

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/380149098>

Image Encryption and Steganography Method Based on AES Algorithm and Secret Sharing Algorithm

Article in *Ingénierie des systèmes d'information* · April 2024

DOI: 10.18280/isi.290232

CITATIONS

0

READS

73

4 authors:



Mustafa Muslih Shwaysh

University of Anbar

3 PUBLICATIONS 7 CITATIONS

SEE PROFILE



Sameer Alani

75 PUBLICATIONS 1,270 CITATIONS

SEE PROFILE



Mohammed Ayad Saad

Universiti Kebangsaan Malaysia

32 PUBLICATIONS 178 CITATIONS

SEE PROFILE




Tabarak Ali

7 PUBLICATIONS 22 CITATIONS

SEE PROFILE



Image Encryption and Steganography Method Based on AES Algorithm and Secret Sharing Algorithm

Mustafa Muslih Shwaysh¹, Sameer Alani^{2*}, Mohammed Ayad Saad³, Tabarak Ali Abdulhussein⁴

¹ College of Education for Humanities, University of Anbar, Anbar 5543, Iraq

² Computer Center, University of Anbar, Anbar 5543, Iraq

³ Department of Medical Instrumentations Technique Engineering, Al-Kitab University, Kirkuk 36001, Iraq

⁴ Department of Computer Technology Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad 10011, Iraq

Corresponding Author Email: sameer.h@uoanbar.edu.iq

Copyright: ©2024 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/isi.290232>

ABSTRACT

Received: 23 November 2023

Revised: 27 March 2024

Accepted: 8 April 2024

Available online: 25 April 2024

Keywords:

Advanced Encryption Standards (AES) algorithm, Shamir secret sharing (SSS), hiding of encryption key with secret sharing, PSNR and MSE

The development that occurred in information technology and the need to transfer knowledge made sensitive information protection very necessary. The key exchange method is an important method between two sides, the sender side, and the receiver side, especially with the use of the symmetric algorithm, the key exchange method achieves two important principles secrecy and authentication. This article presents a new method for the protection of a secret grayscale image. The proposed work is composed of four phases. The initial phase is the key generation. Then the encryption process will be implemented by using the proposed AES encryption algorithm with multiple S-boxes determined by the number of rounds of the algorithm. The third phase applies secret sharing using the Shamir secret sharing scheme (SSSS). The SSSS will split the encryption key of the encryption algorithm that was generated randomly in the previous phase into several shares that will be distributed over multiple locations. The final phase is steganography, which will embed the secret image into an appropriate cover image using the Least Significant Bit (LSB). The obtained results prove that the secret image is completely restored without any change. The reconstruction of the stego image of quality test results was very good with PSNR 46.165 and MSE 1.58.

1. INTRODUCTION

Due to the growth of threats to multimedia information, the demand for multimedia information security that transmits from one side to another has increased. Finding the best-secured method for transmission represents the main challenge [1]. Security is essential for the protection of secret information for storage, and transfer between objects to make sure that there is no distortion, or manipulation allowed on that secret information. In the field of multimedia information security, various techniques are employed to protect sensitive data during transmission. Two important methods used for this purpose are visual cryptography and steganography. Visual cryptography includes converting the original image to different layers that appear randomly and can be retrieved to restore the original image. Besides, the implementation technique can be classified into different techniques such as xor-based and algorithmic methods [2, 3]. Moreover, the steganography algorithm works in covering or hiding information such as audio files, videos, and images. In this article, the proposed method for image encryption, secret sharing, and steganography demonstrates resilience against potential attack vectors. Cryptanalysis attacks are mitigated by utilizing the AES encryption algorithm with multiple S-boxes,

which is a recognized and secure algorithm. Brute force attacks are hindered using secret sharing with the Shamir scheme and enforcing strong encryption keys. Steganalysis attacks are addressed by employing the LSB technique, although more advanced steganographic techniques could enhance system robustness. Collusion attacks are mitigated by requiring a minimum threshold of shares for key reconstruction. While side-channel attacks are not explicitly mentioned, incorporating secure algorithms, constant-time implementations, and physical security measures can protect against them. A comprehensive security analysis, considering implementation details and adherence to best practices, is essential to ensure the system's resilience against vulnerabilities and potential attack scenarios. One of the most used techniques of security is the cryptography technique; it deals with the technique of transforming the understandable and readable form into an understandable and vague form. The key power, which regulates the user's access to confidential information, is essential to both encryption and decryption processes. Depending on how the cryptographic keys are used, there are two types of cryptography: symmetric key cryptography and asymmetric key cryptography. Cryptography may be applied in a variety of ways [4, 5]. Secret sharing is the most used technique for information

sharing to store sensitive and important information. It is implemented by splitting and distributing that information among several participants to increase the confidentiality and reliability of the secret information. The main benefit of secret sharing is the addressing of the problems by making a high level concerning the confidentiality and reliability objectives achieved [6]. Shamir's secret sharing scheme is the most known algorithm for secret sharing, Adi Shamir and George Blakley invented it in 1979. It enables the process of splitting the secret information (s) into many parts (n), so any number of pieces (n) with a number of shares (k) can rebuild the secret information(s). The secret cannot be exposed with ($k-1$) pieces so the information will be kept safe and secret, this scheme is known as a (n, k) threshold scheme. The secret sharing scheme is known as the perfect scheme if (k) can recover all the secret information (s) while the fake or unauthorized (k) will not be allowed to recover any piece of information from the secret (s). This scheme is to enhance convenience and practicality when multiple users are required to perform authorized actions [7]. Steganography is a scheme applied to increase the security of information by hiding secret information in a cover message [8]. Steganography works for sensitive information as a mask by hiding that sensitive information in a particular carrier. The main goal of this technique is to make the sensitive information undetectable [9].

2. RELATED WORKS

Numerous techniques and methods developed in the field of information security such the cryptography, secret sharing, and steganography. Many types of research concerning the secret-sharing scheme. conducted a developed method of visual cryptography to transmit the original image protected by confidentiality and secret sharing and from a secret color image RGB band of pixel values forming separate matrices (R_i, G_i, B_i) [10]. The proposed method is highly security against any deceitful shares that altered the original shares, so it secures the shares secret efficiently it also minimizes the PSNR value and has a fast image encryption execution. Moreover, Shankar and Eswaran [9] proposed a method of using visual cryptography (encryption and decryption) to an image that differs in size and a particular length of the message with embedding time. The proposed method provides a high level of security because of the robust shares that have immunity against different attacks. Also, the binary secret shares vulnerability is surpassed by hiding the shares in some images. Another study proposed a method of making secret sharing more secure since the secret sharing divides the secret into several pieces, each piece sent to a participant to keep it safe and to prevent the attackers from knowing that piece [11]. The developer noticed the shares or pieces could be compromised so the proposed work by using the Shamir secret sharing tries to prevent the attackers from outside and inside, to keep it secret and safe by using fake shares sent with the real shares to the participants. Moreover, Rajput et al. proposed a method of encrypting a secret image SI with n cover images C_i by using the concept of a secret sharing scheme. The proposed method gives very high security and if any shares are altered will not reveal any information or partial information and any attack will affect the secret also the proposed image works on both gray scale and colored image. Furthermore, Wang and Gao [12] has proposed a method of using cryptography and secret sharing for an image to have a high

degree of confidentiality while transmitting. The security requirement in the proposed method is satisfied also the visual testing and the encryption testing performance are high. In another study [13], the author proposed a method for studying information security in cloud computing to handle the issues related to cloud computing. The focus of the proposed work is about the symmetric and asymmetric encryption keys of the encryption algorithms. The proposed technique applies different encryption algorithms such as the AES, DES, 3DES, RSA, and Elliptic Curve. To decide on which algorithm is more secure for enhancing the security of data in the cloud computing system. Kambl and Patil [14] proposed a method of protecting secret information from outside attacks while transmission forms one side to another. Secret sharing is a scheme that is utilized to separate the secret into several shares and distributing it among several locations. Moreover, the recovery process needs several shares that have been distributed to rebuild the secret. The proposed work mainly focuses on the process of reconstruction of cover image quality which should be the same as the original before the hiding process of the secret inside the cover image. Another study was conducted by using a matrix semi-tensor product for a chaotic encryption algorithm image along with a secret key [15]. The initial image plaintext pixels were divided randomly into blocks. The resulting block of pixels is subjected to various Arnold transformation rounds, and the resulting blocks are then concatenated to get the scrambled image. After that, a secret key is developed. A collection of pseudo-secret keys is then filtered using a synchronous Boolean network that is updated for the real secret key generation. The initial value uses a secret key as of the Mixed Linear Non-Linear Coupled Map Lattice System for generating sequential chaos. Finally, the Semi-Tensor Product operation is applied to the sequential chaotic plus the scrambled image for an encrypted image generation. In contrast to other encryption algorithms, the algorithm proposed is more effective and secure, it also works for image encryption with colors. The proposed method of Fractal Sorting Matrix is a class of sorting matrices with fractal properties and results iterative calculation method [16]. To improve the security of the encryption algorithm effectively, the new cluster of matrices scrambles information or images. High encryption efficiency and good security resulted from a new technique of the diffusion of global pixels with two sequential chaotic. This paper constructs a more secure and efficient chaotic image encryption algorithm in contrast to other techniques. The proposed algorithm has a higher rate (in association with Shannon entropy) and is faster too. Data in ant-differential attack (test) are smaller in terms of the fluctuation of data and close to theoretical values. Also, the images that are obtained from the noise attacks and cropping are clearer. As a result, the proposed method results in more resistance to different attacks and security. Finally, a study was proposed by Al-Ghamdi et al. [17]. The article presented a Combination Chaotic System which involves image encryption. A larger key space plus the exhibition of more efficient cryptographic features than their original 1-D chaotic map is proposed. Moreover, due to using the NCCS, a new scheme of bit-level image encryption is produced. The scheme core includes generating the plaintext that relates to the key streams (using SHA-512 Hash) and random decimal points sequence, the NCCS bit-level operations of the image plus the confusion and diffusion. The results show the proposed algorithm's effectiveness in high-security terms, as well as demonstrating better chaotic behavior. In this article, a novel

approach for protecting secret grayscale images based on advanced encryption and steganography. The proposed framework comprises four phases: key generation, encryption, secret sharing, and steganography. The method starts by generating the key. After generating the key, the advanced AES encryption algorithm with multiple S-boxes are introduced to encrypt secret grayscale image. Then, the Shamir secret sharing scheme is applied to split the encryption key for more reliability. Lastly, during the steganography phase, we introduced the LSB technique in order to cover the image (see Figure 1). In addition, a comparison must be conducted with the recent works to show and validate the strength of the proposed method since most of the literature review studies show several challenges in protecting information and susceptibility to attacks. Thus, this article suggests a new framework by introducing advanced encryption techniques, secret-sharing schemes, and steganography to address these limitations.

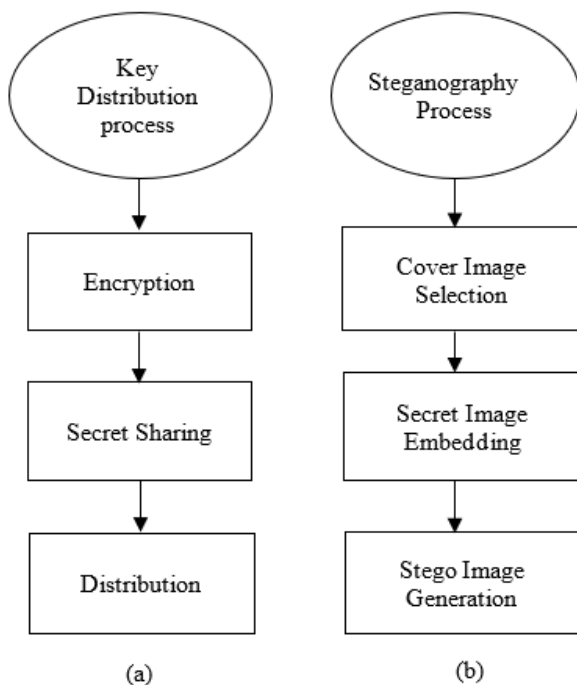


Figure 1. (a) encryption key distribution (b) steganography

The secret image's dependability is guaranteed throughout the encryption stage. By dividing the encryption key, the secret sharing step provides an additional degree of security. The steganography phase further hides the secret picture under a cover image, making it more difficult for adversaries to find or extract the secret data. In addition, the suggested method seeks to strike a balance between visual quality and security. The reconstructed stego picture demonstrated good performance in the quality test results, with a low mean squared error (MSE) of 1.58 and a high peak signal-to-noise ratio (PSNR) of 46.165. This proves that the suggested framework successfully maintains the secret image's confidentiality while preserving its aesthetic appeal.

3. ADVANCED ENCRYPTION STANDARDS (AES) ALGORITHM

The need for protection of sensitive, secret, or private data and information requires specific ways and methods to keep

that data or information safe. In the digital world, one of the most famous methods called encryption is used to keep that data and information safe, the encryption is a process of transforming readable data or information into an unreadable form or unrecognizable and only the people with authorization can access and use that data and information and modify it. The AES algorithm is very important in the communication field and information security. It is a symmetric (one-key) algorithm used for encryption and is considered one of the most powerful algorithms. The main reason that the AES was created was to fix the flaws and improve issues found in the DES (Data Encryption Standard).

4. SECRET SHARING SCHEME (SSS)

Secret sharing is the most widely used technique for information sharing to store sensitive and important information. Is an important concept in cryptography that takes a secret input, divides it into several pieces and distributes it between several users or participants. Shamir secret sharing scheme is the most known algorithm for secret sharing, Shamir and Blakley. It enables the process of splitting the secret (s) into (n) parts with any (k) out of (n) pieces that can be rebuilt as original secret (s). The basic idea of the creation of Shamir's secret sharing was for the protection of cryptographic keys. The purpose of the scheme is to improve convenience and practicality when multiple users are required to perform authorized actions.

5. PEAK SIGNAL-TO-NOISE RATIO AND MEAN SQUARE ERROR

In order to evaluate the proposed method, there are two important metrics that should be measured which are MSE and PSNR. MSE is mean square error between the covered and stego image while PSNR indicates the quality of the image. Both metrics can be defined as follows:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (1)$$

$$MSE = \left(\frac{1}{N}\right)^2 \sum_{i=1}^N \sum_{j=1}^N (x[i,j] - \underline{x}[i,j])^2 \quad (2)$$

6. THE PROPOSED SYSTEM

The proposed method is divided into four phases as presented in Figure 2. Each phase has a specific task to achieve the highest levels of security. The first step is the generation of a random key by the proposed method to be used later. The second phase utilizes the AES algorithm for encryption process and produces a cipher image. The third step, using the secret sharing scheme to increase the security of the secret. The fourth step, the steganography step uses the LSB algorithm for hiding the secret inside a cover image.

Each phase has several steps to be implemented. The detail of these steps and the proposed method is shown in Figure 3.

6.1 Step 1: Random key generation algorithm

The proposed key generation algorithm called (KEY-GENR)

as presented as algorithm 1 creates the secret key that will be the encryption key of the encryption algorithm in a random manner. The size of the produced key from the algorithm KEY-GENR will be 256-bit and it will be used as input to the Shamir secret sharing algorithm to be distributed over many locations or participants to keep that key secret from unauthorized people.

The pseudocode of step 1 is shown below as algorithm 1.

Algorithm 1: Key generator Algorithm KEY-GENR

```

1 Input: Secret Key 256-bit, Register (X, Y, Z)
2 Output: Random Secret Key with 256-bit length
3 Start:
4   Step1: Assign a value to a variable called (Polynom).
5   Step2: Multiply the polynom * 16 to specify the no. of
        bits to the key will be generated (in the proposed method
        the key will be 256-bit so the polynom will be assigned to
        16)
6   Step3: Divide the 256-bit over 8 times to specify the
        bytes numbers of bytes will be store in the register X.
7   Step4: take the result from the register and put it in a
        byte array and then utilize random function to produce
        random numbers to the key
8   X  $\square$  ByteArray
9   ByteArray  $\square$  Key
10  Random (Key)
11  Step5: Divide the Key length over 2
12    For i=1 to length/2
13      Array [ 2*i] << 8  $\square$  Y
14      Array [ 2* i + 1]  $\square$  Z
15      Y+Z  $\square$  W[i]
16  Step6: Converting the result key 256-bit into hex
17    For j= 1 to Keylength
18      ToHexStr(Key)
19  End

```

6.2 Step 2: Encryption process using AES algorithm

The secret image's dependability is guaranteed throughout the encryption stage. By dividing the encryption key, the secret sharing step provides an additional degree of security. The steganography phase further hides the secret picture under a cover image, making it more difficult for adversaries to find or extract the secret data. In addition, the suggested method seeks to strike a balance between visual quality and security. The reconstructed stego picture demonstrated good performance in the quality test results, with a low MSE of 1.58 and a PSNR of 46.165. This suggests that the suggested framework successfully maintains the secret image's confidentiality while preserving its aesthetic appeal. increased by the many S-boxes. Multiple S-boxes provide diversity, which makes it more difficult for an attacker to succeed in an attack by forcing them to crack multiple separate encryption layers. The number of S-boxes makes the secret much more secure. Figures 4, 5, 6, and 7 illustrate one S-Box and IS-Box and two S-Box, IS-Box, three S-Box and IS-Box, and the fourth S-Box and IS-Box.

Algorithm 2: AES Encryption Algorithm

```

1 Input: Gray image, Secret Random Key
2 Output: Ciphred image
3 Start:
4   Step1: Choose the key size (128,192or 256 bit) will
        determine the Nr (10,12 or 14)
5   Step2: Palin image (Original image).
6   Step3: Plain image XOR RoundKey (0)

```

```

7   Step4: Create-SubBytes().
8   For i = 1 to Nr (rounds number) // the rounds number can
        be (10, 12 or 14)
9     Start:
10    For r = 0 to 16
11      Start:
12      For c = 0 to 16
13        Start:
14        Multiplicative inverse[r,c]  $\square$  Value
15        Find S-box (value, Round-Key[i], i)
16    b
17    Fill S-box (r, c, value, i+1)
18  End
19  End
20  Create Inverse S-Box()
21  For r = 0 to 4
22    Start:
23    For c = 0 to 4
24      Start:
25      State[r,c] & 0x0f  $\square$  y
26      (State[r,c] >> 4) & 0x0f  $\square$  x
27      Switch (Key_Enc[i])
28      Start:
29      Isub1[x,y]  $\square$  State[r,c]
30    End
31  End
32  End
33  Creat_Ibox()
34  Start:
35  For counter = 0 to NR
36    Start:
37    Switch (counter)
38    Fill_Ibox(sub1, Isub1);
39  End
40  End
41  End
42  ShiftRows.
43  MixColumn.
44  Add RoundKey (MixColumn XOR RoundKey).
45  Step5: If i = Nr
46  SubBytes.
47  ShiftRows.
48  Add RoundKey (ShiftRows XOR Add RoundKey(NR)).
49  Step6: Output (Cipher Image).
50  End

```

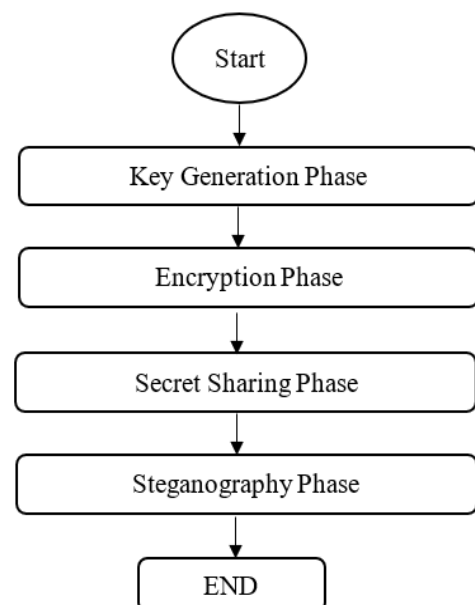


Figure 2. The entire flowchart of the proposed method

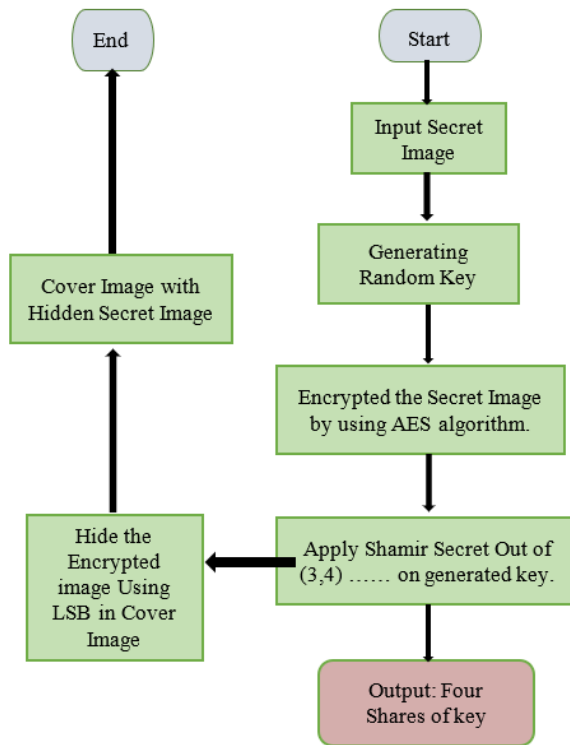


Figure 3. Illustrate the steps of the proposed work

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

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

Figure 4. Illustrate the following is the one S-Box and IS-Box

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

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

Figure 5. Illustrate the following is the two S-Box and IS-Box

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

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

Figure 6. Illustrate the following the three S-Box and IS-Box

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

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

Figure 7. Illustrate the following is the fourth S-Box and IS-Box

6.3 Shamir secret sharing algorithm

The Shamir secret sharing is one of the most known and widely used algorithms. The secret random key created by the (KEY-GENER) algorithm will be used as input to the Shamir algorithm. The Shamir secret-sharing algorithm will process the secret encryption key and will produce several shares distributed to several participants or locations. These shares will be used later to rebuild the secret key for the decryption process. Shamir's (3, 4) threshold secret sharing generates four shares of the secret encryption key. The pseudocode of Shamir's secret sharing algorithm is presented below as algorithm 3.

Algorithm 3: Shamir (3, 4) threshold secret sharing

```

1 Input: Secret Encryption Key (256-bit), n=4, k=3
2 Output: Four shares of key
3 Start:
4   Step1: For i = 1 to key length
5     Begin
6       Read key row (i)
7       Reading the random points from (key row(i), n)
8   Step2: For j = 1 to n
9     f(x) =
10    shares(x) = key length *2
11    Produce the shares (x.share(x))
12  End for
13 Step3: Repeat step1 and step2 until whole key processed
14 End

```

6.4 The proposed hiding technique of encrypted image

The encrypted image that resulted from the AES encryption algorithm and the hashing value is hidden inside the colored cover image using the Least Significant Bit (LSB) method. The LSB method will hide the encrypted image values inside cover image pixels by transforming the secret image into a matrix. The next step will be taking the index of each character that wants to be hidden in a cover image, by transforming each character into an integer consequently taking that value of the character and holding the color element (R or G or B) index that currently processed. Algorithm 4 illustrates the pseudocode of the LSB step.

Algorithm 4: Generating a position of cover image pixels by using (LSB)

```

1 Input: Cover image, Encrypted image
2 Output: Cover Image with Hidden Secret Image Pixels Inside
3 Start:
4   Step1: State matrix hiding □ State matrix
5   Step2: Holds the index
6     0 □ charIndex
7   value of the character that converted and the value of convert
that character into integer
8     0 □ charValue
9   holds the color element (R or G or B) index that currently
processed
10    0 □ pixelElementIndex
11   Step3: For i = 1 to height of image image
12     For j = 1 to width of image

```

```

13      Begin
14      Getpixel (j,i) □ Pixel
15      Clear each LSB from pixel element
16      R - R % 2.
17      G - G % 2.
18      B - B % 2.
19  Step4: For k = 1 to 3
20      Begin
21      Check if whole process has finished
22      If 0 □ Pixel index % 8
23          It is finish when 8 zeros added
24      8 □ State matrix
25      Return Image
26      End for
29  End

```

7. ENCRYPTION KEY

The encryption key used by the encryption process is 256-bit length; it is generated randomly by a proposed key generation method. After the key generation process, it will be used in the process of encryption. When the encryption process is finished the Shamir secret sharing is applied to the key to encryption, and the result will be generating four shares that will be distributed to many participants, the threshold of shares that are needed to reconstruct the original key is three shares as presented in Figure 8.



Figure 8. (a) original encryption key, (b) the shares of the secret key after applying the Shamir secret sharing scheme of (3,4) threshold, (c) the reconstructed encryption key

8. EXPERIMENTAL RESULTS

To achieve the best results, several measuring factors are used. The evaluation factors include entropy, CC, NPCR, AUCI, and the PSNR with the MSE. The tests applied for the evaluation of the system performance of the proposed work. Figure 9 clarifies the difference in histogram between plain and encrypted Lena gray images of size 64×64 pixels.

8.1 Number of changing pixel rate and unified averaged changed intensity

The NPCR and UACI, the NPCR calculate the different pixels of total pixels in the image, and it must be close the 100%. The UACI measures average intensity among several

images; it is preferred to be greater than 33%. Both coefficients are used to measure the strength of the encryption algorithm against attacks like deferential attacks. The result of the NPCR and UACI shows the encryption algorithm is strong against attacks. The results show that the encryption algorithm used for the encryption process is very good and secure. As illustrated in Tables 1 and 2.

8.2 The entropy of gray images

The entropy measurement between the original image and the ciphered image the result shows that there is an increase in the entropy value after the process of the encryption, this means the distortion in the ciphered image is increased. The encryption process results are very good according to the experiments of the entropy coefficient. As illustrated in Table 3. Moreover, correlation coefficients are statistical measures that quantify the degree of linear relationship between two gray-scale images. These coefficients provide a measure of how similar or related two images are in terms of their pixel values. Figure 10 illustrates the correlation coefficients of gray images.

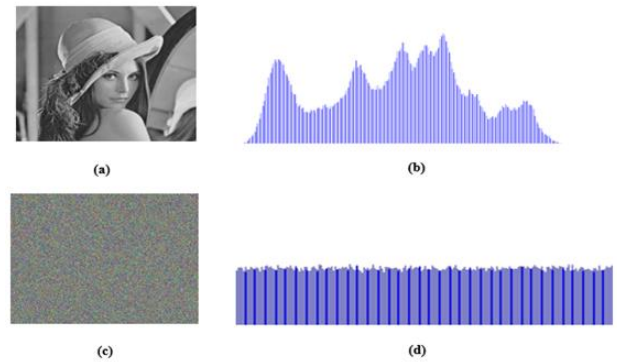


Figure 9. (a) original image (64 x 64), (b) the histogram of the original image (c), the encrypted image (d) the histogram of the encrypted image

Table 1. Illustrate the NPCR and UACI between the plain and cipher image

Gray Image	NPCR%	UACI%
Lena	99.63%	33.21%
Pepper	99.60%	33.33%
Baboon	99.61%	33.20%

Table 2. Illustrate the NPCR and UACI between two ciphered images

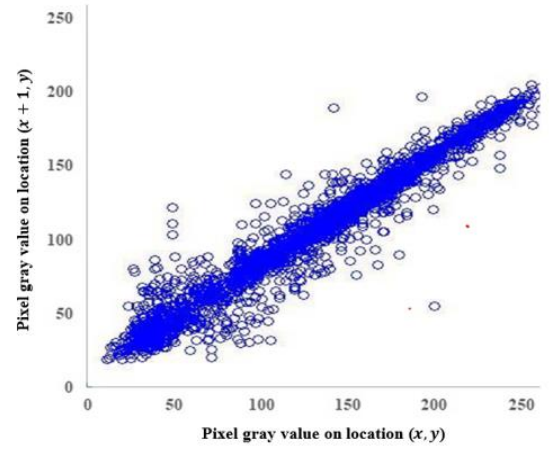
Ciphered Images	NPCR%	UACI%
Lena, Pepper	99.63%	33.37%
Lena, Baboon	99.60%	33.48%
Pepper, Baboon	99.61%	33.46%

Table 3. Illustrate the original image and Entropy for the plain and cipher image and the gray correlation coefficient between the plain and cipher image

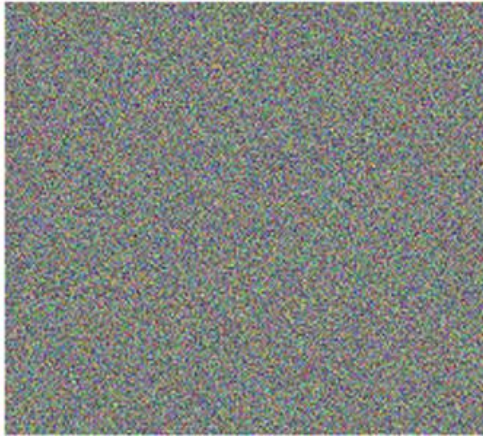
Test Image	Entropy for Plain Image	Entropy for Cipher Image	Correlation Coefficient
Lena	7.4451	7.9919	-0.076
Baboon	7.3577	7.9916	0.0013
Pepper	7.5936	7.9916	-0.0026



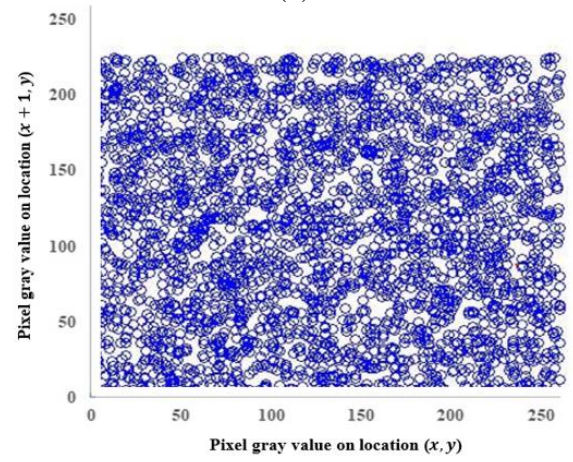
(a)



(b)



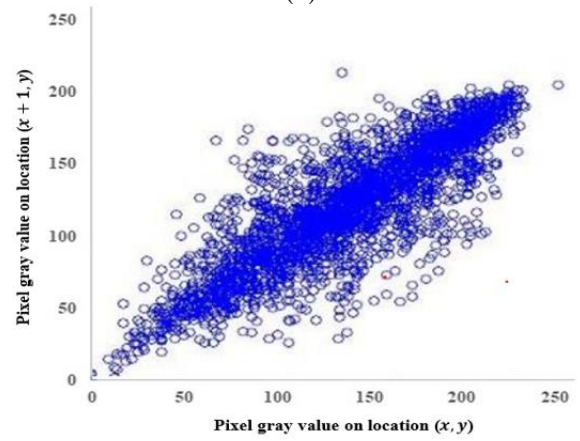
(c)



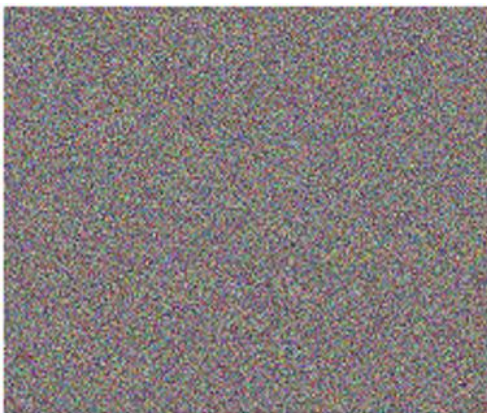
(d)



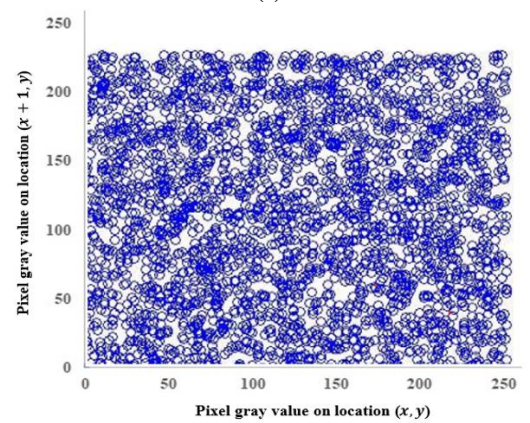
(e)



(f)



(g)



(h)

Figure 10. The correlation coefficients of gray images

8.3 PSNR and MSE

The experiment result shows that the stego image is a high-quality image because the PSNR is high and the MSE is low so the produced stego image of the proposed system is very good in quality. as illustrated in Table 4. Besides, Figure 11 presents the comparison of the original cover image with a histogram of the cover image and stego image.

Table 4. Illustrate the quality of the cover image and stego image

Test Image	Dimension Cover Image	Dimension Secret Image	MSE	PSNR
Lena	512 x 512	64 x 64	1.58	46.165
Baboon	512 x 512	64 x 64	1.59	46.149
Barbara	512 x 512	64 x 64	1.61	46.101

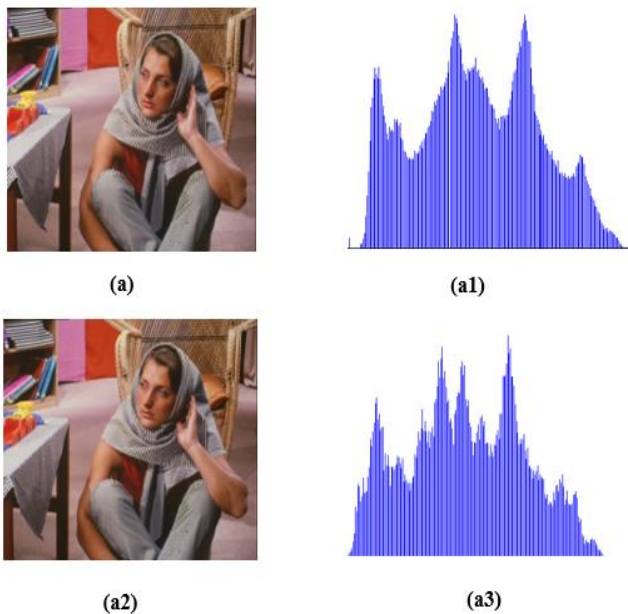


Figure 11. (a) the original cover image (512×512) (a1) the histogram of the cover image, (a2) the stego image (512×512), (a3) the histogram of stego image

In this research, a novel approach for protecting secret grayscale images based on advanced encryption and steganography was presented. The proposed framework comprises four phases: key generation encryption, secret sharing, and steganography. Through the encryption phase, the secret grayscale image is encrypted using the advanced AES encryption algorithm with multiple S-boxes determined by the number of rounds. During the secret sharing phase, the Shamir secret sharing scheme has been used to separate the encryption key to ensure the security of secret data transmission. Lastly, the LSB has been applied to cover the image. Moreover, the system has been compared with recent works in terms of security performance, confidence, reliability, and robustness. The proposed system has been compared with [18] and the results show better achievement due to using multiple S-boxes in the encryption phase. Moreover, the proposed method have been compared with [19, 20]. The integration of the proposed method in this article proves to provide better achievement in protecting secured information during transmission due to the steganography technique.

9. CONCLUSIONS

In this article, a new method to secure the transmission of data and information on the network. The process involves several phases by using the AES algorithm with a size of 128-bit for the data block to implement the encryption phase while the encryption key is generated in a random way to increase the ambiguity of the encryption. Moreover, the secret sharing scheme is applied to separate the secured information key into four shares. in addition, to provide a high protection level, the steganography technique is used to cover the secret information in a cover-colored image by applying the LSB algorithm. The integration of the proposed technique has contributed to providing more security and confidently transmitting data from one side to another. The proposed method offers an optimal solution for protecting transferred data. In addition, the proposed method restores the secured image without changes resulting in high correlation coefficients between the secured image and the retrieved image. The results show a satisfactory impact of the proposed method by achieving a high PSNR of 46.165 and a low MSE of 1.58. This achievement of results proves the effectiveness of the proposed method in securing the transmitted data.

ACKNOWLEDGMENT

The authors would like to thank the University of Anbar for supporting this project.

REFERENCES

- [1] Gayathri, R., Nagarajan, V. (2015). Secure data hiding using steganographic technique with Visual cryptography and watermarking scheme. 2015 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, pp. 118–123. <https://doi.org/10.1109/ICCSP.2015.7322691>
- [2] Hadj Brahim, A., Ali Pacha, A., Hadj Said, N. (2023). An image encryption scheme based on a modified AES algorithm by using a variable S-box. Journal of Optics, 53: 1170–1185. <https://doi.org/10.1007/s12596-023-01232-8>
- [3] Harn, L., Lin, C., Li, Y. (2015). Fair secret reconstruction in (t, n) secret sharing. Journal of Information Security and Applications, 23: 1–7. <https://doi.org/10.1016/j.jisa.2015.07.001>
- [4] Jiang, N., Zhao, N., Wang, L. (2016). LSB based quantum image steganography algorithm. International Journal of Theoretical Physics, 55(1): 107–123. <https://doi.org/10.1007/s10773-015-2640-0>
- [5] Rajput, M., Deshmukh, M., Nain, N. (2017). A novel approach for concealing image by utilizing the concept of secret sharing scheme and steganography. Proceedings-2016 15th International Conference on Information Technology (ICIT), Bhubaneswar, India, pp. 51–56. <https://doi.org/10.1109/ICIT.2016.023>
- [6] Rao, S.K., Mahto, D., Khan, D. A. (2017). A survey on advanced encryption standard. International Journal of Science and Research, 6(1): 711–724. <https://doi.org/10.21275/art20164149>
- [7] Hashim, J., Hameed, A., Abbas, M. J., Awais, M., Qazi, H. A., Abbas, S. (2018). LSB Modification based audio

- steganography using advanced encryption standard (AES-256) technique. In 2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, pp. 1-6. <https://doi.org/10.1109/MACS.2018.8628458>
- [8] Islam, M.R., Siddiq, A., Uddin, M.P., Mandal, A.K., Hossain, M.D. (2014, May). An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography. In 2014 International Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, Bangladesh, pp. 1-6 <https://doi.org/10.1109/ICIEV.2014.6850714>
- [9] Shankar, K., Eswaran, P. (2015). Sharing a secret image with encapsulated shares in visual cryptography. *Procedia Computer Science*, 70: 462–468. <https://doi.org/10.1016/j.procs.2015.10.080>
- [10] Shankar, K., Eswaran, P. (2016). A new k out of n secret image sharing scheme in visual cryptography. *Proceedings of the 10th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, India, pp. 1-6. <https://doi.org/10.1109/ISCO.2016.7726969>
- [11] Wakure, M.A., Holambe, A.N. (2015). A discrete wavelet transform: A steganographic method for transmitting images. *International Journal of Computer Applications*, 129(5): 26-29. <https://doi.org/10.5120/ijca2015906915>
- [12] Wang, X., Gao, S. (2020). Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. *Information Sciences*, 539: 195–214. <https://doi.org/10.1016/j.ins.2020.06.030>
- [13] Xian, Y., Wang, X. (2021). Fractal sorting matrix and its application on chaotic image encryption. *Information Sciences*, 547: 1154–1169. <https://doi.org/10.1016/j.ins.2020.09.055>
- [14] Kamble, P.R., Patil, S. (2018). Exploring secret image sharing with embedding of shares. In *Proceedings of the 2nd International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, pp. 1090-1093. <https://doi.org/10.1109/ICISC.2018.8398972>
- [15] Yassein, M.B., Aljawarneh, S., Qawasmeh, E., Mardini, W., Khamayseh, Y. (2017). Comprehensive study of symmetric key and asymmetric key encryption algorithms. *Proceedings of 2017 International Conference on Engineering and Technology (ICET)*, Antalya, Turkey, pp. 1–7. <https://doi.org/10.1109/ICEngTechnol.2017.8308215>
- [16] Zhou, W., Wang, X., Wang, M., Li, D. (2022). A new combination chaotic system and its application in a new Bit-level image encryption scheme. *Optics and Lasers in Engineering*, 149: 106782. <https://doi.org/10.1016/j.optlaseng.2021.106782>
- [17] Al-Ghamdi, M., Al-Ghamdi, M., Gutub, A. (2019). Security enhancement of shares generation process for multimedia counting-based secret-sharing technique. *Multimedia Tools and Applications*, 78(12): 16283–16310. <https://doi.org/10.1007/s11042-018-6977-2>
- [18] Arab, A., Rostami, M.J., Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. *Journal of Supercomputing*, 75(10): 6663–6682. <https://doi.org/10.1007/s11227-019-02878-7>
- [19] Dahat, A.V., Chavan, P.V. (2016). Secret sharing based visual cryptography scheme using CMY color space. *Physics Procedia*, 78: 563-570. <https://doi.org/10.1016/j.procs.2016.02.103>
- [20] De Los Reyes, E.M., Sison, A.M., Medina, R. (2019). Modified AES cipher round and key schedule. *Indonesian Journal of Electrical Engineering and Informatics (IJEI)*, 7(1): 29-36. <https://doi.org/10.1109/iciibms.2018.8549995>