Text security using lossless portable network graphics

Swapnali Patil[1], Prof.P.B.Koli [2], ProfN.R.Wankhade[3]

[1] *Student, Computer Department,late G.N.Sapkal coe, Maharashtra,India*
[2]*Assoc Professor, Department,late G.N.Sapkal coe, Maharashtra,India*
[3]*HOD and Asst Professor, Department,late G.N.Sapkal coe, Maharashtra,India*

ABSTRACT

Data is an important asset for any individual or organization and must be protected from intruders or hackers. The need to hide data from hackers has existed since ancient times, and nowadays, there are developments in digital media, such as audio, video, images, and so on. To secure secret information, different media methods are used and steganography is one. Steganography hides the data under other data without any differentiable changes. Many individual steganography tools can be used to transfer data securely and, in this report, a new tool is proposed that decreases time and effort. Using this tool, we hide the text in images in one place, so there was no need to have access to multiple tools. This proposed tool developed using the least significant bit (LSB) approach.

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. There for from time to time researchers have developed many techniques to fulfil 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.

Keyword- *Cryptography, Hash-LSB,LSB,RSA Encryption-Decryption, Steganography*

1. INTRODUCTION

Globalization has led to the rapid growth of the internet through which consumers can send and receive large amounts of data (e.g., text, audio and images). In modern communication systems, securing data is of utmost importance. Yet sending and receiving secret files over the internet is still insecure, and therefore hiding data inan effective way protects this secret information. Digital multimedia data provides a robust and easy editing and modifying of data. The data can be delivered over computer networks with little to no errors and often without interference. Unfortunately, digital media distribution raises a concern for any loss in quality and content. This poses a big problem for the protection of intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital data, such as information about the owner, recipient, and access level, without being detectable in the host multimedia data. Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. The technique replaces unused or insignificant bits with the secret data. Steganography is not as robust to attacks since the embedded data is vulnerable to destruction.

2. REVIEW OF LITERATURE

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 [1].

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 its 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.[2]

In [3] the author is concerned with what steganography is and what it can do. thy contrasted it with the related disciplines of cryptography and traffic security, present a unified terminology agreed at the first international workshop on the subject, and outline a number of approaches -many of them developed to hide encrypted copyright marks or serial numbers in digital audio or video. Present a number of attacks, some new, on such information hiding schemes.

This leads to a discussion of the formidable obstacles that lie in the way of a general theory of information hiding systems. However, theoretical considerations lead to ideas of practical value, such as the use of parity checks to amplify covertness and provide public key steganography. Finally, we show that public key information hiding systems exist, and are not necessarily constrained to the case where the warden is passive.

3.SYSTEM ARCHITECTURE / SYSTEM OVERVIEW

The architecture system itself defines the all scenarios of the image steganography. User first select the input image file then add secrete text message using encryption technique. At receiver side user decrypt the image file using key and get the original message

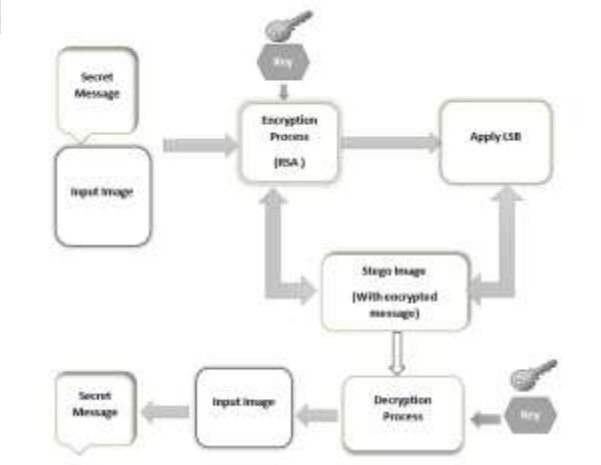

Fig:. System Architecture

3.1 Hiding Secret Messages in Digital File

Figure 2 describes hiding a secret file in a cover file, we began by selecting a key file and an acceptable cover file. The tool alters and modifies the bits of the cover image to allow the insertion of the secret message in the cover image. After this insertion is completed, a new, acceptable file is generated. This new file is called a stego file.

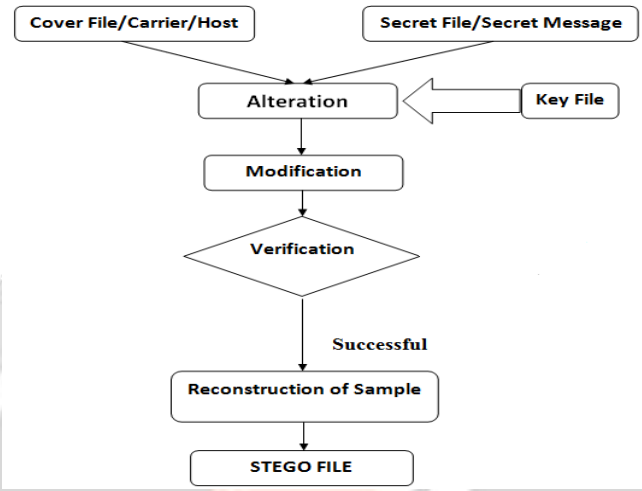

Fig 2:. Encryption

3.2 Decryption process

Figure 3 shows the process of extracting the secret message from the stego file. To extract the secret message, we need the same key file we used to hide the message. We begin by verifying that key file. After verification is successful, the tool extracts the secret message from the cover file.

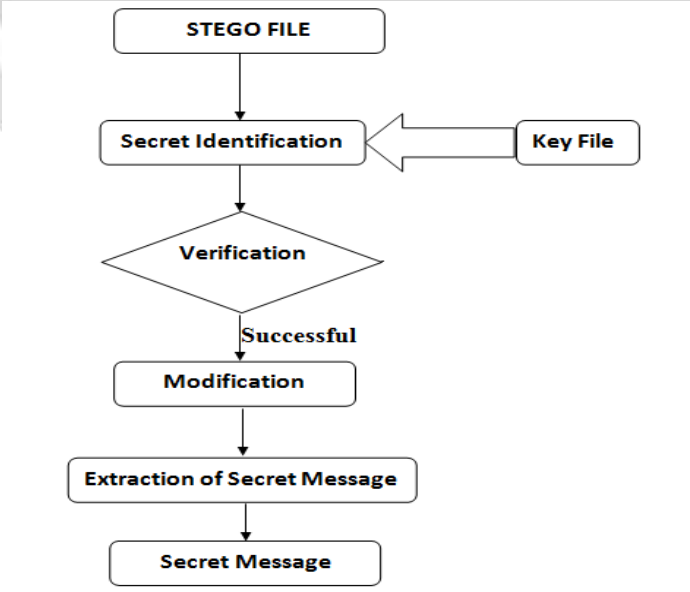

Fig 2:. Encryption

3.3 . LSB Algorithm(Red,Green,Blue algorithm)

- LSB (Least Significant Bit) substitution 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.
- The Least Significant Bit insertion varies according to number of bits in an image.
- For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message.
- In one pixel only one bit data is hiding at red green and blue lsb pixel position

Algorithm work:

- **LSB Hiding technique**

If we want to hide the data like "Aha!"

Then we convert the message "Aha!" into ASCII Code and then there equivalent binary code.

- A=65 (01000001)
- h=104(01101000)
- a=97(01100001)
- ! =33(00100001)

- **RSA Algorithm:**

1. Select two large strong prime numbers, p and q. Let n= p q.
2. Compute Eulers totient value for n: f(n) = (p - 1) (q -1).
3. Find a random number e satisfying 1<e<f (n) and relatively prime to f (n).
4. Calculate a number d such that d = e-1 mod f (n).
5. Encryption: Given a plain text m satisfying m ¡ n, then the Cipher text c = me mod n.
6. Decryption: The cipher text is decrypted by m = cd mod n

4. SYSTEM ANALYSIS AND RESULT

PNG.PSNR is infinity if the two images being compared are exactly the same and if you compare two identical images

Original image

Image with red pixel

Image with green pixel

Image with blue pixel

Result Table:

Image Name	Result obtain using H-LSB with RSA		Red with 1 Pixel		Green with 1 Pixel		Blue with 1 Pixel	
	MSE	**PSNR**	**MES**	**PSNR**	**MES**	**PSNR**	**MES**	**PSNR**
Image 1	0.0036	76.4748	0.0038	76.6932	0.00371	76.5739	0.003	76.65
Image 2	0.002477	74.8697	0.00262	75.05708	0.00245	74.77302	0.00234	74.5716
Image 3	0.003602	76.43572	0.00369	76.5417	0.003819	76.6898	0.003602	76.435722
Image 4	0.00206	74.02367	0.00219	74.27469	0.00240	74.29469	0.00219	74.27469

5. CONCLUSION

Steganography is useful for hiding messages for transmission. One of the major discoveries of this investigation was that each Steganographic implementation carries with it significant trade-off decisions, and it is up to the steganographer to decide which implementation suits him/her best. Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have deferent methods of hiding messages, with

different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase theprobability of detection when in the presence of a warden.

6. REFERENCES

[1] Denemark Denemark,Mehdi Boroumand ,lgorithm "Steganalysis Features for Content-Adaptive JPEG Steganography",IEEE Transactions on Information Forensics and Security,Vol. 11, 8, Aug. 2016.
[2] M. I. H. S. M. Masud Karim, Md. Saifur Rahman, "A new approach for lsb based image steganography secret key," in InternationalConference on Computer and Information Technology (ICCIT),, vol. 2,Dec 2011.
[3] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," in IEEE, Journal International Conference on Signal Processing, vol. 1 May 1998.
[4] G. I. S. Amr A. Hanafy and Y. Z. Mohasseb, "A secure covert communication model based on video steganography," in IEEE Transection on computer engineering, vol. 5,May 2008.
[5] L. v. A. Nicholas Hopper and J. Langford, "Provably secure steganography," in IEEE Transection on computer Engineering, vol. 58, Nov 2009.
[6] P. D. Kousik Dasgupta, J. K. Mandal, "Hash based least signifcant bit technique for video steganography (hlsb)," in International Journal of Security, Privacy and Trust Management (IJSPTM), vol. 2, April 2012.
[7] [S. A. et al, "Wireless access point specific location based encryption," in Systems, Applications and Technology Conference (LISAT), march 2013.
[8] P. S. S. Mamta Juneja, "Designing of robust image steganography technique based on lsb insertion and encryption," in International Conference on Advances in Recent Technologies in Communication and Computing,22-24 Oct 2009.
[9] R. P. M. Swati Tiwari, "A secure image based steganographic model using rsa algo- rithm and lsb insertion," in International Journal of Electronics Communication and Computer Engineering (IJECCE), vol. 3.
[10] Raja,K.B ,Vikasa , Venugopal,"high capaciry lossless secure image a steganography using wavelets," in 14th international conference on advance computing and communcation,ADCOM 2006.
[11] T.S. C. Wien Hong, "A novel data embedding method using adaptive pixel pair match-ing," in IEEE Transactions on Information Forensics and Security, vol. 7, Feb 2012,pp. 176184.
[12] [J. H. Weiqi Luo, Fangjun Huang, "Edge adaptive image steganography based on lsb matching revisited," vol. 5, June, pp. 201-214.
[13] J. H. Weiqi Luo, Fangjun Huang, "Edge adaptive image steganography based on lsb matching revisited," vol. 5, June, pp. 20-214.