Steganography: Implementation on hidden data in a Digital Image

Akhil K.I[#] , Nausheeda B.S[*]

Dept. of MSc Software Technology, AIMIT, St. Aloysius College, Mangalore, India

* Assistant Professor, Dept of M.Sc Software Technology, AIMIT, St. Aloysius College, Mangalore, India

ABSTRACT: The major development of the data transfer throughout the internet has made it easy to send the data from source to destination. There are different methods to send the data such as email, but in this emails can be easily hacked and can misuse the confidential data. Since the data can be easily hacked, we found out the different method to send the data in a secure way by using the cryptography and steganography. Here in this we are using an image and encrypting some data and sending that image to the particular destination and that receiver will decrypt the image and retrieve the text message which was encrypted in that image. Data is sent in a format if the data is stolen but the third party will only retrieve the image but not the text message which was encrypted.

KEYWORDS: Cryptography; Steganography; Least Significant bit; RSA

I. INTRODUCTION

In this modern world the technologies have improved so much that most the people and children use internet to send the data from source to destination because they think that it is an easier way to send and it is much secured enough. But one of the main disadvantage is the security of the data were the some confidential information can be easily stolen without knowing to sender or receiver. Therefore it is very important to necessary issues before the data is transferred. Here in this an algorithm is designed to hide all the data inputted on the image for privacy of the data. Once this is done user can send the data steganography image to receiver is able to retrieve and read the data which is hidden in the steganography image by using the same proposed system. Thus, the data can be protected without revealing the contents to other people. But the while sending the message the sender should encrypt the code by using the password and that password should be known to the receiver so that he could decrypt the content which is there in that image. Steganography is called as a covered writing was for sending the secret message it uses the image to send to the receiver. And this technique is one of the secured ways for sending the messages. This technique instead of sending the image we can use Mp3, Video etc. Figure of Steganography process shown below.
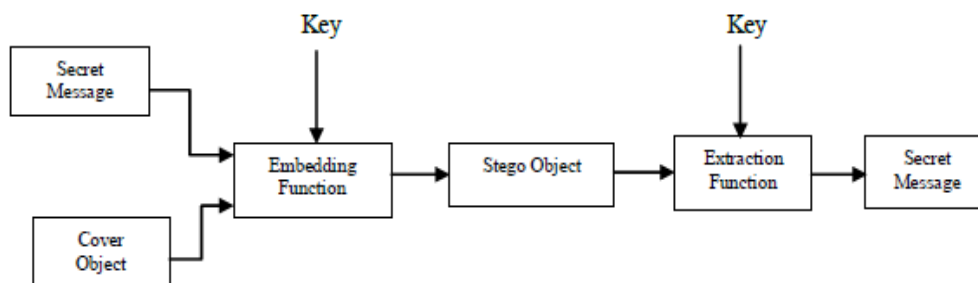
Steganography and Cryptography

Steganography is a method which is used to transmit a secure message from the source to a receiver such that the third person does not come to know that any message is been transmitted. Steganography can be done by inputting the secret message inside the digital media that is an image [5]. The word steganography comes from a Greek which means "concealed writing" and the Greek words steganos means "covered or protected" and graphie means "writing" [2]. This

technique is used to hide message which cannot be seen it is highly secure method for the sending the secret message. To use this technique there are different methods such as
1. Transform domain technique
2. Statistical methods
3. Distortion technique
4. (LSB) Least significant bit method

Cryptography is one of the best method which has come from the rages and still it is been used till date. In this paper there is an essential for transferring the data. Cryptography comes from a Greek word means secret. Cryptography is separated into two words that are cryptosystems which is used for coding and decoding the data. This method which includes:
1. Encryption and decryption algorithm
2. Integrity check function

II. RELATED WORK

Y. K. Jain and R. R. Ahirwal [1] authors have proposed Least Significant technique to embed the message in a image. Thus after embedding the message a steganography key is generated. This key is has a different layers in a image and every layer has a fixed number of bits which is embedded in a least significant image. This technique is very important to hide the message in a bit format in image. The main disadvantage is that we cannot hide the extra bit of text in a image were already the message is stored in a image. Mohmmad A.Ahmed et al. [2] proposed a method where the data or text message can be hidden inside digital image by Least Significant Bit technique and implementing the data or text message in a format then the digital image will be implemented in Hash Significant technique to get the result in hashing value. El-Emam [3] author proposed a image which the message hidden by bit technique. Were the message is stored in form of a pixels. Therefore these pixels can called in order to retrieve the hidden message inside the image. For these encrypting and decrypting the data we use a steganography in order to hide and retrieve the message. Akhtar, N.; Johri, P.; Khan, S., [4] implemented a variation of plain Least Significant algorithm. This technique was to improve the digital image which the message is hidden. This was to cover the image pixels instead of storing it in sequence order.Thus making the hackers or any unauthorized person to retrieve the message in a digital image. This shows a good enhancement to least significant technique to secure the digital image quality.

III. WORKFLOW

A. *RSA Algorithm*
RSA Algorithm uses a encrypt cryptosystem where it uses two prime numbers at the first stage and the results of the values is used as a key such as private and public key where at end the process we uses this key as encryption and decryption of the messages. Here RSA Algorithm used when embedding the original image into the cipher text. Thus by using this algorithm the messages are highly secured. At end of the process the steganalysis only the cipher text can detached which the messages are in the encrypted format but it cannot be readable.
Embedding Algorithm:
Begin
Step 1: Select the Image and a text.
Step 2: Encrypt the text by using RSA algorithm.
Step 3: Select any 4 LSB bits for each image pixels.
Step 4: Use hash function on LSB image to get the position.
Step 5: Insert the bits of encrypted message into 4 bits of LSB of RGB pixels of cover image in the order of 3, 3 and 2 respectively using the position obtained from hash function given in equation 1.
Step 6: Send steganography image to receiver.
End

B. *Least Significant Bit (LSB) Insertion Method*
One of the most common techniques used in steganography today is called least significant bit (LSB) insertion. Also called LSB (Least Significant Bit) substitution and it is the process of adjusting the least significant bit pixels of

the carrier image. It is a simple approach for embedding message into the image. In this method some information from the pixel of the carrier image is replaced with the message information so that it can't be observed by the human visual system, therefore it exploits some limitations of the human visual system. The Least Significant Bit insertion varies according to number of bits in an image [16]. For an 8-bit image, the least significant bit i.e. the 8th bit of each byte of the image will be changed by the 1-bit of secret message. For 24 bit image, the colours of each component like RGB (red, green and blue) will be changed. LSB steganography involves the operation on least significant bits of cover image, audio or video. The least significant bit is the lowest bit in a series of binary number [16]. In LSB substitution the least significant bits of the pixels are displaced by the bits of the secret message which gives rise to an image with a secret message embedded in it. The method of embedding differs according to the number of bits in an image (different in 8 bit and 24 bit images).

Extracting Algorithm:

Begin

Step1. Select the steganography image.

Step2. Select the folder in which you want to extract the hidden text file.

Step3. Apply the security key.

Step4. Convert the binary file into human readable form.

End

IV. CONCLUSION AND FUTURE WORK

It is new way to send the secret message to the receiver were after encrypting the message the image look the same as original image but it makes bits different. And this new way make more secure in sending the messages to other in a secured way. For this we use a cryptography which increases the security of the message and it is not easy to crack the message without the key were the key is to decode the message inside the image. This technique a very usable and trustworthy to send information in an unsecured internet without connecting to virtual private network internet. The future scope is to send the hidden message in 3D image.

REFERENCES

1.   Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, (2010) March 1.
2.   Mohammad A. Ahmad, Dr. Imad Alshaikhli, Sondos O. Alhussainan, "Achieving Security for Images by LSB and MD5", Journal of Advanced Computer Science and Technology Research, Vol. 2, Issue No.3, Pages No. 127-139, Sept., 2012.
3.   N.N. El-Emam, Hiding a large amount of data with highsecurity using steganography algorithm, Journal of Computer Science 3 (2007) 223-232.
4.   Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on , vol., no., pp.385,390, 27-29 Sept. 2013.
5.   Ankit Chaudhary, J. Vasavada, J. L. Raheja, S. Kumar, M. Sharma, "*A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images*", 22nd International Conference on Computer Graphics and Vision, 2012.