International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I9P220
Volume 70 Issue 9, 194-206, September 2022

Original Article

Secure Image Transmission Scheme based on DNA Sequences

Abhishek Sharma Padmanabhan[1], S. Sapna[2]

[1,2]*CHRIST (Deemed to be University), S.G. Palya, Bengaluru, Karnataka.*

[2]*Corresponding Author : sapnas59969@gmail.com*

Received: 09 June 2022 Revised: 02 September 2022 Accepted: 26 September 2022 Published: 30 September 2022

Abstract *- Cryptography and steganography are the most widely utilized and adopted fields of secure data communication. Data transfer can be secured using a combination of these methods. The data is transmitted from sender to receiver using cryptography, the most secure method. At the same time, steganography performs the information hiding in the form of video, image, or text within a cover image. The sensitive data is hidden, so it is not visible to the human eye. The data is stored and transferred more securely by adding DNA technology to the cryptography. It provides additional data security level and is most commonly employed to implement computation. This research developed a new method for combining cryptography with steganography. There are two phases to the proposed method: image encryption and hide phases and image extraction phases. Encryption is done by using the Signcryption algorithm. Four standard images were utilized as test material for the evaluation. Four factors are used to determine the performance of the proposed method as Peak signal-to-noise ratio (PSNR), Mean Square Error, Entropy, and Structural Similarity Index Measure (SSIM) for hiding and extracting the messages. The implementation is done in python. The proposed method achieves better performance when compared to the previously published works.*

Keywords *- Cryptography, steganography, DNA sequences, Data security, Performance evaluation, Ciphertext.*

1. Introduction

Digital information organization, processing, and preservation have all been transformed by information technology [1]. And the attack is also prevented by emphasizing the importance of information security and the steps that must be done. Information security is significant in ensuring appropriate levels of privacy, integrity, authenticity, and non-repudiation [2].

Data hiding techniques such as cryptography and steganography are employed in secret communication [3]. Cryptography is a data scrambling mechanism that prevents unauthorized users from decrypting a secret message without the usage of a secret key [4]. steganography is derived from the Greek word steganos, which means "hiding in plain sight" [5]. Anyone could determine that both parties use cryptography to communicate secretly [6]. Moreover, invalid recipients will not know that the cover medium contains secret data in steganography [7] [8]. The secret image security is strengthened by combining the two types of skills in this research. Three significant elements of advanced steganography systems are security, imperceptibility, payload, and robustness [9] [10].

To fulfill the goal of preserving information content, cryptography works by upsetting the information content and making it appear as random code [11]. The analysis of techniques to hide specific information within other publicly available data and then by transmitting public data, hidden information can be passed is known as information hiding technology [12] [13]. Information security technology based on cryptography and steganography are not mutually exclusive or competitive but complementary. The cryptography and information hiding techniques are combined in this research [14].

The substantial DNA and protein sequences have been generated by the Next Generation Sequencing (NGS) techniques in recent years [15] [16]. Effective analysis of these genetic sequences has strong demands. There are four different types of nucleotides in a DNA sequence: Adenine (A), Guanine (G), Thymine (T), and Cytosine (C) [17]. Digital signal processing techniques can identify intrinsic patterns and features in DNA sequence analysis by converting a symbolic sequence to a numerical sequence [18]. Steganography, encryption, Genome comparison, and compression require numerical representations of DNA sequences [34].

Due to DNA features such as parallel molecular computing, data storage, data transmission, and processing capacity, the data is encrypted and encoded using DNA cryptography with DNA computing techniques [20]. Other uses for DNA include cryptography, intrusion detection systems, and steganography.

The main contribution of the research is

- First, using the Signcryption algorithm, the input secret image is encrypted. After the encryption, the Ciphertext of the input image is obtained.
- Then the Ciphertext is converted into DNA sequences using dynamic DNA sequence; after that, the obtained DNA sequences are encoded (converted) into binary format (0 or 1) using the DNABIT algorithm
- These binary characters are embedded into the cover image by the Modified Least Significant Bit (LSB) technique and sent to the sender. On the receiver side, the decryption process is carried out to retrieve the secret image.
- Four standard images are used for our experiment, and the experiments are performed in the Python platform. It's employed to compare and contrast the proposed and existing methods. According to the experimental results, the proposed model outperforms the previous models.

Section 2 shows several related works that improve the secret-sharing systems of image-based steganography approaches. The proposed methodology and algorithms are presented in Section 3. The results of implementing the proposed secret sharing models are shown in Section 4. The conclusion is presented in the last section of the paper and recommends some areas for future research.

2. Related Works

Hureib et al. [21] investigated ways for encrypting and hiding secret information to enhance the security level of medical health data from being hacked. Image steganography and elliptic curve cryptography are used to accomplish this. ECC would be used to encrypt text in the first stage. The text would be hidden inside an image using steganography in the second stage. Elliptic curves over finite fields have an algebraic structure known as selecting ECC. It is thought of as a desirable option for public-key encryption.

A novel deep learning-based high-capacity image steganography algorithm is introduced by Duan et al. [22]. The secret image is transformed using the Discrete Cosine Transform (DCT). Then the Elliptic Curve Cryptography (ECC) is used to encrypt the image to improve the obtained image's anti-detection property. In this research, image steganography and full-size image extraction are performed using the SegNet Deep Neural Network, which includes a series of hiding and extraction networks.

For confidential data, an innovative security technique is proposed by Saxena et al. [23]; this technique has performed three processes. The wavelet transform-based image compression process is performed; first, it compresses confidential images while reducing their size. The symmetric key-based cryptography is performed second, encrypting the confidential image. The third method is steganography, which uses the least significant bit (LSB) to embed encrypted data inside a cover image.

Alibi et al. [24] introduced a new secure transmission technique, the image encryption is done by a new chaotic map algorithm, and image hiding is performed by the PPM (Pixel Pattern Mapping) algorithm in this research. The methodology uses a chaotic encryption method on the RGB planes of the image to be hidden before using a PPM-based image hiding method on the cover image.

A combination of steganography and cryptography is proposed by Rachmawanto et al. [25]. In this research, discrete cosine transform (DCT) is performed under steganography, and one-time pad or vernal cipher is performed under cryptography. The peak signal-to-noise ratio (PSNR) is used to determine the stego image quality, and the extraction of the decrypted message quality is determined by normalized cross-correlation (NCC).

Two encryption and hiding layer stages are proposed by Ahmed et al. [26]. First, the secret key (extract from MSB) and double XOR operations are used to encrypt the message in binary representation. Then the LSB technique hides the encrypted stream of bits into the cover image. A well-known evaluation measure, such as MSE, PSNR, Entropy, and histogram distribution, was generated to ensure the quality of the proposed technique.

A novel RGB shuffling algorithm is proposed by Rosalina et al. [33]. RGB Shuffling is used for encryption; it distorts the image by shuffling all RGB elements. Each pixel's RGB values in an image are shuffled by the RGB Shuffling method according to the user's password. The initial step in the RGB shuffle process is using an ASCII password to add an RGB element, inverting it, and shuffling.

3. Proposed Methodology

The performance of the cryptography security methods is improved by using the new DNA-based cryptography methods. Following studies in the field of DNA computing, DNA cryptography and information science were born. There are two phases to the proposed method: Image encryption and hiding and image extraction. The cryptography and steganography phases comprise the image encryption and hiding phase on the sender side. The schematic diagram for the proposed model is given in Fig. 1.

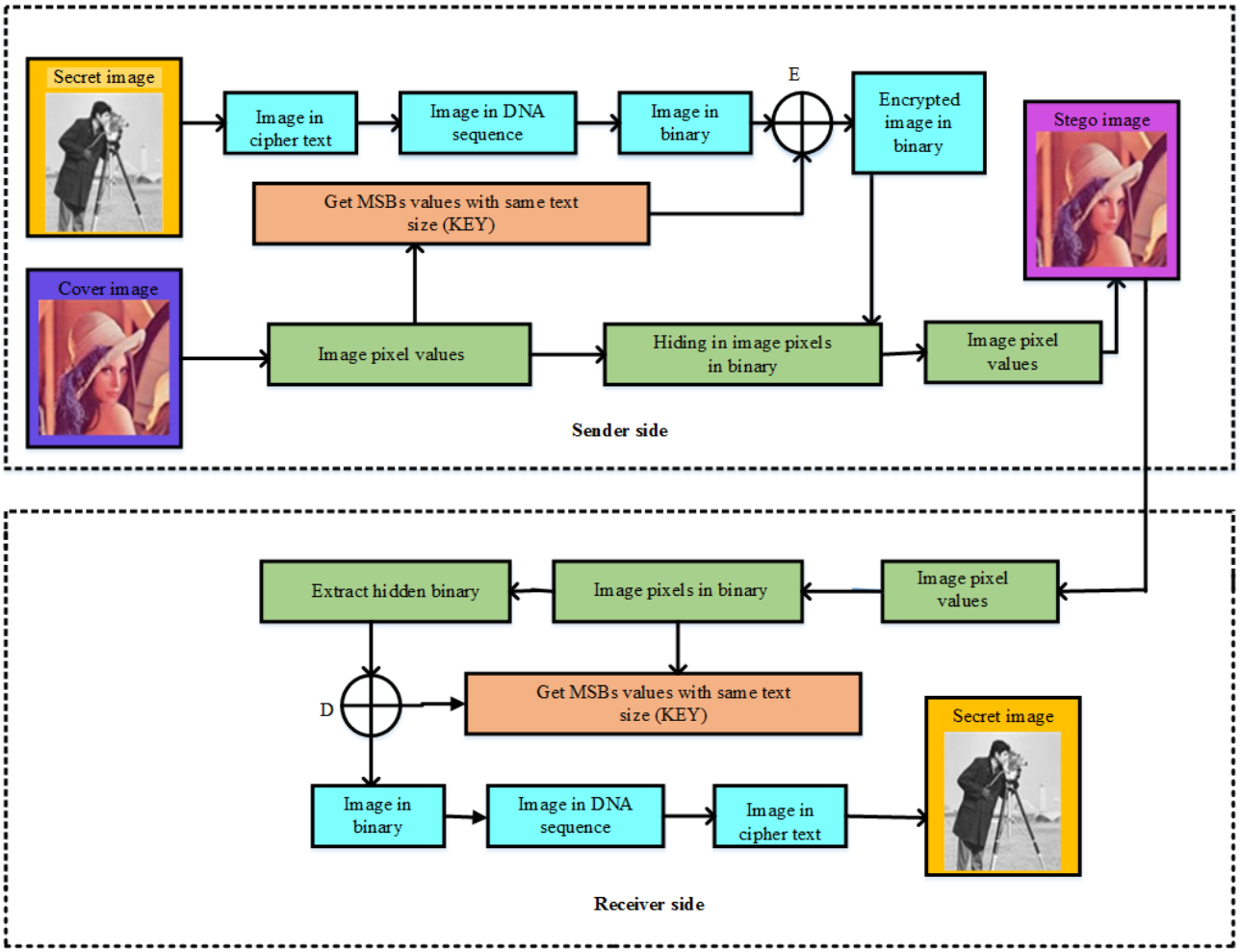


Fig. 1 The proposed DNA Crypto-Steganography model for secure image transmission

Signcryption is used to encrypt the secret input image on the sender side. The input image's Ciphertext is received after encryption. The encrypted text is then transformed into DNA sequences made up of characters A, T, G, and C. After that, the obtained DNA sequences are encoded (converted) into binary format (0 or 1). These binary characters are embedded into the cover image using a modified LSB approach and sent to the sender. On the receiver side, the decryption process is carried out to retrieve the secret image.

3.1. Problem Statement

Multiple existing approaches fail to protect against the vulnerabilities, and solutions typically occur as a result of ineffective design systems, procedures, and protocols that fail to report on the difficulty of access, even for legitimate users, at a critical time when making decisions based on cryptography that is strongly encrypted, authenticated, and digitally signed. The information could be hacked, altered, or even used by attackers in future attacks. We have designed a novel DNA Crypto-Steganography for secure image transmission as a perfect solution to these problems.

3.2. Image Encryption Using Signcryption Algorithm

Signcryption is a revolutionary public key cryptography technique that fulfills both the requirements of open key encryption and digital signature at a lower costIntegrity, Unforgeability, Non-repudiation, and confidentiality are all features of encryption. Additional features, like message confidentiality, secrecy, and public verifiability, are included in certain signcryption. The process of key generation, signcryption, and unsigncryption are presented in our proposed methodology. Due to signcryption with the optimal key selection, the message transmission of past encoded images is highly secured.

3.2.1. Key Generation

The public-key primitive is represented by Signcryption, which consists of two essential cryptographic mechanisms that secure honesty, privacy, and non-repudiation. It performs both encryption functions and digital signature at the same time. The prime numbers, hash functions, and keys are initialized during this step. We obtain the sender's and receiver's private and public keys for this step. The proposed

technique uses high-quality private keys through an optimization process to increase image security.
Initialization:

L_p Larger prime number
L_f Larger prime factor*I*
Integer of order L_f moduloL_p, selected at random from the $[1, \ldots L_p - 1]$ range.

Hash One-way hash function with a minimum output of 128 bits *D* Value, chosen randomly $[1, \ldots . L_f - 1]$

Sender key pair $((A_{k1}, B_{K1}))$

$$A_{k1} = Q^{A_{k1}} mod \quad L_P \tag{1}$$

Receiver key pairs $((A_{k2}, B_{k2}))$

$$B_{k2} = Q^{A_{k2}} mod \quad L_P \tag{2}$$

3.2.2. Optimal Key Selection Using Enhanced Monarch Butterfly Optimization (EMBO)

EMBO has been proven to have distinct advantages over other intelligence algorithms for evaluation and engineering applications and their difficulties. On some problems, however, EMBO may become trapped at local optima. To improve EMBO's searchability, this study combined the primary MBO technique with a self-adaptive strategy, butterfly adjustment, and migration operators.

The fundamental EMBO algorithm is as follows, the BAR (butterfly adjustment rate) is one of the essential factors. The BAR value in MBO is like p, which remains constant throughout the optimization process. As the optimization algorithm progresses from BAR0 to 1, the BAR value evolves self-adaptive.

$$BAR = BAR_0 + (1 - BAR_0) \times \frac{t}{t_{max}} \tag{3}$$

Where, the initial butterfly adjustment rate is BAR0, while the current and maximum generations are t andt_{max}, respectively.

Although BAR is constantly altering the entire MBO procedure, its value remains within the range of (BAR0, 1) from Eq. 12. Some conditions apply to this EMBO model, such as

- In space 1 and space 2, movement administrators from M.B. for each child Monarch Butterfly (M.B.) individual are distributed.
- To be specific, the monarch butterflies in spaces 1 and 2 represent the whole monarch butterfly population.
- The fittest individual, M.B., passes on to the people and the next generation. As a result. Administrators are unable to change them.
- As a result, a fit M.B. individual moves into the general population, the people, and the next generation. Managers have no power to change them.

The EMBO algorithm's major step is described below according to the preceding explanation. The initialization process, which includes the parameters and initial population, is first implemented, as previously explained. After that, the optimization technique is used to update the population of butterfly individuals. Using objective functions, the newly created butterfly individuals are then analyzed. The EMBO algorithm is implemented repeatedly until the specified standards are fulfilled. The ideal butterfly individual is finally decrypted to obtain the optimal key selection process. The population initialization procedure in algorithm three, fourth line encoding, is required to select the optimal keys for the EMBO algorithm. The initial population is created using this encoding. For converting the butterfly individual into the optimal key selection method, the line, 4 decoding process was used. The operations of decoding and encoding are opposed.

Algorithm EMBO Approach

Initialization. Fix the maximum generation $t1_{2_{0_{max}}}$ and *p* & the generation counter to 1.

Analysis of the population: Examine the individual butterflies in terms of their major functions.
while $t < t_{max}$**do**
  Analyze the butterfly population.
  Sort the population into SP1 and SP2 groups.
  for *i*=1 to NP_1 do.
    Create $y_{j,new}^{t+1}$ by implementing a migration operator.
  end
  Implement the new butterfly adjustment operator for all individuals in *SP2* to create $y_{j,new}^{t+1}$.
  Examine the butterfly population.
  t = t+1
end

The notations and descriptions of the algorithm are shown in below table

Notations	Descriptions
NP_1	The number of butterflies located at Land 1
NP_2	The number of butterflies located at Land 2
Peri	Migration period
p	Migration parameter
BAR	Butterfly adjustment rate

3.2.3. Signcryption with Optimal Keys

The signcryption algorithm is used to secure the image using the optimal keys. Signcryption is a primitive that uses a public key that performs both encryption and digital signature at the same time. The hash value is determined by using the public key of the receiver. This process's steps are outlined in detail in the section below.

Steps

Choose the values for the sender from the $(1 - L_f)$ range.

The receiver's optimal Public key (opt_Yk2) is used to determine the sender's hash function and outputs two 64-bit hashes from a 128-bit plain image.

$$H_o = hash(N_{K2}^{D} \, mod \quad P_{rn}) \tag{4}$$

Then, the data encryption is performed using the assistance of encryption (E) H_{01}. Thus we have obtained the cipher image; the cipher image is given by,

$$C_l = Enc\_H_{01}(image) \tag{5}$$

Then the hash of the data is achieved by using the one-way keyed hash function K.H.'s value. This results in the 128-bit hash assigned U.

$$U = L_p H_{02}(image) \tag{6}$$

Finally, Eq. 7 is used to calculate the value S.

$$S_I = \frac{D}{(D+D_{01H}) \, mod \quad L_f} \tag{7}$$

As a result, the sender stores three unique values U, S_1 and C_I, which are then sent to the receiver.

3.3. DNA Sequence conversion using Dynamic DNA Sequence

Converting Ciphertext to DNA sequences is the second step. A DNA sequence comprises four distinct nucleic acid bases: A, T, G, and C. Where Adenine is represented by 'A', Thymine is represented by 'T', 'C' to cytosine, and 'G' to Guanine. The several DNA sequence algorithm uses the predefined encoding rule. We utilize all eight rules in our proposed approach; this depends on choosing a random sequence. For example, if the Ciphertext contains the '$' symbol, the equal DNA character is 'CATT'. We obtain eight different codes for a single value, which presents a significant challenge to the attackers. The nucleotide sequence of DNA coding is represented by the nucleotide 'l' based on the complementary rules as follows

$$l_i \neq C(l_i) \neq C(C(l_i)) \neq C(C(C(l_i))) \tag{8}$$

$$l_i = C(C(C(l_i))) \tag{9}$$

Where l_i, $C(l_i)$ are complement each other. Table 1 is used to convert the Ciphertext into the DNA sequence.

Table 1. Encoding cipher text in DNA

Character	DNA	Character	DNA	Character	DNA
Z	TATA		GGGG	z	AGAA
Y	CTAC	,	CCCC	y	AAGA
X	TGTC	.	AAAA	x	TACA
W	CGAC	(	TGCG	w	TGCC
V	GAAC	)	GCAT	v	TGAG
U	CGAT	?	CTTA	u	AGAT
T	CTAA	=	AAGT	t	CTGA
S	CTTG	/	TCGT	s	CCTG
R	CTCT	*	TTTG	r	GAGA
Q	AAGC	-	AACT	q	GGTA
P	TTTT	+	ATTA	p	CTCC
O	GACC	&	AGCA	o	TTTC
N	TGTT	%	TCTG	n	GTTT
M	CTTT	$	CATT	m	GGAT
L	CATG	#	AAGG	l	CCTA
K	CCCG	@	CGTA	k	GTTG

J	GCAA	!	GTGT	j	TGAA
I	AATT	9	ACTG	i	TCTC
H	TCAT	8	AGCC	h	TACG
G	GTAC	7	CGCC	g	GACT
F	GCGT	6	TTAT	f	AATA
E	GCAG	5	CCGT	e	ATCG
D	ATAT	4	AGAG	d	CAAT
C	CTGG	3	CATC	c	ACTA
B	TTCA	2	TTGT	b	TAAC
A	ACGG	1	GGCC	a	AATG

3.4. Binary Conversion using DNABIT Algorithm

The DNABIT technique is then used to encode (convert) the retrieved DNA sequences into binary format (0 or 1). The nucleotide binary representation is used in the algorithm. First, the algorithm tries to determine adjacent similar or palindromes blocks and compresses them to a binary representation. The DNABIT compression algorithm has been extended in this algorithm. Each nucleotide's frequency is counted by the algorithm first. Then the nucleotides are divided into groups based on their frequency. After that, we classified four nucleotides and assigned them to four categories based on their frequencies: first, second, third, and fourth. The four nucleotides {A, C, G, T} will be encoded as follows:

A=00, C=01, G=10, T=11.

3.5. Image Embedding with Modified LSB Technique

The information is hidden by employing the modified LSB method in this research. This procedure will change the rightmost bit's value. Because the bit's value is so low, the final bit value that was changed did not significantly impact the expected file. The LSB algorithm replaces the bits in the carrier that aren't overly influential with bits in the secret data. The least significant bit (LSB) and most significant bit (MSB) are the two significant bits in a byte (1byte=8bits). The image will not change while using LSB.

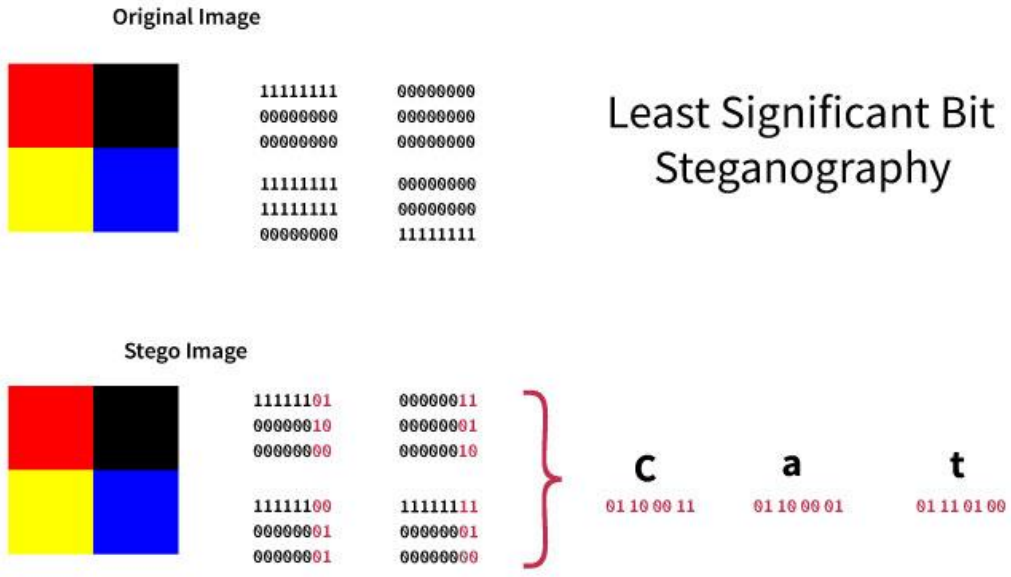


Fig. 2 Modified LSB data embedding in the cover image

Fig. 2 shows how the LSB approach embeds the data "cat" into the image pixels. The stego image and the cover image appear to be the same. The LSB approach processes data that has already been encrypted and converts it to binary format. Using only one LSB, each RGB element in an image can hold the text binary if the carrier is an image.

The cover image and secret image have the same element of RGB when the original input image is hidden in the cover image. But both the cover and secret image sizes are different. The secret image's RGB element of each bit is stored using four LSB, and the secret image will require a cover image twice the secret image size to contain the RGB elements' bits.

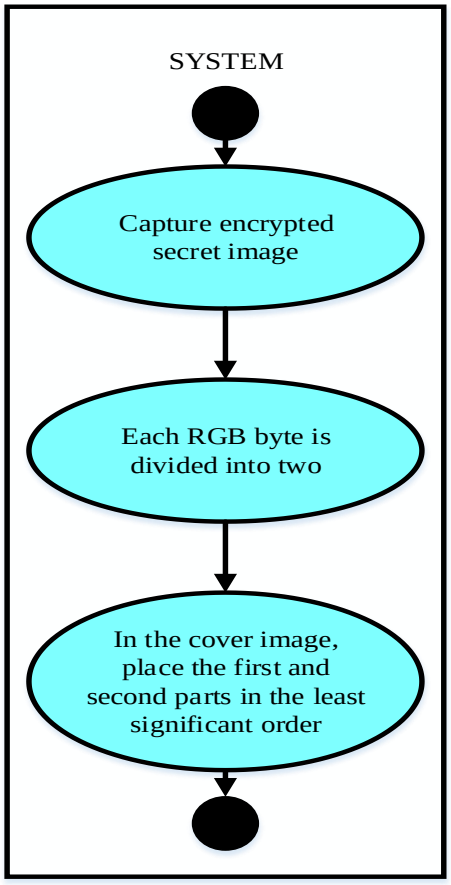


Fig. 3 Modified Least Significant Bit Process

The first and second bits of each RGB element of the secret image is separated when the sender is an image. The one-pixel element of RGB in the secret image will be carried by two pixels in the cover image. The rest of the pixel is equal to the original pixel of the cover image when the pixel in the cover image will be more than sufficient for preserving the secret image's RGB element. The cover image must carry the secret image's size. It is saved in the cover image's last 8 pixels. Assume the secret image's maximum width and height are 65535, or 1111111111111111 in binary. Fig. 3 depicts the LSB method's process. In the cover image, the process is used for changing and storing the bit per element of RGB in each pixel of the encrypted secret image.

3.5.1. Data Inserting Algorithm

Step 1: Choose specific pixels of the original image where data should be inserted.

Step 2: Get the character we want to maintain in the image from the message and convert it to binary.

Step 3: The data security is achieved by some image pixels' bytes must be left.

Step 4: LSBs from the original image should be replaced with LSBs from the message's binary format.

Step 5: Repeat until the entire message has been encoded into the image.

Step 6: Add something here to signify that the message is finished.

Step 7: The image that has been encoded will be obtained.

Step 8: Finish

3.5.2. Data Extraction

The secret image is retrieved by using the decryption process on the receiver side. The hidden message extraction is as follows:

- From the cover image, the Ciphertext can be extracted
- Binary reversal depends on a specific key.
- Transform DNA sequences from binary, 00=A, 01=C, 10=G, and 11=T are the possible values.
- Convert Ciphertext from DNA sequences with the help of Table 1.
- The image is decrypted by using the designcryption algorithm.

4. Results and Discussions

The implementations and experimental results of the proposed digital image embedding and extraction technique are discussed in this section. Python was used to implement the proposed approach. The proposed approach has been tested using data from the Internet. We used images that are "512×512" in size and are publicly accessible. Four standard secret images are considered with different cover images for the test analysis. The performance evaluation is performed by using four factors such as PSNR, MSE, entropy, and SSIM

4.1. Performance Metrics

- The analysis of The PSNR factor is used to find the relationship between the secret image (x) and stego image(y). The following equation can be used to compute PSNR.

$$PSNR = 10\,log_{10}\left(\frac{Max((n,m))^2}{MSE}\right) \quad (10)$$

$$MSE = \frac{1}{P*Q}\sum_{n=1}^{l}\sum_{m=1}^{W}[x(n,m) - y(n,m)]^2 \quad (11)$$

Where the image's sizes are W and L (width and length), and MSE refers to the difference in mean square error between 2 images. When the PSNR measurement is maximum, it indicates that the imperceptibility was better and shows that the two images' similarities are high.

- The similarity between the cover and stego images is measured using SSIM. The SSIM values range from 0 to 1. When the result is larger, SSIM is better. It can be calculated as a formula,

$$SSIM = \frac{(2\mu_s+C_1)(2\sigma_{cs}+C_2)}{(\mu_c^2+\mu_s^2+C_1)(\sigma_c^2+\sigma_s^2+C_2)} \quad (12)$$

Where C_1 and C_2 are two constants. The cover image is depicted by C, and the stego image is represented by S. Furthermore, σ, μ are the standard deviation and the average, respectively.

- Another measure, known as the Entropy (Average content of the information) parameter, is also used for the analysis of cover images and stego-image. The proportions of the details are measured with this test, which is commonly expressed in bits in units. The entropy calculation equation is described below:

$$Entropy = \sum_{i=0}^{G-1} p(i)\, log\, p\,(i) \quad (13)$$

Where the probability density function is represented $p(i)$ at the intensity level of a particular image, the total number of grey levels in the image is represented by l and G.

4.2. Experimental Results

Image encryption using signcryption is the first step; this is the most basic encryption technique and the easiest cipher replacement algorithm. The process depends on a defined position number in which each element of a specified text is replaced with another element. Four standard color test images with distinct cover images, each sized 512x512 pixels, were employed to evaluate the experiment. The images used for our experiment are shown in Fig. 4.

Secret input images **Cover images**

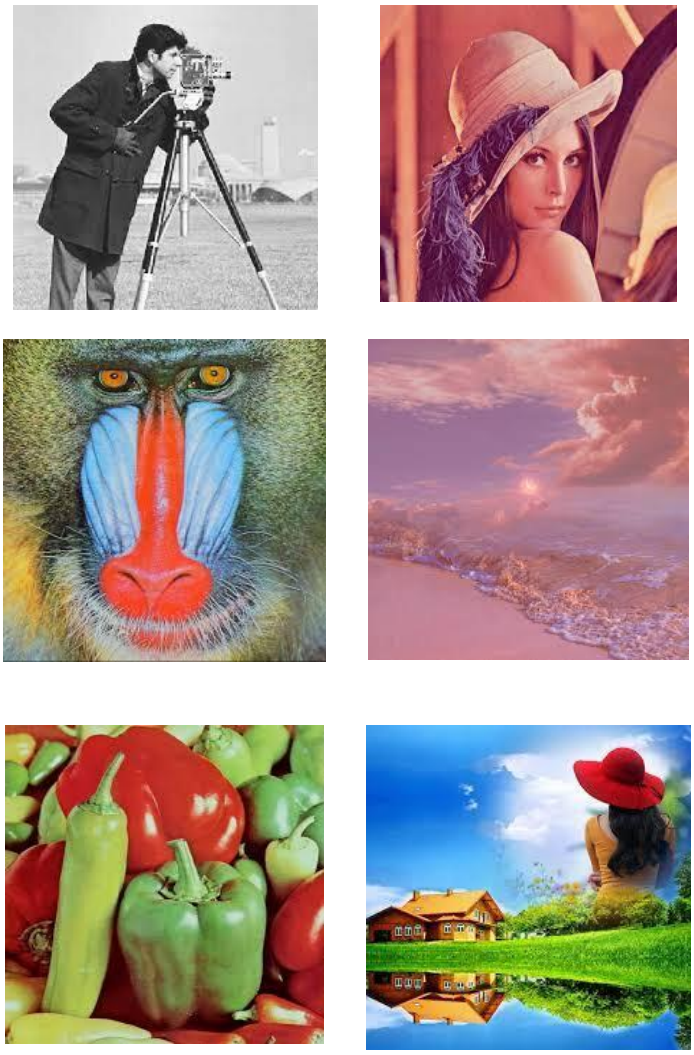


Fig. 4 Secret input images and cover images for our experiment analysis

After encryption, the obtained Cipher text = 11111111.

The conversion of Ciphertext to DNA sequences is the second stage; obtained DNA sequence is "ATAGATAGATAGATAGATAGATAGATAGATAG".

The sequences of DNA are then encoded (transformed) into binary format (0 or 1); the binary sequence for the proposed system is

0011000100110001001100010011000100110001001100010011000100110001

The binary data is hidden in the cover image in the steganography phase and is then given the final step. The first image pixel (0, 0) stores the character length in the developed steganography approach and then finds the random points (random x and y positions). For storing the ciphertext character's first binary value (either 0 or 1), choose a color component at random from R (red), G (green), or B (blue) after choosing the random point. For each binary value, then these steps are repeated. Fig. 5 depicts the stego images after data has been inserted with different secret images.

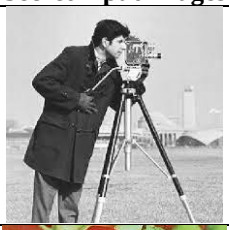
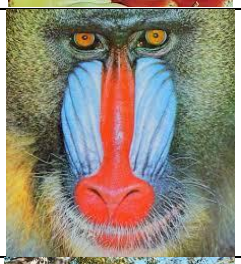
Fig. 5 Stego image (Post-embedding)

After applying the decryption process on the receiver side, the secret input image is obtained.

5. Performance Results

The experimental results of PSNR, MSE, Entropy, and SSIM are shown in Table 2 for hiding four different secret images with each of the four different cover images. We have obtained a more efficient performance of both PSNR and MSE after analyzing and extracting the image. We have achieved the results of PSNR greater than 50 dB, considered an acceptable performance, and acquired the maximum entropy value, improving the image's quality and information. In terms of secret image extraction, the proposed approach performs better based on the performance of SSIM.

Table 2. Performance analysis of the proposed scheme

Secret input images	PSNR	MSE	Entropy	SSIM
	79.15	0.24	8.69	0.89
	78.15	0.31	8.05	0.850
	76.95	0.40	7.88	0.82
	77.41	0.36	8.68	0.856

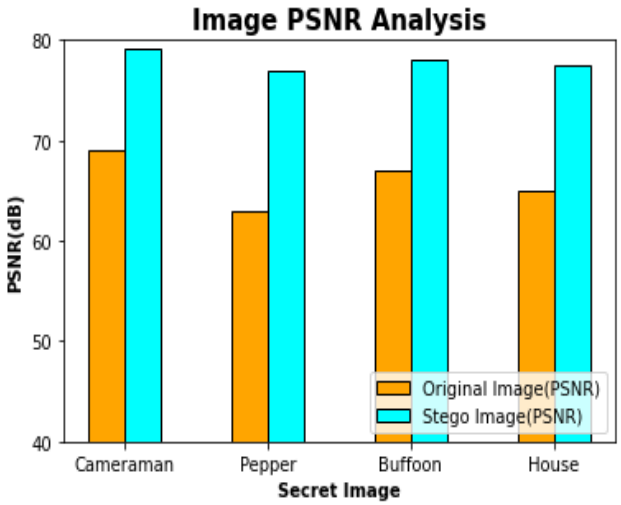


Fig. 6 PSNR performance of cover image and stego image

The proposed model's PSNR performance in the image (secret data) embedding is shown in Fig. 6. The image embedding is improved, and even the PSNR is optimized using the modified LSB in our proposed method. Either the proposed system achieves near original PSNR or significantly enhances image quality when evaluating PSNR performance, resulting in a higher PSNR value.

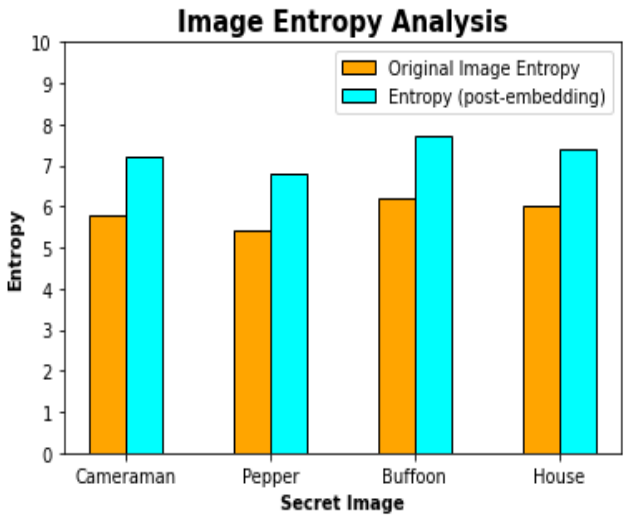


Fig. 7 Entropy performance of cover image and stego image

The observed entropy spike is insignificant from analyzing the results from Fig. 7, resulting in the image quality being unchanged. It ensures the encrypted images' suitability for essential healthcare (telemedicine) applications or significant data communication. As a result, the research findings indicate that the proposed model is suitable for certain purposes like encryption of large-scale data and secure communication.

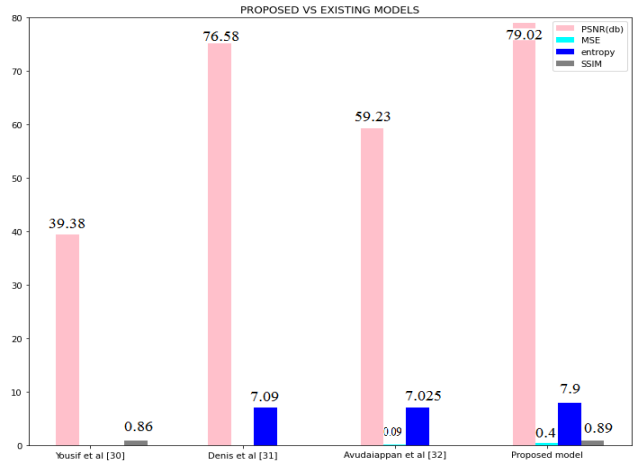


Fig. 8 Comparison results

The performance of the proposed system is more efficient than the state-of-the-art systems in secure image transmission. Fig. 8 shows the comparative results, demonstrating that the proposed approach produces significantly better results. In terms of data security, the proposed method outperformed existing methods.

The stego image produced by the proposed method is clear, and the visual quality of all images is enhanced with the maximum PSNR rate. Taking the suggested DNA-based Crypto-Steganography model and its simulation-based performance into consideration, it can be observed that the proposed system achieves maximum performance, making it more suitable for secure data communication throughout the globe.

6. Conclusion

We established in this research that crypto-steganography could provide two levels of security. Using this methodology, there is no third-party interruption since no one will know that data is embedded in the image because no noise will be formed in the cover image. It ensures that information is kept safe and secure. Multiple algorithms are being developed to solve the limitations in prior algorithms and improve the data security communicated over the Internet. Although several message detection techniques are being developed at the same time, the analysis does not ensure the retrieval of all information. These steps involve using signcryption for image encryption, converting the Ciphertext to DNA sequences, converting the DNA character to binary, shifting binary using a specific key, and hiding the binary in the cover image. The data is embedded in cover image pixels using a modified LSB algorithm. Moreover, the secret image is hidden in binary using the DNABIT conversion algorithm and transmitted to ensure data security. As a result, the cover image and the stego image will be identical.

For hiding and extracting images, the estimated MSE, PSNR, Entropy, and SSIM are used to evaluate the performance. And the MSE and PSNR values obtained are 0.52 and 79.02, respectively. The Entropy and SSIM results are 8.62 and 0.89 for hiding and extracting images. Even when the stego image is exposed to different attacks, the proposed technique provides imperceptibility and robustness, according to experimental and simulated data. To improve the security level of data, we will evaluate medical and identification images in future work with the help of revolutionary framework optimization.

Authors' Contributions

The corresponding author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation.

Ethics Approval

This material is the author's original work, which has not been previously published

Elsewhere. The paper reflects the author's own research and analysis truthfully and completely.

References

[1] Alrikabi, H.T. and Hazim, H.T., "Enhanced Data Security of Communication System Using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, 2015.

[2] Sujitha, B., Parvathy, V.S., Lydia, E.L., Rani, P., Polkowski, Z. and Shankar, K, "Optimal Deep Learning-Based Image Compression Technique for Data Transmission on Industrial Internet of Things Applications," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, pp. E3976, 2021.

[3] El-Khamy, S.E., Korany, N.O. and Mohamed, A.G, "A New Fuzzy-DNA Image Encryption and Steganography Technique," *IEEE Access*, vol. 8, pp. 148935-148951.

[4] Shankar, K., Elhoseny, M., Kumar, R.S., Lakshmanaprabu, S.K. and Yuan, X, "Secret Image Sharing Scheme With Encrypted Shadow Images Using Optimal Homomorphic Encryption Technique," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 5, pp. 1821-1833, 2020.

[5] Shankar, K., Elhoseny, M., Perumal, E., Ilayaraja, M. and Sathesh Kumar, K, "An Efficient Image Encryption Scheme Based on Signcryption Technique With Adaptive Elephant Herding Optimization," *In Cybersecurity and Secure Information Systems* , Springer, Cham, pp. 31-42, 2019.

[6] Gutub, A. and Al-Ghamdi, M, "Hiding Shares By Multimedia Image Steganography for Optimized Counting-Based Secret Sharing," *Multimedia Tools and Applications*, vol. 79, no. 11, pp. 7951-7985, 2020.

[7] Voleti, L., Balajee, R.M., Vallepu, S.K., Bayoju, K. and Srinivas, D, March, "A Secure Image Steganography Using Improved LSB Technique and Vigenere Cipher Algorithm," *In 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)* , IEEE, pp. 1005-1010, 2021.

[8] Nunna, K.C. and Marapareddy, R, March, "Secure Data Transfer Through Internet Using Cryptography and Image Steganography" *In 2020 Southeastcon* , IEEE, vol. 2, pp. 1-5, 2020.

[9] Ambika, Biradar, R.L. and Burkpalli, V, "Encryption-Based Steganography of Images By Multiobjective Whale Optimal Pixel Selection," *International Journal of Computers and Applications*, pp. 1-10, 2019.

[10] Dhevanandhini, G. and Yamuna, G, "An Efficient Approach for Secure Video Watermarking Through Compression Standard: A Signcryption and H. 264 Paradigm," *Annals of the Romanian Society for Cell Biology*, pp. 16610-16620, 2021.

[11] Ullah, S., Li, X.Y. and Lan, Z, "A Novel Trusted Third Party Based Signcryption Scheme," *Multimedia Tools and Applications*, vol. 79, no. 31, pp. 22749-22769, 2020.

[12] Islam, M.R., Tanni, T.R., Parvin, S., Sultana, M.J. and Siddiqa, A, "A Modified LSB Image Steganography Method Using Filtering Algorithm and Stream of Password," *Information Security Journal: A Global Perspective*, vol. 30, no. 6, pp. 359-370, 2021.

[13] Hashim, M.M., Rahim, M.S.M., Johi, F.A., Taha, M.S. and Hamad, H.S, "Performance Evaluation Measurement of Image Steganography Techniques with Analysis of LSB Based on Variation Image Formats," *International Journal of Engineering & Technology*, vol. 7, no. 4, pp. 3505-3514, 2018.

[14] Selvi, S., Gobi, M., Kanchana, M. and Mary, S.F, July, "Hyper Elliptic Curve Cryptography in Multi Cloud-Security Using DNA (Genetic) Techniques," *In 2017 International Conference on Computing Methodologies and Communication (ICCMC) , IEEE*, pp. 934-939, 2017.

[15] Bala, B.K. and Kumar, A.B, "The Combination of Steganography and Cryptography for Medical Image Applications," *Biomedical and Pharmacology Journal*, vol. 10, no. 4, pp. 1793-1797, 2017.

[16] Fang, D. and Sun, S, "A New Scheme for Image Steganography Based on Hyperchaotic Map and DNA Sequence," *Journal of Information Hiding Multimedia* Signal Process., vol. 9, no. 2, pp. 392-399, 2018.

[17] Khari, M., Garg, A.K., Gandomi, A.H., Gupta, R., Patan, R. and Balusamy, B, "Securing Data in Internet of Things (Iot) Using Cryptography and Steganography Techniques," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 73-80, 2019.

[18] Elmasry, W, "New LSB-Based Colour Image Steganography Method to Enhance the Efficiency in Payload Capacity, Security and Integrity Check," *Sādhanā,* vol. 43, no. 5, pp. 1-14, 2018.

[19] Olu Osaronwolu, Matthias Daniel, V. I. E Anireh, "A Secured Deduplication of Encrypted Data Over an Attribute-Based Cloud Storage," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 7, pp. 77-83, 2020. Crossref, https://doi.org/10.14445/23488387/IJCSE-V7I7P113.

[20] Kassim, S., Hamiche, H., Djennoune, S. and Bettayeb, M, " A Novel Secure Image Transmission Scheme Based on Synchronization of Fractional-Order Discrete-Time Hyperchaotic Systems," *Nonlinear Dynamics*, vol. 88, no. 4, pp. 2473-2489, 2017.

[21] Hureib, E.S. and Gutub, A.A, "Enhancing Medical Data Security Via Combining Elliptic Curve Cryptography and Image Steganography," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 20, no. 8, pp. 1-8, 2020.

[22] Duan, X., Guo, D., Liu, N., Li, B., Gou, M. and Qin, C, "A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network," *IEEE Access*, vol. 8, pp. 25777-25788, 2020.

[23] Saxena, A.K., Sinha, S. and Shukla, P, "Design and Development of Image Security Technique by Using Cryptography and Steganography: A Combine Approach*," International Journal of Image, Graphics and Signal Processing*, vol. 10, no. 4, pp. 13, 2018.

[24] Alzubi, J.A., Alzubi, O.A., Suseendran, G. and Akila, D, "A Novel Chaotic Map Encryption Methodology for Image Cryptography and Secret Communication With Steganography," *International Journal Recent Technology Engineering*, vol. 8, no. 1C2, pp. 1122-1128, 2019.

[25] Rachmawanto, E.H. and Sari, C.A, "Secure Image Steganography Algorithm Based on Dct With Otp Encryption," *Journal of Applied Intelligent System*, vol. 2, no. 1, pp. 1-11, 2017.

[26] Ahmed, A. and Ahmed, A, "A Secure Image Steganography Using LSB and Double XOR Operations," *International Journal of Computer Science and Network Security*, vol. 20, no. 5, pp. 139-144, 2020.

[27] Shivam Saxena, "Introduction to DNA Computing," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 2, pp. 19-21, 2020. Crossref, https://doi.org/10.14445/23488387/IJCSE-V7I2P102 .

[28] Dash, S., Das, M.N. and Das, M, "Secured Image Transmission Through Region-Based Steganography Using Chaotic Encryption," *In Computational Intelligence in Data Mining* , Springer, Singapore, pp. 535-545, 2019.

[29] Ramasamy, J. and Kumaresan, J.S, "Image Encryption and Cluster-Based Framework for Secured Image Transmission in Wireless Sensor Networks," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1355-1368, 2020.

[30] Yousif, A.J, "Image Steganography Based on Wavelet Transform and Color Space Approach," *Diyala Journal of Engineering Sciences*, vol. 13, no. 3, pp. 23-34, 2020.

[31] Denis, R. and Madhubala, P, "Evolutionary Computing Assisted Visually-Imperceptible Hybrid Cryptography and Steganography Model for Secure Data Communication Over Cloud Environment," *International Journal of Computer Networks and Applications (IJCNA)*, vol. 7, no. 6, pp. 208-230, 2020.

[32] Avudaiappan, T., Balasubramanian, R., Pandiyan, S.S., Saravanan, M., Lakshmanaprabu, S.K. and Shankar, K, "Medical Image Security Using Dual Encryption With Oppositional Based Optimization Algorithm," *Journal of Medical Systems*, vol. 42, no. 11, pp. 1-11, 2018.

[33] Rosalina, N.H, "An Approach of Securing Data Using Combined Cryptography and Steganography," *International Journal of Mathematical Sciences and Computing (IJMSC)*, vol. 6, no.1 pp. 1-9, 2020.

[34] Guillén-Fernández, O., Meléndez-Cano, A., Tlelo-Cuautle, E., Núñez-Pérez, J.C. and Rangel-Magdaleno, J.D.J, "On the Synchronization Techniques of Chaotic Oscillators and Their FPGA-Based Implementation for Secure Image Transmission," *Plos One*, vol. 14, no. 2, pp. E0209618, 2019.