IRAQI Academic Scientific Journals
Samarra Journal of Pure and Applied Science
SJPAS
www.sjpas.com
p ISSN: 2663-7405
e ISSN: 2789-6838

Using DNA Algorithm to Hide a Compressed Ciphertext in Colored Image

Qusay Samir Alsaffar[1*]
1- Ministry of Higher Education and Scientific Research, Minister Office, Iraq

https://doi.org/10.54153/sjpas.2024.v6i2.910

Article Information
Received: 24/04/2024
Revised: 14/05/2024
Accepted: 25/05/2024
Published:30/06/2024

Keywords:
DNA, GZIP, Cryptography, Steganography, LSB, MSE, PSNR, SSIM, NPCR and UACI.

Corresponding Author
E-mail:
qusay_saffar@mohesr.gov.iq
Mobile:

Abstract

Cryptography is the fundamental key to keeping data that are more trusted for the increasing reliability in the digital community. Steganography is widely used to protect any hidden data in the media so that it may not get hacked. The conventional protection styles do not provide the requirements of cyber security under the new hacker's techniques that are applied for any hacking data and confidential information. Moreover, using the encryption algorithms without providing extra barriers alone could provide an opportunity to be breached therefore, boosting the levels of protection is really urgent to shield information against any intruders. This paper submits a proposed algorithm that can be applied to overcome the risks of hacking and increase the data protection. First, this algorithm uses the DNA to encrypt the data, which is then made complex by a multiplier and compressed by using the GZIP algorithm. The final stage is to hide the compressed data in the media (color image pixels) by using the LSB method. When applying these levels of protection, the amount of data compression becomes at 75%, and the image measures proves that good results are fulfilled, for instance, Lina sample measure is for SSIM = 1, PSNR = 67.6119, MSE = 0.0115, UACI = 7.00284 and NPCR = 0.01152. This algorithm contributes to increase the level of data protection in the communication between any parties to transfer certain confidential information.

Introduction:

Nowadays, securing any confidential information from getting breached become a crucial issue as there is a clear great evolving of information technology and huge growth in the use of internet applications such as military communication, IOT, and cloud systems, etc. Therefore, cyber security is required to keep the safety and confidentiality of the information. Researchers rely on submitting new ideas to improve the classic techniques and present new ones [1]. DNA encryption became a novelty in the field of cryptography and new researches adopted this significant technique because as it has a complex DNA pattern, which is different from the traditional computer digital representation (0,1), DNA bases (Adenine A, Cytosine C, Guanine G, and Thymine T) are used to encrypt and store the data. Thus, the sender can compose any DNA base format to provide an advanced encryption algorithm and add more strength to the security level [2].

The combination of two algorithms (Huffman coding and the LZ77) introduced the DEFLATE algorithm as the GZIP file format, and various data types can be compressed by using GZIP which reduces the system usage [3]. In 1993, the first version of the algorithm was presented, and then, the DEFLATE algorithm was widely used [4]. The DEFLATE algorithm can be applied in many applications such as (.xlsx, .docx, .pptx, and PDFs) [5].

Steganography technique can achieve hiding confidential data (bits) in images without having a third-party realize it to have happened, by replacing these bits with image pixel bits. Least Significant Bit (LSB) is used in image steganography for hiding the data to increase and boost the algorithm's strongness; therefore, it strengthens and shields the algorithm's effectiveness.

To provide robustness in secret data communication, cryptography, and steganography are applied to secure the data before sending it to a second party, and thus the information is more confident when using this technique [1,6,7].

Cryptography is linked to the topics of analysis and design of cryptographic models and plans that allocate secret connections over unsecured media. Secure communication is to be available in media is considered a main traditional problem in cryptography. Robust algorithms have to be developed to overcome this dilemma. The proposed algorithm provides a robust model that protects the information during transmission to the destination. The first party converts the plaintext characters to ASCII numbers, then converts the ASCII numbers into the binary style. The DNA bases (A, G, C, and D) are applied to the binary text in the next stage, and then the DNA text is converted to ASCII numbers, then the complexity of the encryption algorithm is increased by multiplying the result by a positive number, then GZIP algorithm is employed to compress the encrypted text. Finally, the LSB technique is applied to embed the ciphertext into a colored covered. The second party extracts the ciphered text from the image media and applies the inverted steps (the decrypted algorithm).

This method can contribute to communication between the intelligence agencies or military issues that depend on the security of their information to send urgent messages and therefore the support the cybersecurity of these institutions is achieved. An urgent message can be sent from clients after is it encrypted and hidden in an image when an event threat is related to the security of a country. Security authorities analyze and extract the message from the image and take the necessary measures to deter any security threat.

Deter squads like (land, sea and air forces) implement defense missions and exchange information securely by receiving encrypted messages and their ability to send them. As a result, security authorities can communicate information securely and quickly through such system and send information to the pertinent by this method.

This paper is structured as follows: Section 2 provides an overview of the relevant works. Section 3 presents DNA cryptography. Section 4 defines the GZIP technique. The image steganography is described in section 5. Section 6 explains the proposed algorithm. Section 7 presents fidelity measures. Section 8 discusses the experimental results. The last section reveals the conclusions.

Related Works

A Blowfish encryption algorithm was applied by Pujari and Shinde to encrypt a text [8]. Then LSB steganography technique was applied to hide the ciphered text in the cover image. The Blowfish algorithm utilizes a variable key length and is usually a symmetric block cipher.

Dhamija and Dhaka put a secure planner for data communication in the cloud system [9]. SCMACS is the proposed method where 1st complement is used. It depends on the concept of a symmetric key where data is encrypted and decrypted by sharing the same key at both ends. This method used LSB in the steganography stage.

K. S. Sajisha and S. Mathew proposed a triple layer security algorithm. They encrypted any message by providing DNA bases, and then they applied the AES algorithm, the last stage is when they hid the encrypted message into another DNA sequence [10].

M. Sabry, and M. Hashem, proposed an algorithm that applies the DNA bases and AES encryption. The algorithm was developed by adding the DNA instead of bits. This aims at demonstrating the ability to build a sophisticated paradigm that depended on DNA bases, and that makes it appropriate for implementation on DNA computers [11].

A. Khalifa and A. Atito [12], made their efforts to convert the plain text to ciphertext when they employed DNA and Playfair. An adjustment exchange algorithm was used to conceal the data in some DNA references to expand the hiding power, stronger concealment than the main exchange method was achieved.

An algorithm presented by Das and N. Kar [13], states that the data is protected by using two layers of security with two layers of media for covering the ciphertext. The type of cover is DNA bases and images. The image is used to construct the DNA by using a 2D logistic map. The degenerate genetic code substitution is needed to conceal the secret data in the DNA, and the output DNA is again hidden in the image.

Mohaisen, H. N. and Hammoudb, A. K., proposed three approaches to a modified RSA algorithm, then they concealed ciphertext in the colored image by using LSB, and they chose a pixel from the image in a random way. They produce the algorithm to secure information from third party attacks [14].

Mohaisen, H. N. and others, proposed a method for hide information in video stream, this method consists of five stages, first they convert video into parts, second, they select a part randomly, third convert the part to digital form and split it to (R G B), fourth encrypt the text by using RSA algorithm, lastly, they concealed the ciphertext into the part [15].

DNA Cryptography

DNA format is represented by four bases (Adenine (A), thymine (T), cytosine (C), and guanine (G)), that are used to carry information [2,16]. The storage capacity of DNA is tremendous, A gram can store 10^{21} of it, which is equivalent to 10^{8} terabytes, so, where a gram can store a tremendous quantity of data inside DNA. Cryptography with DNA was encouraged based on the properties and advantages that DNA could provide. The technique of DNA bases is arranged in a random way and the bits of secret data are stored based on these bases. This

majestic technique is the key security model for the novel cryptographic systems. It should develop and support the traditional encryption techniques. In the mathematical aspect of DNA, the concept of DNA chemistry is substituted by the technique of DNA cryptography, so, the latter technique is unbreakable by traditional methods, and is more secure. Plaintext is converted to ASCII, and then to a binary format, and lastly to DNA by using the ATCG bases. The DNA bases and their reverses in a binary form are shown in (Table 1). The bases ATCG can be used freely in millions of sequences. So, the opportunity to discover the right arrangement is rather impossible [17].

Table 1: DNA Cryptographic bases and binary form

Bits	00	01	10	11
DNA Base	A	T	G	C

GZIP Technique

The increasing demands on compression technology led to the creation of GUNZip (GZIP) to address these requirements. A compression algorithm such as LZW and others, were replaced by the free utility GZIP. The GZIP algorithm was produced by combining two algorithms (LZ77 and Huffman) and were based on the DEFLATE algorithm. In the GZIP algorithm, the data is kept without losing [3].

Lz77 Algorithm

The GZIP algorithm compresses data by finding duplicate strings. The repeated string is replaced by a pointer that points to the first string. This algorithm uses the name (sliding window), where any special location of data is saved. The 32K sliding window is moved for compression and decompression of the last 32768 symbols are recorded to express what they were. If the content of the sliding window matches with the next string of symbols, the letter is replaced by distance and length, distance means the length back to the window where the string started, and the length is the number of symbols that the string identical [18].

Huffman Coding

This algorithm encloses the data without any shortage. To add different characters, this algorithm allocates a variable length of codes. The algorithm decides the length of the code based on the repeated characters. The longer codes depend on the least number of repeating symbols; however, the shorter ones depend on the highest number. The Huffman algorithm consists of two parts, the first of which creates a Huffman tree, and the second one searches for codes by going through the tree. For example, in the DNA ciphertext “CCCGAACCA”, where the character C appears more frequently than the A one and character G appears less frequently, thus code C of is the shortest length, and code A is longer than code C, while G is the longest one [19].

Image Steganography

Steganography is employed to hide ciphertext in a natural image that appears normal to humans. The natural image is converted into a digital one of matrix numbers by image processing. The image pixel intensity is controlled by image numbers. The pixel in a grayscale image has a size of 8 bits, so each pixel is represented by 256 intensity values. The color (RGB) image pixel contains 24 bits, and this means that each pixel contains approximately 16.7 million colors for a cube of 256. The image changes are difficult to be recognized by the Human Vision System (HVS) as a small modification is made in the pixel density and is still difficult to detect and display normally. The Least Significant Bit (LSB) is employed for steganography and is considered a valuable algorithm. The LSB algorithm is done by swapping the 8th least significant bit of the original pixel with the cipher text bits. This process is implemented after converting the cipher text into binary form [20].

THE Proposed Algorithm

The first-party algorithm is in two parts, encryption and steganography, just for providing a security model, The first part performs three procedures, the first one of which applies the DNA technique to encrypt the data, the second one is the multiplication by a positive number, while the third procedure uses the GZIP algorithm to compress the data. The second part applies LSB steganography to get a color image.

The algorithm at the second party is divided into two parts, the first one of which is to get the data out from the image, While the second one decrypts the ciphertext as follows, the first procedure is decompression by using the GZIP algorithm, the second one divides the result by the positive number, and the third procedure is the conversion to plain text from DNA.

First Party

Begin
Step 1: Input confidential data, and an original image cover.
Step 2: The output is confidential data embedded into a steganography image.
Step 3: Convert confidential data to a ASCII form.
Step 4: Convert ASCII form to a binary form.
Step 5: Convert the data from binary form to DNA according to Table I.
Step 6: Convert DNA bases to a ASCII form.
Step 7: ASCII * positive number.
Step 8: Data is compressed by applying the GZIP technique.
Step 9: Select the cover image to apply the steganography.
Step 10: For each pixel from the cover image do
Step 11: Get R, G, and B of the image pixel
Step 12: Assign 0 to R, G, and B for the LSB
Step 13: End for
Step 14: For each symbol of the ciphertext do
Step 15: Hide 8 bits of the symbol in the LSB of R, G, and B in the contiguous pixels.
Step 16: After hiding all message, add a pointer that refers to the last pixel where the last digit is hiding on it.
Step 17: End for
End

Second Party

Begin

Step 1: Input the image that embeds the ciphertext.

Step 2: Output plaintext.

Step 3: Find the pointer.

Step 4: For each extracted pixel do

Step 5: Get the LSB of the pixel, extract the 8 bits, and then get all the ciphertext.

Step 6: End for

Step 7: Convert to ASCII by applying The GZIP decompression algorithm.

Step 8: ASCII / positive number

Step 9: Convert ASCII number to DNA bases.

Step 10: Convert DNA to a binary form then, to decimal one.

Step 11: Convert decimal form to the plain text.

End.

(Fig. 1 and Fig. 2) show the proposed algorithms

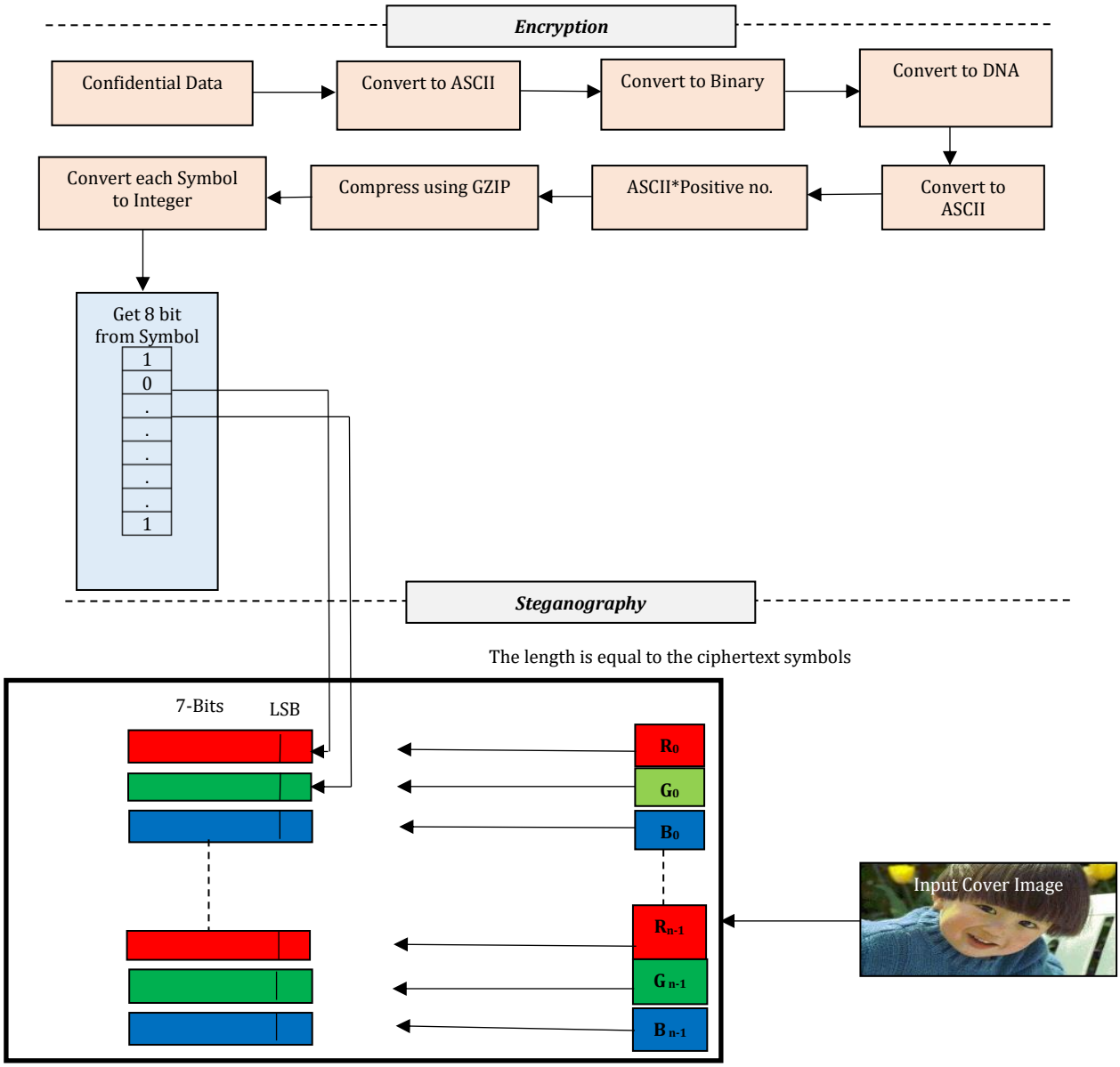


Fig. 1 First party algorithm.

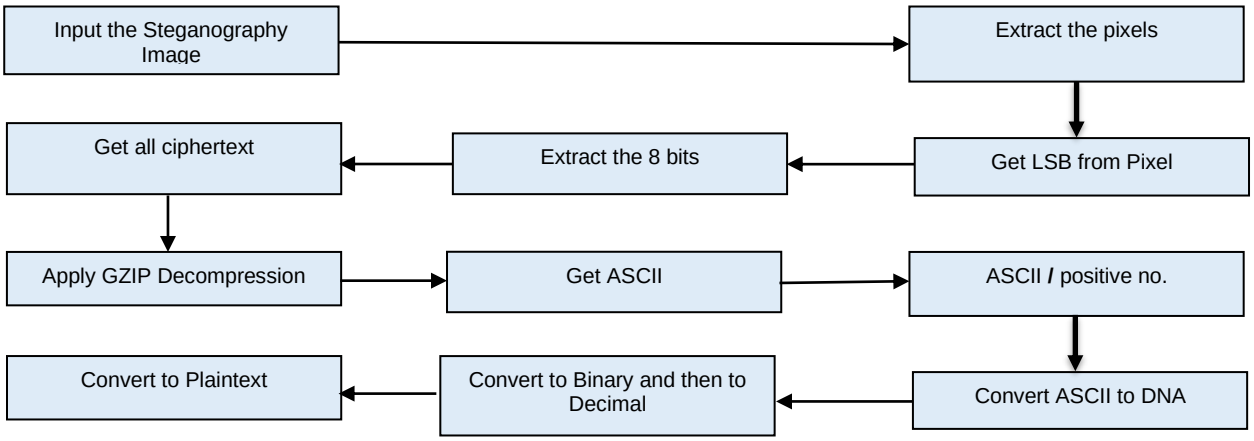


Fig. 2 Second party algorithm.

Fidelity Measures

The contrast between the original image and the steganography one can be estimated by using the fidelity measures.

Mean Square Error (MSE)

Differences in pixels (cumulative squared error) are depicted by using the mean squared error [21] as follows:

$$MSE=\frac{1}{xy}\sum_{i=1}^{x}\sum_{j=1}^{y}[m(i,j)-n(i,j)]^2 \qquad (1)$$

The image dimensions are represented by x and y, The original pixels of the image are m(i,j), and the steganography image pixels are n(i,j).

Peak Signal to Noise Ratio (PSNR)

The peak error can be calculated by using PSNR, a higher value implies better quality of the image [22,23], as follows:

$$PSR=10\log_{10}\frac{R^2}{MSE} \qquad (2)$$

The pixel density that represents the maximum possible values is R.

Structural Similarity Index Measure (SSIM)

SSIM provides a suitable comparison between MSE and PSNR. It is considered a powerful way of evaluating the visual correlation of the images [24]:

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+n_1)(2\sigma_{xy}+n_2)}{(\mu_x^2+\mu_y^2+Cn_1)(\sigma_x^2+\sigma_y^2+n_2)} \qquad (3)$$

The average intensity is μ, the standard deviation is σ, n_1, and n_2 are greater than zero and must be constants. They avoid instability when other parameters are close to zero, and the remaining parameters are close to 0.

Number of Pixels Change Rate (NPCR) and the Unified Averaged Changed Intensity (UACI)

NPCR and UACI are employed to evaluate the deficiency and robustness between the original and encrypted image by evaluating the pixel density [25]:

$$NPCR=\frac{\sum_{i.j=1}^{N*M} D(i,j)}{N*M}*100\% \quad (4)$$

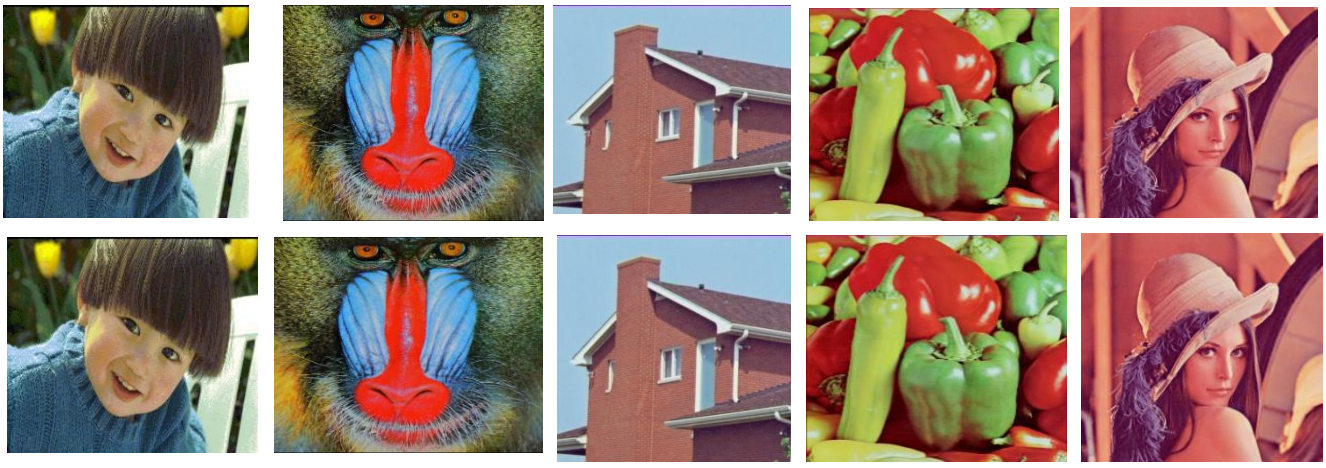
$$D(i,j)=\begin{cases}0\ if\ n1(i,j)=n2(i,j)\\1\ if\ n1(i,j)\neq n2(i,j)\end{cases} \quad (5)$$

$$UACI=\frac{1}{N*M}\left[\sum_{i,j=1}^{N*M}\frac{|n1(i,j)-n2(i,J)|}{Max(n2)}\right]*100\% \quad (6)$$

n_1 and n_2 are the original and encrypted image respectively, i and j are pixels, and N and M are the size of the image.

THE Experimental Result

The performance of the proposed method in this part is determined by the experimental results. The MATLAB platform was exploited for implementation, and the BMP and PNG types were utilized as cover images. The using of DNA and GZIP algorithms with some techniques (result multiplication) demonstrates that the proposed algorithm has made important security advances with producing high image quality. (Fig. 3) explains the proposed algorithm, where the cover images are indicated by the top line of this figure, while stego images containing the ciphertext are indicated by the lower line. The visual appearance of this figure shows that the two groups of images are identical, this means that the algorithm does not include discoverable defects as a result of hiding information.



Boy Mandrill House Peppers Lina

Fig. 3 Sample of experimental results.

In this figure four compressed messages are tested; the length of these messages are: 40, 54, 74, and 103 characters. The analysis results of the proposed algorithm are shown in (Fig. 4 and Fig. 5):

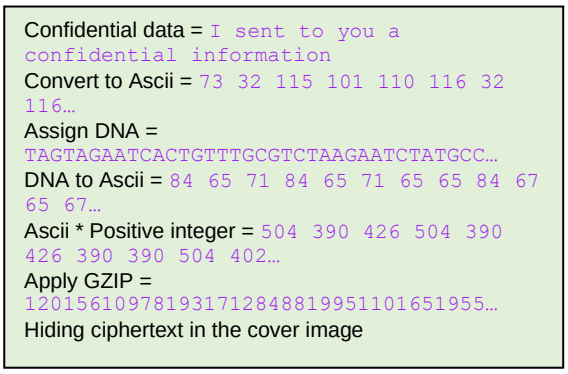


Fig. 4 First party algorithm analysis.

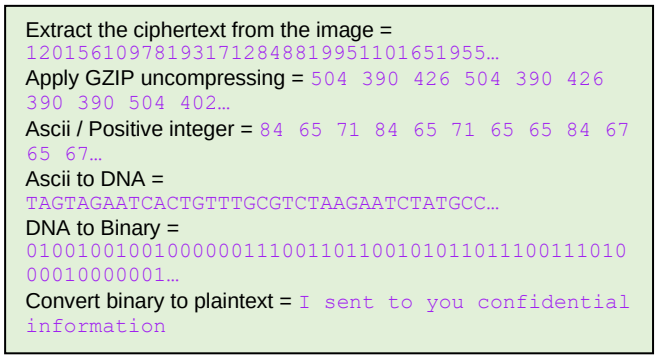


Fig. 5 Second party algorithm analysis.

The minimum MSE value indicates that the error is low. When the SSIM value is close to one and the PSNR value is high, then they indicate fewer defects and good image quality.

The PSNR and MSE results are shown in Table 2 when different lengths of secret text are used. SSIM = 1 for all texts.

Table 2: The values of PSNR, MSE

Number of Characters				PSNR					MSE				
Original Text	Apply DNA	Apply GZIP	Compression Rate	Mandrill	Peppers	Lena	Boy	House	Mandrill	Peppers	Lena	Boy	House
40	142	98	34%	67.7827	67.4754	67.6119	67.7132	68.5868	0.0106	0.0123	0.0115	0.0113	0.0082
54	213	113	49%	66.8696	66.2486	66.6419	66.5428	67.4849	0.0123	0.0151	0.0135	0.0138	0.0118
74	293	127	54%	66.2771	65.7259	65.7571	65.8316	66.8254	0.0158	0.0173	0.0168	0.0165	0.0131
103	303	171	75%	65.4162	64.8753	64.9765	64.6458	65.9612	0.0181	0.0213	0.0213	0.0211	0.0163

NPCR and UACI are used to estimate the encryption ratio of the images, when the high value of NPCR and low value of UACI are got, this indicates that the image is completely encrypted. In this paper high image quality is used, so the low value of NPCR and the high value of UACI are needed to be obtained. The NPCR and UACI results are shown in Table 3 when different lengths of secret text are used.

The RGB histograms of the original image and the steganography image are shown in (Fig. 6) as follows:, the top line of this figure indicates the original image, while the stego image is indicated by the lower line. The two lines indicate that there is a significant similarity between the two of them.

The time complexity of the encryption algorithm (message length 103 char.) can be computed as follows:

- The conversion of confidential data to ASCII form is 0.000121 seconds.
- The conversion of ASCII to binary form is 0.004688 seconds.
- ASCII*Positive number is 0.000403 seconds.
- Data compression by applying the GZIP technique is 0.006502 seconds.
- While the execution time for the entire encryption algorithm is 0.015412 seconds. (Fig. 7) presents the execution time of algorithms

Table 3: The values of NPCR and UACI

Number of Characters				NPCR					UACI				
Original Text	Apply DNA	Apply GZIP	Compression Rate	Mandrill	Peppers	Lena	Boy	House	Mandrill	Peppers	Lena	Boy	House
40	142	98	34%	0.01061	0.00821	0.01152	0.01127	0.00816	4.20571	3.25427	4.55178	4.45304	3.62716
54	213	113	49%	0.01234	0.01484	0.01345	0.01380	0.01183	5.24654	6.24571	5.71180	5.83586	4.67232
74	293	127	54%	0.01463	0.01732	0.01675	0.01647	0.13846	6.17367	7.22734	7.00284	6.87365	5.47816
103	303	171	75%	0.01817	0.02176	0.02126	0.02101	0.01601	7.52261	8.56861	8.37180	8.24023	6.67184

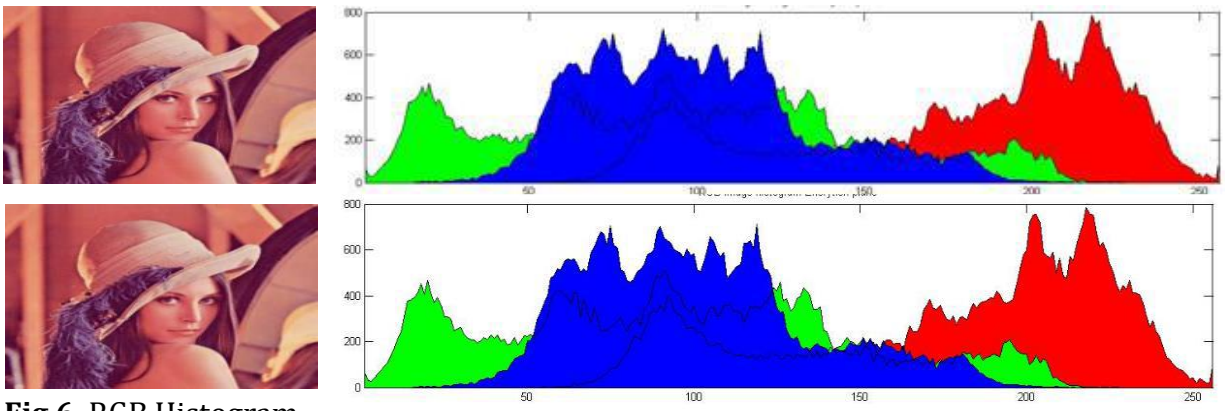


Fig 6. RGB Histogram.

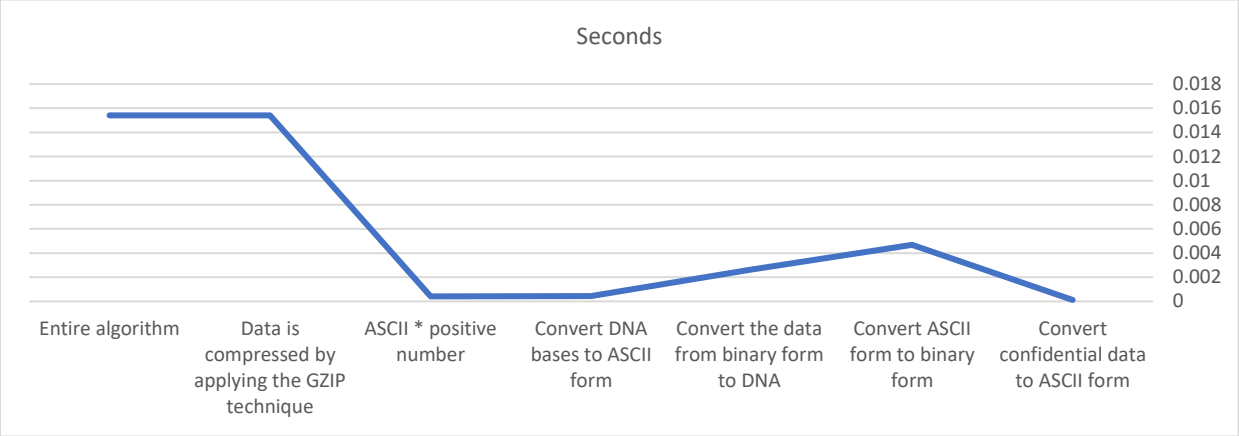


Fig. 7 The algorithm execution time for the message length of 103 characters.

Conclusion

The algorithm used encryption and steganography to get better security results and hybridized them through DNA algorithm and GZIP compression. The GZIP algorithm compresses the size of the ciphertext and the outputs are the amplification process after applying the DNA algorithm to boost the algorithm and enhance steganography. Performing a cryptanalyst inspection becomes very difficult and complex when the algorithm is supported by multiplying the DNA by a positive number, and thus enhancing the security of the system, and using an RGB for hiding the ciphertext in it by using LSB to complicate the problem for the hacker. The ideal values for MSE are close to zero, while the ideal values for PSNR are close to 100, and the ideal ones for SSIM are close to 1. The low values of NPCR and high values of UACI indicate a considerable similarity between the original image and the steganography image. Tables 2 and Table 3 show that the values are excellent, where the high match is confirmed by the histogram between the original and the steganography images. The presented method gives a positive impact by using encryption, compression, and data hiding to provide a robust algorithm with less faults and good vision quality.

References

1. Bahaddad, A. A., Almarhabi, K. A., & Abdel-Khalek, S. (2023). Image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption. *Alexandria Engineering Journal*, (Vol. 75, pp. 41-54). https://doi.org/10.1016/j.aej.2023.05.051

2. Şatir, E., & Kendirli, O. (2022). A symmetric DNA encryption process with a biotechnical hardware. *Journal of King Saud University - Science*, 34(3). 101838. https://doi.org/10.1016/j.jksus.2022.101838

3. Jumar, R., Maaß, H., & Hagenmeyer, V. (2018). Comparison of lossless compression schemes for high rate electrical grid time series for smart grid monitoring and analysis. *Computers & Electrical Engineering*, (Vol. 71, pp. 465-476). https://doi.org/10.1016/j.compeleceng.2018.07.008

4. Das, S. K., & Rahman, M. Z. (2022). A secured compression technique based on encoding for sharing electronic patient data in slow-speed networks. *Heliyon*, 8(10). https://doi.org/10.1016/j.heliyon.2022.e10788

5. Kim, Y., Choi, S., Jeong, J., & Song, Y. H. (2019). Data dependency reduction for high-performance FPGA implementation of DEFLATE compression algorithm. *Journal of Systems Architecture*, (Vol. 98, pp. 41-52). https://doi.org/10.1016/j.sysarc.2019.06.005

6. AbdelWahab, O. F., Hussein, A. I., Hamed, H. F. A., Kelash, H. M., & Khalaf, A. A. M. (2021). Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data. *Procedia Computer Science*, (Vol. 182, pp. 5-12). https://doi.org/10.1016/j.procs.2021.02.002

7. Kordov K., & Zhelezov, S. (2021). Steganography in color images with random order of pixel selection and encrypted text message embedding. *PeerJ Computer Science*, (Vol. 7, e380). https://doi.org/10.7717/peerj-cs.380

8. Pujari, A. A., & Shinde, S. S. (2016). Data Security using Cryptography and Steganography. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 18(4), 130-139. doi:10.9790/0661-180405130139

9. Dhamija, A., & Dhaka, V. (2015). A novel cryptographic and steganographic approach for secure cloud data migration. *International Conference on Green Computing and Internet of Things (ICGCIoT), India, IEEE 2015* (pp. 346-351). doi: 10.1109/ICGCIoT.2015.7380486

10. Sajisha, K. S., & Mathew, S. (2017). An encryption based on DNA cryptography and steganography. *International Conference of Electronics, Communication and Aerospace Technology (ICECA), India* 2017 (pp. 162-167). doi: 10.1109/ICECA.2017.8212786

11. Sabry, M. , Hashem, M., Nazmy, T. & Khalifa, M. E. (2015). Design of DNA-based Advanced Encryption Standard (AES). *2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS), Egypt* (pp. 390-397). doi: 10.1109/IntelCIS.2015.7397250

12. Khalifa A., & Atito, A. (2012). High-capacity DNA-based steganography. *2012 8th International Conference on Informatics and Systems (INFOS), Egypt* (pp. 76-80). https://api.semanticscholar.org/CorpusID:2105884

13. Das, P., & Kar, N. (2014). A DNA based image steganography using 2D chaotic map. *2014 International Conference on Electronics and Communication Systems (ICECS), India* (pp. 1-5). doi: 10.1109/ECS.2014.6892654

14. Mohaisen, H. N., & Hammoudb, A. K. (2021). Application of modify RSA cryptography and randomly LSB steganography on color images of fluid flow in a channel. *International Journal of Nonlinear Analysis and Applications*, 12(2), 1725-1734. doi: 10.22075/ijnaa.2021.5312

15. Mohaisen, H.N., Mohammed, Q. M., & Mustafa H. N. (2024). Hiding secret data in color video applying modify RSA for cryptography with randomly select frame and pixel to steganography. *Journal of Natural and Applied Sciences*, 1(5), 193-206. DOI:10.59799/APPP6605

16. Abdullatif, A., Abdullatif F. A., & Naji, S. A. (2019). An enhanced hybrid image encryption algorithm using Rubik's cube and dynamic DNA encoding techniques. *Periodicals of Engineering and Natural Sciences*, 7(4), 1607-1617. doi: 10.21533/pen.v7i4.885

17. Fernandes, M., Decouchant, J. & Couto, F. M. (2023). Chapter Two - Security, privacy, and trust management in DNA computing. *Advances in Computers*, (Vol. 129, pp. 39-81). https://doi.org/10.1016/bs.adcom.2022.08.009

18. Sitaridi, E., Mueller, R., Kaldewey, T., Lohman, G., & Ross, K. A. (2016). Massively-Parallel Lossless Data Decompression. *2016 45th International Conference on Parallel Processing (ICPP), USA* (pp. 242-247). doi: 10.1109/ICPP.2016.35

19. O'Shaughnessy, S., & Breitinger, F. (2021). Malware family classification via efficient Huffman features. *Forensic Science International: Digital Investigation.* (Vol. 37, p. 301192). https://doi.org/10.1016/j.fsidi.2021.301192

20. Ye , G., Wu , H., Jiao, K., & Mei, D. (2021). Asymmetric image encryption scheme based on the Quantum logistic map and cyclic modulo diffusion. *Mathematical Biosciences and Engineering*, 18(5), 5427-5448. doi: 10.3934/mbe.2021275

21. Taqi, I. A., & Hameed, S. M. (2020). A new beta chaotic map with DNA encoding for color image encryption. *Iraqi Journal of Science*, 61(9), 2371–2384. doi: https://doi.org/10.24996/ijs.2020.61.9.24

22. Houas, A., Mokhtari, Z., Melkemi, K. E., & Boussaad, A. (2016). A novel binary image encryption algorithm based on diffuse representation. *Engineering Science and Technology, an International Journal*, 19(4), 1887-1894. https://doi.org/10.1016/j.jestch.2016.06.013

23. Thakur, R.S., Chatterjee, S., Yadav, R.N., & Gupta, L. (2023). Nature-Inspired DBN based Optimization Techniques for Image De-noising. *Intelligent Systems with Applications*, (Vol. 18, p.200211). https://doi.org/10.1016/j.iswa.2023.200211

24. Omara, A. N., Salem, T. M., Elsanadily, S., & Elsherbini, M. M. (2022). SSIM-based sparse image restoration. *Journal of King Saud University-Computer and Information Sciences*, 34(8), 6243-6254. https://doi.org/10.1016/j.jksuci.2021.07.024

25. Rehman, M. U., Shafique, A., Khan, K. H., & Hazzazi, M. M. (2023). Efficient and secure image encryption using key substitution process with discrete wavelet transform. *Journal of King Saud University-Computer and Information Sciences*, 35(7), 101613. https://doi.org/10.1016/j.jksuci.2023.101613

IRAQI Academic Scientific Journals
Samarra Journal of Pure and Applied Science
SJPAS
مجلة سامراء للعلوم البحتة والتطبيقية
www.sjpas.com
p ISSN: 2663-7405
e ISSN: 2789-6838

استخدام خوارزمية الحامض النووي لإخفاء نص مشفر مضغوط في صورة ملونة

قصي سمير شاكر الصفار[1]*
1- وزارة التعليم العالي والبحث العلمي، مكتب الوزير، العراق

معلومات البحث:
تأريخ الاستلام:
تاريخ التعديل :
تأريخ القبـــول:
تاريخ الـنشر:
الكلمات المفتاحية:
الحامض النووي، ضغط البيانات GZIP، التشفير، إخفاء المعلومات، البت الاقل أهمية، متوسط مربع الخطأ، ذروة الإشارة إلى نسبة الضوضاء، قياس مؤشر التشابه الهيكلي، معدل تغيير عدد البكسل (NPCR) ومتوسط الكثافة المتغيرة الموحدة (UACI)

الخلاصة:
يعد التشفير هو المفتاح الأساسي للحفاظ على البيانات وجعلها اكثر موثوقية في المجتمع الرقمي. يُستخدم إخفاء المعلومات على نطاق واسع لحماية البيانات المخفية في الوسائط حتى لا يتم اختراقها. لا توفر أساليب الحماية التقليدية متطلبات الأمن السيبراني في ظل تقنيات القرصنة الجديدة المطبقة لقرصنة البيانات والمعلومات السرية. علاوة على ذلك، فإن استخدام خوارزميات التشفير وحدها دون توفير حواجز إضافية قد توفر فرصة للاختراق، وبالتالي فإن تعزيز مستويات الحماية أمر ملح حقًا لحماية المعلومات ضد المتسللين. تقدم هذه الورقة خوارزمية مقترحة يمكن تطبيقها للتغلب على مخاطر القرصنة وزيادة حماية البيانات. أولاً، تستخدم هذه الخوارزمية تقنية الحامض النووي لتشفير البيانات، والتي يتم بعد ذلك تعقيدها بواسطة المضاعف وضغطها باستخدام خوارزمية GZIP. المرحلة النهائية هي إخفاء البيانات المضغوطة في الوسائط باستخدام طريقة LSB. عند تطبيق هذه المستويات من الحماية يصبح مقدار ضغط البيانات 75%، وباستخدام خوارزميات اختبار الصورة تم الحصول على مستويات جيدة من الحماية.

معلومات المؤلف
الايميل: qusay_saffar@mohesr.gov.iq
الموبايل: