Review on Steganography with RSA using LSB and Hash LSB techniques

Vipul Negi[1], Supreet Kaur[2], Lisa Gopal[3]
[1,2] Master of Computer Application Student, UIM, Uttaranchal University, Dehradun, India
[3] Assistant Professor, Computer Science, UIM, Uttaranchal University, Dehradun, India

Abstract: Steganography is a practice of embedding confidential messages within another image, file or video while the sender and receiver communicates with each other. In present world, the safety of confidential information and privacy of communication has been a major issue. To resolve these issues of confidentiality and privacy in communication, researchers have been working to develop techniques to send data that are more secure without revealing it to anyone but the receiver. Over the past years, steganography is one of the technique that has been used to communicate securely between sender and receiver. The steganography method of LSB (Least Significant Bit) is the most utilized method for concealing the information in the bits of a picture. In this method, the data bit replaces the right most bit of an image changing the values of color components, like RGB(RED, GREEN, BLUE), of the image. This LSB method is vulnerable to stegnalysis, a new method is introduced of digital steganography by adding Hash function to LSB, it makes our data hiding method more secure. The HASH function is used to create pattern for concealing the message bits in the LSB of color components of each pixel of the selected picture. To make the steganography more secure, the RSA encryption is added to the steganography method, as it makes our data more secure.
Keywords : Cryptography, Steganography, LSB, Hash-LSB, RSA Encryption -Decryption

Introduction

In today's world communication plays an important role to enhance growth in any aspect. The confidential information of work needs to be kept safe and secure. The need for privacy and security in communication has increased, due to the intrusion of computer technology in our daily life and it's recent advances. For transferring and sharing information many insecure pathways, such as internet and telephonically, are used which at a certain level are not safe. Steganography is one of the method which could be used to share information confidentially. In steganography, the data is concealed in the selected picture with the goal that no intermediate person can determine that, whether the message being transmitted consists any confidential information or not. The recipient receives the picture with confidential information concealed in it. With the assistance of the recovering procedure the beneficiary extracts the message from the picture.

A. Steganography

Steganography is a technique by which sender transmits a secret message to the receiver in a way such that any presence of confidential information isn't suspected by a potential intruder. Generally, by inserting the confidential information within another digitized medium such as picture, audio or video, the steganography is achieved. [4]. The word steganography is of Greek beginning and signifies "disguised composition" from the Greek words steganos signifying "secured or ensured", and graphie signifying "stating" [1]. Generally, information appears to be random images, audio or video, the concealed information is imperceptible ink between the obvious message of a private letter. For long data transmission, it is a highly secure method.

Steganography methods discussed in this paper:
· Least significant bit (LSB) method
· Hash - Least significant bit (LSB) method

A. Least significant bit (LSB) method

This is a basic methodology. In this strategy the confidential information's bits replaces the LSB of a few or every bytes of the picture. Using this strategy the data cannot be viewed by the human visual system, along these lines it misuses the restriction of the human visual system. Based on the bits number in a picture, the insertion of LSB is also differ [3].

B. Hash – LSB

This approach is similar to the least significant bit method but to make LSB more secure, it is combined with the HASH function. Hash function generates a pattern in LSB of cover images and determines the position where the data bits will be embedded.

The study of perceiving hidden information by the methods of steganography is called Steganalysis. The method of Least Significant Bit is risked to Steganalysis, therefore to make it more secure we cipher the information with RSA encryption before embedding it into the image bits.

RSA Algorithm

The algorithm was proposed by Rivest, Shamir & Adleman and published in the year 1977. It is a cryptosystem for encrypting information in which initially two prime numbers are taken and a open and a private open key is generated using the product of these two prime numbers, which is then used in ciphering and deciphering. The RSA algorithm in combination with Hash-LSB could be used, the original information will be encrypted to cipher text before being embeded in the selected picture. By using this encryption process the steganography process is made more secure. In case of Steganalysis, the intruder will only have access to the cipher text which is the encrypted form of the secret message and hence it will not be readable, therefore it is secure [2].

Algorithm for RSA Encryption

(I) Pick two prime values, a and b. Let n = a * b.
(ii) calculate n: f (n) = (a - 1) (b – 1), Euler's totient value.
(iii) Locate an irregular integer e satisfying 1 < e < f (n) and generally prime to f (n) i.e., gcd (e, f (n)) = 1.
(iv) Calculate d such that d = e-1 mod f (n).
(v) Encryption: Find m satisfying m < n, at that point the Figure content c = m e mod n.
(vi) Decoding: Decipher by m = c d mod n.

Proposed Work

The problem statement consists of embedding the LSB of each RGB pixels value of the selected picture with the confidential information. The secret message must be encrypted before embedding it into image using RSA encryption to reinforce the classified nature of the information. In this methodology, we combined the LSB insertion on images with the Hash function naming Hash-LSB. In H-LSB, hash function is used to generate a pattern that helps in determining the positions at which the data will be hidden or embedded. The process of merging the two different techniques is a challenging process, one is a cryptography technique i.e. RSA encryption and the second is steganography method i.e. Hash-LSB. The main focus of combining these various methods is transmission of crucial data between the sender and receiver without compromising the confidentiality. All the reputed organizations use one or other techniques of encryption to protect confidentiality of their organizational information from rivals or intruders while transmitting the information over internet. To create a reliable steganography method, hash function LSB method and the RSA encryption technique have been combined together which is more secure and dependable than numerous present methods being used for the end goal of safely transmitting the information.

The Hash function combined with the LSB method for steganography in which a pattern is generated by hash function that determines the least significant bit of RGB pixels to embed the data. The hash function determines the specific position of lSB of each RGB pixel where the data bits are to be hidden. Based on the least significant bit present in RGB pixel, it returns the hash values. The selected picture will be divided into the fragments of RGB format. Then the data bits are hidden into the LSBs of the picture using the values given by the hash function, using the Hash-LSB technique. In this strategy, the confidential message is at first changed into the binary bits, at that point every 8 bits are concealed in LSB's of RGB pixel of the picture arranged as 3 (RED), 3 (GREEN), and 2 (BLUE). As indicated by this technique, initial three bits are covered up in the LSB of the red pixel, the following three bits are stowed away in the LSB of green pixel and the last two bits are covered up in the LSB of blue pixel. These 8 bits are embedded in a specific order in light of the fact that the chromatic impact of green and red colour to the human eye is less than the blue colour. Subsequently the 2 bits are picked to be covered up in the blue pixel by the distribution pattern. Thus the quality of the picture will not be relinquished. The below given equation is used to determine pattern of the concealed information in LSB of each RGB pixels of the selected picture[1] :

$$h = k \% n \qquad (1)$$

where, the LSB position of inside the pixel is given by h; k denotes the position of each concealed pixel of picture and n denotes the number of LSB’s bit. A stego image will be produced, after hiding the encrypted data in the selected picture. The hash function is used again by the receiver to extract the pattern where the encrypted data has been embedded. The cipher text will be extracted from the image. After decryption of the cipher text the secret message is produced by combining the bits into information by recipient.

Encrypting with RSA and Encoding with Hash-LSB

RSA encryption is used to encrypt the message in this approach of image steganography. A message or a document encryption is incorporated into RSA encryption for transforming it into the cipher text. Open key of the recipient is used in encrypting the secret message. By ciphering the confidential information into encrypted form, the information is made secure, which will not be easy to decipher for any invader without the private key of the receiver. Initially we take encrypted message and embed it in the selected picture. In this process, the binary form of the encrypted information is converted into the bits. Then the positions are selected by using Hash function and then at a time, message’s 8 bits will be embedded in the order of 3 (RED), 3 (BLUE), and 2 (GREEN) pixels of the picture. Till the entire bits of message are embedded into the selected picture, the process will be continued [1].

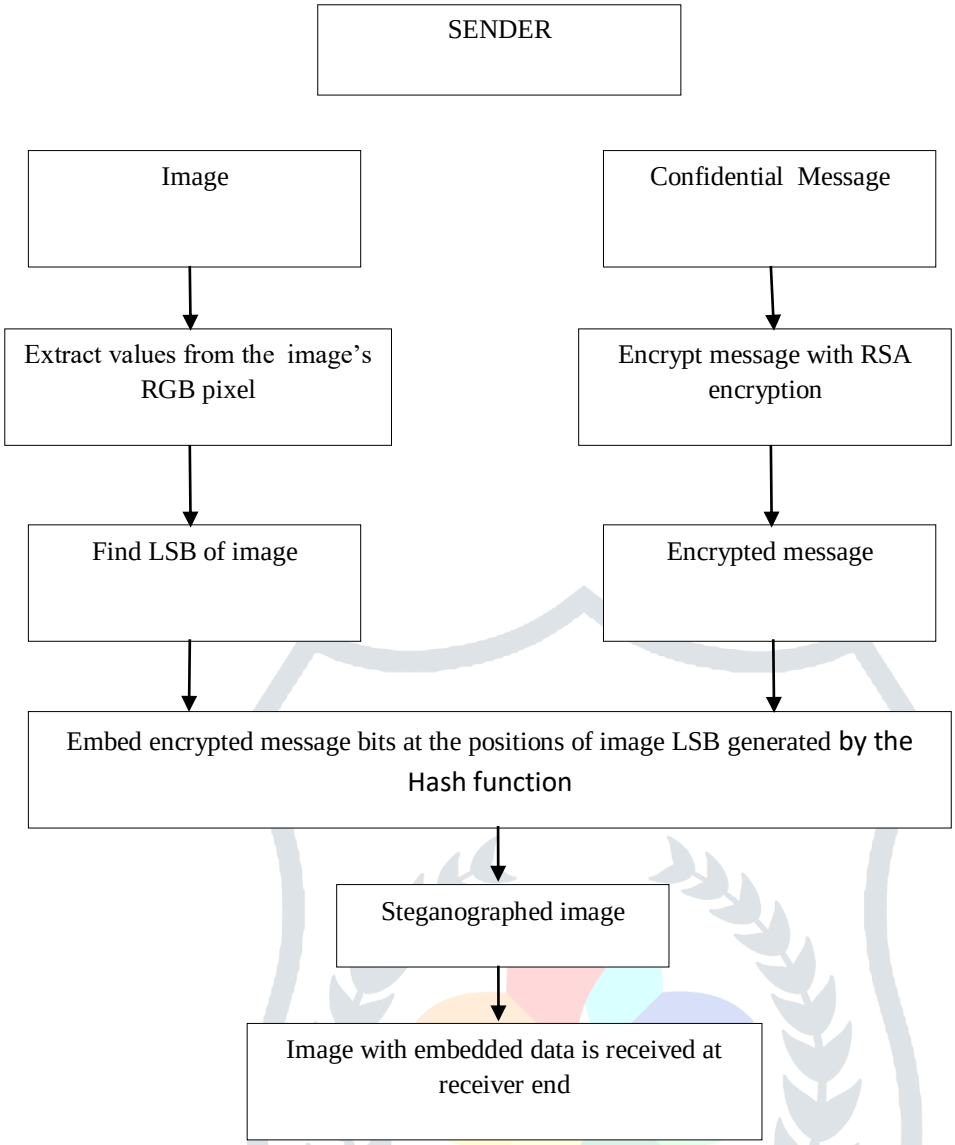

Figure 1: Encryption process of message

Embedding Algorithm

Step 1: Select the picture & confidential information.
Step 2: Cipher the information RSA encryption.
Step 3: Determine the 4 LSB of each RGB pixels from selected picture.
Step 4: Generate a pattern on LSB of selected picture by using hash function.

Stage 5: Insert 8 bit of the ciphered information into 4 bits of LSB of RGB pixels of chosen picture in the order of 3, 3 and 2 respectively, using the pattern produced from hash function given in condition 1.
Step 6: Send picture with hidden data to receiver.

Decoding with Hash-LSB and Deciphering with RSA

During the procedure of decoding, the hash function is once again used to identify the patterns of least significant bits at which the information bits had been inserted. Once the pattern of bits embedded had been determined, the bits are retrieved in the similar pattern from the position as they were inserted. After extracting the bits from image, the message is extracted in the binary form which is then changed into the form of decimals, and the encrypted information is retrieved with the similar process. Once the encrypted information is retrieved from the picture, the recipient uses the RSA decryption algorithm to decipher the recovered encrypted information and generate the secret message from the sender. As the data has been encrypted using the open key of the recipient, the recipient uses his/her private key to decipher the encrypted information and generates the original message in readable format.

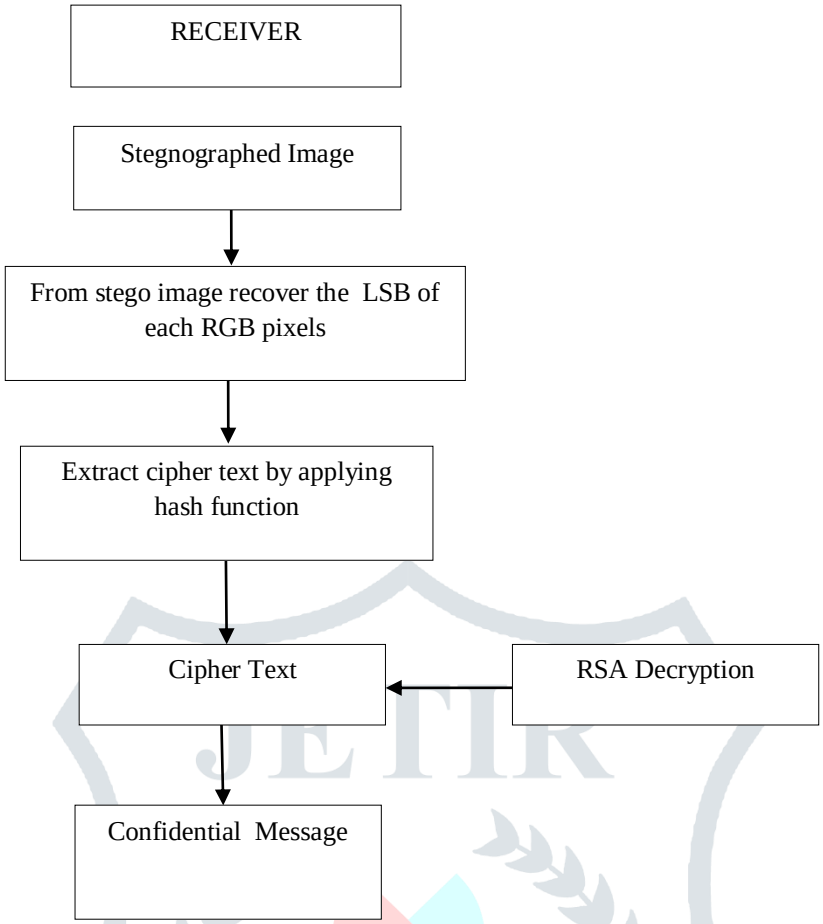

Figure 2: Decryption process of message

Recovery Calculation
Stage 1: Get a stego picture.
Stage 2: Discover 4 least significant bits of each RGB pixels from stego picture.
Stage 3: Apply hash function to determine the pattern of LSB's with shrouded information.
Stage 4: Recover the bits utilizing these patterns in order of 3 (RED), 3 (GREEN), and 2 (BLUE).
Stage 5: Apply RSA decryption to the recovered cipher message.
Stage 6: At last read the information.

Analysis of Performance
On the basis of two measures i.e. PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error), the performance evaluation of hash function and LSB method combined together has been done and graphically presented, and the values that are obtained turned out to be much better than the currently existing technique. Between the steganographed picture and its equivalent cover picture, the PSNR and MSE have been calculated and given by the eq. 2 and 3 as below:

$$MSE = \frac{1}{H*W}\sum_{i=1}^{H}\big(P(i,j) - S(i,j)\big)^2$$

Figure 3. Calculating MSE

Here, height is denoted by H, width is denoted by W, cover image is represented by P (i, j) and the steganographed image corresponding to the cover image is represented by S (i, j).

$$PSNR = 10log_{10}\frac{L^2}{MSE}$$

Figure 4. Calculating PSNR

Where, peak signal level for a color image is represented by L. In this image steganography technique, within three pixels of cover image eight bits of data are embedded.

Conclusion

A secure image steganography technique has been implemented by combining Hash function, LSB method and RSA algorithm. The combination of hash-function and LSB method has attained an effective and efficient method for secret messages to be embedded into image without generating any major changes. A method of cryptography i.e. RSA algorithm for encrypting the confidential information, is also combined in this method, so that decrypting it is not easy without the public or private key. Cryptography method, RSA algorithm is combined in the proposed method to enhance the safety of the information as RSA algorithm itself is very secure. As hash function is used for embedding data and RSA algorithm to render encryption to information, makes this approach more viable to transmit information over any medium that is not secure or internet. The images of .tiff format has been used to apply Hash-LSB technique, however with minor procedural modification, like for compressed images, it can work with any other formats as well. By comparing it with pure steganography technique of least significant bit method, the assessment of performance analysis of the developed procedure has been completed, which has produced good values of PSNR and MSE for the steganographed image.

Refrences

[1] 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.

[2] Chandra.M.Kota, Cherif Aissi, "Implementation of the RSA algorithm and its cryptanalysis", ASEE Gulf-Southwest Annual Conference, American Society for Engineering Education, USA, 2002.

[3] Dr.Ekta Walia, Payal Jainb, Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, Vol. 10, Issue No. 1, April, 2010.

[4] 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, 20