Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 02, pp. 65517-65520, February, 2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

PERFORMANCE ANALYSIS OF SECURE DATA HIDING ALGORITHM

***Harshitha, K. M.**

E&C Engineering Department, Govt. Polytechnic for women, Hassan-573201, India

ARTICLE INFO

Article History:
Received 28th November, 2017
Received in revised form
27th December, 2017
Accepted 19th January, 2018
Published online 28th February, 2018

Key words:
Steganography.

ABSTRACT

In data communication, security is the most important issue in today's world. This project is a combination of stegano graphy and cryptography, which provides a strong backbone for its security. This present work focus is enlightening the technique to secure data or message with authenticity and integrity. In this project work, the secret message is encrypted before the actual embedding process starts. The entire work has done in MATLAB. The hidden message is encrypted using a simple encryption algorithm using secret key and hence it will be almost impossible for the intruder to unhide the actual secret message from the embedded cover file without knowing secret key. Only receiver and sender know the secret key.N-bit LSB substitution technique is used as embedding and extraction method. We propose that this method could be most appropriate for hiding any secret message (text, image, audio, video) in any standard cover media such as image, audio, video files (Harshitha, 2012). And also performance factor such as PSNR, Utilization factor are computed and performance analysis has been made by plotting graph of these factor against no of LSB bits replaced during embedding process.

Citation: Harshitha, 2018. "Performance analysis of secure data hiding algorithm", *International Journal of Current Research*, 10, (02), 65517-65520.

INTRODUCTION

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". The innocent files can be referred to as cover text, cover image, or cover audio as appropriate. After embedding the secret message it is referred to as stego-medium. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data. While cryptography is about protecting the content of messages (their meaning), steganography is about hiding the message so that intermediate persons cannot see the message. Steganography refers to information or a file that has been concealed inside a digital Picture, Video or Audio file (Harshitha, 2012).

Literature review

The Scope of Steganography

With the boost in computer power, the internet and with the development of digital signal processing (DSP), information Theory and coding theory, steganography has gone ''digital''. In the realm of this digital world, steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications, thus its continuing evolution is guaranteed. Cyber-crime is believed to benefit from this digital revolution. Hence an immediate concernis to find out best possible attacks to carry out steganalysis, and simultaneously, finding out techniques to strengthen existing stegnography techniques against popular attacks like steganalysis (Hrytskiv *et al*., 1998)

Cryptography

Cryptography encodes information in such a way that nobody can read it, except the person who holds the key. More advanced cryptotechniques 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.

The proposed system

Data hiding techniques have been widely used to transmission of hiding secret message for long time. Ensuring data security is a big challenge for computer users. Businessmen,

Corresponding author: **Harshitha, K. M.**
E&C Engineering Department, Govt. Polytechnic for women, Hassan-573201, India.

professionals, and home users all have some important data that they want to secure from others. In this proposed system we have the software for data encryption and then embed the cipher text in an cover medium. This system combines the effect of these two methods to enhance the security of the data. The proposed system encrypts the data with a crypto algorithm and then embeds the encrypted data in an cover file. This system improves the security of the data by embedding the encrypted data and not the plain data in cover file. The block diagram of proposed system is as shown in Fig.1.

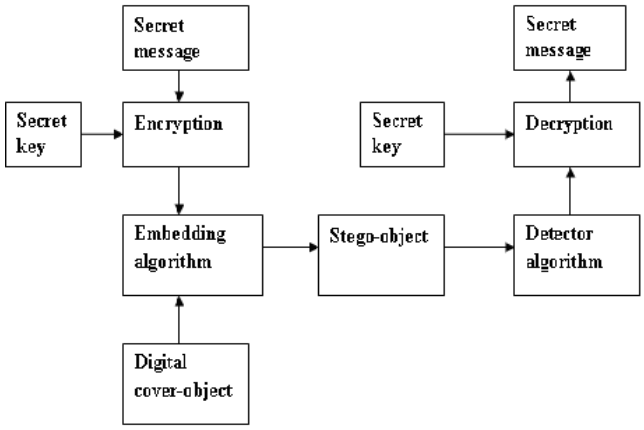

Fig. 1. Block diagram of proposed system

To embed a secret message file in the cover file used two distinct methods:

- encrypt the secret message
- The encrypted secret message is embed in the cover media by using LSB substitution technique. Let us now describe proposed encryption method and then the steganography algorithm.

Encryption algorithm

In this project the secret message is encrypted before embedding .the secret message is randomly permuted using the secret key. The random permutation is carried out by using matlab functions rand and randperm.

rand('twister',key)

p = randperm (length(N))

r and function randomly generates numbers using state ”twister” and key. p stores the randomized positions of the length of the secret message i.e length (N). Then secret message is randomized accordingly. This encryptiom method is simple and efficient and is of symmetric type where only receiver and sender knows secret key. The Secret key length is variable and is of range double precision. At the receiver side during extraction process the decryption, that is the reverse process of encryption is carried out using the same key to obtain the secret message from stego medium. In a nutshell, the reason that we encrypt the message is:

Cryptography + Steganography = Secure Steganography

Least Significant Bit (LSB) substitution method

Least Significant Bit (LSB) substitution method is a very popular way of embedding secret messages with simplicity. The fundamental idea here is to insert the secret message in the least significant bits of the images. This actually works because the human visual system is not sensitive enough to pick out changes in color where as changes in luminance are much better picked out. A basic algorithm for LSB substitution is to take the first N cover pixels where N is the total length of the secret message that is to be embedded in bits. After that every pixel's last bit will be replaced by one of the message bits. Least significant bit (LSB) insertion is a common, simple approach for embedding information in a cover image. The LSB or in other words 8-th bit of some or all the bytes inside an image is changed to a bit of the secret message. Let us consider a cover image contains the following bit patterns:

Byte-1 Byte-2 Byte-3 Byte-4
00101101 00011100 11011100 10100110

Byte-5 Byte-6 Byte-7 Byte-8
11000100 00001100 11010010 10101101

Suppose a number 200 is to embed in the above bit pattern. Now the binary representation of 200 is 11001000. To embed this information at least 8 bytes in cover file is needed. Hence taken 8 bytes in the cover file. Now modify the LSB of each byte of the cover file by each of the bit of embed text 11001000. Now Table 3.2 shows what happens to cover file text after embedding 11001000 in the LSB of all 8 bytes.

Table 3.1. Illustration of LSB technique

Before Replacement	After Replacement	Bit inserted	Remarks
00101101	00101101	1	No change in bit pattern
00011100	00011101	1	Change in bit pattern(i)
11011100	11011100	0	No change in bit pattern
10100110	10100110	0	No change in bit pattern
11000100	11000101	1	Change in bit pattern(ii)
00001100	00001100	0	No change in bit pattern
11010010	11010010	0	No change in bit pattern

Here out of 8 bytes only 3 bytes get changed only at the LSB position. Since changing the LSB hence either changing the corresponding character in forward direction or in backward direction by only one unit and depending on the situation there may not be any change also as seen in the above example. As our eye is not very sensitive so therefore after embedding a secret message in a cover file our eye may not be able to find the difference between the original message and the message after inserting some secret text or message on to it.

Description of proposed work

When the system is executed GUI is displayed for embedding process. The Embed window provides option for selecting secret message file. The secret message file may be text, image audio, video. There is also provision for choosing cover medium (video, audio, image). Enter the key and press encrypt button to encrypt the secret message. And choose the no of LSB bits (1,2,3,4,5,6,7,8) which are replaced by secret message in cover file. As we go on increasing no of LSB bits the size of secret message to be hide also increases. press embed message button to embed the message in cover file to

get stegomedium and the press save button to save the stegomedium. embed window also displays time taken in embedding, Utilization factor and PSNR value. Press message extraction button to extract the secret message from stegomedium or press exit button to get out of the Embed window.

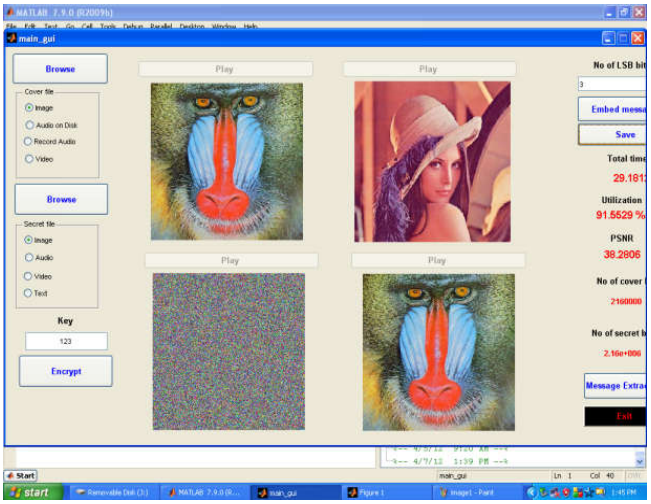

Figure 2. Snapshot of Embed Window

In extract window browse any stego medium file, enter the correct key and then press extract button to extract the secret message from the stego medium. If the incorrect key is entered it is not possible to extract message. The decryption is performed along with extraction when extract button is pressed. The advantage of this extract window is that it can extract any kind of stegomedium (image, audio, video) with secret key known

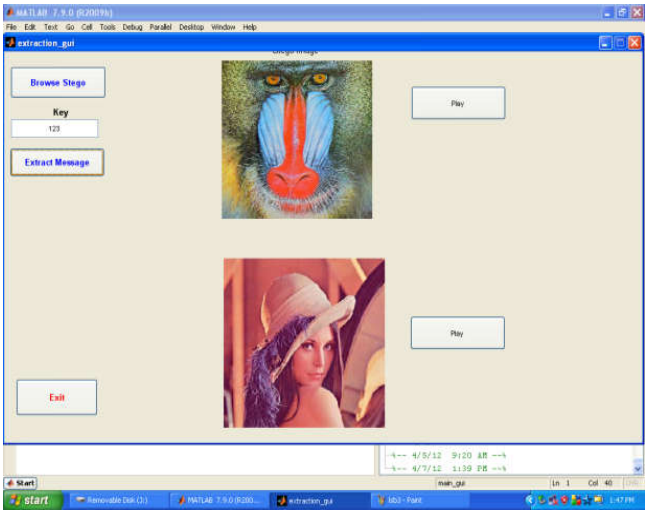

Figure 3. Snapshot of Extract Window

RESULTS AND DISCUSSION

In steganography following factor are considerered after embedding secret message in the cover medium.

Utilization factor

The utilization factor denotes the amount of cover image that has been utilized to embed the secret message into it. And it is given by

Utilization factor =secret message size(bits)/ cover medium size(bits)*100 (1)

PSNR value

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of a logarithmic decibel scale. A higher PSNR value indicates that the reconstruction is of higher quality..PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codes. The signal in this case is the original data, and the noise is the error due to hiding. The PSNR value is calculated by Eqn. (2)

$$PSNR(dB) = 10 * \log\left(\frac{25\xi^2}{MSE}\right) \quad (2)$$

Where MSE: Mean-Square error Mean Square Error (MSE): It is the measure used to quantify the difference between the initial and the distorted or noisy image. And is given by Eqn.3.

$$MSE = \sum_{i=1}^{x}\sum_{j=1}^{y}\frac{(|A_{ij}-B_{ij})^2}{x+y} \quad (3)$$

Where x: width of image.
y: height.
x*y: number of pixels

RESULTS ANALYSIS

As no of LSB bits replaced by secret message in carrier file goes on increasing, the embedding capacity increases but at cost of perceptual transparency. Statistical properties of stegomedium changes which attracts third party. Thus steganography will fail. In order to analyse, graph of PSNR versus No of LSB bits taken is plotted as shown fig 4. In the graph, PSNR attain peak when no of LSB bits is 3(that is replacing 3 last consecutive LSB bits in byte of carrier file by secret message bits) and gradually decreases as no of LSB bits goes on increases. The PSNR is taken zero value for 1, 2 LSB bits which means for these no of bits embedding is not possible. And Peak PSNR indicates that reconstruction quality is better for particular no of LSB bit compared to others. Whereas in other case to know embedding capacity variation of carrier for different no of LSB bits taken graph of utilization factor versus no of LSB bits taken is plotted which is as shown in fig 4. If utilization factor is less than 1(<100 if percentage considered) then embedding is possible, otherwise not because size of secret message is larger than that of carrier. As the no of LSB bits taken for embed goes on increases the embedding capacity also increases which is shown by decreasing values for utilisation factor. For no of LSB bits 3, the utilisation factor is less than 100, hence embedding can be done. The utilisation factor goes on decreasing with increasing in No of LSB bits taken as result embedding capacity goes increasing. Here PSNR, Utilisation factor values are taken from hiding image in image case. These results can be generalized for all other cases.

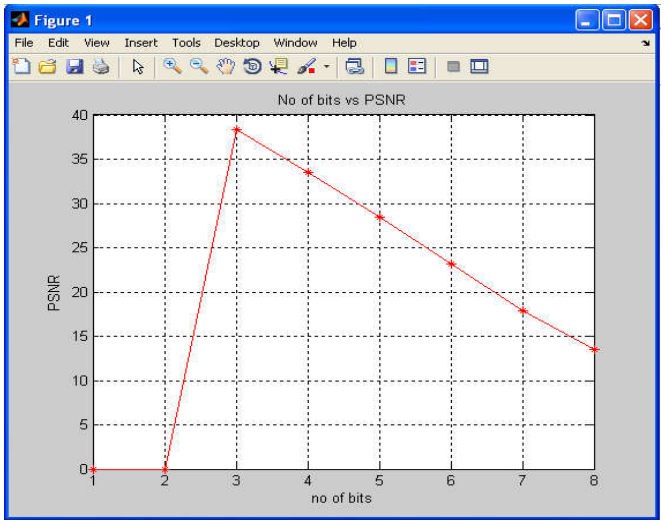

Fig. 4. Graph of PSNR versus no of LSB bits taken for hiding image in image case

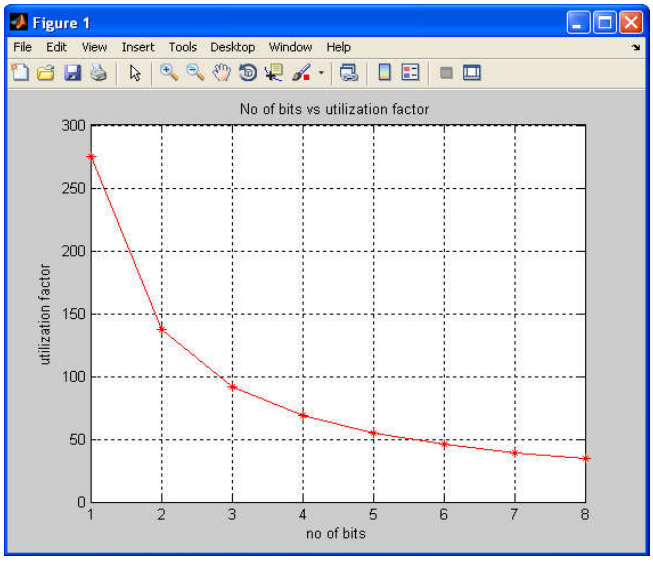

Fig.5. Graph of utilization factor versus no of LSB bits taken for hiding image in image case

Conclusion

In this paper we give an idea to enhance the security of system by combining the two techniques. It can enhance confidentiality of information and provides a means of communicating privately. Here message is first encrypted and then embed in cover file with help of steganographic system.

LSB algorithm is applicable for all kind of cover medium (image, audio, video). LSB algorithm is used for both embedding and extraction process. The entire work is done in MATLAB. And performance analysis of proposed data hiding algorithm is done by plotting graph of PSNR, Utilization factor against no of LSB bits used in embedding process. As no of LSB bits replaced by secret message increases, even though embedded capacity increases, Statistical properties of stegomedium changes which attracts third party. Thus steganography will fail. So during embedding process, choose proper no of LSB bits such that embedding can also done along with better reconstruction quality not at the cost of perceptual transparency.

REFERENCES

Advanced Steganography Algorithm usingencrypted secret message, Joyshree Nath and Asoke Nath. 2011. *International Journal of Advanced Computer Science and Application (IJACSA)* Vol-2 No.3, Page19-24, March

Amin, M.M., Salleh, M., Ibrahim, S., Katmin, M.R. and Shamsuddin, M.Z.I. 2003. "Information Hidingusing Steganography", *IEEE* 0-7803-7773-March 7

Bender, W., Gruhl, D., Morimoto, N. and A.Lu, "Techniques for Data Hiding", *Sysfems Journal,* vol. 35.

Cachin, C. 1998. "An Information-theoretic Model for steganography", inproceeding 2nd Information Hiding Workshop, vol.1525, pp.306-318,

Harshitha, K.M. and Dr. Vijaya, P.A. 2012 "secure datahiding algorithm by encrypted secret message", *ijsrp*, vol 2, issue 6, june.

Hrytskiv, Z., Voloshynovskiy, S. and Rytsar, Y. 1998. "Cryptography of Video Information In Modem communication", *Electronics And Energefics*, vol. 11, pp. 115-125,

Isbell, R.A. 2002. "Steganography: Hidden Menace or Hidden Saviour", Steganography White Paper,IO May

Zollner, J., Federrath, H., Klimant, H. *et al*. 1998. "Modeling the Security of Systems", Steganographic in 2nd Workshop on Informafion Hiding, Portland, April, pp. 345-355.proceeding of IEEE, pp. 1062-1078,July1999.

Neil F. Johnson, Zoran uric, and Sushil. Jajodia. 2000. "Information Hiding: steganography and Watermarking Attacks and Countermeasures", Kluwer Academic Press, Norwrll, MA, New -York,

Provos, N. and Honeyman, P "Detecting Stegano graphy Content on the Internet". Transformation", ZEICE, Tram.

Stinsown, D. "Cryptography: Theoryand practice"

****