Encryption of Color Image Based on DNA Strand and Exponential Factor

https://doi.org/10.3991/ijoe.v18i03.28021

Ibtisam A. Aljazaery[1], Haider TH. Salim ALRikabi[2(✉)], Abdul Hadi M. Alaidi[2]
[1]College of Engineering, University of Babylon, Babylon, Iraq
[2]Wasit University, Wasit, Iraq
hdhiyab@uowasit.edu.iq

Abstract—In this study, a new method has been eliciting for encoding 2D and 3D color images. The DNA strand construction was used as the basis for structuring the method. This method consisted of two main stages, the encryption and decryption stages. As each stage includes several operations to reach the desired goal. In the coding stage, a special table was prepared to show the mechanism of work. It starts with encoding the DNA bases into two binary orders, then two zeros are added to the string to finally consist of four binary bits whose size is parallel to the representation of a set of hexadecimal numbers represented in binary, where the XOR operation is then done between the two values to be the result is completely different from the original code. Then the binary values we obtained are converted to decimal values that are placed in an array with the same size as the image to be encoded. Finally, this last array was processed with the exponential function factor, so the final result is a 100% encoded image. In the decoding stage, another algorithm was built that reflects the work of what preceded it in the encryption stage, where the result was an exact copy of the original image. It is worth noting that standard images of different sizes were used as testing images. The performance evaluation of the method was calculated based on several factors: MSE, peak PSNR, and the time required to perform the encoding and decoding process. The method achieved good results when compared with the results of other methods in terms of quality and time.

Keywords—DNA strand, DNA encoding, MSE, PSNR, XOR operation

1 Introduction

The interchange of data in the era of the internet has resulted in a rapid increase in the amount of information sent and received. The sending information via the internet has made life easier, it faces a significant challenge: secure data transfer [1, 2]. This is entirely attributable to the annual increase in the number of hacking and intrusion incidents. People have entered an era of big data information as a result of the growth of artificial intelligence, the Internet of Things, 5G, and other technologies [3]. To address the issue of secure communication, two distinct approaches have developed and are widely utilized throughout the world: cryptography and steganography. Information

is closely related to people's lives, and various aspects of life will produce a large amount of information [4, 5]. Among them, digital is widely used due to its intuitive and vivid images and has become the mainstream information transmission medium. Therefore, we must pay close attention to the security protection of digital images. The three methods to protect the mainstream of digital images are encryption, information hiding, and digital watermarking. Encryption of Information is widely used in fields such as protecting the confidentiality of documents, and digital watermarking technology is mainly used for identity verification and copyright protection. Recently DNAs are being used as one as the strong technique of encryption owing to their great information density. Based on the above situation, the most commonly used method for digital image protection is image encryption. Security becomes a significant subject for modern computing systems [6–10]. The governmental offices, banks, and military information are the most important places that can't afford any leakages to their secret data. To save data from robberies, secret writing methods were used, and the most popular ones are cryptography and steganography. DNA cryptography can encrypt or encode the data using DNA computing techniques due to the DNA properties like parallel molecular computing, storing, transmitting the data, and computing capabilities [11–14]. DNA is also used for other purposes like Cryptography, Intrusion detection systems, and Steganography. The basic unit of DNA molecules is nucleotide, and a nucleotide is composed of multiple nitrogen-containing bases. Compared with traditional computers, DNA has a greater data density. Using DNA encoding to carry image information, relying on the complementary pairing of the four bases of A, G, C, and T to achieve various logical operations for image encryption, this method is referred to as DNA encryption. While DNA encryption generally requires biological experiments to operate, it is difficult to control external factors such as experimental equipment and experimental environment, and then pseudo-DNA computing is introduced for encryption. In recent years, pseudo-DNA calculations are mainly DNA addition, DNA subtraction, DNA XOR, and DNA XNOR operations [15–17]. These operations are simple and easy to operate, but they are of little biological significance. the principle of DNA mutation into image encryption and applied the biological significance of DNA to encryption. By using the principle of DNA mutation to diffuse the pixel value, the encryption effect is good. Based on the application of the above-mentioned DNA mutant biological operations in image encryption. To introduce more biological operations, this article uses the principle of DNA strand displacement to select a stable DNA structure. In recent years, it has increased biological operations and biological significance, increased the relevance of keys and plain text, and improved randomness.

2 Related works

In [18, 12], the authors developed a modern data security method by considering the advantage of DNA-based Advanced Encryption Standard (AES) cryptography and DNA steganography. This technique will furnish multilayer security to the secret message. The message is firstly encoded into DNA bases then, the DNA-based AES algorithm is applied to it. In the final step, the encrypted DNA will be concealed into another DNA sequence. Triple-layer security is established to the secret message by this

hybrid technique. In [19, 20], a new DNA symmetric cryptography is built to enhance the security of data, where the achieved results approve that the encryption process of plaintext is very secured. Shweta and Indora [21] applied a DNA cryptography method, and they hide the achieved sequence of DNA into video frames. As a consequence of the study, the frame is unnoticeable yet the video appears to be identical. The increase in PSNR and the decrease in MSE demonstrate the technique's effectiveness. Akiwate and Parthiban [22] presented Dynamic DNA as a key-based technique that is capable of accepting a variety of data types, including characters, text files, pictures, and audio. Each time the random key created at the sender is used to decrypt the ciphertext at the receiver, the technique becomes extremely resistant to a variety of assaults. A novel cryptosystem was proposed by Pavithran et al. [23] based on DNA cryptography and the finite automata method. This system generates a key based on receiver attributes and the same key used for encryption. Unlike steganography, which conceals data from hackers, numerous forms of research have been proposed using DNA steganography. Sushma et al. [24] developed a technique in which secret data is translated to binary, then to DNA nitrogen bases and finally to a DNA sequence. The DNA sequence is then translated into amino acids. These amino acids are then translated to binary and inserted into a cover image using the 2-3-3 embedding approach, before being delivered to the receiver over the communication channel. Musanna et al. [25] devised a technique based on a Neural Network algorithm using the DNA codon's Least Significant Bit (LSB) to achieve the lowest cracking probability while maintaining a short execution time. The secret messages are encoded within the sequence of the reference DNA. The combination of encryption and steganography techniques increases the data's security. Qi et al. [18] presented a new haze image steganography approach by embedded the text with the weather effects of the used image. This system is based on three parts: first, estimate the image model parameter, adjust haze effects, and finally embed the message. A new image steganography method was presented [26] that was used to enhance image transformation. This system is introduced a hybrid chaotic map, then represents a new shift operator to shuffle cover image pixel positions to improve the resistance against attacks. A multilevel cryptography method for cloud computing was proposed by Kumar et al. [27], where both DES and RSA methods are used to increase the security of the cloud storage. Kumar et al. [28] presented a new symmetric cryptography method depending on Caesar cipher, where the sender sends the hash code instead of the symmetric key. Nunna and Marapareddy [29] proposed a new system that used both cryptography and steganography techniques by using XOR operation to encrypt text and insert it into the image based on chosen key. A new application was proposed by Pizzolante et al. [30] that used to compress and encrypt a message or file, then sends it by using the standard SMS. Carpentieri et al. [31] proposed a novel steganographic method used for cloud-based data exchange, and this method used compressed archive as an information carrier.

2.1 DNA coding and operations

DNA contains four bases: A, T, C, and G, and two binary numbers are needed to represent the four bases, such as A (00), T (11), C (01), G (10), so there are different

representation methods. As we all know, A and T are complementary, and C and G are complementary. In the binary system, 00 and 11 are complementary. The pixel value of the image is between [0,255] and is composed of an eight-bit binary. Therefore, a single pixel is composed of four DNA bases. For example, for a pixel value of 155, the corresponding binary bit is "10011011", and the DNA sequence generated by the rule in the Table 1 is "GCGT".

Table 1. DNA coding rule

DNA BASE	Coding Rule
A	00
C	01
G	10
T	11

Table 2. Coding rules of the system

DNA BASE	DNA BASE Coding	Add 2 Zeros	Hexa Number	Make XOR
A	00	0000	B(1011)	1011
C	01	0100	D(1101)	1001
G	10	1000	E(1110)	0110
T	11	1100	F(1111)	0011

Image cryptography. The function of this phase is to encrypt standard color images with 2D and 3D as in the following proposed algorithm:

Proposed algorithm for encryption process:

Input original 2D or 3D image.
Begin:
Step 1. Convert each pixel from decimal to binary format, (8 binary bits).
Step 2. Assign every 2-binary bits according to the DNA BASES rules, as given in Table 2.
Step 3. Add 2-zero bits to the DNA binary string.
Step 4. Put (B, D, E, and F) hexadecimal numbers against the DNA BASES rules, as given in Table 2.
Step 5. Make XOR (hexadecimal number, new DNA binary string).
Step 6. Convert the result to decimal format.
Step 7. Apply for every converted number in its original location.
Step 8. Repeat the above steps until the last pixel, getting a new image.
Step 9. Generate (e-function matrix), as e-factor.
Step 10. Make math(new image, e-factor).
Output: Stego image…..End.

Figure 1 illustrates the the proposed algorithm for the encryption process.

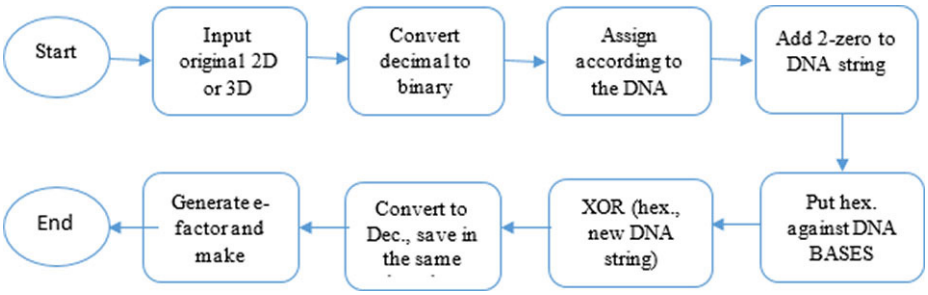

Fig. 1. The encryption algorithm

Image decryption. This phase care about the decryption process of the proposed system, as in the following algorithm:

Input: Stego image.
Begin:
Step 1. Make inverse Math. Operation with (new image, e-factor).
Step 2. Convert each pixel in (new image) to binary format.
Step 3. Make inverse XOR get the original DNA binary string.
Step 4. Remove the two added zeros from the DNA string.
Step 5. Rearrange the string of binary as in origin DNA bases rules.
Step 6. Convert DNA to decimal.
Step 7. Convert decimal to the original image.
Output: Origin 2D or 3D image….End.

Figure 2 shows the proposed algorithm of the decryption process.

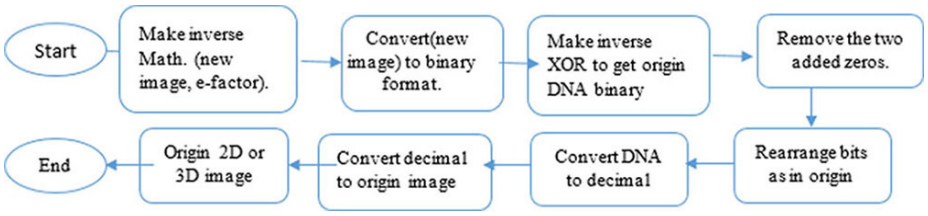

Fig. 2. Decryption algorithm

3 Experimental consequences

The consequences in this research depict that the proposed algorithm achieves important security protection with high-quality images by using DNA bases, XOR, and e-factor.

Figures 3 and 4, show the applying of work. Figure 3a and 3b represents the encryption process whereas the 1st line illustrates the origin images, while the 2nd and 3rd lines illustrate the resulting second and third stego images. Figure 4a and 4b represents

the decryption process whereas the first line depicts decrypted images, while the second and third lines show the reverse stages of image restoration. Finally, the origin image back to its first state in the third stage. The original images are visually completely identical to the causing stego images.Namely, the decoding algorithm worked efficiently to restore the images to their original state.

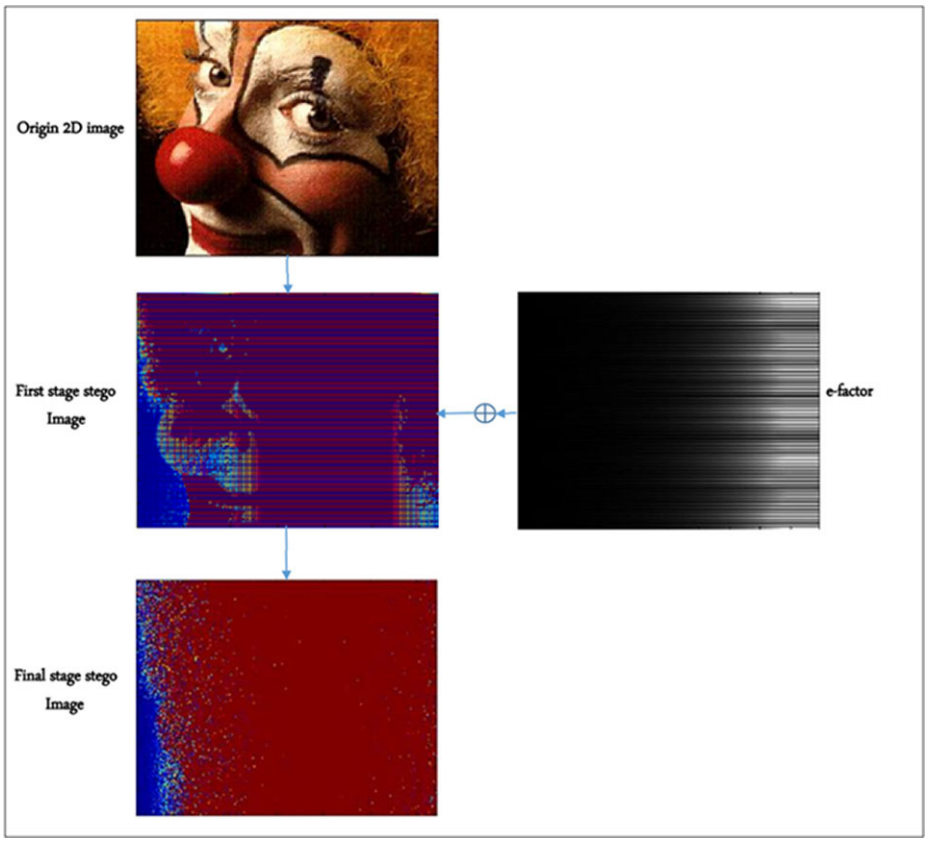

Fig. 3a. Encryption stages of 2D color image

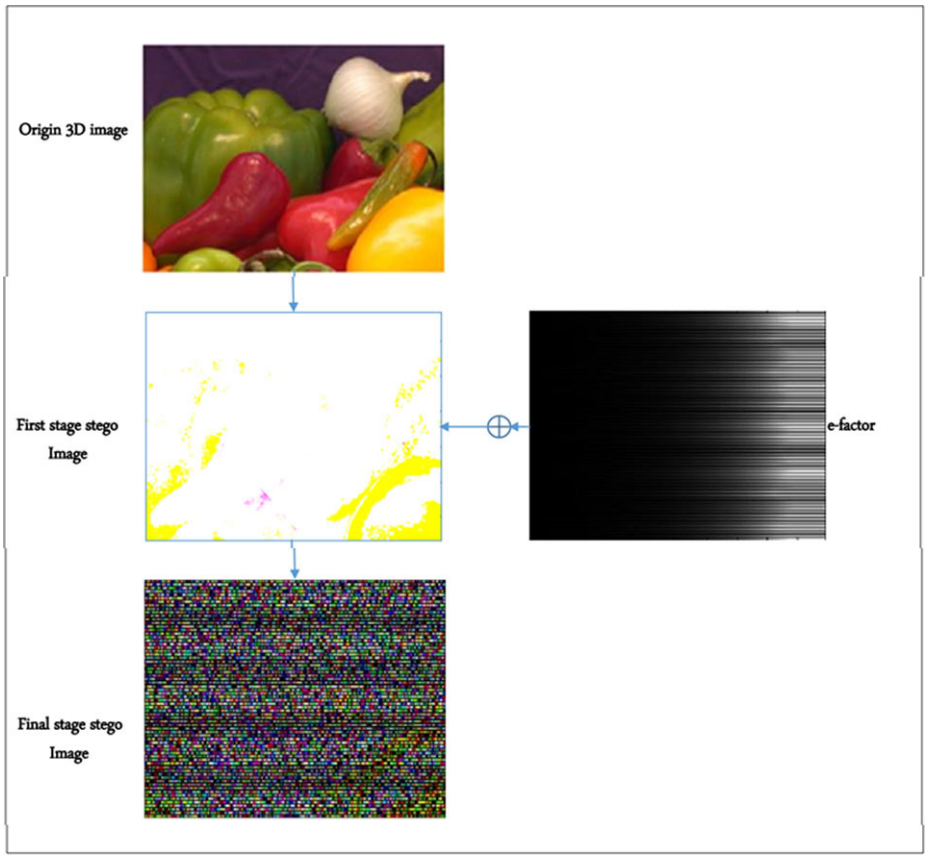

Fig. 3b. Encryption stages of 3D color image

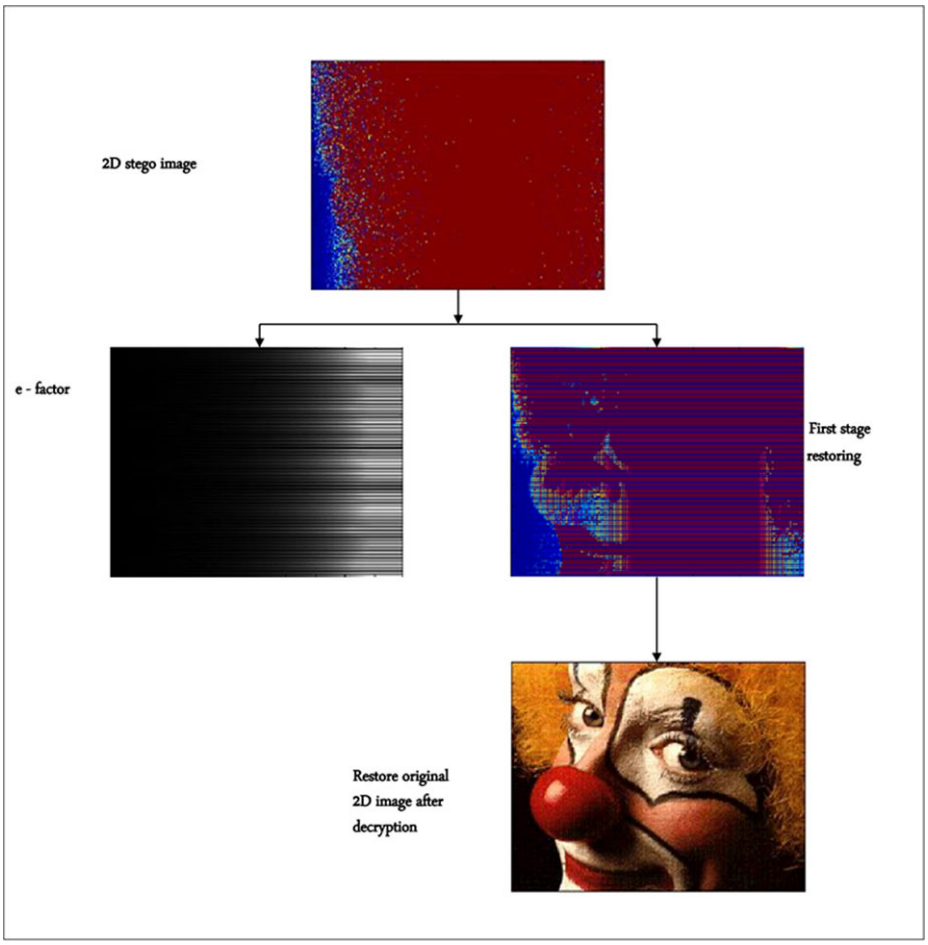

Fig. 4a. Decryption stages of 2D color image

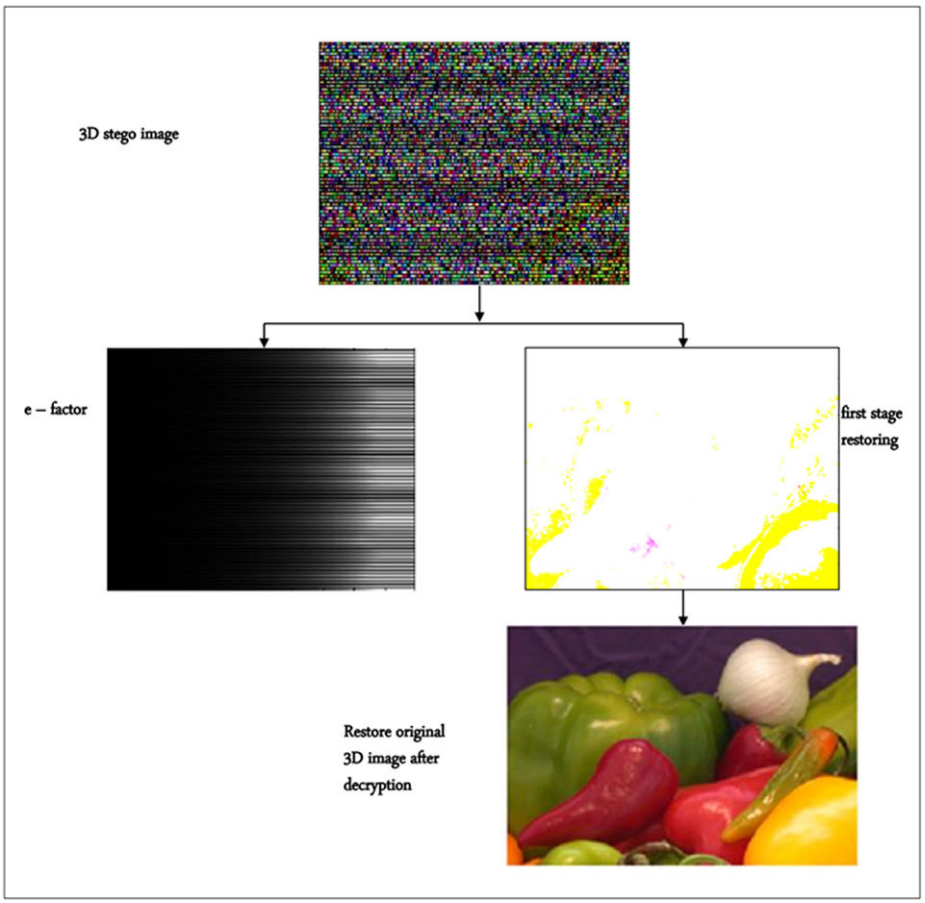

Fig. 4b. Decryption stages of 3D color image

4 Quality evaluation and accuracy measures

They denote the sort of measure used to compute the variation range between images following the application of these measures and encryption of the confidential image. Two widely used and significant metrics are used to demonstrate the image's quality prior to and following the encryption and decryption operations. They are as follows:

4.1 Mean square error (MSE)

The mean square error (MSE) quantifies the cumulative squared error (i.e., pixel deviations) between 2 images.

$$\text{MSE} = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} [c(i,j) - c(i,j)']^2 \quad (1)$$

Where: m and n the image dimensions and $c(i, j)$ the pixels of stego image.

4.2 Peak signal to noise ratio (PSNR)

PSNR can be used to determine the peak error. A greater PSNR indicates a higher image quality:

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

Where: R is the higher potential value of the pixel's densities.

Encoding and decoding times are also utilized as a performance evaluation.

Tables 3, 4 and 5 show the summary results of the work represented by numbers, as follow:

Table 3. MSE values after and before encryption

Origin Image	Size in (kb)	MSE	Decrypted Image	Size in (kb)	MSE
2D image (clown image)	128	30.023	2D image	44	19.4
3D image (pepper image)	140	33.92	3D image	96	21.15

Table 4. PSNR values after and before encryption

Origin Image	Size in (kb)	PSNR	Decrypted Image	Size in (kb)	PSNR
2D image (clown image)	128	29.105	2D image	44	10.348
3D image (pepper image)	140	35.089	3D image	96	12.749

Table 5. Time after and before encryption

Origin Image	Time of Encryption in (ms)	Time of Decryption in (ms)
2D image (clown image)	30.014	19.986
3D image (pepper image)	36.029	25.004

5 Conclusions

The proposed work concentrates to encrypt color images with 2D and 3D in multiple layers of encryption. The DNA is attributed to the pixel properties of the image. Thus this procedure makes it more secured. Obviously from the results, it was obtained the strong encryption of color images by using the DNA rule bases and the rest of the functions of the coded rules. Where these images were mathematically processed with the exponential function to increase encryption and obtain more secrets. It was noted too that the MSE and PSNR values of original images are more than that of encrypted

images, which means very good encryption because when (MSE and PSNR) are high values the distortion will be lower. It was cleared that Spending time on encryption and decryption explains that the encryption algorithm needs more time than the decryption algorithm. It is worth noting that the encrypted images are completely not similar to the original images, and the decoding algorithm returned the encrypted images to their previous era.

6 References

[1] W. Z. Khan, M. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah, "Industrial internet of things: Recent advances, enabling technologies and open challenges," *Computers Electrical Engineering,* vol. 81, p. 106522, 2020. https://doi.org/10.1016/j.compeleceng.2019.106522

[2] H. Salim and N. A. Jasim, "Design and implementation of smart city applications based on the internet of things," *International Journal of Interactive Mobile Technologies (iJIM),* vol. 15, no. 13, pp. 4–15, 2021. https://doi.org/10.3991/ijim.v15i13.22331

[3] H. AlRikabi, A. H. M. Alaidi, A. S. Abdalrada, and F. T. Abed, "Analysis of the efficient energy prediction for 5G wireless communication technologies," *International Journal of Emerging Technologies in Learning,* vol. 14, no. 8, pp. 23–37, 2019. https://doi.org/10.3991/ijet.v14i08.10485

[4] M. Bansal, M. Nanda, and M. N. Husain, "Security and Privacy Aspects for Internet of Things (IoT)," in *2021 6th International Conference on Inventive Computation Technologies (ICICT)*, 2021, pp. 199–204: IEEE. https://doi.org/10.1109/ICICT50816.2021.9358665

[5] H. TH and H. Tauma, "Enhanced data security of communication system using combined encryption and steganography," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[6] V. Signing, R. Mogue, J. Kengne, and M. Kountchou, "Dynamic phenomena of a financial hyperchaotic system and DNA sequences for image encryption," *Multimedia Tools Applications,* vol. 80, pp. 32689–32723, 2021. https://doi.org/10.1007/s11042-021-11180-9

[7] S. Arshad, J. Arshad, M. M. Khan, and S. Parkinson, "Analysis of security and privacy challenges for DNA-genomics applications and databases," *Journal of Biomedical Informatics,* vol. 119, p. 103815, 2021. https://doi.org/10.1016/j.jbi.2021.103815

[8] A. Ouannas and I. Aljazaery, "A new method to generate a discrete chaotic dynamical systems using synchronization technique," *Far East Journal of Dynamical Systems,* vol. 24, nos. 1–2, pp. 15–24, 2014.

[9] S. Najeeb, S. M. Ali, and H. Salim, "Finding the discriminative frequencies of motor electroencephalography signal using genetic algorithm," *TELKOMNIKA,* vol. 19, no. 1, pp. 285–291, 2021. https://doi.org/10.12928/telkomnika.v19i1.17884

[10] I. A. Aljazaery, H. T. S. Alrikabi, and M. R. Aziz, "Combination of hiding and encryption for data security," *International Journal of Interactive Mobile Technologies,* vol. 14, no. 9, pp. 34–47, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[11] M. Roy, S. Chakraborty, K. Mali, R. Swarnakar, K. Ghosh, A. Banerjee, and S. Chatterjee, "Data Security Techniques Based on DNA Encryption," in *International Ethical Hacking Conference*, 2019, pp. 239–249: Springer. https://doi.org/10.1007/978-981-15-0361-0_19

[12] M. Alruily, O. R. Shahin, H. Al-Mahdi, and A. I. Taloba, "Asymmetric DNA encryption and decryption technique for Arabic plaintext," *Journal of Ambient Intelligence Humanized Computing,* pp. 1–17, 2021. https://doi.org/10.1007/s12652-021-03108-w

[13] A. Al-zubidi, R. K. Hasoun, S. H. Hashim, and H. Alrikabi, "Mobile application to detect Covid-19 pandemic by using classification techniques: Proposed system," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 34–51, 2021. https://doi.org/10.3991/ijim.v15i16.24195

[14] M. Al-dabag, H. S. ALRikabi, and R. Al-Nima, "Anticipating atrial fibrillation signal using efficient algorithm," *International Journal of Online and Biomedical Engineering (iJOE),* vol. 17, no. 2, pp. 106–120, 2021. https://doi.org/10.3991/ijoe.v17i02.19183

[15] M. A. Iliyasu, O. A. Abisoye, S. A. Bashir, and J. A. Ojeniyi, "A Review of DNA Cryptograhic Approaches," in *2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA)*, 2021, pp. 66–72: IEEE. https://doi.org/10.1109/CYBERNIGERIA51635.2021.9428855

[16] A. Hazra, S. Ghosh, and S. Jash, "A review on DNA based cryptographic techniques," *International Journal of Network Security,* vol. 20, no. 6, pp. 1093–1104, 2018.

[17] A. S. Abdalrada, O. H. Yahya, A. H. M. Alaidi, N. A. Hussein, H. T. Alrikabi, and T. Al-Quraishi, "A predictive model for liver disease progression based on logistic regression algorithm," *Periodicals of Engineering and Natural Sciences,* vol. 7, no. 3, pp. 1255–1264, 2019. https://doi.org/10.21533/pen.v7i3.667

[18] B. Qi, C. Yang, L. Tan, X. Luo, and F. Liu, "A novel haze image steganography method via cover-source switching," *Journal of Visual Communication Image Representation,* vol. 70, p. 102814, 2020. https://doi.org/10.1016/j.jvcir.2020.102814

[19] N. A. Hikal and M. M. Eid, "A new approach for palmprint image encryption based on hybrid chaotic maps," *Journal of King Saud University-Computer Information Sciences,* vol. 32, no. 7, pp. 870–882, 2020. https://doi.org/10.1016/j.jksuci.2018.09.006

[20] R. Guesmi and M. B. Farah, "A new efficient medical image cipher based on hybrid chaotic map and DNA code," *Multimedia Tools Applications,* vol. 80, no. 2, pp. 1925–1944, 2021. https://doi.org/10.1007/s11042-020-09672-1

[21] S. Indora, "Cascaded DNA Cryptography and Steganography," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 104–107: IEEE.

[22] B. Akiwate and L. Parthiban, "A Dynamic DNA for Key-based Cryptography," in *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*, 2018, pp. 223–227: IEEE. https://doi.org/10.1109/CTEMS.2018.8769267

[23] P. Pavithran, S. Mathew, S. Namasudra, and P. Lorenz, "A novel cryptosystem based on DNA cryptography and randomly generated Mealy machine," *Computers Security,* vol. 104, p. 102160, 2021. https://doi.org/10.1016/j.cose.2020.102160

[24] R. Sushma, M. Namitha, G. Manjula, S. Johar, and G. Hiriyanna, "DNA based Steganography Using 2-3-3 Technique," in *2019 International Conference on Data Science and Communication (IconDSC)*, 2019, pp. 1–6: IEEE.

[25] F. Musanna, D. Dangwal, and S. Kumar, "Novel image encryption algorithm using fractional chaos and cellular neural network," *Journal of Ambient Intelligence Humanized Computing,* pp. 1–22, 2021. https://doi.org/10.1007/s12652-021-02982-8

[26] J. Sharafi, Y. Khedmati, and M. Shabani, "Image steganography based on a new hybrid chaos map and discrete transforms," *Optik,* vol. 226, p. 165492, 2021. https://doi.org/10.1016/j.ijleo.2020.165492

[27] N. C. S. N. Iyengar, G. Ganapathy, P. Mogan Kumar, and A. Abraham, "A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment," *International Journal of Grid Utility Computing,* vol. 5, no. 4, pp. 236–248, 2014. https://doi.org/10.1504/IJGUC.2014.065384

[28] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," *Signal Processing,* vol. 125, pp. 187–202, 2016. https://doi.org/10.1016/j.sigpro.2016.01.017

[29] K. C. Nunna and R. Marapareddy, "Secure Data Transfer Through Internet Using Cryptography and Image Steganography," in *2020 SoutheastCon*, 2020, vol. 2, pp. 1–5: IEEE. https://doi.org/10.1109/SoutheastCon44009.2020.9368301

[30] A. Castiglione, R. Pizzolante, F. Palmieri, A. De Santis, B. Carpentieri, and A. Castiglione, "Secure and reliable data communication in developing regions and rural areas," *Pervasive Mobile Computing,* vol. 24, pp. 117–128, 2015. https://doi.org/10.1016/j.pmcj.2015.04.001

[31] B. Carpentieri, A. Castiglione, A. De Santis, F. Palmieri, and R. Pizzolante, "Compression-based steganography," *Concurrency Computation: Practice Experience,* vol. 32, no. 8, p. e5322, 2020. https://doi.org/10.1002/cpe.5322

7 Authors

Asst. Prof. Ibtisam A. Aljazaery is presently on the faculty of Electrical Engineering Department, College of Engineering, University of Babylon. Babylon, Iraq. E-mail: ibtisamalasady@gmail.com. The number of articles in national databases – 10. The number of articles in international databases – 5.

Asst. Prof. Haider Th. Salim ALRikabi is presently one of the Faculty College of Engineering, Electrical Engineering Department, Wasit University in Al Kut, Wasit, Iraq. He received his B.Sc. degree in Electrical Engineering in 2006 from the Al Mustansiriya University in Baghdad, Iraq. His M.Sc. degree in Electrical Engineering focusing on Communications Systems from California State University/Fullerton/USA in 2014. His current research interests include Communications systems with the mobile generation, Control systems, intelligent technologies, smart cities, and the Internet of Things (IoT). Al Kut City-Hay ALRabee, Wasit, Iraq. E-mail: hdhiyab@uowasit.edu.iq. The number of articles in national databases – 15. The number of articles in international databases – 40.

Abdul Hadi M. Alaidi is a Asst. Prof. in the Engineering College, at the Wasit University, Iraq. His area of research focuses on algorithm and image processing.

Article submitted 2021-11-02. Resubmitted 2021-12-21. Final acceptance 2021-12-21. Final version published as submitted by the authors.