Iraqi Journal of Science, 2025, Vol. 66, No. 11, pp: 5225- 5239
DOI: 10.24996/ijs.2025.66.11.41

ISSN: 0067-2904

A Hybrid Model Based on DNA Method for Encryption Messages and Hiding Secret Keys in Cover Image

Rafeef M. Al Baity[1]*, Asraa Abdullah Hussein [1], Noura H. Ajam [2]
[1]*Department of Computer Science, University of Babylon, Babylon, IRAQ*
[2]*Department of Management Information System, University of Basrah, Basrah, IRAQ*

Received: 26/2/2024 Accepted: 28/11/2024 Published: 30/11/2025

Abstract

Due to the continuous development of information technology and the widespread exchange of digital media, such as text, videos, and images, between parties, protection has become a necessity. In addition, with the latest modern technology, copying and using information illegally has become elementary. In the research community, the given scenario imposes challenges to transferring multimedia files more securely. In such scenarios, various techniques, such as cryptography and steganography, protect secret data from adversaries. The use of biology in cryptography is a new approach to cryptographic research. This paper will present a method of cryptography inspired by DNA structure and its relationship to amino acids. Work has been done on one of the most practical, effective, and modern methods to develop encryption and decryption algorithms, which is DNA-based encryption. Three steps make up the proposed system firstly, the message text is initially hidden in a randomly generated string until it is encrypted. Secondly: encode the message using amino acids and DNA codes. In the third stage, the encryption key is hidden in the cover image using the least significant bit (LSB). The new encryption technology demonstrated several levels of protection by encrypting amino acids and DNA and hiding the encryption keys in the cover image. Moreover, the PSNR metrics used for analysis and comparison show that the proposed approach provides good security.

Keywords: Steganography, Encryption, DNA, LSB, Amino Acid.

نموذج هجين يعتمد على رسائل التشفير وإخفاء المفاتيح السرية في صورة الغلاف

رفيف البياتي*[1], إسراء عبدالله حسين[1], نورا عجام[2]
[1] قسم علوم الحاسوب، جامعة بابل، بابل، العراق
[2] قسم نظم المعلومات الإدارية، جامعة البصرة، البصرة، العراق

الخلاصة

بسبب التطور المستمر لتكنولوجيا المعلومات والتبادل الواسع النطاق للوسائط الرقمية، مثل النصوص والفيديوهات والصور بين الأطراف، أصبحت الحماية ضرورة. بالإضافة إلى ذلك، مع التقنيات الحديثة، أصبح نسخ المعلومات واستخدامها بشكل غير قانوني أمرًا بدائيًا. في مجتمع البحث العلمي، يفرض السيناريو

*Email: wsci.rafeef.ketran@uobabylon.edu.iq

المعطى تحديات لنقل ملفات الوسائط المتعددة بشكل أكثر أمانًا. في مثل هذه السيناريوهات، تحمي تقنيات مختلفة، مثل التشفير والتخفي، البيانات السرية من الخصوم. يعد استخدام علم الأحياء في التشفير نهجًا جديدًا للبحث في التشفير. في هذه الورقة، سنقدم طريقة تشفير مستوحاة من بنية الحمض النووي وعلاقتها بالأحماض الأمينية. تم العمل على واحدة من أكثر الطرق العملية والفعالة والحديثة لتطوير خوارزميات التشفير وفك التشفير وهي التشفير القائم على الحمض النووي. يتكون النظام المقترح من ثلاث خطوات أولاً يتم إخفاء نص الرسالة في البداية في سلسلة يتم إنشاؤها عشوائيًا حتى يتم تشفيرها. ثانيًا: تشفير الرسالة باستخدام الأحماض الأمينية ورموز الحمض النووي. في المرحلة الثالثة، يتم إخفاء مفتاح التشفير في صورة الغلاف باستخدام البت الأقل أهمية (LSB). وقد أظهرت تقنية التشفير الجديدة عدة مستويات من الحماية من خلال تشفير الأحماض الأمينية والحمض النووي وإخفاء مفاتيح التشفير في صورة الغلاف. وعلاوة على ذلك، تظهر مقاييس PSNR المستخدمة للتحليل والمقارنة أن النهج المقترح يوفر أمانًا جيدًا.

1. Introduction

Data transmission and network security are the focus of protection. Data protection is the most crucial component of securely sending data across a network. Achieving optimal data protection for data exchanges over open networks is challenging. The user or unapproved parties may access the information for a number of harmful purposes. Effective coding practices are necessary for sufficient data protection. Cryptography and steganography are the most common and widely used techniques. Cryptography serves to encrypt data, while steganography is used to hide data from hackers. The encryption process requires consideration of specific parameters, such as key generation for the encryption and decryption processes, the format of the encrypted data, and how to retrieve the data from the encrypted data [1], [2], [3], [4], [5]. When a message is encrypted, everyone will know it is there, but those who do not have the decryption key cannot understand or read it. Therefore, accessing the decryption keys must be very difficult so that the person specified to receive the message (the recipient) can decrypt the message and retrieve the original message [6], [7]. As a new hope for strong cryptographic techniques and impenetrable algorithms, DNA computing has been included in information concealment and cryptography [3].

Steganography is a science and technique for protecting confidential data from unauthorized persons. In steganography, the original image is called a cover image, and the image obtained after hiding confidential data is called a stego image. A fundamental requirement of steganography is that a particular recipient can retrieve the hidden information [8], [9], [10], [11]. The main goal of our work is to promote the concept of security based on the DNA coding method. The background of biological DNA and DNA cryptography is reviewed and discussed below.

2. Related Works

Harry Shaw [12] employed a cryptographic model based on gene expression processes to encrypt the message text, thus passing outdated security measures and being compatible with future biological representations of information security. The selected methodology offered a hierarchical structure, from the initial message encoding to the DNA code in transcription and translation to the protein code. Therefore, the strength of the gene expression regulation improved the network security between the two parties.

Krishna, et al. [13] presented a novel method of message encryption using pseudo-biological DNA. The message was translated into the messenger ribonucleic acid (mRNA), transfer ribonucleic acid (TRNA), and deoxyribonucleic acid (DNA) standards. To increase security, multiple sequences of pseudo-random keys were generated as a protein to bind part of the message to the transmitter, making it harder to decipher the ciphertext.

Basu, et al. [14] Machine learning techniques were applied to simulate the biological processes of genetic coding (converting binary bases to DNA), transcription (converting DNA to mRNA), translation (converting mRNA to protein), and decoding (the opposite process), a system based on the Central Doctrine of Molecular Biology (CDMB) for encryption and decryption algorithms was adopted. Random data was used to train a bidirectional associative memory neural network (BAMNN) to create and renew key sets iteratively.

In Reddy et al., [15] on the central doctrine of molecular biology (CMDB), the bidirectional associative memory neural network (BAMNN), and the DNA encryption system were all utilized . Three steps make up the suggested method: encryption, key generation, and decryption. Transcription, translation, and genetic encoding were used for encryption and decryption techniques. Additionally, the encryption method transfers the text in 16-bit blocks utilizing variable length probability-based Huffman coding. The whale optimization algorithm (WOA) is the most appropriate weight.

Satir and Kendirli [16] presented a DNA encryption method in their paper by incorporating DNA operators and DNA encoding into the Feistel network design. Here, biological instruments were employed as implementation tools, and DNA itself was utilized as a carrier rather than more conventional digital media like images, texts, or videos. Additionally, the digitally and biologically generated DNA sequence and the developed simulation software were incorporated into specifically designed biotechnological instruments.

Krishna, et al. [17] an asymmetric algorithm based on deoxyribonucleic acid (DNA) is proposed in this study. The suggested asymmetric algorithm is utilized for image stealth, which encrypts and conceals sensitive data in a cover picture. Xilinx Vivado was used to design and synthesize the dynamic partial reconfiguration (DPR) cryptosystem, while the Vivado simulator was used for simulation.

In their paper, Noor and Matheel [18] propose an encryption method with a LUC algorithm to boost the complexity based on mRNA amino acids and DNA sequences.

Table 1: Comparing different studies

Ref. No.	Method Specifics	Measure	Years
12	Gene expression, DNA code	β-globin gene sequence	2017
13	DNA, MRNA, TRNA	FPGA, CLB	2018
14	DNA, MRNA, CDMB, BAMNN	Encryption and decryption time	2020
15	DNA, MRNA, WOA Algorithm, Huffman coding	Encryption and decryption time	2020
16	DNA, Feistel Network structure	Capacity	2022
17	DNA, DPR, Vivado simulator	Encryption and decryption time	2022
18	DNA, MRNA, LUC	UACI, PSNR,NPCR	2023
Suggested method	DNA,CDNA, Amino acid, LSB	PSNR, Encryption and decryption time	2024

3. Background

This section introduces a brief biological background about DNA sequences, cDNA, RNA sequences, and amino acids. This prior knowledge is necessary to comprehend the following parts fully.

4. DNA Cryptography

One definition of DNA computing is a novel technology that uses biological structures to transport information. Regarded as a pioneer in DNA computing was Leonard Max [19]. In 1994, this method was applied to address intricate algorithmic issues. DNA computing has the advantage of storing vast amounts of data at an approximately 100 times faster speed than computers and requires less energy. For these reasons, data can be transferred and stored via it. The method of encrypting data with DNA sequences is known as DNA encryption. The use of DNA sequences in the encryption of binary data is the main focus of current DNA encryption research [20].

5. DNA Digital Coding

DNA is the acidic material containing the genetic instructions utilized in development. Adenine (also known as A), cytosine (C), guanine (G), and thymine (T) are the four nucleotides that makeup DNA. Using 0 and 1, these four nucleotide bases are represented [20], as the table [2].

Table 2: Binary form of DNA nucleotide conversion scheme

DNA Nucleotide	Binary Form
A	00
C	01
G	10
T	11

Based on Table 2, this encoding makes it simple to encode text messages. Suppose someone wants to send the number 97 to be transmitted via DNA encoding. 97 is first converted to binary, yielding 10000110 as the final binary number. Two successive binary integers are taken, starting from the left bit side, and transformed into the appropriate DNA nucleotide bases using the scheme displayed in Table 1. Because of this, the number 97 will be encoded as CAGC. The encoded message (CAGC) will now be transmitted to the recipient over the channel. After decoding it, the recipient retrieves the original message.

6. Complement DNA Operation

The four nucleotide bases—adenine (A), cytosine (C), thymine (T), and guanine (G)—are substituted in DNA complement operation by the complementary rule and in an antiparallel fashion, where A is substituted with T and vice versa. Similarly, G is used in place of C and vice versa [20]. The complemented DNA sequence, for instance, would be TGACTGAC if the input DNA sequence was ACTGACTG.

7. RNA

RNA has only one strand. RNA is composed of four bases: adenine (A), uracil (U), cytosine (C), and guanine (G) [18].

RNA strands are produced during transcription using the DNA strands. Here, the matching nucleotide bases in RNA are used instead of the nucleotide bases in DNA. They share identical nucleotide bases, A, C, and G, except RNA, where uracil U is used instead of thymine T [21].

8. Amino Acid

Deoxyribonucleic acid (DNA) is the source of the genetic information found in single strands called mRNA, which are utilized to produce proteins. Additionally, it transmits data from DNA to cytosolic ribosomes. An amino acid can be defined by the RNA molecule containing three nucleotides in a row.

A codon is a group of three neighboring nucleotides in the RNA molecule. To represent the amino acids, it comprises multiple codons [18]. Figure (1) below displays the amino acids found in RNA [18].

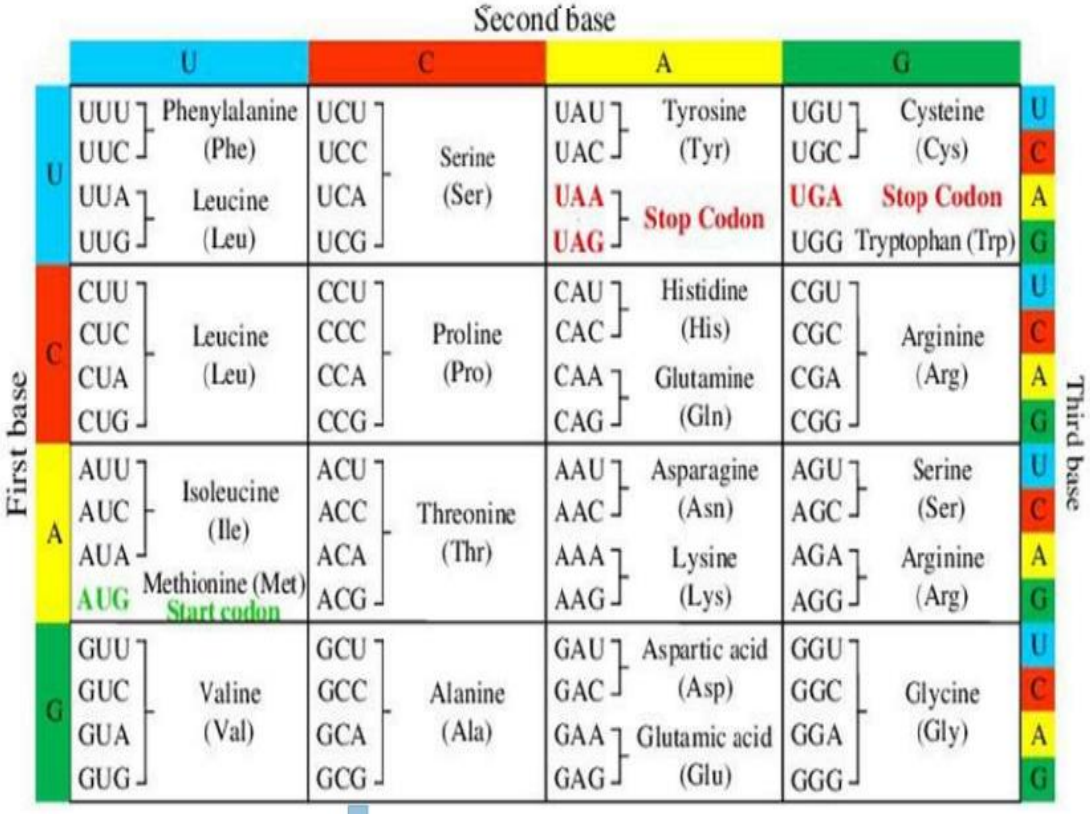

Figure 1: RNA Amino acid

According to the amino acid concept, Table 3 displays the 64 amino acid codons [22].

Table 3: The amino acid-corresponding RNA codons

Character	Protein sequences	Character	Protein sequences
A	UUU, UUC	N	CAU, CAC
B	UUA, UUG	O	CAA, CAG
C	CUU, CUC, CUA, CUG	P	AAU, AAC
D	AUU, AUC, AUA	Q	AAA, AAG
E	AUG	R	GAU, GAC
F	SUU, GUC, GUA, GUG	S	GAA, GAG
G	UCU, UCC, UCA, UCG	T	UGU, UGC
H	CCU, CCC, CCA, CCG	U	UGA
I	ACU, ACC, ACA, ACG	V	UGG
J	GCU, GCC, GCA, GCG	W	CGU, CGC, CGA, CGG
K	UAU, UAC	X	AGU, AGC
L	UAA	Y	AGA, AGG
M	UAG	Z	GGU, GGC, GGA, GGG

The same 64 amino acid codons are included in Table 4, but they are ordered to better fit the proposed work's needs . Getting a coded text that is challenging to decode is the primary goal. For instance, the code is (A1) if the codon is (UUU), but (A2) if the codon is (UUC).

Table 4: Amino acid coding

Letter	RNA	code	Letter	RNA	code	Letter	RNA	code	Letter	RNA	code
A	UUU	1	H	CCU	1	O	CAA	1	V	UGG	**1**
				CCC	2						
				CCA	3		CAG	2			
	UUC	2		CCG	4						
B	UUA	1	I	ACU	1	P	AAU	1	W	CGU	**1**
				ACC	2					CGC	**2**
				ACA	3		AAC	2		CGC	**3**
	UUG	2		ACG	4					CGG	**4**
C	CUU	1	J	GCU	1	Q	AAA	1	X	AGU	**1**
	CUC	2		GCC	2						
	CUA	3		GCA	3		AAG	2		AGC	**2**
	CUG	4		GCG	4						
D	AUU	1	K	UAU	1	R	GAU	1	Y	AGA	**1**
	AUC	2									
	AUA	3		UAC	2		GAC	2		AGG	**2**
E	AUG	1	L	UAA	1	S	GAA	1	Z	GGU	**1**
										GGC	**2**
							GAG	2		GGA	**3**
										GGG	**4**
F	GUU	1	M	UAG	1	T	UGU	1			
	GUC	2									
	GUA	3					UGC	2			
	GUG	4									
G	UCU	1	N	CAU	1	U	UGA	1			
	UCC	2									
	UCA	3		CAC	2						
	UCG	4									

9. Least Significant Bit (LSB)

The least significant bit approach was applied to input data into digital media by substituting the least significant bit for the data bits entered in the message [23].

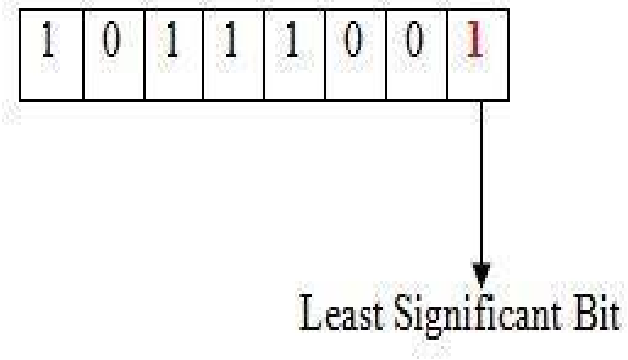

Figure 2: Shows that the final bit has the lowest bit position (Least Significant Bit)

10. Steganography

Steganography is said to have its roots in ancient Greece but is now attracting attention over reasons of security. Steganography is a branch of technology that hides data in files such as text [24], images [25], [26], [27], audio [28], and video [29]. The steganography technique embeds a coded message in the cover file before transmission. Thus, only the sender and receiver know or understand its existence, which cannot be viewed by an outside observer [30]. The sender inserts the secret message (plain text) into the cover file. On the receiver's side, an arbitrary key (the stego key) reveals the secret message [31]. Now, most steganography algorithms involve modifying the cover image to create a stego image that is very similar to the cover image but with different pixel values or creating a mapping relationship between the stego image and the secret message. Thus, an attacker will discover the existence of secret communications from these modifications and variations [32].

Therefore, an improved steganography technique was proposed to hide data in the least significant bits (LSB), get better data embedding capability, and simultaneously provide imperceptibility [33]. Changing the least significant bit of each byte of data in the transport medium does not change the transport image that the human eye can recognize. Therefore, the LSB method relies on hiding data in an area created by ignoring the least significant bits; the LSB method is the most widely used of the bit-space methods [34].

11. Materials and Methods

The suggested cryptographic method includes two stages, the encryption stage, and the decryption stage:

12. In the encryption stage

The sender encrypts the message before sending it to the other party, the receiver, and this process includes a set of steps, as shown in Figure 3 (which displays the sender's block diagram in detail).

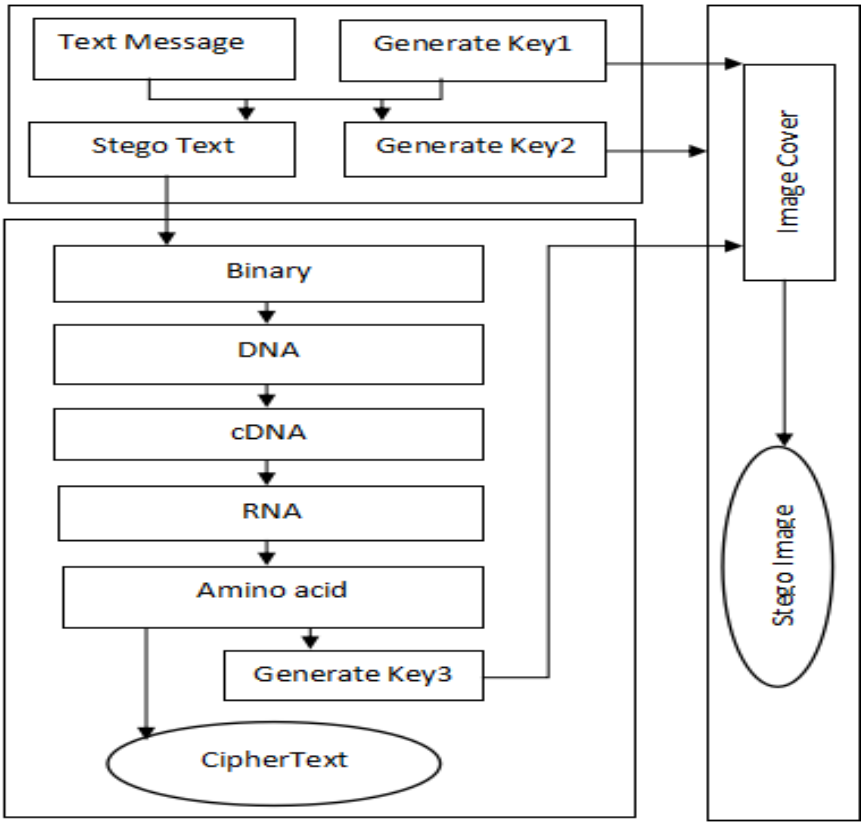

Figure 3: Scheme for encryption.

Stage1 "random keys generating"
Step 1: Use a random number sequence with a length of 255 and range between [0,255] to generate the key1.
Step 2: key2 generated by hiding the message in a random string and then get the hidden string and key 2.
Stage2 "Cryptography"
Step 1: Convert the message to be encoded (resulting from the first stage) into binary and then to DNA.
Step 2: Convert the DNA string to its complement DNA (cDNA).
Step 3: Convert the cDNA string to its (RNA).
Step 4: Create the cipher text and key 3 after transforming the RNA string into an amino acid string by using the table (4).
Stage3 "Keys Hiding based on LSB"
The encryption keys are consecutively hidden inside the cover image using the LSB technique.

13. In the Decryption stage
The receiver decrypts the message. When the message is received by anyone who cannot decrypt it, the person concerned (the receiver) must receive its cover image to recover the encryption keys and decrypt the message as shown in Figure (4).

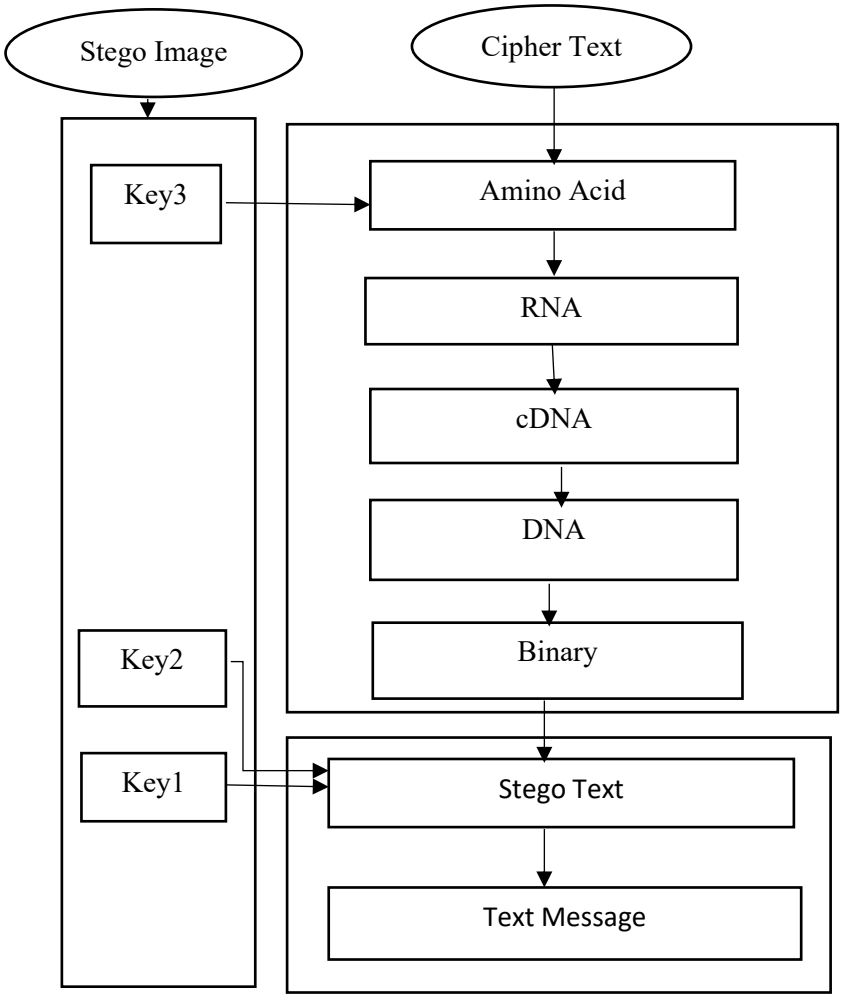

Figure 4: Scheme for decryption

Stage1 "extracting keys from the cover image"
To decrypt the message and recover the original text, keys (key1, key2, and key3) are extracted from the cover image.
Stage2 "decryption"
Step 1: Using table 4 as a guide to convert the encrypted message text to an amino acid string.
Step 2. Transform a string of amino acids into a string of RNA.
Step 3. Convert a string of RNA to one of cDNA.
Step 4. Change the cDNA string to a DNA string and then into binary code.
Stage3 "Original Text Retrieval"
Step1: Convert the string from binary to ASCII.
Step 2: The string included in the encrypted message is recovered using keys 1 and 2 and retrieves the original message text after converting the ASCII code to char.
The following example will show the results of the encryption mentioned above and the decryption of the action steps. Input: Run away as fast as it can.
Sender Side
Stage1 "random keys generating"
Step 1 : Generating a series of random values between (0-255): (Key 1)
27 62 55 53 186 158 51 207 149 161 84 143 249 153 214 9 83 196 47 208 235 177 205 86 107 49 60 25 37 200 139 39 245 52 76 172 209 102 42 253 252 193 126 180 118 90 19 81 75 194 59 115 101 106 142 54 48 58 154 204 248 152 146 68 179 79 175 140 85 218 99 198 46

65 128 215 182 32 6 133 78 156 223 113 71 226 98 148 228 61 110 178 255 135 197 160 89 246 233 44 105 127 162 94 236 224 92 171 91 11 144 119 70 210 227 17 234 31 64 23 131 232 247 219 213 184 10 150 38 28 69 57 103 122 7 203 22 222 18 40 134 80 170 30 230 147 188 77 15 221 33 63 109 187 206 74 123 13 181 3 120 20 216 56 231 173 190 157 155 111 211 137 29 82 229 124 35 5 41 114 129 254 4 117 163 159 251 93 239 199 185 66 241 1 240 141 243 43 238 202 217 195 112 201 24 225 169 132 2 189 220 151 138 72 67 176 16 242 88 212 174 168 8 191 26 100 130 167 136 45 87 192 12 104 96 34 164 125 121 108 145 36 50 97 95 116 183 21 237 250 244 73 14 166 165

Step 2: To generate key 2 must first convert the message to ASCII code as follow:

82 117 110 32 97 119 97 121 32 97 115 32 102 97 115 116 32 97 115 32 99 111 117 108 100 44

Include the message text in the number string resulting from step 1 by taking the site number and obtaining a new string and at the same time generating key 2.

Text stego: 174 184 91 78 244 112 244 239 78 244 52 78 38 244 52 246 78 244 52 78 71 170 184 240 226 100

Key2 : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Stage2 “Cryptography”

Step 1: Convert ASCII values to binary format:

10101110 10111000 01011011 01001110 11110100 01110000 11110100 11101111 01001110 11110100 00110100 01001110 00100110 11110100 00110100 11110110 01001110 11110100 00110100 01001110 01000111 10101010 10111000 11110000 11100010 01100100

Step 2: Converting the binary values to sequences of DNA:

GGTGGTGACCGTCATGTTCACTAATTCATGTTCATGTTCAATCACATGAGCGTTC AATCATTCGCATGTTCAATCACATGCACTGGGGGTGATTAATGAGCGCA

Step 3: Converting DNA sequences into complementary DNA (cDNA):

CCACCACTGGCAGTACAAGTGATTAAGTACAAGTACAAGTTAGTGTACTCGCAA GTTAGTAAGCGTACAAGTTAGTGTACGTGACCCCCACTAATTACTCGCGT

Step 4: Converting DNA sequence to RNA sequence:

CCACCACUGGCAGUACAAGUGAUUAAGUACAAGUACAAGUUAGUGUACUCGC AAGUUAGUAAGCGUACAAGUUAGUGUACGUGACCCCCACUAAUUACUCGCGU

Step 5: The RNA sequence is converted to amino acids (Table 4), which are then used as the cypher text to be transmitted:

Cipher Text : HHCJFOFDQKQKQBFKGOFXQWIXMTIUHHCDIWF

Key 3: 3 3 4 3 3 1 4 1 2 2 2 2 1 4 2 4 1 1 1 2 1 3 1 1 1 4 1 2 3 3 1 1 2 3

Stage3 “Keys Hiding based on LSB”

hide encryption keys (key 1, key 2, key 3) with a grayscale image cover (Stego image) using the LSB method.

Receiver Side

Stage1 “extracting keys from the cover image”

Retrieve cypher keys from the cover image (Stego image):

Decipher Key 3: 3 3 4 3 3 1 4 1 2 2 2 2 1 4 2 4 1 1 1 2 1 3 1 1 1 4 1 2 3 3 1 1 2 3

Decipher Key 2: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Decipher Key 1: 27 62 55 53 186 158 51 207 149 161 84 143 249 153 214 9 83 196 47 208 235 177 205 86 107 49 60 25 37 200 139 39 245 52 76 172 209 102 42 253 252 193 126 180 118 90 19 81 75 194 59 115 101 106 142 54 48 58 154 204 248 152 146 68 179 79 175 140 85 218 99 198 46 65 128 215 182 32 6 133 78 156 223 113 71 226 98 148 228 61 110 178 255 135 197 160 89 246 233 44 105 127 162 94 236 224 92 171 91 11 144 119 70 210 227 17 234 31 64 23 131 232 247 219 213 184 10 150 38 28 69 57 103 122 7 203 22 222 18 40 134 80 170 30 230 147 188 77 15 221 33 63 109 187 206 74 123 13 181 3 120 20 216 56 231 173 190 157 155 111 211 137 29 82 229 124 35 5 41 114 129 254 4 117 163 159 251 93 239

199 185 66 241 1 240 141 243 43 238 202 217 195 112 201 24 225 169 132 2 189 220 151 138 72 67 176 16 242 88 212 174 168 8 191 26 100 130 167 136 45 87 192 12 104 96 34 164 125 121 108 145 36 50 97 95 116 183 21 237 250 244 73 14 166 165

Stage2 “decryption”

Step 1: Converting the cypher code of amino acid to RNA sequences depending on key 3 and as shown Table 4:

CCACCACUGGCAGUACAAGUGAUUAAGUACAAGUACAAGUUAGUGUACUCGC
AAGUUAGUAAGCGUACAAGUUAGUGUACGUGACCCCCACUAAUUACUCGCGU

Step 2: Converting RNA sequence to cDNA sequence:

CCACCACTGGCAGTACAAGTGATTAAGTACAAGTACAAGTTAGTGTACTCGCAA
GTTAGTAAGCGTACAAGTTAGTGTACGTGACCCCCACTAATTACTCGCGT

Step 3: converting the cDNA sequence to DNA :

GGTGGTGACCGTCATGTTCACTAATTCATGTTCATGTTCAATCACATGAGCGTTC
AATCATTCGCATGTTCAATCACATGCACTGGGGGTGATTAATGAGCGCA

Step 4: converting DNA sequence to binary values:

10101110 10111000 01011011 01001110 11110100 01110000 11110100 11101111 01001110 11110100 00110100 01001110 00100110 11110100 00110100 11110110 01001110 11110100 00110100 01001110 01000111 10101010 10111000 11110000 11100010 01100100

Step 5: convert binary values to ASCII values:

174 184 91 78 244 112 244 239 78 244 52 78 38 244 52 246 78 244 52 78 71 170 184 240 226 100

Stage3 “Original Text Retrieval”

Step 1: Based on key 1 and key 2, the ASCII code of the original text is retrieved.

82 117 110 32 97 119 97 121 32 97 115 32 102 97 115 116 32 97 115 32 99 111 117 108 100 44

Step 2: Convert ASCII values to alphabet characters. Accordingly, the original text sent by the sender was obtained.

Original text: Run away as fast as you can."

14. Result and Discussion

The outcomes of the encryption and decryption processes, together with using Lina's image for hiding, are shown below. Before the hiding process, Lina's 256*256 image is displayed in Figure 3.

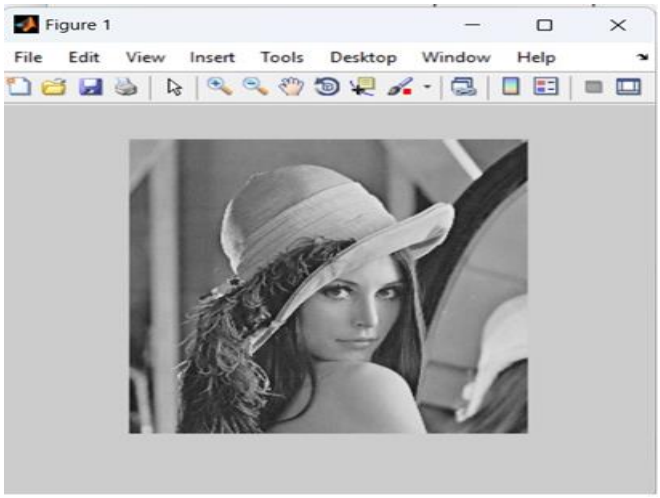

Figure 5: Original grayscale image.

Following the hiding process, Lina's image is displayed in Figure 4.

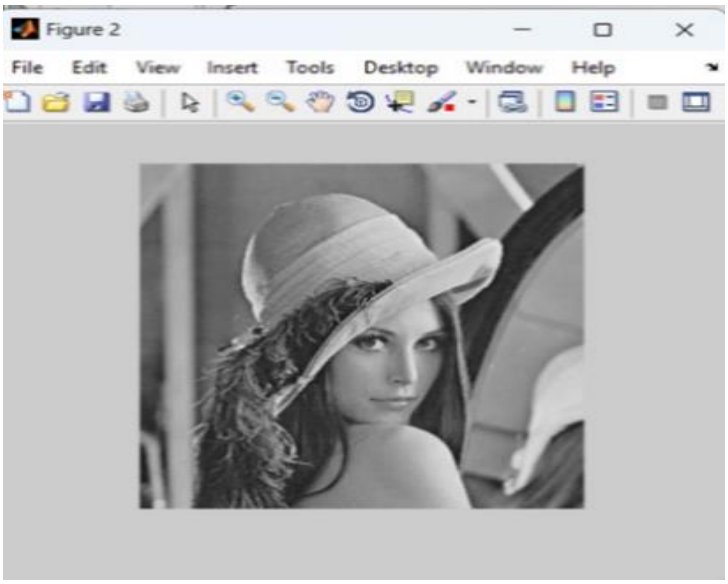

Figure 6: Stego image after embedded cipher keys.

The PSNR measure was used to evaluate the image quality during embedding. According to Eq. (1), PSNR determines the mean pixel variance between the stego image and the cover image. The higher the PSNR value, the better the signal performs against the noise [35].

PSNR = 10 * log10((MAX^2) / MSE) (1)

Where: MAX is the maximum possible pixel value of the image. MSE to calculate the total square error between the cover image and the stego image. The higher value of PSNR indicates better masking, as Table (4) shows these results.

Table 5: The PSNR value.

Text File Size in bits	Dimension Image	PSNR
200 bits	120*120	71.1261
1800 bits		57.2976
5048 bits		56.0100
13920 bits		49.4547
200 bits	256*256	82.2927
1800 bits		70.6515
5048 bits		69.8545
13920 bits		62.9982
200 bits	517*517	93.1054
1800 bits		80.0494
5048 bits		78.6100
13920 bits		70.7062

Table 6 below shows the time of encryption and decryption, depending on the length of the encrypted message and the size of the image in which encryption keys were hidden.

Table 6: Encryption/decryption time.

Length of message in bits	Dimension of Image	Encryption Time/ seconds	Decryption Time/ seconds
200 bits	120*120	0.189126	0.005070
1800 bits		0.395647	0.040492
5048 bits		0.303035	0.044977
13920 bits		1.119520	0.187466
200 bits	256*256	0.165566	0.021435
1800 bits		0.357626	0.047034
5048 bits		0.406864	0.060497
13920 bits		1.545142	0.257998
200 bits	517*517	0.217488	0.006349
1800 bits		0.359695	0.040046
5048 bits		0.694740	0.087239
13920 bits		2.786355	0.469305

15. Conclusion

Ultra-small information can be stored via DNA cryptography. Efficient algorithms are being implemented to bring DNA computing to the digital level and use it on a large scale. One of the primary focuses of researchers is investigating the many characteristics of DNA molecules and its application in cryptography. In order to increase the level of security, encryption and concealment techniques have been combined, and a hybrid technique has been invented. Asymmetric encryption keys have also been developed, which makes the system more secure. Where the encryption process's security comes from three levels: the length of the random key generated to produce the random number sequences, the key to access the cypher text locations in the random sequence, and the amino acid encoding key, the data can be accessed and decrypted only when these three keys are present.

16. Author Contributions

Conceptualization, the background theory for the paper, methodology analysis, implementation, and execution of the system, the first author has done test results. The second and third authors have done the visualization, review of the paper and project administration, investigation, validation, editing, and formal analysis.

References

[1] A. Priyadharshini Thiruthuvadoss, "Comparison and Performance Evaluation of Modern Cryptography and DNA Cryptography." 2013.

[2] E. Suresh Babu, C. Nagaraju, and M. H. M. Krishna Prasad, "Light-Weighted DNA-Based Cryptographic Mechanism Against Chosen Cipher Text Attacks," *Adv. Comput. Syst. Secur. Vol. 1*, pp. 123–144, 2016. https://doi.org/10.1007/978-81-322-2650-5_9

[3] A. Aich, A. Sen, S. R. Dash, and S. Dehuri, "A symmetric key cryptosystem using DNA sequence with OTP key," in *Information Systems Design and Intelligent Applications: Proceedings of Second International Conference INDIA 2015, Volume 2*, Springer, 2015, pp. 207–215. https://doi.org/10.1007/978-81-322-2247-7_22

[4] S. D. Athab and A. A. Karim, "Automatic Image and Video Tagging Survey," *Iraqi J. Sci.*, pp. 4865–4875, 2023. DOI: 10.24996/ijs.2023.64.9.44

[5] T. A. Anai, S. S. Mersal, and M.-S. M. Mostafa, "The Effect of Meta-heuristic Methods on the Performance of Image Classification," *Iraqi J. Sci.*, pp. 2881–2897, 2024. doi:doi.org/10.24996/ijs.2024.65.5.41

[6] A. Broumandnia, "Image encryption algorithm based on the finite fields in chaotic maps," *J. Inf. Secur. Appl.*, vol. 54, p. 102553, 2020. doi:doi.org/10.1016/j.jisa.2020.102553

[7] A. A. Rashid and K. A. Hussein, "A Lightweight Image Encryption Algorithm Based on Elliptic Curves and a 5D Logistic Map," *Iraqi J. Sci.*, pp. 5985–6000, 2023. **doi:** 10.1109/IT-ELA57378.2022.10107924

[8] M. Mundher, D. Muhamad, A. Rehman, T. Saba, and F. Kausar, "Digital watermarking for images security using discrete slantlet transform," *Appl. Math. Inf. Sci.*, vol. 8, no. 6, p. 2823, 2014. Available :http://dx.doi.org/10.12785/amis/080618

[9] T. Mahmood, Z. Mehmood, M. Shah, and T. Saba, "A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform," *J. Vis. Commun. Image Represent.*, vol. 53, pp. 202–214, 2018. doi:doi.org/10.1016/j.jvcir.2018.03.015

[10] T. Bhuiyan, A. H. Sarower, R. Karim, and M. Hassan, "An image steganography algorithm using LSB replacement through XOR substitution," in *2019 International Conference on Information and Communications Technology (ICOIACT)*, IEEE, 2019, pp. 44–49. doi: 10.1109/ICOIACT46704.2019.8938486

[11] X. Liao, J. Yin, M. Chen, and Z. Qin, "Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features," *IEEE Trans. Dependable Secur. Comput.*, p. 1, 2021, doi: 10.1109/tdsc.2020.3004708. doi: 10.1109/TDSC.2020.3004708

[12] H. Shaw, "A cryptographic system based upon the principles of gene expression," *Cryptography*, vol. 1, no. 3, p. 21, 2017. doi:doi.org/10.3390/cryptography1030021

[13] B. M. Krishna, H. Khan, and G. Madhumati, "Reconfigurable pseudo biotic key encryption mechanism for cryptography applications," *Int. J. Eng. Technol.*, vol. 7, no. 1.5, pp. 62–70, 2018. doi: Doi.org/10.14419/ijet.v7i1.5.9124

[14] S. Basu, M. Karuppiah, M. Nasipuri, A. K. Halder, and N. Radhakrishnan, "Bio-inspired cryptosystem with DNA cryptography and neural networks," *J. Syst. Archit.*, vol. 94, pp. 24–31, 2019. doi:doi.org/10.1016/j.sysarc.2019.02.005

[15] M. Indrasena Reddy, A. P. Siva Kumar, and K. Subba Reddy, "A secured cryptographic system based on DNA and a hybrid key generation approach," *Biosystems*, vol. 197, p. 104207, 2020, doi: 10.1016/j.biosystems.2020.104207. doi:doi.org/10.1016/j.biosystems.2020.104207

[16] E. Şatir and O. Kendirli, "A symmetric DNA encryption process with a biotechnical hardware," *J. King Saud Univ.*, vol. 34, no. 3, p. 101838, 2022. doi:doi.org/10.1016/j.jksus.2022.101838

[17] B. M. Krishna, C. Santhosh, S. Suman, and S. K. S. Shireen, "Evolvable hardware-based data security system using image steganography through dynamic partial reconfiguration," *J. Circuits, Syst. Comput.*, vol. 31, no. 01, p. 2250014, 2022. doi:doi.org/10.1142/S0218126622500141

[18] N. M. Abbas and M. E. Abdulmunim, "mRNA Approach Image Encryption Using LUC Algorithm," *Iraqi J. Sci.*, pp. 2545–2560, 2023. doi: 10.24996/ijs.2023.64.5.37

[19] L. M. Adleman, "Molecular Computation of Solutions to Combinatorial Problems," *Science (80-.).*, vol. 266, no. 5187, pp. 1021–1024, 1994, doi: 10.1126/science.7973651.

[20] A. Hazra, S. Ghosh, and S. Jash, "A Review on DNA Based Cryptographic Techniques.," *Int. J. Netw. Secur.*, vol. 20, no. 6, pp. 1093–1104, 2018. doi: 10.6633/IJNS.201811 20(6).10

[21] A. El-deeb, A. Elsisi, and A. Youssef, "A Substitution-based method for data hiding in DNA sequences," *IJCI. Int. J. Comput. Inf.*, vol. 8, no. 1, pp. 87–105, 2021. doi: 10.21608/ijci.2021.56184.1037

[22] A. Smith, "Nucleic acids to amino acids: DNA specifies protein," *Nat. Educ.*, vol. 1, no. 1, p. 126, 2008. **doi:** 10.4103/0971-6866.124354

[23] Handrizal, J. T. Tarigan, and D. I. Putra, "Implementation of Steganography Modified Least Significant Bit using the Columnar Transposition Cipher and Caesar Cipher Algorithm in Image Insertion," *J. Phys. Conf. Ser.*, vol. 1898, no. 1, p. 12003, 2021, doi: 10.1088/1742-6596/1898/1/012003.

[24] S. Shi, Y. Qi, and Y. Huang, "An approach to text steganography based on search in internet," in *2016 International Computer Symposium (ICS)*, IEEE, 2016, pp. 227–232. **doi:** 10.1109/ICS.2016.0052

[25] A. U. Islam *et al.*, "An improved image steganography technique based on MSB using bit differencing," in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, IEEE, 2016, pp. 265–269. **doi:** 10.1109/INTECH.2016.7845020

[26] S. N. Mohammed, "Color Image Steganography Using Gradient Selective Bezier Curves," *Iraqi J. Sci.*, pp. 3625–3641, 2023. doi: 10.24996/ijs.2023.64.7.39

[27] V. S. Kamatar and V. P. Baligar, "Image Compression Using Mapping Transform with Pixel Elimination," *Iraqi J. Sci.*, pp. 4704–4718, 2023. doi: 10.24996/ijs.2023.64.9.33

[28] K. Bhowal, D. C. SARKAR, S. Biswas, and P. P. Sarkar, "A steganographic approach to hide secret data in digital audio based on XOR operands triplet property with high embedding rate and good quality audio," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 25, no. 3, pp. 2136–2148, 2017. **doi:** 10.3906/elk-1602-267

[29] R. J. Mstafa and K. M. Elleithy, "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes," *Multimed. Tools Appl.*, vol. 75, pp. 10311–10333, 2016. doi:doi.org/10.1007/s11042-015-3060-0

[30] M. Islam, M. Shah, Z. Khan, T. Mahmood, and M. J. Khan, "A new symmetric key encryption algorithm using images as secret keys," in *2015 13th International Conference on Frontiers of Information Technology (FIT)*, IEEE, 2015, pp. 1–5. **doi:** 10.1109/FIT.2015.12

[31] L. Fillatre, "Adaptive Steganalysis of Least Significant Bit Replacement in Grayscale Natural Images," *IEEE Trans. Signal Process.*, vol. 60, no. 2, pp. 556–569, 2012, doi: 10.1109/tsp.2011.2174231.

[32] X. Bi, X. Yang, C. Wang, and J. Liu, "High-capacity image steganography algorithm based on image style transfer," *Secur. Commun. Networks*, vol. 2021, pp. 1–14, 2021. doi:doi.org/10.1155/2021/4179340

[33] A. Rehman, T. Saba, T. Mahmood, Z. Mehmood, M. Shah, and A. Anjum, "Data hiding technique in steganography for information security using number theory," *J. Inf. Sci.*, vol. 45, no. 6, pp. 767–778, 2019. doi:doi.org/10.1177/0165551518816303

[34] F. Crick, "Central dogma of molecular biology," *Nature*, vol. 227, no. 5258, pp. 561–563, 1970. doi:doi.org/10.1038/227561a0

[35] A. A. Abdallah and A. K. Farhan, "A New Image Encryption Algorithm Based on Multi Chaotic System," *Iraqi J. Sci.*, pp. 324–337, 2022, doi: 10.24996/ijs.2022.63.1.31.