

## Steganography Based On Chaotic System for Random LSB Positions

Rusul Mansoor Al-Amri<sup>1,2,\*</sup>, Dalal N. Hamood<sup>1</sup> and Alaa Kadhim Farhan<sup>1</sup>

<sup>1</sup>Computer Department/College of Science University AL-Nahrain, Baghdad, 10001, Iraq

<sup>2</sup>College of Nursing, University of Al-Ameed Karbala, PO No: 198 Iraq

\*Corresponding Author: Rusul Mansoor Al-Amr

DOI: <https://doi.org/10.31185/wjcm.95>

Received: September 2022; Accepted: November 2022; Available online: December 2022

**ABSTRACT:** The objective of hiding text in an image is hiding text without raising suspicions that the image contains a hidden message or text, which leads to protecting and maintaining text confidentiality. The previous hiding methods have problems in capacity, randomization, and imperceptibility. This paper will be solved some of these problems; we suggested a new method for hiding text in an image. Firstly, encrypting the text by the AES-192 bit algorithm for obtaining a secret message. When the initial key of the AES-192 (bit) algorithm is generated by a chaotic system for randomness purposes, secondly, hiding the secret message is into a gray image for obtaining a stego-image. The hiding step is based on a proposed map that chooses from the last round of key expansion in the AES-192 algorithm. This map represented random positions of LSB in each byte of the gray image. The experimental result of this method proved a successful method based on metric criteria. Also, this method is the very speed for hiding ciphertext in the gray image as well as extracting ciphertext from the gray image. Also, it is very safe because it is difficult for attackers to distinguish between the original image and the stego image therefore the correlation between the original image and the stego- image is very close to 1.

**Keywords:** Chaotic System, Gray Image, Stegoimage, LSB Technique



### 1. INTRODUCTION

Covered Text" is a word synonymous with Steganography. The hiding texts, data and information is very important [1, 2], as it aims to hide data without raising suspicions that it contains a hidden message or file, which leads to protecting it and maintaining its confidentiality [3]. The science of invisibility is completely different from the science of cryptography. To simplify the meaning, data encryption is represented as a safe that contains data, texts, and information. The safe can only be opened with a specific key, while steganography only refers to camouflaging [4–6]. In reality, steganography is an integral part of cryptography after the process of encrypting the text in one of the well-known encryption algorithms and after obtaining the ciphertext, the ciphertext is hidden under the cover and, steganography used to protect data from unauthorized persons [7]. Just as the protection of information requires a great effort, some encryption and concealment algorithms have had great success in concealing information, but some algorithms suffer from delaying the encryption time, delaying the time of concealment, and the quality of concealment. In this research, we have strived to achieve a balance between the speed of the encryption process and proposing a steganography map that achieves very high quality. The chaotic system was used to generate the encryption key. Chaos is one of the conducts that connect nonlinear systems and that develops specific values of an information system [8]. The discovery of this random system was considered a revolution that led to many interrelated issues, stability theory, new engineering features, and offers to distinguish signatures. The chaotic function has been used mainly to develop mathematical models for non-linear systems and has

\*Corresponding author: [sosoalhaji28@gmail.com](mailto:sosoalhaji28@gmail.com)

<https://wjcm.uowasit.edu.iq/index.php/wjcm>

been attracted by many mathematicians because of the high sensitivity of the initial value and its applications to daily life problems [9]. The chaotic functions have good features “sensitivity to initial conditions”, Fractal dimensions, the Lyapunov exponent, “strangeness”, and ECT [10, 11], therefore, it used in this research to generate the encryption key (Symmetric key) of the AES-192 bit algorithm to increase the confidentiality of the transmitted information and secure the transmission process. Also, the chaotic system is characterized by there are many types of chaotic functions, each of which has an advantage over the others of these types: Lorenz Equation., Rössler Equation, and Logistic Equation (this function has been used in our work) [12]. In this research, the chaotic system was used to generate the encryption key, and this is one of the most prominent strengths in our work, as it helped to increase the strength of the encryption and the speed of generating the encryption key, also use the last round of key expansion such as random positions of LSB technique for hiding secret text into gray image, therefore, the chaotic system helps the process of encryption and concealment gained durability and Speed and success this the proposed method. Section 2 describes some of the related work; Section 3 describes the proposed method; section 4 describes the experiments and results. Conclusions are explained in Section 5

## 2. LITERATURE REVIEW

Hussein L. Hussein [13] in this Search Steganography has done several masking methods according to the proposed maps to hide the message inside a gray image, so that the text is masked by drawing a map from ASCII that used (AMT) to create an encrypted table by mapping the text message and matching some bits with the cover image. The result is referred Low computational efficient performance to be used for multiple purposes Applications. Alaa Kadhim F and Rasha Subhi Ali [14] in this research, an advanced map was used to hide data, with which they used biotechnological methods for encryption and to improve the strength of data security while hiding messages inside an image. In this research, data hiding using LSB and DNA arithmetic were presented and they presented a new secret map to hide the data. (DNA) computing was used to encrypt data, and LSB was used to arrange the encrypted data to the least important elements of the cover, and they used a new secret map to locate locations. And Steganography. The researchers pointed out that the same equation is used for both the sender and the receiver to create a map, and this map depends on a common key.

Alaa Kadhim Farhan , Nadia M.G. Al-Saidi, Abeer Tariq Mold, Fahimeh Nazarimehr and Iqtadar Hussain [15], in this research, a new and unique chaotic system has been proposed, represented by crossing inside and outside the cylinder repeatedly. As an engineering system, the efficiency of the system in encryption images was tested. The performance of the encryption method is analyzed using the histogram, correlation coefficient, Shannon entropy, and encryption quality. The results show that the encryption method using the proposed chaotic system has reliable performance. Relying on this system and the tests conducted on it, the same tests were used in the research and the proposed method for our work.

Jagan Raj Jayapandiyar, Ph.D. Research Scholar, Kavita, Assistant Professor and Sakthivel and Professor [16] this proposed work improving the (LSB) method is based on the spatial domain. The proposed method is based on encrypting the text in two stages. The first stage is creating metadata and storing header information in the first few bytes of the images. The second stage is the process of including secret texts. Inside the cover image using the improved method, and in this proposed method, it results in the acquisition of space or a lesser method for the secret message in the cover image, and this leads to improving the quality of masking and obtaining standards for better results than the results obtained (eLSB). Our research presented in this paper has obtained much better results than the results obtained in this method in terms of evaluation criteria, and the consideration has been taken from several. This method will be encoded (eLSBRAISDSCSO) in our research in order to compare it with its results.

Ranyiah Wazirali, Waleed Alasmay, Mohamed Mahmoud and Ahmad Alhindi [17], In the research, the researchers presented a proposal for a new information steganography that works on the basis of a genetic algorithm. The researchers confirmed that this research works to increase the embedding capacity and reduce distortion. The research showed that scanning is better for pixels for vertical and horizontal directions, circular transformation, secret bit fluctuation, and transmission of confidential information after using the genetic algorithm. The (LSB) to include the data and the evaluation criteria were applied to it. The paper for our work was compared with this work and it was proven that the work presented in our research is better in terms of evaluation metrics. This method will be encoded (AOSHCAIUGA) in our research in order to compare it with its results.

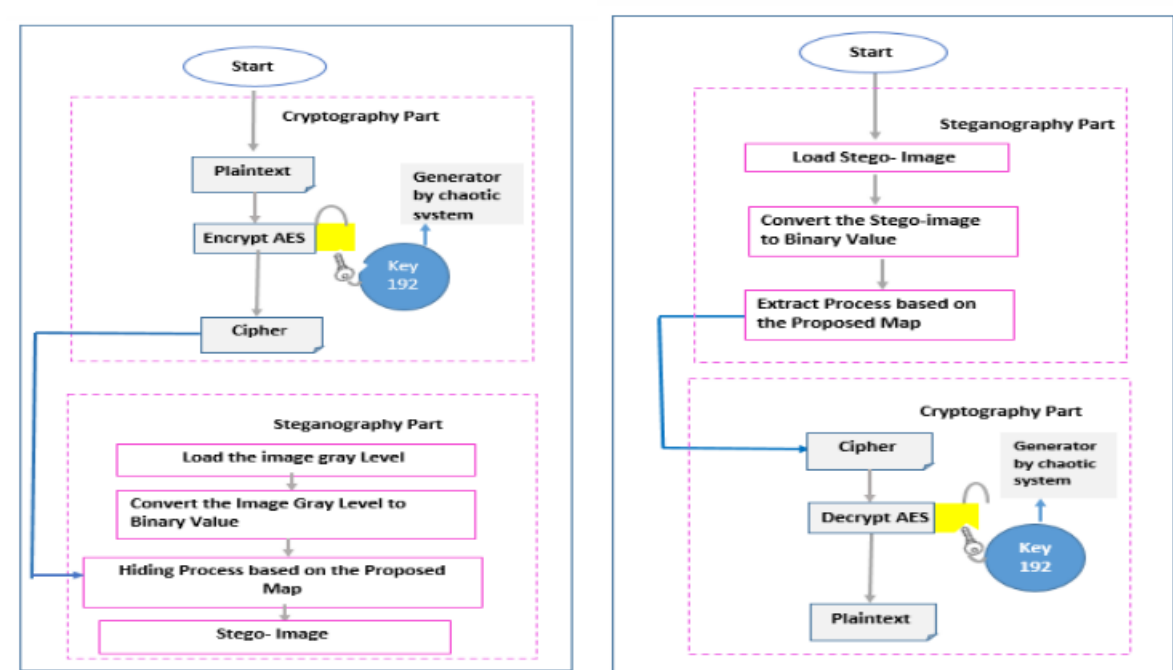
Mansoor Fateh, Mohsen Rezvani, and Yasser Iran [18], In this paper, the LSB approach has been proposed with an updated version, where the proposed matching approach works to LSB that the number of bits in the secret text is greater than 2 The work has been clarified in two steps, the first is to hide the secret text and the second is to extract the text. It has been shown that the method of the proposed approach needs to be changed less than LSBMR when the number of bits is greater than 2. The capacity in the proposed approach is higher than the F5 method when the number of the bit =3, where it was found that the number of secret text bits is greater than 2, its value = 75% this method is considered a new coding method because it reduces the change in the image. The results showed that this new method provides a 10% larger detection error for SRNet via two Steganography schemes. This method will be symbolized in our research (CFSLSB) in

order to be compared with its results.

Ali Salem Ali, Mohammed Sabbih Hamoud Al-Tamimi and Alaa Ahmed Abbood [19], in this research improvement of the (Bit Inverting Map) method of narrowing the gap to obtain effective results to maintain a balance between image accuracy, protection, and security. Comparisons of this method with previous methods have proven that the method is effective and superior to the rest of the methods. This method will be symbolized in our research (SISTMS) in order to be compared with its results.

### 3. METHOD

In the proposed method, the chaotic system was used to generate the encryption key, and this is one of the most prominent strengths in our work, as it helped to increase the strength of the encryption and the speed of generating the encryption key, also use the last round of key expansion such as random positions of LSB technique for hiding secret text into the gray image as shown in figure 1. The proposed method consists of two phases: the hiding phase and Extracting Phase. Both phases have two parts: cryptography and steganography. The hiding phase consists of the encryption process and the hiding process. Also, extracting phase consists of the decryption process and extracting process.



**FIGURE 1.** Main flowchart of the proposed method: (a) hiding phase and (b) extracting phase

In cryptography part, the AES-192 (bit) algorithm used for encrypting a text. The text consists of different lengths of characters. This algorithm has several advantages in terms of:

- Security: AES has the ability to resist attacks better than other encryption algorithms.
- Cost: This algorithm includes unlimited global domain and royalty-free.
- Implementation: The AES algorithm is flexible and well suited when implemented in hardware and software.

The AES-192 (bit) used because it is more complex than the AES-128 (bit) and less expensive than the AES-256 (bit). The initial key generated by chaotic system where a 24-digit was generated randomly each time to generate the key. The chaotic system was chosen in the generation of the key in order to achieve high protection strength and an increase in the chaos of key generation and the difficulty of predicting it. Where modern methods were used in chaotic sampling of data TOA (Time - of - arrival) in chaotic samples instead of random samples, and thus we will produce a sequence of chaotic values called (Chaotic sequences). And as we know that the chaotic system is a non-linear system its structure is unstable and the output behaves as a random behaviour in some steps and depends on the (initial condition) and (control

parameters).in order to determine the (Localization GD) and therefore equation (1) is the equation of the simple chaos logistics function chosen to generate the key of the algorithm AES192 bits. [20, 21]:

$$(X_{N+1}) = \lambda X_N (1 + X_N) \quad (1)$$

Where,  $N = 0, 1, \dots, L$  Length of Sequence  $\lambda$  = control Parameter

Table 1 shows chaotic system generated a different sequence with a different initial value. This key is distinguished by the speed of generation and the strength of the key, as it is difficult to predict the value of the key by an attacker.

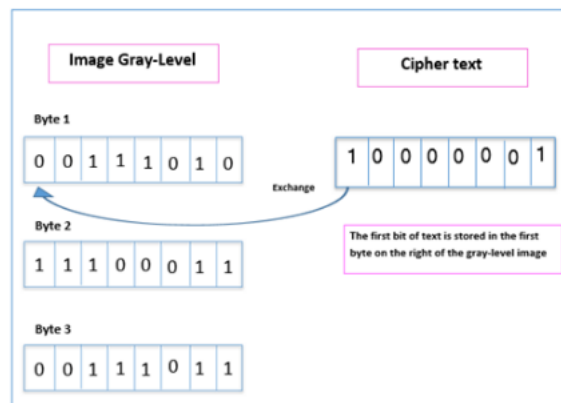
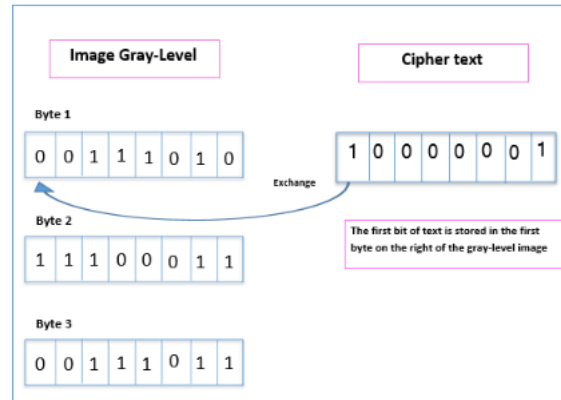
**Table 1. The chaotic system generated a different sequence with a different initial value**

No	Initial value	Initial key ( sequence)
1	0.33	131301301230123130013132
2	0.93	312222301223013023000123
3 4	0.20 0.59	123122301302300000122230 230130123230000013000130

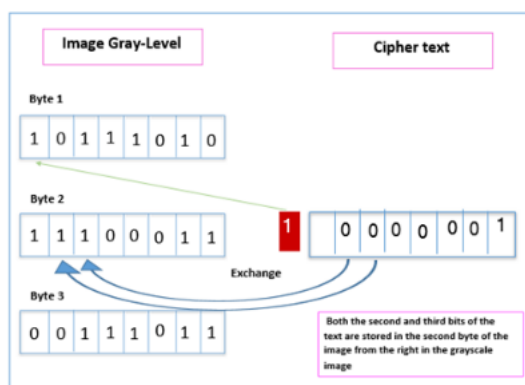
In the steganography part, the secret message hides in gray image based on a map that represented a random positions of the LSB as shown in table 2. The proposed map represented last round of key expansion in the AES-192 algorithm. In the map, when the value equal to 1, meaning hide one bit from secret message into the byte of gray image, when the value equal to 2, meaning hide two bits from secret message into the byte of gray image, when the value equal to 3, meaning hide three bits in the byte, and when the value equal to zero, meaning no hide in the current byte of the gray image. This map repeated for the length of secret message.

**Table 2. The proposed hiding map (last Round of Key Expansion)**

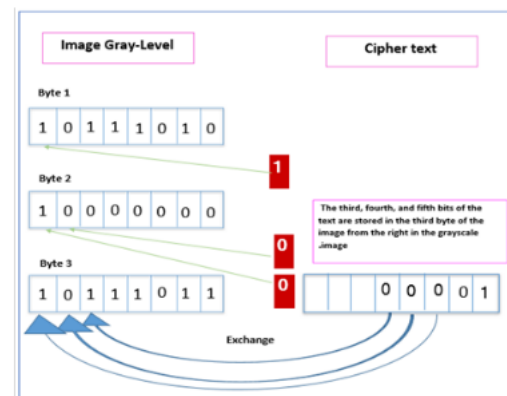
No.	Value in Hex	Decimal number	Map (Reminder of 3)
1	58	88	1
2	9d	157	1
3	36	54	0
4	Eb	235	1
5	fd	253	1
6	ee	238	1
7	38	56	2
8	7d	125	2
9	0f	15	0
10	Cc	204	0
11	9b	155	2
12	ed	237	0
13	4c	76	1
14	40	64	1
15	46	70	1
16	bd	189	0



(a)



(b)



(c)

**FIGURE 2.** (a) (b) (c) Hide the secret message into gray image based on random positions of the LSB

in the LSB of the first byte of gray sub-image as shown in figure 2(a). In the second step, hide the second and third bits of ciphertext "00" in the LSB of the second byte of gray sub-image as shown in figure 2(b). The third step, hide the fourth, fifth, and sixth bits of cipher text "001" in the LSB of the third byte of gray sub-image as shown in figure 2(c).

## 4. RESULTS AND DISCUSSION

In testing the proposed system for variant data and testing many coefficients for both the cryptography part and steganography parts. Take as an example 10 plaintext with different lengths and 10 gray images (or colored image transform for gray image) for the text steganography.

## 5. CRYPTOGRAPHY PART

This is the first part of the proposed system, applying the AES 192-bit algorithm. The initial key generated by the chaotic system, table 3 illustrated the different lengths of the plaintext that take different times for the encryption process, including the key generation time that generation chaotic system for achieving randomness. The encryption time is measured by picosecond because of the faster encryption process.

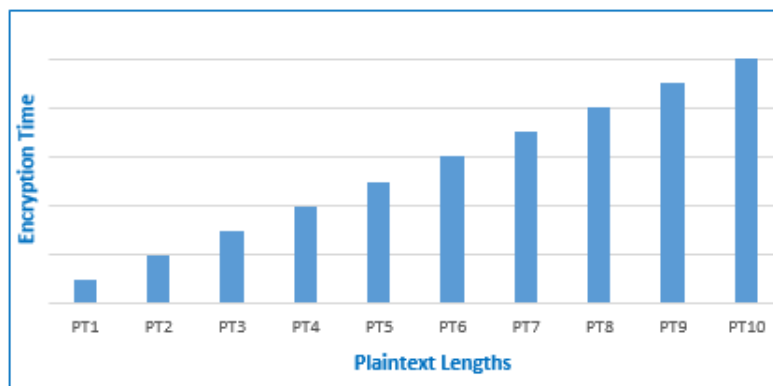
**Table 3. Encryption time for different lengths of plaintext and Hiding Time for different lengths of Ciphertext**

No	Plaintext (Char)	CipherText	Length Text (char)	Length Text (Block)	Encryption (Picosecond)	Time
1	Securities	7BC5FC6DF981BDC1E 687B98791DE84D9	10	1B	00:00:00.0064022	
2	College Science	481CE5A868F5CB5ED 9F87717C7A6C5E0	15	1B	00:00:00.0103620	
3	Al-Nahrain University	8030D2C95DA1430D66 F1385557C2E2E3F0 2E29F7000AB2FB7 5D0A7BEE8BE340D	20	2B	00:00:00.0120211	
4	In This Research We Used idea	8076498979C11B952B 839A5DEA0D9461917 3B9401AED39295 CBF95572814BA87	25	2B	00:00:00.0124387	
5	(AES) Algorithm With Key 192.	EED071F281E768317 BD54481D10369D9 DE3868457A88825422C 0E3044985830C	30	2B	00:00:00.0124844	
6	The Texts Consisting Of Difference	D30281A802181D32B9 2B861E78C8E07C7 544E7EF03A6E347CA4 5EB39CD6E4B9425D 3DCEE784DF67BD EA4E171A871FE3F	35	3B	00:00:00.0124889	
7	Cost: This Algorithm Includes Unlimited	9E0F3765EB13C54DBC 8C5FA2FD85D0AD71BF 9799BD905AA27AE7 B12070442A836E8F9548 FC2BA2A920 93D6C30B7382CB	40	3B	00:00:00.0125163	
8	Implementation: The AES Algorithm Is Flexible	B28CC01C55D49FBDDE1 3FFFF234AC59DB2B7 A3B7656182B6CCB57 BACB6F6FA7AF2EBFA 3401D8CF9E8F82 4E905D395BF	45	3B	00:00:00.0126289	

*Continued on next page*

<i>Table 3 continued</i>					
9	The 192 Cipher Keys Was Used Because It Is More	90A38700717B859CFD01 E929CE08D04B45 BDBDCDDCECF93CBA2D 8CEB5E1F4FC88 2D4C132E0D65B52E9BD 9084D039AA80819 E07D285241915 A9BEDA11F925859	50	4B	00:00:00.0134009
10	And After Selecting The Image We Convert The Value Of Each Pixel In The Image To The Binary System.	7BA3A6573629A46FBDF 58EA1238292228E F6E9AD3CCC1622E6419 70214EF4557DADA D8ABFE3DFF914806C B8D4C0326ABDDA3A A636E8A49F76D BDB24C8B530F1EF5E257F9 EC7E07A14381289 CF8E0E10DA3BAC4B019F 5E1F013DA3312 77DD27B42B58FF6F	100	7B	00:00:00.0855387

From the above result in table 3, the range of the plaintext from 10 (char) to 100 (char) in the other words, the range of the plaintext from (1) Block to (7) Block when increases the plaintext length due to increase the encryption time. The positive Relationship between the encryption time and plaintext length, as shown in figure 3.



**FIGURE 3. The positive Relationship between Encryption Time and Plaintext lengths.**

The proposed method that used chaotic system to generate initial key of the AES-192-bit standard algorithm, when examined the security of the cipher text against attacking by using the NIST. The proposed method proved is the strongest security and its success in all testing. Table 4 explains the cipher text encrypted by using key generation of chaotic system. From the result explain in table 4 the proposed modified key generation is stronger because its very secure ciphertext against the most attacks in all different cases.

## 6. THE STEGANOGRAPHY PART

This is the second part of the proposed system, apply Hiding process in the LSB but with random positions Of bits (based proposed map explain in table 1) in each byte of the gray image. Table 5 on the illustrated the gray image properties that used for hiding process.

From the result in table 5, the gray images have a different size and different image resolution. The proposed work checks the image size with the ciphertext length for making decisions that image has enough capacity for hiding

From the above result, the original images similar to the stego-images that any person could not show the effectiveness of the hiding process of your eye. When increases the cipher text length due to increase the hiding time. The Positive



**Table 4. NIST Test for The Ciphertext that Encrypted based on Chaotic System**

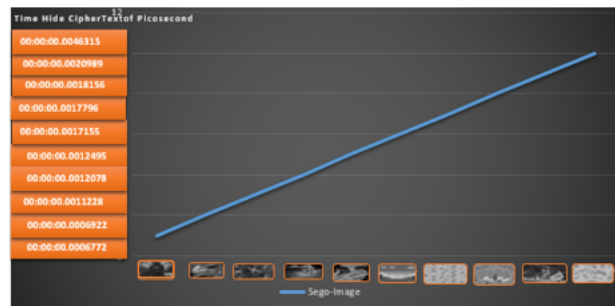
No	The Proposed AES-192 bit Proportion															
1	Attacks	Frequency	Block-Frequency	cumulative-sums	cumulative-sums	runs	longest-run	rank	Ft	nonperiodic-templates	overlapping-templates	Universal	Apen	Serial	tempel-ziv	linear-complexity
	Ciphertext															
1	7BC5FC6DF9818D C1E687B98791DE 84D9	0.1500	1.0000	0.4500	0.2500	0.3500	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.7300	1.0000	1.0000
	481CE5A868F5C8 5ED9F87717C7A6 C5E0	1.0000	1.0000	0.7990	0.8990	0.7990	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.6500	1.0000	1.0000
3	8030D2C95DA143 0D66F1385557C2 E2E3F0 2E29F700AB2FB 75D0A7BEE8BE34 0D	0.9300	0.8300	0.6900	0.7900	0.9810	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.7800	1.0000	1.0000
4	8076498979C11 B9528839A5DEA0 D9461917 3B9401AED39295 CBF95572814BA8 7	0.7700	1.0000	0.9600	0.9770	0.9980	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9900	1.0000	1.0000
5	EE0D71F281E768 317BD54481D103 69D9 DE38B8457A8B82 5422C0E3044985 830C	0.8600	1.0000	0.7890	0.9860	0.7690	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.8400	1.0000	1.0000
	D30281A802181D 32B928861E78C8 E07C7 544E7EFD3A6E34 7CA45EB39CD6E4 B9425D 3DCEE784D6F7BD EA4E171A871FE3 F	0.6200	1.0000	0.9430	0.8300	0.8300	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9800	1.0000	1.0000
7	9E0F3765E813C5 4DB8C8C5A2FD85 D0AD71BF 97998D905AA27 AE7812070442A8 36E8F9548 FC2BA2A92093D6 C30B7382CB	0.9500	1.0000	0.9250	0.9250	0.8990	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.8990	1.0000	1.0000
8	B2BCC01C55D49 FBDDE13FFFF254 AC59DB287 A3B7656182B6CC B57BACB6F6FA7A F2E87A 3401D8CF9EF82 4E9050395BF	0.8410	1.0000	0.9290	0.8200	0.9430	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9870	1.0000	1.0000
	90A38700717885 9CFD01E929CE08 DD4B45 B0B0CDDCECF9 3CBA2D8CEB5E1F 4FC88 2D4C132E0D65B5 2F9B09084D039A A80B19	1.0000	0.8330	0.8220	0.8220	0.9220	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9110	1.0000	1.0000
10	7BA3A6575629A 46F8DF58EA1238 292228F F6E9AD3CCC1622 E641970214EF45 57DADA D8ABFE3DFF9148 96CB8D4C0326AB DDA3A A636E8A49F76DB DB24C8B530F1EF 5E257F9 EC7E07A1438128 9CF8E0E10DA3BA C4B019F 5E1F013DA33127 7DD27842B58FF6 F	0.8965	1.0000	0.6520	0.7830	0.7880	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.8520	1.0000	1.0000



**Table 5.** Gray images properties

Original Image Properties				
.No	Image Name	Size Image	Image Resolution	Image Format
1	Image 1	KB 114.2	781 * 573	(Jpg.)
2	Image 2	Kb 16.4	241 * 318	(Jpg.)
3	Image 3	Mb 3.1	1024 * 1280	(Jpg.)
4	Image 4	Mb 1.7	1600 * 900	(Jpg.)
5	Image 5	Kb 315.8	225 * 225	(Jpg.)
6	Image 6	Kb 607.5	1208 * 1200	(Jpg.)
7	Image 7	Mb 1.1	1201 * 1200	(Jpg.)
8	Image 8	Kb 391.9	567 * 1200	(Jpg.)
9	Image 9	Kb 349.3	483 * 487	(Jpg.)
10	Image 10	Kb 708.1	1208 * 1200	(Jpg.)

Relationship between hiding time and cipher text lengths, as shown in figure 4

**FIGURE 4.** The positive relationship between hiding time and cipher text lengths.





















Tested 10 gray images with different properties for hiding ciphertext with different lengths. The measurements that used in this research, mean square error (MSE), Signal-To-Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR), Embedded Capacity measured (EC), Entropy, and Histogram. Table 7 illustrated the result of the previous metrics.

In the a blew table 7, the MSE that all values ranged between the highest value of 0.195816697 for gray image that has resolution (318X241) and the lowest value being very close to Zero 0.000977083 for gray image that has resolution (900 X 1600). Also, the gray image that has the lowest value of MSE that has the highest value of PSNR 75.72135129 and the highest value of the SNR 68.61384535 And the gray image that has the highest value of MSE that has the lowest value of PNSR 52.70217015 and the lowest value of SNR 47.15894861 These results indicate that the proposed method is a good quality and high secret according to the specific values of MSE, PSNR, and SNR [22].















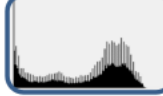


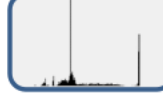





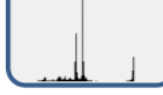


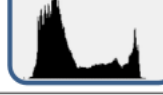



Also, EC measured is to embed and calculate the highest number of safe bits that can be hidden in the image that it is measured in units bits per pixel (bpp) [21, 23]. The largest value of EC in table 6 is (0.006680759) and smallest value of EC is (0.00015009). This result gives a good trace achieved through the proposed method, (EC) depends on the properties of the image as well as the length of the ciphertext.

Entropy is a measure of the degree of randomness between the original image and the stego image [24, 25], the entropy values ranged between (2.820111545) and (5.160472612). From entropy values notice that the entropy ratio is an acceptable and a good ratio compared to other steganography methods, where the lower the value is more optimize. The histogram shape was drawn to the stego image that hidden a ciphertext of different lengths, in table 7, the histogram shape has a good result that depends on the properties of the image and the length of the ciphertext. In additional, the investigation Variance and correlation that calculated between original image and Steganography image, as shown in figure 5.

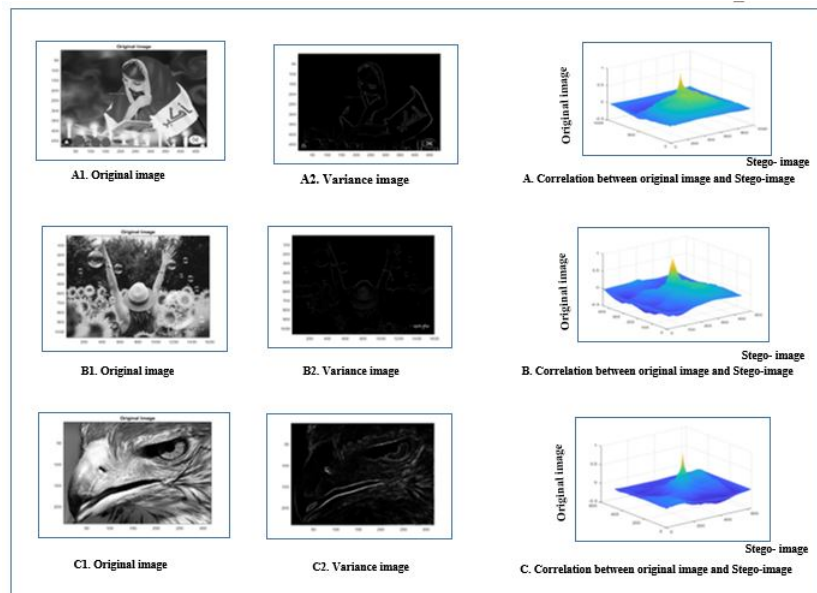
**Table 6.** the hiding time for different lengths of ciphertext

No	CipherText	Original image	Sego-Image	Time Hide Cipher Text of Pico-second
1	7BC5FC6DF981BDC1E687B98791DE84D9			00:00:00.0006772
2	481CE5A868F5CB5ED9F87717C7A6C5E0			00:00:00.0006922
3	8030D2C95DA1430D66F1385557C2E2E3F0 2E29F7000AB2FB75D0A7BEE8BE340D			00:00:00.0011228
4	8076498979C11B952B839A5DEA0D9461917 3B9401AED39295CBF95572814BA87			00:00:00.0012078
5	EED071F281E768317BD54481D10369D9 I. DE3868457A88825422C0E3044985830C			00:00:00.0012495
6	D30281A802181D32B92B861E78C8E07C7 544E7EF03A6E347CA45EB39CD6E4B9425D 3DCEE784DF67BDEA4E171A871FE3F			00:00:00.0017155
7	A. 9E0F3765EB13C54DBC8C5FA2FD85D0AD71BF B. 9799BD905AA27AE7B12070442A836E8F9548 FC2BA2A92093D6C30B7382CB			00:00:00.0017796
8	B28CC01C55D49FBDDE13FFFF234AC59DB2B7 A3B7656182B6CCB57BACB6F6FA7AF2EBFA 3401D8CF9E8F824E905D395BF			00:00:00.0018156
9	90A38700717B859CFD01E929CE08D04B45 BDBDCDDCECF93CBA2D8CEB5E1F4FC88 2D4C132E0D65B52E9BD9084D039AA80819 E07D285241915A9BEDA11F925859			00:00:00.0020989
10	7BA3A6573629A46FBDF58EA1238292228E F6E9AD3CCC1622E641970214EF4557DADA D8ABFE3DFF914806CB8D4C0326ABDDA3A A636E8A49F76DBDB24C8B530F1EF5E257F9 EC7E07A14381289CF8E0E10DA3BAC4B019F 5E1F013DA331277DD27B42B58FF6F			00:00:00.0046315

**Table 7.** The result of the MSE, SNR, PSNR, EC, Entropy, and Histogram

No	Original Image	<i>a)</i> Stego-image	MSE	SNR	PSNR	EC	Entropy	Histogram
1			0.016719067	56.27142619	63.38854686	0.000286025	4.756356902	
2			0.195816697	47.15894861	52.70217015	0.006680759	5.160472612	
3			0.008908081	58.09952948	66.07723042	0.000195313	4.706273263	
4			0.000977083	75.72135129	68.61384535	0.000177778	4.982106828	
5			0.26224197531	46.05826704	51.34221401	0.00505679	4.857598492	
6			0.006272765	64.09699232	67.64607724	0.000264901	3.865668401	
7			0.033364557	59.49768484	60.38781368	0.000266445	2.820111545	
8			0.031293357	57.75807129	60.66614582	0.000564374	3.282382696	
9			0.230595908	45.88919929	51.90072013	0.002176676	4.80577407	
10			0.040427704	58.77464446	59.55387655	0.000618102	3.093078133	

Entropy is a measure of the degree of randomness between the original image and the stego image [24, 25], the entropy values ranged between (2.820111545) and (5.160472612). From entropy values notice that the entropy ratio is an acceptable and a good ratio compared to other steganography methods, where the lower the value is more optimize. The histogram shape was drawn to the stego image that hidden a ciphertext of different lengths, in table 7, the histogram shape has a good result that depends on the properties of the image and the length of the ciphertext. In additional, the investigation Variance and correlation that calculated between original image and Steganography image, as shown in figure 5.






**FIGURE 5. The investigation Variance and The Correlation.**

From the above result in figure 5, it shows the variance of the images. The variance refers to how the pixel values are spread in the images, where the variance calculated for the original image and the stego-image was the result of the image (A) = 1.4981 and (B) = 5.1627 and (C) = 5.9343. Figure 5 illustrated the last measurement that is the Correlation between original image and Steganography image. It shows the Correlation between the original image and the steganography image according to the graph shown the Correlation of A = (0.982) and B = (0.999) and = (0.951). The results show that the relationship between the original image and the image is very close to 1 meaning that it is difficult to distinguish between the two images and this is evidence it is difficult for attackers to distinguish and the proposed method has proven to be a successful method.

Compare the results obtained through our proposed work to hide the ciphertext in a gray-level image based on the proposed map. It is worth mentioning that each of the methods in the comparison table 8 has used different properties of the images, as well as texts of different lengths. Then Compare the results for the best value in each method.

In the blew table (8), the evaluation results between the different remaining steganography methods and the proposed method showed. According to the results, the results of the proposed method are very good results compared to the rest methods.

**Table 8.** The comparison Evaluation Criteria between proposed method and other methods

Evaluation Criteria	proposed method	eLSBRAI SDSCSO	SIST MS	CFS LSB	AOSHC AIUGA
<b>MSE</b>	0.0009	0.00122		0.0147	-----
<b>PSNR</b>	75.7213	74.2795	72.82	66.4486	66.46
<b>SNR</b>	68.613	-----	-----	-----	-----
<b>Entropy</b>	2.8201	-----		-	-----
<b>EC</b>	0.00015 bit	-----	131,02Byte 6	3276 Byte 8	8,192 byte
<b>Variance</b>	5.1627	-----	-----	-----	-----
<b>Correlation</b>	0.999	-----	-----	-----	-----
<b>Histogram</b>			-----	-----	

#### 4.3 Algorithm of the proposed Method

**Algorithm name:** Steganography Based on Chaotic System for Random LSB Positions

**Input:** Plaintext, Initial value, Image as Img

**Output:** Stego-Image

**Processes:**

**Begin**

**Step 1:** Initial\_key=chaotic System (initial\_value)  
// Generate Initial Key by using chaotic system

**Step 2:** Key\_rounds=Expansion key(Initial\_key)  
// Generate key rounds by using expansion key of the AES algorithm

**Step 3:** ciphertext=Encryption process (plaintext, key\_rounds)

**Step 4:** Img\_binary=convert\_array\_of\_binary(Img)

**Step 5:** CT=Convert\_CipherText\_to\_Binary(ciphertext)

**Step 6:** set hidden\_map=first\_round (key\_rounds)

```

Step 7:    Hidden_R=Reminder (hidden_map,3)
Step 8:    Set i , j
Step 9: Set L=Length (Ciphertext)
Step 10: While i<L
Step 11:    If (Hidden_R==1)
                Hide One bit of CT (i) Into Img(X, Y).R
Step 12:    Else if (Hidden_R==2)
                Hide Two bits of CT (i) Into Img(X, Y).G
Step 13:    Else if ( Hidden_R==3)
                Hide Three bits of CT (i) Into Img(X, Y).B
Step 14:    InCremment X
Step 15:    if X = Img.Width & i <= L Then
Step 16:    ReSet X
Step 17:    InCremment Y
                End if
Step 18:    i = i + 6
                Wend //end While
End

```

## 7. CONCLUSION

Because increase the attackers and intruders that theft the information, the text steganography need for achieving the confidentiality. In this paper, suggested a new method for hiding a text in an image. Firstly, encrypting the text by the AES-192 bit algorithm for obtaining a secret message. When the initial key of the AES-192 (bit) algorithm is generated by chaotic system for randomness purpose, secondly, hiding the secret message into a gray image for obtaining a stego-image. The hiding step based on a proposed map that choice from last round of key expansion in AES-192 algorithm. This map represented a random positions of LSB in each byte of gray image. This map cannot guested testing of the proposed method obtained a faster method for hiding ciphertext in the gray image as well as extracting ciphertext from gray image. Also, it is difficult to distinguish between the original image and stego-image because the correlation between the original image and the image is very close to 1 meaning that it is difficult for attackers to distinguish among two images and the proposed method has proven to be a successful method based on Mean Square Error (MSE), Signal to Noise Rate (SNR), Peak Signal Noise Rate (PSNR), Embedding Capacity (EC), Entropy, and Histogram.

## FUNDING

None

## ACKNOWLEDGEMENTS

The authors would like to thank Al-Nahrain University, University of Technology and Iraqi Ministry of Education for their support to conduct the work published in this paper.

## CONFLICTS OF INTEREST

The author declares no conflict of interest.

## REFERENCES

- [1] A. Bhatnagar, S. Chaku, and M. Sainger, "Hiding Compressed and Encrypted Data byusing a Technique of Steganography," *International Journal of Engineering Research & Technology (IJERT)*, vol. 09, no. 04, 2020.
- [2] J. Ashok, Y. Raju, S. Munishankaraiah, and K. Srinivas, "Steganography: An Overview," *International Journal of Engineering Science and Technology*, vol. 2, no. 10, pp. 5985–5992, 2010.
- [3] Q. M. T. Ahvanooy and Li, "Modern Text Hiding, Text Steganalysis, and Applications: A Comparative Analysis," vol. 2019, pp. 355–355.
- [4] N. Dalal, K. A. Hmood, M. S. Khudhia, and Altaei, "A New Steganographic Method for Embedded Image In Audio File," *International Journal of Computer Science and Security (IJCSS)*, no. 6, pp. 2012–2012.
- [5] "Combination of Steganography and Cryptography: A short Survey," *2nd International Conference on Sustainable Engineering Techniques (ICSET 2019)*, *IOP Conf. Series: Materials Science and Engineering*, vol. 518, pp. 52003–52003, 2019.
- [6] A. R. Hamza, "Text-based Steganography using Huffman Compression and AES Encryption Algorithm," *Iraqi Journal of Science*, vol. 62, no. 11, pp. 4110–4120, 2021.
- [7] N. Zainab, Sultani, N. Ban, and Dhannoon, "Image and audio steganography based on indirect LSB," *Kuwait J.Sci*, vol. 48, no. 4, pp. 1–12, 2021.



- [8] A. Gupta, D. Tiwari, V. Kumar, K. P. S. Rana, and S. Mirjalili, "A Chaos-Infused Moth-Flame Optimizer," *Arabian Journal for Science and Engineering*, 2022.
- [9] R. V. Soléa and Jordibascompte, "Measuring chaos from spatial information," *Journal of Theoretical Biology*, vol. 175, no. 2, pp. 139–147, 1995.
- [10] Z. Rahman, X. Yi, I. Khalil, and M. Sumi, "Chaos and Logistic Map based Key Generation Technique for AES-driven IoT Security," 2022.
- [11] R. Huffaker, M. Bittelli, and R. Rosa, "Nonlinear Time Series Analysis with R," 2018.
- [12] Q. V. Lawande, B. Ivan, and P. S., "Chaos Based Cryptography," A new approach To Secure Communication," 2005.
- [13] H. L. Hussein, A. A. Abbass, A. Sinan, S. Naji, J. H. A.-A. A, and Lafa, "Hiding text in gray image using mapping technique," *Article in Journal of Physics Conference Series*, 2018.
- [14] A. K. F. R. Subhi, and Ali, "Hidden Encrypted Text Based On Secrete Map Equation And Bioinformatics Techniques," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 1, 2019.
- [15] A. K. Farhan and N. M. G. Al-Saidi, "Abeer Tariq Maolood, Fahimeh Nazarimehr and Iqtadar Hussain "Entropy Analysis and Image Encryption Application Based on a New Chaotic System Crossing a Cylinder," *Entropy*, vol. 2019, no. 10, pp. 958–958.
- [16] C. J. R. Jayapandiyan, K. Kavitha, and Sakthivel, "Enhanced Least Significant Bit Replacement Algorithm in spatial domain of Steganography using character sequence optimization," *IEEE Access*, 2020.
- [17] "An Optimized Steganography Hiding Capacity And Imperceptibly Using Genetic Algorithms," *IEEE Access*, 2019.
- [18] M. Fateh, M. Rezvani, and Y. Iran, "A New Method of Coding for Steganography Based on LSB Matching Revisited," *Hindawi Security and Communication Networks*, 2021. 2021.
- [19] "Secure Image Steganography through Multilevel Security," *International Journal of Innovation, Creativity and Change*, vol. 11, no. 1, 2020.
- [20] S. Dhawan and R. Gupta, "Analysis of various data security techniques of steganography: A survey," *Information Security Journal: A Global Perspective*, vol. 30, pp. 2021–2021, 2020.
- [21] "Image Steganography Based On Odd/Even Pixels Distribution Scheme and Two Parameters Random Function"," *Journal of Theoretical and Applied Information Technology*, vol. 95, pp. 22–22, 2017.
- [22] N. Manohar and P. V. Kumar, "Data Encryption & Decryption Using Steganography," *Proceedings of the International Conference on Intelligent Computing and Control Systems*, vol. ISBN, pp. 978–979.
- [23] "Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document," *IEEE Access*, vol. 8, pp. 27448–27458, 2020.
- [24] A. S. Nuha, Z. M. Alwan, and Hussain, "Compressive Sensing with Chaotic Sequences: An Application to Localization in Wireless Sensor Networks," *Wireless Personal Communications*, 2019.
- [25] A. Kaiser, Reshak, N. Ban, Z. N. Dhannoon, and Sultani, "Explicit feedback based movie recommendation system: A survey," *AIP Conference Proceedings*, vol. 2290, pp. 40009–40009, 2020.
- [26] A. Azhaar, A. K. Abdallah, and Farhan, "A New Image Encryption Algorithm Based on Multi ChaoticSystem," *Iraqi Journal of Science*, vol. 63, no. 1, pp. 324–337, 2022.