

Color Image Steganography Based on Artificial DNA Computing

Najat H. Qasim¹, Sahera A. S. Almola²

E-mail: najat.qasim@uobasrah.edu.iq, sahera.sead@uobasrah.edu.iq

¹Department of English language, College of Arts, University of Basrah, Iraq,

² Department of information system, College of Computer sciences and Information Technology, University of Basrah, Iraq

Keywords: steganography, DNA, image, LSB, encoding, security

Received: March 30, 2023

Modern genetic engineering developments have made it possible for artificial DNA strands to be included in living cells of creatures. Many methods of artificial insertion have been developed using DNA, which has excellent data storage capacity. Most of these techniques are used to encode text data, while there has been little research on encoding other types of media. Methods for encoding images have very little studied, and most of them are dedicated to black-and-white images. The proposed method focuses on encoding a secret color image and then embedding it in another color image, this comprises two levels of security. The first level is provided by converting binary color images into DNA sequences. A second level is provided by embedding the bits of DNA sequence into LSBs of the cover image to generate the stego image. Extraction process is in the reverse procedure. The proposed method is significantly efficient, according to the experimental results.

Povzetek: Sodobni razvoj genskega inženiringa omogoča vključitev umetnih DNA nizov v žive celice bitij. Metoda predlaga podobno kodiranje skrivne barvne slike in njeno vdelavo v drugo barvno sliko, kar zagotavlja dve stopnji varnosti.

1 Introduction

The emergence of the big data era has resulted in the everyday generation of various digital images that are highly informational. As a result, the security concerns with digital images have gotten much worse. However, extensive security flaws, in addition to, high correlation between pixel points and their large data capacity then, traditional data encryption methods are not appropriate for image encryption. As a result, scientists started looking for novel approaches to image encryption. Cause to DNA's special properties, great parallelism, and high information density, DNA coding is a popular topic in the images encryption field. The use of DNA computing in cryptography and steganography has been identified as a potential technology that could provide a new hope for unbreakable algorithms. The combination of encryption and steganography can provide a high level of security and protect the privacy of information. Steganography is the science of concealing data in a cover, which can be audio, text, image, or video.

In our work, we present a new method that combines DNA encryption and LSBs steganography. Where, the color image encrypts and compressed before hiding them in the cover image.

The rest of this research arranges as: Section 2 present the related works. Section 3 explains the DNA encoding rule. We explain the suggested algorithm in section 4. We describe research results and analyses in section 5. The discussion is in section 6. We present the conclusions of this work in section 7. The future work introduce in section 8.

2 Related works

Researchers have improved DNA encryption techniques to increase the performance of cryptography algorithms. They apply DNA encryption in many articles on data encryption. While compared with a conventional system, DNA is perfect for developing an efficient and secure cryptosystem due to its enormous information storage capacity, powerful parallel processing capability, and low energy usage. For realizing image coding, current studies use DNA encryption methods, a DNA encryption procedure (addition, subtraction, complement, XOR, etc.), or a combination of several coding operations. In other words, no existing study explains why a specific DNA encryption method (static or dynamic), the DNA encryption process, or a combination of several encryption methods was chosen to achieve image encryption.

Today, scientists are very interested in experimenting with DNA to improve encryption techniques and offer a more efficient method for encrypting color images.

3 DNA encoding rule

Adleman originally applied DNA computing in the field of encryption in 1994, ushering in a new stage for data processing. DNA encryption is a novel field that is currently at the forefront of global research in cryptography. DNA molecules are highly energy-efficient, have a high storage density, and can run in enormous parallel. As a result, DNA-based image encryption techniques have certain features that other

cryptography techniques do not have. The technique of mapping the nucleotide sequence that makes up a DNA strand is known as DNA sequencing. Adenine (A), thymine (T), guanine (G), and cytosine (C) are the four nucleic acid bases that combine to create DNA sequence components and the building blocks of genetic coding. A DNA sequence has the form of a binary string, and every two nucleic acid bases on either side of the string are complementary, according to the criteria that A and T are complementary to each other as well as G and C. Only eight possible DNA coding combinations are suitable for the complementarity principle. Table 2 includes a list of these. Where, the binary numbers 00, 01, 10, and 11 are complementary and represent the four deoxynucleotides A, C, G, and T respectively. We are percipient that every pixel in a digital image can be represented by an 8-Bit binary value. Then each pixel in a digital image can be represented by a string of nucleotides. So, sequence of nucleotides corresponds to the binary number (11100100) according to the preceding principles (TGCA).

Table 1: Represent the state-of-the-art about DNA encryption for color images

Year	References	Method	Solved problem
2015	[34]	A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps.	Suggested a novel color image encryption method based on DNA sequence and a number of improved one-dimensional chaotic maps
2016	[35]	Color image encryption scheme using CML and DNA sequence operations	Presented a technique for color image encryption using chaotic systems and DNA sequence. The pixels matrix was created by CML (coupled map lattice) using three components for the color plain image. the pixels matrix was then confused
2017	[36]	CNN-based color image encryption algorithm using DNA sequence operations	Developed a special encryption method based on cellular neural networks (CNN) and DNA sequence. The initial color image was split into three matrices (R, G, and B), and these matrices were afterwards transformed into DNA matrices.
2018	[6]	A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2	Presented a color image encryption method that modifies the chaotic system's begin conditions and control parameters using the SHA-256 hash algorithm. The Piecewise Linear Chaotic Map (PWLCM) was used to arrange three-color image channels into a chaotic sequence.
2019	[39]	An RGB image cipher using chaotic systems, 15-puzzle problem and DNA computing	Proposed a special RGB image encryption based on DNA computing. The color image was split into three segments of Red, green, and blue. After that, the grayscale images were merged to create a single grayscale image. Many blocks have been split from this one grayscale image. On this grayscale image, a block level permutation (BLP) was suggested using the 15-puzzle problem
2020	[37]	Color image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set	Presented encryption method based DNA sequence and chaotic map. Where, on each of the three channels of the color image, the Arnold map was separately applied to increase security.
2021	[40]	Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption	A DNA-based RGB image encryption and an updated genetic algorithm, in addition to a matrix semi-tensor product (STP), were suggested. The phase of the encryption process were, DNA encoding, crossover, mutation, and DNA decoding.
2022	[43]	Encryption of Color Image Based on DNA Strand and Exponential Factor	developed a novel approach for encrypting 2D and 3D color images in multiple levels of security based on DNA computing

Table 2: DNA coding Rule.

Rule	1	2	3	4	5	6	7	8
00	A	A	T	T	G	G	C	C
01	C	G	G	C	A	T	A	T
10	G	C	C	G	T	A	T	A
11	T	T	A	A	C	C	G	G

4 Suggested method

Steganography is the science of conveying a message concealed inside a cover medium. So that only the sender and the intended recipient are aware of its presence. Steganography strives to hide the existence of a message, while cryptography only seeks to render a message unreadable. The suggested method consists of two levels of security: the first level is the encryption stage, which constructs DNA in the encryption mechanisms, and the second is the hiding stage. The following is an explanation of each level:

4.1 The DNA encryption algorithm

At this stage first, we secure the color image using the DNA coding rule. Second, we compress the binary image and then hide it in the least significant bit of the host image. The encryption algorithm summarizes in the following steps:

1. Enter colored secret image.
 2. Specifies the secret image size to 256×256.
 3. Partition the secret image into three layers (Red, Green, and Blue).
 4. Using the DNA method to encode the secret image as follows:
 - A. Convert the secret image data into binaries while working on the first (red) layer.
 - B. In the first layer, convert four LSB of each byte to the decimal number d and then calculate the remainder as $R = \text{mod}(d, 8)$. Example: $R = \text{mod}(15, 8) = 7$.
 - C. The output of the prior step ranges from 0 to 7, representing the base number used for encryption, according to Table 2. Example: 01111111 = AGGG (using Rule 7).
 - D. Every 2 bits in the current byte replace with its corresponding symbol in Table 2.
 - E. Following the repetition of steps (B, C, and D) on all the red layer's bytes, we repeat step 4 on each of the green and blue layers. So that we can acquire RDNA, GDNA, and BDNA, respectively, and their sizes are (4, N, M).
 5. Converting DNA codes into binary based on the Davis method, we give ascending order to the bases by Davis. These results are $C = 1$, $T = 2$, $A = 3$, and $G = 4$. This approach reduces the binary digits of the bit-mapped image into fewer DNA base codes, with each base indicating how many times each code is repeated. This method is widely used in data compression.
- The following procedures are used to produce the symbols of the coding table. Which are formed upon implementation and have a separate coding table for each secret image.

- Analyze the output of the preceding coding step to determine how many times each DNA symbol is repeated. We use the following illustration to explain this process. Table 3 will be the result of this procedure.
- The representations of Table 3 arrange in descending order, so the results presented in Table 4 as :
- The four symbols ((T, C, A, and G)) are each assigned a code since the most common symbol uses the fewest binaries. Where fewer binaries will be required to reduce the DNA codes. As we see in Table 5. and Table 9.

Table 3: Analyze the output of DNA Encoding

Representations	Base
50	T
30	C
20	A
40	G

Table 4: Descending order of Table 3

Representations	Base
50	T
40	G
30	C
20	A

Table 5: DNA Encoding scheme based Davis

Bit sequence	Base
1 or 0	T
11 or 00	G
111 or 000	C
1111 or 0000	A

Then, the current DNA code will replace with a few zeros or ones. Depending on Table 5, as well as depending on the binary value of the symbol that accepted it. For example, TGATC= 10011110111.

4.2 The steganography algorithm

This level applies the least significant bits (LSB) technique to hiding the binary codes of a secret color image in the LSB of a host image. The hiding algorithm summarizes in the following steps:

1. Select the colored host image as input.
2. Specify the host image size to 300×300.
3. Partition the host image into three layers (Red, Green, and Blue).
4. Transform the host image data into binaries and work on the first (red) layer.
5. Load sequentially bits from the first layer of the encrypted image into the third least significant bit of the host image. Where the

first and second LSB of the stego image will be changing as follows:

- **Case 1:** If the third LSB of the host image is zero and the current bit of the encrypted image is one. So, the values of the (1st and 2nd) least significant bits of the stego image will become zeros, as demonstrated the example in figure 1.(a) .
 - **Case 2:** If the third LSB of the host image is one and the current bit of the encrypted image is zero. So, the values of the (1st and 2nd) least significant bits of the stego image will become ones, as demonstrated the example in the figure 1.(b).
 - **Case 3:** In the case of the absence of either of the two mentioned conditions, the current bit of the encrypted image will only include the third least significant bit of the stego image without any other changing.
6. Apply steps (4 and 5) over two others layers (green and blue).
 7. Obtain the stego image.

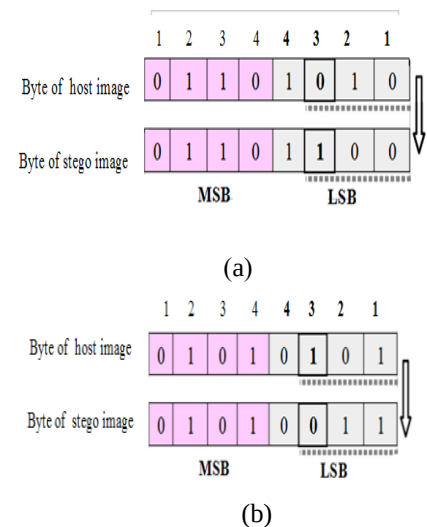


Figure 1: Examples for hiding the binary codes of a secret image in the LSB of a host image.

4.3 The recovered algorithm

This algorithm represents the reverse of the second level of security where the stego image is used to generate the encrypted image.

4.4 The decryption algorithm

We typically use a decryption algorithm, which is the opposite of an encryption algorithm. This algorithm is the inverse of the first level of security. The encrypted image and the secret keys are required to restore the original image.

5 Experimental results and analysis

We carried many experiments results to present the performance and validity of the suggested method in two levels of security. The first test; starts with the results that evaluate the encryption/decryption processes on the different images. We test three cover images (Lena, Baboon, and Pepper) to reveal the power of DNA encryption and the hiding algorithm. To verify the security and performance of the algorithm, we must test and evaluate this algorithm based on the properties of the stego image. A good algorithm would produce a stego image that meets the evaluation metrics requirements. We can classify metrics into two categories. The first group evaluates the efficiency of the substitution process, which includes histograms, entropy coefficients, and correlation. The second group evaluates the approach's ability to propagate the original image. That includes MSE, PSNR, NPCR, and UACI. The suggested method is compared to the performance of competing methods based on a variety of parameters. The results showed that the suggested method is superior to other methods in terms of safety. Correlation comparison results (color images calculated by averaging the values of the horizontal, vertical, diagonal, red, green, and blue components) and information entropy comparison these results are presented in Table 7.

5.1 Mean Square Error (MSE) Analysis

The amount of distortion in the image that indicates the variance between the cover and a stego image is measured using the MSE. The quality of the image is good if the MSE value is low.

$$MSE = \frac{[I_1(M,N) - I_2(M,N)]^2}{M \times N} \quad (1)$$

$I_1(M, N)$ denotes the host image pixel in the (M, N) point, where M and N define the rows and columns numbers in the host image, and $I_2(M, N)$ denotes the stego image pixel in the (M, N) location. Table 6 presents results obtained from the suggested method; as can be seen, the MSE values are low, indicating very acceptable stego image quality.

5.2 Peak Signal to noise ratio (PSNR) analysis

The Peak Signal to Noise Ratio is a metric used to calculate the decibel level of imperceptibility. It compares the original host images' and stego images' quality. Refers to a tiny difference between a host and stego images when the PSNR value is high. The algorithms used in steganography are designed to boost PSNR. According to the following equation, PSNR is:

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

The results of the experiments and the analysis discussed above show that the proposed method yields the highest PSNR values, making it hard to discover the hidden

image. The results in Table 6 show the algorithm offers higher protection against threats and improved security.

Table 6: Illustrates the experimental results of PSNR and MSE

Cover Image	Cover Image Size	MSE	PSNR	Secret Image
	463×516	0.0000977	88.2316	
	463×516	0.000098	88.1988	
	256×256	0.0000975	88.2406	

(a)

Cover Image	Cover Image Size	MSE	PSNR	Secret Image
	463×516	0.00010113	88.0818	
	463×516	0.00010176	88.0552	
	256×256	0.00010114	88.0816	

(b)

5.3 Information entropy analysis

We measure the ambiguity of a system using information entropy. That quantifies the unpredictability of an image plus the quantity of information included within it. A distribution of pixel values in an image can be determined using information entropy. The greater the

importance of using encryption, the better the results. So, entropy $H(d)$ for data d will calculate as follows.

$$H(d) = \sum_{i=1}^{2^l-1} p(d_i) \log_2 \left(\frac{1}{p(d_i)} \right) \quad (3)$$

where $p(d_i)$ represents the probability of d .

5.4 Correlation analysis

Correlation analysis calculates the degree of correspondence between the host image before and after hiding. When the correlation coefficients of the pixels in the host image are the least possible, the color image-hiding technique will withstand statistical attacks. Equations (4), (5), and (6) determine the correlation coefficients between two neighboring pixels along their diagonal, horizontal and vertical axes:

$$corr_{xy} = \frac{cov(x,y)}{\sqrt{\sigma_x} \sqrt{\sigma_y}} \quad (4)$$

$$cov(x,y) = \frac{1}{N} \sum_{i=1}^N (x_i - \bar{x})(y_i - \bar{y}) \quad (5)$$

$$\sigma_x = \frac{1}{N} \sum_{i=1}^N (x_i - \bar{x})^2, \quad \sigma_y = \frac{1}{N} \sum_{i=1}^N (y_i - \bar{y})^2 \quad (6)$$

Correlation coefficients are calculated for several rates of close pairs (horizontal, vertical, and diagonal) chosen randomly from the host image. Table 7 shows the comparative results of the suggested method for the (Entropy, Correlation) between the stego and host images. Correlation studies show this technique has excellent steganography.

6 Discussion

Many of the previous studies used hybrid approaches based on DNA to increase image encryption and resistance to attacks, as illustrated in Table 1.

But, when transmitting data over an unsafe public connection, steganography is frequently preferred over encryption. We cannot achieve security via cryptography only. So, several computing-related settings are suggested for using various DNA sequence biological properties in steganography and secure cryptography. Researchers have developed DNA-based methods for hiding data that offer unmatched confidentiality and protection without limiting adaptability or storage capacity. And they have created unique data-hiding strategies based on DNA after learning about the biological characteristics of DNA sequences. Such has prompted the creation of a whole new scientific area. To ensure secure digital color images, including those used in medicine, satellite remote sensing, social networking, etc., in this research, we suggested a new encoding algorithm to generate a DNA code for a confidential image. Furthermore, we produced an encoding technique for reducing DNA data storage, which is a relatively recent advancement in the world of digital data storage. Table 9 shows the obtained results. Then, we proposed a new approach to hide the bits of DNA sequence in the least significant bits (LSB) of the cover image.

Table 7: Experimental results of the suggested method for (Entropy, Correlation) between the host image and stego-image

Cover Image	Cover Image Size	Entropy Cover Image	Entropy stego Image	Correlation Cover Image	Correlation stego Image	Secret Image
Lena	463×516	7.2825	7.1630	0.9626	0.9644	
Baboon	463×516	7.3864	7.2761	0.9666	0.9670	
Peppers	256×256	7.6586	7.5402	0.8009	0.7973	

(a)

Cover Image	Cover Image Size	Entropy Cover Image	Entropy stego Image	Correlation Cover Image	Correlation stego Image	Secret Image
Lena	463×516	7.2825	7.1894	0.9636	0.9627	
Baboon	463×516	7.3864	7.3043	0.9677	0.9665	
Peppers	256×256	7.6586	7.5668	0.7956	0.7987	

(b)

7 Conclusions

In this paper, we suggested a color image steganography constructed using artificial DNA computing to provide more security to the system. Maintaining a high level of robustness against attacks is the objective of the suggested technology. Differential and statistical analyses we used with various tools demonstrate the security of our algorithm. To test used different image formats and a variety of image sizes to compute the (PSNR) and (MSE). The results and analysis proved that the proposed algorithm for differential analysis is resilient against attacks. Table 8 shows the obtained results compared to the other techniques. The results of the tests on the three standard images where a higher PSNR value between the host

images and the stego images and a lower MSE value, which shows that the algorithm's security is robust and this technique has excellent steganography.

Table 8: PSNR and MSE comparison results based on three colored images (Lena, Baboon, and Peppers).

Images	Method	PSNR	MSE
Lena	Ours	88.2316	0.0000977
	[44]	83.022	-----
	[25]	65.459	0.0016
	[21]	50.12	0.63
	[15]	39.1357	2.9967
	[22]	57.49	0.09
	[23]	60.4429	0.06
	[46]	82.59	0.153
Baboon	Ours	88.2406	0.0000975
	[44]	83.022	-----
	[25]	68.115	0.00889
	[21]	46.01	1.62
	[15]	45.9012	1.5887
	[22]	58.19	0.09
	[23]	60.4534	0.06
	[46]	82.59	0.153
Peppers	Ours	88.1988	0.000098
	[44]	83.022	-----
	[25]	68.0086	0.0088
	[21]	50.00	0.64
	[15]	45.0216	2.0621
	[16]	52.48	0.37
	[23]	60.5805	0.06
	[45]	71.7357	0.0075
	[46]	82.59	0.153

Table 9: Results of the encryption algorithm that reduced DNA data storage.

Secret Images	Images Sizes	Number of Bits in Binary Secret Images	Number of DNA codes in Secret Images	Number of Bits in Encrypted Secret Image
	75×75	135000	5625	54666
	75×75	135000	5625	43437
	75×75	135000	5625	47106
	75×75	135000	5625	47704

8 Future work

We can expand this work in the future to include: Both speech and video can be encoded using the method. To secure the image and maintain the proper size, it is advised to use image encryption and image data reduction technologies.

References

- [1] Q. Liu and L. Liu, "Color image encryption algorithm based on DNA coding and double chaos system," *IEEE Access*, vol. 8, pp. 83596–83610, 2020.
<https://doi.org/10.1109/access.2020.2991420>
- [2] X. Y. Wang, P. Li, Y. Q. Zhang, L. Y. Liu, H. Zhang et al., "A novel color image encryption scheme using DNA permutation based on the lorenz system," *Multimedia Tools Applications*, vol. 77, no. 5, pp. 6243–6265, 2018.
<https://doi.org/10.1007/s11042-017-4534-z>
- [3] H. R. Amani and M. Yaghoobi, "A new approach in adaptive encryption algorithm for color images based on DNA sequence operation and hyper-chaotic system," *Multimedia Tools Applications*, vol. 78, no. 15, pp. 21537–21556, 2019.
<https://doi.org/10.1007/s11042-018-6989-y>
- [4] X. Wang, Y. Wang, X. Zhu and C. Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level," *Optics and Lasers in Engineering*, vol. 125, no. 2, pp. 105851, 2020.
<https://doi.org/10.1016/j.optlaseng.2019.105851>
- [5] P. Liu, T. Zhang and X. Li, "A new color image encryption algorithm based on DNA and spatial chaotic map," *Multimedia Tools Applications*, vol. 78, no. 11, pp. 14823–14835, 2019.
<https://doi.org/10.1007/s11042-018-6758-y>
- [6] A. Rehman, X. Liao, R. Ashraf, S. Ullah and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2," *Optik (Stuttg.)*, vol. 159, pp. 348–367, 2018.
<https://doi.org/10.1016/j.ijleo.2018.01.064>
- [7] H. G. Mohamed, D. H. ElKamouchi and K. H. Moussa, "A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences," *Entropy*, vol. 22, no. 2, pp. 158, 2020.
<https://doi.org/10.3390/e22020158>
- [8] M. Samiullah, W. Aslam, H. Nazir, M. I. Lali, B. Shahzad et al., "An image encryption scheme based on DNA computing and multiple chaotic systems," *IEEE Access*, vol. 8, pp. 25650–25663, 2020.
<https://doi.org/10.1109/access.2020.2970981>
- [9] M. S. Taha et al, "Combination of Steganography and Cryptography: A short Survey", 2nd International Conference on Sustainable Engineering Techniques (ICSET) 2019, IOP Conf. Series: Materials Science and Engineering, 518 052003.
<https://doi.org/10.1088/1757-899x/518/5/052003>
- [10] F. Masood, J. Masood, L. Zhang, S. S. Jamal & W.i Boulila, "A new color image encryption technique using DNA computing and Chaos-based substitution box", *Soft Computing* 26:7461–7477, 2022.
<https://doi.org/10.1007/s00500-021-06459-w>
- [11] A. A. Tamimi, A. M. Abdalla, O. Al-Allaf, "Hiding

- an Image inside another Image using Variable-Rate Steganography", *International Journal of Advanced Computer Science and Applications*, Vol. 4, No. 10, 2013.
<https://doi.org/10.14569/ijacsa.2013.041004>
- [12] S. A. Mahdi & M. A. Khodher Sally, "An Improved Method for Combine (LSB and MSB) Based on Color Image RGB", *Engineering and Technology Journal*, Vol. 39, No. 01, pp. 231-242, 2021.
<https://doi.org/10.30684/etj.v39i1b.1574>
- [13] L. Kothari & S. Khara, "Data hiding on web using combination of Steganography and Cryptography", In *2017 International Conference on Computer, Communications and Electronics (Comptelix)*. 448-452, IEEE, July 2017.
<https://doi.org/10.1109/comptelix.2017.8004011>
- [14] N. Singh, "High PSNR based Image Steganography", *International Journal of Advanced Engineering Research and Science (IJAERS)*, Vol. 6, No. 1, Jan. 2019.
<https://doi.org/10.22161/ijaers.6.1.15>
- [15] A. ALabaichi, M. Abid Ali K. Al-Dabbas, and A. Salih, "Image steganography using the least significant bit and secret map techniques", *Int. J. Electr. Comput. Eng. (IJECE)*, Vol. 10, No. 1, pp. 935~946, February 2020.
<https://doi.org/10.11591/ijece.v10i1.pp935-946>
- [16] Y. Y. Wai and E. E. Myat, "Comparison of LSB, MSB and New Hybrid (NHB) of Steganography in Digital Image", *International Journal of Engineering Trends and Applications*, Vol. 5, No. 4, 2018.
- [17] N. Nandy, D. Banerjee & C. Pradhan, "Color image encryption using DNA based cryptography", *International Journal of Information Technology* volume 13, pages 533–540 (2021).
<https://doi.org/10.1007/s41870-018-0100-9>
- [18] S. Danish, & D. Tamer, "A novel image steganography technique based on similarity of bits pairs", *IEEE 8th Control and System Graduate Research Colloquium (ICSGRC)*, 99-104, IEEE, 2017.
<https://doi.org/10.1109/icsgrc.2017.8070576>
- [19] M. H. Mohammed, A. Abdel-Razeq, "DNA-based steganography using genetic algorithm", *Information Sciences Letters*: Vol. 9, No. 3, pp: 205-210, 2020.
<https://doi.org/10.18576/isl/090307>
- [20] S. Priya & D. Meera, "A Novel Approach for Highly Secured and Robust Image Steganography", *IJSET - International Journal of Innovative Science, Engineering & Technology*, Vol. 6 Issue 8, August 2019.
- [21] N. Yassin "DATA HIDING TECHNIQUE FOR COLOR IMAGES USING PIXEL VALUE DIFFERENCING AND CHAOTIC", *Jordanian Journal of Computers and Information Technology (JJCIT)*, Vol. 08, No. 03, September 2022.
<https://doi.org/10.5455/jjcit.71-1642508824>
- [22] D. Shehzad & T. Dag, "LSB Image Steganography Based on Blocks Matrix Determinant Method", *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS* VOL. 13, NO. 7, Jul. 2019.
<https://doi.org/10.3837/tiis.2019.07.024>
- [23] S. Kumar, S. Kumari, S. Patro, T. Shandilya & A. Kumar, "Image Steganography using Index based Chaotic Mapping", *International Journal of Computer Applications (IJCA)*, pp:0975–8887, *International Conference on Distributed Computing and Internet Technology (ICDCIT)*, 2015.
- [24] S. Zhou, P. He and N. Kasabov, "A Dynamic DNA Color Image Encryption Method Based on SHA-512", *Entropy*, 22, 1091; 28 September 2020.
<https://doi.org/10.3390/e22101091>
- [25] S. A. Sead, N. H. Qasim & H. A. Abd., "Robust Method for Embedding an Image inside Cover Image based on Least Significant Bit Steganography", *Informatica*, Vol. 46, No. 9, 2022.
<https://doi.org/10.31449/inf.v46i9.4362>
- [26] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map", *Nonlinear Dyn.*, vol. 69, no. 4, pp. 2079–2087, 2012.
<https://doi.org/10.1007/s11071-012-0409-z>
- [27] N. Iqbal, S. Abbas, M. A. Khan, T. Alyas, A. Fatima, and A. Ahmad, "An RGB image cipher using chaotic systems, 15-puzzle problem and DNA computing", *IEEE Access*, vol. 7, pp.174051–174071, 2019.
<https://doi.org/10.1109/access.2019.2956389>
- [28] J. Zhang, D. Fang, and H. Ren, "Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps", *Hindawi Publishing Corporation Mathematical Problems in Engineering* Volume 2014, Article ID 917147, 10 pages.
<https://doi.org/10.1155/2014/917147>
- [29] K. Sujana, R. Akhtar & S. Singh, "Image Steganography using Least Significant Bit algorithm", *International Journal Of Advance Research And Innovative Ideas In Education (IJARIIE)*, e- ISSN: 2395-4396, Vol-4, Issue-2, 2018.
- [30] S. A. Sead Almola, "Hiding Images in the Spatial Domain", *Informatica*, Vol. 46, No. 8, 2022.
<https://doi.org/10.31449/inf.v46i8.4252>
- [31] A. Kadhim Hammoud, H. Nahi Mohaisen & M. Q.

- Mohammed," Secret information hiding in image randomly method using steganography and cryptography", *Int. J. Nonlinear Anal. Appl.*, Vol. 12, Special Issue, Winter and Spring 2021, 1283-1291.
<http://dx.doi.org/10.22075/ijnaa.2021.5644>
- [32] S. Pramanik & S. K. Bandyopadhyay," Image Steganography Using Wavelet Transform And Genetic Algorithm", *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*, Vol. 1, Issue 1, March 2014.
- [33] S. Pramanik and S. S. Raja," A SECURED IMAGE STEGANOGRAPHY USING GENETIC ALGORITHM", *Advances in Mathematics: Scientific Journal* 9 , no.7, 4533–4541, 2020.
<https://doi.org/10.37418/amsj.9.7.22>
- [34] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Appl. Soft Comput.*, vol. 37, pp. 24–39, 2015.
<https://doi.org/10.1016/j.asoc.2015.08.008>
- [35] X. Wang, H. Zhang, and X. Bao, "Color image encryption scheme using CML and DNA sequence operations," *Biosystems*, vol. 144, pp. 18–26, 2016.
<https://doi.org/10.1016/j.biosystems.2016.03.011>
- [36] J. Wang, F. Long, and W. Ou, "CNN-based color image encryption algorithm using DNA sequence operations," in *2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)*, 2017, pp. 730–736.
<https://doi.org/10.1109/SPAC.2017.8304370>
- [37] K. C. Jithin and S. Sankar, "Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set," *J. Inf. Secur. Appl.*, vol. 50, p. 102428, 2020.
<https://doi.org/10.1016/j.jisa.2019.102428>
- [38] S. Zhou, P. He, and N. Kasabov, "A dynamic DNA color image encryption method based on SHA512," *Entropy*, vol. 22, no. 10, p. 1091, 2020.
<https://doi.org/10.3390/e22101091>
- [39] N. Iqbal, M. Hanif, S. Abbas, M. A. Khan, S. H. Almotiri, and M. A. Al Ghamdi, "DNA strands level scrambling based color image encryption scheme," *IEEE Access*, vol. 8, pp.178167–178182,2020.
<https://doi.org/10.1109/ACCESS.2020.3025241>
- [40] X. Chai, X. Zhi, Z. Gan, Y. Zhang, Y. Chen, and J. Fu, "Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption," *Signal Processing*, vol.183,p.108041,2021.
<https://doi.org/10.1016/j.sigpro.2021.108041>
- [41] S. Patel, V. Thanikaiselvan, D. Pelusi, B. Nagaraj, R. Arunkumar, and R. Amirtharajan, "Colour image encryption based on customized neural network and DNA encoding," *Neural Comput. Appl.*, vol. 33, no. 21, pp. 14533–14550, 2021.
<https://doi.org/10.1007/s00521-021-06096-2>
- [42] Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding," *Multimed. Tools Appl.*, vol. 80, no. 9, pp. 13841–13864, 2021.
<https://doi.org/10.1007/s11042-020-10437-z>
- [43] I. A. Aljazeera, H. T. ALRikabi, A.I Hadi, M. Alaidi, "Encryption of Color Image Based on DNA Strandand Exponential Factor", *iJOE .*, Vol. 18, No. 03, 2022·
<https://doi.org/10.3991/ijoe.v18i03.28021>
- [44] X. Man and Y. Song," Encryption of Color Images with an Evolutionary Framework Controlled by Chaotic Systems", *Entropy* 2023, 25, 631.
<https://doi.org/10.3390/e25040631>
- [45] Malathi S. et al., "AN AUTOMATIC COST LEARNING FRAMEWORK FOR IMAGE STEGANOGRAPHY USING DEEP REINFORCEMENT LEARNING", *Dogo Rangsang Research Journal, UGC Care Group I Journal* , ISSN : 2347-7180, Vol-13, Issue-5, No. 4, May 2023.
<https://doi.org/10.36893/drsr.2023>
- [46] A. AbdelRaouf, "A new data hiding approach for image steganography based on visual color sensitivity", *Springer, Multimedia Tools and Applications*, June 2021.
<https://doi.org/10.1007/s11042-020-10224-w>