International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Secure Data Hiding System by using AES Algorithm and Indicator-Based LSB Method

Myo Ma Ma, Zar Zar Hnin, Yin Min Htwe

Lecturer, Faculty of Computer Science, University of Computer Studies, Mandalay, Myanmar

How to cite this paper: Myo Ma Ma | Zar Zar Hnin | Yin Min Htwe "Secure Data Hiding System by using AES Algorithm and Indicator-Based LSB Method" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.970-974, **https://doi.org/10.31142/ijtsrd26500**

IJTSRD26500

ABSTRACT

Security of data is one of the most challenging problems in today's technological world. In order to secure the transmission of secret data over the public network (Internet), numerous data security and hiding algorithms have been developed in the last decade. Steganography combined with cryptography can be one of the best choices for solving this problem. In this paper, the proposed framework is the dual layer of security, in which the first layer is to encrypt the secret text message using advanced encryption standard (AES) algorithm and in the second layer to embed this message using the indicator-based least significant bit (LSB) method which is used to hide the encrypted text message into the cover image. It differs from the LSB algorithm in that it does not embed the bytes of the cover data sequentially but it embeds into one bit or two bits at once. Actually, it depends on indicators to determine where and how many bits to embed at a time. The Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) measure the imperceptibility of the system. Experimental results show that the stego image is usually indistinguishable from the cover image.

KEYWORDS: *advanced encryption standard (AES) algorithm, indicator-based least significant bit (LSB) method, encryption, embedding, MSE, PSNR*

1. INTRODUCTION

Security is one of the major concerns which provide for the safe and secure transmission and receiving of data without any interference.

Internet is commonly used for the sharing of information. Since the Internet is an open channel of communication, there is a need to protect the confidential data from intruders that are transmitted over the Internet. To protect the secret data, cryptography and steganography techniques are widely used. A combination of these two techniques can be used to increase data security [1].

Cryptography and steganography are the major areas which work on information hiding and security. Cryptography means converting the text from readable format to unreadable format. It applies encryption techniques to convert the message into non-readable form but it does not hide the message i.e., the encrypted message is visible [2]. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately, it is sometimes not enough to keep the contents of a secret message, it may also be necessary to keep the existence of the message secret [3]. The technique used to implement this is called steganography.

Steganography hides secret data in a cover object. This cover object may be a digital media such as image, an audio file, video file or network/protocol. Steganography provides good security in itself and it also possible to combine with encryption to increase the security of the system. The word steganography is a Greek word; Stefanos mean covered or secret and graphy mean writing or drawing [4],[5],[6],[7]. Therefore, the meaning of steganography is hidden writing. Secret information is embedding in a manner such that the existence of the information is hidden. The purpose of steganography is to avoid drawing suspicion to the existing communication.

This paper is providing the security to the communication channel thereby preventing attackers from hacking secure text message. The AES and indicator-based LSB method will be provided the two layers of security which make difficult to detect the presence of a hidden secret text message.

The rest of this paper is organized as follows: In Section 2, a brief review of the related work is presented. In Section 3, AES algorithm, indicator-based LSB method, experiment and result and performance are described. Finally, Section 4 concludes the paper.

2. RELATED WORK

Internet is essential and fastest media for communication in the modern era. In data communication, it is susceptible to face many problems such as copyright protection, hacking, eavesdropping etc. Security in communication is highly appreciable. Cryptography and steganography are different techniques for data security.

This paper [9] is focused on spatial domain technique i.e. LSB technique of image steganography. The method used in the paper hides the data in a combination of LSBs instead of hiding the data only in the least significant one bit.

Combination of bits used is LSB (1, 2) bits and (2, 3) bits. Results are compared qualitatively using parameters PSNR, MSE, BER, Entropy, Standard deviation.

Paruchuri [10] proposed a system in which steganography is combined with cryptography to enhance security. First the message to be sent is embedded into a cover image using steganography and the stego image is encrypted to produce the cipher image. The cipher image is then sending to the recipient. This approach is secure, but the existence of the message is not hidden since the encryption is done after steganography and the cipher image is sent to the recipient. The cipher image does not resemble the cover image and will be distorted.

In [11], Ajit Singh and Swati Malik proposed a combination of steganography and cryptography has been used for improving the security. The blowfish encryption algorithm is encrypting the message to be hidden inside the image for making it non readable and secure. After encryption, this paper will be applied LSB technique of steganography for further enhancing the security. For cryptography, Blowfish algorithm is used which is much better than AES and DES but LSB technique for hiding the encrypted file is easy to detect the secret message as it is directly replaced into the least significant bit of the pixels of the image.

In the proposed framework system [12], the data is dual encrypted and the resultant cipher is then embedded within an image using LSB steganographic technique to ensure secrecy and privacy. The encryption algorithms used are much secure as each step in the process is fully dependent on the key. The LSB steganographic technique hides the data in the least significant bits of the pixels of the image and therefore the reflected change in the stego image is hardly noticeable to the human eye. The key management for the system is done using the RSA encryption technique. These two algorithms are computational complexity for the encryption process and for hiding process; the hidden data can be easily destroyed by the third party.

This research [13] discussed the data hiding information using steganography and cryptography. The steganographic method is used to find the similarity bit of the message with a bit of the MSB (Most Significant Bit) image cover. The finding of similarity process is done by divide and conquer method. The results are bit index position and then encrypted using cryptographic. In this paper we using DES (Data Encryption Standard) algorithm. The experiment with adding noise to the image has been caused some changes in the message content. In the black and white image, the changes are not significant, while in the colorful image the message content has been changed a lot. Damage occurred on the addition of salt and pepper noise start from MSE 0.00049.

This paper [14] presented to provide the transfer of secret data embedded into a master file (cover-image) to obtain new image (stego-image), which is practically indistinguishable from the original image, so that other than the indeed user, can not detect the presence of the secrete data sent. Least Significant Bit (LSB) and Pseudo-Random Number Generator (PRGN) are used to hide the secret data. The proposed approach is better in PSNR value and capacity as shown experimentally than existing techniques.

Steganography is a message hiding technique so that a user can send or communicate to the other user about their secret message securely. LSB is one of the most popular techniques in image steganography which are used for hiding the secret message. So LSB technique for hiding the encrypted file is easy to detect the secret message as it is directly replaced into the least significant bit of the pixels of the cover image. Therefore there may be one possibility to remove this problem and will make the secret message more secure and enhance the quality of the image is proposed.

3. METHODOLOGY

AES algorithm is firstly to transform secret messages into unintelligible forms, thus whoever does not have the secret key cannot obtain the original message. Secondly, the indicator-based LSB method is randomly dispersing the bits of the encrypted message in the cover image and thus making it harder for unauthorized people to extract the original message. This indicator-based method is the randomness used to confuse intruders as it does not use fixed sequential bytes and it does not always embed one bit at a time. The block diagram of the AES algorithm and indicator-based LSB method are described as Fig.1.

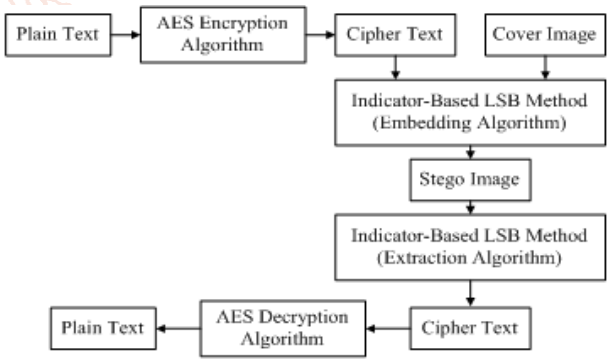

Figure1. Block diagram of the AES algorithm and indicator-based LSB method

3.1. Advanced Encryption Standard

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 nowadays. The plain text (secret text) must be 128 bits because the block size is 128 bits in AES. In the proposed system, the key size 128 bits choose as standard key size. Also, 192 bits and 256 bits are strong keys, but the key is so long and difficult to remember. The block diagram of AES 128-bit algorithm is shown in Fig.2.
The plain text (secret text) of size 128bits is given as input using a symmetric key enables to perform four-step operations to get the ciphertext (unreadable form). The four-step operations involve the substitution of bytes, shifting rows, mixing of columns, and add round key. This encryption and decryption processes of AES consist of four-step operations undergo 10 rounds. These four steps are namely as follow:

1. **SubBytes:** AES contains 128-bit data block, which means each of the data blocks has 16 bytes. In sub-byte or substitute byte transformation, each byte (8-bit) of a data block is transformed into another block using an 8-bit substitution box which is known as Rijndael S-box.
2. **Shift Rows:** It is a simple byte transposition. The bytes in the last three rows of the state, depending upon the row location, are cyclically shifted. The first row is not shifted,

the second row is circularly left-shifted by one-byte position, the third row is circularly left-shifted by two-byte position, and the last row circularly left-shifted by three-bit positions.

3. MixColumns: A round is equivalent to a matrix multiplication of each column of the states. A fix matrix is multiplied to each column vector. In this operation, the bytes are taken as polynomials rather than numbers.

4. AddRoundKey: Round key is combined with each byte of the state using bitwise XOR operation. The 4X4 matrix is used to represent the original key consisting of 128 bits. This 4-word key is converted to a 43 words key.

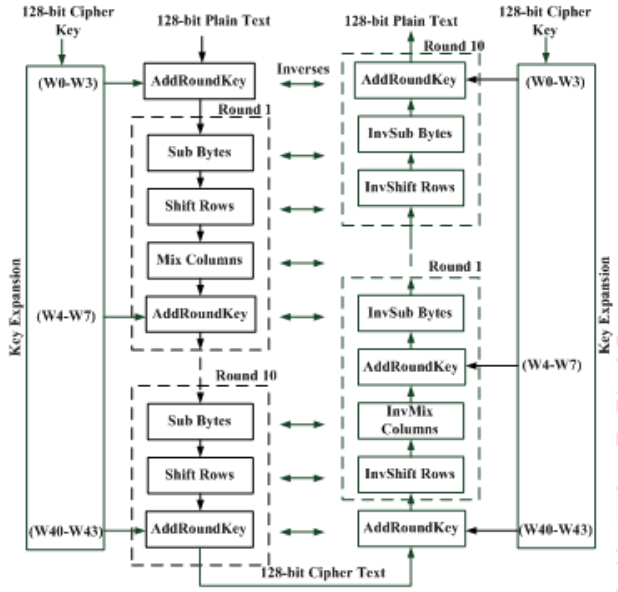

Figure2. Block diagram of AES 128-bit algorithm

Decryption algorithm uses the expanded key in reverse order. All functions are easily reversible and their inverse form is used in decryption. Decryption algorithm is not identical to the encryption algorithm. In the beginning, there is a pre-round operation using the ciphertext as the state matrix and the last round key as the key matrix (i.e. W40 to W43). The final round consists of only three stages. Mix-column operation is omitted here.

3.2. Indicator-Based LSB Method

The indicator byte is a fixed bit in every byte of the cover bytes other than the least two bits because the last two bits are used to hide the secret data. Firstly, byte array [0] is assigned the previous byte, byte array [1] is set indicator byte and after indicator byte is next byte as byte array [2]. The first-bit position of indicator byte is assumed index 4 from the right of RGB byte array which determines the previous or next bytes for hiding the secret bits. Let the second-bit position of indicator byte be index 3 from the right of RGB byte array. The indicator-based LSB method consists of first-bit position and second-bit position as shown in Figure.3

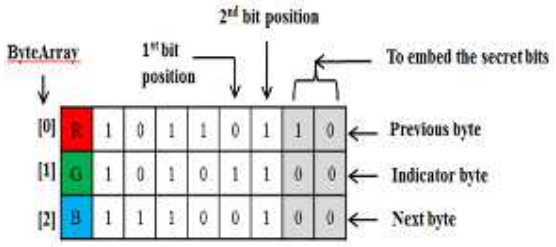

Figure3. Indicator-based LSB method

The indicator-based LSB method consists of previous bytes, indicator byte and next bytes. This indicator byte is included two-bit positions of RGB bytes array of cover image pixels. The first-bit position of indicator byte determines the previous or next bytes for hiding the secret bits. The second-bit position of indicator byte determines for hiding one or two bits of secret data bits. Embedded secret bits depend on the bit positions of indicator byte of cover image as shown in Table 1.

Table1. Embedded Secret Bits Depend on Indicator Bytes

Indicator Byte		Embedded Secret Bits
1st Bit Position	2nd Bit Position	
0	0	1 bit of secret bits are hidden into the previous byte of RGB bytes array of the cover image
0	1	2 bits of secret bits are hidden into the previous byte of RGB bytes array of the cover image
1	0	1 bit of secret bits are hidden into the next byte of RGB bytes array of the cover image
1	1	2 bits of secret bits are hidden into the next byte of RGB bytes array of the cover image

Figure 4 shows the flow chart of the hiding process. All of these factors increase the randomness and confusion of the hiding process, which makes it hard to retrieve the secret data by unauthorized parties. The hiding process is not done sequentially like simple LSB. The secret bits are hidden into cover bytes randomly depending on the values of the two bits position of indicator byte of the cover image.

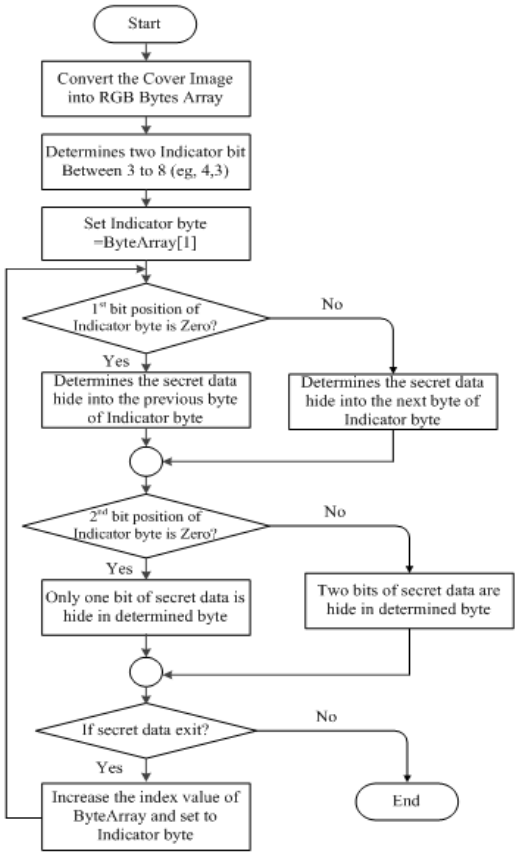

Figure4. Flow chart of hiding process of indicator-based LSB method

3.3. Peak Signal to Noise Ratio

The evaluation of the quality of the stego image is evaluated by using the peak signal-to-noise ratio (PSNR), the most popular measurements of steganography performance. PSNR is expressed in terms of a logarithmic decibel scale. The PSNR value is defined as follows:

$$PSNR=10\log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (1)$$

Where MAX is the maximum possible pixel value of the images. For example, if the pixels are represented using 8 bits per sample, then the MAX value is 255.

3.4. Mean Square Error

MSE is the mean square error between the cover and stego images which is described as the following equation 2:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(f(i,j)-g(i,j))^2 \quad (2)$$

Where f represents the matrix data of the original image, g represents the matrix data of stego image, m represents the numbers of rows of pixels of the images and i represents the index of that row, n represents the number of columns of pixels of the image and j represents the index of that column.

3.5. Experiment and Result

This approach was implemented and tested on photos without any noticeable. This is because the approach uses the LSB technique for hiding data, and this technique does not make any noticeable modification in the carrier medium. A carrier image before and after the hiding process is shown in Figure 5 and 6.

Figure5. The cover image

Figure6. The Stego image

3.6. Performance

The most popular measurements of steganography performance are MSE and PSNR. As a consequence there are 256 possibilities of varying intensities of each primary color, altering the most significant bit of pixel results in only a small change in the intensity of the color. These small changes cannot be perceived by the human eye and thus the message is successfully hidden. Our method is applied on only image size for 125x125 of the 24-bit color image; Lena. Capacity can save as maximum between 5.72 bytes and 11.44 kbytes. The MSE should be as less as possible. If the original image and the stego image are the same then MSE is zero. Higher PSNR value means lesser distortion. The results of MSE and PSNR are given in below Table 2.

Table2. MSE and PSNR Values

Image Size (pixels)	Hidden Message Size (KB)	MSE	PSNR (dB)
125x125	0.05	0.008	69.1
125x125	0.19	0.03	63.36
125x125	1	0.172	55.776
125x125	2	0.346	52.74
125x125	3	0.517	50.996
125x125	4	0.692	49.73
125x125	5	0.873	48.721
125x125	5.38	0.939	48.404
125x125	5.59	0.975	48.241
125x125	5.72	1.007	48.101
125x125	8.58	1.497	46.379

A PSNR value is more than 40 decibels (dB) is very good. If it is between 30 dB and 40 dB, can be acceptable, but a PSNR less than 30 dB is not acceptable because the distortion is very high. The experimental results show that the proposed scheme can embed 8.58 kbytes of information while keeping an acceptable visual quality in Figure 7.

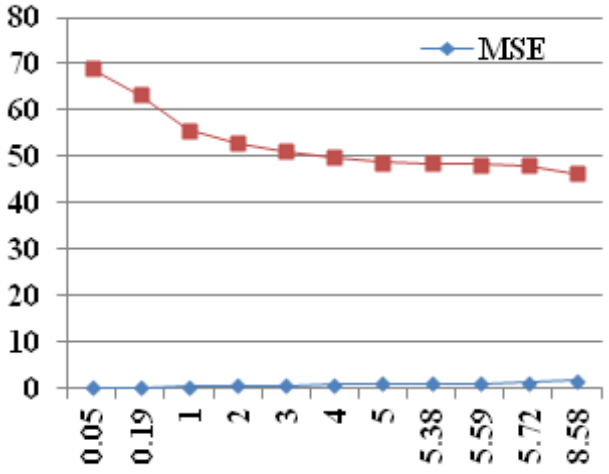

Figure7. MSE and PSNR values versus secret message size

Figure 8 shows PSNR values versus message size for 125x125 pixels of the cover image.

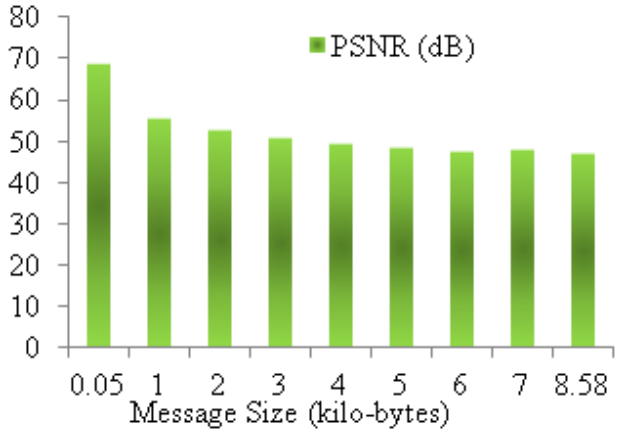

Figure8. PSNR Values versus Message Size for 125x125 Pixels of Cover Image

4. CONCLUSIONS

This paper has combined both cryptographies which is used for encryption and decryption algorithms and steganography which is used for embedding and extraction algorithms together to achieve the desired results. The security of the secret text message is one of the most important in today's technological world. Encryption technique plays an important role in the information security system. AES algorithm is used a block size of 128-bit with 128-bit key size to encrypt and decrypt text data for 10 rounds. The randomness of the indicator-based method is based on the LSB method which makes it harder for unauthorized parties to detect and retrieve the hidden data. This indicator-based LSB method is provided the position and determined the number of embedded bits. The AES and indicator-based LSB method are embedded 8.58 kilo-bytes of data with an acceptable visual quality which has greater than 40dB of PSNR. This method has increased the security of the system and will also be increased the capacity compared with simple LSB as it sometimes hides two bits at once.

5. ACKNOWLEDGMENTS

My thanks go to all of my teachers and I would like to express my deep appreciation to my dearest parents who have always given great help, encouragement, sacrifice and support throughout my life.

6. REFERENCES

[1] Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for Data Hiding", IBM Systems Journal, Vol. 35, Issue 3-4, 1996, pp. 313-336.

[2] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography", IEEE Conference on Security and Privacy, pp. 32-44, 2003.

[3] Miss. Vaishali V. Jadhav, Mrs. P.P. Belagali, "An Effective Image Steganography using LSB Matching Revisited", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 3, March 2016.

[4] Amitava Nag, Saswati Ghosh, "An Image Steganography Technique using X-Box Mapping", IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012.

[5] Tanmay Bhattacharya, Nilanjan Dey, S. R. Bhadra Chaudhuri, "A Session-based Multiple Image Hiding Technique using DWT and DCT", International Journal of Computer Applications (0975 – 8887), Volume 38– No.5, January 2012.

[6] V. Nagaraj, Dr. V. Vijayalakshmi, Dr. G. Zayaraz, "Modulo based Image Steganography Technique against Statistical and Histogram Analysis", IJCA Special Issue on "Network Security and Cryptography" NSC, 2011.

[7] Er. Mahender Singh, Er. Rohini Sharma, Er. Dinesh Garg, "A New Purposed Issue for Secure Image Steganography Technique Based On 2-D Block DCT and DCT", ijarcsse, Volume 2, Issue 7, July 2012.

[8] Dhawal Seth, L. Ramanathan, "Security Enhancement: Combining Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, November 2010.

[9] Ramanpreet Kaur, "A Comparative Study of Combination of Different Bit Positions in Image Steganography", International Journal of Modern Engineering Research (IJMER), www.ijmer.com, Vol.2, Issue.5, pp-3835-3840, Sep-Oct, 2012.

[10] Dr. R. Sridevi, Vijaya, Paruchuri, K. S. SadaShiva Rao, "Image Steganography combined with Cryptography", Council for Innovative Research Peer Review Research Publishing System Journal: IJCT Vol 9, No.1, ISSN 22773061 976/ Page July 15, 2013. editor@cirworld.com

[11] Ajit Singh, Swati Malik, "Securing Data by Using Cryptography with Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[12] A Aswathy Nair, Deepu Job, "A Secure Dual Encryption Scheme Combined With Steganography", International Journal of Engineering Trends and Technology (IJETT) – Volume 13 Number 5 – Jul 2014.

[13] Alamsyah, Much Aziz Muslim, Budi Prasetiyo, "Data Hiding Security Using Bit Matching-Based Steganography and Cryptography without Change the Stego Image Quality", Journal of Theoretical and Applied Information Technology Vol.82. No.1, 10th December 2015.

[14] Nadia Mohammed, "Increasing Security in Steganography by Combining LSB and PRGN", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.2, February- 2016, pg. 34-38.