LSB AND RSA BASED IMAGE STEGANOGRAPHY

Mandeep Kaur[1], Mrs. SUKHJINDER KAUR[2]

[1] Research Scholar, Sri Sukhmani Institute Of Engineering and Technlolgy, Dera Bassi.,
[2] Assistant Professor, Dept of ECE, Sri Sukhmani Institute Of Engineering and Technlolgy, Dera Bassi.,

Abstract:

Steganography is a an act of hiding secret messages in images in a way that it could be accessed only by the sender and receiver. Security of confidential information has been always a major issue from the past times to present time. It's always been very much in the interest of 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. Steganography is basically a combination of Greek words Steganos and graphei which means covered or protected writing. In ancient time steganography was used in many ways which includes writing or etching confidential messages on wood planks and then cover it with wax and other compounds. As the time changed the ways of hiding the confidential information get changed. Now various computer softwares could employ to hide the secret messages in images, videos and sound in combination with many encryption methods so as to make it hard to steganalyse the information. The most recent way of steganography is to use modified LSB technique in combination with RSA message encryption technique. This technique makes sure that the message has been encrypted before hiding it into a cover image so as if in any case it got revealed, the intermediate person other than receiver can't access the message as it is in encrypted form

Keywords: steganography, LSB, RSA message encryption, sender , receiver.

1. Introduction

The basic need of of every growing area in today's world is communication. Everyone wants to keep the inside information of work to be secret . We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a 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 to 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 as it couldn't be clearer to any intermediate person that whether there is any message hidden in the information being shared. The image containing the secret message is then transferred to the recipient. The recipient is able to extract the message with the help of secret information provided to him by the sender .There are various methods of steganography :

1. Least significant bit (LSB) method
2. Transform domain techniques
3. Statistical methods
4. Distortion techniques

As our research interest is the LSB method therefore we will be explaining it further and leaving others apart. LSB technique is quite useful when used in combination with RSA message encryption technique.

LSB method

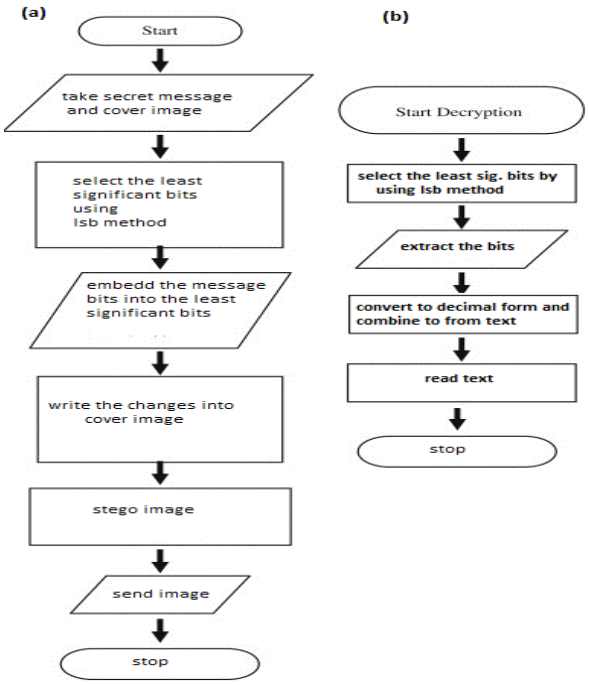

Fig 1: LSB stegnography (a) encryption (b)decryption

Least Significant Bit (LSB) method is a basic method of steganography. In this method some information from the

pixel 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.
LSB steganography involves the operation on least significant bits of cover image, audio or video. This lessens the change in colors that the displacement creates. The least significant bit is the lowest bit in a series of numbers in binary; the LSB is located at the far right of a string.
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 in8 bit and 24 bit images)

RSA message encryption technique

The algorithm was given by Rivest, Shamir & Adleman of MIT in 1977 . RSA 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 key ,which is further used in encryption.

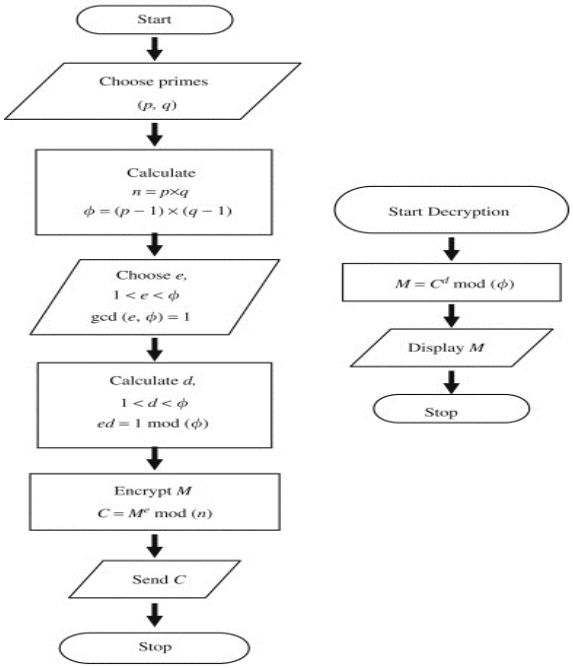

Fig 2: RSA cryptography encryption and decryption.

Decryption could be done only by using the same public key. Rsa algorithm could be used in combination with LSB in a way that original text is embedded in the cover image in the form of cipher text. This increases security to a level above. In case of steganlysis only cipher text could be extracted which is in the encrypted form and is not readable therefore secure.
It is a fundamental procedure of
various security protocols. It can be illustrated in brief as follows:
(i) Select two large strong prime numbers, p and q. Let $n = pq$.
(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 ***mod*** f (n).
(v) **Encryption:** Given a plain text m satisfying $m < n$, then the Cipher text $c = me$ ***mod*** n.
(vi) **Decryption** : The cipher text is decrypted by $m = cd$ ***mod*** n.[2]

2. Problem Definition

In our research we are implementing an image steganography technique using modified LSB (Least Significant Bit) method and along with this to improve security we are using RSA algorithm. For this we are starting with the encryption of the message into cipher text by RSA algorithm and then we are performing LSB to select the specific locations in RGB least significant bits of a pixel.

SENDER SIDE:-

Step 1. Chose the cover Image & Secret message.

Step 2. Encrypt the message using RSA algorithm.

Step 3. Find Least Significant Bits from Cover Image.

Step 4. Embed the Encrypted message within LSB.

Step 5. Send Stego Image to Reciever.

RECIEVER SIDE:-

Step 1. Receive a Stego Image.

Step 2. Find the LSB of Stego Image.

Step 3. Extract the hidden data from LSB'S

Step 4. Apply RSA to decrypt the hidden data.

Step 5. finally read the message.

3. Methodology

This 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 to their rivals or anyone.we have used a modified LSB and RSA algorithm to create a steganography algorithm which is far more secure than many systems being used for the purpose of secretly sending data.

Cover image and secret message

In our research first of all we selected RGB images as a cover image.. A secret message which was to be embedded in the image was specified.

RSA encryption

This message is converted into ASCII values of the text alphabets, contained in the message. ASCII stands for the American standard code for information interchange which is a character encoding scheme based on the English alphabet. They represent text in computers. Then we applied RSA algorithm, in we we took two big prime numbers in start. Then the key generation step got initialized ,RSA algorithm produced a public key by using two prime numbers and encrypted the ASCII codes in the form of Ciphertext. Which was encrypted form of the text we had taken at the start.

LSB encryption and decryption

At the start of this process we take cipher text as 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 we detected the least significant bits in RGB pixel values. Then we embedded 8 bits of message in the red green and blue components. The process is continued till full message bits got embedded in the cover image.

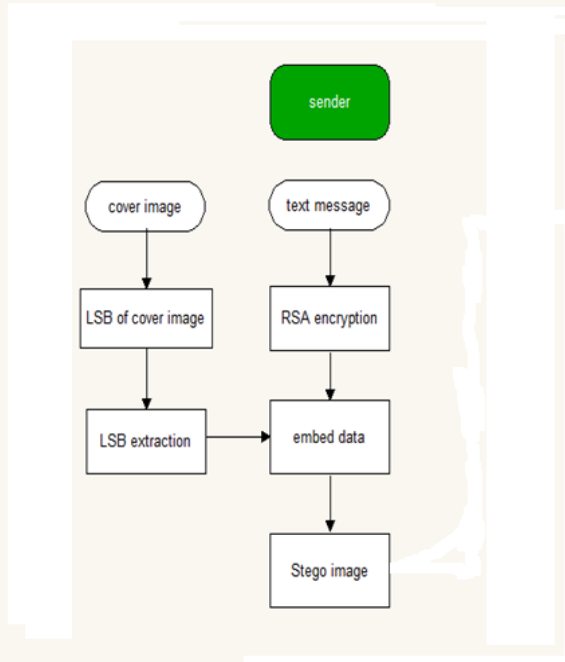

Fig 3: Showing encryption of secret message in cover image using RSA encryption and LSB embedding

In the decryption process we again used LSB process to detect the position of the bits where the message bits had been embedded. When the position of the bits had been specified then the bits are extracted from the position in the same order as they were embedded. At the end of this process we got message in binary form which was again converted to decimal form, and like this we got our cipher text message.

RSA decryption

The cipher text we got after the process of LSB is then taken as input in RSA decryption. By using public key generated in the key generation step of RSA encryption . using decrypt function of RSA algorithm we decrypted the cipher text into the ASCII values of the text. ASCII values were then easily converted back to the their corresponding alphabets and in combination we got our text message taken at the start in a decrypted form.

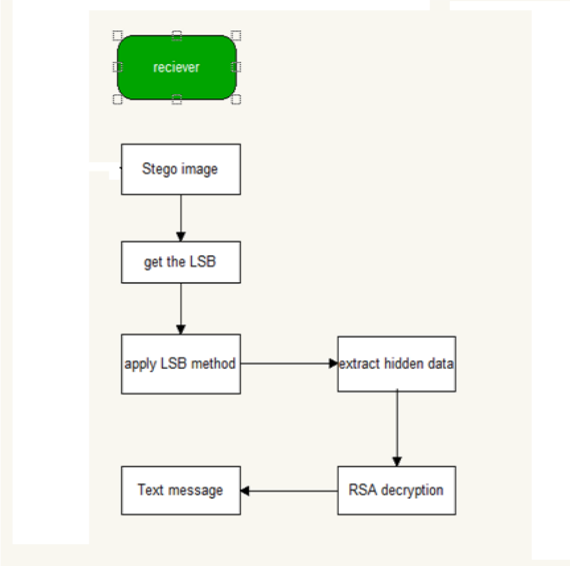

Fig 4: Showing decryption by LSB From stego image and then cipher decryption by RSA resulted in secret text retrievel.

4. Experimentation

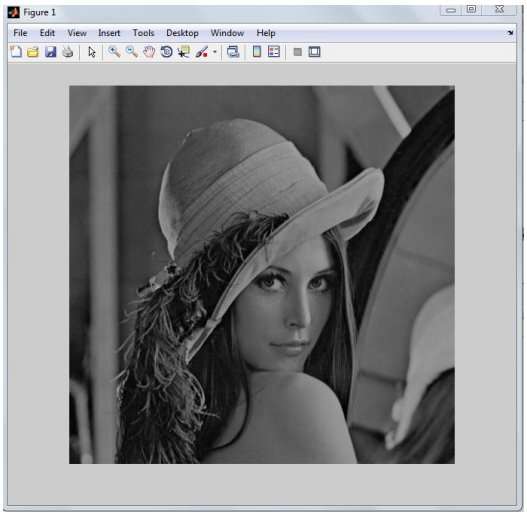

Fig 5: Input image

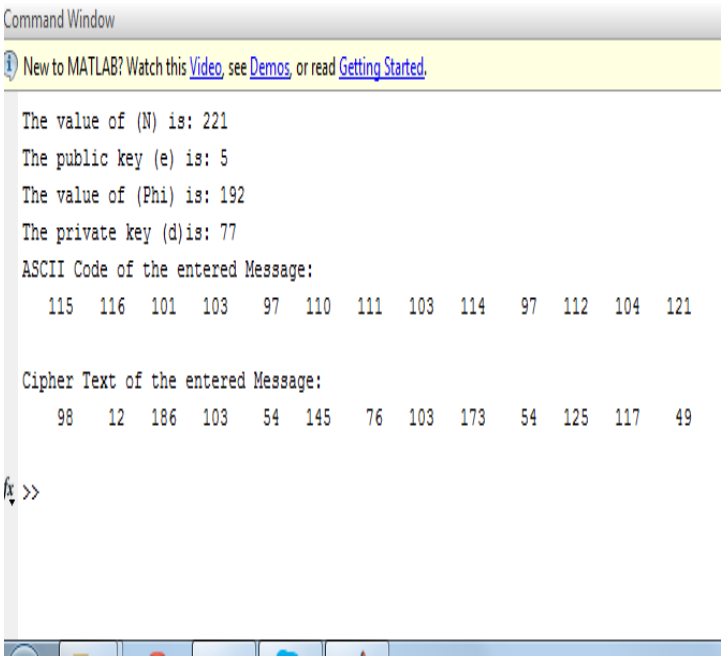

Fig 6: Message encrypted in the form of cipher text by RSA encryption.

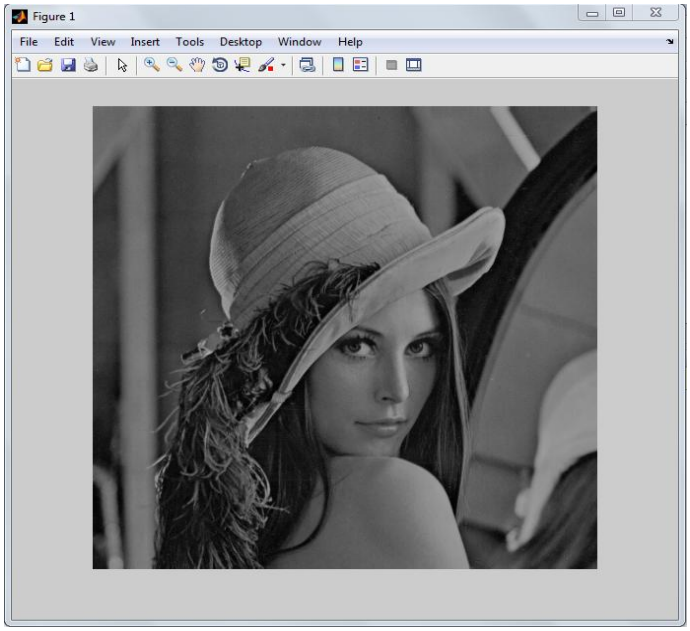

Fig 7: Stego image after LSB RSA steganography

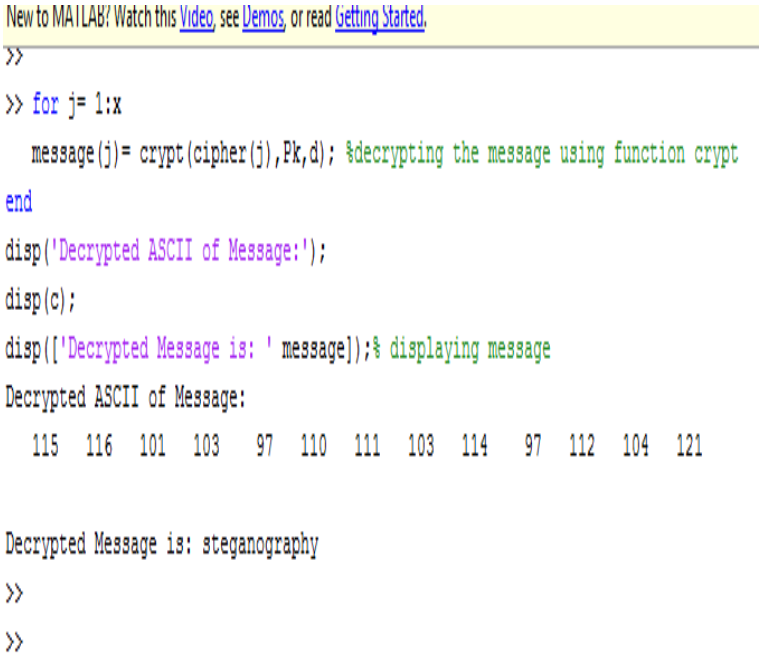

Fig 8: Decrypted message after RSA decryption.

5. Conclusion

In this research we have created a new way of hiding information in an image which is very secure and efficient. This method is also secure in the way that it's not easy to break the encryption of both RSA and modified LSB. RSA itself is very secure that's why used in our research to increase the security of the process. Specified embedding and secure encryption by RSA keys makes this method a very much usable and trustworthy to send information using the internet and over insecure servers.

Future work may contain combination of this method to message digesting algorithms

References

[1] Kousik Dasgupta1, J.K. Mandal2 and Paramartha Dutta "Hash Based Least Significant Bit Technique For Video Steganography(HLSB)" International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012

.

[3]Mamta Juneja , Parvinder Singh Sandhu "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption" 2009 International Conference on Advances in Recent Technologies in Communication and Computing. 978-0-7695-3845-7/09 $25.00 © 2009 IEEE DOI 10.1109/ARTCom.2009.228

[4] D. Stanescu, M. Stratulat, B. Ciubotaru, D Chiciudean, R. Cioarga and M. Micea, Embedding Data in Video Stream using Steganography, in 4th International Symposium on Applied Computational Intelligence and Informatics, SACI-2001, pp. 241-244, IEEE, 2007.

[5] Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao Guo, Video Steganography using Motion Vector and Linear Block Codes, in IEEE 978-1-4244-6055-7/10/, pp. 592-595,2010.

[6] Fillatre. L, Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption, IEEE Transactions on Signal Processing, Volume 60, Issue:2, pp. 556-569, Feb, 2012

[7] Masud K. S.M. Rahman, Hossain, M.L., A new approach for LSB based image steganography using secret key, in Proceedings of 14th International Conference on Computer and Information Technology (ICCIT-2011), pp.-286-291, Dec. 2011.

[8] U. Budia, D. Kundur and T. Zourntos, Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain, in IEEE Transactions on Information Forensics and Security, vol. 1, no. 4, pp. 502 – 516, December 2006.

[9] Ming, Chen, Z. Ru, N. Xinxin, and Y. Yixian, "Analysis of Current Steganography Tools: Classifications & Features", Information Security Centre, Beijing University of Posts & Telecommunication, Beijing, December 2006.

[10] N. F. Johnson and S. Jajodia, "Steganography: seeing the unseen," IEEE Computer., Feb., 26-34 (1998).

[11] J. Fridrich, M. Long, "Steganalysis of LSB encoding in color images," Multimedia and Expo, vol. 3, pp. 1279-1282, July 2000.

[12] R.Chandramouli, N. Memon, "Analysis of LSB based image steganography techniques," Image Processing, Vol. 3, pp. 1019-1022, October 2001.

[13] Tao Zhang, Wenxiang Li, Yan Zhang, Xijian Ping" Detection of LSB Matching Steganography Based on Distribution of Pixel Differences in Natural Images" Publication Year: April-2010, Page(s): 548 – 552.

[14] E. Koch, J. Rindfrey, and J. Zhao, "Copyright Protection for Multimedia Data," Proc. Int'l Conf. Digital Media and Electronic Publishing, Leeds, UK 1994.

[15] F.A.P.Petitcolas, et al.,"Information Hiding – A Survey", Proceedings of the IEEE, Vol.87, No.7, July 1999, pp.1062-1078.