

The Effect of DNA in Image Steganography on Privacy Preservation in Smart City

Habib Esmaeelzadeh Rostam¹, Homayun Motameni^{2,*}, Rasul Enayatifar³

Abstract–The smart city is one of the Internet of Thing based application that its use is increasing today. One of the requirements of this system is privacy which protects citizens from disclosure. To protect privacy, security systems are usually used, which steganography is one of the best methods. In steganography methods, secret data is hidden in a cover media in an undetectable way. This paper proposes to protect citizens' privacy by combining chaotic functions and a new method of steganography and image blocking. In this paper, two methods for steganography are proposed. In the first proposed method, randomly selected secret data bits are hidden in the pixels of image blocks that have also been randomly selected least significant bit method. In the second proposed method, the secret data and image are first converted to DNA sequence, then the secret data genomes are replaced with least significant genomes of the pixels of the image. Simulation results show that DNA use increases the quality of hidden images compared to without DNA methods and existing methods.

Keywords: Internet of Things, Smart city, privacy preservation, Steganography, DNA

1. Introduction

The Internet of Things is a collection of peoples, computers, equipment, and resources that communicate and transmission information for a variety of purposes[1]–[5]. One of the IOT-based apps is Smart City. Smart city technology allows authorities in a city to interact directly with the community and urban infrastructure and monitor what is happening and what is evolving. In Smart City, different types of electronic sensors are used to collect, hold and analyze information, including information collected from citizens, devices, and urban resources used to monitor and manage the transportation network, water network, power grid, gas network, telephone system, garbage network, school system, library, hospital, and other social services. One of the most important problems in this system is the misuse of citizens' information, which can have negative consequences for citizens, which is why privacy is an essential requirement for the smart city [6]–[12].

In order to protect privacy, security systems are usually used, which steganography is one of the best methods. The main idea of steganography is to hide personal information inside a cover media in an unobservable way. In steganography techniques, confidential information is

hidden in digital media such as film, audio, and video. The use of images is common among different types of digital media. In image steganography, bits of secret data are hidden in least significant bits of image pixels, with different techniques [13]–[16].

One of the safest and most effective methods of image steganography is DNA-based image steganography. In these methods, firstly, the secret data and the cover image by DNA rules are converted into DNA sequences, then the secret data is hidden in the cover image and finally, the DNA sequence is converted to the stego-image. And secondly, at the final destination, the stego-image is converted into DNA sequences, then the secret data is extracted from the DNA sequence [17]–[20].

One of the key issues in image cryptography and steganography techniques is image blocking, for which different methods have been presented. In these techniques, the image is divided into several blocks; moreover, the desired processing is conducted on each block independently. Then the blocks are merged; finally, the final image is produced [19]–[22].

In recent years, many algorithms based on chaotic functions have been offered that have been accepted by researchers due to their sensitivity to initial values and randomness. In many image cryptography and steganography techniques, pseudo-random numbers are used to choose or displace pixels or blocks that chaotic functions are used to create these pseudo-random numbers [23]–[26].

In this paper, two algorithms have been proposed to

¹ Department of Computer Engineering, Sari Branch, Islamic Azad University, Sari, Iran. Email: h.esmaeelzadeh@gmail.com

^{2*} **Corresponding Author:** Department of Computer Engineering, Sari Branch, Islamic Azad University, Sari, Iran. Email:h_motameni@yahoo.com

³Department of Computer Engineering, Firoozkooh Branch, Islamic Azad University, Firoozkooh, Iran. Email:r.enayatifar@gmail.com

privacy preservation. In the first method, the image is first blocked, a block is randomly selected, and then the secret data bits are randomly selected and hidden in the pixels of the selected block except central pixel of the block, with the least significant bit method. In the second proposed method, the blocks of image and secret data are converted into DNA sequences, and randomly selected genomes of secret data are hidden in the pixels of the block except central pixel of the block. The central pixels of the block are used to generate the secret key of the chaos function for random selection of blocks and secret data. In both proposed methods to increase security of privacy preservation, three levels of security are provided in the information hiding process. In the first level of security, the centers of the blocks have been used to generate the secret key of the chaos function. To provide security at the second level, the blocks are randomly selected for hiding. The random selection of secret data bits is the third security level of the proposed method.

The rest of the article is organized as follows: in part 2, the preliminary of research was presented, and in part 3, the literature reviews have been investigated. In part 4 the proposed method is presented, the simulation results were presented in part 5 and the final part is concluded.

2. Related work

Almawgani et al. proposed a hybrid steganography method based on Haar Discrete Wavelet Transform, Lempel Ziv Welch algorithm, genetic algorithm, and optimal pixel adjustment process to improve the quality of the stego image and increase the capacity of secret data. First, the cover image was divided into $n \times n$ pixel blocks, then they used a Haar Discrete Wavelet Transform to increase the strength of the stego image against attacks. In order to increase the capacity and security of the image, they used the Lempel Ziv welch algorithm and genetic algorithm to encode, compress and find the optimal mapping function to each block [27].

Taha et al. presented a three-step method of hiding the secret data in the image to achieve a steganography design. First, they presented a new encryption method called mixed pieces of secret data with an advanced Hoffman compression algorithm to improve text security and hiding capacity. In the second step, the Fibonacci-based decomposition method was used to improve image strength. And in the third step, they presented an improved hiding method by randomly selecting the block/pixel and merging it with the degree of differentiation value and generating the implicit secret key to intangibly enhance the design [13].

Wahab et al. provided a combination of RSA

cryptography, Hoffman code, and discrete wavelength transform. First, the secret data was encrypted using RSA encryption and compressed it with Hoffman code. In the next step, the image was compressed using discrete wavelength transform and converted from RGB format to YCbCr format. Finally, they hid the secret data in the image by the least significant bit method [28].

Bairagi et al. used the least significant bit method of image steganography to secure their information. They did not use all the complexes of all red, green, and blue channels for replacement, but in some pixels determined by the carrier environment, the secret key, and the secret data. Ambiguity in the selection of cells as well as channels increases the complexity of analysis and also the yield [29].

Parah et al. proposed a method of hiding with computational efficiency, security, and high capacity in medical images for privacy in the healthcare system. First, they reduced the image size by the two-line interagency method, then when increasing the image size, they hid the secret data in the pixels that are added. To hide the secret data in pixels, they used the remaining method divided by 4 [6].

Kumar et al. used wavelet-based steganography and Hennon chaos mapping for integration and authentication to hide consumer smart meter information in smart grid systems. Discrete wavelength transformation decomposes the readings into sub-band coefficients, which are used as cover media [30].

To thwart adversary attacks and ensure data confidentiality, Hurra et al. proposed a robust multilevel security approach based on information hiding and chaos theory. Contrary to traditional methods, they randomly used two non-neighboring blocks for concealment so that the information is spread over different regions of the cover image [31].

Devi et al. concealed patient information in medical images by replacing least significant bits to protect privacy. In this way, patient-sensitive information cannot be misused by unauthorized parties and patient privacy is protected [12].

Lee et al. examined methods of sharing with steganography. They presented a secure image sharing scheme based on Shamir polynomials covered in the IOT system, in which IOT devices can share images seamlessly between them through the cloud. Secure sharing comes from cover image and secret information [32].

Table 1 shows the comparison between privacy preservation methods in terms of technique, method, chaos function, and key and application area.

Table 1. Comparison of privacy preservation methods

authors	Method	Technique	Chaotic function	Key	application
Bairagi et al. [29]	Steganography	LSB	No	Yes	Smart home
Parah et al. [6]	Steganography	PRM	No	No	Smart healthcare system
Li et al. [33]	Steganography	DCT	No	Yes	Wireless sensor network
Kim et al. [34]	Steganography	LSB	No	No	Android based applications
Kumar et al. [25]	Steganography	DWT	Henon	Yes	Smart grid
Hura et al. [35]	Steganography	DCT	Yes	20-bit	Smart healthcare system
Devi et al. [12]	Steganography	LSB	No	No	Smart healthcare system
Wahab et al. [28]	Steganography & cryptography	LSB	No	Yes	Transmission in internet
Almawgani et al. [27]	Steganography & genetic algorithm	DWT	No	No	Image transmission in internet
Taha et al. [13]	steganography	LSB	Henon	Yes	Transmission in internet
Proposed method	steganography	LSB& Blocking	Tent	Block centers	Internet of things

3. Preliminaries

The basics of chaotic functions and DNA, which are used in the proposed method, are explained in this section.

3.1. Chaotic Map

These functions are similar to noise signals; however, they are quite definite, i.e. if we have the initial values and the mapping function, we can reproduce the exact signal. Hence, these functions are used in areas where security and privacy-preserving are of great importance. Some of the specifications of these functions are as follows:

a. Sensitivity to initial values: These functions are very sensitive to initial values, i.e. if we have a slight change in the initial values, we will see many changes in later values.

b. Apparent random feature: Unlike functions that produce random numbers; moreover, these numbers can no longer be reproduced under any circumstances, chaotic functions produce pseudo-random numbers that can be reproduced by having initial values and a chaotic function.

Tent chaotic mapping is a one-dimensional chaotic mapping that enjoys the discrete-time and real spatial domain. As shown in Equation 1, the Tent mapping generates pseudo-random numbers with only one parameter μ [36].

$$x_{n+1} = f_{\mu}(x_n) = \begin{cases} \mu x_n & \text{for } x_n < \frac{1}{2} \\ \mu(1 - x_n) & \text{for } \frac{1}{2} \leq x_n \end{cases} \quad (1)$$

3.2. DNA

DNA is a nucleic acid having genetic instructions that are used for the biological function and development of living organisms and viruses. Each nucleotide acid has only one nitrogenous organic base, which can be adenine (A) or guanine (G) or cytosine (C), or thymine (T). These bases are either pyrimidine (such as T and C) or purine (such as A and G). Based on the Watson–Crick relationship, adenine is always the thymine pair; moreover, guanine is the cytosine pair. Therefore, A and T are complementary and C and G are also complementary. In the binary system, 00 is

complementary of 11; in addition, 10 are complementary of 01. By mapping each base A, G, C, T to one of the codes 00, 01, 10, and 11, 24 types of coding can be mapped, of which only 8 types of mapping are in accordance with Watson – Crick rules that are shown in Table 2.

For an instance, if the color intensity of two of the image pixels is 48 and 78, the binary values and DNA code are as illustrated in Table 3:

Table 2. Binary coding rules for DNA sequences

	A	T	C	G
Rule 1	00	11	10	01
Rule 2	00	11	01	10
Rule 3	11	00	10	01
Rule 4	11	00	01	10
Rule 5	10	01	00	11
Rule 6	01	10	00	11
Rule 7	10	01	11	00
Rule 8	01	10	11	00

Table 3. Binary value and DNA sequence of 48 and 78 numbers

Decimal	Binary	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
48	00110000	ATAA	ATAA	TATT	TATT	CGCC	CGCC	GCGG	GCGG
78	01001110	GATC	CATG	GTAC	CTAG	TCGA	ACGT	TGCA	AGCT

4. The proposed method

In this paper, two algorithms have been proposed to steganography and to investigate the effect of using DNA in steganography. In the proposed method, first, the image is blocked, then the blocks are randomly selected to hide the secret data. The secret data is converted to a binary string using the ASCII coding system and its bits are randomly selected, eventually, the randomly selected secret data bits are hidden in block pixels which are also randomly selected by the least significant bit method. In the second method, the secret and cover image are converted to the DNA sequence, then the genomes of the secret data are randomly selected and hidden in image blocks, which are also randomly selected.

The hiding stages of the first proposed method are shown in Figure 1-a. First, the cover image is blocked. Block centers are used to generate the secret key of the chaos function with the aim of randomly selecting blocks and bits of secret data. Then the bits of the selected secret data are hidden in the selected block pixels.

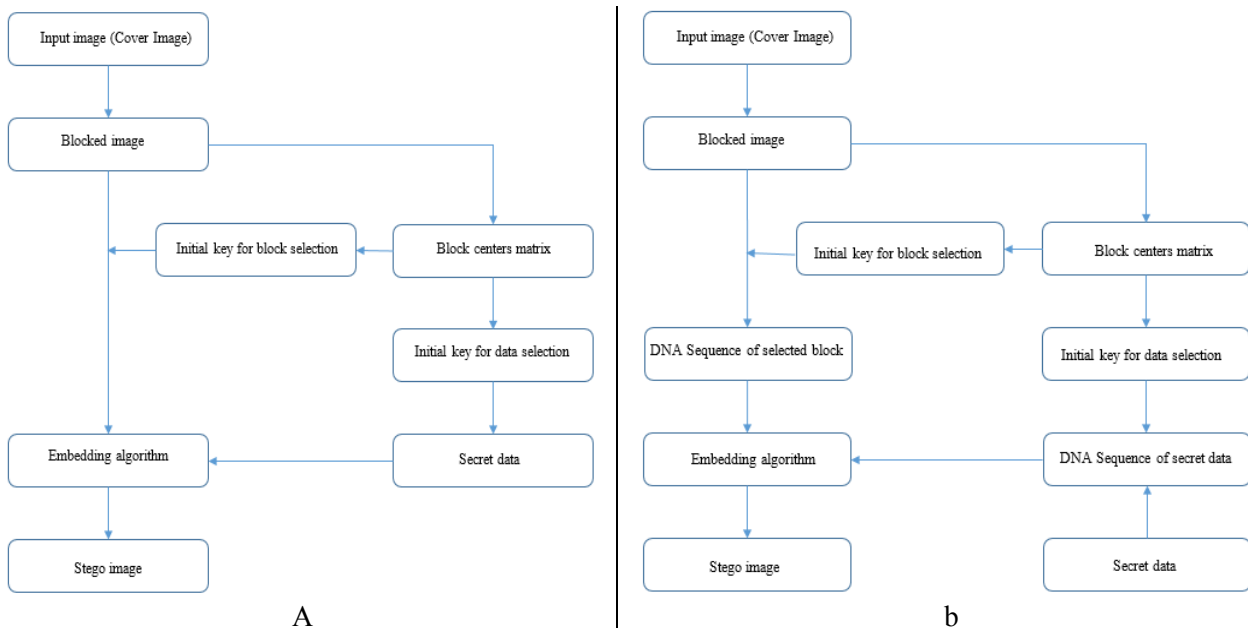


Fig. 1. Block-diagram of proposed method. A) First proposed method without DNA. B) Second proposed method with DNA.

The hiding steps of the second proposed method are shown in Figure 1-b. First, the cover image is blocked. The block centers is used to generate the secret key of chaos function with the aim of a random selection of blocks and secret data genomes. Then the selected block pixels are converted to DNA sequences, the secret data is converted to DNA sequence, and finally, the genomes of the selected secret data are hidden in the selected block pixels.

The steps of the proposed methods are explained in more detail below.

4.1. Image Blocking

In this stage, the cover image is divided into blocks of 3×3 pixels. Assuming an image with dimensions of $n \times m$ pixels, such as Figure 2, a number of $(n \times m) \div 9$ blocks is formed, which can be considered as a matrix with dimensions $i \times j$ ($i = n \div 3$, $j = m \div 3$) in which each matrix element is a block with 3×3 pixels. To hide the secret data, the blocks are randomly selected and the secret data is hidden in the pixels of the selected blocks other than the central pixel, which is considered the axis. Pixels of central block are used to produce the secret key of chaos function to produce pseudo-random numbers.

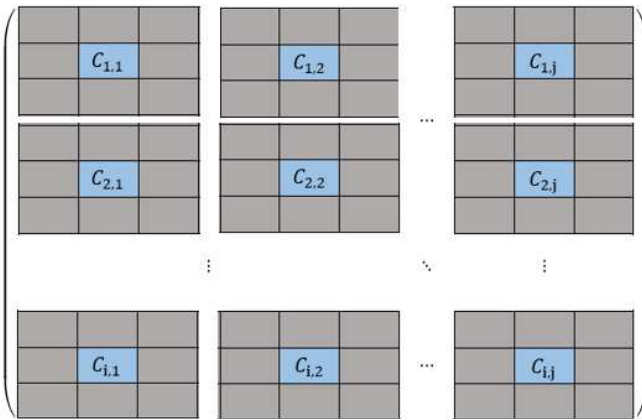


Fig.2. Blocked image

4.2. Select Block

To hide the secret data in the image, a block of the image must be selected randomly. In this paper, block centers are used to randomly select blocks and generate the secret key of the tent chaotic function. In this way, first, the values of each row of the centers of the blocks are XOR together, and then the resulting values are gathered together. Finally, the resulting value is divided by the number of matrix elements ($i \times j$). The initial key value of the tent chaos

function (x_0) is generated according to equation(2).

$$x_0 = \frac{(C_{1,1} \oplus \dots \oplus C_{1,j}) + (C_{2,1} \oplus \dots \oplus C_{2,j}) + \dots + (C_{i,1} \oplus \dots \oplus C_{i,j})}{i \times j} \quad (2)$$

4.3. Select secret data

To increase the security of steganography, the chaos tent function is used to randomly select bits of secret data. In this stage, block centers are used, as in sections 4.2, to generate the secret key of the tent chaos function. First, the values of each row of block centers are gathered together, then the resulting values are XOR together, and finally, the resulting value is divided by the number of matrix elements. In this way, the secret key value of the tent chaos function (x_0) is obtained according to equation(3).

$$x_0 = \frac{(C_{1,1} + \dots + C_{1,j}) \oplus (C_{2,1} + \dots + C_{2,j}) \oplus \dots \oplus (C_{i,1} + \dots + C_{i,j})}{i \times j} \quad (3)$$

4.4. DNA conversion

In the second proposed method, the use of DNA is suggested to increase the quality of the stego image. In this stage, the secret data and the cover image were converted to DNA sequences using the first Watson-Crick rule according to Table 2.

4.5. Hiding algorithm

In the process of hiding information in the first proposed method, a block is randomly selected, and for each pixel other than the center pixel of the selected block, two random bits selected from the secret data are replaced by two least significant bits of each pixel.

For example, Figure 3-a shows an example of a random block and its binary stream equivalent. Figure 3-b shows the ab secret data, ASCII code, and their binary stream equivalents. Suppose that Fig. 3-c shows a pseudo-random number generated by the Tent function. Using this number, the data bits are selected (Fig. 3-d). For concealment, the first two bits selected from secret data are replaced by two least significant bits of the first pixels of block. Similarly, the second randomly selected two bits from the secret data are replaced by the two least significant bits of second pixel, and the remaining bits are similarly replaced by the next pixels in the block except for the center pixel. Figure 3-e shows the color intensity of the pixels in the block after the hiding process.

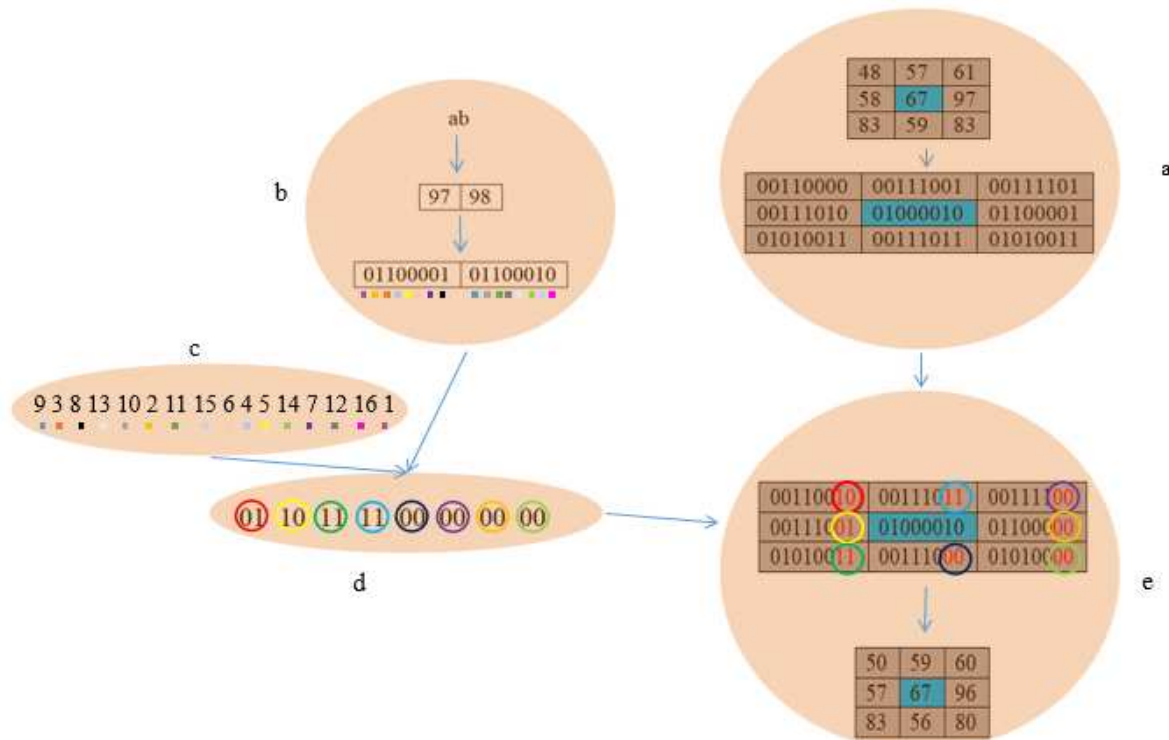


Fig. 3. An example of the steganography steps of the first proposed method

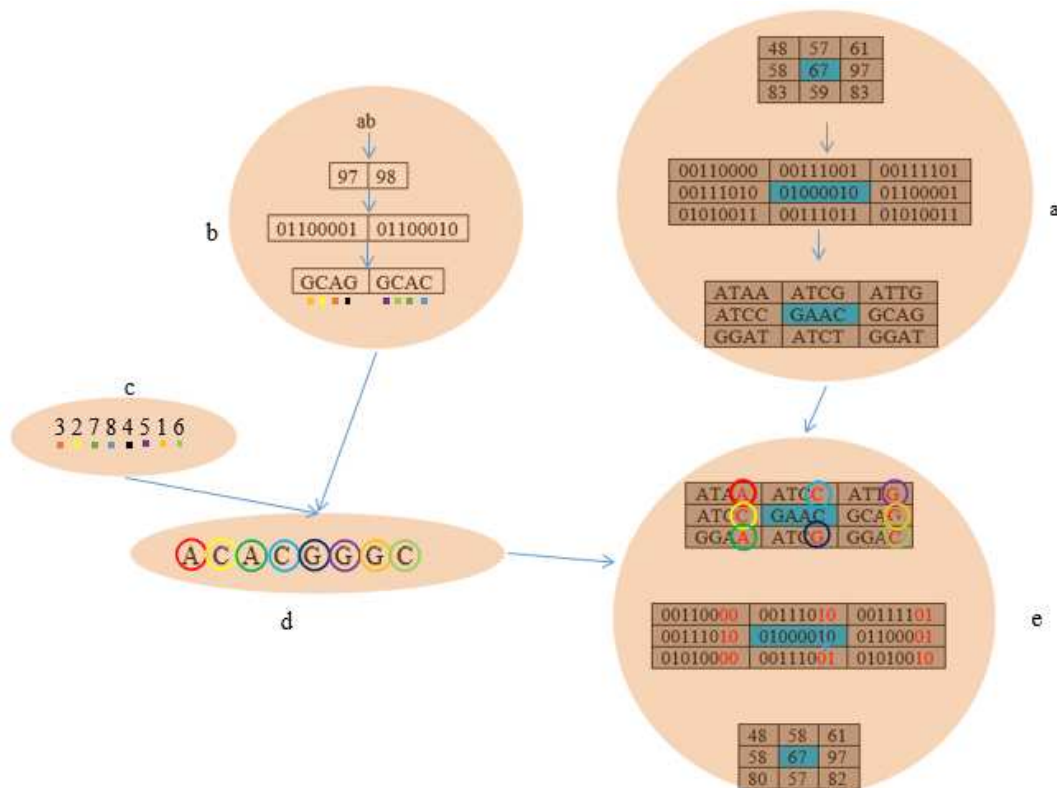


Fig. 4. An example of the steganography steps of the second proposed method

In the second proposed method to hide information, blocks are first randomly selected, and for each pixel other

than the center pixel of the selected block, a random genome selected from the secret data is replaced by the least significant genome of each pixel.

For example, Figure 4-a shows an example of a random block, its binary equivalent, and the DNA sequence of each pixels. Fig. 4-b shows the secret data, the binary equivalent, and the DNA sequence of the secret data ab. Figure 4-c shows a pseudo-random number generated by the Tent function. This number is used to select the genome of the secret data (Figure 4-d). For concealment, the first genome, randomly selected from the secret data, is replaced by the least significant genome of the first pixel of block. Similarly, the second randomly selected genome from the secret data is replaced by least significant of the second pixel of block, and the remaining genomes are similarly replaced in the next pixel in the block except for the central pixel of block. Figure 4-e shows the color intensity of the block pixels after the hiding process.

4.6. Extracting secret data from stego images

For data extraction in the first proposed method, the image is divided into blocks of 3×3 pixels (Fig. 5-a). The central pixels of the blocks is used to randomly selecting the blocks by the Tent function. Two least significant bits of pixels other than the center pixel of the selected block are extracted from the image to obtain the secret data, and the Tent function is used to determine the position of the bits in the secret data.

In the second proposed method, the image is divided into 3×3 pixel blocks (Fig. 5-b); central pixels of blocks is used to randomly selecting blocks by the Tent function, and the selected blocks are converted into a DNA sequence. To obtain the secret data, the least significant genomes of the pixels of the selected block, except the central pixel, are extracted from the image, and the position of the genome in the secret data is determined by the Tent function. The DNA sequence of the secret data is then converted into a binary string, after which the equivalent ASCII code is determined and the secret data is extracted.

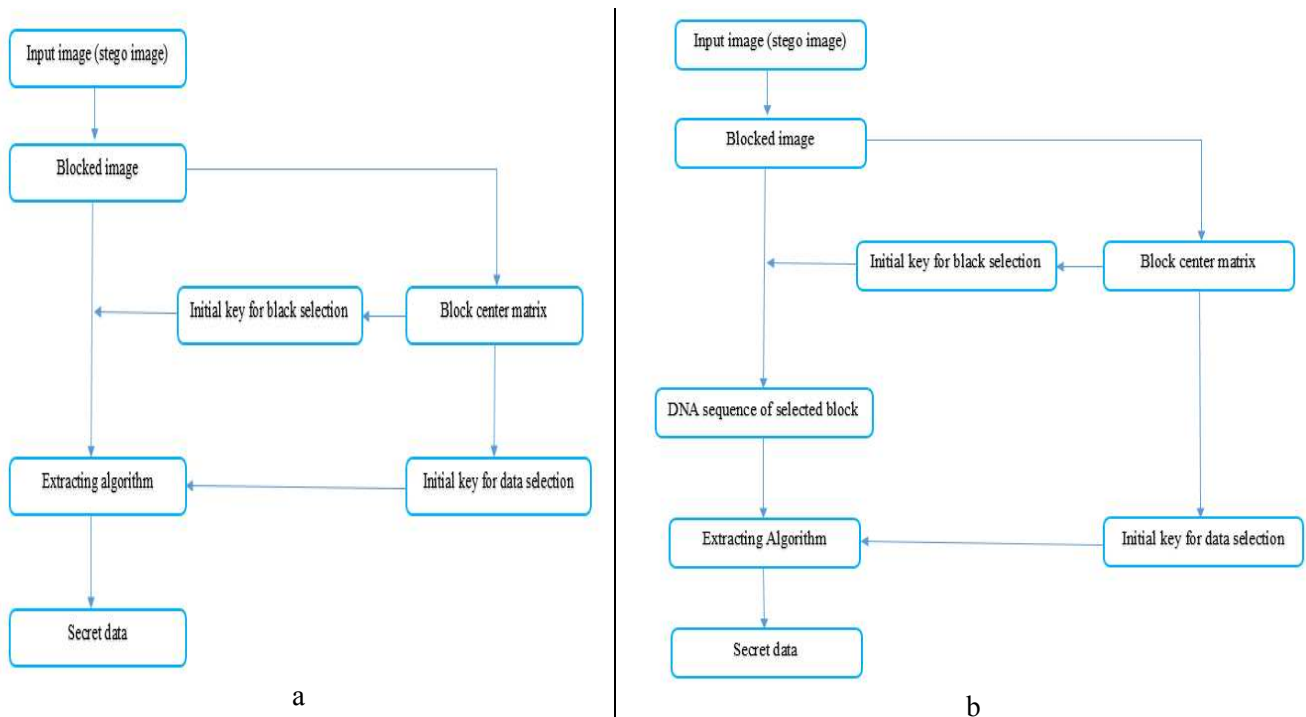


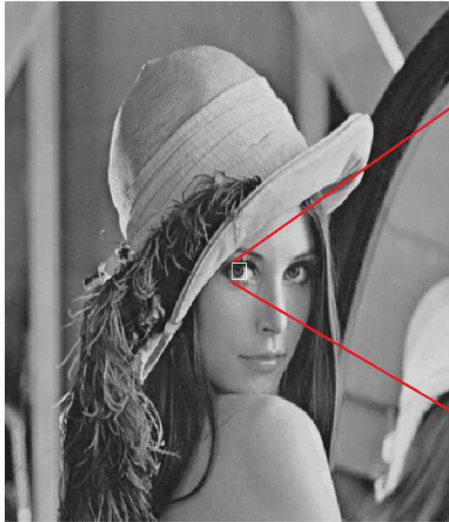
Fig. 5. Extracting Algorithm block diagram. a) First proposed method without DNA. b) Second proposed method with DNA

Figures 6-a and 6-b shows Lena cover image, stego image and enlarged view of small part of their. As you can see from these two images, the color intensity of the pixels have changed due to the concealment of secret data in the image, but the visual impairment of the human eye does not

allow it to detect small changes in the color intensity of the pixels. For example, the value of the first pixel from the dock in the cover image is 48 (the binary equivalent of 00110000), but in the stego image, it changes slightly to 49 (the binary equivalent of 00110001). In this case, the two

least significant bit of pixel value changes from 00 to 01. In this pixels, the two bits 0 and 1 of secret data are hidden,

and cannot be detected by the human eye.



46	46	46	46	46	46	46	46	42	42	46	57	42	51	51
46	57	46	42	46	46	42	42	42	44	42	47	51	59	77
51	53	51	51	42	42	42	42	43	42	45	67	61	98	116
51	42	46	46	42	42	43	44	43	48	57	61	87	138	152
42	42	51	42	48	40	43	43	77	58	67	97	127	159	194
37	42	59	54	42	35	31	38	81	83	59	83	122	175	200
42	57	74	77	42	35	31	39	52	84	59	48	71	160	208
46	52	95	92	76	45	41	40	70	115	75	51	69	161	200
67	46	91	92	84	73	67	66	77	101	74	48	86	179	208
96	67	52	76	92	82	82	84	76	71	57	64	127	201	207
116	84	52	57	72	81	83	72	75	50	63	121	179	208	207
121	109	85	59	53	50	57	51	61	79	105	156	200	207	207
113	115	109	94	78	62	62	73	87	124	155	199	199	202	202
119	120	130	117	110	104	103	118	135	154	190	199	199	199	202
117	131	140	140	130	136	138	157	155	179	185	191	198	198	201

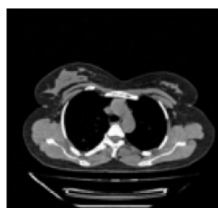
a



44	46	45	47	44	45	46	44	41	41	47	58	42	50	49
46	57	47	43	46	45	41	42	41	47	42	44	51	59	77
48	53	50	51	41	40	42	41	42	42	44	65	62	96	118
50	41	47	45	42	41	43	44	43	49	56	63	87	138	152
40	42	51	42	48	43	43	43	77	56	67	97	127	159	194
37	41	59	54	42	33	31	38	81	80	56	80	122	175	200
43	58	72	79	42	32	31	39	52	84	56	48	70	163	208
45	52	92	92	76	44	41	40	70	114	75	51	68	161	202
65	47	89	94	84	74	67	66	77	103	74	50	86	176	208
96	66	52	79	94	80	81	87	77	68	59	64	124	202	204
118	84	55	57	72	83	80	72	72	48	63	120	178	208	204
123	108	86	56	55	48	56	49	62	76	104	156	200	204	206
113	115	109	92	79	62	62	74	87	127	155	199	196	200	201
119	120	130	118	110	104	101	118	133	154	190	197	198	199	202
117	131	140	143	131	136	139	156	154	176	186	190	199	196	200

b

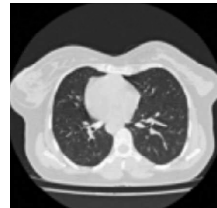
Fig.6. Lena image. a) Cover Lena image. b) Stego Lena image



Med 1



Med 2



Med 3



Med 4

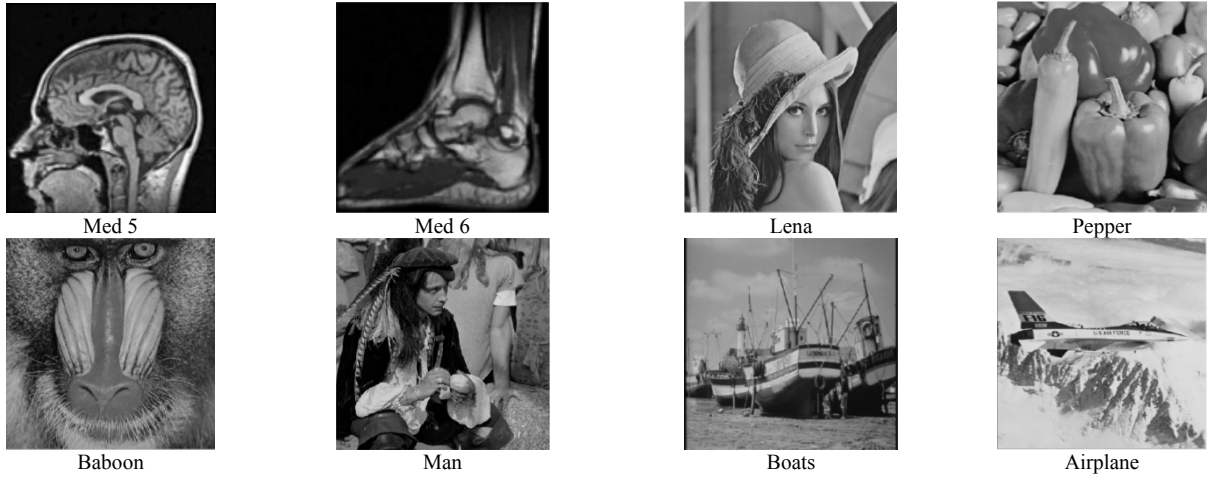


Fig.7. 12 examples of cover images from the UCID database with scale of 512×512 pixels

5. Simulation

MATLAB software version R2015a on a laptop with an Intel core 2 DUO 2.66 GHz processor, 4 GB of memory, and Windows 10 Enterprise version operating system was used for simulation. Standard cover images from the UCID database [42] were selected for simulation and 12 examples were used, including six grayscale images and six medical images, as shown in Figure 7.

Simulations were performed on standard UCID images with scales 128×128, 256×256, 512×512, and 1024×1024 pixels were considered as covering images, and text file with 3, 12, 48, and 192 kilobytes, equivalent 1.5 bit per pixel were considered as secret data, to be hidden in the cover image (Table 4).

Table 4. Simulation

Image scale	Secret data (kilobyte)	Data set
128×128	3	
256×256	12	UCID-Image
512×512	48	Database(v2) [42]
1024×1024	192	

Such image quality parameters as maximum signal (data) to noise ratio (PSNR), mean square error (MSE), bit error rate (BER), and structural similarity index (SSIM) were used to evaluate the effectiveness of the proposed method.

The most common parameter to measure image quality is the PSNR parameter, which indicates the ratio of maximum signal (data) rate to image noise, expressed in decibels (dB); a ratio greater than 1:1 (greater than 0 dB) indicates a higher signal-to-noise ratio. In general, less than 12 dB indicates high image noise, more than 12 dB is adequate, and more than 30 dB is more favorable. In fact, a

higher index indicates a better situation and a higher useful signal ratio. Equation 4 shows how the PSNR parameter is calculated [37], [38].

$$PSNR = 10 \log_{10} \frac{C_{Max}^2}{MSE} \quad (4)$$

The MSE parameter is a method of estimating the magnitude of the error, which is the actual difference between the cover image and the stego image. This measure always has a non-negative value, and the closer it is to zero, the smaller the error. Equation 5 shows how this parameter is calculated [37], [38]].

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N [C(i,j) - S(i,j)]^2 \quad (5)$$

In the above Equation, M and N represent the size of the image, C represents the hidden image, and S represents the stego image.

The BER (bit error rate) parameter is another parameter for error estimation and represents the number of changed pixels relative to the total number of pixels; the closer the BER parameter is to zero, the lower the error rate. Equation 6 shows how this parameter is calculated [31], [39].

$$BER = \frac{\text{Number of errored bits}}{\text{Total number of bits}} \quad (6)$$

The SSIM parameter is a structural criterion for comparing two images based on the natural structure of the image. The natural structure of an image is such that a pixel has a large dependence on neighboring pixels, and this dependence contains important information about the structure of objects in the image; by calculating SSIM, we

can calculate the structural similarity in the vicinity of an individual pixel. The values of this parameter are in the range (0, 1), where the closer this parameter is to number 1, the higher the structural similarity. The calculation of the SSIM parameter is shown in Equation 7 [1], [38], [40].

$$SSIM(C, S) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (7)$$

The proposed method used medical images and grayscale image with scales 128×128, 256×256, 512×512, and 1024×1024 pixel, to hide 3, 12, 48, and 192 KB secret data. Figure 8 shows one medical image and one grayscale

image with 512×512 pixels before and after hiding with 48 KB of secret data, and their histogram obtained by both of the proposed methods.

According to Fig. 8, the histograms of the images before and after hiding in the proposed method change slightly, indicating that cover image and stego image are similar. As a result, the human eye cannot recognize the difference between the two images.

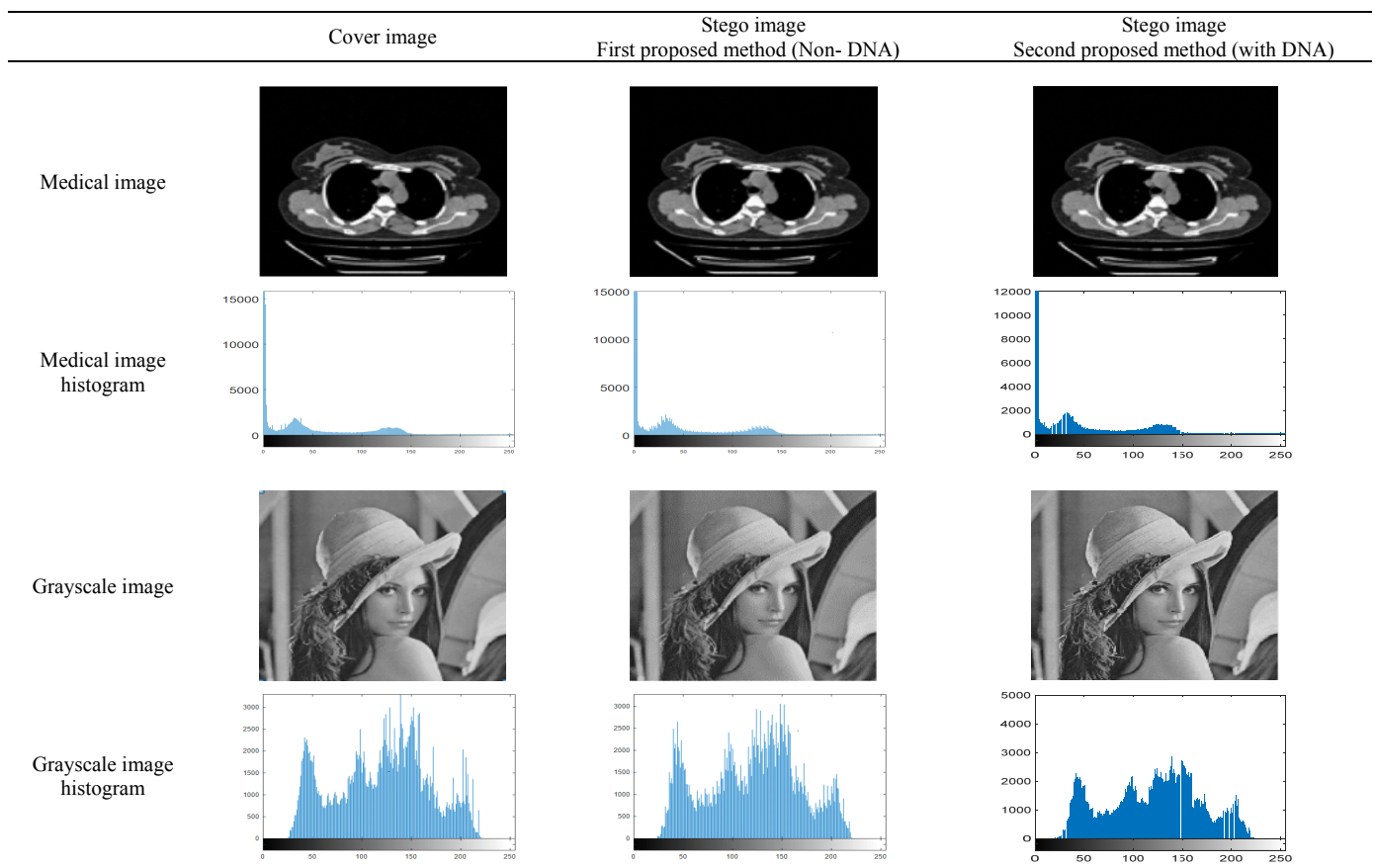


Fig. 8. Cover image and histogram, before and after steganography with two proposed method

Tables 5 show the values of PSNR, SSIM, MSE, and BER parameters of medical images by the first and second proposed methods, and Tables 6 show the values of PSNR, SSIM, MSE, and BER parameters of grayscale images by the first and second proposed methods.

Table 5. PSNR, SSIM, MSE, and BER parameters of medical images with different scales

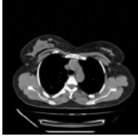

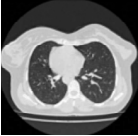

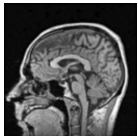
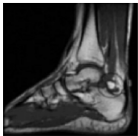
Cover image	Scale	Secret data (KB)	PSNR		SSIM		MSE		BER	
			Non-DNA	With DNA	Non-DNA	With DNA	Non-DNA	With DNA	Non-DNA	With DNA
	128×128	3	46.30	46.96	0.9767	0.9804	0.5402	0.4061	0.0792	0.0695
	256×256	12	46.26	46.90	0.9697	0.9746	0.5566	0.4269	0.0798	0.0695
	512×512	48	46.30	46.99	0.9616	0.9671	0.5385	0.4032	0.0797	0.0685
	1024×1024	192	46.27	46.93	0.9547	0.9611	0.5428	0.4128	0.0799	0.0687
	128×128	3	46.32	46.89	0.9810	0.9847	0.6826	0.5210	0.0806	0.0711
	256×256	12	46.25	46.82	0.9739	0.9786	0.7172	0.5430	0.0811	0.0705
	512×512	48	46.22	46.96	0.9664	0.9714	0.7164	0.5089	0.0812	0.0692
	1024×1024	192	46.24	46.91	0.9616	0.9722	0.7156	0.5139	0.0811	0.0690
	128×128	3	46.05	46.69	0.9888	0.9904	0.9650	0.6888	0.0824	0.0717
	256×256	12	45.96	46.68	0.9821	0.9849	0.9628	0.6852	0.0828	0.0714
	512×512	48	45.97	46.78	0.9772	0.9795	0.9689	0.6547	0.0832	0.0705
	1024×1024	192	45.98	46.73	0.9743	0.9722	0.9658	0.6665	0.0830	0.0694
	128×128	3	45.96	46.86	0.9874	0.9896	0.9893	0.6847	0.0834	0.0709
	256×256	12	45.99	46.79	0.9826	0.9852	0.9909	0.6866	0.0833	0.0711
	512×512	48	46.00	46.88	0.9770	0.9795	0.9709	0.6491	0.0830	0.0697
	1024×1024	192	45.99	46.93	0.9745	0.9723	0.9894	0.6850	0.0832	0.0707
	128×128	3	45.93	46.54	0.9919	0.9932	1.0166	0.7154	0.0832	0.0736
	256×256	12	45.97	46.52	0.9894	0.9908	1.0007	0.7301	0.0830	0.0734
	512×512	48	45.92	46.64	0.9856	0.9876	1.0237	0.7195	0.0836	0.0722
	1024×1024	192	45.93	46.67	0.9819	0.9788	1.0187	0.7085	0.0835	0.0718
	128×128	3	46.17	46.76	0.9881	0.9902	0.9143	0.6628	0.0824	0.0721
	256×256	12	46.17	46.82	0.9833	0.9870	0.9234	0.6691	0.0830	0.0711
	512×512	48	46.22	46.83	0.9772	0.9817	0.9050	0.6500	0.0825	0.0704
	1024×1024	192	46.19	46.88	0.9716	0.9779	0.9156	0.6468	0.0827	0.0708

Table 6. PSNR, SSIM, MSE, and BER parameters of grayscale images with different scales







Cover image	Scale	Secret data (KB)	PSNR		SSIM		MSE		BER	
			Non-DNA	With DNA	Non-DNA	With DNA	Non-DNA	With DNA	Non-DNA	With DNA
	128×128	3	45.88	46.44	0.9929	0.9938	1.0088	0.7272	0.0829	0.0742
	256×256	12	45.86	46.38	0.9890	0.9901	1.0128	0.7438	0.0833	0.0742
	512×512	48	45.89	46.48	0.9873	0.9884	1.0070	0.7330	0.0832	0.0735
	1024×1024	192	45.87	46.52	0.9838	0.9869	1.0106	0.7401	0.0832	0.0731
	128×128	3	45.83	46.33	0.9941	0.9949	1.0186	0.7572	0.0842	0.0751
	256×256	12	45.86	46.42	0.9896	0.9907	1.0056	0.7450	0.0831	0.0740
	512×512	48	45.86	46.41	0.9865	0.9882	1.0141	0.7441	0.0835	0.0741
	1024×1024	192	45.88	46.44	0.9829	0.9864	1.0093	0.7432	0.0832	0.0744
	128×128	3	45.89	46.46	0.9960	0.9964	1.0028	0.7314	0.0832	0.0740
	256×256	12	45.84	46.37	0.9956	0.9961	1.0239	0.7482	0.0834	0.0737
	512×512	48	45.87	46.42	0.9954	0.9961	1.020	0.7433	0.0833	0.0740
	1024×1024	192	45.85	46.41	0.9932	0.9962	1.0241	0.7453	0.0834	0.0739
	128×128	3	45.83	46.37	0.9958	0.9963	1.0209	0.7530	0.0834	0.0751
	256×256	12	45.87	46.45	0.9935	0.9943	1.0009	0.7305	0.0832	0.0737
	512×512	48	45.89	46.44	0.9908	0.9920	0.9913	0.7253	0.0832	0.0739
	1024×1024	192	45.90	46.40	0.9885	0.9931	0.9813	0.7127	0.0831	0.0743
	128×128	3	45.84	46.62	0.9920	0.9936	1.0294	0.7157	0.0841	0.0724
	256×256	12	45.89	46.54	0.9898	0.9913	1.0182	0.7270	0.0829	0.0730
	512×512	48	45.90	46.47	0.9870	0.9886	0.9893	0.7397	0.0834	0.0740
	1024×1024	192	45.89	46.43	0.9842	0.9868	1.0109	0.7412	0.0834	0.0747
	128×128	3	45.91	46.46	0.9912	0.9923	1.0140	0.7468	0.0836	0.0738
	256×256	12	45.86	46.47	0.9882	0.9895	1.0198	0.7230	0.0839	0.0734
	512×512	48	45.87	46.48	0.9856	0.9872	1.0147	0.7363	0.0833	0.0735
	1024×1024	192	45.89	46.48	0.9826	0.9859	1.0113	0.7297	0.0832	0.0733

Figure 9 shows the comparison of the two proposed methods based on the PSNR parameters. The figure shows that the second method has an average PSNR value of 46.62, which is higher than the first method with an average value of 45.98. This difference indicates that the use of DNA improved the quality of the proposed method.

Figure 10 shows the comparison of two proposed methods based on the SSIM parameter. As it turns out, the use of DNA increased the average similarity of the cover image and the hidden image from 0.9835 to 0.9859.

Figure 11 shows the comparison of two proposed methods based on the MSE parameter. DNA use reduced the average square error from 0.9331 to 0.6733.

Figure 12 shows the comparison of two proposed

methods based on BER parameters. As is evident in the diagram, the average bit error rate using DNA decreased from 0.0827 to 0.0722.

Table 7 and Figure 13 show the comparison of the two proposed methods with the methods presented in articles [6], [38] and [41].

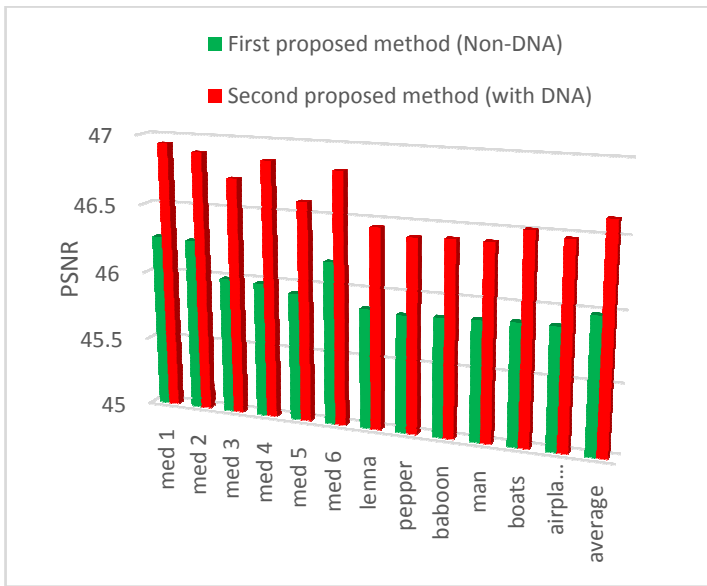


Fig. 9. Comparison of two proposed methods based on PSNR parameter

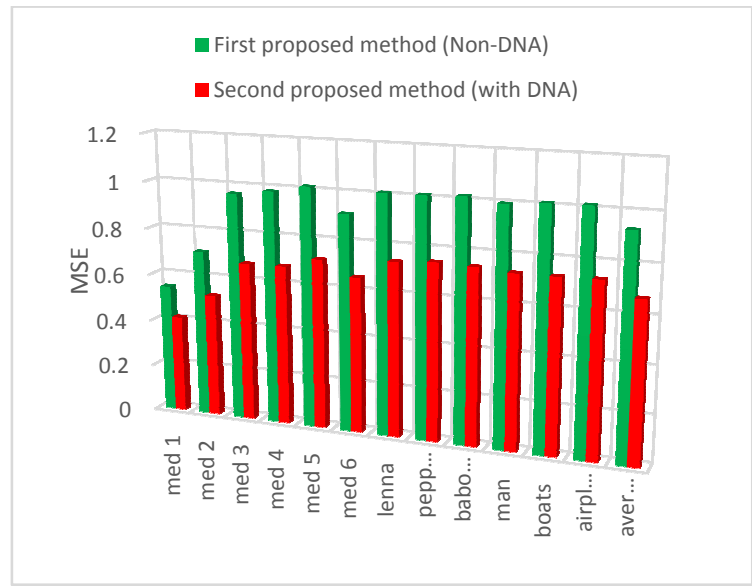


Fig.11. Comparison of two proposed methods based on MSE parameter

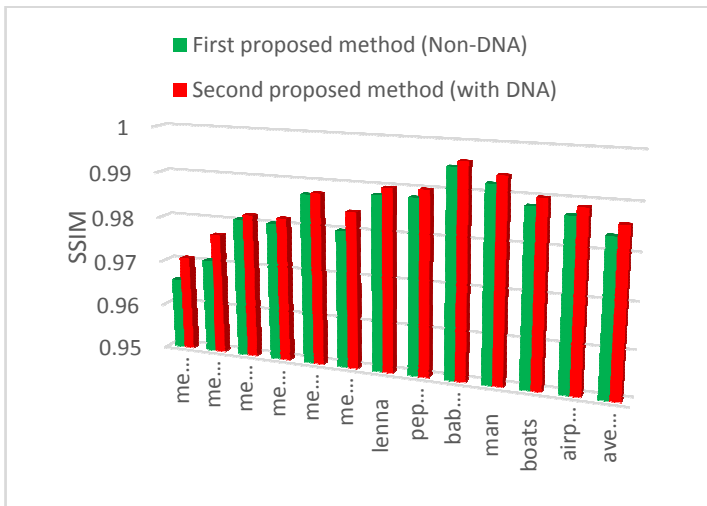


Fig.10. Comparison of two proposed methods based on SSIM parameter

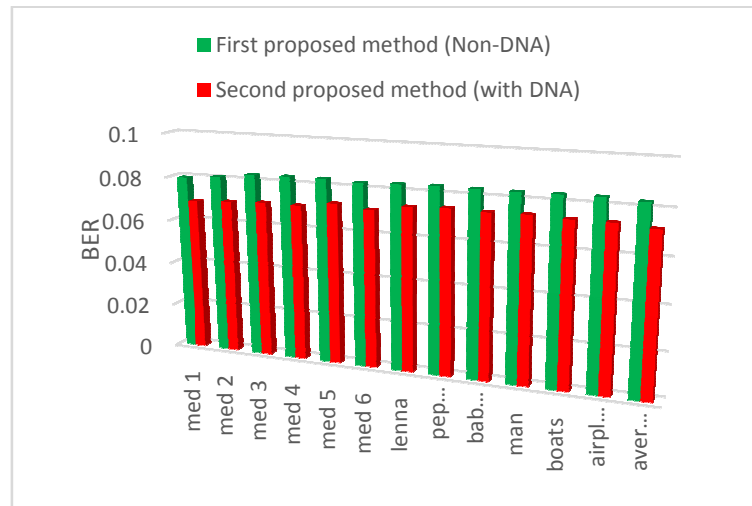








Fig. 12. Comparison of two proposed methods based on BER parameter

Table 7. Comparison of two proposed method with existing methods based on the PSNR parameter

Cover image							Average
Ref. [41]	43.95	43.93	43.94	43.92	43.93	43.95	43.93
Ref. [6]	45.40	45.39	45.41	45.47	45.39	45.37	45.40
Ref. [38]	45.70	45.62	45.24	45.57	45.68	45.65	45.57
First proposed method	45.89	45.86	45.87	45.89	45.90	45.87	45.88
Second proposed method	46.45	46.4	46.41	46.41	46.51	46.47	46.44

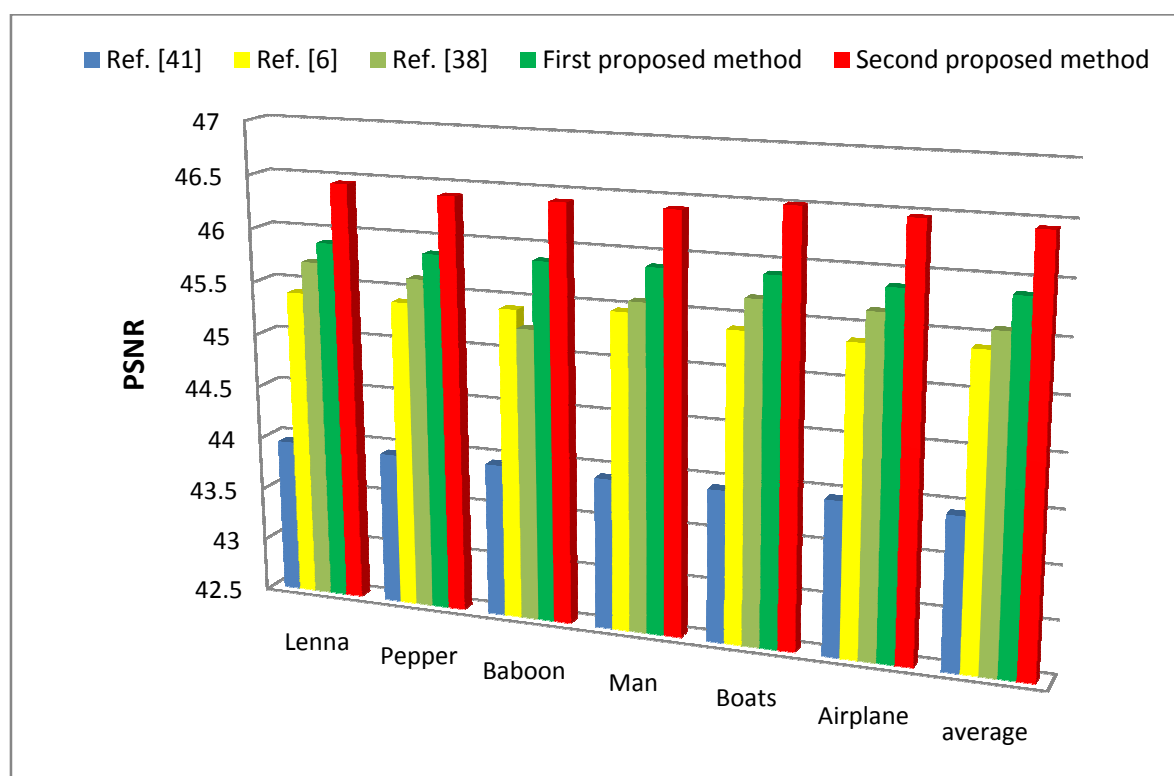


Fig.13. Comparison of the proposed method with existing methods based on the PSNR parameter

5.1 Comparison

For simulation and evaluation, standard cover images of the UCID database have been used. For more detailed evaluation, 96 experiments were performed using 12 cover images with 4 different scales. In the experiments, the parameters of PSNR, MSE, BER, and SSIM were evaluated. In the experiments, the mean PSNR of the second proposed method was 46.44, which is more desirable than the first proposed method with an average value of 45.88 and the methods presented in the articles [6], [38] and [41]. The results of the evaluations show that the use of DNA has increased the quality of image steganography, thus increasing the privacy preservation.

6. Conclusion

Due to the increasing expansion of the Internet of Things and the necessity of privacy in its applications, two new methods of image blocking have been proposed. In the first proposed method, the image blocking is first, a block is randomly selected, and then the secret data bits are randomly selected and hidden in pixels of selected block except central pixels of the block with the least significant bit method. In the second method, image and secret data are converted to DNA sequence, and randomly selected secret

data genomes are hidden in pixels of block except the central block. The central pixels of block are used to produce the secret key of the chaos function for the random selection of block and secret data. Simulation results show that the second proposed method, which uses DNA for steganography, is much more desirable than the first method without DNA and other existing methods.

The advantages of the proposed method can be enumerated as follows:

- To hide the secret data in the image, both the image block and the secret data bits have been randomly selected using the chaos function. To distribute the secret data bits over the pixels of the image, the system becomes more secure by randomly selecting blocks and bits of secret data.

- Conventional use of the chaos function requires the sender to generate a pseudorandom number with a secret key, and the receiver to reproduce a pseudorandom number with the same secret key. Therefore, leakage of this key can lead to leakage of confidential information. In this paper, image pixels are used to create the secret key. This eliminates the need to send the secret key separately to the recipient, thereby eliminating the risk of disclosure of the secret key and hence information leakage.

The disadvantages of the proposed method are:

- In this paper, block centers are used to generate the

secret key of the chaos function, considering that in data transfer, one or more bits may be changed for any reason and this error will change the secret key and as a result, the data will be lost.

References

- [1] A. Alarood, N. Ababneh, M. Al-Khasawneh, M. Rawashdeh, and M. Al-Omari, "IoTSteg: ensuring privacy and authenticity in internet of things networks using weighted pixels classification based image steganography," *Cluster Comput.*, vol. 4, 2021, doi: 10.1007/s10586-021-03383-4.
- [2] L. Hou *et al.*, "Internet of Things Cloud: Architecture and Implementation," *IEEE Commun. Mag.*, vol. 54, no. 11, pp. 32–39, 2016, doi: 10.1109/MCOM.2016.1600398CM.
- [3] A. K. Srivastava, A. Agarwal, and A. Mathur, "Internet of Things and its enhanced data security," *Int. J. Eng. ...*, no. 2, pp. 79–81, 2015.
- [4] M. Eltayeb, "Internet of Things: Privacy and Security Implications," *Int. J. Hyperconnectivity Internet Things*, vol. 1, no. 1, pp. 1–18, 2017, doi: 10.4018/IJHIoT.2017010101.
- [5] H. E. Rostam, A. M. Rahmani, and K. Zamanifar, "Resource Management in Semantic Grid System Based on QoS," in *2009 Second International Conference on Computer and Electrical Engineering*, 2009, vol. 2, pp. 418–421, doi: 10.1109/ICCEE.2009.171.
- [6] S. A. Parah, J. A. Sheikh, J. A. Akhoun, and N. A. Loan, "Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication," *Futur. Gener. Comput. Syst.*, 2018, doi: 10.1016/j.future.2018.02.023.
- [7] W. Strielkowski, *Smart grids of tomorrow and the challenges for the future*. 2020.
- [8] A. A. Abi Sen, F. A. Eassa, K. Jambi, and M. Yamin, "Preserving privacy in internet of things: a survey," *Int. J. Inf. Technol.*, vol. 10, no. 2, pp. 189–200, 2018, doi: 10.1007/s41870-018-0113-4.
- [9] H. Hui, Y. Ding, Q. Shi, F. Li, Y. Song, and J. Yan, "5G network-based Internet of Things for demand response in smart grid: A survey on application potential," *Appl. Energy*, vol. 257, no. August 2019, p. 113972, 2020, doi: 10.1016/j.apenergy.2019.113972.
- [10] W. Kong, J. Shen, P. Vijayakumar, Y. Cho, and V. Chang, "A practical group blind signature scheme for privacy protection in smart grid," *J. Parallel Distrib. Comput.*, vol. 136, pp. 29–39, 2020, doi: 10.1016/j.jpdc.2019.09.016.
- [11] H. E. Rostam, H. Motameni, and R. Enayatifar, "Privacy-preserving in the Internet of Things based on steganography and chaotic functions," *Optik (Stuttg.)*, vol. 258, no. March, p. 168864, 2022, doi: 10.1016/j.ijleo.2022.168864.
- [12] S. Devi, M. N. Sahoo, K. Muhammad, W. Ding, and S. Bakshi, "Hiding medical information in brain MR images without affecting accuracy of classifying pathological brain," *Futur. Gener. Comput. Syst.*, vol. 99, pp. 235–246, 2019, doi: 10.1016/j.future.2019.01.047.
- [13] M. S. Taha, M. Shafry, and M. Rahem, *High payload image steganography scheme with minimum distortion based on distinction grade value method*. Multimedia Tools and Applications, 2022.
- [14] S. Hossain, S. Mukhopadhyay, and B. Ray, "A secured image steganography method based on ballot transform and genetic algorithm," 2022.
- [15] D. Mehta and D. Bhatti, "Blind image steganography algorithm development which resistant against JPEG compression attack," *Multimed. Tools Appl.*, pp. 459–479, 2022, doi: 10.1007/s11042-021-11351-8.
- [16] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, 2019, doi: 10.1016/j.neucom.2018.06.075.
- [17] A. Abdullah, S. Ali, R. Mstafa, and V. Haji, "Image steganography based on DNA sequence translation properties," *UKH J. Sci. Eng.*, vol. 4, no. 6, pp. 15–26, 2020, doi: 10.25079/ukhjse.v4n1y2020.pp15-26.
- [18] O. A. Al-Harbi, W. E. Alahmadi, and A. O. Aljahdali, "Security analysis of DNA based steganography techniques," *SN Appl. Sci.*, vol. 2, no. 2, pp. 1–10, 2020, doi: 10.1007/s42452-019-1930-1.
- [19] D. Na, "DNA steganography: Hiding undetectable secret messages within the single nucleotide polymorphisms of a genome and detecting mutation-induced errors," *Microb. Cell Fact.*, vol. 19, no. 1, pp. 1–9, 2020, doi: 10.1186/s12934-020-01387-0.
- [20] M. S. L. A, "A Review on DNA based Encryption and Steganography," *Int. J. Sci. Res.*, vol. 6, no. 2, pp. 309–312, 2017, [Online]. Available: <https://www.ijsr.net/archive/v6i2/ART2017612.pdf>.
- [21] G. Kumaresan, N. P. Gopalan, and T. Vetriselvi, "An Efficient Image Block Encryption for Key Generation using Non-Uniform Cellular Automata," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 2, pp. 28–35, 2019, doi: 10.5815/ijenis.2019.02.04.
- [22] S. Yi and Y. Zhou, "Binary-block embedding for reversible data hiding in encrypted images," *Signal Processing*, vol. 133, no. October 2016, pp. 40–51, 2017, doi: 10.1016/j.sigpro.2016.10.017.
- [23] M. Mahmud, Atta-ur-Rahman, M. Lee, and J.-Y. Choi, "Evolutionary-based image encryption using RNA codons truth table," *Opt. Laser Technol.*, vol. 121, no. June 2019, p. 105818, 2020, doi:

- 10.1016/j.optlastec.2019.105818.
- [24] A. Jarjar, "Two Feistel rounds in image cryptography acting at the nucleotide level exploiting dna and rna property," *SN Appl. Sci.*, no. June, 2019, doi: 10.1007/s42452-019-1305-7.
- [25] A. Kumar and N. S. Raghava, "Chaos-based steganography technique to secure information and integrity preservation of smart grid readings using wavelet," *Int. J. Comput. Appl.*, vol. 0, no. 0, pp. 1–7, 2019, doi: 10.1080/1206212X.2019.1692511.
- [26] M. Wang, X. Wang, Y. Zhang, S. Zhou, T. Zhao, and N. Yao, "A novel chaotic system and its application in a color image cryptosystem," *Opt. Lasers Eng.*, vol. 121, no. December 2018, pp. 479–494, 2019, doi: 10.1016/j.optlaseng.2019.05.013.
- [27] W. H. A. A. Y. Al-ashwal, "Hybrid image steganography method using Lempel Ziv Welch and genetic algorithms for hiding confidential data," *Multidimens. Syst. Signal Process.*, vol. 33, no. 2, pp. 561–578, 2022, doi: 10.1007/s11045-021-00793-w.
- [28] O. Fouad and A. Wahab, "Hiding Data Using Efficient Combination of RSA Cryptography , and Compression Steganography Techniques," vol. 9, pp. 31805–31815, 2021, doi: 10.1109/ACCESS.2021.3060317.
- [29] A. K. Bairagi, R. Khondoker, and R. Islam, "An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," *Inf. Secur. J.*, vol. 25, no. 4–6, pp. 197–212, 2016, doi: 10.1080/19393555.2016.1206640.
- [30] S. kumar, R. Kumar, S. Kumar, and S. Kumar, "Cryptographic construction using coupled map lattice as a diffusion model to enhanced security," *J. Inf. Secur. Appl.*, vol. 46, pp. 70–83, 2019, doi: 10.1016/j.jisa.2019.02.011.
- [31] N. N. Hurrah, S. A. Parah, N. A. Loan, J. A. Sheikh, M. Elhoseny, and K. Muhammad, "Dual watermarking framework for privacy protection and content authentication of multimedia," *Futur. Gener. Comput. Syst.*, vol. 94, pp. 654–673, 2019, doi: 10.1016/j.future.2018.12.036.
- [32] H. Bae, B. Lee, S. Kwon, and S. Yoon, "DNA Steganalysis Using Deep Recurrent Neural Networks," pp. 88–99, 2017, [Online]. Available: <http://arxiv.org/abs/1704.08443>.
- [33] H. Li, L. Hu, J. Chu, L. Chi, and H. Li, "The maximum matching degree sifting algorithm for steganography pretreatment applied to IoT," *Multimed. Tools Appl.*, vol. 77, no. 14, pp. 18203–18221, 2018, doi: 10.1007/s11042-017-5075-1.
- [34] S. R. Kim, J. N. Kim, S. T. Kim, S. Shin, and J. H. Yi, "Anti-reversible dynamic tamper detection scheme using distributed image steganography for IoT applications," *J. Supercomput.*, vol. 74, no. 9, pp. 4261–4280, 2018, doi: 10.1007/s11227-016-1848-y.
- [35] N. N. Hurrah, S. A. Parah, J. A. Sheikh, F. Al-Turjman, and K. Muhammad, "Secure data transmission framework for confidentiality in IoTs," *Ad Hoc Networks*, vol. 95, p. 101989, 2019, doi: 10.1016/j.adhoc.2019.101989.
- [36] N. Singh and A. Sinha, "Optical image encryption using fractional Fourier transform and chaos," *Opt. Lasers Eng.*, 2008, doi: 10.1016/j.optlaseng.2007.09.001.
- [37] M. K. Priyanka Dongardive Neelesh Gupta, "Review on Different Methods of Image Steganography," *Int. J. Sci. Res.*, 2014.
- [38] D. R. Igantius and M. Setiadi, "PSNR vs SSIM : imperceptibility quality assessment for image steganography," 2020.
- [39] J. A. Michel-Macarty, M. A. Murillo-Escobar, R. M. López-Gutiérrez, C. Cruz-Hernández, and L. Cardoza-Avendaño, "Multiuser communication scheme based on binary phase-shift keying and chaos for telemedicine," *Comput. Methods Programs Biomed.*, vol. 162, pp. 165–175, 2018, doi: 10.1016/j.cmpb.2018.05.021.
- [40] P. Singh and B. Raman, "Reversible data hiding based on Shamir's secret sharing for color images over cloud," *Inf. Sci. (Ny)*, vol. 422, pp. 77–97, 2018, doi: 10.1016/j.ins.2017.08.077.
- [41] C. F. Lee and Y. L. Huang, "An efficient image interpolation increasing payload in reversible data hiding," *Expert Syst. Appl.*, vol. 39, no. 8, pp. 6712–6719, 2012, doi: 10.1016/j.eswa.2011.12.019.
- [42] ...L.University,UCIDImageDataset,<http://homepages.lboro.ac.uk/cogs/datasets/ucid/data/ucid.v2.tar.gz>[03, 01,13].