ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Implementation of High Security Data Hiding Technique in Encrypted Image

Umesh M. Umate, Dr. V. N. Nitnaware,

M. E Student (Signal Processing), Dept. of E&TC, D.Y Patil School of Engineering Academy, Ambi, Pune, India

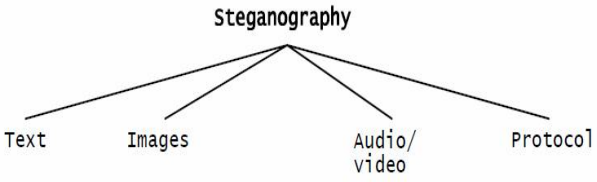
Principal, DYPSOEA, Ambi, Pune, India

ABSTRACT: Now a day's secrecy is most popular issue in over internet. This paper introduces literature review of image steganography and how to hide encrypted message in image using proposed method. Encrypting data has been the most popular problem for protective information but this protection can be broken with enough computational power. Another method to encrypting data would be to hide it by making this information look like something else. In this way only receiver would understand its true content. In particular, if the data is hidden in a carrier image then everyone would view it as a picture. At the same time receiver could still recover the true information. This technique is often called data hiding or steganography. For implementing steganography the images which are collection of pixels should be in a appropriate format. For this purpose image processing is done to convert the required image in appropriate format.
Image processing usually refers to digital image processing. Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or, a set of characteristics or factors related to the image. The basic operations performed on images are contrast enrichment, gray scale conversion, reversing the image etc. We will be verdict 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 founding a more protected communication.

KEYWORDS: encryption; decryption; LSB; steganography; 12 square algorithms

I.INTRODUCTION

Today's requirement of computer networks still has many problems in transmitting messages, keeping it secretive from an third party. In these days incredible transmission over internet therefore security problem occurs in very large manner to overcome these problem steganography is very broadly used for it. Inappropriately it is sometimes not enough to retain the contents of a message secret, it may also be necessary to keep the existence of the message secret. The method 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.
Steganography is the skill and science of imperceptible communication. This is consummate through hiding information in other information, thus hiding the existence of the communicated information. Thus image steganography is a better method than cryptography. Persistence of image processing is to make the quality of an image well so that the required operations can be easily performed on it. Image steganography is performed on the preferred formats which are suitable. Steganography comprises the concealment of information within computer files. In digital steganography, electronic communications may comprise steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are perfect for steganographic transmission because of their

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

large size. As a simple example, a sender might start with an innocuous image file and alter the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not precisely looking for it is unlikely to notice it.
Cryptography was formed 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 implant these secrete message into carrier image file. Cryptography is not enough for more security therefor both the cryptography and steganography are well known and widely used methods that manipulate information in order to cipher or hide their existence respectively. Cryptography modifies the message so it cannot be understood; steganography hide that message into carrier image so it cannot be understood.

II. ANALYSIS OF EXISTING IMAGE STEGANOGRAPHY METHODS

Usually for walloping any information to cover image Least Significant Bit (LSB) technique is used. In this method usually last 8^{th} bit is used for hiding the data [1]. This technique works fine in the image transporters because if the least significant bit is altered from 0 to 1 or vice versa, there is hardly any change in the entrance of the color of that pixel. The LSB method frequently does not increase the file size, but reliant on the size of the information that is to be hidden privileged the file, the file can become noticeably inaccurate.
As a Gandharba Swain and Saroj Kumar Lenka they uses LSB to implant the cipher text in the carrier image in 6^{th} and 7^{th} bit place or 7^{th} and 8^{th} bit place or 6^{th} and 8^{th} bit place of the dissimilar pixels (bytes) of the cover image depending on the value of an index variable[2]. Here the 7^{th} bit means the LSB minus one position and the 6^{th} bit means the LSB minus two positions. The index variable value can be 0 or 1 or 2. The index variable values will variation from 0 to 1 or 1 to 2 or 2 to 0 afterward each embedding. The first value of the index variable is contingent upon the length of the cipher text. As per the image in image steganography technique proposed by P. Mohan Kumar and D. Roopa one can apply block equivalent method to search the highest resemblance block for each block of the secret image and embed in LSBs of the cover image [3]. ByBasantSahand Vijay Kumar Jhathey proposed that, first of all find the public key and private key rendering to RSA approach and encrypt secret information. To deliver higher security the secret information is encoded first and encoded ASCII value is transformed into binary form .encrypt the data and then after substituting the LSB bit and MSB bit with the data. The planned scheme uses RSA to encrypt secret information [4].
By Mohammed A.F. AlHusainy familiarizes a very different way of steganography by plotting the pixels of image to English letters and special characters [5]. Color Image Steganography Created on Discrete Wavelet and Discrete Cosine Transforms from [6], In this paper the color cover image is divided into similarly four parts, for each part select one network from each part(Red, or Green, or Blue), selecting one of these channel depending on the high color ratio in that part. The chosen part is rotting into four parts {LL, HL, LH, HH} by using discrete wavelet transform. The walloping image is divided into four part n*n then apply DCT on each part. Finally the four DCT coefficient parts inserting in four high frequency sub-bands {HH} in cover image. By MohMohZan, Nyein Aye are presents a method for image steganography based on DWT, where DWT is used to convert the cover image from spatial domain to frequency domain. The secret message is encoded using the Blowfish encryption algorithm. This system will modify the LSB method by putting the encryption step and new insertion 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 decoded by the Blowfish decryption algorithm process. Influence of the proposed system is a new insertion method for hiding data in carrier 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 obtainable to provide high processing speed to RSA key cohort for embedded platform with imperfect processing capacity. In order to exploit more data level parallelism as per BoddupalliSrinivasaRao and M.Ramesh they use Verilog to implement a 16- bit RSA block cipher system. The whole implementation contains three parts: key generation, encryption and decryption process. The key generation stage purposes to generate a pair of public key and private key, and then the private key will be dispersed to receiver conferring 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) technique [8]. In paper [9] represented a double layered embedding technique 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.Olivier intends to give a summary of image steganography, its uses and techniques. It also tries to identify the requirements of

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

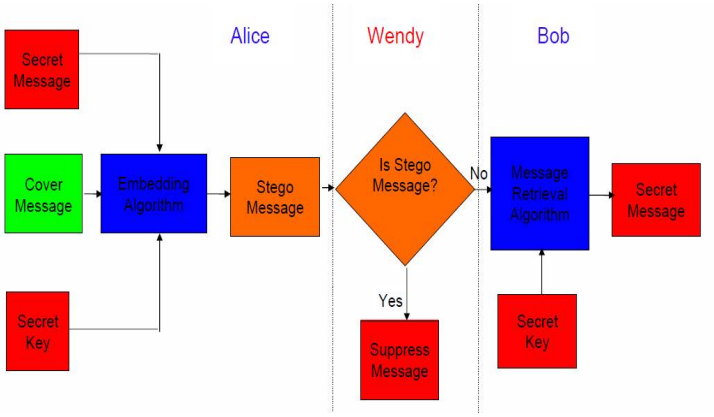
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

a good steganographic algorithm and briefly reflects on which steganographic techniques are more appropriate for which applications [10].

III. SYSTEM DESIGN

In this paper wedo embed whichever in 2nd and 4th or both bit locations of the bytes of the image based on the different values of the index variable. In its place of hiding the direct information, we hide the encrypted text. For this we used encryption algorithm called twelve-square substitution cipher.



Above figure shows the embedding/extraction process of the Image Steganography. Here we take the BMP image, distinct the plane of image in R, G, B form and then select any one plane or the entire three plane for supplement text. Our Secrete data are not directly stored in image plane they are firstly encode with the help of 12-square algorithm which are exhaustive 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 communication for further process.

B. Twelve Square Substitution Method

In this paper, an well-organized technique called twelve square substitution algorithms is used to encrypt the hidden text data. It comprisesnumerals, alphabets and special characters. The twelve-square cipher encrypts alphabets, digits and special characters and thus is less vulnerable to frequency analysis attacks. It uses six 5 by 5 matrices each categorical in a square, as shown in table-I. Each of the 5 by 5 matrices comprises the letters of the alphabet (usually omitting "Q" to reduce the alphabet to fitting into the square) and another six 6 by 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
a bcd e	f g hi j	k l m n o
f g h i 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

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

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 r i t	n o p s u
n o p s u	n o p s u	v w x y z
v w x y z	v w x y z	g m r i t

Table I decided as above. In Square-1, we have twenty five alphabets without the alphabet q, in each row we decided five alphabets. Square-2 is produced from square-1 by taking the first row of square-1 to fifth row place and other rows one position up. Likewise square-3 is produced from square-2 by taking the first row of square-2 to fifth row place and other rows one position up. In square-4, we have used a word gmrit in the first row which encompasses of the five alphabets and the residual twenty alphabets are arranged in other four rows continuously without the alphabets of the word "gmrit". Square-5 is made from square-4 by taking the first row to third row place. Likewise square-6 is made from square-4 by taking the first row to fifth row place. In table II square-7, the numerals and special characters from a standard laptop are arranged in six rows and seven columns. Square-8 is made from square-7 by taking the first row to sixth row place. Similarly square-9 is made from square-8 by taking the first row of square-8 to sixth row place. Square-10 is created from square-7 by positioning the row elements in columns. Square-11 is made from square-10 by taking the first row of square-10 to third row place. Likewise square-12 is constructed from square-10 by taking the first row into sixth row place.

For example:-

Secrete message - umesh@5$

Encrypted message – ujzsc, |7

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 ` ~ ! @

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

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 ! & + ; <

D. LSB (Least Significant Bit)

In this paper, the cover image is the file in which we will pelt the secrete message, which may also be encoded using the 12 square cipher algo. The subsequent file is the stego image (which will be the same as to the carrier image). The cover image (and thus, the stego image) is distinctive image. In this paper, I will focus on image files and will, therefore, refer to the cover image and stego image. Before we going to deliberate first see how secrete information is hide in a cover image, it is substance a fast review of how images are stored in the first place. An image file is simply a binary file covering a binary representation of the color or light intensity of each picture element (pixel) encompassing the image.

Images classically use either 8-bit or 24-bit color. When using 8-bit color, there is a definition of up to 256 colors starting a palette for this image, each color signified by an 8-bit value. A 24-bit color scheme, as the term proposes, uses 24 bits per pixel and delivers a much better set of colors. In this condition, each pixel is represented by 3 bytes, each byte representing the strength 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 cover file. In this method the least significant bits of few or all bytes inside an image is substituted with a bits of the text message. Firstly read the image and transform it into the pixel intensity or separate the plane R,G,B and least bit is replace with data but this technique 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.

IV.ALGORITHM

Algorithm to embed text message:
Step 1: Read the cover image and text message which is to be concealed in the carrier image.
Step 2: Renovate text message in binary.
Step 3: Calculate LSB of each pixels of carrier image.
Step 4: Substitute LSB of carrier image with each bit of secret message step by step.
Step 5: Write stego image.

Algorithm to recover text message:
Step 1: Read the stego image.
Step 2: Estimate LSB of each pixels of stego image.
Step 3: Retrieve bits and alter each 8 bit into character.

V. RESULT ANALYSIS

Here two figure1 is taking as input mage and that input image is separate in three different plane which is shown in figure2.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Figure1 Input Image

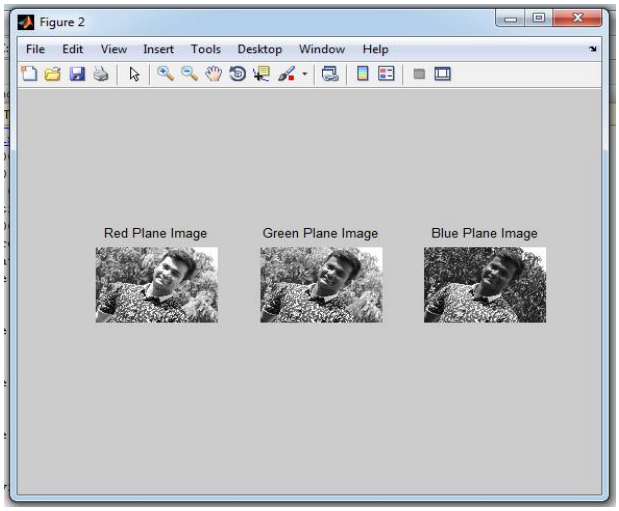


Figure2 Plane Separation

Figure3 shows the secrete message, this secrete message converted using 12 square algorithm after encrypting secrete message you will get message like in figure4.

Figure 3 Secrete Message

Figure 4 Encrypted Message

After encrypting secrete message I am going to hide this message using LSB methode into Stego Plane. After hiding secrete message you will get stego plane like figure5. After that all these plane are mix with each other an you get the one stego image an you also see there is no effect occure on stego image an input image after hiding secrete message.

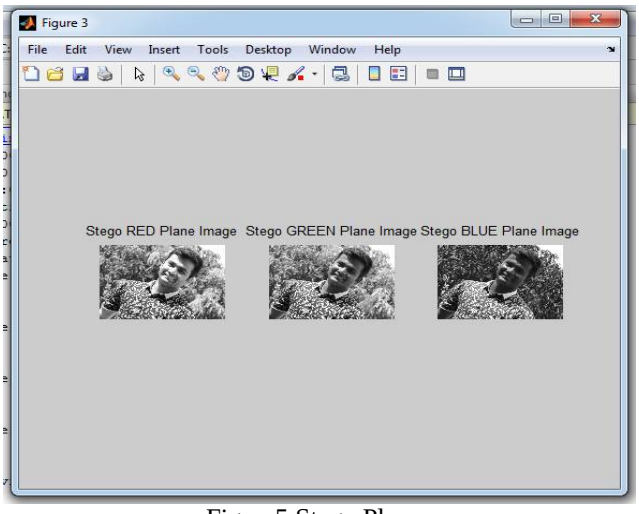


Figure5 Stego Plane

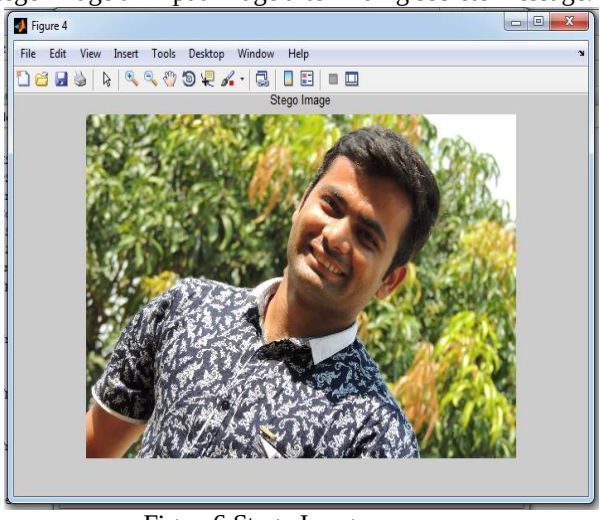


Figure6 Stego Image

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Once you decrypt the stego image you will get the original message shows in figure7.

Figure7 Decrypted Message

A Mathematical Calculation

- MSE = sum(sum((Embedded-input).^2))/(r*c);
- PSNR = 10*log10(255*255/MSE);
- Entropy = entropy(Embedded);
- ccoef = corr2(input,Embedded);
- ssim = ssim_index(input,Embedded);
- Sensitivity = (Tp./(Tp+Fn)).*100;
- Specificity = (Tn./(Tn+Fp)).*100;
- Accuracy = ((Tp+Tn)./(Tp+Tn+Fp+Fn)).*100;

B. Result Table

In this table I am showing few sample result on different images.

Images	MSE	PSNR	ENTROPY	CORRELATION	SSIM
Umesh	0.000005	100.94782	0.000002	1.00000	1.000000
Lena	0.000275	83.742878	-0.000000	1.00000	0.999998
Surya	0.000403	82.080387	0.049958	1.00000	0.999997
DYP Logo	0.002136	74.833913	0.000875	0.99999	0.999990

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

VI. ADVANTAGES

Secrecy: a people should not be able to excerpt the secrete data from the stego image without the information of the proper secret key used in the mining procedure.
Imperceptibility: the medium afterward being embedded with the secrete data should be imperceptible from the original medium. One should not become doubtful of the being of the secrete data within the medium.
High capacity: the maximum length of the secrete message that can be inserted should be less than carrier data.
Resistance: the secrete data should be able to endure when the host medium has been operated, for example by some lossy compression scheme.
Accurate extraction: the abstraction of the secrete data from the medium should be perfect and consistent.
Flexible system and Better compression ratio.
Less Bandwidth utilization.
Highly secure communication.

VII. APPLICATION

- Alleged use by intelligence division.
- Privacy and obscurity is a concern on the internet.
- Allows for two parties to communicate secretly and clandestinely.
- It allows for copyright guard on digital files using the message as a digital watermark.
- One of the other main usages for Image Steganography is for the transportation of high-level or top-secret documents between international governments.

VIII. CONCLUSION

In this paper, steganography used is imitative from Greek word stegos and graphy which means covered and writing. Here we familiarizes evaluation of the previous paper how they use steganography for hiding the secrete message. And here also shows the small associated work about the project. Examples are giving here for the 8 bit LSB in which stowed data in last bit location but in our future work we are using 8 bit LSB to store data in the 2^{nd} and 4^{th} bit location. In this paper we reference the way of how to encrypt secrete message using the twelve square algorithms and how to hide the cover image.

REFERENCES

[1] Mohammad Ali BaniYounes and AmanJantan, "A NewSteganography 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] BasantSah, 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] MohMohZan, 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.SrinivasaRao, 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.
[11] Umesh M. Umate1, Dr.V.N.Nitnaware2, "Analysis And High Security Data Hiding Technique In Encrypted Image", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 4, April 2016.