IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. IV (Jan – Feb. 2016), PP 39-43
www.iosrjournals.org

A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique

Rituparna Halder, Susmit Sengupta, Sudipta Ghosh, Debashish Kundu
ESL, Dumdum Lab, Salt Lake City, Kolkata - 700064

***Abstract**: Steganography is a method of hiding secret messages in a cover object while communication takes place between sender and receiver. Security of confidential information has always been a major issue from the past times to the present time. It has always been the interested topic for researchers to develop secure techniques to send data without revealing it to anyone other than the receiver. Therefore from time to time researchers have developed many techniques to fulfill secure transfer of data and steganography is one of them. In this paper we have proposed a new technique of image steganography i.e. Hash-LSB with RSA algorithm for providing more security to data as well as our data hiding method. The proposed technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. This technique makes sure that the message has been encrypted before hiding it into a cover image. If in any case the cipher text got revealed from the cover image, the intermediate person other than receiver can't access the message as it is in encrypted form.*

***Keywords;** Cryptography, Steganography, LSB, Hash-LSB, RSA Encryption –Decryption*

I. Introduction

The basic need of every growing area in today’s world is communication. Everyone wants to keep the inside information of work to be secret and safe. We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a certain level it's not safe. Steganography and Cryptography are two methods which could be used to share information in a concealed manner. Cryptography includes modification of a message in a way which could be in digesting or encrypted form guarded by an encryption key which is known by sender and receiver only and without using encryption key the message couldn’t be accessed. But in cryptography it’s always clear to intermediate person that the message is in encrypted form, whereas in steganography the secret message is made to hide in cover image so that it couldn’t be clearer to any intermediate person that whether there is any message hidden in the information being shared. The cover image containing the secret message is then transferred to the recipient. The recipient is able to extract the message with the help of retrieving process and secret key provided by the sender. A model of the steganographic process with cryptography is illustrated in Fig. 1.

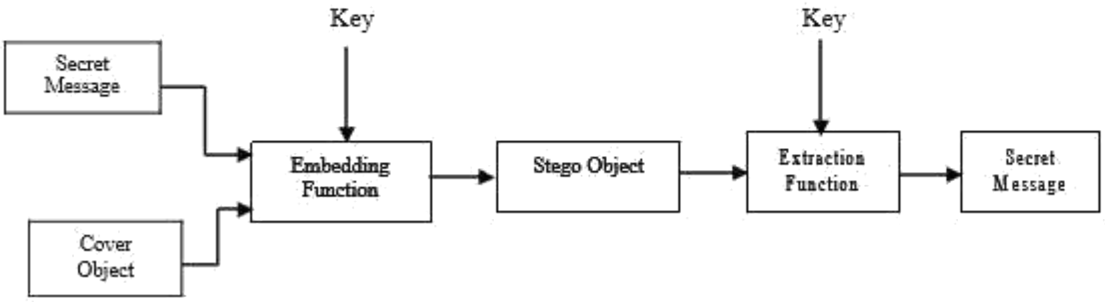


Fig. 1 A model of the steganographic process with cryptography

II. Cryptography

The field of cryptography has a rich and important history, ranging from pen and paper methods, to specially built machines, to the mathematical functions that are used today. In this paper only brief discussion that is essential for knowledge transfer has been presented. Cryptology is the science of coding and decoding secret messages. (Cryptology is the Greek root for secret or hidden) [27]. It is usually divided into cryptography, which concerns designing cryptosystems for coding and decoding messages. It states that the term cryptography generally refers to the collection of cryptographic mechanisms that include:

- Encryption and decryption algorithms
- Integrity check functions
- Digital signature schemes B. Steganography

Steganography is a technique used to transmit a secret message from a sender to a receiver in a way such that a potential intruder does not suspect the existence of the message. Generally this can be done by embedding the secret message within another digital medium such as text, image, audio or video. [19]. The word steganography is of Greek origin and means “concealed writing” from the Greek words steganos meaning “covered or protected”, and graphie meaning “writing”
[2]. The first recorded use of the term was in 1499 by Johannes Trithemius in his Stegano-graphia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other “cover-text” and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. It is a high security technique for long data transmission. There are various methods of steganography:

- Least significant bit (LSB) method
- Transform domain techniques
- Statistical methods
- Distortion techniques II. Related Work

There are many steganography techniques which are capable of hiding data within an image. These techniques can be classified into two categories based on their algorithms: (1) spatial domain based techniques; (2) transform domain based techniques [14]. The spatial domain based steganography technique use either the LSB or Bit Plane Complexity Segmentation (BPCS) algorithm [22]. The most widely used technique to hide data is the usage of the LSB [6]. The existing techniques are mainly based on LSB (Least Significant Bit) where LSBs of the cover file are directly changed with message bits. A significant number of methods have been proposed for LSB steganography [1], [2], [3], [4], [9], [11], [13], [17], [18], [19], [23]. Masud et al. [1] has proposed a LSB technique for RGB true color image by enhancing the existing LSB substitution techniques to improve the security level of hidden information. In [3], [4], [21], [23] and [25] designing of robust and secure image steganography based on LSB insertion and RSA encryption technique has been used. In [9] proposed a LSB matching revisited image steganography and edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. Mohmmad A.Ahmed et al. [17] proposed a method in which a message hidden inside an image by using the Least Significant Bit technique and after creation of the hidden message, the image will pass it in hash function to obtain hashing value using the MD5 technique. In [18] two steganography technique proposed for hiding image in an image using LSB method for 24 bit color images. In [19] a hash based approach proposed for secure keyless steganography in lossless RGB images that an improved steganography approach for hiding text messages in lossless RGB images. The paper [5], [8], [16], and [20] provides an overview of image steganography, its uses and analysis of various steganography techniques. In [15] a security analysis on spatial domain steganography for JPEG decompressed images has been presented. Anderson and Petitcolas [10] posed many of the open problems resolved in this article regarding to steganography. In particular, they pointed out that it was unclear how to prove the security of a steganographic protocol. They also posed the open question of bounding the bandwidth that can be securely achieved over a given cover channel.

Video steganography of late has also gained quite significance for researchers. Various techniques of LSB exist to implement video steganography [2], [7]. In [2] a hash based least significant bit technique for video steganography has been proposed. Where the secret information is embedded in the LSB of the cover frames and a hash function is used to select the position of insertion in LSB bits. In paper [7] proposes a secure covert communication model based on video steganography which is based on pixel-wise manipulation of colored raw video files to embed the secret data.

III. Existing Techniques Used

There are a large number of cryptographic and steganographic methods that most of us are familiar with. The most widely used two techniques are:

- RSA Algorithm
- LSB Insertion Method

A. RSA Algorithm

The algorithm was given by three MIT's Rivest, Shamir & Adleman and published in year 1977.

RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and then the product of these values is used to create a public and a private key, which is further used in encryption and decryption. The RSA algorithm could be used in combination with Hash-LSB in a way that original text is embedded in the cover image in the form of cipher text. By using the RSA algorithm we are increasing the security to a level above. In case of steganalysis only cipher text could be extracted which is in the encrypted form and is not readable, therefore will be secure.

RSA algorithm procedure can be illustrated in brief as follows [28]:

(i) Select two large strong prime numbers, p and q. Let $n = p\, q$.
(ii) Compute Euler's totient value for n: $f(n) = (p - 1)(q - 1)$.
(iii) Find a random number e satisfying $1 < e < f(n)$ and relatively prime to $f(n)$ i.e., $\gcd(e, f(n)) = 1$.
(iv) Calculate a number d such that $d = e-1 \bmod f(n)$.
(v) Encryption: Given a plain text m satisfying $m < n$, then the Cipher text $c = me \bmod n$.
(vi) Decryption: The cipher text is decrypted by $m = cd \bmod n$.

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 colors 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).

IV. Problem Formulation and Work Methodology

The problem statement consists of embedding the secret message in the LSB of each RGB pixels value of the cover image. Before embedding the secret message have to be converted to cipher text using RSA algorithm to enhance the secrecy of the message. In this approach we implemented a technique called Hash-LSB derived from LSB insertion on images. In this Hash-LSB, we are using a hash function to evaluate the positions where to hide the data bits or to be embedded. It is a challenging process which will lead us to combine the two technologies, one of them is RSA algorithm from cryptography and other is Hash-LSB from steganography. Our research has focused on providing a solution for transferring and sharing important data without any compromise in security. All the reputed organizations while sending business documents over the internet always use encryption of the data to protect leakage of information about their organization from their rivals or intruders. We have used Hash-LSB and RSA algorithm to create a secure steganography algorithm which is far more secure than many systems being used for the purpose of secretly sending the data.

A. Cover Image and Secret Message

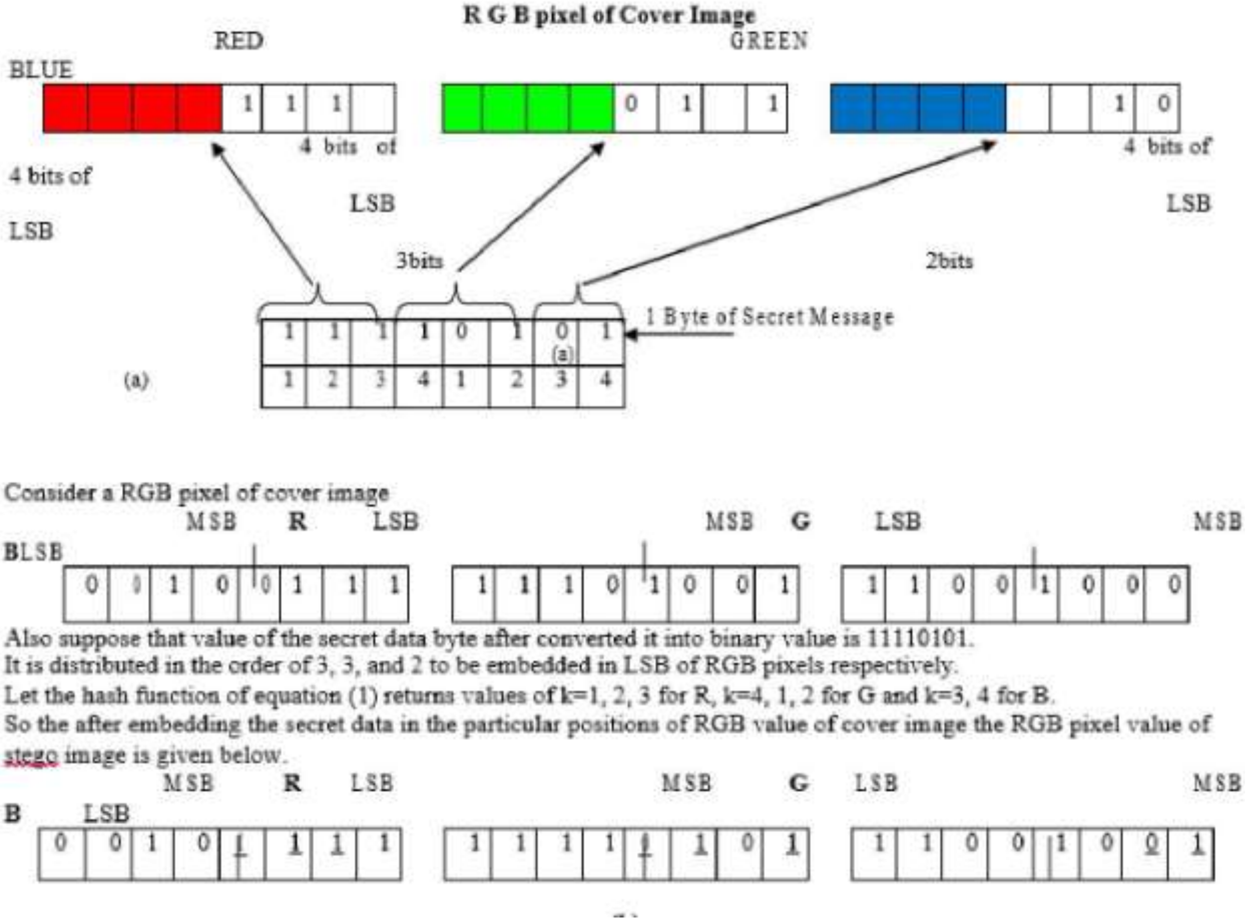
In our proposed system, first of all we select a true color image of size 512 x 512 for to it as a cover image and a secret message which will be embedded in the cover image.

B. 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 [2].

$k = p \% n$ ………..………….…… (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.



1	1	1	1	0	1	0	1
1	2	3	4	1	2	3	4

Consider a RGB pixel of cover image

MSB R LSB MSB G LSB MSB B LSB

0	0	1	0	0	1	1	1
1	1	1	0	1	0	0	1
1	1	0	0	1	0	0	0

Also suppose that value of the secret data byte after converted it into binary value is 11110101.
It is distributed in the order of 3, 3, and 2 to be embedded in LSB of RGB pixels respectively.
Let the hash function of equation (1) returns values of k=1, 2, 3 for R, k=4, 1, 2 for G and k=3, 4 for B.
So the after embedding the secret data in the particular positions of RGB value of cover image the RGB pixel value of stego image is given below.

MSB R LSB MSB G LSB MSB B LSB

0	0	1	0	1	1	1	1
1	1	1	1	1	1	0	1
1	1	0	0	1	0	0	1

C. RSA Encryption and Hash-LSB Encoding

This approach of image steganography is using RSA encryption technique to encrypt the secret data. Encryption includes a message or a file encryption for converting it into the cipher text. Encryption process will use recipient public key to encrypt secret data. It provides security by converting secret data into a cipher text, which will be difficult for any intruder to decrypt it without the recipient private key. At the start of this process we take cipher text encrypted from the secret message to be embedded in the cover image. In this process first we converted cipher text into binary form to convert it into bits. Then by using hash function it will select the positions and then 8 bits of message at a time will be embedded in the order of 3, 3, and 2 in red, green and blue channel respectively. The process is continued till entire message of bits will got embedded into the cover image [2].

Embedding Algorithm:
Step 1: Choose the cover image & secret message. Step 2: Encrypt the message using RSA algorithm.
Step 3: Find 4 least significant bits of each RGB pixels from cover image. Step 4: Apply a hash function on LSB

of cover image to get the position.

Step 5: Embed eight bits of the 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 stego image to receiver.

D. Hash-LSB Decoding and RSA Decryption

In the decoding process we have again used the hash function to detect the positions of the LSB's where the data bits had been embedded. When the position of the bits had been specified, the bits are then extracted from the position in the same order as they were embedded. At the end of this process we will get the message in binary form which again converted into decimal form, and with same process we got the cipher text message. After retrieving the positions of LSB's that contain secret data, the receiver will decrypt secret data using RSA algorithm. To apply RSA algorithm receiver will use his/her private key because the secret data have been encrypted by recipient public key. Using receiver private key cipher text will be converted into original message which is in readable form.

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.

V. Performance Analysis and Results

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. This technique is a combination of one steganographic technique and one cryptographic technique which enhances the security of data and data hiding technique. Our implemented Hash-LSB technique on images is used to hide information in the RGB pixels value of the cover image in the form of 3, 3, and 2 bit order and positions to hide the data bits have been calculated by hash function. The use of RSA algorithm has made our technique more secure for open channel. RSA algorithm has been used with Hash-LSB so that the original text will be embedded into cover image in the form of cipher text. The Hash-LSB technique has been evaluated and graphically represented on the basis of two measures are – Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) and obtained values are much better than existing techniques. The technique called

"A Secure Steganography Based on RSA Algorithm and Hash-LSB Technique" has been implemented on MATLAB tool by analyzing four color images of size 512 x 512 tiff format as selected to hide a fixed size of secret data. In this process stego-image is generated using Hash-LSB and RSA encryption which carried out to enhance the security of hidden data.

VI. Conclusion and Future Scope

A secured Hash based LSB technique for image steganography has been implemented. An efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through Hash-LSB method. In this work, a new way of hiding information in an image with less variation in image bits have been created, which makes our technique secure and more efficient. This technique also applies a cryptographic method i.e. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that's why we used in this technique to increase the security of the secret message. A specified embedding technique uses hash function and also provide encryption of data uses RSA algorithm; makes our technique a very much usable and trustworthy to send information over any unsecure channel or internet. The H-LSB technique have been applied to.tiff images; however it can work with any other formats with minor procedural modification like for compressed images. Performance analysis of the developed technique have been evaluated by comparing it with simple LSB technique, which have resulted a very good MSE and PSNR values for the stego images. The future scope for the proposed method might be the development of an enhanced steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly the steganography technique can be developed for 3D images. The further work may contain combination of this method to message digesting algorithms.