IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Analysis and High Security Data Hiding Technique in Encrypted Image

Umesh M. Umate[1], Dr. V.N. Nitnaware[2]

ME, E&TC (Signal Processing), D.Y Patil School of Engineering Academy, Ambi, Pune[1]

Principal DYPSOEA, Ambi, Pune[2]

Abstract: In this paper introduces analysis of previous steganographyand introduction of proposed method, and also how to hide secrete message in carrier image with help of LSB method. In previous days there are lots paper introduces on data hide in a carrier image. Steganography is very old approach to hide data into a some object. Steganography comes from Greek word that means covered or secrete writing; stegan means covered and graphy means writing. In this day there is lots of security thread over internet through carrying some information. There are lots disadvantages while handling this type embedding system like capacity, accuracy and robustness. Transmission of image over the internet is vulnerable to verity attacks from untrustworthy system administrators. So it should be stored and processed in an encrypted format to maintain security and privacy. It is necessary to implement secrete message in these encrypted image. In this paper, We proposing data hiding is to performed by the encryption of a text data using twelve square substitution cipher, and then embed the cipher text in the carrier image depending on plane separation of the image and select any plane R,G,B or all for embed. We will be finding LSB algorithm on the basis of Mean Square Error, Peak Signal to Noise Ratio, Relative Payload and Rate of Embedding. The system is therefore, recommended to be used by the internet users for establishing a more secure communication.

Keywords: encryption; decryption; LSB; steganography; 12 square algorithms.

I. INTRODUCTION

Today's need of computer networks still has many issues in transmitting messages, keeping it secretive from an third party. In these days tremendous transmission over internet therefore security issue occurs in very large manner to overcome these issue steganography is very widely used for it. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. There are different kinds where steganography is used, like text, image and audio/video within innocuous cover carrier, which too are of the same form in a way that secrete information hidden is undetectable. In ancient times the Greek historian Herodotus was the first person to use steganography. There are few more technology which are same as to steganography and these are cryptography, watermarking and fingerprinting. These are essentially used in the field like security and privacy issue over the internet transmission of information. As stated earlier, images are the most popular cover objects used for steganography. In the domain of digitalimages many different image file formats exist, most of them for specific applications. For these different image file formats, different steganography algorithms exist.

Steganography: Image
A- Transform Domain
JPEG

B- Image Domain
LSB in BMP
LSB IN GIF

Above these are different algorithms which are used for image file format, there are also many more algorithms which are used in image steganography. In this paper we are using LSB in BMP. Cryptography was created for secrecy of the text message there are many algorithm for encrypt and decrypt the message. Here we encrypt/decrypt the secrete message using the 12 square substitution cipher algorithm and then embed these secrete message into carrier image file.Cryptography is not sufficient for more security therefor both the cryptography and steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Cryptography alters the message so it cannot be understood; steganography hide that message into image so it cannot be seen

II. ANALYSIS OF EXISTING IMAGE STEGANOGRAPHY METHODS

Usually for hiding any information to carrier image Least Significant Bit (LSB) technique is used. In this method commonly last 8^{th} bit is used for hiding the data [1]. This method works fine in the image carriers because if the least significant bit is changed from 0 to 1 or vice versa, there is hardly any change in the appearance of the color of that pixel. The LSB method usually does not increase the file size, but depending on the size of the information that is to be hidden inside the file, the file can become noticeably distorted.

As a Gandharba Swain and Saroj Kumar Lenka they use LSB to embed the cipher text in the carrier image in 6^{th} and 7^{th} bit locations or 7^{th} and 8^{th} bit locations or 6^{th} and 8^{th}

bit locations of the different pixels (bytes) of the carrier image depending on the value of an index variable[2]. Here the 8th bit means the least significant bit (LSB) location, the 7th bit means the LSB minus one location and the 6th bit means the LSB minus two locations. The index variable value can be 0 or 1 or 2. The index variable value will change from 0 to 1 or 1 to 2 or 2 to 0 after each embedding. The initial value of the index variable depends upon the length of the cipher text. As per the image in image steganography method proposed by P. Mohan Kumar and D. Roopa one can apply block matching procedure to search the highest similarity block for each block of the secret image and embed in LSBs of the carrier image [3]. By Basant Sah and Vijay Kumar Jha they proposed that, first of all find the public key and private key according to RSA approach and encrypt secret information. To provide higher security the secret information is encrypted first and encrypted ASCII value is converted into binary form .encrypt the data and then after replacing the LSB bit and MSB bit with the data. The proposed scheme uses RSA to encrypt secret information [4]. By Mohammed A.F. AlHusainy introduces a very different way of steganography by mapping the pixels of image to English letters and special characters [5]. Color Image Steganography Based on Discrete Wavelet andDiscrete Cosine Transforms from [6], In this paper the color cover image is divided into equally four parts, for each partselect one channel from each part(Red, or Green, or Blue), choosing one of these channel depending on the high color ratio in that part. The chosen part is decomposing into four parts {LL, HL, LH, HH} by using discrete wavelet transform. The hiding image is divided into four part n*n then apply DCT on each part. Finally the four DCT coefficient parts embedding in four high frequency sub-bands {HH} in cover image.By Moh Moh Zan, Nyein Aye are presents atechnique for image steganography based on DWT, where DWT is used to transform the original image (cover image) from spatial domain to frequency domain. The secret message is encrypted using the Blowfish encryption algorithm. This system will modify the LSB technique by putting the encryption step and newinsertion algorithm. Firstly, extract the LSB from each HH, LH and HL. After that, it needs to transform back into octal number and then to hexadecimal format. The output hexadecimal format of cipher text can be decrypted by the Blowfish decryption algorithm process. Contribution of theproposed system is a new insertion method for hiding data in cover image and is more secure than inserting LSB of the image directly into the steganographic system [7].

An Efficient Parallel Algorithm for Secure Data Communication, a novel architecture is presented to provide high processing speed to RSA key generation for embedded platform with limited processing capacity. In order to exploit more data level parallelism as per Boddupalli Srinivasa Rao and M.Ramesh they use Verilog to implement a 16- bit RSA block cipher system. The whole implementation includes three parts: key generation, encryption and decryption process. The key generation stage aims to generate a pair of public key and private key, and then the private key will be distributed to receiver according to certain key distribution schemes. Also they are implementing steganography concept for more securing of data. By using steganography we can hide the data in the image by using LSB (Least Significant Bit) method [8].In paper[9] represented a double layered embedding method for implementing plus minus steganography in which binary covering codes and wet paper codes are used to hide messages in the LSB plane and second LSB plane respectively.An Overview of Image Steganography by T. Morkel, J.H.P. Eloff and M.S.Olivierintends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications [10].
In this paper wedo embed either in 2ndand 4th or both bit locations of the bytes of the image based on the different values of the index variable. Instead of hiding the direct information, we hide the encrypted text. For this we used encryption algorithm called twelve-square substitution cipher. The entire approach is discussed in the following sections. In section-III, the working of the block diagram and related work is discussed, in section-IV the methodology, in section-V the advantages; in section-VI the application, in section-VII the Conclusion.

III. BLOCKDIAGRAM & RELATED WORK

A. Embedding Process

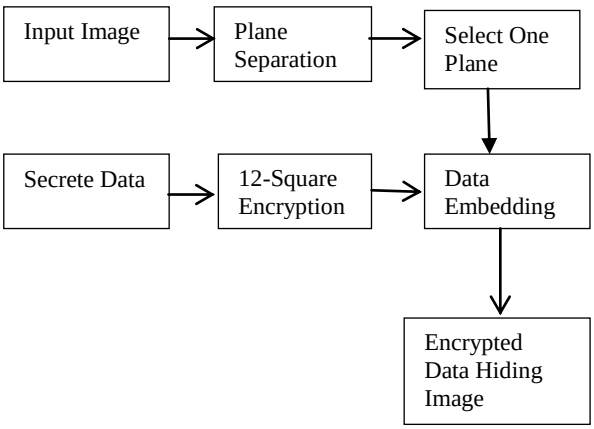

Fig1:- Embedding Process

Above figure shows the embedding process of the Image Steganography. Here we firstly take the BMP image, separate the plane of image in R, G, B form and then select any one plane or the entire three plane for insert text. Our Secrete data are not directly stored in image plane they are firstly encrypt with the help of 12-square algorithm which are detailed explain in section C and then embed in image plane with the help of our embedding process which is LSB method. In this LSB method we are using 2nd and 4th bit LSB for embedding.Finally encrypted data hiding image is sent over transmission for further process.

B. Extraction Process

Above figure shows the extraction process of Image

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

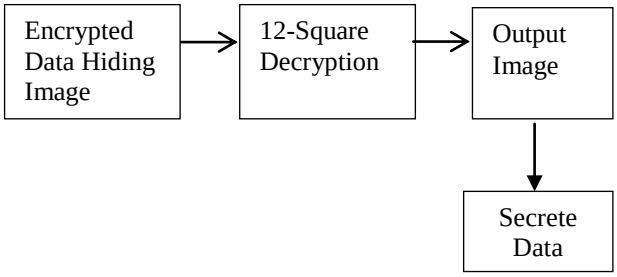

Fig2:- Extraction Process

Steganography. Here we get encrypted data hiding image, using 12 square decryption process extract the image and we get separate secrete message and original image. During this process there is no effect will occur at the time of extraction process?

C. Twelve Square Substitution Method

In this paper, an effective method called twelve square substitution algorithms are used to encrypt the hidden text data in carrier image. Generally in this substitution include alphabets, numbers and special characters. In this twelve square cipher encrypt text therefore we get higher security for hide text. Generally it uses six 5 X 5 matrices each arranged in a square, as shown in table-I. In this 5 X 5 matrices contains the alphabet (excluding "Q" to reduce the alphabet to fit into the square) and another six 6 X 7 matrices arranged in squares for digits and special characters, as shown in table-II. All the special characters and digits from your desktop/laptop keyboard.

TABLE I Plain Text & Cipher Text (Alphabets)

Square 1	Square 2	Square 3
abcd e	f g hi j	k l m n o
f g hi j	k l m n o	p r s tu
k l m n o	pr st u	v w x y z
p rs t u	v w x y z	a b c d e
v w x y z	a b c d e	f g h i j
Square 4	Square 5	Square 6
g m r i t	a b c d e	a b c d e
a b c d e	f h j k l	f h j k l
f h j k l	g m ri t	n o p s u
n o p s u	n o ps u	v w x y z
v w x y z	v w xy z	g m ri t

Arrangement of Table I as follows, square 1 arrange in alphabetical format in 5X5 matrices, In each row 5 alphabets excluding q to arrange it in 25 alphabet. Square 2 is arranging from square 1 by putting 1st row to the last and remaining rowsare one position up. Square 3 is arranging from square 2 by putting 1st row to the last and rows remaining one position up. In square 4 we just arrange by 1st row gmrit and remaining are serial alphabetical arrange by the row. Square 5 is made from square 4 by putting 1st row to 3rd place and above row one position up, remaining rows keep as same position. Square 6 created from square 4 by putting 1st row to the last and remaining rows is one position up. In table II square-7, the Numbers and special characters from a laptop are arranged in 6 rows and 7 columns. Square-8 is created from square-7 by putting the 1st row Square-8 to 6th row place of square 7. Similarly square-9 is made from square-8 by putting the 1st row of square-8 to 6th row place square 9. Square-10 is made from square-7 by arranging the row elements in columns. Square-11 is created from square-10 by putting the 1st row of square-10 to 3rd row in place of square 11. Similarly square-12 is made from square-10 by putting the 1st row into 6th row place.

TABLE II Plain Text and Cipher Text (Numbers & Special Characters)

Square-7	Square-8	Squre-9
0 1 2 3 4 5 6	7 8 9 ` ~ ! @	# $ % ^ & * (
7 8 9 ` ~ ! @	# $ % ^ & * (	) _ - + = { [
# $ % ^ & * (	) _ - + = { [	}] ; : " ' \
) _ - + = { [	}] ; : " ' \	| < , > . ? /
}] ; : " ' \	| < , > . ? /	0 1 2 3 4 5 6
| < , > . ? /	0 1 2 3 4 5 6	7 8 9 ` ~ ! @
Squre-10	Squre-11	Squre-11
0 6 ! & + ; <	1 7 @ * = : ,	1 7 @ * = : ,
1 7 @ * = : ,	2 8 # ({ " >	2 8 # ({ " >
2 8 # ({ " >	0 6 ! & + ; <	3 9 $) [' .
3 9 $) [' .	3 9 $) [' .	4 ` % _ } \ ?
4 ` % _ } \ ?	4 ` % _ } \ ?	5 ~ ^ -] | /
5 ~ ^ -] | /	5 ~ ^ -] | /	0 6 ! & + ; <

For example:-

Secrete message - umesh@5$
Encrypted message – ujzsc, |7

D. LSB (Least Significant Bit)

In this paper, the carrier image is the file in which we will hide the secrete message, which may also be encrypted using the 12 square cipher algo. The resultant file is the stego image (which will be the same as to the carrier image). The carrier image (and thus, the stego image) is typical image. In this paper, I will focus on image files and will, therefore, refer to the carrier image and stego image.Before we going to discuss first see how secrete information is hide in a carrier image, it is worth a fast review of how images are stored in the first place. An image file is simply 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. A 24-bit color scheme, as the term suggests,

uses 24 bits per pixel and provides a much better set of colors. In this situation, each pixel is represented by 3 bytes, each byte representing the intensity of the three primary colors red, green, and blue (RGB), respectively.
Carrier medium + Secrete message (Encrypted by 12 square cipher) = stego image
This is a very simple way to hide the some information in carrier file. In this approach the least significant bits of few or all bytes inside an image is replaced with a bits of the text message. Firstly read the image and convert it into the pixel intensity or separate the plane R,G,B and least bit is replace with data but this method is useful when very less no of data is to be hide. People can't detect because image quality very slightly decrease so this is very useful.

Procedure For Insert Data In Image
A. select image an separate the plane in R, G, B pixel
B. Find the pixel values.
C. Select the pixel on which we want to insert data or select all pixels.
The procedure of selecting pixels is totally depends on users they can choose continuous, alternate or at a fixed distance. We see with the help of one example how hide text in last bit. LSB insertion modifies the LSBs of each color in 24-bit images, or the LSBs of the 8-bit value for 8-bit images.
For Example:-
The letter 'U' has an ASCII code of 65(decimal), which are 10000101 in binary.
It will need three consecutive pixels for a 24-bit image to store a 'U':
Let's see that the pixels before the insertion are:
10110000, 10100010, 11110010, 11000010
11100010, 10111000, 11101000, 1011000
Then value after inserting 'U'
10110001, 10100010, 11110010, 11000010
11100010, 10111001, 11101000, 1011001
(The values in **bold** are the ones that were modified by the transformation)
From these examples we can infer that 1-LSB insertion usually has a 50% chance to change a LSB every 8 bits, thus adding very little noise to the original picture. For 24-bit images the modification can be extended sometimes to the 2nd or even the 4thLSBs without being visible. 8-bit images instead have a much more limited space where to choose colors, so it's usually possible to change only the LSBs without the modification being detectable.

IV. METHODOLOGIES

- Plane Separation of Image
- Secret Data Section
- Convert Encrypted Data using 12 Square Algorithm
- Encrypted Data Hiding in Images using LSB Method
- Reconstruct the Original image
- Parameter Analysis

V. ADVANTAGES

Secrecy: a people should not be able to extract the secrete data from the stego image without the knowledge of the proper secret key used in the extracting procedure.
Imperceptibility: the medium after being embedded with the secrete data should be invisible from the original medium. One should not become suspicious of the existence of the secrete data within the medium.
High capacity: the maximum length of the secrete message can be embedded should be less than cover data.
Resistance: the secrete data should be able to survive when the host medium has been manipulated, for example by some lossy compression scheme.
Accurate extraction: the extraction of the secrete data from the medium should be accurate and reliable.
Flexible system and Better compression ratio.
Less Bandwidth utilization.
Highly secure communication.

VI. APPLICATION

- Multimedia Security
- Defense Field
- Data Communication

VII. CONCLUSION

In this paper, steganography used is derived from Greek word stegos and graphy which means covered and writing. Here we introduces review of the previous paper how they use steganography for hiding the secrete message. And here also shows the small related work about the project. Examples are giving here for the 8 bit LSB in which stored data in last bit location but in our future work we are using 8 bit LSB to store data in the 2nd and 4thbit location. In this paper we mention the way of how to encrypt secrete message using the twelve square algorithms and how to hide the carrier image. Our future work for this paper is implanting with result and proposed method.

REFERENCES

[1] Mohammad Ali Bani Younes and Aman Jantan, "A New Steganography Approach for Image Encryption Exchange by using the LSB insertion", International Journal of Computer Science and Network Security, Vol 8, No 6,2008, pp. 247-254.
[2] Gandharba Swain, Saroj Kumar Lenka, "Steganography Using the Twelve Square Substitution Cipher and an Index Variable", 978-1-4244-8679-3/11/ ©2011 IEEE
[3] P.Mohan Kumar and D.Roopa, "An Image Steganography Framework with Improved Tamper Proofing", Asian Journal of Information Technology, Vol. 6, No.10, 2007.
[4] Basant Sah, Vijay Kumar Jha, "A New Approach to Data hiding using Replacement of LSB and MSB", IJARCSSE, Volume 3, Issue 11, November 2013.
[5] Mohammad A.F. Al-Husainy, "Image Steganography by mapping pixels to letters", Journal of Computer Science, Volume 5, 2009.
[6] A. A. Abdul Latef, "A Color Image Steganography Based on Discrete Wavelet and Discrete Cosine Transforms", IBN AL-HAITHAM J. FOR PURE & APPL. SCI. VOL.24 (3) 2011.
[7] Moh Moh Zan, Nyein Aye, "A Modified High Capacity Image Steganography using Discrete Wavelet Transform", International Journal of Engineering Research & Technology, Vol. 2 Issue 8, August – 2013
[8] Boddupalli.Srinivasa Rao, M.Ramesh, "An Efficient Parallel Algorithm for Secure Data Communication Using RSA Algorithm", IJESC, ISSN2321 3361 © 2015.
[9] Weiming Zhang, Xinpeng Zhang and Shuozhong Wang, "A Double layered Plus-Minus One data Embedding Scheme", IEEE Signal Processing, Volume 14, 2007.
[10] T. Morkel , J.H.P. Eloff , M.S. Olivier, "An Overview Of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa.