International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol. 8, No. 5 (2015), pp. 259-266
http://dx.doi.org/10.14257/ijsip.2015.8.5.27

Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm

Satwinder Singh and Varinder Kaur Attri

Computer Science & Engineering Department
GNDU RC, Jalandhar, India
er.satwindermehmi@gmail.com, varinder2002@yahoo.com

Abstract

In today's scenario security of data is very big challenge in any communication. Numerous data security and hiding algorithms have been developed in the last decade. The Digital image Steganography is science of hiding sensitive information in another transmission medium to achieve secure and secret communication. In this paper we present the dual layer of security to the data, in which first layer is to encode data using Least Significant Bit image steganography method and in the second layer encrypt the data using Advance Encryption Standard Algorithm. Steganography does not replace the encryption of data, instead it provides extra security feature to it. In our work secret text message is hiding behind the digital image file and this image file is then encrypted using AES encryption algorithm.

Keywords: *Steganography, AES Algorithm, Digital Image, LSB, Encryption, Security*

1. Introduction

1.1. LSB Image Steganography

The word "Steganography" is a Greek word which means "covered or hidden writing". In other words Steganography is technique of hiding information behind the cover medium. Steganography can be done with Text, images, video, audio media and protocol steganography. In our work we are going to use digital image steganography because digital images have a large amount of redundant data and for this reason it is possible to hide message inside image file [1]. Image Steganography requires following elements to carry out the work:

- **Cover medium:** It is an image that holds secret message.
- **The Secret message:** it is message to be transmitted. It can be plain or encrypted text, images or any other data.
- **The Stego-key:** it is key used to hide the message (May or may not be used).

Data is hidden in such a way that nobody notices its presence in cover medium. The main motive of steganography is to hide the existence of communication [2].

1.2. Advance Encryption Standard (AES-128 bits)

Advanced Encryption Standard (AES), also known as Rijindael is used for securing information. AES is a symmetric block cipher that has been analyzed extensively and is used widely now-a-days. AES, symmetric key encryption algorithm is used with key length of 128-bits for this purpose. High security, mathematical soundness, resistance to all known attacks, high encryption speed, worldwide royalty free use, suitability across wide range of hardware and software are the characteristics of AES algorithm. Loopholes are there in DES and 3DES encryption

ISSN: 2005-4254 IJSIP

algorithm but AES algorithm does not have such loopholes so far [3]. The basic structure of AES is shown in Figure 1.

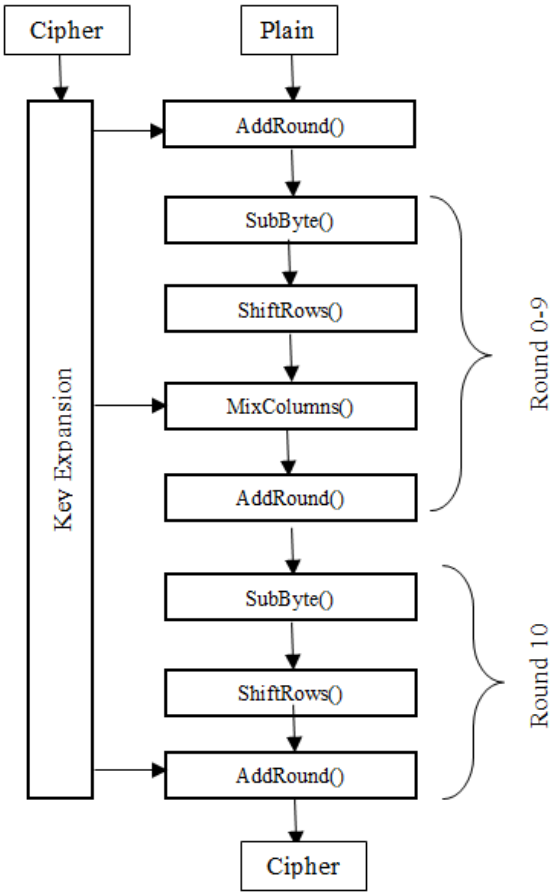

Figure 1. Basic Structure of AES 128 Bit Algorithm

AES Algorithm consists of mainly four transformations, namely:

- **SubBytes:** In this transformation S-Box is used to perform byte by byte substitution of the block. Non-Linearity in cipher is achieved by this transformation. Multiplicative inverse over GF (2^8) is used to derive the S-Box.
- **ShiftRows:** This transformation is performed on rows of the states. First row will remain unchanged but second, third and fourth row will be changed by cyclic one byte shift, two byte and three byte shift respectively. This operation makes columns linearly independent that's why AES degenerates four independent block ciphers.
- **MixColumns:** This transformation is performed on every column in the state. Invertible linear transformation is used to combine the four bytes of the each column of the state. This transformation is used to achieve diffusion in the cipher.
- **AddRoundKey:** Round key is combined with each byte of the state using bitwise XOR operation. 4X4 matrix is used to represent the original key consisting of 128 bits. This 4 word key is converted to a 43 words key.

2. Previous Work

There are lots of methods available that can be used to implement steganography using various multimedia content.

S.M. M. Karim et al. [4] proposed a new approach that provides very good security to data. They use LSB approach with secret key. This secret key is used to hide the sensitive information and this information is stored on different LSB's of image.

On the bases of Human visual system (HVS) X. Qing, *et al.*, [5] proposed a new technique in which sensitive information is embedded in all planes of RGB components of an image.

In [6] author proposes an enhanced LSB algorithm for image steganography. In this proposed work they only embed secret information in blue component of the RGB model. This method reduces the leap in color scale because only blue components are used to embed the secret information.

H. Yang, *et al.*, [7] presented a new adaptive LSB based method for image steganography. It uses the pixel adjustment technique for better stego image quality. This adaptive LSB substitution results in high hidden capacity.

Authors in [8] use the vector quantization table to embed the secret information by which the hidden capacity and stego size is increased.

Nouf A. Al-Otaibi, *et al.*, [9] designed a new system called 2-layer security system for hiding the sensitive information on personal computers. They divide the system in two layer namely cryptography layer and steganography layer. For steganography layer LSB algorithm is used. This system is designed on visual basic platform. Authors also done study on improving hidden capacity.

In [10] LSB based image steganography method is proposed. To hide the data common bit pattern is used. According to the message and the pattern bits LSB's of pixels are modified. This method has low hidden capacity.

Kamali, S.h., *et al.*, [11] analyze and present the modified AES image encryption algorithm (MAES) which provide greater security to image data. The modification done in ShiftRow transformation. The results also prove that the MAES gives better encryption results than original AES algorithm, against various statistical attacks.

3. Proposed Work

Data security is a biggest concern of any organization. We propose the work called "Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm". The main idea of our work is to provide dual layer of security to sensitive data or messages by hiding it behind the digital images using LSB image Steganography algorithm and the second layer encrypt this stego image using AES-128 bits encryption algorithm.

3.1. Structure of Proposed System

In our work we utilize both cryptography and steganography. In order to get more security to the data we combine both the technique. Proposed System consists of two layers, namely Steganography Layer and Encryption/Decryption Layer.

3.1.1. Steganography Layer: In this process first we have to provide two inputs to the LSB steganography algorithm. First input is cover image in which secret message is embedded and second is secret message itself. Output of this process is Stego Image (image with secret message). Figure 2(a) shows Embedding and encryption process and Figure 2(b) depicts how message extraction and decryption is done.

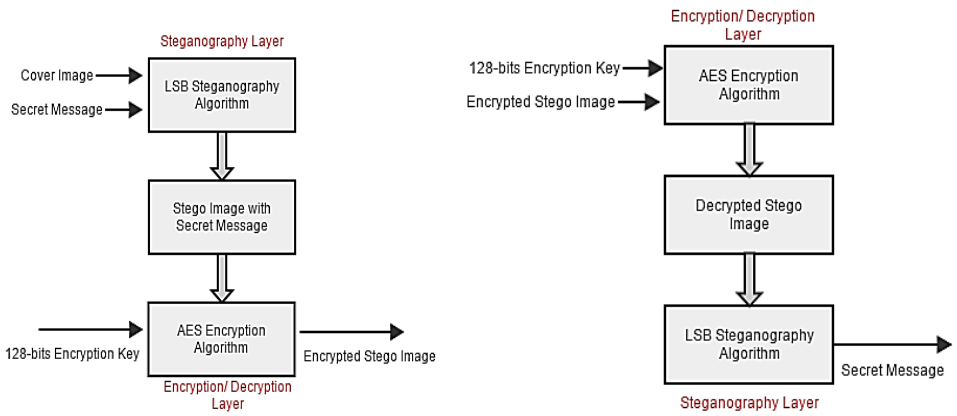

Figure 2. (a) Embedding and Encryption Process (b) Extraction and Decryption Process

The Steganography layer in our work uses the Least Significant Bit image steganography algorithm. If the LSB of the pixel value of cover image C(i,j) is equal to the message bit SM of secret massage to be embedded, C(i,j) remain unchanged; if not, set the LSB of C(i, j) to SM. The message embedding Procedure is given below:

$$S(i,j) = C(i,j) - 1, \text{ if } LSB(C(i,j)) = 1 \text{ and } SM = 0$$
$$S(i,j) = C(i,j) + 1, \text{ if } LSB(C(i,j)) = 0 \text{ and } SM = 1$$
$$S(I,j) = C(i,j), \text{ if } LSB(C(i,j)) = SM$$

Where LSB(C(i, j)) stands for the LSB of cover image C(i,j) and "SM" is the next message bit to be embedded. S(i,j) is the stego image. The Basic idea behind LSB algorithm is explained by an example of hiding alphabet "S" whose ASCII code is 83 and in binary form it is 1010011. These binary bits are embedded into Least Significant Bit of Pixel value. Take a three pixel Values as follows:

Pixels before Embedding:

Pixel 1: 10001100	01001111	00001111
Pixel 2: 01010100	11010101	11011010
Pixel 3: 11101000	11110110	10000001

Pixels after Embedding "1010011", *i.e.*, alphabet "S" using LSB Algorithm:

Pixel 1: 1000110**1**	0100111**0**	00001111
Pixel 2: 01010100	1101010**0**	1101101**1**
Pixel 3: 1110100**1**	11110110	10000001

In the above example note that only five bits have been changed out of nine bits. It depends upon the secret message that is to be embedded.

Digital images can be of two types 8 bit or 24 bit. In 8 bits image only one bit of information can be embedded. But in 24 bits image we can embed three bits of information in each pixel as shown in above example. A picture of resolution of 800×600 can store 1,440,00 bits of embedded data [12]. Changing the LSB of each pixel does not affect the appearance of the original image and hence the Stego-image looks almost similar to the cover image. LSB is simplest algorithm with high payload capacity.

3.1.2. Encryption/Decryption Layer: The core of second layer in our system is AES 128 bits Encryption algorithm. The output of first layer is Stego image with embedded secret message in it. In this layer we encrypt the stego image with AES algorithm by providing 128 bits public key for encryption. In the receiver end reverse process is applied by decrypting the stego image.

4. Implementation and Discussion

The dual layer security of data using LSB and AES is implemented in JAVA programming using NetBeans IDE. We use java language for implementation due to its flexibility and robustness and many more useful features. The main objective of this implementation is to study the dual layer security system in greater details and to analyze the various situations to enhance its importance in academic research field as well as industrial research. Application starts its work with steganography layer by asking cover media i.e. RGB image in which secret message is to be embedded and the secret message itself. Images are of different formats such JPEG, BMP or PNG etc. They make use of different Compression techniques such as Lossy and Lossless [13]. In our work we make use of lossless compression Images i.e. Bitmap (.bmp) and Portable Network Graphic (.png). Each RGB image has three color components (Red, Green, and Blue) each of which is 8 bits [14]. So we hide the data in every least significant bit of each color component to achieve steganography.

4.1. Embedding Data using LSB Embedding Process

The implementation interface of dual layer data security system is shown in the following figures. There are open, embed, save file and reset button to carry out the process. In Figure 3 cover image is the original image and after embedding the message, it is shown on right hand side of the interface under the stego image block. Now the both images look similar but the stego image has that secret message embedded in it.

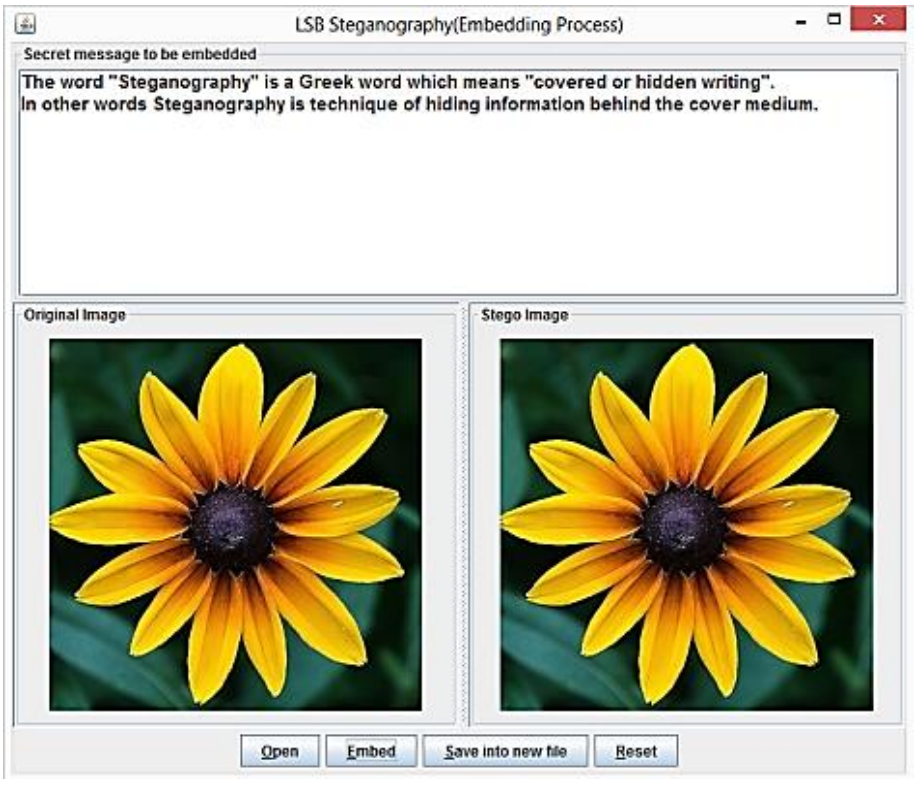

Figure 3. Steganography Layer (Embedding Process)

4.2. Encrypting /Decrypting Stego Image using AES 128 bit Algorithm

Encryption/Decryption layer shown in Figure 4. We provide stego image and 16 characters (128 bits) encryption key as input to this layer and the output of this layer is encrypted stego image shown in figure 6(c). Stego image is encrypted using AES 128 bit algorithm because of its numerous advantages over other encryption algorithms and there is no brute force and cryptanalysis has been encountered on AES [15].

Figure 4. Encryption/Decryption Layer

On the receiver end the user use same 128 bit encryption key to decrypt the stego image. Output of this decryption process is original stego image. This stego image is then provided to steganography layer to get the desire secret message.

4.3. Extracting data using LSB Extraction Process

Extraction process starts with providing the decrypted stego image to the system. After clicking on decode button user will get the desire secret message that was embedded using LSB steganography during embedding process. Figure 5 shows the interface of system that is used to extract the message using decrypted stego image.

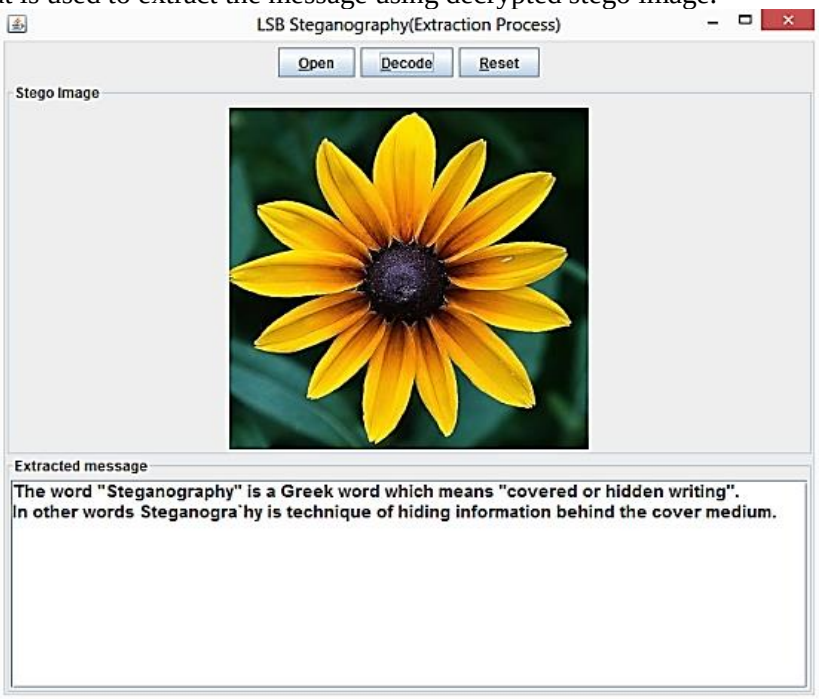

Figure 5. Steganography Layer (Extraction Process)

4.4. Comparison between Cover Image, stego and Encrypted Stego Image

In this section all the three possible images are observed, *i.e.*, cover image, stego and encrypted stego image as shown in Figure 6(a), 6(b), and 6(c). As we observed that there is no difference in both the stego and cover image. Nobody can observe the usage of steganography to hide the data in cover image and changes are so minimal that human eye can't even see. Changes in image are done at pixel level that is almost unnoticeable which leads to high security. After the encryption of stego image, it becomes encrypted as shown in Figure 6(c).

(a) (b) (c)

Figure 6. (a) Cover Image (b) Stego image (c) Encrypted Stego Image

5. Conclusion and Future Work

In our work we have presented how to provide the dual layer security to sensitive data. We combine both the steganography and cryptography (Encryption/ Decryption) together to achieve desire results. The system is implemented on Java platform using Netbeans IDE. For image steganography we have used simplest yet effective method called LSB image steganography algorithm. For the encryption/decryption layer we have use error less AES encryption algorithm. In future work, we try to work on steganography layer by enhancing the current LSB algorithm. We can also work on other steganography techniques to improve upon the results. We can also test our test with other symmetric and asymmetric key encryption algorithms.

References

[1] R. Chandramouli and N. Memon, "Analysis of LSB based Image Steganography Techniques", Proceeding of IEEE International Conference on Image Processing, **(2001)** October 7-10, Thessaloniki, Greece.

[2] K. B. Raja, C. R. Chowdary, K. R. Venugopal and L. M. Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", Proceeding of 3rd IEEE International conference on Intelligent Sensing and Information Processing (ICISIP), **(2005)** December; Bangalore, India.

[3] S. Singh and R. Maini, "Comparison of Data Encryption Algorithms", International Journal of Computer Science and Communication, vol. 2, no. 1, **(2011)**.

[4] S. M. M. Karim, M. S. Rahman and M. I. Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", Proceedings of 14th IEEE International Conference on Computer and Information Technology, **(2011)** December 22-24, Dhaka, Bangladesh.

[5] X. Qing, X. Jianquan and X. Yunhua, "A High Capacity Information Hiding Algorithm in Color Image", Proceedings of 2nd IEEE International Conference on E-Business and Information System Security, **(2010)** May 22-23, Wuhan, China.

[6] S. Gupta, G. Gujral and N. Aggarwal, "Enhanced Least Significant Bit Algorithm for Image Steganography", International Journal of Computational Engineering & Management, vol. 15 no. 4, **(2012)**.

[7] H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal of Radio Engineering, vol. 18, no. 4, **(2009)**.

[8] S. Sachdeva and A. Kumar, "Colour Image Steganography Based on Modified Quantization Table", Proceedings of IEEE 2nd International Conference on Advanced Computing & Communication Technologies, **(2012)** January 7-8, Rohtak, India.
[9] N. A. Al-Otaibi and A. A. Gutub, "2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers", Lecture Notes on Information Theory, vol. 2, no. 2, **(2014)**.
[10] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering (IJCSE), vol. 1, no. 3, **(2009)**.
[11] S. H. Kamali, R. Shakerian, M. Hedayati and M. Rahmani, "A new modified version of Advanced Encryption Standard based Algorithm for Image Encryption", proceeding of IEEE International Conference on Electronics and Information Engineering (ICEIE), **(2010)** August 1-3, Kyoto, Japan.
[12] J. R. Krenn, "Steganography and Steganalysis", **(2004)** January.
[13] T. Moerland, "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science.
[14] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", Computer Journal, **(1998)** February.
[15] A. Sachdev and M. Bansali, "Enhancing Cloud security using AES algorithm", International Journal of Computer Application, vol. 67, no. 9, **(2013)**.

