IJCSE International Journal of Computer Sciences & Engineering Open Access
Research Paper Volume-3, Issue-7 E-ISSN: 2347-2693

Comparative Study of Multibit LSB Steganography with Cryptography

Mandeep Kaur Gill[1] and Rupinder Kaur Randhawa[2]

[1*,2] *Dept. of Computer Science and Engineering,*
Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, India

www.ijcseonline.org

Received: Jul/23/2015 Revised: Jul/25/2015 Accepted: Jul/27/2015 Published: Jul/31/2015

Abstract **—** Security has an important role in data communication through internet. When data travel through public network, sometimes unaccredited users access the confidential data. For secure communication various techniques are used from ancient time to the present time. Steganography is such type of technique used for data transmitting through insecure network. It is an art of hiding information inside other cover media such as text, image, audio and video. Various types of Steganography techniques are Text Steganography, Image Steganography, Audio and Video Steganography. But from these, Image Steganography is more usable due to increased frequency of images on the internet. Cryptography is a technique used for encrypting the plain text into cipher text securing from hackers. Cryptography is disparate from Steganography. In Cryptography, data is converted into different form of data. But in Steganography, data are invisible inside other data. In Cryptography, third party knows the presence of the secret message. In Steganography, unauthorized users do not know about the presence of the secret message. Hence, amalgamation of Steganography and Cryptography gives meticulous results. This paper instigates comparative study of pure LSB Steganography and LSB Steganography with Cryptography. One bit and two bits LSB steganography is implemented. Data are encrypted using RSA algorithm. Proposed technique is used to compare results of MSE (mean square error), RMSE (root mean square error), PSNR (peak signal to noise ratio) and NC (normalized coefficient) for both techniques.

Keywords **—**LSB, Cryptography, Steganography, RSA, PSNR, MSE, NC

I. INTRODUCTION

A. *Steganogarphy*

Steganography is an art of hiding raw data inside other data. Data are hidden in such a manner that no one other than recipient knows the existence of the hidden message. Various applications use various techniques for encoding data. Some applications need to store large amount of data and others need more security of confidential data [1].

Steganography is derived from Greek word "stegos" meaning "secret" and "graphia" meaning "writing" defined as "secret writing". Various steganographic techniques are used for data hiding. Steganographic techniques are divided into two main terms:

1) Spatial domain technique

The Least significant bit method is a spatial domain technique used for data hiding. In LSB technique, message is hidden into the least significant bit of cover media. We can also hide data inside 2 bits, 3 bits and 4 bits of cover media. Although hiding data using multibit LSB, increases data hiding capacity. But quality of cover media is deteriorated [6][7].

2) Transform domain technique

In frequency domain, mathematical components are used for converting pixel values into transformed coefficients. Then message is hidden inside the transformed coefficients which are significant areas for embedding data. Different transform techniques are:

B. *Cryptography*

Cryptography is a technique which is also used for data encryption. Cryptography is used to keeping the contents of message secret. But Steganography is used to keeping the existence of the message secret. By combining both of cryptography and Steganography, communication becomes more secure and confidential.

1) Symmetric key Cryptography

In this cryptosystem, same key is used for both encryption and decryption. This is also called secret key cryptosystem. The disadvantage of this system is key distribution. So, we go for asymmetric key cryptosystem [8].

2) Asymmetric key Cryptography

In this cryptosystem public key is used for encryption and private key is used for decryption. It is more secure than symmetric key cryptography. Well known asymmetric key cryptography algorithms are RSA, Diffie Hellman and DSS (Digital Signature Standard) [9][10].

II. RELATED WORK

In [1] authors discuss a new Steganography method for secure communication. This new technique uses symmetric key cryptography for encrypting the data. Then this data enciphered using the least significant bit insertion method and transferred over channel. Thus encrypted message increases the security of the secret message. In [2] authors work on least significant bit insertion technique for embedding data inside other cover media. First encrypt

data using cryptographic algorithms. RSA and Diffie Hellman algorithms are used for encrypting the message. In this paper, Cryptography and Steganography is in combined form. This result shows that time complexity increase if RSA algorithm is used instead of Diffie Hellman. Measure impacts of one bit, two bits, three bits and four bit Steganography on images. In [3] authors discuss a new method for image Steganography such as Hash-LSB with RSA algorithm and LSB with RSA algorithm for providing more security of data communication through public network. This technique uses hash function for hiding data into LSB of cover image. This technique encrypts data before embedding it. Compare performance with two parameters such as PSNR and MSE. The H-LSB technique works well with .tiff images. In [4] authors proposed multiple LSB base algorithm and measure quality of stego image. Two methods of Multiple LSB techniques are Multiple LSB based on Pixel value and Multiple LSB based on MSB digits. In Multiple LSB based on Pixel value, data embedding method is based on pixel value P (i, j) locating at i^{th} row and j^{th} column. According to pixel value, numbers of bits are embedded into the LSB of cover media. In Multiple LSB based on MSB digits, data bits embedding is base on the N for pixel value P (i, j). N denotes the number of one's in three MSB digits of cover media. Then based on N value, numbers of bits are embedded into the cover media. Compare the capacity and PSNR values for both methods which show that Multiple LSB based on Pixel value gives good results for capacity and Based on MSB digits give good results for peak signal to noise ratio. In [5] authors introduce a new method for protecting data from unwanted users. They use LSB insertion method for hiding data in cover media. Evaluate the performance of LSB method on GIF file format and PNG file format. This evaluation show that PNG does not work for animation like GIF. In online applications, PNG works well than GIF. GIF works well for embedding large amount of data in a gray scale image. In [6] authors implement the least significant bit modification technique for hiding into an image. The proposed method used two bit and three bit LSB algorithm for hiding secret data into cover media (image, audio &video). Method is applying on gray scale images. Various parameters are used for comparing the performance of the system such as total insert able bits and no. of characters hidden. In [7] authors introduce a new technology for covert channels. They discuss various Steganographic techniques for embedding purpose. They also analyze the strengths and weaknesses of existing methods. This paper represents the simple method for embedding data such as Least Significant Bit Insertion method. But it uses edges for hiding data into an image. So, first encrypt the text and find edges to embed data. Same algorithm is use for data extraction. In [8] authors present an accurate method for data transfer through World Wide Web. They implement DES algorithm for encryption purpose. 64 bits plain text and 56 bits secret key is applied for encipher the data. Extraction of message is difficult due to use of mapping rules of S-Box and secret key of function. Steganography is applying for increase the capacity, robustness and security. Two bit LSB method is use for embedding the data into image (e.g. of 64X64). In [9] authors proposed a novel method for data transmission between different networks. They implement RSA algorithm with modified keys exchange. Key generation is done in offline mode and store in a database. Database which is created for storing key must be identical at each network. Exchanged indexes allude to the fields that hold the public and private keys which stored in database tables before encrypting and decrypting the data, rather than exchange of n, e and d. RSA Handshake database protocol is used for checking the identical gateway's database. In [10] authors represent an effective technique for data hiding. Classical LSB algorithm is represented in randomized way. RC4 stream cipher is used to generate stego-key. This stego-key is further applied for calculating the cover image pixels for data hiding. This generates a secure stego-image which won't detect by unauthorized persons. This method improves security as well as capacity.

III. PROPOSED METHODOLOHY

The problem statement uses the two techniques for embedding message inside an image which are:

A. RSA Algorithm:

RSA is a public key cryptosystem used for encrypting the data for security purpose [2][3]. RSA generates a key for encryption and decryption. RSA worked in three steps:

1) Key Generation:

RSA includes a public key and private key. The public key is known by everyone and is use for encrypting the message. The message is decrypted only with the private key in a reasonable time. The steps for generating the keys are:

- Choose two different prime numbers a and b.
- Calculate n=a b
- Calculate g(n)=(a-1)(b-1), where g is Euler's totient function
- Compute a random number e satisfying 1<e<g(n) and gcd (e, g(n))=1; i.e; e and g(n) are prime numbers
- Find $d \equiv e^{-1} \pmod{g(n)}$

2) Encryption:

Let we want to send m message such that $0 \leq m < n$, then computes the ciphertext corresponding to $c \equiv m^e \pmod{n}$

3) Decryption:

Message is recovered from cipher such as $m \equiv c^d \pmod{n}$

B. LSB Insertion Method:

The least significant bit method is used for embedding data bit in the LSB of cover image. In the paper, we proposed one bit, two bit and three bit LSB Steganography for hiding data in the cover media [4][5]. The message embedding procedure is given below-

S (i, j) = C (i, j) - 1, if LSB(C (i, j)) = 1 and m = 0

S (i, j) = C (i, j), if LSB(C (i, j)) = m
S (i, j) = C (i, j) + 1, if LSB(C (i, j)) = 0 and m = 1
Where LSB(C(i, j)) stands for the LSB of cover image C(i, j) and m is the next message bit to be embedded.

IV. RESULTS and DISCUSSIONS

The main points regarding the results are:
Fig. 2 and Fig. 4 show the embedding of one bit and two bit LSB steganography without RSA. Fig. 3 and Fig. 5 show the embedding of one bit and two bit LSB steganography with RSA algorithm.
Table a. show that results obtained using LSB and LSB with RSA remains same for different parameters. Hence, using RSA with LSB increases the security of message without changing the PSNR value. Table b. show that results obtained using LSB and LSB with RSA give different values for different parameters. Hence, using RSA with LSB increases the security of message with changing the least value of PSNR.

Fig.1. Original Image

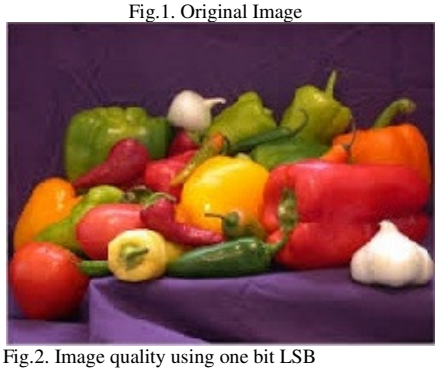

Fig.2. Image quality using one bit LSB

Fig.3. Image quality using one bit LSB with RSA

Cover image	Parameters	Results obtained using LSB	Results obtained using LSB with RSA
Original image	MSE	0.0013	0.0013
	RMSE	0.0366	0.0366
	PSNR	76.8705	76.8705
	NC	1	1

a. Results of one bit LSB steganography

Fig.4. Image quality using two bit LSB

Fig.5. Image quality using two bit LSB with RSA

Cover Image	Parameters	Results obtained using LSB	Results obtained using LSB with RSA
Original image	MSE	0.0037	0.0041
	RMSE	0.0610	0.0637
	PSNR	72.4281	72.0543
	NC	1	1

b. Results of two bit LSB steganography

V. CONCLUSION

Steganography is an effective way for hiding sensitive information. In this paper, I have used the one bit, two bit and three bit LSB technique without RSA and with RSA. Different parameters are used for comparing performance of these techniques. Table a. and Table b. shows that, although least value of PSNR decreases using RSA algorithm but security of message increases. These results show that image resolution doesn't change much and is negligible when message is embedded into it and message is protected using public-key cryptography.

VI. FUTURE SCOPE

This cryptographic method can be implemented with other Steganographic techniques. In the future, this technique

would be used to hide data in audio, video or in other file formats. In the near future work these techniques will be used with different file formats. Data will be embedded into three, four or five bits of an image for storing more number of bits of data.

REFERENCES

[1] V Tyagi, A Kumar, R Patel, S Tyagi and S Singh Gangwar, "IMAGE STEGANOGRAPHY USING LEAST SIGNIFICANT BIT WITH CRYPTOGRAPHY", Journal of Global Research in Computer Science, Volume-**03**, No-**03**, Page No (**53-55**), March **2012**.

[2] S Gupta, A Goyal and B Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", I.J.Modern Education and Computer Science, Page No (**27-34**), June **2012.**

[3] A Kumar and R Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", Int. Journal of Advanced Research in Computer Science and Software Engineering, Volume-**03**, Issue-**07**, July **2013.**

[4] R Patel and D Shah "Multiple LSB data hiding based on Pixel value and MSB value", Nirma University International Conference on Engineering, ISBN: **978-1-4799-0727-4,** Page No (**1-5**), **2013**.

[5] K Thangadurai and G Devi, "An analysis of LSB Based Image Steganography Techniques", Int. Conference on Computer Communication and Informatics, ISBN: **978-1-4799-2352-6**, Jan **03 – 05**, **2014**.

[6] S Patil, P Bhendwad and R Patil, "Steganographic Secure Data Communication", Int. Conference on Communication and Signal Processing, ISBN: **978-1-4799-3358-7,** Page No (**953-956**), April **03-05**, **2014**.

[7] G Seivi, L Mariadhasan and K Shunmuganathan, "Steganography Using Edge Adaptive Image", Int. Conference on Computing, Electronics and Electrical Technologies, ISBN: **978-1-4673-0210-4**, Page No (**1023-1027**), **2012.**

[8] M Ramaiya, N Hemrajani and A Saxena, "Improvisation of Security aspect in Steganography applying DES", Int. Conference on Communication Systems and Network Technologies, ISBN: **978-0-7695-4958-3**, Page No (**431-436**), **2013**.

[9] S Nagar and S Alshamma, "High Speed Implementation of RSA Algorithm with Modified Keys Exchange", Int. Conference on Sciences of Electronics, Technologies of Information and Telecommunications, ISBN: **978-1-4673-1658-3**, Page No (**639-642**), **2012**.

[10] N Akhtar, P Johri and S Khan, "Enhancing the Security and Quality of LSB based Image Steganography", Int. Conference on Computational Intelligence and Communication Networks, Page No (**386-390**), **2013**.

AUTHORS PROFILE

Mandeep Kaur Gill received her B.Tech degree in Computer Science in 2013 from Punjab Technical University, Jalandhar. Currently, She is doing M.Tech at B.B.S.B.E.C. Her research interest includes image Processing, Steganography, Information Retrieval and Data Security.