ISSN NO. 2320-5407

Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/6779
DOI URL: http://dx.doi.org/10.21474/IJAR01/6779

RESEARCH ARTICLE

IMAGE STEGANOGRAPHY USING IMPROVED LSB ALGORITHM.

Rohit Chaudhary, Rishabh Kaushik and Tuariq Beg.
B. Tech 4th year/CSE IMS Engineering college Ghaziabad, U.P., INDIA.

……………………………………………………………………………………………………....

Manuscript Info

……………………..

Manuscript History

Received: 19 January 2018
Final Accepted: 21 February 2018
Published: March 2018

Keywords:-
Steganography, Public key steganography, LSB method, Modified LSB method of Public key steganography, Image steganography, Encryption Techniques.

Abstract

………………………………………………………………

The goal of Steganography is to hide communication. So, a fundamental requirement of this Steganography system is that the hidden message should not be visible to human beings. The other goal of this method is to avoid suspicion to the presence of hidden message. This technique has recently became important in a number of application areas.

The project has various objectives such as:

- To produce security tool based on Steganography techniques
- To enhance techniques of hiding data using encryption.
- To extract hidden data using decryption methods.

Steganography is sometimes used when encryption is not allowed. An encrypted file may still hide information using Steganography, so even if encrypted file is deciphered, the hidden message is not seen. The objective of "Steganography" is to increase the efficiency of a system to reduce the manual labour.

……………………………………………………………………………………………………....

Introduction:-

During communication through insecure network the main issue arises is security. For sure communication we use different techniques such as cryptography, Steganography etc.

- Steganography is an art of hiding information inside information.
- The main purpose of Steganography is mainly troubled with the protection of contents of the hidden information.
- Images are ideal for information hiding because of the large amount of surplus space is created in the store of images.

Corresponding Author:- Rohit Chaudhary.
Address:- B. Tech 4th year/CSE IMS Engineering college Ghaziabad, U.P., INDIA.

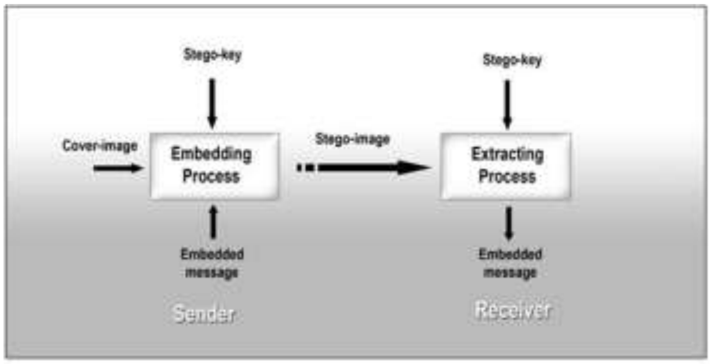


Image 01: General Diag. of Steganography

Secret Communication	Secrecy	Reliability	Unremovability
Encryption	Yes	No	Yes
Digital Sign	No	Yes	No
Steganography	Yes/No	Yes/No	Yes

Table 01:- Comparison of secret communication Techniques

Cryptography was created as a technique for securing the privacy of communication and many methods have been invented to encrypt and decrypt data in order to keep the message secret.

Symmetric algorithms are used to encrypt and decrypt original significance by means of identical key. While public key encryption algorithm methods work in sundry way. In these there is a pair of keys: One is recognized as public key that is worn to encrypt information and a private key to decrypt the information.

Steganography is a way of communication in such a way that attendance of message is not known. Steganography is helpful for hiding messages for broadcast. One of the major find of this study was that each steganographic accomplishment carries with it noteworthy trade of decisions, and it is up to the steganographic to decide which accomplishment suits him/her best. With the advance in the field of production and knowledge we are able to protect data from spiteful intruder. Work is being done to agitate out more methodical, proficient and sheltered algorithms and technique. This method provide better sanctuary for information than conventional methods. This method should not show any buckle in eminence of the image.

The message can be concealed in audio,vedeo, text, image etc. Cryptography and Steganography can also be used mutually.

Steganography vs Cryptography

- Cryptography hide the stuffing of a secret message from a malevolent people, whereas steganography even obscure the subsistence of the message.
- In cryptography, the method is kaput when the invader can read the secret message.
- Breach a steganography method need the invader to perceive that steganography has been worn.

Related Work

Nowadays, mostly images are used as wrap entity because images are recurrently exchange over email and other statement media. The main process to apply Steganography on images is LSB method which is describe underneath.

The LSB Technique:-

LSB is the most trendy Steganography technique. It hide the secret message in the RGB image based on it its twofold coding. Figure 2 present an paradigm about pixel values and show the secret message. LSB algorithm is worn to hide the secret messages by by means of the mention algorithm. LSB hiding technique hide the secret message directly in the least two significant bits in the image pixels, hence that influence the image resolution, which condense the image quality and make the image easy to attack. As well as this method is already has been attack and broken. Therefore a innovative technique that able to make the secret message more secure and enhance the quality of the image is proposed. The proposed method hides the secret message based on searching about the identical values between the secret messages and image pixels, see the picture below. The estimated method is used to hide the secret messages by using given algorithm.

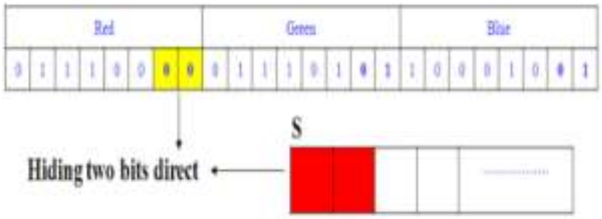
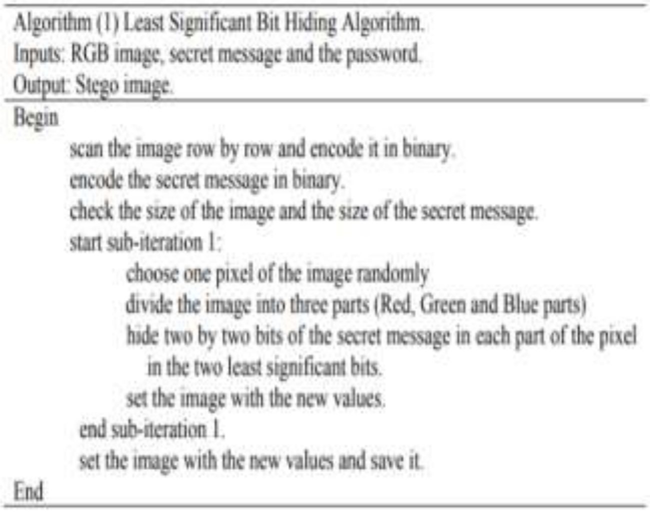


Figure (2) Least Significant Bit Hiding Technique



```
Algorithm (1) Least Significant Bit Hiding Algorithm.
Inputs: RGB image, secret message and the password.
Output: Stego image.
Begin
        scan the image row by row and encode it in binary.
        encode the secret message in binary.
        check the size of the image and the size of the secret message.
        start sub-iteration 1:
                choose one pixel of the image randomly
                divide the image into three parts (Red, Green and Blue parts)
                hide two by two bits of the secret message in each part of the pixel
                   in the two least significant bits.
                set the image with the new values.
         end sub-iteration 1.
         set the image with the new values and save it.
End
```

The projected method hides the secret message based on searching about the identical bits between the secret messages and image pixels values. The proposed method was compared with the LSB method for hiding the secret message which hide the secret message directly in the least two significant bits of the image pixels.

The proposed method is more efficient, simple, appropriate and accurate than LSB method, it search about the identical then start hiding, hence the change in the image resolution is quite low, as well as it makes the secret message more secure, , hence it will obtain a higher precision ratio as compare to LSB method.

The cover image in custom-made method will be of higher resolution.

The main terminologies used in the Steganography systems are: the cover message, secret message, secret key and embedding algorithm. The cover message is the transporter of the message such as image, video, audio, text, or some other digital media. The secret message is the information which is desirable to be hidden in the apposite digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the initiative that frequently use to embed the secret information in the cover message. In the Steganography system state of affairs, before the hiding process, the sender must select the apposite message carrier (i.e image, video, audio, text) and select the effectual secret messages as well as the robust password (which suppose to be known by the receiver). The valuable and suitable Steganography algorithm must be selected that able to instruct the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other fresh techniques. The Stego file is the carried message with the secret information. After receiving the message by the receiver, he can decipher it using the extract algorithm and the same password used by the sender.

Many carrier messages can be used in the latest technology, such as Image, text video and many others. The image file is the most well-liked used for this purpose because it easy to propel during the communication between the sender and receiver. The images are separated into three types: binary (Black- White), Gray scale and Red-Green-Blue (RGB) images.

The binary image has one bit value per pixel characterize by 0 for black and 1 for white pixels. While the gray scale image has 8 bits value per pixel characterize from 00000000 for black and 11111111 for white pixels. The RGB image has 24 bits values per pixel represent by (00000000, 00000000 and 00000000) for black and (11111111, 1111111 and 11111111) for white pixels.

The RGB image is the most appropriate because it contain a lot of information that help in hiding the secret information with a bit vary in the image resolution which does not affect the image eminence and make the message more secure. In this research paper the RGB images are used as a carrier message to hide the secret messages by the Least Significant Bit hiding method (LSB) as well as the projected method.

Modified Version

LSB Hiding technique directly hides the secret message in the least significant bit of the image pixels, hence that effect the image resolution, which resude the quality of the image and make it easy to be attacked.

As well as this method is already attacked and broken. Therefore a new technique that able to make the secret message more secure and enhance the quality of the image is proposed.

The proposed method hides the secret messages based on searching about the identical values between the secret messages and the image pixel. The following algorithm is utilized in implementing this method:

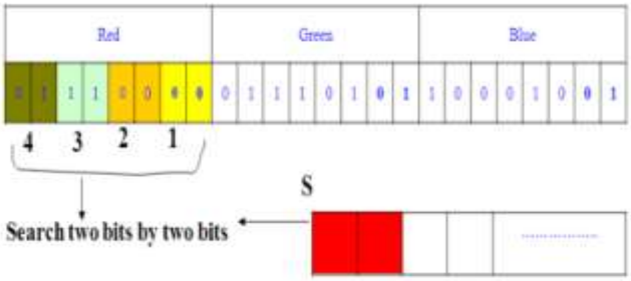


Figure 3:-

```
Begin
scan the image row by row and encode it in binary
encode the secret message in binary
check the size of image and size of secret message
start sub iteration 1:
choose one pixel of image randomnly
divide the image into RGB
hide two by two bits of secret message in each part of the pixel by searching about the identical
if the identical is satisfied set the image with new values
otherwise hide in the least significant bit and set image with new values
save the location of hiding bits in binary table
end sub iteration 1
set the image with the new values and save it
End
```

The modified version works on removing redundancy of changes of bits hence the size of image do not vary much. It also ensures the quality of image is maintained and preserved.

The changes done is saved in a binary table that can be used in a secret key to encrypt and decrypt the message The user should know this key in order to decrypt the secret code embedded in the image pixels. The quality of image is preserved as well its size is also not changed much thus reducing the risk of breaking the secrecy.

This proposed work adds to the motto of steganography which is not to give away the secret message of even the fact that image contains any secret message with in it..

Steganography In A Nutshell

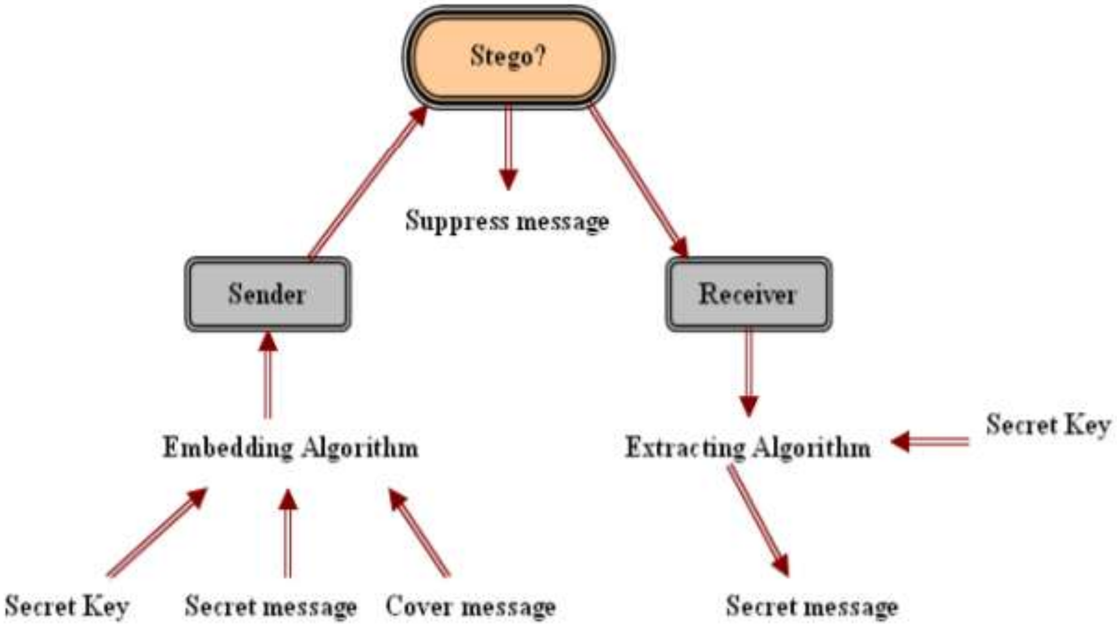


Figure 4

This is the purposeful diagram of Steganography and it explain various parts of a steganographic communication system in as slightest details as possible. A steganographic communication is principally divided into two sides:

1. Sender side
2. Reciever side

The sender writes a message to be sent in a safe manner . After that, he picks an image and uses the steganography tool to embed the message into the image. While liability that, the steganography tool generates a "Secret Key" which works as a password to unlock the message. This secret key should not be given to any illegal person and only the sender(s) and recipient(s) must have it in order to securely send and pull out data through an image. The reciever on receiving the encrypted image can effortlessly use the key and steganography tool to extract data and get the anticipated message. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that typically use to embed the secret information in the cover message. In the Steganography system circumstances, before the hiding process, the sender must select the apposite message carrier (i.e image, video, audio, text) and select the effectual secret messages as well as the robust password (which suppose to be known by the receiver). The effective and appropriate Steganography algorithm must be preferred that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other recent techniques. The Stego file is the carried message with the secret information. After receiving the message by the receiver, he can decipher it using the extract algorithm and the same password used by the sender.

Conclusion:-

We talked about Steganography and LSB method to employ it. There are innovative state-of-the-art technologies being developed and current technologies. The proposed method hides the secret message based on penetrating about the indistinguishable bits between the secret messages and image pixels values. The proposed method was compare with the LSB benchmarking method for hiding the secret message which hide the secret message unswervingly in the least two significant bits of the image pixels.

Acknowledgments:-

Our praises and obligations to the experts who have helped by providing us with their research material and authorities of IMSEC for providing the opportunity and for the valuable time they took out to guide us.

References:-

1. Atallah M. Al-Shatnawi " A New Method in Image Steganography with Improved Image Quality "Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 - 3915.
2. Vivek Jain,Lokesh Kumar,Madhur Mohan Sharma,Mohd Sadiq and kshitiz Rastogi Volume 3,No.4,April 2012 " Public Key Steganogtraphy based on modified LSB method" Journal of Global Research in Computer Science.
3. Silman,J.,"Steganography and Steganalysis: An Overview", SANS Institute,2001.
4. Williams Stallings (2006) "Cryptography and Network Security Fourth edition"
5. C.E., Shannon,(1949),Communication theory of secrecy systems, Bell System Technical Journal,28,656-715.
6. Dunbar,B.,"Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002