Journal of Engineering Science and Technology
Vol. 14, No. 3 (2019) 1434 - 1450

SECURE AND HIDDEN TEXT USING AES CRYPTOGRAPHY AND LSB STEGANOGRAPHY

MAY HATTIM ABOOD*, ZAHRAA KHUDHAIR TAHA

College of Engineering, Al Iraqia University, Baghdad-Iraq
*Corresponding Author: may_it2004@yahoo.com

Abstract

For secure data transmission over the internet, it is important to transfer data in high security and high confidentiality, information security is the most important issue of data communication in networks and the internet. Our main goal of this paper is to enhance the existing method of secure data communication possibly by combination cryptography and steganography. Cryptography and Steganography are two popular ways to transmit information in a secret way. In this paper, the Advanced Encryption Standard (AES) algorithm is utilised to change over content from its unique structure (plain text) to incoherent structure (figure content) then figure content is concealed in the picture by Least Significant Bit (LSB). The content is encoded with key 128 bit. Indeed, even with an alternate arrangement sorts and diverse sizes of the chosen pictures is utilised to cover up scrambled content. The experiments demonstrate the span of the spread picture influences the nature of the stego picture; in these manner quality, PSNR increments and the MSE decreases with the expansive size of spread picture. The outcomes demonstrate the suggested technique is powerful and add Security levels for information transfer.

Keywords: Advance encryption standard, Ciphertext, Cover image, Cryptography, Least significant bit, Plain text, Steganography, Stego image.

1. Introduction

Due to the increasing amount of data being exchanged over the internet, more secure messages is required. The vast number of clients requires security, especially since the numerous usage of PCs, networks, and the Internet with its worldwide availability [1].

There are many techniques is used to protect the user data. One such technique is cryptography that is the art of conversion the readable original data from a state to evident babble [2, 3]. In the encryption process, confidential data is encrypted into the cypher form, which it became very hard (even impossible for unauthorised to recognize or read data [4].

The second technique is Steganography, where the data is covered up inside any sight and sound substance like the picture, sound, video so that, just the authenticated individual knows the message content [5]. In this paper, cryptography and steganography are utilised to implement a secure host for data transmission. AES-128 bit key is used to encrypt the message and LSB is used to encode the encrypted text into the image to be sent.

This section presents a review of the secure data transmission system. Sharma et al. [1] proposed a framework that combines cryptography with steganography to improve the security of data. The message byte is XORing with a random key created by a pseudo-random generator then embeds plaintext in an image file. Sharma et al. [2] proposed the BLOWFISH algorithm, which is utilised to encrypt the secret image and the LSB method for concealing the encrypted image in a video.

Vijay and Swati [3] implemented the Data Encryption Standard (DES) algorithm, which is used to encrypt the message and MD5 algorithm is used to compute the message digest, which is used to check the integrity of a message. Then it is hidden into image file. Singh and Attri [6] suggested the dual layer of security to the data, the Least Significant Bit, in which, is used to encode data and encrypt the data using Advanced Encryption Standard Algorithm. Discrete Cosine Transform is applied on the RGB layer (cover image). Varghese [7] explained that the secret image is concealed into RGB layers.

2. Theoretical part

The insurance of delicate information and guaranteeing to send messages in the concealable frame so that just the Authenticated recipients can read the message is principal target for any organization [1, 6]. Two techniques are suggested to provide more security for transmission data by encryption information using ASE-128 bits encryption algorithm and the second conceal this result in the image using LSB image Steganography algorithm [6].

The proposed methodology for secure and hidden text using AES-LSB is shown by the block diagram in Fig. 1. The suggested method will satisfy four requirements, which are confidentiality, the integrity of message content, authentication, and security in an open system [1].

The following sections describe this method in details.

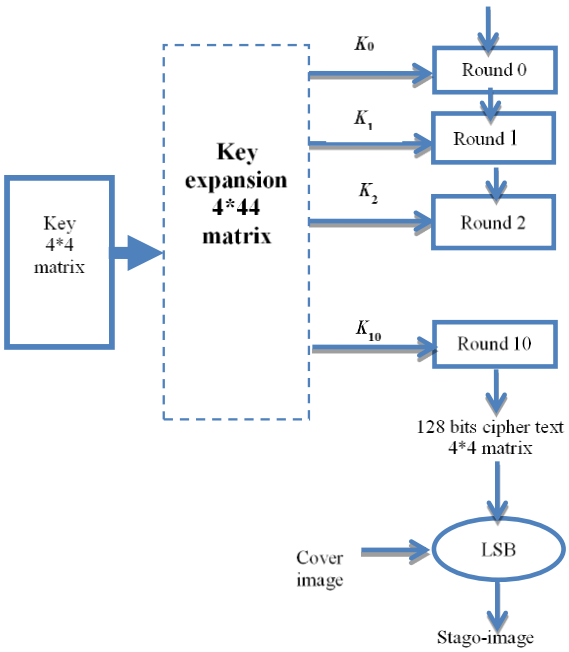


Fig. 1. General block diagram for AES-LSB system.

2.1. AES Algorithm for cryptography

Cryptography is a procedure guarantee to transmit information crosswise over the unreliable network (such as the Internet) so that just the planned beneficiary can read the message [8]. Many services are presented by cryptography such as confidentiality, authenticity, integrity, and security [9].

The cryptographic system protects the data against unauthorized parties to transform a plaintext in a disguised form. It empowers the classification of correspondence through an insecure channel [10].

Among the many techniques, AES is one of the most powerful techniques used. Advanced Encryption Standard (AES) calculation is utilised issued by the National Institute of Standards and Technology (NIST).

The state is 128 bits, which allowed encrypting and decrypting with three different key lengths: AES-128, AES-192 or AES-256 [11]. A number of rounds relies on upon the key length. It is 10 rounds for a 128-piece key, 12 rounds for 192-piece keys, and 14 rounds for 256-piece keys [12]. The design goal of this paper is to implement text encryption using AES-128 encryption algorithm.

The AES calculation comprises ten rounds of encryption, as shown in Fig. 2. To start with, the 128-piece key is eleven alleged round keys, each of the 128 bits in size. Each round incorporates a change utilizing the relating cypher key to guarantee the security of the encryption.

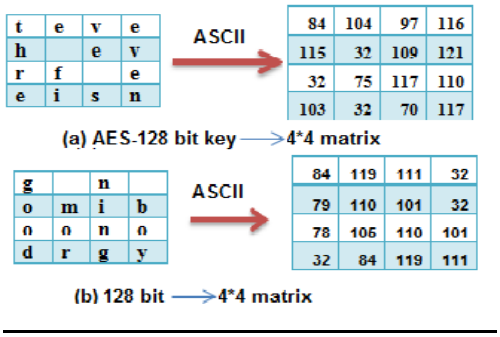


Fig. 2. (a) Key matrix, (b) State matrix.

After a beginning round, amid, which the first round key is XORed to the plain content (Addroundkey operation), nine equally organised rounds take after. Each round comprises the following operations shown in Fig. 3.

AES is an iterated piece with a settled square size of 128 bits and a variable key length. The diverse changes operate on the middle results, called state. The state is a rectangular exhibit of bytes and since the piece size is 128 bits, which is 16 bytes, the rectangular cluster is of measurements 4×4. Both the key and the information (additionally referred to as the state) are organized in a 4×4 network of bytes as shown in Fig. 2.

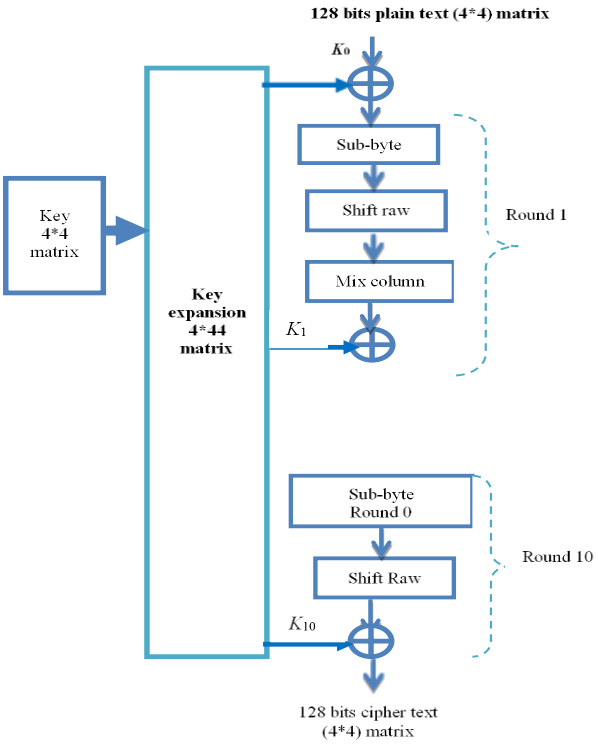


Fig. 3. General block diagram for AES encryption algorithm.

2.1.1. Sub-byte transform

In the first stage of each encryption round, an S-box is used to translate each nibble into a new nibble as illustrated in Fig. 4.

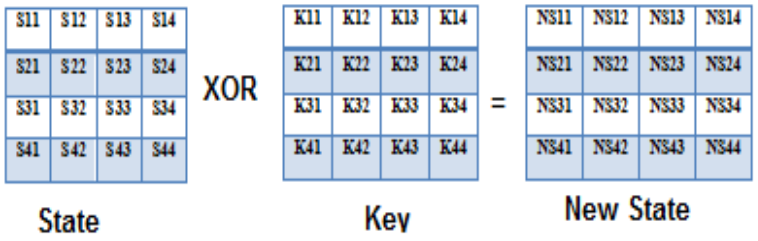


Fig. 4. Substitute byte transformation.

$$NS(1,1) = S(1,1)\ XOR\ K(1,1) \quad (1)$$

The bytes substitution change Byte sub (state) is a non-direct substitution of bytes that works autonomously on every byte of the state utilizing a substitution table (S-box) presented in Fig. 5 [10].

During encryption, each value of the state is replaced with the corresponding S-BOX value. For example, HEX 1B is substituted by the entry of S-Box in row 1 and column B, AF is gotten.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fig. 5. S-box substitution values for byte (in HEX).

2.1.2. Shift row operation

In this stage, every crude in the state is moved consistently to the left by counterbalances of 0, 1, 2, and 3 as illustrated in Fig. 6 [10].

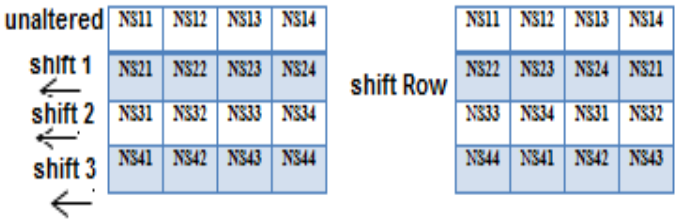


Fig. 6. Shift rows.

2.1.3. Mix columns

Mix columns operate on individual columns of the state. Current state matrix is multiplied by a fixed matrix. The individual augmentations and duplications are performed in GF (2^8) as illustrated in Fig. 7.

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Fig. 7. Mix columns matrix multiplication.

2.1.4. Key expansion

The key expansion algorithm is used to produce 44 words from original key 128 bit. These words are arranged in 44 words. They are represented as W0, W1, … W43 [12, 13].

To register round key (n+1) from the round key (n) these strides are performed.

RotWord performs a one-byte round left move on a word. This implies that an information word [b0, b1, b2, b3] is changed into [b1, b2, b3, b0].

SubWord performs a byte substitution on every byte of its input word, using the S-box. The consequence of step 1 and step 2 is XORed with a round steady Rcon[j].

The round steady is a word in which, the three furthest right bytes are constantly zero. Thus, the impact of XOR of a word with Rcon is to just perform a XOR on the left byte of the word. The round steady is for each round and is characterized as:

Rcon[j] = (RC[j],0,0,0), with RC[1]=1; RC[j]=2*RC[j-1].

And with multiplication over the field GF(2^8) [14].

2.2. LSB Algorithm for steganography

Steganography is a method used to conceal correspondence information in other information. There is a wide range of transporter document configurations can be utilised a spread to hide messages like text, image and video. Digital images are the most popular cover files that can be used to hide secret data. A huge assortment of stenographic methods are utilised for hiding data as a part of pictures, some are

more complex than others and every one of them have individual strong and weak points [15]. The steganography system consists of the embedded algorithm, secret message, cover image and stego-key [1]. The most prominent and regularly strategy for Steganography is the Least Significant Bit inserting (LSB). A touch of the mystery data is put at all critical piece (as it were, the 8th piece) of a few or the majority of the bytes inside a spread image [7]. Suppose 110 is a value of secret image its binary value is 01101110, it is distributed in LSB of the bytes inside cover image pixels as shown in Fig. 8.

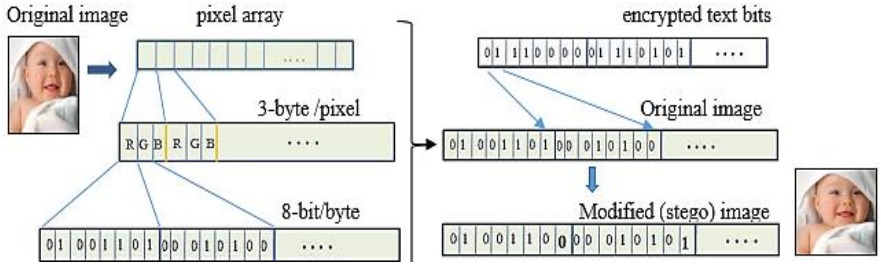


Fig. 8. An example of a cover pixel.

3. Proposed Method

The proposed algorithm is symmetric block cypher cryptography (AES) with LSB steganography that is simple and more efficient for sending a hidden message. AES is quick in both programming and hardware and is used to prevent sensitive data from being available in a readable format, LSB provides robust for data confidentiality.in the proposed method the bits are randomly submitted in the three LSBs of stego-image. Figure 9 shows an example of applying the proposed algorithm AES-LSB. The minimum huge piece (LSB) is utilised to shroud a scrambled text (text is encrypted by AES) in a cover image by change 8-bit image pixels by bits of the encrypted text. Steps of proposed algorithm AES-LSB is:

Step 1: Determine the arrangement of round keys from the figure key.

Step 2: Initialize the state cluster with the square information (plaintext).

Step 3: Add the beginning round key to the beginning state array.

Step 4: Perform nine rounds of state manipulation.

Step 5: Perform the round 10 and last round of state manipulation.

Step 6: Copy the final state array out as the encrypted data (ciphertext).

Step 7: Convert the encrypted text from decimal to binary

Step 8: Read cover image

Step 9: Convert the Cover Image from decimal to binary

Step 10: Change 8 bit in cover image by bits of the encrypted text.

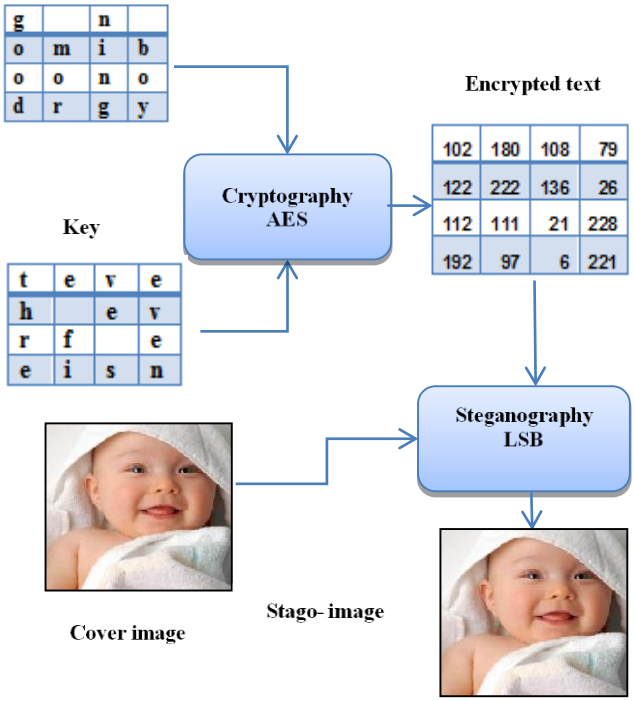


Fig. 9. Example of applying the proposed algorithm AES-LSB.

4. Results

In this section, the experimental result shows the evaluation of our proposed technique. AES can be used to protect text and LSB can be accustomed to concealing an instant message in the image. Our method is tested over different size and different type of cover images such as (jpg, tiff and png).

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two mistake measurements used to measure stago-picture quality. The MSE speaks to the cumulative squared mistake between resultant stago-picture and the spread picture, while PSNR speaks to a measure of the crest blunder. *m* and *n* are the widths and high of spread images, individually. I indicate the spread picture and K denotes the stego-picture MSE is characterised as:

$$\text{MSE}=\frac{1}{M*N}\sum_1^M\sum_1^N((I(i,j)-K(i,j))^2 \quad (2)$$

PSNR is figured utilising the accompanying equation:

$$\text{PSNR} = 10\log_{10}\frac{R^2}{MSE} \quad (3)$$

In the past mathematical statement (3), *R* is assigned to the extreme value of a pixel in dark scale picture. For instance, if the input picture has a twofold accuracy drifting point information type, then *R* is 1. In the event that it has an 8-bit unsigned number information type, *R* is 255, etc. [16].

5. Applied Experiment

The proposed calculation AES-LSB applied to the text, since the plaintext is converted to hexadecimal as shown in Fig. 10 and the key is converted to hexadecimal as shown in Fig. 11.

g		n	
o	m	i	b
o	o	n	o
d	r	g	y

67	20	6e	20
6f	6d	69	62
6f	6f	6e	6f
64	72	67	79

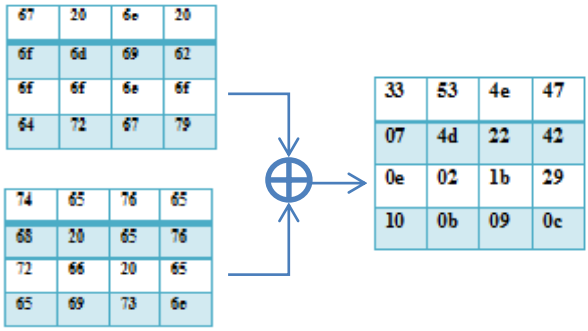
Fig. 10(a) Plain text: 'good morning boy', (b) Convert text to hexadecimal.

t	e	v	e
h		e	v
r	f		e
e	i	s	n

74	65	76	65
68	20	65	76
72	66	20	65
65	69	73	6e

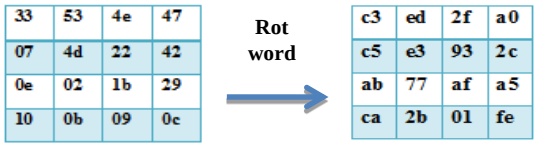
Fig. 11(a) Key: 'three five seven', (b) Convert key to hexadecimal.

Step 0: Add round key



Round = 1

Step 1: Sub-byte



Step 2: Shift left

c3	ed	2f	a0
c5	e3	93	2c
ab	77	af	a5
ca	2b	01	fe

Shift left →

c3	ed	2f	a0
E3	93	2c	C5
Af	A5	Ab	77
fe	ca	2b	01

Step 3: Mix column

F2	00	Aa	79
0a	Ee	Ba	A9
7c	6a	33	88
F5	95	A0	4b

Step 4: Add round key

10	91	1b	af
38	fc	e3	d0
80	fb	d7	2a
04	1d	46	d8

After 10^{th} round, the result is:

Step 1: Sub-byte

29	86	08	3d
d5	e0	2f	1c
ea	63	c0	5e
f3	6e	cf	1a

Step 2: Shift left

29	86	08	3d
e0	2f	1c	d5
c0	5e	ea	63
1a	f3	6e	cf

Step 3: Add round key

a8	ba	a1	5b
6a	7f	1b	66
76	ef	fd	79
85	a8	65	72

- LSB is applied on encrypted text

Step 1: Convert the encrypted text from decimal to binary.

ENCRYPTED TEXT bin2dec → 01100111

Step 1: Read the cover image

53	44	34	…
105	103	102	
116	120	117	
130	128	124	…

Step 2: Convert the cover image from decimal to binary.

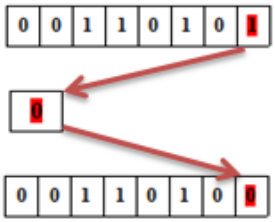
00110101	00101100	00100010	…
01101001	01100111	01100110	
01110100	01111000	01110101	
10000010	10000000	1111100	…

Step 3: Change 8th bit in the cover image by bits of the encrypted text.

The first bit of the encrypted text to be hidden is:

0

Replace 8th bit in the cover image



And others.

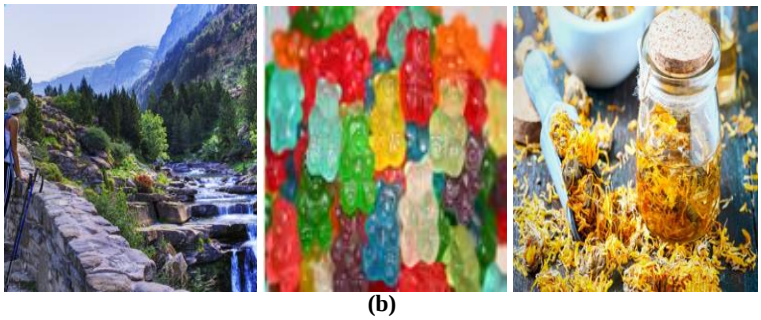
- **AES-LSB algorithm applied on images with different type and size**

In the first experiment, AES-LSB algorithm is applied to the images size 128×128 as shown in Figs. 12. The PSNR and MSE between source plain picture and stego image of this analysis are shown in Table 1.

Table 1. Average results of MSE and PSNR for images size 128×128 using the proposed AES-LSB algorithm.

Image	Format	MSE	PSNR	Time
1	JPEG	3.5604e-04	82.6158	1.4221 s
2	PNG	6.6121e-05	89.9274	1.4558 s
3	Tiff	7.1035e-04	79.6161	1.4846 s

(a)



(b)

Fig. 12(a) Original image with size 128×128, (b) Stego image result of AES-LSB.

The statistical features of images are presented using histogram that plots the frequency of the occurrence of image pixel value, this analysis is done to compare original and stego images where there should be no differences between histograms of original and stego image as shown in Figs. 13 and 14.

The second experiment exhibited the measure of the spread picture, which is an important element that impacts on the fairness of the stego image. Table 2 shows the results of the PSNR and MSE, which measures respectively for the tested images with a size of 256×256.

Table 2. Results of MSE and PSNR for images size 512×512 using the proposed AES-LSB algorithm.

Image	Format	MSE	PSNR	Time
1	JPEG	7.6294e-05	89.3059	1.5815 s
2	PNG	3.0690e-05	93.2608	1.5511 s
3	Tiff	5.24037e-04	80.9372	1.5647 s

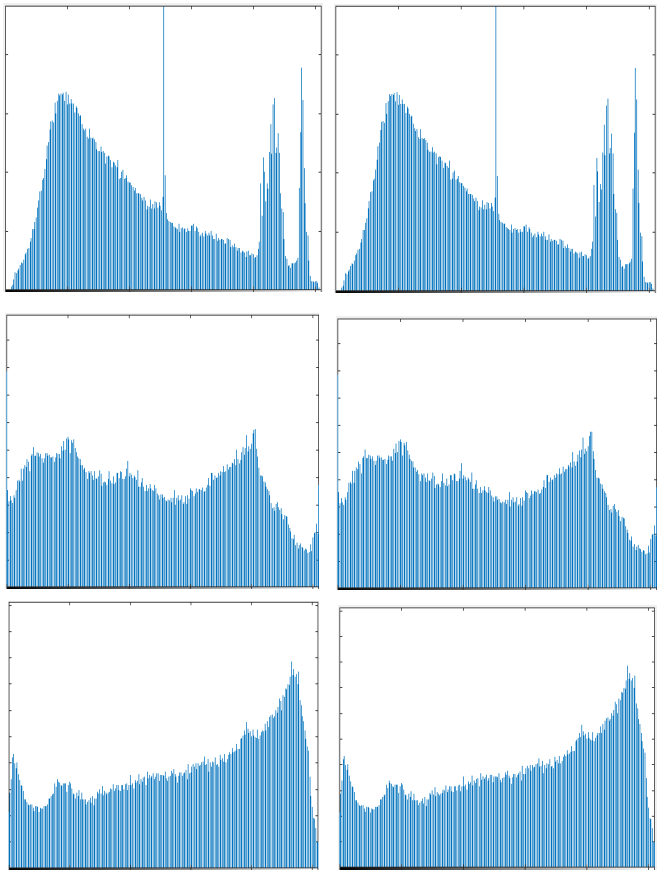
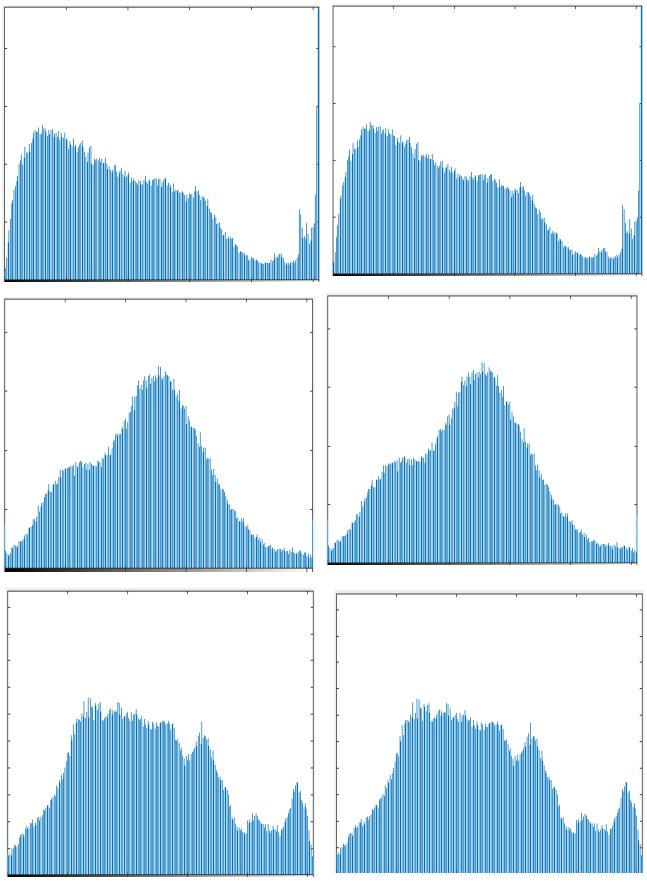


Fig. 13(a) Histogram for original images 128*128, (b) Histogram for stego image result of AES-LSB.



(a) **(b)**

Fig. 14(a) Histogram for original image 512*512,
(b) Histogram for stego image result of AES-LSB.

This experiment is applied using cover image type jpg with size 512×512 as shown in Figs. 15. The relation of the results of the MSE and PSNR measure for the tested images with different types and sizes as shown in Figs. 16 and 17.

(a)

(b)

Fig. 15(a) Original image with size 512×512, (b) Stego-image result of AES-LSB.

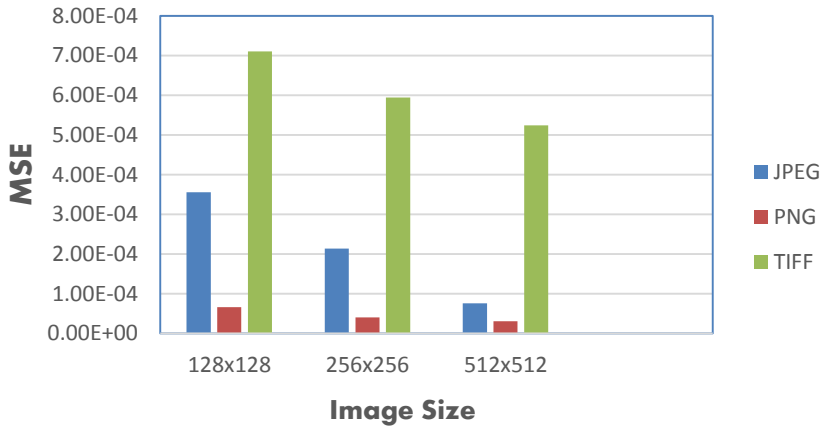


Fig. 16. Results of MSE measure for tested images with different type and size.

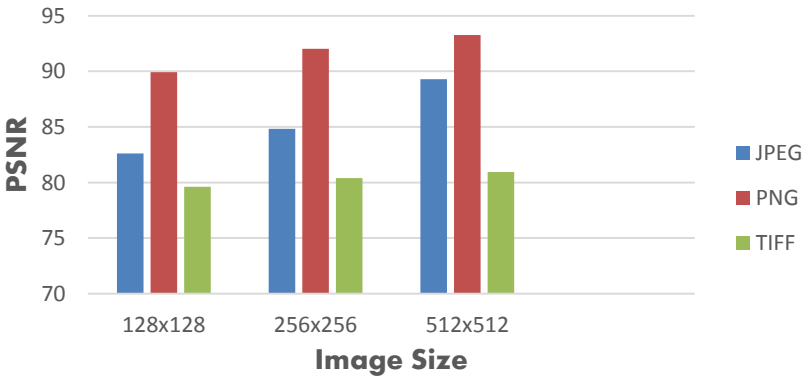


Fig. 17. Results of PSNR measure for tested images with different type and size.

6. Conclusion

In this paper, a cryptography and steganography algorithms proposed to provide higher security for data communication. Two techniques AES-LSB are proposed to ensure secure data transmission between sender and receiver in unsecured networks. AES algorithm is used to encrypt the text then the encrypted text is hidden in image (jpg, png, gif, bmp) using LSB algorithm. The proposed system hiding encrypted data in an image with less variety in image bits makes it secure and effective system. The performance evaluation of the proposed method is measured by two Factors PSNR and MSE and When we consider the image histogram we notice that no differences between histograms of original and stego image. The quality of the stego picture increments with expanding the size of the spread picture on the basis that the proportion of the picture pixels to the quantity of the text characters increments in this way the distortion decreases. The experiments demonstrate that the suggested method is robust and more superior for secure data communication.

Nomenclatures

K_n	Key values of round, n
NS	New states values of bytes substitution
R	Extreme value of a pixel in grayscale picture
RC	Non-zero byte in round constants
Rcon	Round constant for i^{th} round
S	Current states values of bytes substitution
W	Word output of key expansion algorithm

Abbreviations

AES	Advanced Encryption Standard
GF	Galois Field
LSB	Least Significant Bit
MSE	Mean Square Error
NIST	National Institute of Standards and Technology
PSNR	Peak Signal to Noise Ratio

References

1. Sharma, N.; Bhatia, J.S.; and Gupta, N. (2013). An encrypto-stego technique based secure data transmission system.
2. Sharma, H.; Mithlesharya; and Goyal, D. (2013). Secure image hiding algorithm using cryptography and steganography. *IOSR Journal of Computer Engineering (IOSR-JCE)* ,13(5), 1-6.
3. Vijay, B.; and Swathi, J.(2014). Implementation of digital steganography using image files-a computational approach. *International Journal of Engineering Research and Development*, 10(5), 6-10.
4. Alia, M.A.; Tamimi, A.A.; and Al-allaf, O.N.A. (2014). Cryptography based authentication methods. *Proceedings of the World Congress on Engineering and Computer Science (WCECS)*. San Francisco, United States of America, 6 pages.

5. Kour, J.; and Verma, D. (2014). Steganography techniques - A review paper. *International Journal of Emerging Research in Management and Technology*, 3(5), 132-135.
6. Singh, S.; and Attri, V.K. (2015). Dual layer security of data using LSB Image steganography method and AES encryption algorithm. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 8(5), 259-266.
7. Varghese, A.E. (2015). Reconfigurable processor for image steganography using DCT with morphological operations. *International Journal of Innovative Research in Computer and Communication Engineering*, 3(9), 8053-8061.
8. Zimmerman, P. (1999). *An introduction to cryptography*. Santa Clara, California, United States of America: Network Associates, Inc.
9. Borkar, A.M.; Kshirsagar, R.V.; and Vyavahare, M.V. (2011). FPGA implementation of AES Algorithm. *Proceedings of the 3rd International Conference on Electronics Computer Technology*. Kanyakumari, India, 401-405.
10. Babu, J. (2007). *Advanced encryption standard (AES)*. Retrieved May 14, 2007, from https://www.coursehero.com/file/28426275/AESpdf/.
11. Kretzschmar. U. (2009). AES128 A C implementation for encryption and decryption. *Application Report*, ECCN 5E002 TSPA-Technology/Software Publicly Available.
12. Argarwal, A. (2001). *The Advanced Encryption Standard (AES). The AES Algarithm*, Chapter 7, 58-73.
13. Funde, S.V.; and Padole, D.V. (2015). Design of advanced encryption standard algorithm using xilinx project navigator, ISE 13.1. *International Journal of Engineering Research and General Science (Part* 2), 3(2), 573-576.
14. Karthigaikuma, P. and Rasheed, S. (2011). Simulation of image encryption using AES algorithm. *IJCA Special Issue on Computational Science - New Dimensions and Perspectives (NCCSE)*, 166-172.
15. Morkel, T.; Eloff, J.H.P.; and Olivier, M.S. (2005). An overview of image steganography. *Proceedings of the Conference on Fifty Annual Information Security South Africa (ISSA*). Sandton, South Africa, 12 pages.
16. Kamdar, N.P.; Kamdar, D.G. and Khandar, D.N. (2015). Performance evaluation of LSB based steganography for optimization of PSNR and MSE. *Journal of Information, Knowledge and Research in Electronics and Communication Engineering*, 2(2), 505-509.