Colour Image Encryption Using DNA Coding and Logistic Diffusion

[1]Amani Theramban
Dept. of Electronics and Communication Engineering
M.E.A Engineering College
Malappuram, Kerala, India
amu.rouf@gmail.com

[2]Renjith V. Ravi
Dept. of Electronics and Communication Engineering
M.E.A Engineering College
Malappuram, Kerala, India
renjithravi.research@gmail.com
ORCID: 0000-0001-9047-3220

2021 Fourth International Conference on Microelectronics, Signals & Systems (ICMSS) | 978-1-6654-4885-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICMSS53060.2021.9673628

***Abstract*—The necessity to meet the security demands of digital images has led to effective encryption methods. The suggested encryption technique combines image encryption utilizing chaotic transforms and DNA (Deoxyribonucleic acid) coding procedures. DNA computing techniques are 100 times faster and have less power consumption than other algorithms in modern computers. Using a suitable chaotic map, the encryption technique is done separately on the color image's R, G, and B channels. After chaotic encryption, a technique called DNA encoding is used. A novel conditional shift based on Mandelbrot Set is presented to apply confusion to the three channels successfully. The suggested encryption method, according to security analysis, performs admirably in terms of security.**

***Index Terms*—DNA encryption, Chaotic encryption, Image encryption, Mandelbrot set.**

I. Introduction

Data and information communication have become essential assets in today's modern world. If information's confidentiality is breached, it may be exploited for malicious reasons. Current advancements in information technology and its many uses in our daily lives have resulted in a massive increase in data sent via the internet. As vulnerable assets, private information must be safeguarded from intruders. As a result, data must be protected before being sent, and techniques must be developed to convert it into a form that is useless to intruders. Cryptographic algorithms are mathematical approaches and strategies for data security [1]. For example, Bit-by-bit or byte-by-byte transformations are used in stream ciphers. Simultaneously, block ciphers divide data into pieces of several bits or bytes. Block ciphers are one of the most powerful instruments for data security in contemporary symmetric encryption [2].

Secure real-time communication has become more popular as communication technology advances in health, aerospace, education, the military, and other areas. Digital image information has become extremely popular as a method of visible communication. Fast image encryption is critical for masking information to secure private images while still ensuring a high transmission rate [1]. Due to the pandemic situation of COVID -19, the increase in the use of online resources (education, online shopping, banking and so on) requires high demand for data security. As cyber-attacks are increasing day by day, security needs to be more necessary, and thus, new encryption schemes become more prominent. Therefore, sensitive data hiding becomes the most crucial area in securing network information. Due to cryptanalysts always attempting to access any accessible cryptographic systems, constructing a completely secure encryption method is very difficult. The correct algorithm selection is critical for meeting the stringent requirement that safeguards cryptographic components from cryptanalysis.

During transmission, the image data must be encrypted to protect it from other assaults. The government, financial institutions, military, and hospitals all deal with personal images of their patients, financial conditions, geographic regions, enemy positions, and other sensitive information. Most of this information is now collected and stored on electronic computers and transmitted over the public network. If all the confidential images about enemy positions, patients, and geographical areas are getting into the wrong hands, such security could lead to the declination of war, unfair treatment etc. As a result, the safeguarding of sensitive images is a must. An image may conceal private or sensitive information. It is encrypted and then decoded using secure keys. Encrypting images by converting them from a means to a meaningless version is a well-known effective technique for maintaining integrity [2]. Images contain enormous data capacity, and it is well known that neighboring pixels have a strong correlation. Therefore, RSA, DES, and AES are not appropriate for image encryption [3]. Researchers from all around the globe have recently explored several types of image enciphering methods based on chaos, Fourier transforms, cellular automata, and DWT [4].Confusion and diffusion are the fundamental components of chaos-based image encryption.

During the permutation alias shuffling step, the pixel locations are altered randomly without affecting the pixel values. Diffusion, the next stage in the encryption process, is used to enhance security. Diffusion is accomplished using certain chaotic transforms. It is done by replacing the actual pixel values with random values sequentially produced by chaotic maps. Various academics have suggested many chaos-based image encryption methods. [2] presented a CML and DNA-based image encryption method. Researchers have recently

This project was financially supported by Kerala State Council for Science and Technology Environment, under the *Student Project Scheme* with reference number 00548/SPS65/2021/KSCSTE.

978-1-6654-4885-7/21/$31.00 ©2021 IEEE.

Authorized licensed use limited to: Università di Bari Aldo Moro. Downloaded on October 02,2025 at 09:44:46 UTC from IEEE Xplore. Restrictions apply.

become increasingly interested in image encryption systems utilizing CML [5]. Many researchers have integrated chaos and DNA encoding methods, generation of pseudo-random numbers, and DNA computing to improve image security in all areas.

Every day, the chance of cyber-attacks has tremendous increases, there comes the importance of developing new encryption techniques. There have been various encryption systems related to DNA sequence operations. DNA is considered a promising technology for encryption due to extraordinary data density and vast parallelism. Moreover, DNA itself is a unique signature. As the cryptanalytic processes are improving day by day, more sophisticated algorithms are necessary for secure image data transmission. In this paper, we have modified the work proposed by Jithin et. al. in [6] enhanced the key generation process. In [6], a single chaotic key derived from Arnold map was used for the entire encryption process and included three DNA encoding blocks together with two DNA XoR operations. We have modified this work by using two different keys derived from henon map and logistic map for the entire encryption scheme, only used two DNA encoding blocks together with one DNA XoR operation, and also exchanged the blocks for diffusion and conditional shift algorithms. The quality of our encryption algorithm is analyzed by performing various security analysis methods such as histogram analysis, correlation analysis, Shannon entropy, structural similarity index measure (SSIM), and evaluation of robustness against differential attack by measuring NPCR and UACI, and the metrics PSNR and MSE.

II. Related Works

The following is a rundown of the most recently suggested image encryption techniques.A novel medical image was developed to perform pixel permutation bit level substitution in the article. [7]. To conduct diffusion on pixel data, the DNA encoding method is used. [8] presented an encryption method that used DNA sequence operations to encrypt images. Their technique of increasing the hamming distance enhanced the capacity to withstand known and selected plain text assaults. Even though the novel methods in this area increased all assessment criteria, the key space is still inadequate. Furthermore, only grey images are supported by the encryption methods described in the articles [1] [9] [8]. As a result, there is an additional load of transforming colour image data and other data into the same gray images before applying encryption.

Liu H et al. [10] used the MD5 hash to generate chaotic map starting conditions, followed by DNA encoding. Norouzi et al. [11] also use the chaotic, random sequences created using CNN to change the gray level values of the pixel and interrupt the correlation between an image's neighboring pixels. Any encryption scheme that relies on the keys and the input plaintext image is required. Wu X. et al. [12] suggested a technique that would allow performing differently for every image generated by crucial image encryption streams from an initial image and a secret key. This technique likewise defeats known-plaintext and chosen-plaintext assaults. When compared to other works in the same area, the entropy value is quite low. [3] integrated memristive hyperchaotic systems, CA, and DNA coding operations to create an encryption scheme for grey images. In terms of computing, the system seems to be quite complicated. Most studies addressing image encryption using DNA [2] use DNA additions, subtractions, and the XOR method. In different studies [2] [13], hash functions like SHA-256 are utilized to update the starting conditions to create key streams.

We introduce a color image encryption method based on chaos theory, DNA coding operations, and the Mandelbrot set. The Henon map is used to create key streams, which are then encoded with DNA. Between the R, G, and B components and the key streams, a Hamming distance computation is conducted, which is then encoded with DNA. Finally, a method is used to do channel-wise DNA encoding. Diffusion and confusion phases are included in this process. A novel conditional shift technique is used to confuse pixel values to create the cipher image, and diffusion is done using an XOR operation.

III. Materials and Methods

A. Henon Map

The henon transform or henon map is a dynamic system that is discrete in the time domain and behaves chaotically well. The henon map selects a point (x_n, y_n) and moves it to another pixel location as follows [14]:

$$x_{n+1} = 1 - ax^2 + y_n \tag{1}$$

$$y_{n+1} = 1 - bx_n \tag{2}$$

This map is based on two variables: a and b. This map gets its chaotic behavior only when a and b gets the value 1.4 and 0.3.

B. Logistic Map

The logistic map [15] may be represented mathematically as:

$$\chi_{n+1} = \gamma X_n \left(1 - X_n\right) \tag{3}$$

The parameter is utilized here, and the values must be between $[0, 4]$. When the value is between 3.5 and 4, it is shown empirically that the randomness or chaotic behavior is incredibly high.

C. DNA Encoding

DNA is a molecule that incorporates genetic information—used in every living organism and various viruses' evolution, development, working, and reproduction. DNA encoding [6] has a large data capacity, making it suitable for cryptography. Process DNA may also be utilized to store data in picture encryption during transmission. The DNA logic word is utilized in DNA computing, and just two digits are needed to generate four nucleic acid bases. As a result, the bases Adenine (A), Cytosine (C), Guanine (G), and Thymine (T) are used to store information. The four nucleotides are

Authorized licensed use limited to: Università di Bari Aldo Moro. Downloaded on October 02,2025 at 09:44:46 UTC from IEEE Xplore. Restrictions apply.

utilized to capture information in DNA cryptography. The letters "A" and "T," as well as "C" and "G," are paired duos. There are eight rules for DNA encoding, as shown in Table I.

TABLE I: Rules in DNA Encoding

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

D. XOR operation of DNA sequence

There are eight different types of DNA XOR operation, just as we have eight different types of DNA rules that fulfil the Watson-Crick complementary rule [16]. For example, when the two DNA coded sequences "CTGA" and "TGAC" are combined using an XOR operation (as per rule 1), the output is "GCGC." For instance, the result obtained is 'GCGC' after applying XOR operation on two different DNA sequences (CTGA & TGAC).

TABLE II: Rule for DNA XoR

XoR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

1) Mandelbrot Set: A Mandelbrot set is a collection of complicated planar points. For example, a complex number $c \in C$ expressed as $c = x + y_i$, where x and y are both R, may be used to describe a point in the plane. Here, the new structure is obtained by coloring the Mandelbrot points in grey. The values produced by the Mandelbrot set are utilized in our encryption system's shifting procedure [6].

$$\lim_{n\to\infty} Z_{(n+1)} = Z_n^2 + C, \qquad \text{Where } Z_0 = 0 \tag{4}$$

We use the method outlined below to eliminate all zero-value black pixels to get a modified form of the Mandelbrot result. Let $W(i, j)$ be the value of a pixel in the position (i, j) in Fig. 1, where C is a constant term in our experiment and has the value $(= 10^{14})$.

2) Conditional Shift Algorithm: An algorithm is used to shift images based on the Mandelbrot set. Modified Mandelbrot set image obtained from the original Mandelbrot set to perform cyclic shift on the image. Conditional shift algorithm [6] used to meet the need of confusion procedure.

The modified Mandelbrot set [6] image is used, and its corresponding maximum value of i^{th} column is selected. Then, it is compared with a maximum value of elements in i^{th} row of color image matrices. According to the comparison, the image is applied left or right cyclic shift.

IV. Proposed Work

The primary operations carried out in the proposed encryption approach are keystream generation using chaos, DNA Encoding, and confusion-diffusion (Conf-Diff). The enciphering process systematically integrates three significant components: chaotic map sequences, the Mandelbrot set's collection of points, and the DNA sequence operation. While transmitting via media, the encryption process creates the most encrypted version of the plaintext image, impenetrable by attackers.

Decryption is the opposite process of encryption. Therefore, the reverse process of all the steps carried out in the encryption process will be executed in the reverse order to get the plaintext image from the cipher image.

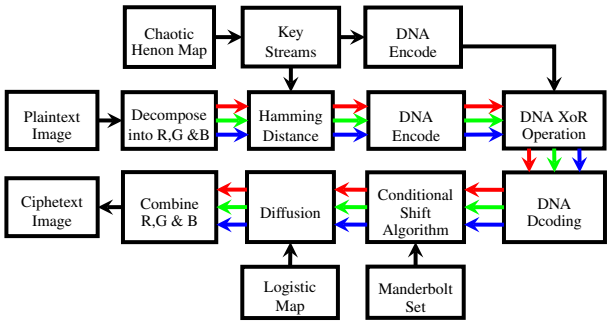


Fig. 1: Encryption Algorithm with modified key

A. Steps in the Algorithm

1) K_1, K_1, K_2, and K_3 are the key streams produced by the Henon map.
2) Each K_i is translated to binary. A sequence of DNA bases E_1, E_2, and E_3 is generated using the DNA Encoding Operation.
3) Initially, the plaintext image will be separated into R, G, and B components
4) To produce H_R, H_G, and H_B, Hamming distance calculations are performed between key streams (K_i) and RGB component matrices.
5) To get the three DNA coded matrices DH_R, DH_G, and DH_B, perform a DNA encoding procedure on the hamming matrices H_R, H_G, and H_B.
6) The three DNA coded matrices and key streams acquired from the chaotic key generation are combined using the XOR technique.
7) Use the *Conf-Diff* algorithm to perform the *Conf-Diff* operation as mentioned in [6]. Lastly, the encrypted image is formed by combining the cypher image components C_R, C_G, and C_B.

V. Results and Discussion

This section mentions how well our work performs compared with other existing works in the literature. Comparison is made based on the evaluation metrics entropy, PSNR, SSIM, NPCR, UACI, etc. The proposed method can resist all types of differential, statistical and occlusion attacks, proving that

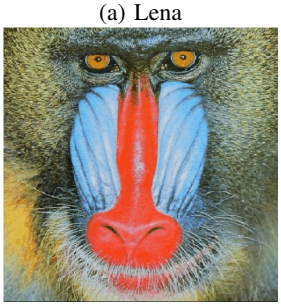
Authorized licensed use limited to: Università di Bari Aldo Moro. Downloaded on October 02,2025 at 09:44:46 UTC from IEEE Xplore. Restrictions apply.

all values are equal to the theoretical value and provide more security than the existing ones.

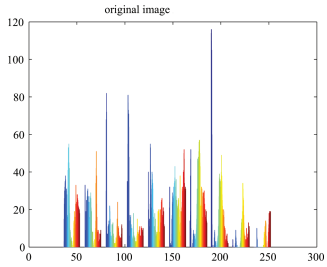
We chose some typical colour images with a size of 256×256 to illustrate our method's benefits. By encrypting several images, we can assess the quality of our encryption system. The suggested work's simulation results are shown in Fig 2 and Fig 3.

(a) Lena

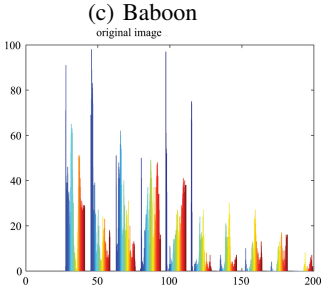
(b) Barbara



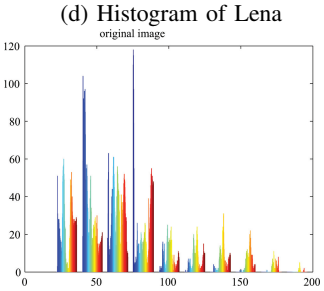
(c) Baboon



(d) Histogram of Lena



(e) Histogram of Barbara



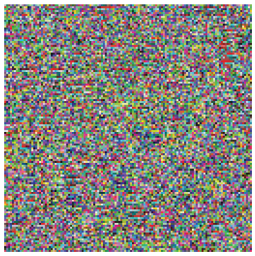
(f) Histogram of Baboon

Fig. 2: Plaintext images and histograms

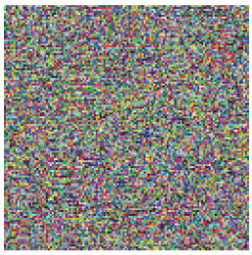
A. Histogram Analysis

The distribution of pixel intensity levels is shown in an image histogram, which also offers statistical information about the image. A secure image encryption system may provide a consistent histogram to the encrypted image, making it resistant to statistical attacks. The histograms of plain and encrypted images are shown in Fig 2 and Fig 3.

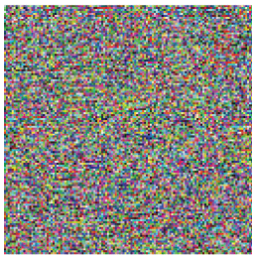
It acts as a graphical illustration of the tones in a very digital image. It shows the number of pixels for every tonal worth. By observing this for a particular image, a viewer is ready to decide the complete tonal distribution at a look. The graph's horizontal axis represents the tonal variations, whereas the vertical axis represents the entire variety of pixels therein specific tone. It is an important parameter to verify that the cipher image resists statistical attack. The Histogram analysis must be uniform.



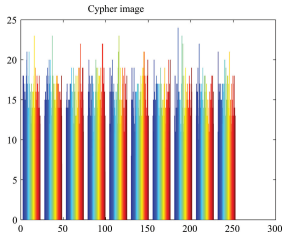
(a) Ciphertext image of Lena



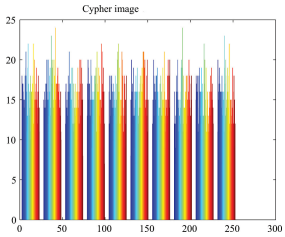
(b) Ciphertext image of Barbara



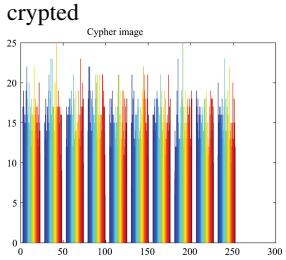
(c) Ciphertext image of Baboon



(d) Histogram of Lena Encrypted



(e) Histogram of Barbara-Encrypted



(f) Histogram of Baboon-Encrypted

Fig. 3: Ciphertext images and histograms

B. Correlation Of Adjacent Pixels

In a natural plaintext image, the coefficient correlation of two neighboring pixels is often vital. Therefore, an effective encryption method employed on a plaintext image should achieve a low coefficient correlation among neighboring pixels in the matching ciphertext image. The test results are given in Table 5 using Eq. 5, Eq. 6 and Eq. 7, and randomly selecting some pairs of neighboring pixels in horizontal, vertical, and diagonal directions from Lena. Using our approach, we can observe that the coefficient correlations in the ciphertext image become close to zero.

$$r_{xy} = \frac{N^2 \cdot \operatorname{cov}(x, y)}{\sum_{i=1}^{N} (x_i - E_x)^2 \cdot \sum_{i=1}^{N} (y_i - E_y)^2} \tag{5}$$

$$E_x = \frac{\sum_{i-1}^{N} x_i}{N} \tag{6}$$

$$\operatorname{cov}(x, y) = E\left((x - E_x)(y - E_y)\right) \tag{7}$$

1) NPCR and UACI: Because our system must resist differential assaults, the attackers should have difficulty figuring out how the plain and encrypted images are linked. The NPCR

Authorized licensed use limited to: Università di Bari Aldo Moro. Downloaded on October 02,2025 at 09:44:46 UTC from IEEE Xplore. Restrictions apply.

and UACI are the primary parameters utilized. The following are the definitions for these parameters:

$$NPCR = \frac{\sum_{i-1}^{m}\sum_{j-1}^{n} D(i,j)}{m \times n} \times 100 \tag{8}$$

$$UACI = \frac{1}{255 \times m \times n}\left[\sum_{i=1}^{m}\sum_{j=1}^{n} C(i,j) - C1(i,j)\right] \times 100 \tag{9}$$

The width and height of the image are indicated by the numbers m and n.$-C1(i,j)$ slightly change, respectively. The UACI score has a demonstrated value of approximately 0.33, whereas the NPCR score is closer to 1. The values of NPCR and UACI are shown in Table III.The average NPCR and UACI of our proposed algorithm and other existing works are shown in Table IV, both of which are higher when comparing with other works in the literature.

TABLE III: NPCR and UACI Values

Image Name	NPCR	UACI
Lena	0.99844	0.33.64
Baboon	0.99624	0.28974
Barbera	0.99591	0.30528

TABLE IV: NPCR and UACI analysis - Lena image

Works	NPCR	UACI
[5]	99.62	33.61
[7]	.99.6536	33.41
[6]	99.571	33.33
Proposed algorithm	99.84	33.64

TABLE V: Correlation coefficient of Cipher Images

Test Image	Colour Channel	Horizontal	Vertical	Diagonal
Fig 3a	R	0.065793	-0.0049251	-0.013682
	G	0.10427	-0.024172	-0.040558
	B	0.10332	-0.015368	-0.013396
Fig 3b	R	0.037239	0.015404	0.0088292
	G	0.00716	-0.0049739	-0.0090754
	B	0.019034	0.0038615	-0.0028343
Fig 3c	R	0.033374	-0.00010556	-0.0013279
	G	0.026709	-0.0068922	-0.0009608
	B	0.038279	-0.013044	-0.011346

TABLE VI: Correlation analysis - Lena image

Works	Horizontal	vertical	Diagonal
Plain image-"Lena"	0.9417	0.9696	0.9149
[5]	-0.0010	0.0012	-0.0012
[7]	0.0013	-0.0049	0.0057
[6]	-0.00116	0.00106	-0.0043
Proposed algorithm	0.0078636	-0.0028031	-0.0002627

The correlation coefficient analysis of existing works and our proposed algorithm is given in Table VI. It is clear that the correlation coefficient in three directions is almost close to 0, also lower than other existing works, hence can resist statistical attack.

C. Shannon Entropy

Shannon Entropy is a metric for how unpredictable an image is. For an 8-bit image, the entropy is calculated as follows:

$$H(m) = -\sum_{i=0}^{255} P(x_i) \times \log P(x_i) \tag{10}$$

The probability of x_i appearing in an image is $P(x_i)$, where x_i is the grey value. Therefore, it is necessary to have an entropy value near 8 for better performance in encryption.Table VII shows entropy value of plain and cipher images respectively for different test images. Also TableVIII show comparison of proposed work with existing works.Our entropy value is 7.9947,nearly equal to 8 and hence can resist statistical attack.

TABLE VII: Entropy Values

Image Name	Entropy of Plain Image	Entropy of Cipher Image
Lena	7.4056	7.9947
Baboon	7.6129	7.9939
Barbera	7.7905	7.9945

TABLE VIII: Entropy analysis-Lena image

Works	Entropy of plain Image	Entropy of Cipher Image
[5]	7.4056	7.9974
[7]	7.4056	7.9994
[6]	7.4056	7.9992
Proposed	7.4056	7.9947

D. Peak signal-to-noise ratio (PSNR),Mean square error(MSE) and Structural similarity index measure (SSIM)

Because the signal outperforms the noise, a greater PSNR value is desirable [6].PSNR is computed as,

$$PSNR = \log \frac{255 \times 255}{MSE} \tag{11}$$

MSE is the mean square value of error and is represented mathematically as follows,

$$MSE = -\frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - C(i,j)]^2 \tag{12}$$

where I_{mn} and C_{mn} are the plain image and its corresponding cipher image, respectively. The SSIM index is a technique for determining how similar two images are (On the receiver side, the real plaintext image and the decrypted image are compared for resemblance. Thus, it is a measure used to find out how similar the decrypted and plaintext images are. The SSIM index should be nearly close to 1 for a better encryption scheme. The SSIM value between plaintext and decrypted image for our work and K.C.Jithin et al., [6] shown in Table

Authorized licensed use limited to: Università di Bari Aldo Moro. Downloaded on October 02,2025 at 09:44:46 UTC from IEEE Xplore. Restrictions apply.

XI. For a good image separation result between plaintext and decrypted image, the PSNR value must be large.We calculated PSNR value between plaintext and decrypted image for [6], [7] and proposed work. The values of PSNR, MSE and SSIM between plain and ciphertext are shown in Table IX. From this, we can infer that the values of PSNR is quite low and MSE quite is high. Hence, we can infer that there is a comparatively huge dissimilarity between plaintext and ciphertext images.

TABLE IX: PSNR,MSE AND SSIM between Plaintext and Ciphertext images

Image Name	PSNR	MSE	SSIM
Lena	8.3969	9105.7514	0.001
Baboon	8.5999	9120.2314	0.004
Barbera	8.5973	9081.4305	0.0002

TABLE X: SSIM between Plaintext and decrypted images

Image Name	SSIM
Lena	0.9399
Baboon	0.9380
Barbera	0.9391

TABLE XI: Structural similarity index analysis

Image Name	[6]	Proposed work
Lena	0.9354	0.9399

TABLE XII: PSNR analysis

Image Name	[6]	[7]	Proposed work
Lena	36.0656	30.0205	37.523

VI. Conclusion

Due to advances in networking and multimedia coding, material like images is generally saved and shared over the Internet. Unfortunately, this renders them susceptible to nefarious usage. Image security and encryption have thus become a highly sought-after field to secure confidentiality and prevent unauthorized access to digital information. This paper proposes a new image encryption method based on chaos theory and DNA encoding. To increase security, encryption is performed individually to each of the three color channels of the image.

Furthermore, because our method encrypts utilizing random sequences created using chaotic maps, the attacker will be unable to decode the cipher image produced by our algorithm. This work's analytical section contains histogram analysis, correlation analysis, entropy, NPCR, and UACI, among other things. These assessment criteria, when taken into account, provide more remarkable results than prior studies. Furthermore, it demonstrates that the algorithm produces a more secure method of transmitting image data.

References

[1] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," *Optics and Lasers in engineering*, vol. 88, pp. 197–213, 2017.

[2] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image dna encryption using nca map-based cml and one-time keys," vol. 148, no. C, 2018. [Online]. Available: https://doi.org/10.1016/j.sigpro.2018.02.028

[3] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and dna sequence operations," *Signal Processing: Image Communication*, vol. 52, pp. 6–19, 2017.

[4] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Processing*, vol. 148, pp. 124–144, 2018.

[5] Y.-Q. Zhang, H.-F. Huang, X.-Y. Wang, and X.-H. Huang, "A secure image encryption scheme based on genetic mutation and mlncml chaotic system," *Multimedia Tools and Applications*, vol. 80, no. 13, pp. 19 291–19 305, 2021.

[6] K. Jithin and S. Sankar, "Colour image encryption algorithm combining arnold map, dna sequence operation, and a mandelbrot set," *Journal of Information Security and Applications*, vol. 50, p. 102428, 2020.

[7] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and dna encoding," *IEEE access*, vol. 7, pp. 36 667–36 681, 2019.

[8] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using dna sequence operations," *Optics and Lasers in Engineering*, vol. 73, pp. 53–61, 2015.

[9] J. Wu, X. Liao, and B. Yang, "Image encryption using 2d hénon-sine map and dna approach," *Signal Processing*, vol. 153, pp. 11–23, 2018.

[10] H. Liu, X. Wang *et al.*, "Image encryption using dna complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457–1466, 2012.

[11] B. Norouzi and S. Mirzakuchaki, "An image encryption algorithm based on dna sequence operations and cellular neural network," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13 681–13 701, 2017.

[12] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on dna sequences and multiple improved 1d chaotic maps," *Applied Soft Computing*, vol. 37, pp. 24–39, 2015.

[13] A. ur 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*, vol. 159, pp. 348–367, 2018.

[14] L. Chen, H. Yin, L. Yuan, J. T. Machado, R. Wu, and Z. Alam, "Double color image encryption based on fractional order discrete improved henon map and rubik's cube transform," *Signal Processing: Image Communication*, vol. 97, p. 116363, 2021.

[15] M. Kumar and P. Gupta, "A new medical image encryption algorithm based on the 1d logistic map associated with pseudo-random numbers," *Multimedia Tools and Applications*, vol. 80, no. 12, pp. 18 941–18 967, 2021.

[16] X.-y. Wang, H.-l. Zhang, and X.-m. Bao, "Color image encryption scheme using cml and dna sequence operations," *Biosystems*, vol. 144, pp. 18–26, 2016.

Authorized licensed use limited to: Università di Bari Aldo Moro. Downloaded on October 02,2025 at 09:44:46 UTC from IEEE Xplore. Restrictions apply.