implying some encryption methods, steganography emphasize on hiding the existence of message inside another data in such a way that nobody can detect it. In image steganography the image used to camouflage the secret data is called the cover-image while the cover-image with the secret data embedded in it is called the stego-image[3].

II. THE CONVENTIONAL STEGANOGRAPHY AND LIMITATIONS

The Least Significant Bit (LSB) insertion is the most common spatial domain technique, which consecutively replaces the least significant bit of cover image with the message bits. This method exploits the natural weakness of Human Visual System (HVS) in recognizing the slight difference of colours . The LSB method changes some or all the 8th bit of image's data so that the image's alteration is not perceptible for any human eyes. In like manner, when using a colour image the LSB of each of the red, green and blue components can be used. Therefore, the potential capacity for hiding secret data in a colour image is triple of the same image size in the grayscale mode.[4]An immediate concern is to find out best possible attacks to carry out steganalysis, and simultaneously, finding out techniques to strengthen existing steganography techniques against popular attacks like steganalysis.

A. Cryptography

Cryptography encodes information in such a way that nobody can read it, except the person who holds the key. More advanced crypto techniques ensure that the information being transmitted has not been modified in transit. There is some difference in cryptography and steganography, in cryptography the hidden

message is always visible, because information is in plain text form but in steganography hidden message is invisible.

B. Steganalysis

Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes". [1]The goal of steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if
possible, recover the hidden information. The challenge of steganalysis is that:

1. The suspect information stream, such as a signal or a file, may or may not have hidden data encoded into them.
2. The hidden data, if any, may have been encrypted before being inserted into the signal or file.
3. Some of the suspect signal or file may have noise or irrelevant data encoded into them (which can make analysis very time consuming).

III. PARAMETERS IN IMAGE STEGANOGRAPHY

When a large amount of data is embedded into an image the visual specifications of image such as colour and smoothness are altered. Among the methods of steganography, the most common thing is to use images for steganography. This is called image steganography. In this image hiding method, the pixels of images are changed in order to hide the secret data so as not to be visible to users, and the changes applied in the image are not tangible. It is very important to specify how the secret is embedded in the image .There are some essential factors that should be considered in image steganography process [4] :

1) *Capacity* - The capacity parameter in the steganographic methods refers to the maximum number of bits that can be embedded in a particular cover file with a small probability of revealing by an antagonist.

2) *Security* - The security measure denotes the assurance of keeping the secret data unreadable for the adversary when it is extracted by attacks.

3) *Imperceptibility* - Imperceptibility is defined as the degree of changes in the appearance of the cover data whenever the message is embedded. The appearance or format of cover files must remain intact after hiding the secret data.

IV. PROPOSED STEGANOGRAPHY METHOD

In this section , the proposed scheme in which at initial step vigenere encryption is used to encrypt the text message ,then first component alteration technique is used to hide the encrypted message inside an image . In this technique, 8 bits of blue components in a pixel are replaced with secret data bits ,in second step ,then that image can be hidden in cover image in non sequential pixel by using variable hope value power of 2 [2,4,8,16] .[5]

A. Proposed Embedding Process

This phase includes all the activities that must be carried out to hide and protect the secret data inside the cover image. The sender uses some algorithms to encode and then embeds the bit stream into the image.

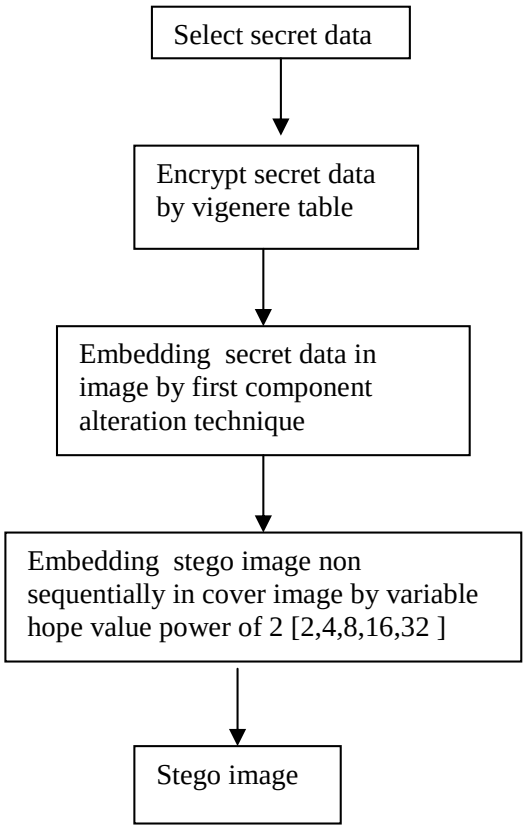


Fig.1 Proposed Embedding Technique

- *Encryption* - In the first step of the embedding phase, the plain text will be encrypted using the Vigenere table . There are several encryption methods that can be applied to encrypt the data, but in this situation, we need a method that does not produce a cipher text longer than the plain text. Furthermore, among the desired encryption methods, Vigenere table, which is a symmetric encryption technique and maps each input character into exactly one character for output, is more secure than similar methods[4]. The biggest advantage of Vigenere table over the other symmetric encryption methods is that based on the specified secret key, it produces different outputs for a certain input character.

- *Embedding* - The embedding algorithm is the most prominent part of the steganographic methods. In fact, it defines which pixels of the image should be changed and also in what order they will be altered with the secret data.

The first component Alteration technique used. In this scheme, the bits of first component (blue component) of pixels of image have been replaced with data bits. Blue channel is selected because a research was conducted by Hecht, which reveals that the visual perception of intensely blue objects is less distinct that the perception of objects of red and green.

For example, suppose one can hide a message in three pixels of an image (24-bit colors). Suppose the original 3 pixels are[3]:

(*00100111* 11101001 11001000) (00100111
1100100011101001)
(11001000 00100111 11101001)

A steganographic program could hide the letter "A" which has a position 65 into ASCII character set and have a binary representation "01000001", by altering the blue channel bits of pixels.

(*01000001* 11101001 11001000) (00100111
1100100011101000)
(11001000 00100111 11101001)

B. *Proposed Extraction Process*

At the receiver site, extraction is done. Another procedure is required to recover the content of message . In extracting algorithm the secret image will be recovered from cover image ,then bits of secret message are obtained by extracting data bits from blue component , finally then decrypt the secret data by using vigenere table ,plain message will be revealed.

V. CONCLUSIONS

In this paper ,several methods are used at every step of algorithm .In encryption step ,vigenere table is used encrypt the data so as to produce cipher text not longer than the plain text .In embedding ,first component alteration technique is used in first layer ,in second layer variable hope value power of 2 is used for hiding non sequentially in cover image. Here we have proposed that the improved algorithm we have introduced will enhance the capacity ,security measures and also minimize the detection .We will implement this algorithm in JAVA or MATLAB .

REFERENCES

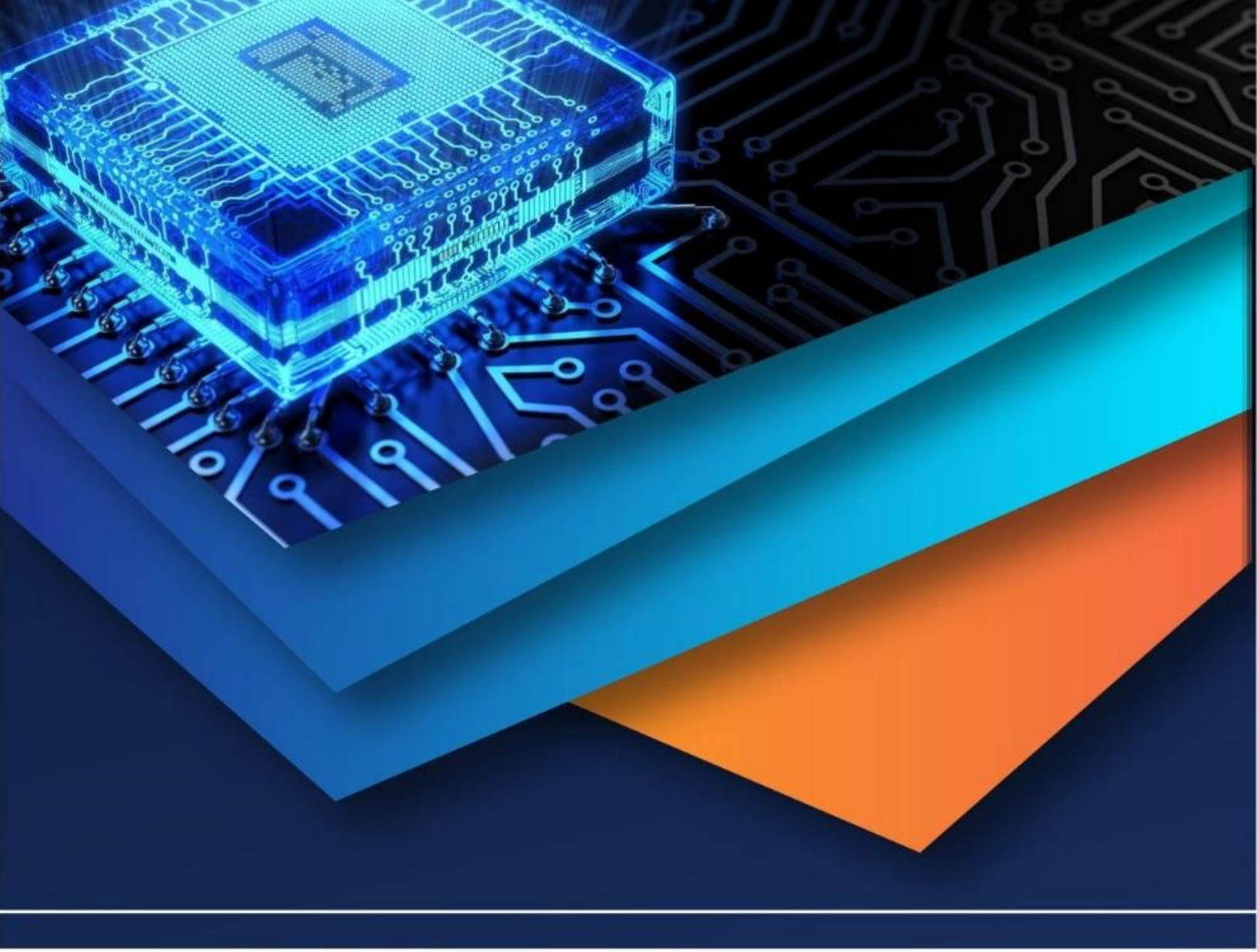
[1] Amanpreet Kaur1, Renu Dhir2, and Geeta Sikka3 .A New Image Steganography Based On First Component Alteration Technique((IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No.3, 2009)

[2] 1Vijay Kumar Sharma ,2Vishal Shrivastava. A Steganography Algorithm For Hiding Image in Image by Improved LSB Substitution by Minimize Detection , Journal of Theoretical and Applied Information Technology (JATIT), 15th February 2012. Vol. 36 No.1

[3] Vipul Sharma ,Sunny Kumar . A New Approach to Hide Text in Images Using Steganography, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 3, Issue 4, April 2013

[4] Morteza Bashardoost 1, Ghazali Bin Sulong 2 and Parisa Gerami, Enhanced LSB Image Steganography Method By Using Knight Tour Algorithm, Vigenere Encryption and LZW Compression, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013.

[5] Mamta.Juneja and Parvinder S. Sandhu, An improved LSB based Steganography with enhanced Security and Embedding/Extraction, 3rd International Conference on Intelligent Computational Systems (ICICS'2013) January 26 27, 2013 Hong Kong (China)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY