Wasit Journal of Engineering Sciences

Journal homepage: https://ejuow.uowasit.edu.iq

An encryption by using DNA algorithm for hiding a compressed message in Image

Qusay S. Alsaffar

Affiliations
Ministry of Higher Education and Scientific Research, Minister Office, Baghdad, Iraq
Email: qusay_saffar@mohesr.gov.iq

Received
5-Novemebr-2021
Revised
18-December-2021
Accepted
10-January-2022
Doi: 10.31185/ejuow.Vol10.Iss1.249

Abstract
Cryptography is the main item to generate confidence and empower services in the digital technology, while Steganography has vastly expanded in digital medias. The using of traditional protection methods does not meet the requirements of data protection in light of development hackers techniques to breach it, in addition to use encryption algorithms without shielding may not secure the data, and it has become necessary to strengthen information security in new ways by providing several levels of protection.

A proposed algorithm is used to overcome of these challenges, it encrypts a message by using DNA encryption algorithm, then multiply the output by a factor then compress the multiplying message by using GZIP algorithm, the last stage is hiding a compressed message in (LSB) image pixels. The ratio of data compression is up to 75%. when combining these technologies, a good results have been obtained for instance the cover image of House sample result is (SSIM (Structural Similarity Index Measure) is equal 1, PSNR (Peak Signal to Noise Ratio) is equal 68.2827, MSE (Mean Square Error) is equal 0.0028, UACI (The Unified Averaged Changed Intensity) score is 4.59072 and NPCR (Number of Pixels Change Rate) score is 0.00383). This work contributes to reducing the risk of information breach when sending and receiving confidential information between parties.

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

الخلاصة: التشفير هو العنصر الرئيسي لتوليد الثقة وتمكين الخدمات في التكنولوجيا الرقمية بينما توسعت إخفاء المعلومات بشكل كبير في الوسائط الرقمية. ان استخدام طرق الحماية التقليدية لا توفي بمتطلبات حماية البيانات في ظل تطور طرق المتسللين من اختراقها بالإضافة الى استخدام خوارزميات التشفير وحدها قد لا تؤمن البيانات وأصبح من الضروري تدعيم امن المعلومات بأساليب جديدة من خلال توفير عدة مستويات من الحماية. تم استخدام خوارزمية مقترحة للتغلب على هذه التحديات، حيث تقوم بتشفير الرسالة باستخدام خوارزمية تشفير الحمض النووي، ثم ضرب الناتج بعامل معين ومن ثم ضغط الرسالة باستخدام خوارزمية GZIP، المرحلة الأخيرة هي إخفاء الرسالة المضغوطة في نقاط صورة معينة باستخدام تقنية (LSB). تصل نسبة ضغط البيانات الى ٧٥%. عند الجمع بين هذه التقنيات، تم الحصول على نتائج جيدة، على سبيل المثال، نتيجة صورة غلاف عينة البيت SSIM يساوي ١ وPSNR يساوي ٦٨.٢٨٢٧ و MSE يساوي ٠.٠٠٢٨ ونتيجة UACI هي ٤.٥٩٠٧٢ و درجة NPCR هي ٠.٠٠٣٨٣. يساهم هذا العمل في الحد من مخاطر خرق المعلومات عند إرسال واستقبال المعلومات السرية بين الأطراف.

1. INTRODUCTION

Recently, a protecting data from hacking has become fundamental issue as an output of the huge developing of information technology and the enormous raise in internet access via transmitting and receiving information. Therefore, to protect data, researchers concentrated on establishing a new ideas and schemes, studies are adopted to improve old methods and providing new ones to securing information against intruders [1].

DNA encryption is a new field in cryptographic world and many researchers are interested on this important technique, there is a unique DNA format for every person, there are four bases Adenine,

Guanine, Cytosine, Thymine (A, G, C and T) that represent the bases of DNA. The message characters are represented as DNA format (A, G, C and T). The DNA structure was created by Watson and Crick in 1953 [2].

The Huffman coding and the LZ77 are created the DEFLATE algorithm, DEFLATE reduces of utilizing the system size and provides suitable compression results on various data types. The first algorithm was launched in 1993 [3]. Since then, DEFLATE compression algorithm has become wide ranging, it used in many applications such that PDFs, gzip and can be used in ZIP archives (the zip format is considered as a container that contains Microsoft Office documents formats (.xlsx, .docx, .pptx) and it embedded into zip [4].

The steganography technique in images provides features to conceal secret information without hacker's awareness. Steganography technique is hiding a bits into image through replacing the image bits with the secret message. To increase the algorithm robustness, Least Significant Bit (LSB) is employed to hiding the secret message, so that it supports and strengthening the algorithm efficiency [5][6], to enhance the task of exchanging secret information, it has been utilized the cryptography and steganography to protect data before transmission and the data is becoming safer when using this algorithm.

Cryptography has been connected with the issues of analysing and designing encryption layouts, plans that supply confidential communication through insecure connection media. The problem of producing confidential communication through insecure media is the most conventional and primary problem of cryptography, the connection includes of two sides communicating through insecure media. The proposed algorithm secures the confidential information over the communication, the sender will convert the characters of message to ASCII number then converts the message to binary format the next stage is applying of DNA basis (A, G, C and D) over the message then again convert to ASCII number the output is multiplied by positive integer number to increase the complexity of the encryption algorithm, then compress the message by using GZIP algorithm, finally the encrypted message is embedded into cover image by using LSB technique. The receiver will extract the encrypted message from cover image and applies the decrypted algorithm that is reverse the algorithm in the sender side.

2. RELATED WORKS

Pujari and Shinde used a Blowfish algorithm to encrypt a plain text. They concealed encrypt text into image by applying LSB steganography. The key length is variable and encryption block by symmetric in the Blowfish [7]. Blowfish algorithm is considered totally insecured becuse it uses 64 bit of block size.

Dhamija and Dhaka, proposed a method called SCAMS, it is one's complement transmit protected information between servers. To exchange information, they utilized LSB algorithm and symmetric key [8]. The authors have to support the algorithm with one of the approved encryption methods

K. S. Sajisha, S. Mathew, proposed a security system to protect a confidential text by presenting multilayer of security. The confidential text is cyphered by using DNA format, the next level is applying the AES algorithm. Eventually, another DNA format was used to hide the original encrypted DNA. The presented three levels of protection to secure a confidential text [9]. It is better to enhance the protection way by using the feature of hide data inside a specific media.

M. Sabry, M. Hashem, developed and executed technique by using DNA and the AES algorithm [10]. They designed an algorithm of DNA instead of bits. To providing the ability of implementing the DNA format by creating an evolved system based on DNA algorithm. The proposed algorithm carries the same security features. The method used is strong, but it needs to be strengthened by adding the level of concealment into a particular media

A steganography technique was proposed by Khalifa and Atito[11], DNA and playfair cipher were used to encrypt data then by using a modified exchanging method data is hidden in the real DNA order to extend the hiding capacity. While, it fulfilled maximum concealing capacity than main exchanging method, the concealing capacity is not effective adequate caused by ambiguity problem.

Das and N. Kar, proposed an algorithm that secure data based on two layers of protection and they used two layers of media to covering the secret data, the covers are DNA and image. A 2D logistic map is used to build the DNA from the image, the degenerate genetic code exchange is required to hide data into DNA. The gained

converted DNA is embedded back inside image [12]. The algorithm gives good protection and dual embedding layers but the weak point of this algorithm requires more than one key through the taking out of the processing.

From the above the related works have some clear weak points and require more security and more quality in steganography.

3. DNA CRYPTOGRAPHY

There are four bases that construct into DNA these bases are Adenine, thymine, cytosine, and guanine (ATCG) that are used to represent information. DNA holds enormous storage rang, each gram can store 10^{21} of DNA and roughly represents 10^{8} tera-byte, so, it can store enormous amount of data into DNA. These attributes and advantages of DNA promoted the notion of the cryptography by using DNA. Cryptography employed to protected the significant data for long time. The DNA mechanism bases ordered in random way and the bits of secret message is arranged according to DNA bases. This impressive way is the primary of security paradigm of the recent protection systems, which should substitute of the classical cryptographic algorithms. In mathematical side DNA cryptography used instead of DNA chemistry concept, therefore, the DNA cryptography technique can be used and it is unbreakable by traditional methods. First, converting the plain text to ASCII after that converting ASCII to binary format and eventually, appling the DNA bases (ATCG). Table 1 illustrates DNA bases and the opposite binary format. The DNA bases (ATCG) can be ordered in millions of sequences that is used freely. So, the opportunity to discover the correct sequence is very rare [13].

Table 1 DNA Cryptographic Format

Bits	Base
00	**A**
01	**T**
10	**G**
11	**C**

4. GZIP TECHNIQUE

According to the growing of compression technique demands the GUNZip (GZIP) was constructed to process these requirements. The GZIP utility was created instead of LZW and other algorithms that used in compression. The LZ77 is integrated with Huffman coding to produce GZIP algorithm and rely on DEFLATE algorithm, GZIP algorithm is keeping on data without losing [3].

4.1. Lz77 algorithm

GZIP algorithm search on duplicate strings for data to compress it. The string that appeared in second time replaced with pointer to first one. It uses the term sliding window means that there is a record that any particular location in the data saves of what symbols went before. In the compression and decompression of 32K sliding window there is a record about what the last 32768 symbols were. When the following series of symbols to be compressed match to what found inside the sliding window, the series of symbols is exchanged by distance and length, the distance is how far return to the window where the series started, the length is the number of symbols for which series is matched [14].

4.2. Huffman coding

In this algorithm the data is compressed without any missing. Huffman's concept is fixed length codes (like ASCII) is exchanged by variable length codes, The shorter codewords is assigned instead of more repeated symbols subsequently reducing the length of total data. It is better to construct a (uniquely dismountable) code of prefix by using a variable-length code, preventing the require for a separator to specify code boundaries. Code can be created by Huffman coding. A Huffman code tree is used to describe the Huffman algorithm. The steps for creating the Huffman code tree are:

1. The tree is starting with leaf nodes and each node represents a symbol in the text.
2. From the list choose two leaf nodes with minimum weight.

3. Make a parent node for the two leaf nodes, the weight of parent must be equal to the weight of sum of two leaf nodes.
4. From the list delete the two leaf nodes and add the parent node to the list, now parent node became the new leaf node.
5. Repeat the procedure by starting from step two and stop when become single tree.

When Huffman tree is constructed, A prefix code is created by the algorithm passing through each symbol of alphabet in the binary tree, in the tree the left branch is assigned by 0 and right branch is assigned by 1.

Huffman algorithm needs to know the repeated symbol in the alphabet. The compressed output, the Huffman codes and Huffman tree for repeated symbol or symbols must be stored. The Huffman codes and Huffman tree for repeated symbol or symbols must be stored in the header of compressed file and this information is required when making the decoding processing [14].

5. IMAGE STEGANOGRAPHY

Steganography uses a cover image for concealing a text or encrypted text. The conversion of physical picture to array of digits (digital image) called image processing, the image pixels intensity is illustrated by these digits. Each pixel has 256 intensity values due to the grayscale image that is represented by 8 bits for each pixel. The colored image (RGB) is represented by 24 bits for each pixel, therefore, the cubic of 256 is represented by each pixel in the colored image. We can a little modify in pixel intensity to obtain insensible view for pixel adjustment and it keeps

difficult to discover by the Human Vision System (HVS). The Least Significant Bit (LSB) is a valuable algorithm and it can be used in steganography. The LSB algorithm works through the replacing of the eighth bit of least significant of original pixel with the bit of secret text, this is done after convert the secret text to binary format [15].

6. PROPOSED WORK

The proposed work is consist of cryptography and steganography, the first stage is divided into three processes the first process is encryption by using DNA algorithm, the second process is multiplication by a factor and the third process is compression by using GZIP algorithm. the second stage is steganography by using colored image as a cover with (LSB), this work is applied at sender side While on the receiver side, the same steps are repeated, but in the opposite format to obtaining the plaintext.

At the receiver side is consist of two stages:the first stage is extracting the cipher text from cover image, the second stage is decryption the cipher text. the seconed stage is divide into three processes: the first process is decompression by using GZIP algorithm, the second process is divided on the factor and the third process converts the DNA to plain text.

6.1. Sender side

Input: Confidential message and original image.

Begin

1. The confidential message is converted to ASCII format.
2. Applying binary format on ASCII.
3. The DNA bases are assigned on the binary message according to the Table-1.
4. DNA is converted to ASCII.
5. ASCII is multiplied by Factor.
6. The confidential message is compressed through applying the GZIP algorithm.
7. Now it is used covered image to apply the steganography through:
    a) Looping through image pixels to change the least significant bit of red, green and blue to zero, then embed the characters of cipher confidential text into image.
    b) The eight bits of first character is converted to integer then conceal bits into red, Green and Blue on neighbouring pixels, the bits of character are concealed in each LSB.
    c) Repeat the procedure after eight bits are embedded and bring the following character.
    d) After embedding all cipher text set a flag to indicate the end of text.

Output: Obtained the steganography image.

End.

6.2. Receiver side

Input: Steganography image that contains confidential encrypted message.

Begin

1. Extracting of confidential encrypted message from stego image, this operation is done by searching on flag then proceed to image pixels, bring the value of least significant bit that related to RGB, after obtaining of first eight bits, keep going to obtain all secret message.
2. Apply GZIP decompression algorithm to convert the message to ASCII.
3. Divide ASCII over Factor.
4. Convert ASCII to DNA.
5. Turn the text to binary then to decimal format.
6. Convert to Plaintext.

Output: Plaintext.

End.

Figures 1 and 2 explain the algorithm:

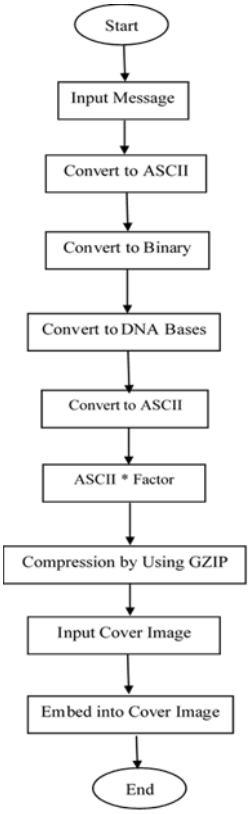

Figure 1 Sender Side Algorithm.

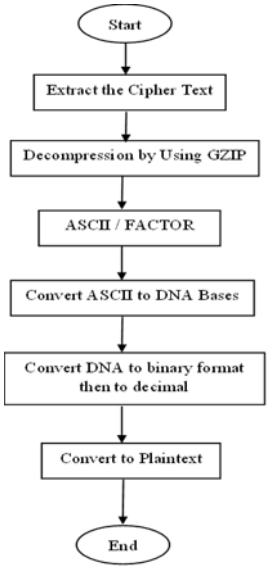

Figure 2 Receiver Side Algorithm

7. FIDELITY MEASURES

These measures are employed to compute the difference scope between two images the first image is original image and second image is stego image.

7.1 Mean square error (MSE)

It illustrates the commutative quadratic fault (pixel changes) after comparing 2 images, the equation of MSE is [16]:

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

Where the image measures are m and n, C(i,j) represents original image pixels , S(i,j) is stego image pixels.

7.2 Peak signal to noise ratio (PSNR)

The PSNR is utilized to compute peak fault, the maximum PSNR means the quality of image is good [17].

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

The higher possible value related to pixels concentration can be represented by R.

7.3. Structural similarity index measure (SSIM)

It can be made a comparison between MSE and PSNR by using SSIM measure. The SSIM is used to evaluate the vision convergence of images [18].

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \quad (3)$$

The mean density is represented by μ, the standard diffraction is represented by σ. The Two constants C1 and C2 are greater than zero and provide the stability when the rest parameters are close to '0'. The other paremeters (μx, μy, σxy, μ_x^2, μ_y^2, σ_x^2 and σ_y^2) are approach to '0'.

7.4. Number of pixels change rate (NPCR) and the unified averaged changed intensity (UACI)

These measures are utilized to compute failure or efficiency between original and encrypted images by account pixels intensity [19]:

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

$$D(i,j)=\begin{cases}0\ if\ C1(i,j)=C2(i,j)\\1\ if\ C1(i,j)\neq C2(i,j)\end{cases} \quad (5)$$

$$UACI=\frac{1}{N*M}\left[\sum_{i,j=1}^{N*M}\frac{|C!(i,j)-C2(i,J)|}{Max(C2)}\right]*100\% \quad (6)$$

M and N, are the size of image and i,j are pixels, the original image is C1, the cipher image is C2.

8. EXPERIMENTAL RESULT

The proposed work is implemented in this section, this section explains the experimental results. The types PNG and BMP images cover have been used. The techniques DNA and GZIP was used and cover image to obtain the results that show that the proposed work provides a significant security protection. Figure 3 offers the execution of the work, the first upper group of images represent the original cover, however the second lower group of

images represent the images after applying the steganography on the secret message. The first upper group of images are seeming almost identical with the second lower group of steganography images. In other phrase, the second lower groups of images (stego images) do not cause detectable faults.

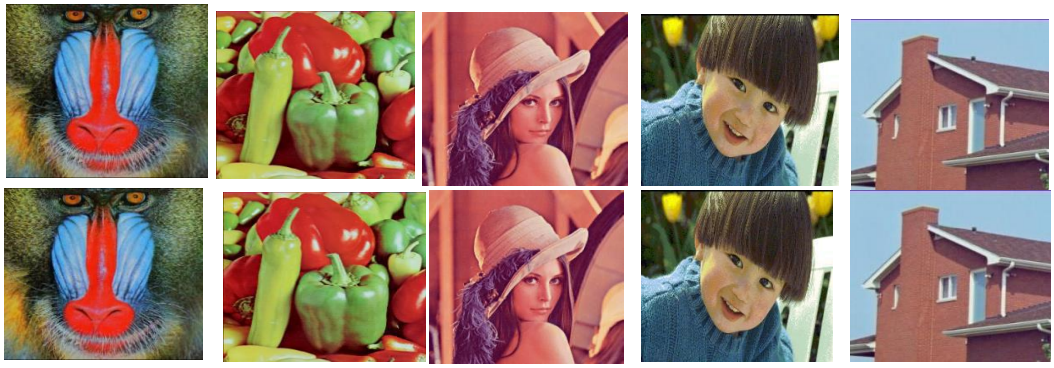

Figure 3 Sample of Results.

Figure 3 demonstrates the extension of the confidential compressed texts which include 89, 109,130, and 170 characters.

Figures 4, 5 explain changing on the message.

```
Message = Hello qusay how are you are you ok.
Message to ASCII = 72 101 108 108 111 32 113 117…
Assigning DNA=TAGATGTTTGCATGCATGCCAGAA…
DNA to ASCII= 84 65 71 65 84 71 84 84 84 71 67…
ASCII * Factor= 504 390 426 390 504 426 504 504 504 426 402…
GZIP compression= 120156227969801311524616582092257 99…
Appling steganography.
```

Figure 4 Confidential Compressed Text at Sender

```
Extracting from image the cipher text= EAAAACCR0fcy5KjsCw6vxp/yXkw…
GZIP uncompressed= 504 390 426 390 504 426 504 504 504 426 402 390…
ASCII / Factor= 84 65 71 65 84 71 84 84 84 71 67 65 84 71…
ASCII to DNA= TAGATGTTTGCATGCATGCCAGAATCATTCTTT…
DNA to binary =
0100100001100101011011000110110001101111001000000111000 1…
Binary to the plain text= Hello qusay how are you are you ok.
```

Figure 5 Confidential Compressed Text at Receiver

For quantitative evaluation, the least value of the MSE means the least error. The highest value of the PSNR and SSIM is equivalent to one imply lower faults and good seeing for image quality. Table 2 illustrates various extensions of secret text according to results of PSNR, MSE and SSIM.

Table 2 The SSIM, MSE and PSNR Results

The no. of Char. in original Mess.	The no. of char. in DNA mess.	The no. of char. in GZIP Mess.	Compression Rate	PSNR					MSE					SSIM
				Mandrill	Peppers	Lena	Boy	House	Mandrill	Peppers	Lena	Boy	House	
29	140	89	32%	68.7528	68.2523	66.4178	68.5132	67.6815	0.0016	0.0031	0.0025	0.0023	0.0082	1
55	209	109	50%	67.8191	67.2434	67.4219	67.5214	68.2827	0.0045	0.0051	0.0037	0.0058	0.0028	1
77	288	130	57%	67.2843	66.4177	66.7551	66.6116	65.6152	0.0099	0.0093	0.0054	0.0068	0.0031	1
102	399	170	76%	66.2272	65.6754	65.9771	65.8438	66.7613	0.0083	0.0027	0.0027	0.0121	0.0061	1

To evaluate the rate of image encryption, there are two methods are used (NPCR and UACI). The value of NPCR is high and the value of the UACI is low, this means the image is fully encrypted. To make the proposed algorithm more robust the operation must be opposite because hiding a text not encrypted image (UACI is high and NPCR is low). Table 3 shows the values of UACI and NPCR by using lengths 89, 109,130, and 170 characters

Table 3 The NPCR and UACI Results

The no. of Char. in original Mess.	The no. of char. in DNA mess.	The no. of char. in GZIP Mess.	Compression Rate	NPCR					UACI				
				Mandrill	Peppers	Lena	Boy	House	Mandrill	Peppers	Lena	Boy	House
29	140	89	32%	0.00145	0.00744	0.00137	0.01014	0.01216	4.31691	3.42912	4.82721	4.53215	3.72954
55	209	109	50%	0.01224	0.01486	0.01291	0.02127	0.00383	532614	6.37246	5.83159	5.79842	4.59072
77	288	130	57%	0.01468	0.01732	0.01678	0.01642	0.11759	6.28151	7.42391	7.21721	6.87536	5.64827
102	399	170	76%	0.01823	0.01298	0.01523	0.01219	0.00852	7.61462	8.65418	8.46261	8.63126	6.74263

Figure 6 demonstrates the histograms of the base 3 colors Red, Green and Blue to the image before steganography and after it. The first line demonstrates the original image and the second one demonstrates the results after steganography. A similarity was obtained between them.

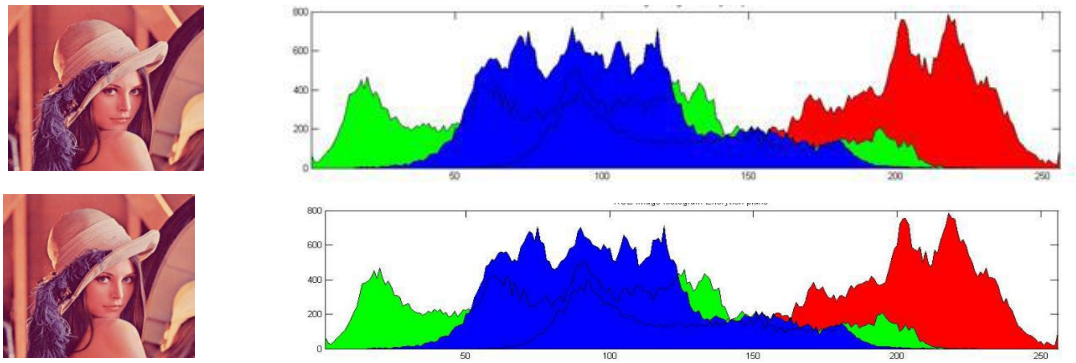

Figure 6 The Histogram.

9. CONCLUSIONS

The best results of security can be obtained by utilizing cryptography and steganography, and combining them by implementing the DNA and using GZIP compression algorithms, the GZIP decreases the extension of the secret text and reduce the size of DNA extension to providing a proper steganography. The system complicates the cryptanalysis procedure of attacker when making multiplication by factor with DNA numbers to make the breaching very difficult and accordingly develops the system general security, then concealing it in RGB image by using LSB steganography method. The perfect values of MSE are small and approximately close to zero however the perfect values of PSNR are big and near to 100 while the values of SSIM is close to one, also a small scores of NPCR and high scores of UACI were got that mean a greate match between the original and stego images. therefore tables 2 and 3 have a good values. There is high similarity between steganography image and original image that proved by the histogram. The encryption, compression and data hiding were reflecting a robust work and decrease errors and good seeing quality, this means the proposed work provides a positive impact.

References

1. Morkel, T, Eloff, J, Olivier, M, (2005). An overview of image steganography. *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*. Sandston, South Africa.

2. Narendren S, Yashas B Y, Chandra M B, (2018). A cryptosystem using two layers of security-DNA and RSA cryptography. *International Journal of Pure and Applied Mathematics*, 119, 217-224.

3. Oswal S, Singh A, Kumari A, (2016). Deflate compression Algorithm. *International Journal of Engineering Research and General Science*, **4**(1), 430-436.

4. Brown Ralf D, (2011). Reconstructing corrupt DEFLATE files, *Proceedings of the eleventh annual DFRWS conference*, New Orleans.

5. Joshi K, Puniani K, Yadav R, (2016). A Review on different image steganography techniques. *Digital Image Processing*, **8**(6), 179-186.

6. Noor H, Rajaa A, Hazim N, Adel A, (2018). Multilevel hiding text security using hybrid technique steganography and cryptography. *International Journal of Engineering and Technology*, **7,** 3674-3677.

7. Pujari A A, and Shinde S S, (2016). Data security using cryptography and steganography IOSR. *Journal of Computer Engineering (IOSR-JCE*), **18**(4), 130-139.

8. 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)*, 346-351.

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

10. Sabry M, Hashem M, Nazmy T, Khalifa M E, (2015). Design of DNA-based advanced encryption standard (AES). *IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)*, Cairo. 390-397

11. Khalifa, A. and Atito, A. (2012). High-capacity DNA based steganography. *The 8th International Conference on INFOrmatics and Systems.*76-80

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

13. Karandeep Kaur, (2016). A Double layer encryption algorithm based on DNA and RSA for security on cloud. *IRJET*, 3, 1742-1745.

14. Sitaridi E, Mueller R, Kaldewey T, Lohman G, Ross K A, (2016). Massively-parallel lossless data decompression. (*ICPP) 45th International Conference IEEE*.

15. Sinan A, Naji S N, Mohaisen H N, Alsaffar Q S, Omran S H, (2019). A modified RSA algorithm for hiding text in colored images with pixel selection. *Opcion*, 2899-2921.

16. Hameed S M, Taqi A I, (2020) A new beta chaotic map with DNA encoding for color image encryption. *Iraqi Journal of Science*, 61, 2371-2384.

17. 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, 1887–1894.

18. Sinan A, Naji S N, Mohaisen H N, Alsaffar Q S, Jalab H A, (2020). Automatic region selection method to enhance image-based steganography, *Periodicals of Engineering and Natural Sciences*, **8**(1), 67-78.

19. Oza P, Kathrecha, Malvi P, (2016). Encryption algorithm using rubik's cube principle for secure transmission of multimedia files, *Third International Conference on Multidisciplinary Research and Practice.* **4**(1), 239-243.