SECURED CRYPTO STEGANO DATA HIDING USING LEAST SIGNIFICANT BIT SUBSTITUTION AND ENCRYPTION

Subarna Shakya[1], Sanjita Lamichhane[2]

[1]Department of Electronics and Computer Engineering, Central Campus, Institute of Engineering, Tribhuvan University, Lalitpur, Nepal

Email Address: drss@ioe.edu.np

[2]Email Address: sanjitalamichhane06@gmail.com

Abstract

Information Exchange has always been an integral part of our lives. With the rapid advancement in Information and communication technologies, communication and information exchange have become much easier and faster but at the same time the issues regarding security of data and its confidentiality have become our major concern. Cryptography and Steganography are two such data hiding techniques that can be combined together in order to enhance data security. Cryptography scrambles a message so that it cannot be understood whereas Steganography hides its existence. In this process, message is first encrypted using an algorithm based on Fibonacci series or the Rijndael cryptographic algorithm and then the encrypted message is embedded inside an image using improved Least Significant Bit substitution method where the secret information is stored into a specific position of Least Significant Bit of an image based on the security key entered. This combinational methodology will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.

Keywords: *Cryptography, Steganography, plain text, encryption, decryption, Least Significant Bit, Mean square error and Peak Signal to Noise Ratio.*

1. Introduction

Cryptography and Steganography are two popular methods of sending secret information. One hides the existence of the message and the other distorts the message itself. These are well known and widely used techniques that manipulate messages in order to cipher or hide their existence respectively. Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted [1]. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood whereas the Steganography hides the message so that it cannot be seen. Cryptography assures privacy whereas Steganography assures secrecy [2]. Steganography and cryptography are both used to ensure data confidentiality.

2. Literature Review

The Advanced Encryption Standard (AES), also known as Rijndaelis a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.It is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. It has been adopted by the U.S. government and is now used worldwide. RIJNDAEL is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware.Zhi and Fen [8] proposed method of LSB image steganography, which used a method called detection of random LSB in which secret message was inserted in selected part of image randomly not

in fixed or predefined manner due to this steganalysis became difficult. Zhang *et al*.[7] introduced a new method of LSB steganalysis which is based on statistical distribution of pixel difference in spatial domain which can be done on high resolution images. Based on the difference of zero and non-zero values of pixels and also finds the error which is used to determine the steganographic features. It also uses Laplacian distribution. As we know that pixels are highly correlated to each other in image and zero, non-zero values occur frequently. If change in some neighbor's pixel value occurs then it may slightly change the intensity level of colours. Li *et al.*[9] proposed LSB Information Hiding algorithm which could lift wavelet transform image. Furthermore, made the objective evaluation of image quality by the PSNR and normalized cross correlation coefficient. Achieving the purpose of information hiding with the secret bits of information to replace the random noise, using the lowest plane embedding secret information to avoid noise and attacks, utilized redundancy to enhance the sound embedded in the way nature to be addressed[10]. Results showed that the proposed algorithm has a very good hidden invisibility, good security and robustness for a lot of hidden attacks.

3. Methodology

An image is the most common type of digital media used for steganography. Digital images often have a large amount of redundant data and for this reason it is possible to hide message inside image file. Image steganography is about exploiting the limited power of the human visual system where we hide information in the least significant bit (LSB) of the image data [7]. This embedding method is based on the fact that the least significant bits in an image can be thought of as random noise, and consequently they become less responsive to any change on the image. In this method we first encrypt a message using an algorithm based on Fibonacci series and RIJNDAEL cryptographic algorithm then embed the encrypted message inside an image using LSB embedding method. Hiding data using LSB modification alone is not highly secure. The combination of these two methods will enhance the security of the data embedded. This combinational methodology will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.

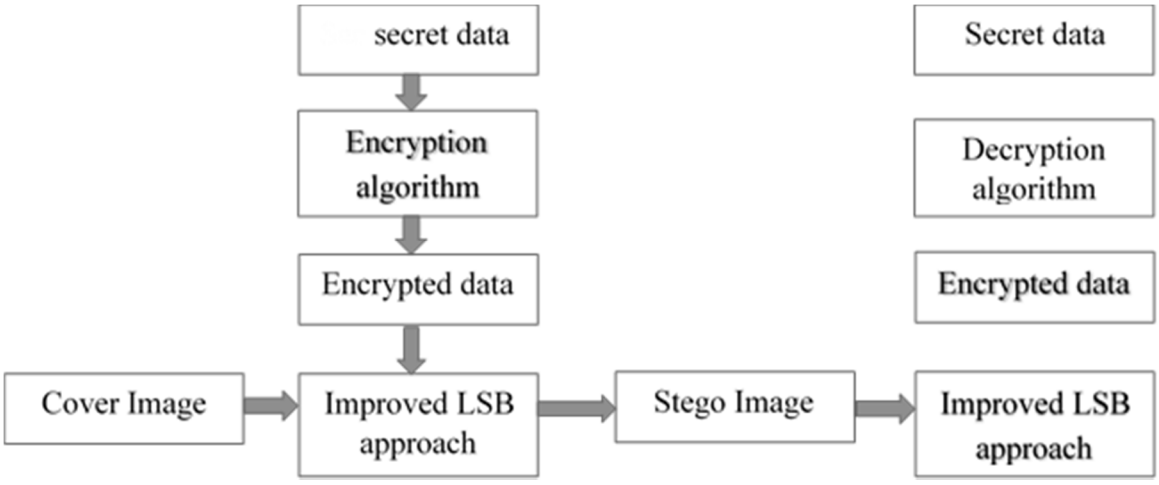


Fig1 Block Diagram of system

METHOD I: CRYPTOGRAPHIC ALGORITHM BASED ON FIBONACCI SERIES

In this method, the original message called plain text is converted into cipher text by using a key and Fibonacci numbers generated. The algorithm being used can produce a different output each time it is used, based on the key selected.

Plain Text to Cipher Text

Plain text: IOE PULCHOWK

Security Key: k

Characters**: k l m** n **o** p q **r** s t u v **w** x y z a b c d **e** f g h i j k l m n o p q **r** s t u v w x ….

Fibonacci Series: 1 2 3 5 8 13 21 34 55 89 144 233.....and so on.

Cipher Text: klmorwermuxi

Cipher text to decimal numbers

In the second level of security, the required decimal numbers are obtained by the sum of the ASCII code of each character obtained from the cipher text and the ASCII code of the equivalent character in the original message. Hence, the secret data is converted into a set of decimal numbers.

Decimal Number Vector thus obtained:[180 187 178 143 194 204 177 181 181 196 207 180]

Decryption

Decimal Number Vector:[180 187 178 143 194 204 177 181 204 177 181 181 196 207 180]

Security Key: k

Characters**: k l m** n **o** p q **r** s t u v **w** x y z a b c d **e** f g h i j k l m n o p q **r** s t u v w x ….

Fibonacci Series: 1 2 3 5 8 13 21 34 55 89 144 233.....and so on.

Cipher Text: klmorwermuxi

Now the ASCII values of the individual characters in cipher text is subtracted from the obtained decimal number vector in order to get the original text.

Decimal number vector:[180 187 178 143 194 204 177 181 181 196 207 180]

180-107(k)=73(I)

187-108(l)=79(O)

178-109(m)=69(E)

143-111(o)=32( )

194-114(r)=80(P)

204-119(w)=85(U)

177-101(e)=76(L)

181-114(r)=67(C)

181-109(m)=72(H)

196-117(u)=79(O)

207-120(x)=87(W)

180-105(i)=75(K)

METHOD II: RIJNDAEL CRYPTOGRAPHIC ALGORITHM

Rijndael or The Advanced Encryption Standard (AES) is the specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST).It is

based on a design principle known as substitution permutation network.It has a fixed block size of 128 bits, and a key size of 128,192 or 256 bits.There are four main steps which applies for both encryption and decryption where each stage of a round in the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

Sub Bytes Transformation: It is a non-linear substitution step in which each byte is replaced with another according to the entries in a lookup table called an S-box. ASbox is a one to one mapping for all byte values from 0 to 255.

Shift Rows: It is a transposition step in which each row of the state is shifted cyclically at a certain number of steps. . The rows are shifted x number of bytes to the left where x is the row number.

Mix Columns: After applying the S-box and shift rows operation to the state, the operation of a MixColumn is used. In this step a mixing operation is operated on the columns of the state, combining the four bytes in each column.

Add Round Key: The RIJNDAEL key expansion algorithm takes as input a 4-word (16-byte) key and gives a linear array of words, providing a 4-word round key for the initial Add Round Key stage and each of the 10 rounds of the cipher. It involves copying the key first in to the group of 4 words, and then constructing subsequent groups of 4 based on the values of the previous 4th words. Finally, we get the cipher text.

For decryption all layers must actually be inverted, i.e., the Byte Substitution layer becomes the Inv Byte Substitution layer, the Shift Rows layer becomes the InvShift Rows layer, and the Mix Column layer becomes InvMix Column layer. However, the inverse layer operations are fairly similar to the layer operations used for encryption.

IMPROVED LSB ALGORITHM

In LSB Algorithm, only least significant bit is replaced by information bit but in Improved LSB, least significant bit is not directly changed. Here we introduce a secret key to protect the hidden information.

Cover image + secret key + secret information = stego image

Step 1: Take a cover image and divide it into three matrices (Red, Green and Blue).

Step 2: Get the secret key and convert it into 1D array of bit stream.

(Secret key and Red matrixes are used only for decision making to allocate the secret information bits into either Green matrix or Blue matrix).

Step 3: Perform XOR operation between each bit of secret key with the each LSB of Red matrix. (The resulting XOR value decides whether to hide information on Green matrix or the Blue matrix.)

Step 4: If the XOR value is 1 then replace the LSB of Green matrix by the first bit of secret information. If the XOR value is 0 then the LSB of Blue matrix is replaced by the first bit of secret information and it is continued as until all the bits are hidden.

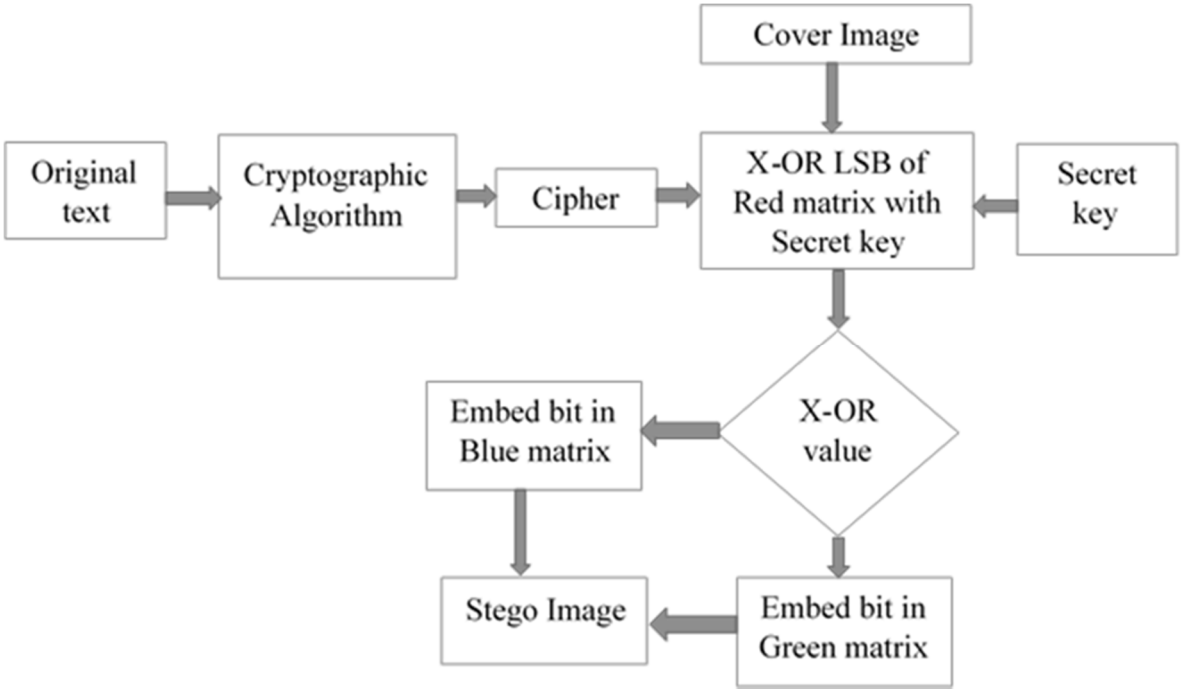


Fig 2 Flowchart of Improved LSB Algorithm

Message Extraction Process

To recover the hidden information, the stego image is divided into three matrices (Red, Green and Blue).Now the bits from the secret key is X-ORed with the bits from the LSB of Red matrix. If the XOR value is 1 then the secret bit should be taken from the LSB of Green matrix. And if the XOR value is 0 then the secret bit should be taken from the LSB of Blue matrix. In this way, the secret bits from are extracted and stored to get the required secret information. Thus obtained secret information is the cipher text which is to be decrypted using the cryptographic algorithms discussed above.

Usually, the invisibility of the hidden message is measured in terms of the Peak Signal-to-Noise Ratio [4]. To analyze the quality of the embedded texture image with respect to the original, the measure of PSNR will be employed,

$$\text{PSNR} = 10\log_{10} \frac{255^2}{MSE}$$

where mean square error (MSE) is a measure used to quantify the difference between the cover image I and the stego (distorted) image I'. If the image has a size of M * N then

$$MSE = \frac{1}{MxN} \sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - \Gamma(i,j)]^2$$

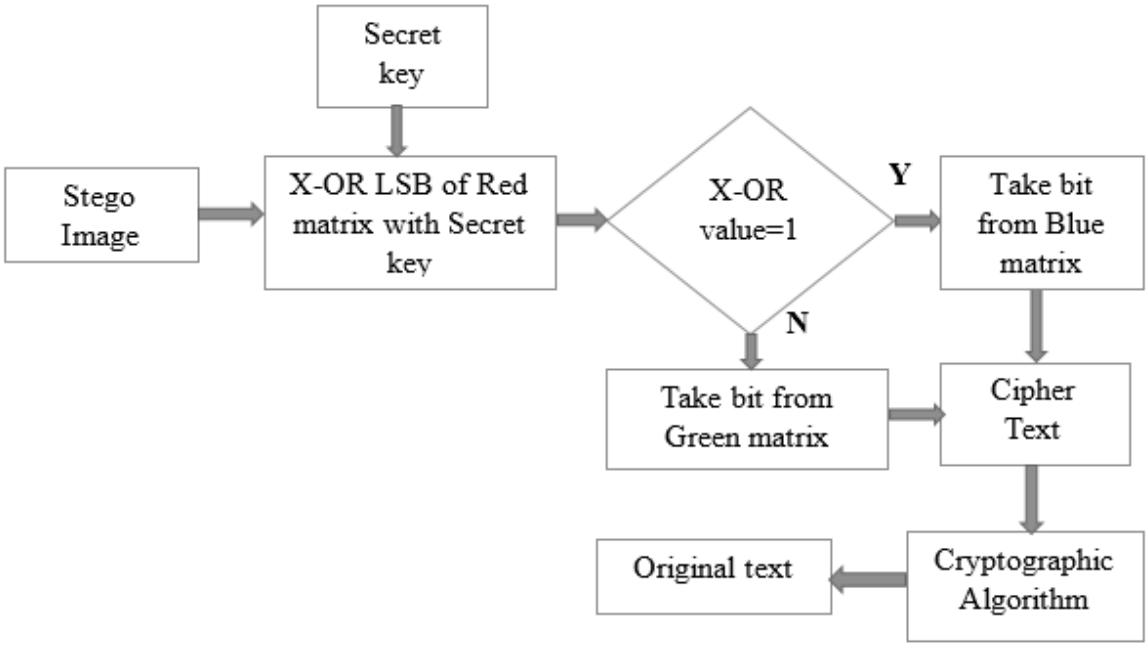
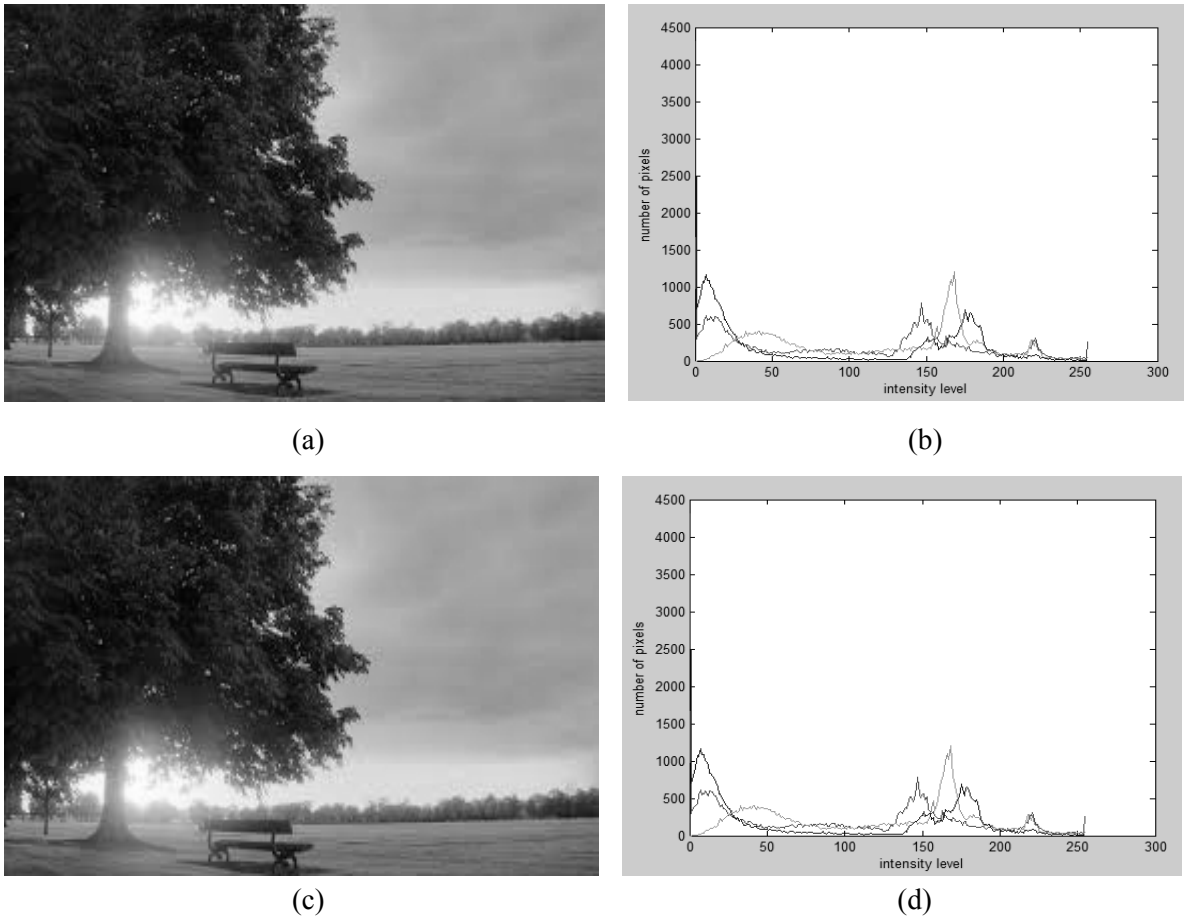


Fig 3 Flowchart of Message Extraction Process



(a) (b)

(c) (d)

Fig 4 (a) Original Image (b) Histogram of Original Image (c) Stego Image (d) Histogram of Stego Image

Fig 5

Fig 6

Table 1 Comparative analysis of LSB Substitution and Improved LSB Substitution

Images	LSB substitution		Improved LSB substitution	
	MSE	PSNR	MSE	PSNR
Figure 4 (Image 1)	0.0041	72.0236	0.0036	72.6236
Figure 5 (Image 2)	0.0025	74.132	0.0019	75.3167
Figure 6 (Image 3)	0.0025	74.2362	0.0015	76.236

4. Conclusion

Cryptography has evolved from an ancient science to an important area of research to secure communications. By the use of cryptography along with steganography for secure communication, we can safe guard ourselves from being compromised by those who could steal our information. Hence, an efficient image steganography algorithm has been made more secure with the help of cryptographic algorithms based on Fibonacci series and Rijndael cryptographic algorithm. The combination of these two methods will enhance the security of the data embedded. With the negligible difference in original image and stego image, the embedded information can be transmitted securely. The increase in complexity level in retrieving information further enhances the security of secret data in improved LSB substitution. Compared with Least Significant Bit Substitution, Improved Least Significant Bit substitution has lower MSE and higher PSNR. This shows that Improved Least Significant Bit substitution is an improvement over simple Least Significant Bit substitution. Hence, this combinational methodology provides resistance against various visual and statistical attacks.

References

1. Raphael, J., Sundaram, V. *"Secured communication through Fibonacci series and Unicode symbols"*. International journal of scientific and engineering research, Volume 3, Issue 4, 2012, 1-5.

2. Gangwar, A. Shrivastava, V. *"Improved RGB-LSB Steganography Using Secret Key"*, International Journal of Computer Trends and Technology-Volume 4, Issue2-2013

3. Patel, K., Vishwakarma, S., *"Triple Security of Information Using Steganography and Cryptography"*. International journal of Emerging Technology and Advance Engineering, 2013

4. Caldwell, J., *"Steganography using the technique of orderly changing pixel component",* International Journal of Computer Applications, Vol.58, No.6, 2014.

5. Sumathi C. P. and Santanam T., *"A Study of Various Steganographic Techniques Used for Information Hiding"*, International Journal of Computer Science & Engineering Survey, 2013

6. Ahmad M. A. et al., *"Achieving Security for Images by LSB and MD5"*, Journal of Advanced Computer Science and Technology Research, 2012

7. Zhang T. and Ping X., "*Reliable detection of LSB steganography based on the difference image histogram*", IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 3, pp.545-548 April 2003.

8. Zhi Li, Fen Sui Ai., *"Detection of Random LSB Image Steganography",* The IEEE 2003 International Symposium on Persona1, lndoor and Mobile Radio Communication Proceedings, 2004.

9. Li, C., Xu, W., Meng, L., Liu, B., Wang, Y. and Wu, L. ; *" Realization of a LSB Information Hiding algorithm Based on Lifting Wavelet Transform Image"*, International Conference on Mechatronic Science, Electric Engineering and Computer, pp.1015-1018, 2011.

10. Joseph Raphael A. and Sundaram V., *"Secured crypto stegano communication through unicode symbols",* World of computer science and information technology journal, Volume 1, 2011.

11. Fabien A. P., Petitcolas, F. A. P., Anderson R. J. and Kuhn M. G. *"Information Hiding: A Survey"*, Proceedings of the IEEE, Vol. 87, No. 7, pp. 1062-1078, 1999.

12. Provos, N. &Honeyman, P.; *"Hide and Seek: An introduction to steganography"*, Security and Privacy, Vol.1, pp.32-44, 2003.

13 Shirali-Shahreza, S. and Shirali-Shahreza M.; *"Steganography in Textiles"*, 4th International Conference on Information Assurance and Security, pp.56-61, 2008.

14. Singh, K. M., Singh, L. S., Singh, A. B. and Devi, K. S.; *"Hiding Secret Message in Edges of the Image"*, International Conference on Informationand Communication Technology (ICICT), pp.238-241, 2007.

15. Rahate, N. D. and Rothe, P. R.; *"Data Hiding Technique for Security by using Image Steganography"*, International Conference on Industrial Automationand Computing (ICIAC),pp. 33-36, 2014.

16. Daemen J. and Rijmen V., "*AES Proposal: Rijndael"*, AES Algorithm Submission, September 3, 1999.