



ISSN: 0067-2904

## Linear Feedback Shift Registers-Based Randomization for Image Steganography

Mohammed Abod Hussein\*, Saad Al-Momen

Department of Mathematics, College of Science, University of Baghdad, Baghdad, Iraq

Received: 12/4/2023

Accepted: 27/5/2023

Published: 30/8/2023

### Abstract:

Steganography involves concealing information by embedding data within cover media and it can be categorized into two main domains: spatial and frequency. This paper presents two distinct methods. The first is operating in the spatial domain which utilizes the least significant bits (LSBs) to conceal a secret message. The second method is the functioning in the frequency domain which hides the secret message within the LSBs of the middle-frequency band of the discrete cosine transform (DCT) coefficients. These methods enhance obfuscation by utilizing two layers of randomness: random pixel embedding and random bit embedding within each pixel. Unlike other available methods that embed data in sequential order with a fixed amount. These methods embed the data in a random location with a random amount, further enhancing the level of obfuscation. A pseudo-random binary key that is generated through a nonlinear combination of eight Linear Feedback Shift Registers (LFSRs) controls this randomness. The experimentation involves various 512x512 cover images. The first method achieves an average PSNR of 43.5292 with a payload capacity of up to 16% of the cover image. In contrast, the second method yields an average PSNR of 38.4092 with a payload capacity of up to 8%. The performance analysis demonstrates that the LSB-based method can conceal more data with less visibility, however, it is vulnerable to simple image manipulation. On the other hand, the DCT-based method offers lower capacity with increased visibility, but it is more robust.

**Keywords:** Information hiding, Embedding data, Image security, Spatial domain Frequency domain, LSB, DCT, Randomness, LFSR, Payload capacity.

### أخفاء البيانات في الصور عشوائياً بالاعتماد على المسجلات الخطية الزاحفة ذات التغذية الرجعية

محمد عبود حسين\*، سعد محمد علي المؤمن

قسم الرياضيات، كلية العلوم، جامعة بغداد، بغداد، العراق

### الخلاصة:

تتم عملية إخفاء المعلومات عن طريق تضمين البيانات في وسائط الغلاف، ويمكن تصنيف الطرق التي تستخدم لهذا الغرض إلى نوعين رئيسيين: الطرق التي تعمل في النطاق المكاني والتي تعمل في النطاق الترددي. تقترح هذه الورقة طريقتين: الأولى، تعمل في النطاق المكاني، حيث تستخدم وحدات البت الأقل أهمية (LSBs)

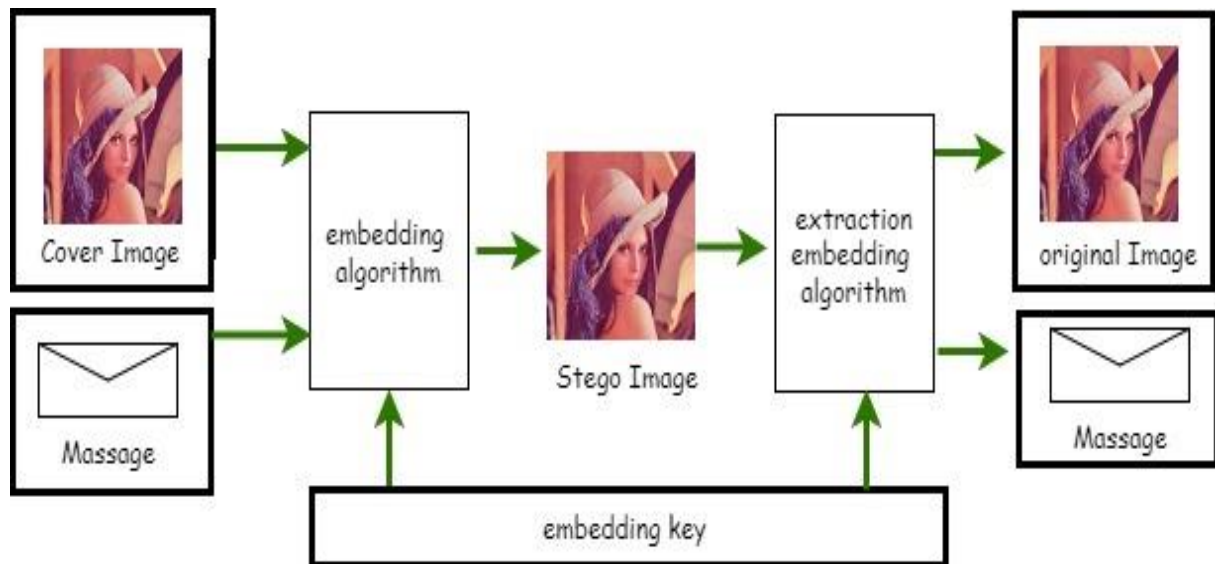
\*Email: [mohammed.hasan2103m@sc.uobaghdad.edu.iq](mailto:mohammed.hasan2103m@sc.uobaghdad.edu.iq)

لإخفاء رسالة سرية. فيما تعمل الطريقة الثانية في النطاق الترددي، حيث تخفي الرسالة السرية داخل LSBs لنطاق التردد المتوسط لمعاملات تحويل جيب التمام المنفصل (DCT). تعمل هذه الطرق على تحسين التشويش من خلال استخدام طريقتين من العشوائية: تضمين البكسل العشوائي ودمج البت العشوائي داخل كل بكسل. على عكس الطرق الأخرى المتاحة التي تقوم بتضمين البيانات بترتيب تسلسلي بكمية ثابتة، فإن هذه الأساليب تضمن البيانات في موقع عشوائي بكمية عشوائية، مما يزيد من تعزيز مستوى التشويش. يتحكم مفتاح ثنائي عشوائي زائف بهذه العملية، تم إنشاؤه من خلال تركيبة غير خطية من ثمان مسجلات خطية زاحفة ذات تغذية رجعية (LFSR). تضمنت التجربة صور غلاف مختلفة بحجم  $512 \times 512$ . حققت الطريقة الأولى متوسط PSNR يبلغ 43.5292 مع سعة حمولة تصل إلى 16% من صورة الغلاف. في المقابل، حصلت الطريقة الثانية على متوسط PSNR يبلغ 38.4092 مع سعة حمولة تصل إلى 8%. أظهر تحليل الأداء أن الطريقة المستندة إلى LSB يمكنها إخفاء المزيد من البيانات مع قابلية ملاحظة أقل ولكنها عرضة للتأثر بأي تلاعب بسيط بالصورة. من ناحية أخرى، توفر الطريقة القائمة على DCT سعة أقل وقابلية ملاحظة أكبر، لكنها أكثر ثباتاً.

## 1. Introduction

Due to the widespread use of digital networks in exchanging and transmitting information through various communication channels, information security has become an imperative necessity to preserve data from manipulation or theft by an intruder [1]. Among the most popular used methods in information security are encryption and Steganography [2, 3]. These are two methods to secure data either by encrypting it with a key or hiding it in a secret way [4]. steganography is the science and art of covert communications and involves two procedures. First, the required message is concealed in a particular carrier, e.g., image, audio, text, etc., that is called a steganographic cover. The second procedure concerns transmitting the cover to the message recipient without drawing suspicion. Fundamentally, the steganographic goal is not to hinder the adversary from decoding a hidden message, but to prevent the adversary from suspecting the existence of covert communications [5]. Some examples of steganography that have been used in the past include invisible inks and writing messages on the envelopes of letters in the area that is covered by postage stamps. Benedict Arnold used codes and steganography to communicate with the British during the American Revolutionary War. His coded messages were written in invisible ink (though now visible) and interspersed between the lines of a normal letter written by his wife, Peggy Shippen Arnold [6].

There are five domains that are used with digital steganography each domain has some techniques that help to improve the hiding processing. These domains are the spatial domain, transform domain, spread spectrum domain, statistical domain, and distortion domain [7]. This paper will focus on spatial and transform domains. The least significant bit (LSB) method will be the technique used in the spatial domain, where the message is directly embedded in the cover media [8]. On the other hand, the discrete cosine transform (DCT) method is the technique that will be used in a transform domain where the cover media is transformed and then the message is embedded in the transformed representation [9].



**Figure 1:** General block diagram of secret key image steganography

## 2. Related work

In both the spatial and transform domains, various ideas and approaches have been contributed by numerous researchers. By reviewing studies conducted in recent years, the advancements and achievements that are made by these researchers in the field are to be understood. Ahd Aljarf and John Filippas introduced an algorithm to embed data within meticulously chosen clean images, aiming to generate STEGO images containing one or more embedded data files. This procedure incorporated diverse statistical tools to conceal individual and multiple data files using masking techniques. Subsequently, a comprehensive analysis and testing were conducted to assess the differences between the initial clean images and their corresponding Stego versions [10]. Huda Najeeb and Israa Ali proposed a steganography method utilizing the Least Significant Bit (LSB) to embed text files in conjunction with the associated image within a gray-scale image. They also explored the concept of the bit plane which consists of eight separate segments that, when merged, create the actual image. [11]. Beenish Siddiqui and Sudhir Goswami described the various techniques using the LSB substitution method to hide the data in images and proposed a new approach based on transform domain using NSGA (Non-Dominated Sorting Algorithm) for a better quality of stego image [12]. Mohammed Mahdi et al, summarized the current image steganography techniques in the spatial domain and also analyzed different problems and the drawbacks of each method that have been innovated in the last few years. Few of their works on better image quality, while others on the data hiding capacity or security [13]. Sonali K. Powar et al concluded that the spatial domain technique provides a good capacity but it does not robust against different attacks. While the frequency domain technique provides good robustness with less capacity [14].

Many researchers have been observed to employ sequential embedding methods, hiding the same number of bits in each pixel designated for embedding. This approach makes these methods more susceptible to detection due to their routine behavior. To address this issue, this paper introduces a two-layer randomness strategy: one layer for selecting the pixel to store the secret message and another for determining the number of bits to be hidden in that pixel. This randomness is regulated by a pseudo-random key, as it is depicted in Figure 1, which is generated by a random key generator. The details of the generating process are discussed in Section 1.2.

Moreover, two embedding methods are proposed: the first is based on LSBs, the details are provided in Section 2.2. The second is based on DCT with specifics outlined in Section 2.3.

The experimental part of this study and the analysis of results are covered in Section 3 and its sub-sections.

### 3. The Proposed Methods

Ensuring the secure concealment of information within images is crucial for data security, as previously mentioned. This paper presents two methods for hiding information randomly both of which rely on generating a random binary sequence through the use of the Linear Feedback Shift Registers (LFSR). This sequence is used as a key for hiding the information. The first proposed method operates in the spatial domain and hides a varying number of bits within the Least Significant Bits (LSBs) of a chosen cover pixel. While, the second proposed method operates in the transform domain, hiding a varying number of bits within the LSBs of a chosen coefficient from the middle-frequency range of the Discrete Cosine Transform (DCT) coefficients.

#### 3.1 Random Key Generator

The proposed methods use a random binary sequence as a key that is generated by connecting 8 LFSRs as shown in Figure 2, The connection is done according to the following equation:

$$X = X_1 \oplus (X_2 \oplus (X_3 \oplus (X_4 \oplus (X_5 \oplus (X_6 \oplus (X_7 \oplus X_8))))))$$

Where  $X$  is the final output of the random key generator and  $X_i$  is the output of the  $i^{th}$  LFSR ( $i = 1,2, \dots 8$ ) and the symbol  $\oplus$  represents the XOR operation

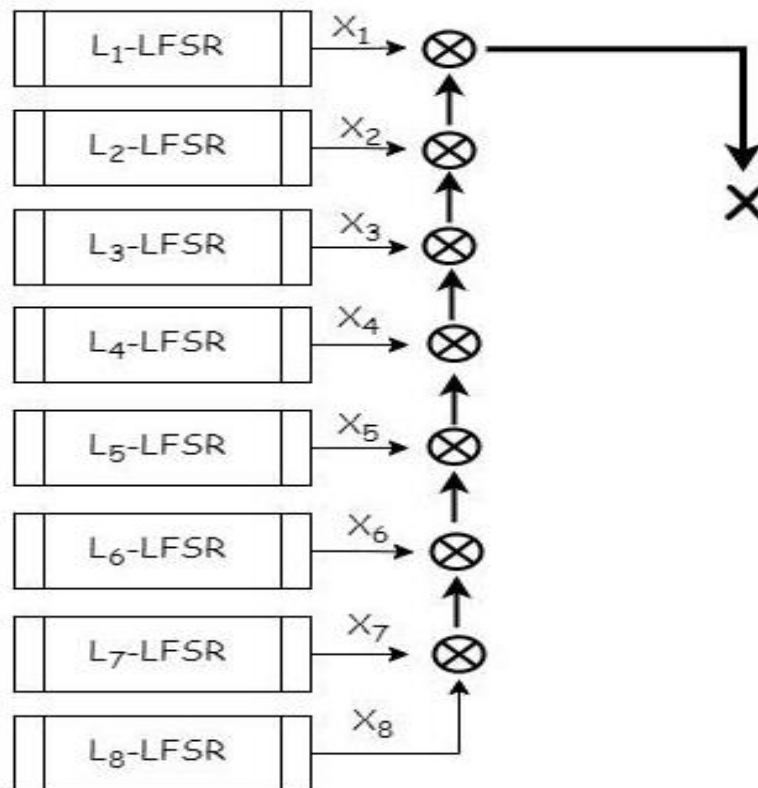


Figure 2: Random Key Generator.

The lengths of these LFSRs are selected to be distinct and satisfy the condition  $gcd(L_i, L_{i+1}) = 1$ , where  $L_i$  is the length of the  $i^{th}$  LFSR ( $i = 1, 2, \dots, 7$ ). To achieve a maximal sequence length [15], the feedback polynomial of each LFSR is chosen to be a primitive polynomial of order  $L_i$ , which guarantees a period of  $2^{L_i} - 1$  for that LFSR [16]. The length of the key sequence  $X$  should be sufficiently greater than 8 times the length of the message to accommodate the entire plaintext without repeating the key stream. Each LFSR needs a primitive feedback polynomial and an initial state to operate. The selection of these two factors can be made by the sender. The sender chooses a text key  $K$ , which is converted into a binary sequence  $KB$ . The first  $L$  bits of  $KB$  are used as initial states for the LFSRs and are distributed according to the needs of each of them, where  $L = \sum_{i=1}^8 L_i$ . This process is shown in Figure 3.

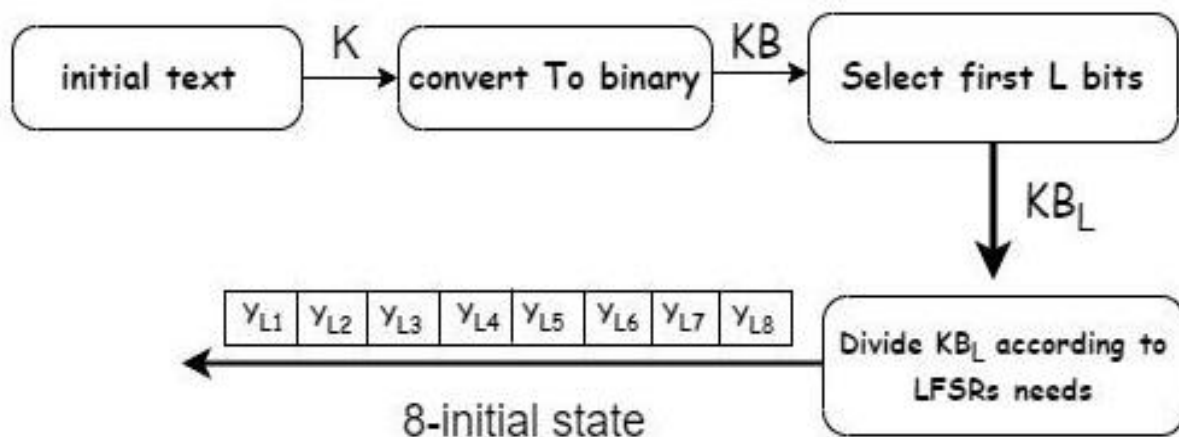


Figure 3: Block Diagram of Initial States Selection.

On the other hand, the first 96 bits of  $KB$  are divided into eight sub-sequences  $c_i$  of 12 bits each, and each  $c_i$  is converted to a decimal number  $w_i \in [0,4095]$ . According to the factorization theorem [15], there are  $\frac{\varphi(2^n-1)}{n}$  primitive polynomials of order  $n$ , where  $\varphi(x)$  is the Euler totient function. Hence, for the  $i^{th}$  LFSR, the primitive polynomial number  $q_i$  in the list of all primitive polynomials of order  $L_i$  will be chosen such that  $q_i = w_i \bmod \frac{\varphi(2^{L_i}-1)}{L_i}$ . This process is shown in Figure 4.

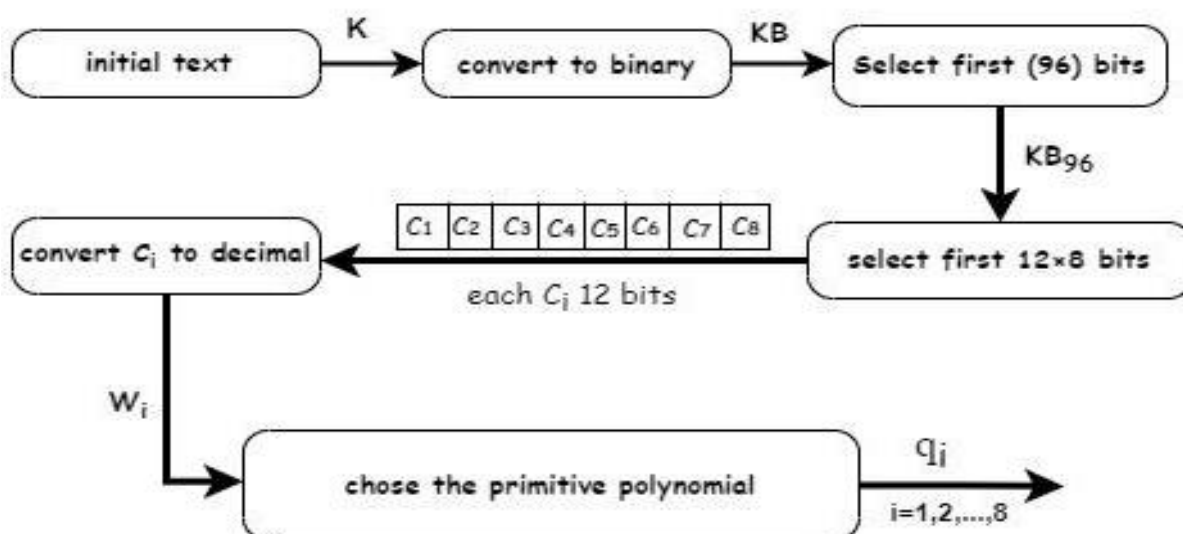


Figure 4: Block Diagram of Primitive Feedback Polynomials Selection.

### 3.2 LSB-Based Steganography using Variable-Length Embedding

To begin the process, the cover image is converted into a binary sequence  $CK$  by converting each pixel's integer value into an 8-bit binary number. Simultaneously, the text message  $M$  to be hidden is transformed into a binary sequence  $MS$  of length  $8L_1$ , where  $L_1$  is the number of characters in the original text message. This is done by converting the ASCII code of each character into an 8-bit binary number.

Next, the key  $KS$  generated in section 3.1 is divided into blocks  $b_k$ , each block consists of 2 bits. These blocks are converted into decimal numbers  $d_k$  where  $0 \leq d_k \leq 3$ . Each  $d_k$  is then used to determine how many bits of the  $MS$  sequence will be hidden in the LSBs of each pixel of the cover image. It is important to note that the number of bits that will be changed from the original pixel value will differ from one pixel to another including when  $d_k = 0$ , which means that the pixel will be overridden and does not hide any bit in it. This process produces a binary  $SK$  sequence.

Finally, the  $SK$  sequence is converted to decimal numbers and then reshaped to match the dimensions of the original image. The steps of this method are summarized in Algorithm 1, while Figure 5 provides a block diagram that illustrates the process.

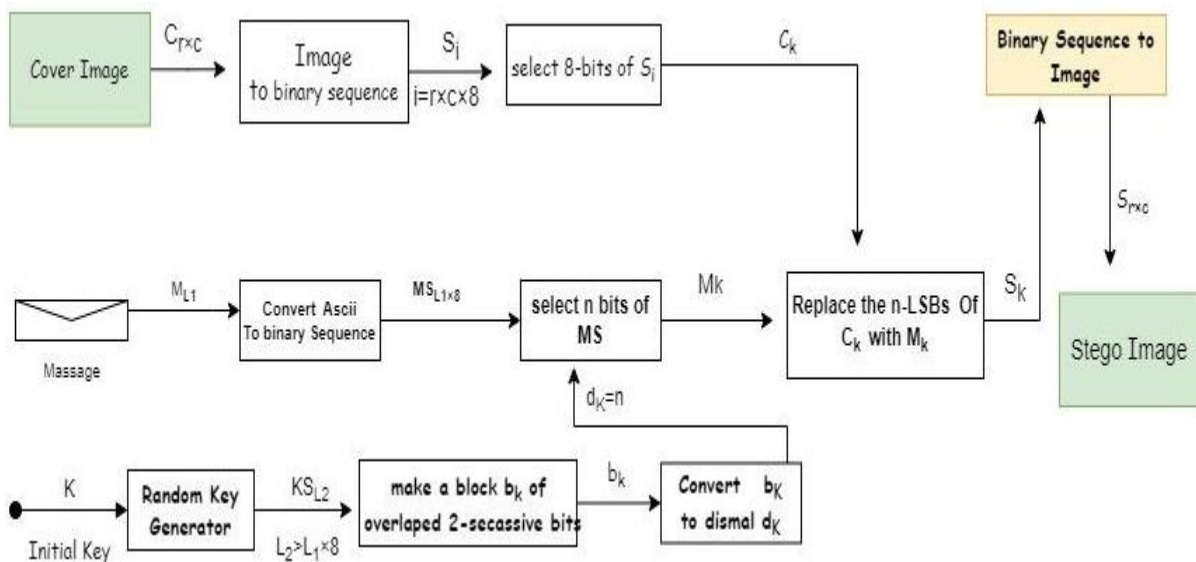


Figure 5: Block Diagram of LSB-Based Steganography using Variable-Length Embedding.

#### Algorithm 1: LSB-Based Steganography using Variable-Length Embedding

**Input:** Cover image  $C$ , Message  $M$ , Key  $KS$ .

**Output:** Stego-image  $S$ .

Step 1: Convert the cover image  $C$  into a binary sequence  $CK$  by converting each pixel's integer value into an 8-bit binary number.

Step 2: Convert the message  $M$  into a binary sequence  $MS$  of length  $8L_1$ , where  $L_1$  is the number of characters in the message. This is done by converting the ASCII code of each character into an 8-bit binary number.

Step 3: Divide the key  $KS$  into blocks  $b_k$ , each consisting of 2 bits.

Step 4: Convert  $b_k$  into a decimal number  $d_k$ , where  $0 \leq d_k \leq 3$ .

Step 5: For each pixel in  $CK$ :

a. If  $d_k = 0$ , skip to the next pixel.

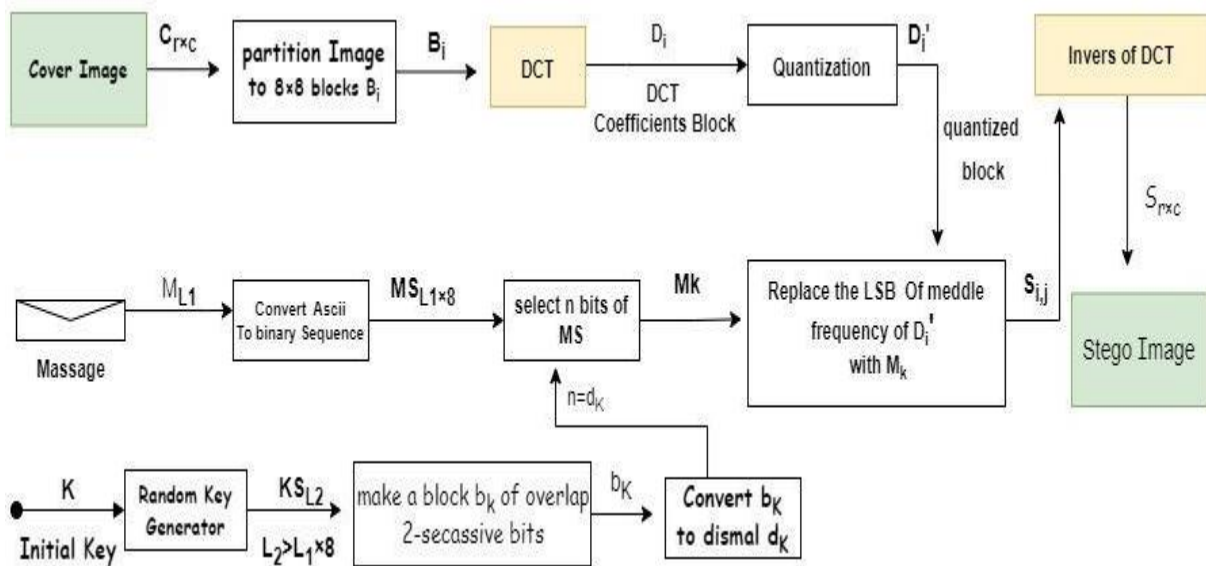
b. Otherwise, replace the least significant bits of the pixel's binary value with the corresponding bits from the **MS** sequence, up to a maximum of  $d_k$  bits. (The resulting sequence is the binary **SK**)

Step 6: Convert the **SK** into decimal numbers and reshape the resulting sequence to produce the stego-image **S** which is the same size as the original image.

### 3.3 DCT-Based Steganography using Variable-Length Embedding

In the second proposed method, the LSBs of the Discrete Cosine Transform DCT coefficients of the cover image will be utilized for hiding the message. It is widely known that if an image is converted into DCT, then the frequencies are redistributed as low, medium, and high, respectively, from the left-top corner to the right-bottom corner. Additionally, it is common knowledge that all the details of the image are represented by the low frequencies. Thus, changing the low-frequency range can have a significant impact on the final stego-image, and therefore, the hiding information should be avoided in this part. Meanwhile, the high-frequency range is susceptible to loss of its values when the image is compressed (e.g., JPEG compression). Thus, information hiding in this part can result in information loss. Based on these two points, the middle-frequency area is chosen for hiding the message.

As illustrated in Figure 6, the process of generating  $d_k$  and **MS** is identical to that of the first proposed method. However, the second method distinguishes itself by concealing the message in the LSBs of the middle frequencies of the DCT coefficients instead of the LSBs of the spatial domain pixels.



**Figure 6:** Block Diagram of DCT-Based Steganography using Variable-Length Embedding.

The cover image is first split into multiple sub-images of size 8x8. Next, the DCT is computed for each sub-image. Following this, the quantization operation is performed to produce integer values. Then, the message is concealed in the LSBs of DCT coefficients in the middle frequencies part. The parameter  $d_k$  determines the number of bits to be hidden in each selected coefficient. This process results in a set of sub-images labeled as  $S_{ij}$ . Finally, the inverse DCT is computed to each sub-image to generate the stego image. The steps of this method are summarized in Algorithm 2.

**Algorithm 2: DCT-Based Steganography using Variable-Length Embedding**

Input: Cover image  $C$ , Message  $M$ , Key  $KS$ .

Output: Stego-image  $S$ .

Step 1: Convert the cover image  $C$  into a binary sequence  $CK$  by converting each pixel's integer value into an 8-bit binary number.

Step 2: Convert the message  $M$  into a binary sequence  $MS$  of length  $8L_1$ , where  $L_1$  is the number of characters in the message. This is done by converting the ASCII code of each character into an 8-bit binary number.

Step 3: Divide the key  $KS$  into blocks  $b_k$ , each consisting of 2 bits.

Step 4: Convert  $b_k$  into a decimal number  $d_k$ , where  $0 \leq d_k \leq 3$ .

Step 5: Split the cover image  $C$  into multiple sub-images of size  $8 \times 8$

Step 6: For each sub-image:

a. Compute the DCT coefficients.

b. Quantize the coefficients to produce integer values.

c. Determine the middle frequency coefficients and select a set of coefficients to hide the message.

Step 7: For each chosen coefficient:

a. If  $d_k = 0$ , skip to the next coefficient.

b. Otherwise, replace the least significant bits of the coefficient with the corresponding bits from the  $MS$  sequence, up to a maximum of  $d_k$  bits.

Step 8: Compute the inverse DCT for each sub-image to generate the stego-image  $S$ .

Step 9 : Return the stego-image  $S$ .

#### 4. Experimental Results and Analysis

The tests and performance evaluation are presented in two parts, the first is a Randomness sequence test, and the second is a performance test of the proposed inclusion method.

##### 4.1 Evaluating Key Randomness

In order to verify the statistical characteristics of the key, the SP800-22 test package, developed by the National Institute of Standards and Technology (NIST), is utilized for random performance detection [17]. The selection of SP800-22 as a tool for evaluating randomness is based on its use in assessing the AES cipher and its frequent application in formal certification or approvals. In the tests, a keystream sequence of length 1,000,000 bits that are generated by the proposed keystream generator is examined. Table 1 illustrates the results of the tests. Each row of the table presents the name of the test, the P-value, and the test result. No deviation from a truly random sequence is shown in the results mentioned in the table, as all P-values are greater than the significant value  $\alpha = 1\%$ .



**Table 1:** Evaluating Key Randomness

Test	P-value	Result
Frequency (Monobit)	0.3544	Success
Block Frequency	0.3953	Success
Runs	0.6390	Success
Longest Run of Ones	0.3769	Success
Binary Matrix Rank	0.8825	Success
DFT	0.3083	Success
Non Over Lapping Templates	0.4922	Success
Over Lapping Template	0.9915	Success
Universal Statistical	0.4399	Success
Serial Test	0.9420	Success
Approximate Entropy	0.5086	Success
Cumulative Sums (Forward)	0.5130	Success
Random Excursions Test		Test Not Applicable
Random Excursions Variant		Test Not Applicable
Linear Complexity		Test Not Applicable

**4.2 Performance Metric on Spatial and Transform Domain**

Several commonly used metrics for evaluating performance and ensuring image quality. Among the most important assessments are the signal-to-noise ratio (PSNR), mean squared error (MSE), and normalized cross-correlation (NCC). [18] [19].

- The Peak Signal to Noise Ratio (PSNR) evaluates the resemblance between two images (original and stego images) and is directly related to the Mean Squared Error [20, 21]. The equation for PSNR is as follows:

$$PSNR = 10 \log_{10} \left[ \frac{I^2}{MSE} \right].$$

In this equation,  $I$  represents the dynamic range of pixel values or the maximum possible value for a pixel. For 8-bit images,  $I$  is equal to 255. MSE refers to the mean square error.

- The Mean Squared Error (MSE) quantifies the difference between two images; a lower MSE value indicates higher image quality [22, 23]. The equation for MSE is as follows:

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [I(i, j) - K(i, j)]^2 .$$

In this equation,  $I(i, j)$  represents the original image, while  $K(i, j)$  denotes the stego image. The variables  $M$  and  $N$  correspond to the dimensions of the image.

- Normalized Cross Correlation (NCC) assesses the level of similarity (or difference) between two images being compared. Its primary advantage is its reduced sensitivity to linear changes in illumination amplitude within the compared images [24, 25]. The equation for NCC is as follows:

$$NCC = \frac{\sum_{i=1}^N \sum_{j=1}^M (I_{ij} \times K_{ij})}{\sum_{i=1}^N \sum_{j=1}^M (I_{ij})^2}.$$

Figure 7 illustrates a set of standard images, both before and after incorporating a hidden binary message, along with their respective histograms. The final column displays the randomization map. In this map, the red points signify the embedding of 1 bit in a pixel, the green points represent the embedding of 2 bits, and the blue points indicate the embedding of 3 bits. The black points, on the other hand, denote skipped pixels. Simultaneously, Table 2 provides a comprehensive display of the numerical values corresponding to the three-performance metrics discussed earlier: PSNR, MSE, and NCC.

On the other hand, the embedding in the frequency domain using the proposed method is illustrated in Figure 8, and the numerical values for the three metrics are provided in Table 3.

It should be noted that the modified quantization table proposed by Li and Wang was utilized for the quantization step. [26].

Furthermore, the results of the proposed method for frequency domain embedding have been compared with both the widely recognized Jsteg method and the method proposed by Senthoran and Ranathunga [27].

For comparison purposes, the same images and payloads used in [27] were utilized. The images involved in this comparison can be seen in Figure 9.

**Table 2:** Performance Metric in Spatial Domain

Cover Image	Image size	Payload (bits)	PSNR	MSE	NCC
<b>Lena</b>	512×512	345215	43.5410	2.8773	0.9994
<b>Barbara</b>	512×512	345215	43.5439	2.8754	0.9994
<b>Baboon</b>	512×512	345215	43.5288	2.8854	0.9992
<b>Peppers</b>	512×512	345215	43.5313	2.8837	0.9996
<b>Goldhill</b>	512×512	345215	43.4969	2.9067	0.9994
<b>Cameraman</b>	512×512	345215	43.5331	2.8825	0.9996
<b>Average</b>	512×512	345215	43.5292	2.8852	0.9994


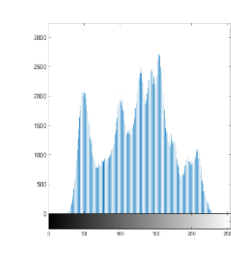

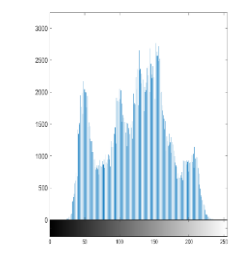
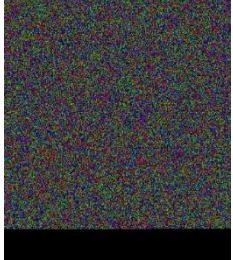

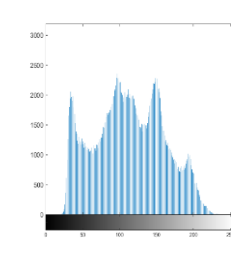

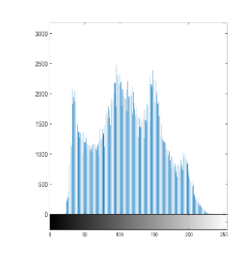
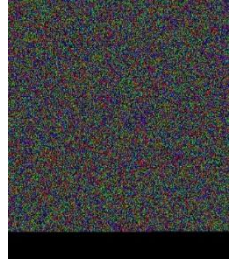
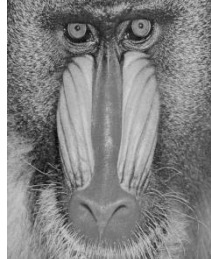
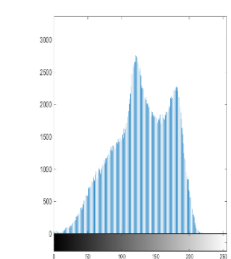
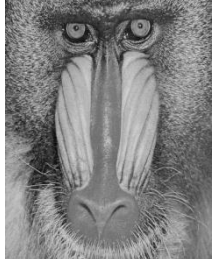
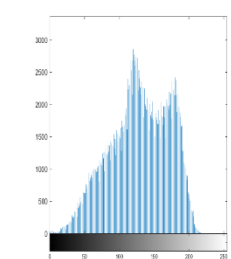
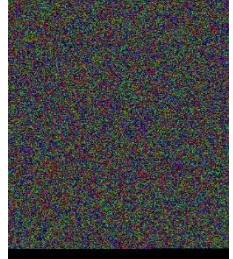

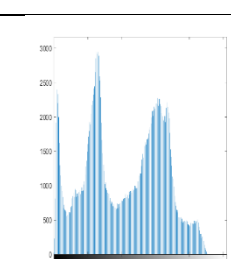

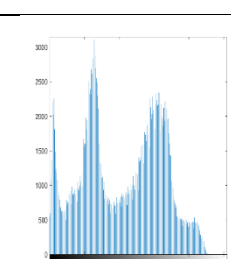
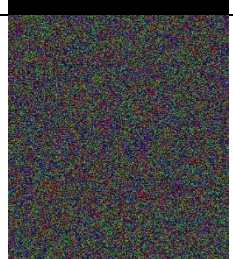
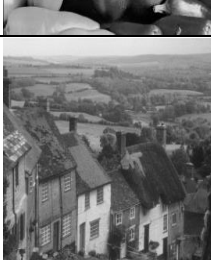
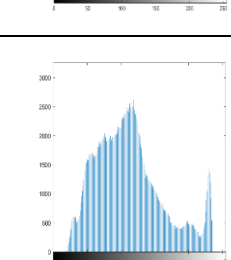

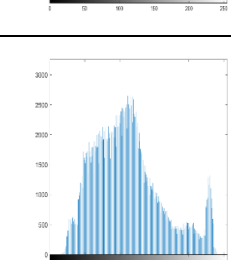
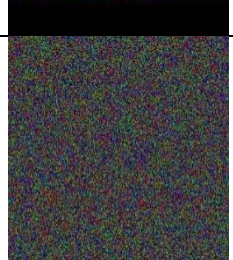

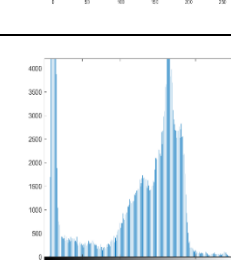

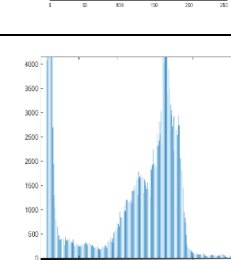
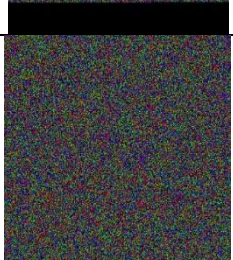

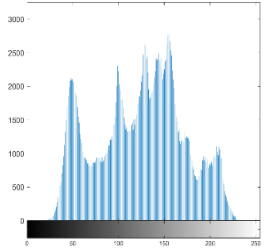

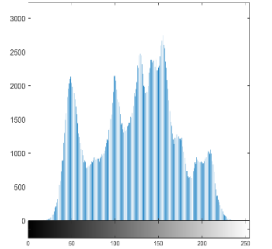

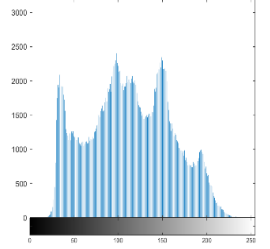

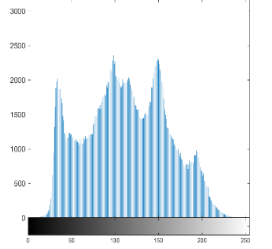
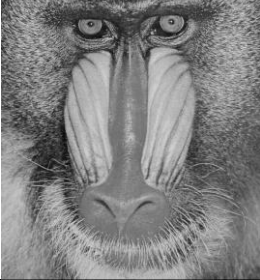
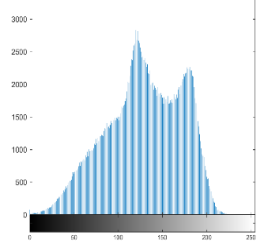

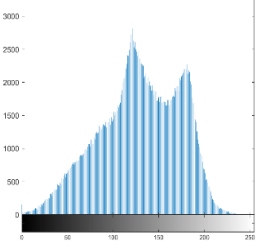

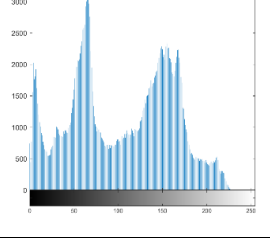

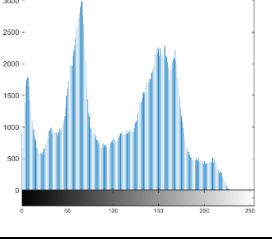

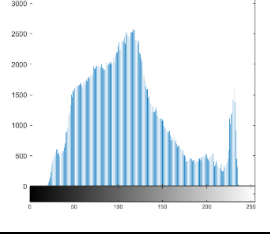

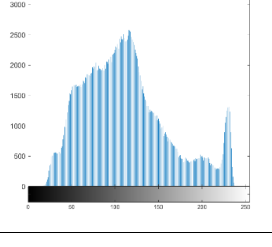

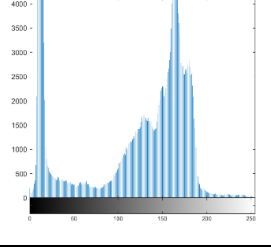

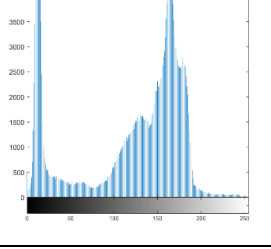
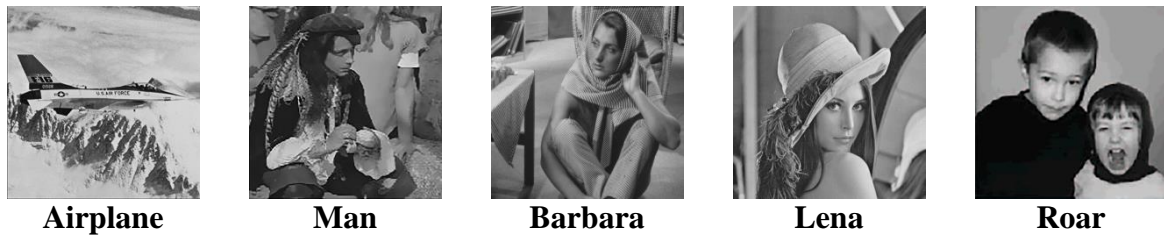
Name	Cover image	Cover image histogram	Stego image	Stego image histogram	Randomization map
Lena					
Barbara					
Baboon					
Peppers					
Goldhill					
Cameraman					

Figure 7: The images before and after embedding the secret message in the spatial domain

Name	Cover image	Cover image histogram	Stego image	Stego image histogram
Lena				
Barbara				
Baboon				
Peppers				
Goldhill				
Cameraman				

**Figure 8:** The images before and after embedding the secret message in the frequency domain



**Figure 9:** The collection of images utilized for conducting the comparison

The average results that are presented in Table 4 indicate that the proposed method outperforms the other two methods, as it exhibits the lowest error and highest PSNR. Additionally, a graphical representation of the comparison based on MSE and PSNR is illustrated in Figures 10 and 11, respectively.

Figure 12 illustrates the relationship between payload and PSNR, MSE, and NCC, respectively. It is apparent that the first and third relationships are inverse, while the second relationship is proportional

**Table 3:** Performance Metric in Transform Domain

Cover Image	Image size	Payload (bits)	PSNR	MSE	NCC
Lena	512×512	167936	42.1517	3.9619	0.9992
Barbara	512×512	167936	35.0522	20.3168	0.9955
Baboon	512×512	167936	30.3041	60.6278	0.9842
Peppers	512×512	167936	42.1283	3.9834	0.9994
Goldhill	512×512	167936	40.7536	5.4667	0.9989
Cameraman	512×512	167936	40.0652	6.4057	0.9992
<b>Average</b>	512×512	167936	38.4092	16.7937	0.9967

**Table 4:** Comparative Results for Jsteg, Senthooran & Ranathunga, and the Proposed Method

Cover Image	Payload	MSE			PSNR		
		Jsteg	Senthooran & Ranathunga	Proposed Method	Jsteg	Senthooran & Ranathunga	Proposed Method
Airplane	105536	31.4586	26.1262	2.6692	33.1534	37.2589	43.8670
Man	121714	50.345	34.801	1.6507	31.1112	36.7316	45.9542
Barbara	122952	65.5876	55.8191	19.7663	29.9626	33.0522	35.1715
Lena	95936	19.8841	20.0296	3.0544	35.1457	33.0567	43.2815
Roar	59624	9.8284	12.8471	0.8240	38.206	37.4658	48.9714
<b>Average</b>	<b>101152</b>	<b>35.4207</b>	<b>29.9246</b>	<b>5.9292</b>	<b>35.5158</b>	<b>35.5130</b>	<b>43.4500</b>

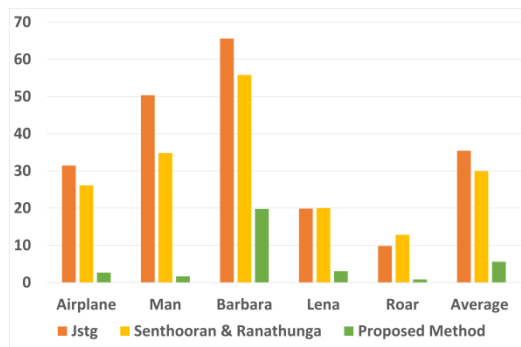


Figure 10: Comparison of MSE Values

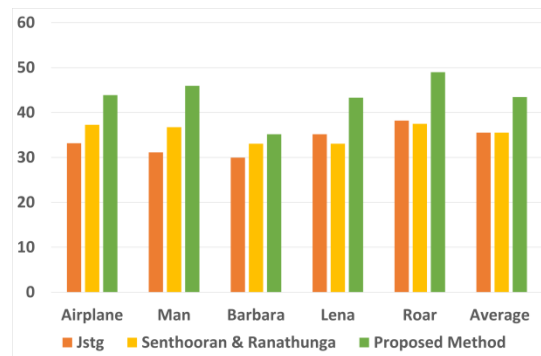


Figure 11: Comparison of PSNR Values

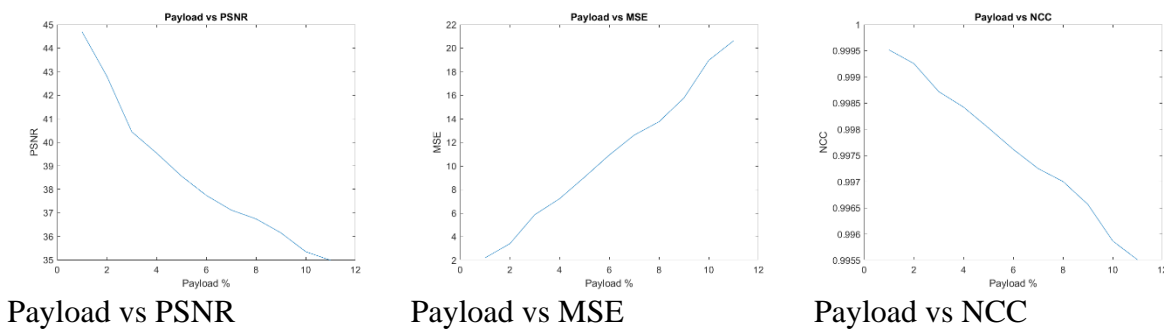


Figure 12: Payload vs. PSNR, MSE, and NCC Relationships

### 5. Conclusions

The objective of steganography is to have secret messages concealed within cover images. In most existing techniques, information is embedded sequentially in the image, and a fixed number of bits is utilized for each pixel, making the hidden message more susceptible to attacks. In this study, it is proposed that obfuscation can be enhanced by having the pixel for message embedding randomly selected, and by having the number of bits hidden within the chosen pixel randomly determined. For this purpose, a random binary key that is generated from a non-linear combination of eight LFSRs is employed. Due to its speed, simplicity, determinism, and affordability, the method is selected.

Two approaches are proposed, namely having the data hidden in the spatial domain and having it hidden in the frequency domain. In the first approach, while a large volume of data can be concealed, the preservation of the data becomes challenging if the cover image is subject to external influences. Consequently, the second approach involves having the data hidden in the frequency domain, specifically in the middle range of frequencies, offering greater resilience against influences on the cover image. However, the amount of hidden data is smaller than in the first approach. Experimental results indicate that high image quality and substantial message capacity are provided by both proposed methods, in addition to the obfuscation achieved through the two layers of randomness mentioned.

### References:

- [1] N. M. G. AL-SAIDI, S. S. AL-BUNDI and N. J. AL-JAWARI, "An improved harmony search algorithm for reducing computational time of fractal image coding," *Journal of Theoretical and Applied Information Technology*, vol. 95, pp. 1669-1679, April 2017.
- [2] M. S. Taha, . M. S. Mohd Rahim, S. a. lafta, M. M. Hashim and H. M. Alzuabidi, "Combination of steganography and cryptography: A short survey," *materials science and engineering*, vol. 518, p. 052003, 2019.
- [3] E. S. I. Harba, "Secure data encryption through a combination of AES, RSA and HMAC," *Engineering, Technology & Applied Science Research*, vol. 7, pp. 1781-1785, 2017.
- [4] S. Almuhammadi and A. Al-Shaaby, "A survey on recent approaches combining cryptography and steganography," *Computer Science Information Technology (CS IT)*, pp. 63-74, 2017.
- [5] A. Desoky, *Noiseless steganography: The key to covert communications*, CRC Press, 2012, p. 275.
- [6] S. Tanna, *Codes, Ciphers, Steganography & Secret Messages*, U K: Answers 2000 Limited, 2020.
- [7] F. . Q. A. Alyousuf, R. Din and A. J. Qasim, "Analysis review on spatial and transform domain technique in digital steganography," *Bulletin of Electrical Engineering and Informatics*, vol. 9, pp. 573-581, 2020.
- [8] G. Swain and S. K. Lenka, "Classification of image steganography techniques in spatial domain: a study," *Journal of Computer Science & Engineering Technology (IJCSET)*, vol. 5, pp. 219-232, 2014.
- [9] S. DUTTA and K. SAINI, "Securing Data: A Study on Different Transform Domain," *WSEAS Transactions on control*, pp. 110-120, January 22, 2021.
- [10] A. Aljarf, S. Amin and J. Filippas, "Creating Stego-Images through hiding single and multiple data using different steganographic tools," in *Signal Processing, Pattern Recognition and Applications (SPPRA 2013)*, Innsbruck, Austria, 2013.
- [11] H. D. Najeeb and I. T. Ali, "A proposal of Multimedia Steganography Algorithm based on Improved," *Iraqi Journal of Science*, vol. 58, pp. 2188-2199, 2017.
- [12] B. Siddiqui and S. Goswami, "A survey on image steganography using LSB substitution," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 5, pp. 345-349, may 2017.
- [13] M. M. HASHIM, M. S. MOHD RAHIM and A. A. ALWAN, "A review and open issues of multifarious image steganography techniques in spatial domain," *Journal of Theoretical & Applied Information Technology*, vol. 96, pp. 956-977, 28 February 2018.
- [14] S. . K. Powar, H. T. Dinde and R. M. Pati, "A Study and Literature Review on Various Image Steganography," *International Research Journal of Engineering and Technology (IRJET)*, vol. 7, no. 8, pp. 3258-3261, August 2020.
- [15] F. Masoodi, S. Alam and M. Bokhari, "An analysis of linear feedback shift registers in stream ciphers," *International Journal of Computer Applications*, vol. 46, pp. 46-49, 2012.
- [16] M. A. Abdulwahed and A. G. N. Al-Shammari, "Construct a New System as a Combining Function for the LFSR in the Stream Cipher Systems Using Multiplicative Cyclic Group," *Iraqi Journal of Science*, vol. 59, pp. 1490-1500, 2018.
- [17] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson , M. Vangel, D. Banks , N. Heckert , J. Dray, S. Vo and L. Bassham, Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications, National Institute of Standards & Technology, 2010.
- [18] F. Q. A. Alyousuf, R. Din and A. J. Qasim, "Analysis review on spatial and transform domain technique in digital steganography," *Bulletin of Electrical Engineering and Informatics*, vol. 9, pp. 573-581, 2020.
- [19] U. Ali, M. Sohrawordi and M. P. Uddin, "A robust and secured image steganography using LSB and random bit substitution," vol. 8, pp. 39-44, 2019.
- [20] N. H. M. Ali, A. M. . S. Rahma and A. S. Jamil, "Text hiding in color images using the secret key transformation function in GF (2 n)," *Iraqi Journal of Science*, vol. 56, pp. 3240-3245, 2015.
- [21] R. N. Kadhun and N. H. M. Ali, "Using steganography techniques for implicit authentication to enhance sensitive data hiding," *International Journal of Nonlinear Analysis and Applications*, vol. 13, pp. 3973-3983, 2022.
- [22] R. J. Essa, N. A. Abdullah and R. D. AL-Dabbagh, "Steganography technique using genetic algorithm," *Iraqi Journal of Science*, vol. 59, pp. 1312-1325, 2018.

- [23] M. A. A. Khodher, A. Alabaichi and A. A. Altameemi, "Steganography Encryption Secret Message in Video Raster Using DNA and Chaotic Map," *Iraqi Journal of Science*, vol. 63, pp. 5534-5548, 2022.
- [24] P. Liu, Z. Zhu, H. Wang and T. Yan, "A novel image steganography Using chaotic map and visual model," in *International Conference on Intelligent Systems and Knowledge Engineering 2007*, Atlantis Press, 2007, pp. 1351-1355.
- [25] E. Elshazly, . S. A. Abdelwahab, R. Fikry, S. Elaraby, O. Zahran and M. El-Kordy, "FPGA implementation of robust image steganography technique based on least significant bit (LSB) in spatial domain," *International Journal of Computer Applications*, vol. 145, pp. 43-52, 2016.
- [26] X. Li and J. Wang, "A steganographic method based upon JPEG and particle swarm optimization algorithm," *Information Sciences*, vol. 177, no. 15, pp. 3099-3109, 2007.
- [27] V. Senthoran and L. Ranathunga, "DCT coefficient dependent quantization table modification steganographic algorithm," in *2014 First International Conference on Networks & Soft Computing (ICNSC2014)*, 2014.
- [28] S. M. Hameed and I. . A. Taqi, "A new RGB Image Encryption Based on DNA Encoding and Multi-chaotic Maps," in *New Trends in Information and Communications Technology Applications*, Baghdad, Iraq, Springer, 2018, pp. 69-85.