Journal of Theoretical and Applied Information Technology
15th January 2019. Vol.97. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HIDDEN ENCRYPTED TEXT BASED ON SECRETE MAP EQUATION AND BIOINFORMATICS TECHNIQUES

[1] ALAA KADHIM F., [2] RASHA SUBHI ALI

[1] Computer Sciences Department, University of technology/ Baghdad, Iraq

dralaa_cs@yahoo.com

[2] Department of Computer Techniques Engineering, AL Nisour University College/ Baghdad, Iraq

danafush@Gmail.com

ABSTRACT

The speedy development in informationtechnology desires the secure transmissionof confidential information that gets an excellent deal ofattention. Therefore; it's necessary to use effective methods to reinforce information security. Steganography is one in all leading technologies getting utilized around the world for along time. Biotechnological methods can be used for cryptography to improve security of data. Steganography is the act of hiding messages inside an image. Combining these two methods is a topic of high relevance since secure communication is inevitable for mankind. This research presents an analysis of steganography, by using LeastSignificantBit (LSB), DNA computing and creating a secret map for hiding data. The DNA computing was used to encrypt secret data, LSB was utilized to add the encrypted data into leastsignificantbits of the cover and the secret map was utilized to specify the location of hiding data. The same equation must be used by the sender and the receiver to create the secret map and the creation for this map depends on the shared key.

Keywords- *Least Significant Bit (LSB), DNA Computing, Secret Map, Steganography.*

1. INTRODUCTION

Data security has become a big resource nowadays for the effective operations of the various demands of any organization. One among the most necessary demands of those networks is to supply secure transmission of knowledge from one place to a different. Cryptography is one among the mechanisms that give most secure way to transfer the sensitive info from sender to supposed receiver. Its major aim is to create sensitive info unclear to all or any totally different, except the supposed receiver [1]. Data hiding is that the method of in secret embedding info within a data sources without ever-changing its perceptual quality. Information hiding is that the art and science of writing hidden messages in a way that no-one except the sender and supposed recipient even realizes there is a hidden message. The goal of steganography is to hide a message m in any audio or video (cover) data d, to induce new data d, practically indistinguishable from d, by people, in such how that associate snooper cannot discover the presence of m in d [2]. Image Steganography for data Security 1st we tend to write data with the assistance of desoxyribonucleic acid algorithmic rule then we tend to choose secrete image that we would like to transfer with data and that secrete image is additionally used to hide encrypted information [3]. Shortly, the cryptography used for protecting the content of messages; steganography utilized for concealing its terribly existence. With the inclusion of newer cover media and stronger algorithms we are able to deal with the most recent attacks [4]. The advantage of hiding data over cryptography alone is that the intended secret message doesnot attract attention to itself as an object of security. Desoxyribonucleic acid secret writing is one in every of the foremost secure cryptography and decryption technique. Desoxyribonucleic acid (DeoxyribonucleicAcid). DNA is considered as the genetic pattern of living or existing creatures. All individual body cells have a complete set of DNA. DNA is a polymer madeout of monomers called DeoxyriboseNucleotides. A DNA sequence consists of four nucleic acid bases A (adenine), C (cytosine), G (guanine), T (thymine), where A and T are complementary, and G and C are complementary withinthe secretwriting algorithmic the desoxyribonucleic acid writing rule performed as a part of secret key and DNA addition and subtraction operations is employed to confuse the DesoxyribonucleicAcid sequences. Eight desoxyribonucleic acid map rules are used to satisfy the Watson Crick complement rule the detailed of desoxyribonucleic acid conversion was shown in table 1 [5]. The number of possible coding patterns is illustrated in table 1. Steganography incorporates a range of drawbacks compared to encryption. It needs to Ns of overhead to hide a comparatively few bits of information, though utilizing some scheme like that proposed within the preceding paragraph could build it more effective or else a message can be 1st encrypted and then hidden by utilizing steganography[4]. The main purpose of this study is hiding secret data by using secret map, LSB and DNA cryptosystem, which is a new science in information security. In this research a new the cryptography and steganography methods was used and implemented to encrypt the data that was required to be hiding in the cover image. The objective of stenography is to avoid drawing suspicion to the transportation of the secret message between sender and receiver.

A secure data transmission is made using cryptography and stenography. A combination of both these two techniques results in appearing a highly secured method for data communication [6]. Steganography involves four steps [7]:

1. Choice of the cover media within which the info are going to be hidden.

2. The secret message or data that's required to be masked within the cover image.

3. A function which will be wont to hide information| within the cover media and its inverse to retrieve the hidden data.

4. An optional key or the password to certify or to hide and unhide the info.

Table 1: Eight Map Rules [5]

	1	2	3	4	5	6	7	8
0	A	A	C	C	G	G	T	T
1	C	G	A	T	A	T	C	G
2	G	C	T	A	T	A	G	C
3	T	T	G	G	C	C	A	A

Table 2: addition and subtraction operations on DNA nucleotides

+	A	T	C	G		-	A	T	C	G
A	T	G	A	C		A	C	G	A	T
T	G	C	T	A		T	A	C	T	G
C	A	T	C	G		C	G	T	C	A
G	C	A	G	T		G	T	A	G	C

Table 3: XOR operation on DNA nucleotides [8]

⊕	A	T	C	G
A	A	T	C	G
T	T	C	G	A
C	C	G	A	T
G	G	C	T	A

Steganography hides the existence of a secret message and within the best case no one will see that eachparties are communicating in secret. This makes steganography applicable for some tasks that secret writing aren't, comparable to copyright marking. Table four shows a comparison of varied techniques for communicating in secret [9].

TABLE 4: COMPARISON OF SECRET COMMUNICATION TECHNIQUES

SECRET COMMUNICATION TECHNIQUE	CONFIDENTIALITY	INTEGRITY	UMREMOVABILITY
ENCRYPTION	YES	NO	YES
DIGITAL SIGNATURES	NO	YES	NO
STEGANOGRAPHY	YES/NO	YES/NO	YES

2. IMAGE STEGANOGRAPHY

The most wide used technique these days is hiding secret messages into a digital image. This steganography method exploits the failure of the human visual system(HVS). The HVS cannot detect the difference in luminance of color vectors at set of pixels color. Forexample:a24-bit picture can have 8bits, representing every 3 color values (red, green, and blue) at every pixel. If we have a tendency to take into account just the blue there'll be two totally different values of blue. The distinction between11111111and11111110within the value of blue intensity is probably going to be undetectable by the human eye. Hence, if the terminal recipient of data} is nothing however human the least (HVS) then the least significant Bit (LSB) are often used for one thing else excluding color information. The only approach to hiding information within a picture file is termed least significant bit (LSB) insertion [10].

The LSB is that the lowest bit in an exceedingly series of numbers in binary E.g. within the binary number:10110001, the least significant bit is much right one. The LSB primarily based Steganography is one in all the steganographic strategies, utilized to embed the key information into the least significant bits of the pixel values in an exceedingly cover imageE.g. 240 can be hidden within the 1st eight bytes of 3 pixels in an exceedingly 24 bit image [11].

PIXELS: 00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001
240 : 011110000
RESULT: 00100110 11101001 11001001
00100111 11001001 11101000
11001000 00100110 11101000

Here the number240is embedded into first eight bytes of the grid and only 6 bits are changed.

3. SOME METRICS FOR PICTURE QUALITY EVALUATION (PQE) [12] [10]

For the sake of measuring the quality of the encrypted image must be using the Picture Quality Evaluation (PQE),which is depicted in below points [13] [14]:

1. **Mean Square Error (MSE):** It is the measurement of thesquare oferror, the error isthe amount by which the originalimage's pixelvalue is different to the encryptedimage's pixelvalue.

$$\boldsymbol{MSE} = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{[f(i,j) - f`(i,j)]^2}{MN}$$

Where, M and N represent theimage's height and width respectively. f (i, j) isthe $(i,j)^{th}$pixelvalue of the originalimage and $f'(i, j)$ isthe $(i,j)^{th}$the value of thepixel of the decryptedimage.

2. **Peak Signal to Noise Ratio (PSNR):** Represents theratio between the maximum probablesignal power and the power of corrupting noise whichinfluences the fidelity ofits representation. PeakSignaltoNoiseRatio is typicallyrepresented in terms of thelogarithmic decibel. PeakSignaltoNoiseRatiois calculated by:

$$PSNR = \frac{10\log(2^n - 1)^2}{MSE}$$

3. **Average Difference (AD):** Itis the averageerror measurement between bothimages the originalone and the decryptedone and is calculated as:

$$\boldsymbol{AD} = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{[f(i,j) - f`(i,j)]^2}{MN}$$

Where;$[f(i, j) - f'(i, j)]$correspond to the error between the pixelvalue of the originalimage and the pixelvalue of the decryptedimage at height i and width j.

4. **Maximum Difference (MD):** It is themeasurement of the maximumerror value between bothimages the originalone and the decrypted one.

$$\boldsymbol{MD} = Max|(f(i,j) - f'(i,j))|$$

The Maximum error for graylevel image is upto255;while the originalimage pixelvalue at (I, j)is255 and the decryptedimage pixelvalue at(i, j) *isequal to*0. The maximal difference between bothimages the original and the decryptedone is supposedto be minimum, for the sake of preserving thequality of theimage.

5. **Normalized Cross-correlation (NC):** It is a measure of how the decrypted imagepixel value at (I ,j) is connected with the originalimage pixelvalue at (I ,j) when there is nodistortion in the decryptedimage, then NormalizedCross-correlation will be equivalent to 1.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j) - f`(i,j)]^2}{\sum_{i=1}^{M}\sum_{j=1}^{N} f(i,j)^2}$$

6. **Mean Absolute Error (MAE):** It is a number utilizedfor mesuring how close predictions or forecasts are tothe genuineoutcomes.

$$\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|f(i,j) - f`(i,j)|^2}{MN}$$

7. **Normalized Absolute Error (NAE):** It is the sumof diffirences among both the originalimage f(i, j) and the decryptedimage f ′(i, j) divided by the sum ofthe pixel square value for the originalimage.

$$\boldsymbol{NAE} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|f(i,j) - f`(i,j)|^2}{\sum_{i=1}^{M}\sum_{j=1}^{N} f(i,j)^2}$$

8. **Structural Content (SC):** It is the sum of pixels'square values for the originalimage divided by the pixelsquare values for the decryptedimage, it is also a measuree for the corrrelation between the twoimages, the SC will be equivalent to1 if there is nodistortion in the decryptedimages.

$$\boldsymbol{SC} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} f(i,j)^{2'}}{\sum_{i=1}^{M}\sum_{j=1}^{N} f`(i,j)^2}$$

9. **Signal-To-Noise Ratio(SNR):** It is a measurement utilized in science and engineering that compares the levelof the desiredsignal to the levelof backgroundnoise. It is defined as the ratio ofsignal power tothe noisepower, often expressedin decibels. A ratio higher than1:1(greater than0dB)indicates there is more signal than noise. WhileSNR is commonly quoted for electricalsignals, it can be applied toany form ofthe signal.

$$\boldsymbol{SNR} = \sqrt{\frac{\sum_{i=1}^{M}\sum_{j=1}^{N} f`(i,j)^{2'}}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(f(i,j) - f`(i,j)\right)^2}}$$

10. **Similarity Measure (SIM):** It is utilized for measurring the similaritybetween twoimages. SSIM is designed to improve on traditionalmethods such as **PSNR**and**MSE**; which have proven to beinconsistent with humanvisual perception.

$$SIM = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} f(i,j) \ast f`(i,j)'}{\sum_{i=1}^{M}\sum_{j=1}^{N}\sqrt{f(i,j)} \ast \sqrt{f`(i,j)}}$$

11. **Unified average changing intensity Measure (UACI):** The UACI measuress the average intensity of differences between the plainimage and cipheredimage.

$$UACI = \frac{1}{W \ast H}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|f(i,j) - f`(i,j)|}{256}\right] \ast 100\%$$

12. **Delay:** It is the timetaken by the process of steganography or cryptography with steganography.

4. DESIGN AND IMPLEMENTATION

Secrets can be hidden in all forms of cover info. Thefollowing formula provides a very generic description of the steganographic process:

cover_medium + hidden_data + secret map = stego_medium

In this context, the cover_medium means that the file in that the hidden_data are going to be hidden. The resultant file is that the stego_medium (which can, of course, be identical kind of file as the cover_medium). There are four ways that to implement steganography using (text; images; audio files or video files). For security, most effective encryption might not be enough; as a result the proposal consists of Steganography wherein encrypted data is hidden in the image after which the stego_image is transmitted inside the network.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

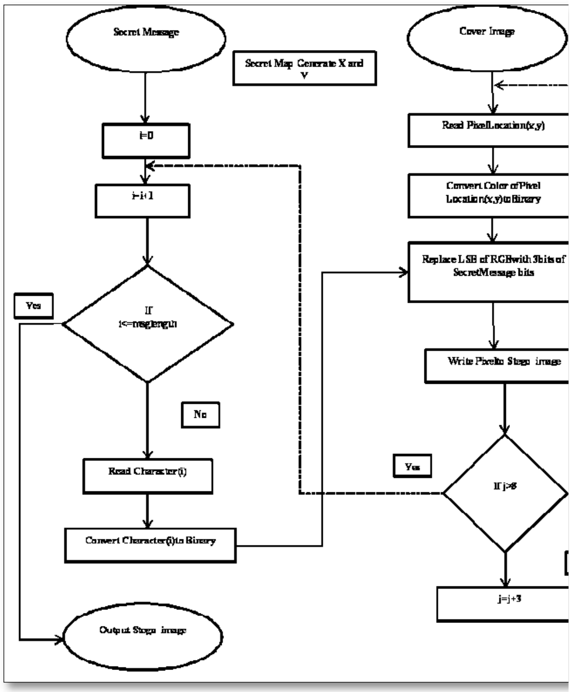


Figure1: The Proposed Method

1. Key generation process: Read the secret key and converting it to DNA codon. There are many approaches for converting the binary data to DNA sequence and these are known as DNA coding technology. In this study the conversion of DNA sequence depends on the DNA coding rules that are shown in tables (I and II) sequentially. The key generation process explained in figure 2 with an example for each step.

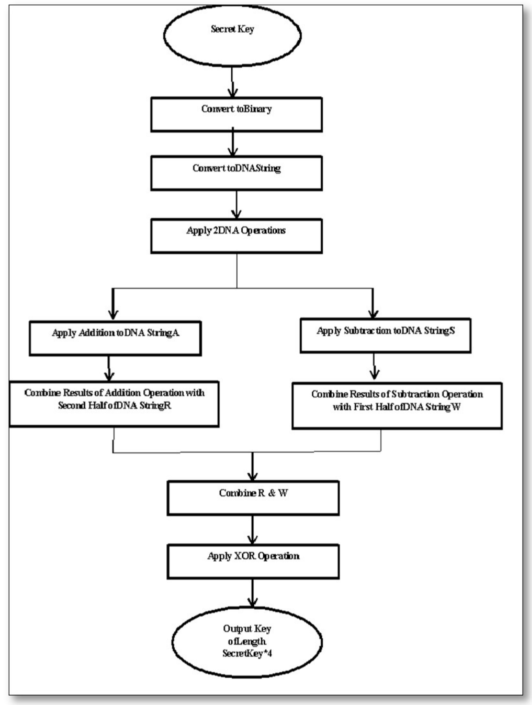


Figure 2: key generation

Example about key generation let

Secret Key=asd

Binary=011000010111001101100100

DNAString=CCCTACTACCAC

Addition=CTAGCA

Subtraction=TACTCC

Combine Subtraction with first half of DNA String=TACTCCCCCTAC

Combine Addition with second half of DNA String=CTAGCATACCAC

Combine Pervious Results=CTAGCATACCACTACTCCCCCTAC

XOR Operation=GTCCACGCAGAA

Output=GTCCACGCAGAA

Length=3*4=12 Characters

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The following steps in figure 3 used to convert user strings to the DNA coding scheme:

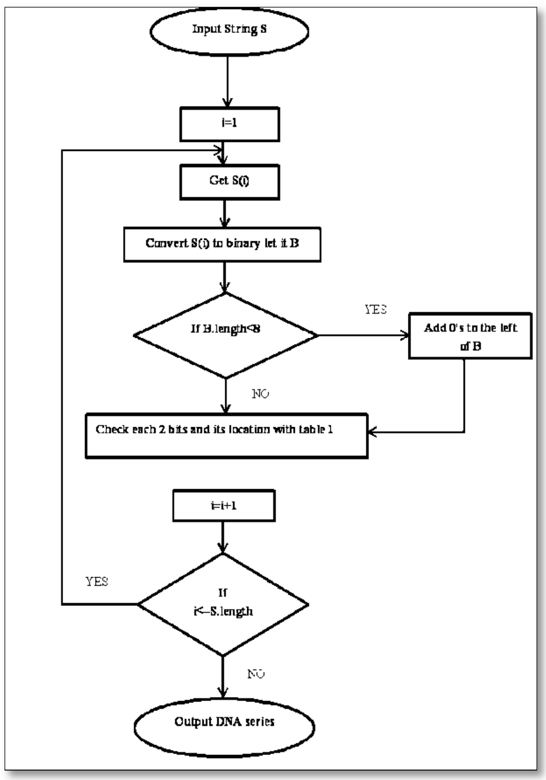


Figure3: Conversion to DNAcodes

After conversion strings to DNA codon apply 2 DNA operations on this string (addition and subtraction operations). In the next step combine results of addition operation with the second part of the DNA string let it be (R) and combine the results of the subtraction operation with the first part of the DNA string let it be (W). Finally combine R and W, and finally the DNA XOR operation is implemented for the combination to produce the output key (the output key length=key length*4).

2. Encryption process: Read the plain text (secret message) and encrypting it by using the XOR operation with the generated, then check the size of the secret message with that of the cover image such that the size of the secret message should be less than the size cover image. After that the secret map will be generated depending on the length of the secret message. The secret map should be same on both sides (sender and receiver sides). The steps of encryption process are explained in figure 4 with an example.

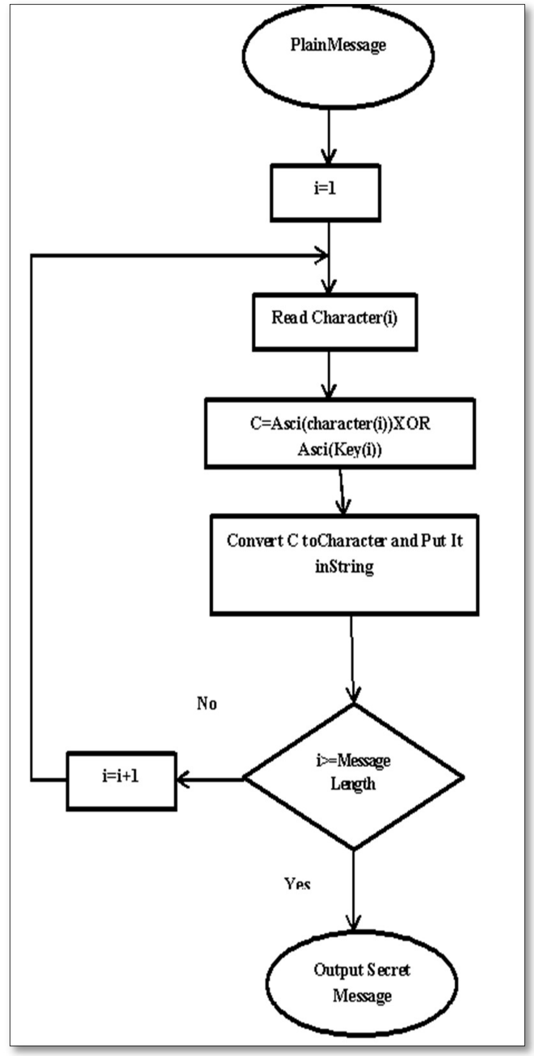


Figure4: Encryption Process

Example about Encryption Process let

Plain Message=Computer

Character (i)=C

Cipher=Chr (Asci(C)XOR Asci(G)=_

i=1

i<=8

i=i+1=2

Cipher=Chr(Asci(o)XOR Asci(T))=(

This process ending until last message character is reached

3. Steganography process: this concept includes reading the cover image data, secret map locations and secret message. After that each character of secret message is converted to binary data, if the length of binary data less than 8 bits the padding it left by0's. Each character of the secret message will be hiding in 3 pixels. In this work the LSB method will be used for hiding data. The steps for hiding and retrieving data are illustrated in the algorithm (1 and 2):

Algorithm1 to hide text message:-

Input: Cover image, Secret message, Secure lookup table

Output: stego_image.

Begin:

Step 1: Read the cover image and secret message which is to be hidden in the cover image.

Step 2: Read secret message and write the length of secret message into the secret location shared between the sender and receiver

Step 3: Generate hiding locations by using 2 secret maps.

Hiding locations= message length*3 e.g. if message length= 3 characters, then hiding locations=3*3=9

Secret maps: first one for x location and second one for y location.

X=(i + messageLength) Mod (picture.Width - 1)) + 1

Y= ((asc1(s((i Mod messageLength) + 1)) + X) Mod (picture.Height - 1))

Where i from 1 to messageLength*3 ,s(i) is an array for message characters and asc1 extract asci code value for the message characters depending on secure lock up table.

Step 4: For each character in the secret message do

Step 5: Convert the character to binary form.

Step 6: For each character read three locations from secret map, these locations include the pixel position in the cover image.

Step 7: Calculate LSB of each pixel in secret map of cover image.

Step 8: Replace LSB of the cover image with each bit of secret message one by one.

Step 9: Write stego image.

End.

Example for hiding text=Computer and key=asd

First step generates key as shown in figure 2 and after that encrypt message as shown in figure4.

1- The encrypted message=secret message=_(9365&5

2- Key Length =3

Write Message Length in pixel (3,3) in Red value

3- Select locations for hiding secret message hiding locations=MessageLength*3=8*3=24 pixels

The first location for this example X=9 and Y=106

Second location X=10 and Y=125

This process continued until generate 24 locations

4- Convert characters of the Secret Message to binary

5- Hide each character in 3 pixels in LSB of RGB values as shown in example1

6- Write the result to the Stego_image

7- This process continued until all secret message characters are hidden

Algorithm2 to retrieve text message:-

Input: Stego_image image, Secret Key, Secure lookup table

Output: Plain message.

Begin:

Step 1: Read the stego image.

Step 2: Extract the length of message from the shared secret location.

Step 3: Generate hiding locations by using 2 secret maps.

Hiding locations= message length*3 e.g if message length= 3 characters, then hiding locations=3*3=9

Secret maps: first one for x location and second one for y location.

X=(i + messageLength) Mod (picture.Width - 1)) + 1

Y= ((asc1(s((i Mod messageLength) + 1)) + X) Mod (picture.Height - 1))

Where i from 1 to messageLength*3 ,s(i) is an array for message characters and asc1 extract asci code value for the message characters depending on secure lock up table.

Step 4: From each location in the secret map calculates LSB of each pixel of stego image.

Step 5: For getting one byte repeat step 4 for 8 locations.

Step 6: Retrieve bits and convert each 8 bits into a character.

Step 7: Repeat step 4 to 6 until achieving maximum length of the message.

End.

The main steps for hiding and extracting data are summarized in the following steps:

Firstly an image is read from the computer; generate 3 locations for each character and then convert the character and RGB values of the extracted location to binary form. After that, the message characters are embedded using the LSB method for each character 3 pixels were needed. Next, writing the results of substitution into the stego_image, then hide the message length into image cover in pixel (key length, key length) in Red Value. Finally the extraction process, this process includes extracting the length of the secret message and secret message which was embedded during the embedding process in the first step. At first declare message bytes by reading a pixel location from the secret map starting from the first location of the secret map (for extracting one byte we need to read 3 locations from secret map). Extract the LSB bits and put it in k, when k =8, a byte is extracted. Repeat for extracting next byte.

5. ANALYSIS & RESULTS

In this work, vb.net is implemented for processing the proposed system. The performance measure depends on the success rate of the implementation of the overall system with respect to the following points.

a) The integrity of the hidden information should not change after embedding.

b) The stego _image must remain almost remain unchanged to the naked eye.

c) There should be accuracy in the extracted data.

In order to demonstrate the online transmission of hidden data by using the proposed system. At the sender side, it is required to provide original image, creating of secret map, secret key, DNA table coding and secret message to be hiding in the stego_image. At the receiver side, it is required to provide stego_image, creating secret map, secret key, DNA table coding, retrieving the encrypted message and finally decrypting the retrieved message to get the plain text.

The analysis and results of this work illustrated in five measures:

1- Time space

2- Complexity

3- Key space

4- Brute force attack, and

5- Statistical tests: these tests include several parameters like MSE, PSNR, AD, MDR, MDG, MDB, NC, MAE, NAE, SC, SNR, UACI and SIM. The values for these parameters are shown in table 5.

5.1 Time space

This measurement involved the consumed time for encryption, decryption, hiding and retrieving messages. The consumed time was shown in table 4.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 4: Time consuming for encryption hiding data and decryption retrieving data

File name	File size	File Type	Length of secret msg	E+S time	D+S time
computer	8 k	jpg	90	0.49	1.165
download	12 k	jpg	46	0.315	0.622
download	149 k	bmp	46	0.268	0.484
download	149 k	Bmp	78	0.369	0.836
images(3)	11 k	Jpg	74	0.418	0.915
images flower	7k	Jpg	143	0.634	1.433
images flower	7k	Jpg	37	0.261	0.512
images flowerbmp	149 k	Bmp	26	0.177	0.342
Images	11 k	Jpg	39	0.24	0.484
imagesbmp	148 k	Bmp	39	0.239	0.466
imagesGIF	28 k	GIF	39	0.237	0.472
imagespng	137 k	Png	39	0.249	0.478
lena original	21 k	Jpg	46	0.351	0.619
lena originalpng	79 k	Png	46	0.306	0.52
lena originalbmp	118 k	Bmp	129	0.589	1.34
Pappers	9 k	Jpg	37	0.196	0.418

E+S time=consumed time for Encryption and Steganography process

D+S time=consumed time for Decryption and Retrieval message process

The time was measured in milliseconds, it is noted that the proposed algorithm consumed too small amount of time for encryption, hiding data, decryption, and retrieving messages. The time taken does not exceed a second.

5.2 Complexity

For the proposed method to be broken the attacker needs to know the utilized algorithm, secret key, length of key, length of encrypted message, secret maps for generating hiding locations, location of hiding message length, which color value the length of message was embedded, key generation algorithm and finally there is important thing needs to know the secure lock up table which is shared between the sender and receiver, these seven objects are increased the complexity of the proposed method. So, if the attacker gains one of these requirements, then it was remaining needs another eight things to gain the plain message. The strength of the proposed method depended on this nine points.

5.3 Key space

In this work the key space is varying from user to another. The key length was not fixed and it was depended on utilized secret key of the receiver, but the length of generating key equal to the three time utilized key length.

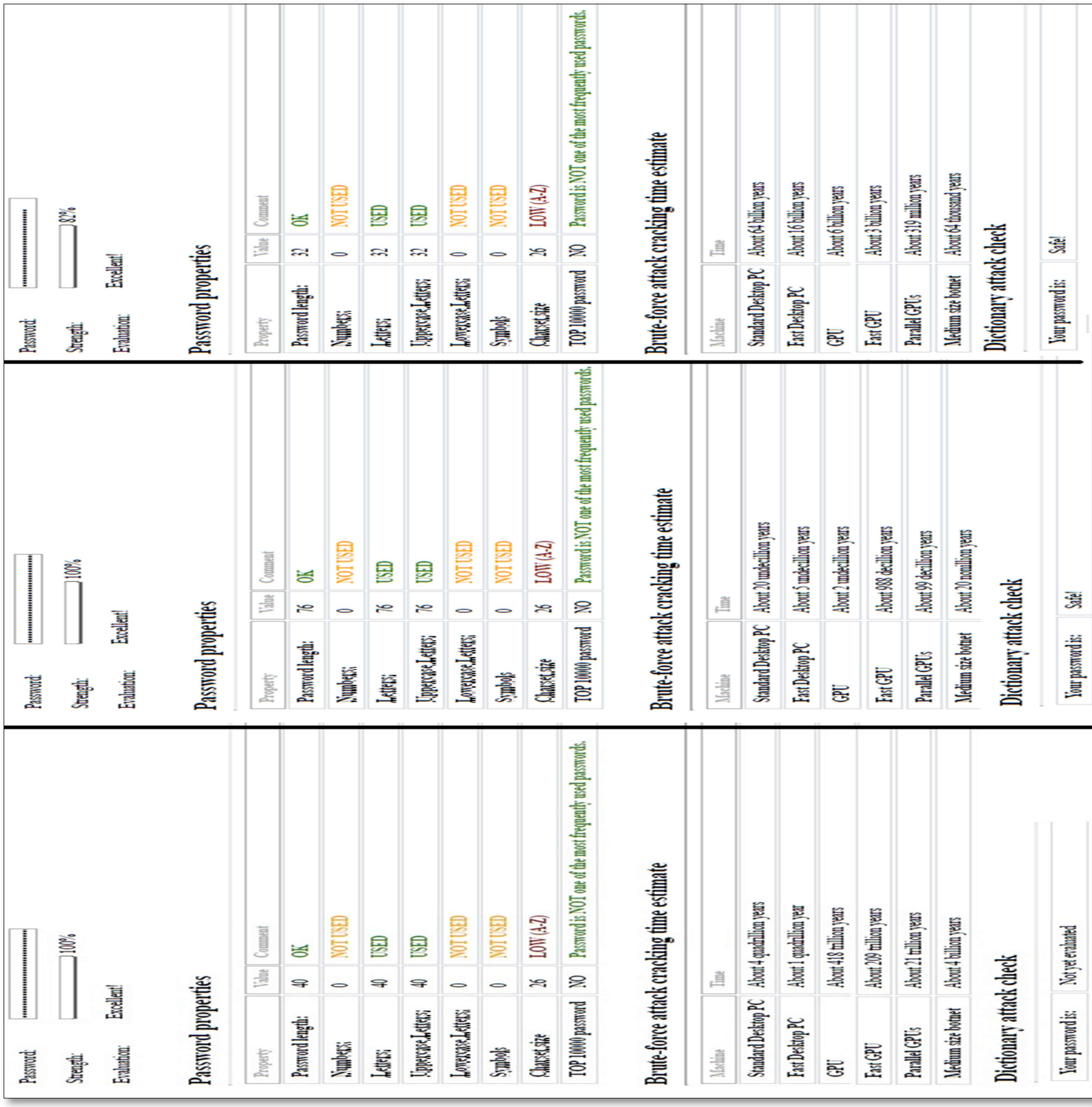
5.4 Brute force attack

In cryptography, a brute force attack consists of an attacker trying many keys generated from password with a hope of guessing pthe correct key. The attacker checks all possible keys until the correct one is guessed. The following reports show that the generate key using the proposed method cannot be broken by using brute force attack.

Journal of Theoretical and Applied Information Technology
15th January 2019. Vol.97. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Report: brute force attack tests for passwords of length 10, 11 and 8 characters respectively.



5.5 Statistical tests

The test images differ in their sizes, and hidden data also differ in their sizes. The hidden data composed Arabic characters, English (capital and small letters), symbols and numerical data. From table 5 it is noted the proposed method produced a good result, there is slightly different even when hiding large amounts of data; the similarity between the original image and stego_image a proximity more than 99 %, it is clear in table 5 while for ciphering image the SIM measurement should be decreased a proximity equal to zero. The comparison between original images and stego_images was presented in figure 5, and this is shown that there are universal changes (nobody can see the hidden data) between the original and stego_images. The UACI measures the average intensity of differences between the plain image and stego_image or ciphered image, the result of UACI for ciphered image should be between 32 and 33 but for stego_image should be nearing to zeroes and this is presented in table 5; it was very near for zeroes. PSNR for steganography should be increased, the best results when the PSNR value is high. While the PSNR for ciphered image should be decreased. Also, another measurement the MSE, for steganography this

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

measurement should be decreased and this was shown in table 5; but the MSE for ciphered image should be increased.

Table 5: Result of Statistical Tests for the Proposed Method

File name	File size	File Type	Length of secret msg	MSE	PSNR	AD	MDr	MDg	MDb	NC	MAE	NAE	SC	SNR	UACI	SIM %
Computer	8 k	jpg	90	0.008	89.36	0.008	1	1	1	1	0.008	1	1	69.2	0.003	99.9
Download	12 k	jpg	46	0.004	95.77	0.004	1	1	1	9.4	0.004	9.4	1	70.2	0.001	99.8
Download	149 k	bmp	46	0.004	95.77	0.004	1	1	1	9.4	0.004	9.4	1	70.2	0.001	99.8
Download	149 k	bmp	78	0.007	90.7	0.007	1	1	1	1.6	0.007	1.6	1	67.7	0.002	99.8
images(3)	11 k	jpg	74	0.005	92.8	0.005	1	1	1	8.1	0.005	8.1	1	70.9	0.002	99.9
images flower	7 k	jpg	143	0.013	85.62	0.013	1	1	1	8.7	0.013	8.7	1	70.6	0.005	99.9
images flower	7 k	jpg	37	0.003	97.2	0.003	1	1	1	2.2	0.003	2.2	1	76.5	0.001	99.9
images flowerbmp	149 k	bmp	26	0.002	99.19	0.002	1	1	1	1.8	0.002	1.8	1	77.5	0.001	99.9
Images	11 k	jpg	39	0.003	96.78	0.003	1	1	1	5.4	0.003	5.4	1	72.7	0.001	99.8
Imagesbmp	148 k	bmp	39	0.003	96.78	0.003	1	1	1	5.4	0.003	5.4	1	72.7	0.001	99.8
imagesGIF	28 k	GIF	39	0.003	97.8	0.003	1	1	1	4.7	0.003	4.7	1	73.2	0.001	99.8
Imagespng	137 k	png	39	0.003	96.78	0.003	1	1	1	5.4	0.003	5.4	1	72.7	0.001	99.8
lena original	21 k	jpg	46	0.004	94.24	0.004	1	1	1	1.4	0.004	1.4	1	68.6	0.001	99.7
lena_originalpng	79 k	png	46	0.005	94.1	0.005	1	1	1	1.4	0.005	1.4	1	68.6	0.001	99.7
lena_originalbmp	118 k	bmp	129	0.013	85.62	0.013	1	1	1	3.4	0.013	3.4	1	64.3	0.005	99.7
Pappers	9 k	jpg	37	0.003	98.03	0.003	1	1	1	5.9	0.003	5.9	1	72.3	0.001	99.99

Journal of Theoretical and Applied Information Technology
15th January 2019. Vol.97. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Original Image	Stego_Image	Hiding Message
		Digital image encryption techniques play crucial roles in preventing unauthorized access.
		International Data Encryption Algorithm (IDEA)
		International Data Encryption Algorithm (IDEA)
		The S-box is an important part in the structure of any block symmetric system.
		Proposal New S-Box Depending on DNA computing and Mathematical Operations
		A block cipher is considered to detect the avalanche effect if for a single change in a single bit of the input, the output varies drastically.
		Cluster: A collection of data objects
		Differential Cryptanalysis
		DNA ADDITION AND SUBTRACTION OPERATION
		DNA ADDITION AND SUBTRACTION OPERATION
		DNA ADDITION AND SUBTRACTION OPERATION
		DNA ADDITION AND SUBTRACTION OPERATION
		Message Transmission Based on DNA Cryptography
		12/18/2011 [illegible] 38 [illegible]
		The operations used for transforming plaintext to cipher text is based on general principle: (a) Substitution, (b) Transposition.
		A Brief History of Information Hiding

6. CONCLUSION

This paper proposes to design an effective scheme for efficient Secure Image Steganography design using DNA sequence based on DNA Cryptography, LSB technique and secret map for creation hiding locations. LSB primarily based steganography imbed information within the least significant bits of digital pictures. The LSB insertion may be a common and straightforward approach for embedding info into cover file. DNAsequencing is any method usedto design the sequence of thenucleotides that comprise astrand ofDNA. The data was encrypted with the help of DNA sequence (for creating keys) , XOR operation for encrypting data and secure asci code lookup table. After that the locations for hiding secret data was generated by using two secret maps. The secret data was hidden by cover image with the help of Image Steganography. This paper provides effective steganography technique, so that the person can detect the variety of choosingthe method to protect theinformation. In Image Domain, we tend to mentioned the foremost powerful technique referred to as LSB to hide information specially within images in any format (BMP, JPG, PNG and….etc). The proposed method takes few milliseconds for encryption and steganography processes. Also, the statistical tests show the proposed method achieves good results. The results of similarity measure proximity 99.8 %, so the hiding data cannot be detected without knowing (the utilized algorithm, secret key, length of key, length of encrypted message, secret maps for generating hiding locations, location of hiding message length, which color value the length of message was embedded, key generation algorithm and finally there is important thing needs to know the secure lock up table which is shared between the sender and receiver). Also, the other statistical test give a good results such as (MSE, PSNR, UACI, …..etc). Finally this paper ends with Application of a good new steganography method.

REFERENCES

[1] Kadhim F, Majeed G, Ali R. , "Enhancement CAST Block Algorithm to Encrypt Big Data ", In New Trends in Information & Communications Technology Applications (NTICT), Annual Conference, 13 July 2017, Publisher: IEEE, DOI: 10.1109/NTICT.2017.7976119.

[2] Bhattacharyya D. and Bandyopadhyay S. Kumar, " Hiding Secret Data in DNA Sequence", International Journal of Scientific & Engineering Research Volume 4, Issue 2,ISSN 2229-5518 , February-2013.1

[3] Pardhi A. and Joshi R., " Secure Image Steganography using DNA sequence based on DNA Cryptography", *4th International Conference on Latest Innovations in Science, Engineering and Management, ICLISEM-17*, ISBN:978-93-86171-51-1, 1st July 2017.

[4] W. Stallings, "CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE",FIFTH EDITION, Copyright © 2011 .

[5] Kadhim F, Majeed G, Ali R, "Proposal new s-box depending on DNA computing and mathematical operations", *In Multidisciplinary in IT and communication science and applications (AIC-MITCSA)*, Publisher: IEEE , 2016, pp 1–6.

[6] Dwivedi P., Mahadik S. and Kamble A., "Performance evaluation of data hiding techniques ", *IEEE Conference Publication, 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* , 9 April 2018

[7] Kayarkar H. and Sanyal S., " A Survey on Various Data Hiding Techniques and their Comparative Analysis ", *ACTA Technica Corviniensis*, Vol. 5, Issue 3, July-September 2012, pp. 35-40.

[8] Girdhar A. & Kumar V., " A RGB image encryption technique using Lorenzand Rossler chaotic system on DNA sequences ", @Springer Science+Business Media, LLC, part of Springer Nature 2018, Multimed Tools Appl, https://doi.org/10.1007/s11042-018-5902-z.

[9] Channalli S. and Jadhav A., " Steganography An Art of Hiding Data ", *International Journal on Computer Science and Engineering* Vol.1(3), 2009, 137-141, ISSN : 0975-3397.

[10] Doshi R., Jain P. and Gupta L., " Steganography and Its Applications in Security ", *International Journal of Modern Engineering Research (IJMER)* www.ijmer.com Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638 ISSN: 2249-6645.

[11] Walia E., Jain P. and Navdeep, " An Analysis of LSB & DCT based Steganography", *Global Journal of Computer Science and Technology*, Vol. 10 Issue 1 (Ver 1.0), April 2010.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[12] Patel F., A. N. Cheeran, " Performance Evaluation of Steganography and AES encryption based on different formats of the Image", *International Journal of Advanced Research in Computer and Communication Engineering*, ISSN (Online) 2278-1021, ISSN (Print) 2319-5940 Vol. 4, Issue 5, May 2015.

[13] Jaryal S. and Marwaha C., "Comparative Analysis of Various İmage Encryption Techniques", *International Journal of Computational Intelligence Research*, ISSN 0973-1873 Volume 13, Number 2 (2017), pp. 273-284 © Research India Publications http://www.ripublication.com

[14] Zena M. Saadi and Matheel E. ,"Image Encryption Using DNA Addition", Thesis, Computer Science Department, University of Technology, 2017