Secure Data Hiding Algorithm Using Encrypted Secret message

Harshitha K M, Dr. P. A. Vijaya

Abstract- In any communication, security is the most important issue in today's world. Lots of data security and data hiding algorithms have been developed in the last decade, which worked as motivation for the research. This project is a combination of steganography and cryptography, which provides a strong backbone for its security. The scenario of present day of information security system includes confidentiality, authenticity, integrity, non-repudiation. 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.

I. 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[1].

II. LITERATURE REVIEW

A. 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[2]

B. 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.

III. 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, 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 fig1

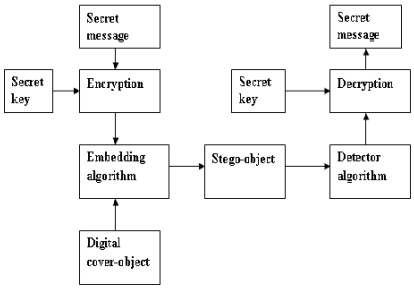


Fig. 1: Block diagram of proposed system

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

(1) encrypt the secret message

(2) 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.

A. 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))

rand 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

B. 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 Table3.2 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.

C. 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.

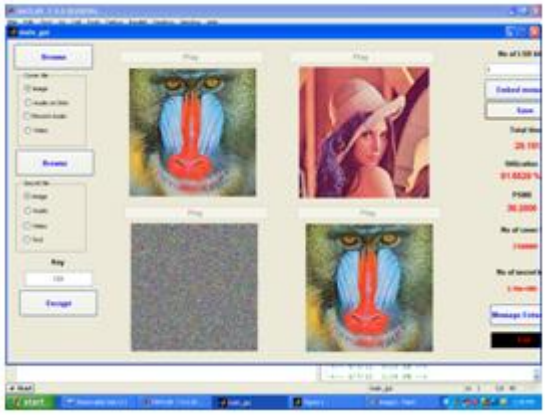


Fig. 2: Snapshot of Embed Window

In extract window browse any stegomedium file, enter thecorrect key and then press extract button to extract the secret message from the stegomedium.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

Fig. 3: Snapshot of Extract Window

IV. RESULTS AND DISCUSSION

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

A. 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 = ecret message size(bits)/ cover medium size(bits)*100 (1)

B. 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)

$$PSNR(dB) = 10 * \log\left(\frac{255^2}{MSE}\right) \quad (2)$$

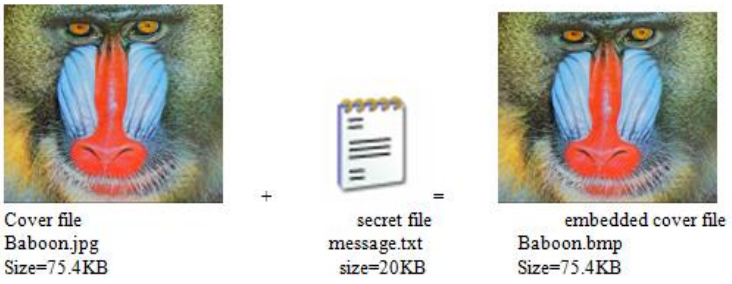
Where MSE: Mean-Square error Mean Square Error (MSE): It is the measure used to quantify the difference between the initial and the distorted or noisy image.and is given by Eqn.3.

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

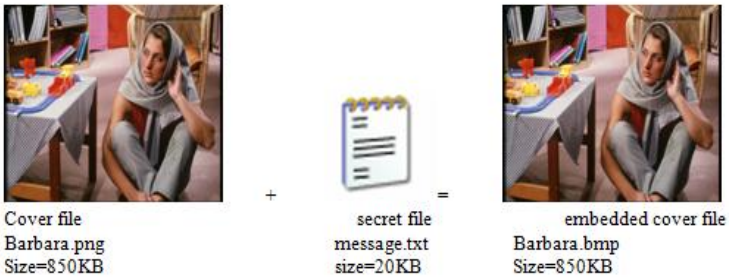
Where x: width of image.
y: height.
x*y: number of pixels

We applied our present method on different cover files and secret message files and the results are given below:

Case-1 cover medium=image (Jpeg,Png ,bmp) secret message =text file



Cover file Baboon.jpg Size=75.4KB | secret file message.txt size=20KB | embedded cover file Baboon.bmp Size=75.4KB



Cover file Barbara.png Size=850KB | secret file message.txt size=20KB | embedded cover file Barbara.bmp Size=850KB

Case-2 cover medium=audio (.wav file or recording) secret message =text file

Cover file Sslr.wav Size=238KB | secret file message.txt size=20KB | embedded cover file stegivideo.avi Size=238KB

Case-3 cover medium= video (mpg file) secret message = text file

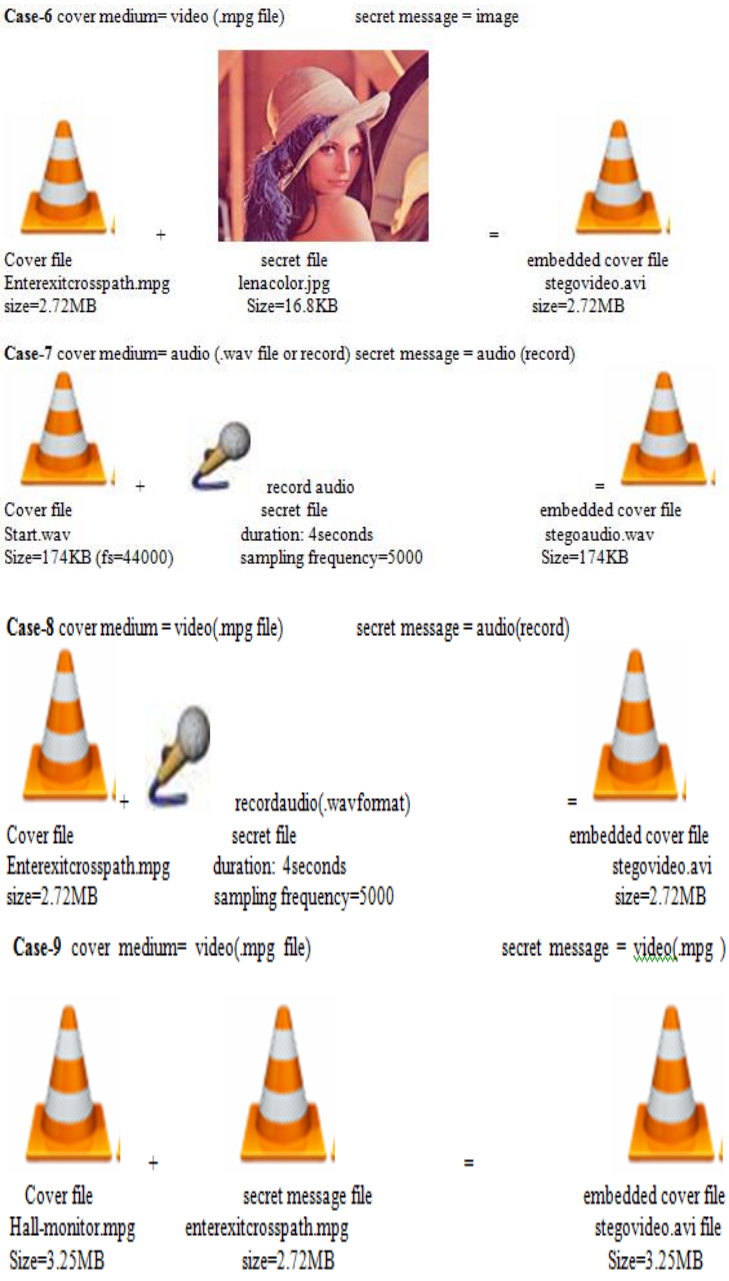
Cover file Hall-monitor.mpg Size=3.25MB | secret file message.txt size=20KB | embedded cover file stegovideo.avi Size=3.25MB

Case- 4 cover medium = image secret message =image

Cover file Barbara.jpeg Size=850KB | secret file lenacolor.jpeg size=16.8KB | embedded cover file stegoimage.bmp Size=850KB

Case-5 cover medium= audio (.wav file on disk or record audio) secret message = image

Cover file Sslr.wav Size=238KB | secret file logo.jpeg size=4.48KB | embedded cover file stegoaudio.wav Size=238KB



V. CONCLUSION

Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography.Steganography has its place in security.It is not intended to replace cryptography but supplement it. 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 There are infinite number ofsteganography applications for digital image including copyright protection,feature tagging, and secret communication. This paper explores a tiny fraction of the art of steganography. The steganography method may be further secured if we compress the secret message first and then encrypt it and then finally embed inside the cover file.

REFERENCES

[1] Z. Hrytskiv, S. Voloshynovskiy & Y. Rytsar "Cryptography of Video InformationIn Modem communica-tion", Electronics And Energefics, vol. 11, pp. 115-125, 1998

[2] Stinsown,D."Cryptography:Theory and practice"

[3] C. Cachin, "An Information-theoretic Model for steganography", in proceeding 2nd Information Hiding Workshop, vol.1525, pp.306-318,1998

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

[5] R A Isbell, "Steganography: Hidden Menace or Hidden Saviour", steganography White Paper,IO May 2002

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

[7] W. Bender, D. Gruhl, N. Morimoto and A.Lu, "Techniques for Data Hiding", Sysfems Journal, vol. 35, 1996

[8] M. M Amin, M. Salleh, S. Ibrahim, M .R. Katmin, and M. Z. I. Shamsuddin," Information Hiding using Steganography", IEEE 0-7803-7773-March 7,2003

[9] N. Provos, P. Honeyman, "DetectingSteganography Content on the Internet".Transformation", ZEICE Tram.

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

AUTHORS

First Author - Harshitha K M, USN:4MC10LDS10, Mtech(DE&CS), MCE,Hassan-573202
Email id - harshimce022@gmail.com

Second Author - Dr. P. A. VIJAYA BE., M.E., PhD, Professor and Head, Dept. of E&C Engg. MCE, Hassan-573202
Email id - pavmkv@gmail.com