KNOWLEDGECUDDLE PUBLICATION

International Journal of Computer Engineering and Sciences(IJCES) Volume-1 Issue-2, 2015

Image Steganography Techniques

Ravi K Sheth
Assistant Professor (IT)
Raksha Shakti University
Ahmedabad

Rashmi M. Tank
M.E.(C.E.), student
B.V.M.Engineering College
V V Nagar

***Abstract*— Steganography is the technique of hiding the fact that communication is taking place, by hiding data in other data. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques. Steganalysis, the detection of this hidden information, is an inherently difficult problem.In this paper,I am going to cover different steganographic techniques researched by different researchers.**

Keywords — Cryptography, Steganography, LSB, Hash-LSB, RSA Encryption –Decryption

I. INTRODUCTION

Steganography is widely used techniques that manipulate information in order to hide their existence. Steganography is the art and science of communicating in a way which hides the existence of the communication. Though Steganography provides good security,it can be combined with Cryptography for better confidentiality and security. The aim of this paper is to describe different methods for Steganography and also methods for integrating together cryptography and steganography through some media such as image, audio, video, etc.

II. HISTORY

The history of Steganography can be traced back from 440 B.C

1) Wax Tablets: In ancient Greece, people wrote secret messages on wood and then covered it with Wax.

Fig.1 Wax Tablets

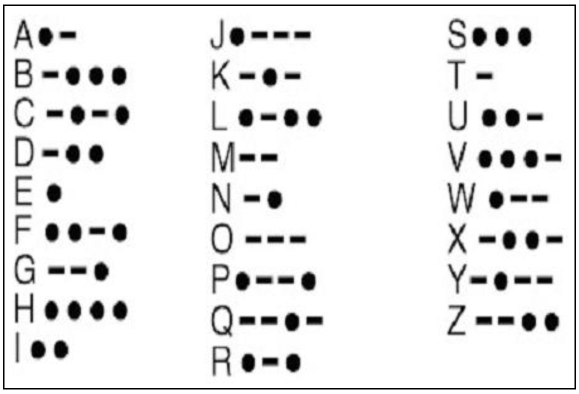
2) Shove Heads: This was also used back in ancient Greece. Slave’s heads were shove and secret messages were written on the scalp. Then, the slave’s hair was allowed to grow and the secret message was exposed to the recipient after shaving the head again. Fig.2 Shove head with the secret message

Figure 2

3) Invisible Ink: Secret messages were written using invisible ink which became visible only when the paper carrying the message was heated. Liquids such as milk, vinegar and fruit juices were used as invisible inks.

Figure 3

4) Morse code: Secret messages were written in Morse code on the knitting yarn. A cloth was made out of the yarn which was worn by the carrier. Also, Jeremiah Denton blinked his eyes in Morse code to spell the word ―Torture‖ in a Television conference. This ensured the US Military that American POWs were tortured in North Vietnam.



A	•–
B	–•••
C	–•–•
D	–••
E	•
F	••–•
G	––•
H	••••
I	••
J	•–––
K	–•–
L	•–••
M	––
N	–•
O	–––
P	•––•
Q	––•–
R	•–•
S	•••
T	–
U	••–
V	•••–
W	•––
X	–••–
Y	–•––
Z	––••

Figure 4

III. STEGNOGRAPHY MODEL

Basic Steganography model consists of secret message, cover message, secret key and embedding algorithm.

1) Secret Message: The secret message is information which needs to be hidden into some suitable digital media.

2) Cover Message: It is the carrier of message such as image, audio, video or other digital media.

3) Stego Key: It is used to embed message depending on the hiding algorithm. Embedding algorithm is the method of embedding the secret message into the cover. The cover-object with the secretly embedded message is then called the Stego-object. Steganography process basically consists of encoding at the sender end to obtain the StegoImage and decoding at the receiver end to provide the secret or private information. Fig.5 Steganography Encoding and Decoding

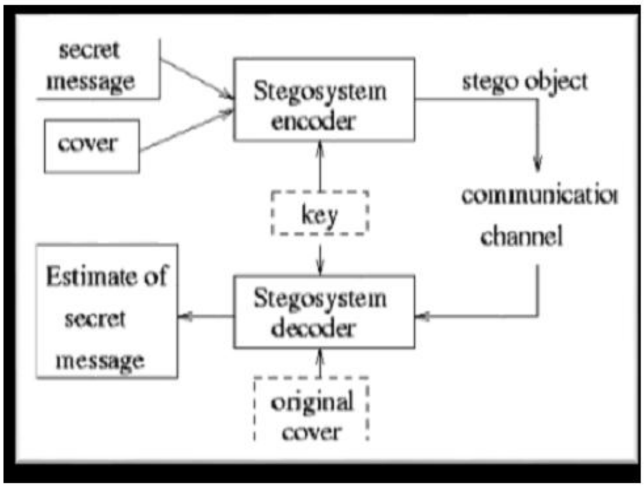


Figure 5

4) Encoding: The secret text message is encrypted using an encryption key.

5) Decoding: The Stego-Image is fed into the decoder which uses a decryption algorithm to provide the original cover and the secret message as output.

IV.CATAGORIES OF STAGNOGRAPHY

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain. Image – also known as spatial domain techniques embed messages in the intensity of the pixels directly, Transform – also known as frequency domain, images are first transformed and then the message is embedded in the image . Many carrier messages can be used in the recent technologies, such as Image, text video and many others. The image file is the most popular used for this purpose because it easy to send during the communication between the sender and receiver. The images are divided into three types: binary (Black- White), Gray scale and Red-Green-Blue (RGB) images. The binary image has one bit value per pixel represent by 0 for black and 1 for white pixels. While the gray scale image has 8 bits value per pixel represent 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 suitable because it contains a lot of information that help in hiding the secret information with a bit change in the image resolution which does not affect the image quality and make the message more secure. In this research paper the RGB images are used as a carrier message to hide the secret messages. There are various methods of steganography:

- Least significant bit (LSB) method
- Transform domain techniques
- Statistical methods
- Distortion techniques
- Hash-LSB and RSA algorithm

1) **Least significant bit (LSB) method :**

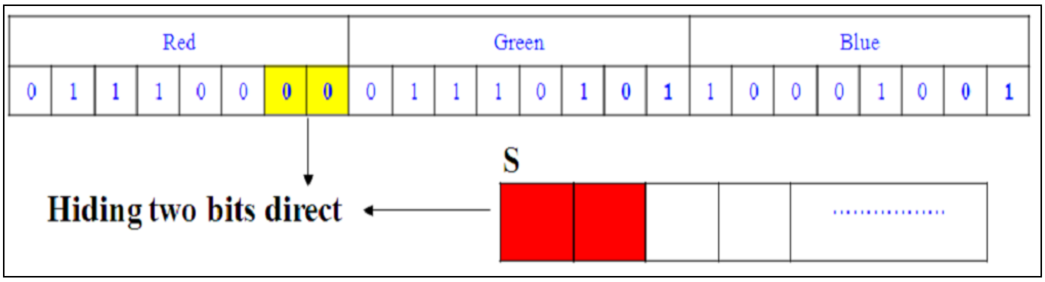


Figure 6

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:
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

2) **The proposed method**

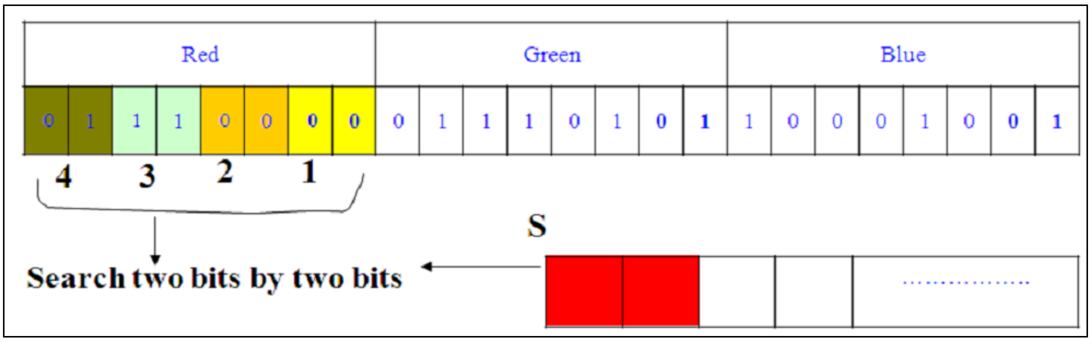


Figure 7

Algorithm (2) the Proposed 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 by searching about the identical. If the identical is satisfied then set the image with the new values. otherwise hide in the two least significant bits and set the image with the new values save the location of the hiding bits in binary table.
End sub-iteration 1.
Set the image with the new values and save it.
End

3) Hash-LSB and RSA algorithm

A. Cover Image and Secret Message:

In our proposed system, first of all we select a true color image of size 512 x 512 for to it as a cover image and a secret message which will be embedded in the cover image.

B. B. Hash-LSB (Least Significant Bit) Process

The Hash based Least Significant Bit (H-LSB) technique for steganography in which position of LSB for hiding the secret data is determined using hash function. Hash function finds the positions of least significant bit of each RGB pixel's and then message bits are embedded into these RGB pixel's independently. Then hash function returns hash values according to the least significant bits present in RGB pixel values. The cover image will be broken down or fragmented into RGB format. Then the Hash LSB technique will uses the values given by hash function to embed or conceal the data. In this technique the secret message is converted into binary form as binary bits; each 8 bits at a time are embedded in least significant bits of RGB pixel values of cover image in the order of 3, 3, and 2 respectively. According to this method 3 bits are embedded in red pixel LSB, 3 bits are embedded in green pixel LSB and 2 bits are embedded in blue pixel LSB as illustrated in Fig. 2. These 8 bits are inserted in this order because the chromatic influence of blue color to the human eye is more than red and green colors. Therefore the distribution pattern chooses the 2 bits to be hidden in blue pixel. Thus the quality of the image will be not sacrificed. Following formula is used to detect positions to hide data in LSB of each RGB pixels of the cover image.
$k = p \% n$ ………..……………..…… (1)
Where, k is the LSB bit position within the pixel; p represents the position of each hidden image pixel and n is the number of bits of LSB which is 4 for the present case. After embedding the data in cover image, a stego image will be produced. The recipient of this image has to use the hash function again to extract the positions where the data has been stored. The extracted information will be in cipher text. After decryption of it, combining of bits into information will produce the secret message as required by the receiver.

C. C. RSA Encryption and Hash-LSB Encoding

This approach of image steganography is using RSA encryption technique to encrypt the secret data. After encryption Hash-LSB method is applied on ciphertext. D. Hash-LSB Decoding and RSA Decryption
Retrieval Algorithm:
Step 1: Receive a stego image.
Step 2: Find 4 LSB bits of each RGB pixels from stego image.
Step 3: Apply hash function to get the position of LSB's with hidden data.
Step 4: Retrieve the bits using these positions in order of 3, 3, and 2 respectively.
Step 5: Apply RSA algorithm to decrypt the retrieved data.
Step 6: Finally read the secret message.
The objective of the work have been implemented an image steganography technique using Hash-LSB (Least Significant Bit) method with RSA algorithm to improve the security of the data hiding technique.

4) Blow-fish Encryption-LSB Steganography

Method: It first encrypts data using Blow-fish Encryption algorithm and then applies LSB steganography method on it.

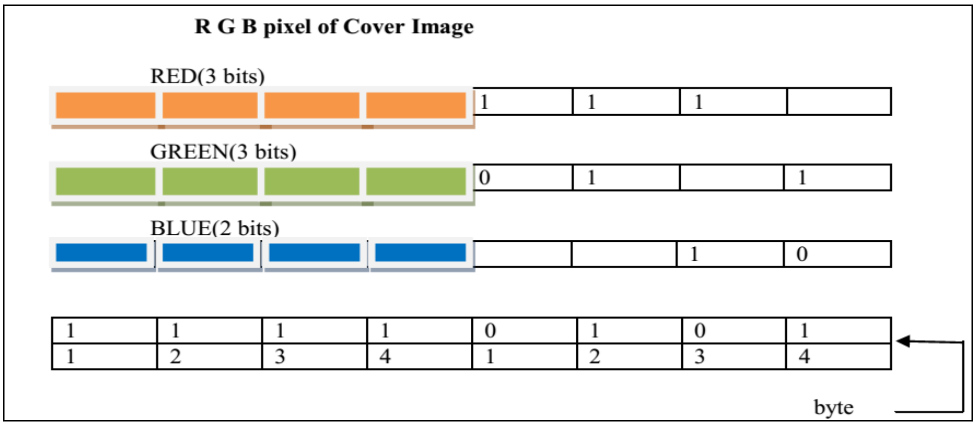


Figure 8

V. CONCLUSION

Steganography is the art and science of communicating in a way which hides the existence of the communication. Though Cryptography gives good security, the attacker can come to know that communication is taking place. But in Steganography, attacker does not have any knowledge of communication. The information can be revealed in such cases in which attacker knows that information is hidden in cover text, video, image etc. Therefore security of steganography can be increased by combining it with cryptographic techniques. For future research in steganography can be doneUsing image processing techniques such as edge detection algorithm.

REFERENCES:

[1] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain ―A New Approach for LSB Based Image Steganography using Secret Key‖, International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.
[2] Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, ―Hash Based Least Significant Bit Technique for Video Steganography (HLSB)‖, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.
[3] Mamta Juneja, Parvinder Singh Sandhu, ―Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption‖, International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 – 305, 27-28 Oct., 2009.
[4] B. Dunbar. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment, Sans Institute, 1(2002).
[5] C. Christian. An Information-Theoretic Model for Steganography, Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science. 1998.
[6] H. Wu, H. Wang, C. Tsai and C. Wang, Reversible image steganographic scheme via predictive coding. 1 (2010), ISSN: 01419382, 35-43.
[7] Ajit Singh, Aarti Nandal, Swati Malik ―Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security ―IJARCSSE Dec,2012
[8] Atul Kahate (2009), Cryptography and Network Security, second edition, McGraw-Hill.
[9] Vijay Kumar Sharma ,Vishal Shrivastav‖ A steganography algorithm for hiding image in image by improved LSB substitution by minimize detection ―Journal of Theoretical and Applied Information Technology 15th February 2012.
[10] Owens, M., A discussion of covert channels and steganography, SANS Institute, 2002
[11] ohnson, N.F. & Jajodia, S., Steganalysis of Images Created Using Current Steganography Software, Proceedings of the 2nd Information Hiding Workshop, April 1998
[12] Venkatraman, S., Abraham, A. & Paprzycki, M., Significance of Steganography on Data Security, Proceedings of the International Conference on Information Technology: Coding and Computing, 2004