# Secured Information Transaction using RSA Steganography

**Prabakaran. S[1] Dr. M. Chidambaram[2]**
[1]Research Scholar [2]Assistant Professor
[1,2]Raja Serfoji Govt. College, Thanjavur-5, India

*Abstract*— Steganography is an art of hiding the secret message in a cover object not including departure a remarkable track on the original message. It is used to increase the security of message sent over the internet. In contrast to cryptography, it is not used to scramble the data but it is used to conceal the data in digital media. This research paper will deal with text and video steganography, cryptography, hash-LSB and a encryption algorithm. At the end, there will be a discussion about the goal of this paper and what types of techniques worked on text and video steganography. A proposed technique for text and video steganography say Hash-LSB with the RSA algorithm is implemented to provide more secure data and data hiding method. This technique uses a hashing function to generate a mask model for the data bits in the LSB of RGB pixel values of the cover text and video. This technique ensures that the message is encrypted before hiding in a cover text and video frame. If in any case the cipher text has revealed the cover video frames, the intermediate person other than the receiver cannot access the message as it is in encrypted form. So Hash-LSB technique is more secure and responsible to transfer the important data on any unsecure channel. The encryption algorithm which is named as RSA (Rivest, Shamir & Adelman) algorithm, increase the security of valuable or precious data.

***Key words:*** Steganography, Cryptography, Hash-LSB, Encryption Algorithm, RSA

## I. INTRODUCTION

Digital Steganography is defined as method of hiding the data and system Steganography is a way to inset the secret information in a media of public coverage. There are two main features of steganographic techniques: the ability of Steganography and undetectable. However, these two features are opposed to each other. This is very toughest task to expand the capacity of Steganography. This technique manage the imperceptibility of system with steganography. In addition, there are many methods of Steganography for use with ways of communication and they are not conventional but describing media Steganography. Steganography in texts or video images uses a way to transmit a secret data through the texts or video images from one sender to other receiver side. This seeks without doubt of third party to such communication. Thus, this research focuses on and provides methods for improving these features of Steganography in texts or video images digitally. Therefore, the characteristic of texts or video images has been used to increase the capacity and advance steganographic quality of stego texts or video images.

Steganography and cryptography obtains different objectives. Cryptography technique covers the secret data by scrambling this messages. On the other give Steganography hides the secret data. The Steganographic technique allows suppression and security of important information. Additionally, there is a weak point of encryption systems is that the survival of secret message is not removed. Although the Steganography and the cryptography techniques give secret communication, these techniques can be defined in various ways.

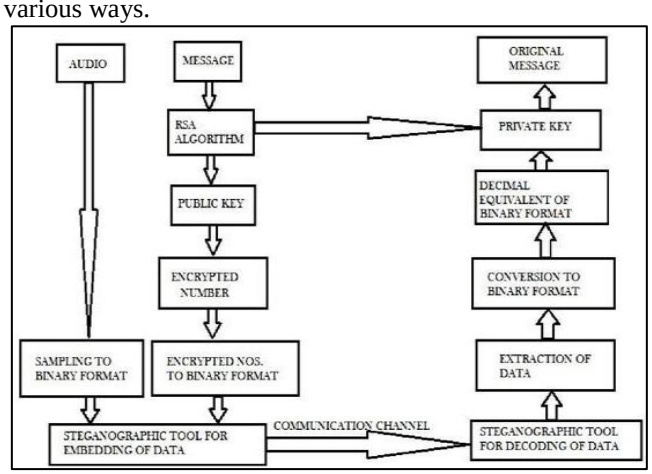


Fig. 1: System Architecture

In this methodology, an implementation of a technique called Hash-LSB insertion, derived LSB for text, image and video frames. In this Hash-LSB, the hash function is used to check positions to hide the secret bits or to be combined. It is a difficult process that will lead other techniques to merge the two technologies, one of them is Hash-LSB steganography and other is RSA cryptography. This research has concentrate on given that a solution for the transfer and sharing of important data without any kind of interference. All creditable organizations while sending any business documents on the internet or any channel always use encryption algorithm to protect important information from leakage. The proposed technique also provides security from frame dropping attack while sending the important data in cover texts and video images. This thesis used Hash-LSB and the RSA algorithm to produce a secure steganography algorithm which is much safer than many systems in order to on the sly send data.

## II. PROPOSED TECHNIQUE

### *A. Hash-LSB Technique*

The Least Significant Bit Hash Function (H-LSB) Steganography technique for LSB position in which to hide the secret data. This technique used to determine the hash function. Hash function finds the position of least significant bit of each RGB pixel, and then message bits are implanted in this RGB pixel individually. Then, the hash function takings hash values be determined by upon LSB in values of RGB of pixels. An image of the cover will be broken or fragmented in RGB format. Then Hash technical LSB will use the values from the hash function to integrate or hide data. This technique, the secret message is changed into binary form as binary bits; each 8 bits at a time are encompassed in the least significant values of RGB pixel image covering about 3, 2 and 3 bits respectively. Under this method three

 

bits are embedded in red pixel LSB 3 bits are embedded in green pixel and 2 LSB bits are embedded in blue pixel.

### *B. Hash Function*

Hash technique the Least Significant Bit as a function that produces the hash function. This hash function deals with the LSB position. The pixel position of each pixel covered image, and also with the number of LSB bits. Hash value takes a variable size input and returns a fixed-size digital output string. Hash function is also used to detect duplicate folder in large files.

Hash function generally given by i = j % k

Where, i is the position of LSB bit within the image or video frame pixels, j represents the position of each hidden video frame pixel and k is number of bits of LSB.

### *C. RSA Algorithm*

The RSA algorithm was defined by Rivest, Shamir and Adleman three MITs. This algorithm is used to encrypt the secret message into twisted form. This algorithm works by taking two values of primes and then the product of these values. This product value is used to make a public and a private key and this is also used in the encryption and decryption methods. The RSA algorithm can be used in arrangement with Hash-LSB so that the original message is inserted into the cover video frame as cipher text. RSA algorithm increases the security level of video steganography.

In most situations, the security is discriminating by a required key to reverse the Steganography process.

1) To develop a RSA algorithm for cryptography. Firstly we develop a algorithm for the loading the image in the database. We develop a code for steganography by using a novel score-level combination strategy.
2) Planning and implement the developed algorithm for the steganography resolution for the texts and image. Develop a code for Procedures for hide text or video images. This procedure hides the encrypted data into the image by searching the best position in the image. The best position defines those Least Significant Bits of the image which particularly match with the encrypted data bits. The output of this procedure is the updated image in which data is hidden.
3) Procedure for Reveal Text: This procedure reveals the secret message which is hidden in the best position of the stego image. This message is in the encrypted form so the message is decrypted by the receiver's private key. Then the original message is open to the receiver.
4) The independent of steganography is to hide a secret message within a cover-media. Such a way that others cannot detect the frequency of the hidden message. Technically in simple words "steganography means hiding one piece of data within another".
5) Current steganography uses the opening of hiding information into digital texts or video images files and also at the network packet level.
6) The stego function operates over cover media and the message (to be hidden) along with a stego-key (optionally) to produce a stego media (*S*).
7) This method binary alike of the message (to be hidden) is blowout among the LSBs of each pixel.

There are various algorithms which are been applied on the image so as to produce the outcome i.e. the original message. The Embedding Algorithm: In the technique presented here, the colour image is decomposed into three components R, G and B. Watermark information will be implanted in the G plane using equation 1 to produce G'. Assume that f (i,j) represents the pixel of the component of the RGB representation of the colour host image, w (i,j) represents the binary pixel of the watermark.


Fig. 2: The Basic layout of the Secret Key

Creation in the above figure, we just show the starting secret key of the proposed system, it consists of the Encoder part of the system. The basic function of the encoder part is to hide the information or text. And provide this information to the decoder. And the decoder will decode the original message from the image. The above figure basically shows the cryptography part of the proposed system, in this the outcome image of the steganography part will act as an input of the cryptography system and further on this image we divide it into shares and we also apply the keys on it for better security purposes.


Fig. 3: The layout of the Encoder list details.

The encoder part consists of the steganography and the cryptography part, in this the original message is hidden with the help of steganography and the cryptography and then that message is sent to the receiver. So that it will get the original message.

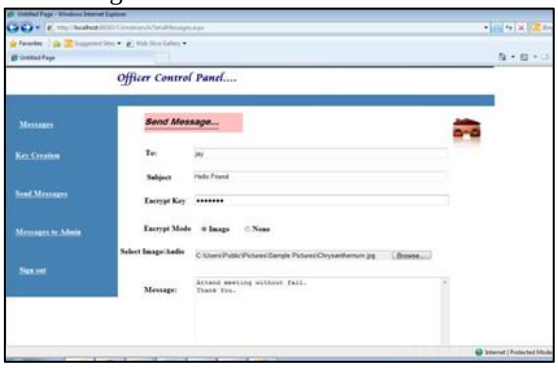


Fig. 4: The Delete in which steganography part is carried out.

 

In the above figure we basically hide the text or message, in an image so the unauthorised user is not able to access the data easily to delete the data to send.

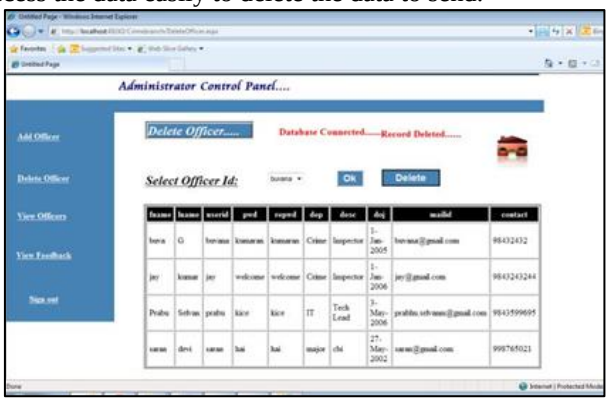


Fig. 5: The Viewer Used for the cryptography part.

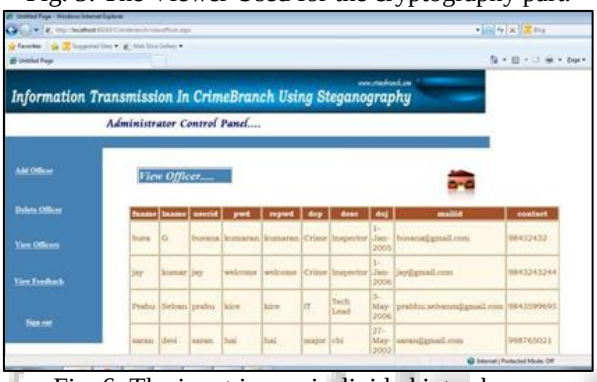


Fig. 6: The input image is divided into shares.

A usefulness is developed for RSA algorithm. With the help of this utility user can generate public and private keys by providing two prime numbers. The user can enter prime numbers according to his/her choice and an automatic generated prime numbers are also provided as an aid to the user. The utility generates a pair of public and private key, which can be saved in the file or user may remember these keys. The image utility takes the jpeg image or the folder of images (users library) and convert them into lossless jpeg images. The path is provided by the user in which these converted images are saved. In the text box user can type the secret message and this message is encrypted with the receiver's RSA public key. This key is loaded from the file where it was saved. The stego image is obtained by user at the receiver side. The user then gets the message in the encrypted form. The recipient then decrypts the message only with his private key which is made available to him through any media. After decryption user gets the original message. The reveal text utility is developed for this.


Fig. 7: The layout of the Decoder part.

In the decoder part we retrieve the original message from the input image. In this proposed system, only the authorized user will be able to access the data or message properly.

## III. Conclusion

The steganography is used in the covert communication to transport secrete information. In this per Steganography using visual cryptography is proposed. The secret message is embedded into smaller matrix of size 8x8 and inserted into input image. In future the technique can be verified for robustness. We added the RSA algorithm process with it. Presently, this application supports hiding data in lossless jpg images. Future improvement of this application would be extending its functionality to support hiding data in video files or in other file format.

## References

[1] Raja K B, C R Chowdary, Venugopal K R, L M.Patnaik. (2005): "A Secure Steganography using LSB, DCT and Compression Techniques on Raw Images," IEEE International Conference on intelligence Sensing and Information processing, pp.171-176.

[2] Kumar V and Kumar D. (2010): "Performance Evaluation of DWT Based Image Steganography," IEEE International Conference on Advance Computing, pp. 223-228.

[3] Weiqi Luo, Fangjun Huang, and Jiwu Huang. (2010): "Edge Adaptive Image Steganography Based on LSB Matching Revisited," IEEE Transactions on Information Forensics and Security, no. 2, vol. 5, pp. 201-214.

[4] R O El Safy, H H Zayed and A El Dessouki (2009): "An Adaptive Steganographic Technique Based on Integer Wavelet Transform," International Conference on Networking and Media Convergence, pp.111-117.

[5] G.Andrew Duthie "Microsoft Asp.Net Step by Step" Prentice Hall of India, 2006 Edition.

[6] V Vijaylakshmi, G Zayaraz and V Nagaraj. (2009):"A Modulo Based LSB Steganography Method," International Conference on Control, Automation, Communication and Energy Conservation, pp. 1-4.

[7] Wien Hong, Tung-Shou Chen and Chih-Wei. (2008):"Lossless Steganography for AMBTC-Compressed Images," Congress on Image and Signal Processing, pp.13-17. Gaurav Singh, Kuldeep Tiwari, Shubhangi Singh, "Audio Steganography using RSA Algorithm and Genetic based Substitution method to Enhance Security", International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014, ISSN 2229-5518. M Hassan Shirali-Shahreza and Mohammad Shirali-Shahreza. (2008): "A New Synonym Text Steganography," International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1524-1526.

[8] Vladimir Banoci, Gabriel Bugar and Dusan Levicky (2009): "Steganography Systems by using CDMA Techniques," International Conference on Radio electronika, pp.183-186.

[9] Chen Ming, Zhang Ru, Niu Xinxin and Yang Yixian (2006):"Analysis of Current tegano graphic Tools: Classifications and Features," International Conference

 

on Intelligent Hiding and Multimedia Signal Processing, pp. 384-387.
[10] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt. (2008): "Enhancing Steganography in Digital Images," Canadian Conference on Computer and Robot Vision, pp. 326-332.



 