International Journal of Engineering Research & Management Technology ISSN: 2348-4039
March-2016 Volume 3, Issue-2
Email: editor@ijermt.org www.ijermt.org

A Secured Approach to Steganographic LSB Algorithm

Riddhima Sinha, Deeksha Upadhyay, Ashima Sinha
Department of Information Technology
SRM University

ABSTRACT:

In the paper we propose a new technique in steganography for hiding digital images. An approach to encrypting data would be to hide it by making this information look like something else. In this way only receiver would realize its true content. For implementing steganography the images which are collection of pixels should be in a proper format. This technique is basically for securing confidential data through image.

In our proposed system we take .png image to hide the data. Security is the main concept behind steganography. Here we use a simple LSB and our innovative algorithm and their analysis on the basis of their image intensity, and security. Comparison is done between LSB and Patterned LSB algorithm. When compared with other algorithms, it is proved that the difficulty of decoding our proposed algorithm is high. Hence this is an efficient technique to hide highly confidential data.

INDEXTERMS: Analysis, Patterned LSB, LSB algorithm, Steganography, confidential data.

I. INTRODUCTION:

Steganography is the practice of concealing secret messages within other digital image. The word steganography combines [7]the greek words steganos meaning "covered, concealed, or protected", and graphein meaning "writing". In steganography. The hidden message appears to be something else. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information.

In cryptography we hide the message into some secret code and the identity is revealed whereas in steganography the presence of any secret message is not revealed. Thus steganography is a better approach than cryptography.

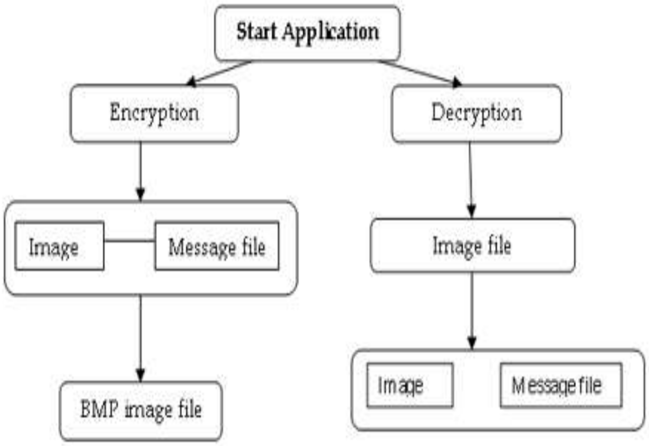

Fig1: Steganography process

Basic elements of steganography are: the carrier image called the “cover image” and the image that has encoded data is called “stego image”. The encoding is usually controlled using shared secret key between the parties.[5]

The goal of steganography is to prevent highly secured messages and confidential data from any active or passive attacks. If a person views the image he will not be able to determine if there is any hidden information, therefore he

will not attempt to decrypt the image message behind it.[6]

DEPENDING ON THE TYPE OF THE COVER OBJECT THERE ARE VARIOUS STEGANOGRAPHIC TECHNIQUES:

1. Image steganography: Taking the cover object as image in steganography is known as image steganography.
2. Network steganography: Taking the cover object as network protocol (TCP, UDP, ICMP,IP) where protocol is used as carrier known as network protocol stegannography.
3. Video steganography: The technique of hiding any kind of file or information into digital video format is known as video steganography.
4. Audio steganography: Taking the cover object as an audio which acts as a carrier for information hiding is called audio steganography.
5. Text steganography: The technique of using text such as tabs, whitespaces, capital letters etc. to hide the information is known as text steganography.

The goal of steganalysis is to break steganography. [2]They basically deal with three basic attacks: Visual attack, statistical attack and structural attack. So in order to prevent our data from these attacks se perform various steganographic techniques.

APPLICATION OF STEGANOGRAPHY:

1. For confidential communication and maintaining the secrecy of data.
2. Protection of data from being altered.
3. Best for media database system.
4. Video/audio synchronization where company performs safe circulation of secret data.

II. LEAST SIGNIFICANT BIT METHOD:

The simplest form of digital steganography is the Least Significant Bit (LSB) method. LSB is the method of binary representation of data where the data is converted into streams of bits. [1]The overall changes in the image is so negligible that it can not be identifies with a naked eye. Steganography implements the LSB method for hiding text inside an image.

ENCODING:

The secret message is read and converted into bit sequence. A stego array is created that stores the length of the message in the first four bits followed by the rest of the message. The carrier image is read (.png format) and is converted into bytes. Now the image is checked. If it is large enough to store the stego array. Now store each bit of the stego array by modifying last bit of each image byte according to the stego array bit. The pattern of the modified bits can be altered by the offset variable. Store the modified image with the new name.[3]

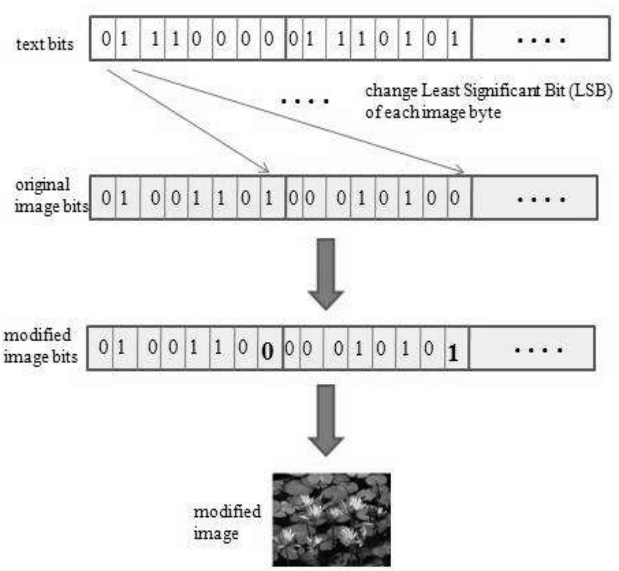

Fig2: Encoding using LSB

DECODING:

Read the image and convert it into bytes. Now the message length is retrieved from the first four bytes of the image followed by the message by extracting the LSB of each byte of the image till the end of the message is reached. Further the bit sequence is converted into string and the decoded message is saved as a text file.[3]

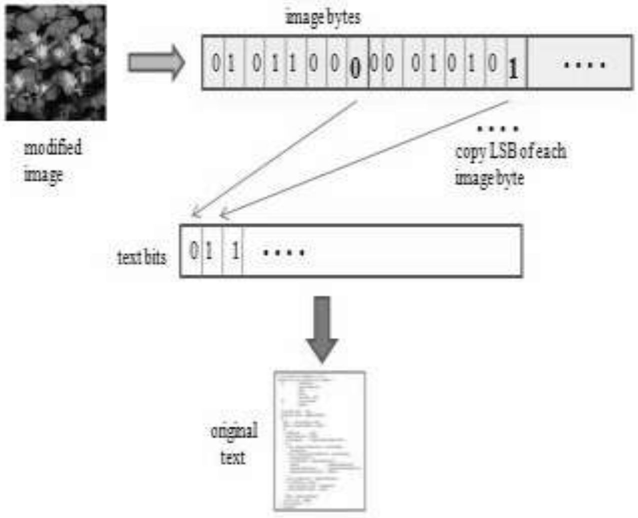

Fig3: Decoding using LSB

In our proposed work we are developing a user interface system to compare the two algorithms on the basis of their ability to secure data.

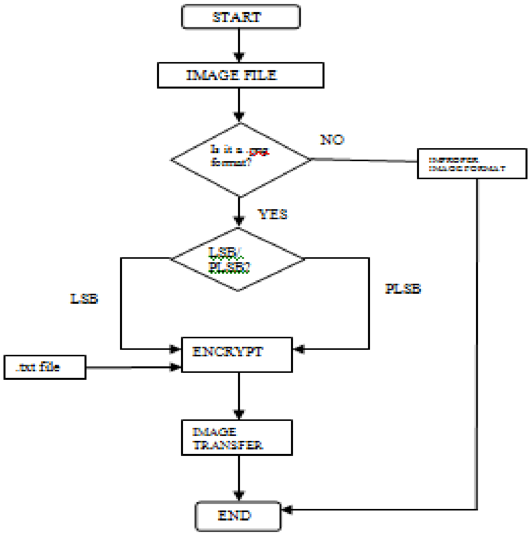

Fig4:Encoding

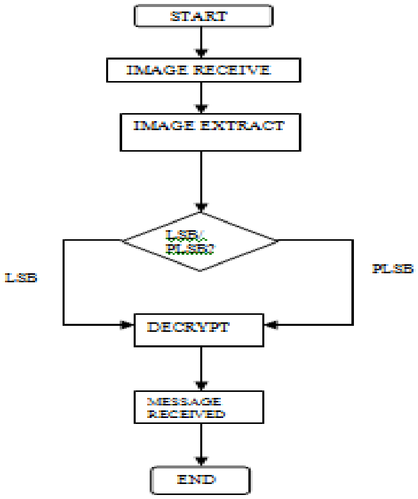

Fig5:Decoding

III. PATTERNED LSB ALGORITHM:

In this technique, the intention is to develop a more secured algorithm using a randomly generated key pattern for the RGB values.[4]

Basically Doubled lsb algorithm aims at improving our traditional lsb algorithm technique. According to the research. it is revealed that reaction of human eyes to the red, green and blue colours is different.

Brightness formula(I) = 0.3R + 0.59G + 0.11B

A human eye are least sensitive to blue followed by red and is most sensitive to green.

Therefore, the different least bits of brightness of the red, green, and blue value of each pixel can be replaced by the hiding message data . according to the principle of least significant bit algorithm the effect of replacing nth value is 2n-1 which is the first least bit replacement effect is 1, the second is 2 and the third's is 4. When the bit is higher the effect is greater.

Now as we know according to simple LSB the message bits are incrementally embedded into the pixels in the image, this makes it easy for the hackers to extract the message easily, who has the knowledge of Steganography to be carried out to obtain the secret message. This problem of simple LSB is solved by using a method where you divide the whole image into 8x3pixel blocks in which embedding is to be done. Hence this will result in distribution of the message over the entire image pixel blocks. Thus, even if the hacker uses LSBs and read, they do not get any appropriate information. The 8x3pixel block will be distributed Each block follows a pattern for embedding as the first line of each block bit pattern is embedded with RED plane. Then for the next line of that block, GREEN plane is embedded and the same is followed for the BLUE plane as well or vise versa. A particular pattern needs to be followed .This makes the system more secure because the reader of the message must know the pattern of RGB pixels in order to determine the hidden message. This random pattern would improve the message security . This increases the hiding efficiency and security of our traditional LSB method.

ENCODING:

1. We start by calculating the total number of image pixels.
2. Divide the image into 8xpixel blocks.
3. The text message is converted into bit stream.
4. The message is divided into 8X3bit blocks.
5. Red plane is embedded in the first line of the block .
6. Similarly green plane is embedded for the next line of the same block and
7. blue is embedded in the third line of the block.
8. The entire steps is repeated from 5-7 to embed the entire message.

DECODING:

1. The image is obtained with the secret message and is divided into 8X3 pixel blocks.
2. Now the blocks are permuted in 8x3 pixel block.
3. Follow the RGB pattern to decode
4. The message is obtained by patterned lsb
5. Obtain the entire message stream and convert it into ASCII values.

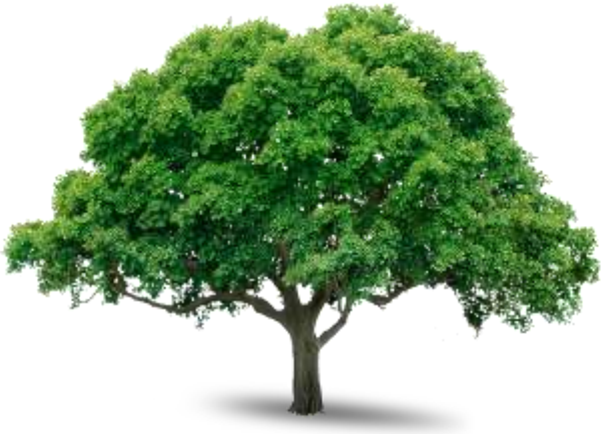

Fig6: tree_PNG216(original image)

Fig7: tree_PNG216Msg(encoded image)

IV. CONCLUSION:

The work in this paper is basically to develop a more secured LSB algorithm which improves the performance intensity and security of traditional LSB algorithm. This algorithm improves security. Our proposed technique performs better than traditional LSB as we are generating a randomized key pattern. Thus we have proposed a technique for securing more confidential private message through this steganography system. In future our system can be used with high robustness and high capacity payload.

REFERENCES:

1. Andrew D. Ker, "Steganalysis of embedding in two least-significant bits", IEEE Transactions on Information Forensics and Security, vol.2,march, 2007, pp. 46-54
2. N. F. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," IEEE Computer, vol. 31, no. 2, pp. 26–34, 1998.,
3. avierfjard.com/PDFs/Cryptography/Steganography/Java Steganography.pdf
4. Bhabdhosh, C., Digital Image Processing and Analysis, 8th Edn., Prentice Hall, India, 2006
5. Rahul Jain and Naresh Kumar "Efficient data hiding scheme using lossless data compression and image steganography" International Journal of Engineering Science and Technology (IJEST) Vol. 4 No.08 August 2012.
6. Siddharth Singh and Tanveer J. Siddiqui "A Security Enhanced Robust Steganography Algorithm for Data Hiding" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.
7. Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf.