ISSN: 0067-2904

An Image Coding and Embedding Strategy Based on Channel Variations and DNA Sequences

Matheel Emaduldeen Abdulminuim*
Department of Computer Science, University of Technology, Baghdad, Iraq

Abstract

The digital multimedia systems become standard at this time because of their extremely sensory activity effects and also the advanced development in its corresponding technology. Recently, biological techniques applied to several varieties of applications such as authentication protocols, organic chemistry, and cryptography. Deoxyribonucleic Acid (DNA) is a tool to hide the key information in multimedia platforms.

In this paper, an embedding algorithm is introduced; first, the image is divided into equally sized blocks, these blocks checked for a small amount color in all the separated blocks. The selected blocks are used to localize the necessary image information. In the second stage, a comparison is between the initial image pixel and the watermark bit pixel is done to select the key that represents the location of a specific bit location that exist in all channels with its most dominant. If the compared bits are equal then (0) is added in least significant bit of least dominant color channel otherwise (1) is added. In the last stage, a regeneration process for the key is done. DNA based cryptographic algorithm has been suggested to develop secures image encryption techniques. This algorithm gives a good results, the MSE was (0.0007) for one test also the key generation method is successful.

Keywords: Channel variation, DNA coding, Watermark.

ستراتيجية ترميز صوره وطمرها بالاعتماد على اختلافات القناة وسلاسل الحمض النووي

مثيل عمادالدين عبد المنعم*
قسم علوم الحاسوب، الجامعة التكنولوجية، بغداد، العراق

الخلاصة:

الوسائط المتعددة الرقمية اصبحت منتشرة في الوقت الحاضر بسبب آثارها الحسية للغاية وتطوير التكنولوجيا المتقدمة المقابلة لها. في الآونة الأخيرة، اصبحت التقنيات البيولوجية أكثر وأكثر شعبية، ويتم اضافتها على أنواع كثيرة من التطبيقات مثل بروتوكولات التوثيق، الكيمياء الحيوية، وعلم التشفير. الحمض النووي هو وسيلة لاخفاء معلومات المفتاح في فايلات الوسائط المتعددة.

في هذا البحث تم اقتراح خوارزمية لترميز الصورة خلال ثلاث مراحل: الأولى، يتم فصل الصورة إلى كتل مختلفة، ويتم اختبار هذه الكتل لمعرفة أقل قناة لونية مهيمنة في هذه الكتل. يتم استخدام هذه القناة لتضمين الصوره. المرحلة الثانية هي عملية المقارنة باستخدام مفتاح وكل رقم في المفتاح يمثل موقع معين لبت موجود في واحد من اثنين من قنوات اللون الأكثر هيمنة. اذا كانت البت المستخرجة من قناة لون أقل المهيمنة مساوية للبت المستخرجة من العلامة المائية يتم وضع صفر في (LSB) للبت الاقل هيمنة ويوضع واحد خلافا لذلك. المرحلة الثالثة هي عملية اعادة توليد المفتاح. تم اقتراح خوارزمية تشفير بواسطة تقنية الحمض النووي لتطوير تقنية امينة لتشفير الصور. هذا البحث يعطي صورة مرمزه ذات جودة عالية فضلا عن توفير درجة عالية من التعقيد من خلال عملية التوليد.

*Email: matheel_74@yahoo.com

1. Introduction

Nowadays, the network processing becomes more robust plenty with the immense network revolution where the demands on the communication increased due to the knowledge of the web. So, the web could be known and the channel that is insecure can transmit knowledge. So, necessary data transmitted information should be processed to hide information via the web channels. There are two essential strategies for concealing secret message encryption and steganography [1].

The requirement of hiding information credibility is enlarged in different multimedia fields like image, video, audio and so on. "Stego Color Cycle" (SCC) method is strategy that indicates the channel that saves the data on it. Also, SCC strategy act on the color image to transmit the data in a secure desired channel. Therefore there is a hidden data between the overall channels regarded by its color [1, 2]. The essential problem of this method is that the data acts in these channels systematically, therefore finding the information easily in the beginning of the pixels causes a real problem [3]. By this idea, the embedding technique trusts a small amount of data in the dominant channel, and the small information is going to be modified in blocks so the modification is done automatically.

Parvez and Gutub in 2008 presented a method of sorting different bits in channels (R, G or B) that supports the values of pixels colors; then high bit rates stored in the part of the lower color. Various operations performed on DNA include synthesis, insertion, truncation, deletion, transformation, ligation and polymerase chain reaction etc. Parvez and Gutub [4] proposed an encryption method that used DNA subsequence operations such as truncation, deletion and transformation operation combined with chaos system to scramble the location and value of image pixel.

Also, Gutub in 2010 presented a new method that have the information from the bits that associated in every component within the color images. Each channel has knowledge that takes brings it from the Least Significant Bit (LSB) of the other two channels. Instead of depending upon different keys from a key management, one can use the key message to indicate the channel to insert the security for more randomize [5]. Tiwari and Shandilya in 2010 proposed two methods: The first one was component indicator technique and the other was "triple-A" algorithmic rule. This encryption method used DNA complementary rule where piecewise linear chaotic map is used for permutation and then substitution is performed using complementary rule [6].

In 2012 Lili and et al. presented a method for image encoding based on DNA cryptography with chaotic map. Simulation result shows that the proposed algorithmic rule encompasses a massive secret key and powerful secret key sensitivity. The results show that it is non-invertible and also it is weak against chosen plain text attack [8]. Por and et al. proposed a new algorithm on color system. For achieve the security, a steganography with several layers may be done by removing the secret message of the cover-images. The proposed algorithm has a good performance in security with no distortion on the image [7].

In this paper, an algorithm to encode and embed the image using the DNA strategy for key generation is presented. The paper is organized as follows. Section 2 describes DNA encoding, section 3 illustrates the proposed algorithm, and section 4 shows the results of the proposed algorithm. Finally, the conclusions are presented in section 5.

2. DNA encoding

DNA cryptography is emerging as a new cryptographic field where DNA is used to carry the information. The ability for huge storage and parallelism are making it suitable for image encryption. DNA encryption means combining DNA technique with cryptology and producing new cryptography to provide safe and efficient cipher services [6].

The information in DNA is kept as a code created of four chemical bases: "adenine (A), guanine (G), cytosine (C), and thymine (T)". DNA bases combine up with one another, A with T and C with G, to make units known as base pairs. Every base is additionally hooked up to a sugar molecule and a phosphate molecule. Together, a base, sugar, and phosphate square measure known as "nucleotide" [8].

Nucleotides are organized in two long strands that kind a spiral known as a "double helix". The structure of the spiral is somewhat sort of a ladder, with the bottom pairs forming the ladder's rungs and also the sugar and phosphate molecules forming the vertical side pieces of the ladder [9]. A very important property of DNA is that it will replicate, or build copies of itself. Every strand of DNA within the spiral will function a pattern for duplicating the sequence of bases. This is often crucial

once cells divide as a result of every new cell has to have a certain copy of the DNA present within the recent cell as in Figure-1.

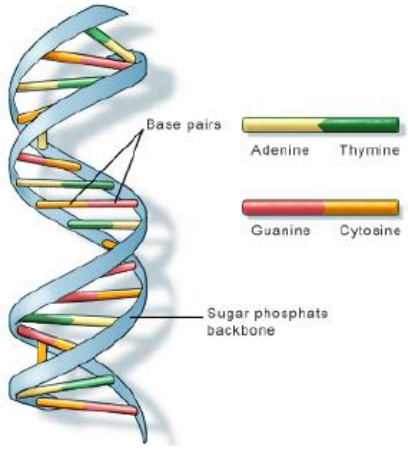


Figure 1- DNA is a double helix formed by base pairs attached to a sugar phosphate backbone.

In DNA with cryptography theory, the information is represented by DNA sequences. To use the specific four bases in DNA, one tend to use binary digits because the four binary digits 00 and 11, 01 and 10 are complementary and the range of cryptography components is equal 4! That is twenty four. Then there are an eight forms of combinations that is used for coding to satisfy the principle of complementary base in 24 forms of coding combination. Table-1 gives eight writing rules [8].

Table 1- Eight kinds of DNA map rules.

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

3. The proposed Algorithm

The proposed algorithm is designed to take a color image then adding a watermark to it. The resulted image is encrypted using a DNA strategy to generate the key sequence with high degree of performance.

The proposed method has different stages. Initially, the color image is read and concludes which image color was suitable for embedding. The color with no change in its pixels value represents a least dominant channel and the two other are the two most dominant channels.

The watermark binary image is added after converted to a single bit stream to the blocks that has not the smooth area of the blocks then every block that are extracted are checked to form the most dominant channel with small amount of bits.

The logistic map is a polynomial mapping of degree 2. It is an example of how chaotic behavior can arise from very simple non-linear equations. Mathematically, the logistic map is given by the following equation:

$$x_{i+1} = \mu x_i (1 - x_i) \quad \textbf{(1)}$$

where x_i (0,1) is the iterative value and x_0 is the initial value. When μ has a range [3.9, 4) it is highly sensitive to initial conditions and exhibits chaotic behavior. For μ = 3.57, the sequence X (μ, *x0)* = {*x0 x1, x2,...}* depend crucially on the initial condition *x0.* Even slight variations in *x0* result in highly different sequences, which is an important characteristic of chaos. Beyond μ = 4, the values eventually leave the interval [0, 1] and diverge for almost all initial values. In the logistic map, the quadratic difference in equation (1) should be on the interval (0, 1) as a stretching-and-folding operation. Here the initial conditions are taken as μ = 3.905, *x0* = 0.25 and *y0* = 0.36.

The key is generated by the DNA operation; the output from this operation is scrambling using the logistic map. This is achieved amongst the two most dominant channels of the image and generates the key again by XOR operation with the blocks of data pixels. When the key is ended a shift and rotate operation is done to begin again.

The steps of the method are obtained in Algorithm-1. Also Figure-2 represents a flowchart that determines how the algorithm is operated.

Algorithm 1- Embedding a watermark image in coded color image algorithm.
I/P: A 256 x 256 color image and a watermarked binary image (A).
O/P: Encrypted image with watermark.

Begin

Step 1: The color image is decomposed to different blocks, so the block with little loss of information is chosen.
Step 2: Convert the watermark image to single bit stream.
Step 3: For each block, determine the least dominant channel.
Step 4: Hide the bit of stream within the least dominant channel.
Step 5: When the set of key is completed, regeneration method will be done by shifting and rotate operation.
Step 6: Repeat steps from 3 to 5 till the entire watermarked image A is completed.
Step 7: Generate key image B by pseudo random sequence generator.
Step 8: B image is encoded using the DNA rule to get Be matrix.
Step 9: Two sequences x = (x1, x2,..., xn), y = (y1, y2,…, yn), are generated through logistical map using permutation operation over the DNA rule map.
Step10: The two indices value lx and ly are taken as (lx, ly) that are chosen from the sequences x and y to encode the DNA.
Step 11: Watermarked matrix is disorganized as Ae.
Step12: Then Ae and Be are XORed using DNA key that are generated form step 8 by XOR operation.
Step13: Finally by the DNA rule, the image is encoded to get the encrypted image.

End

This algorithm is used in reverse order to get the original image. The secret keys and also the key image are obtained from the sender before translation operation.

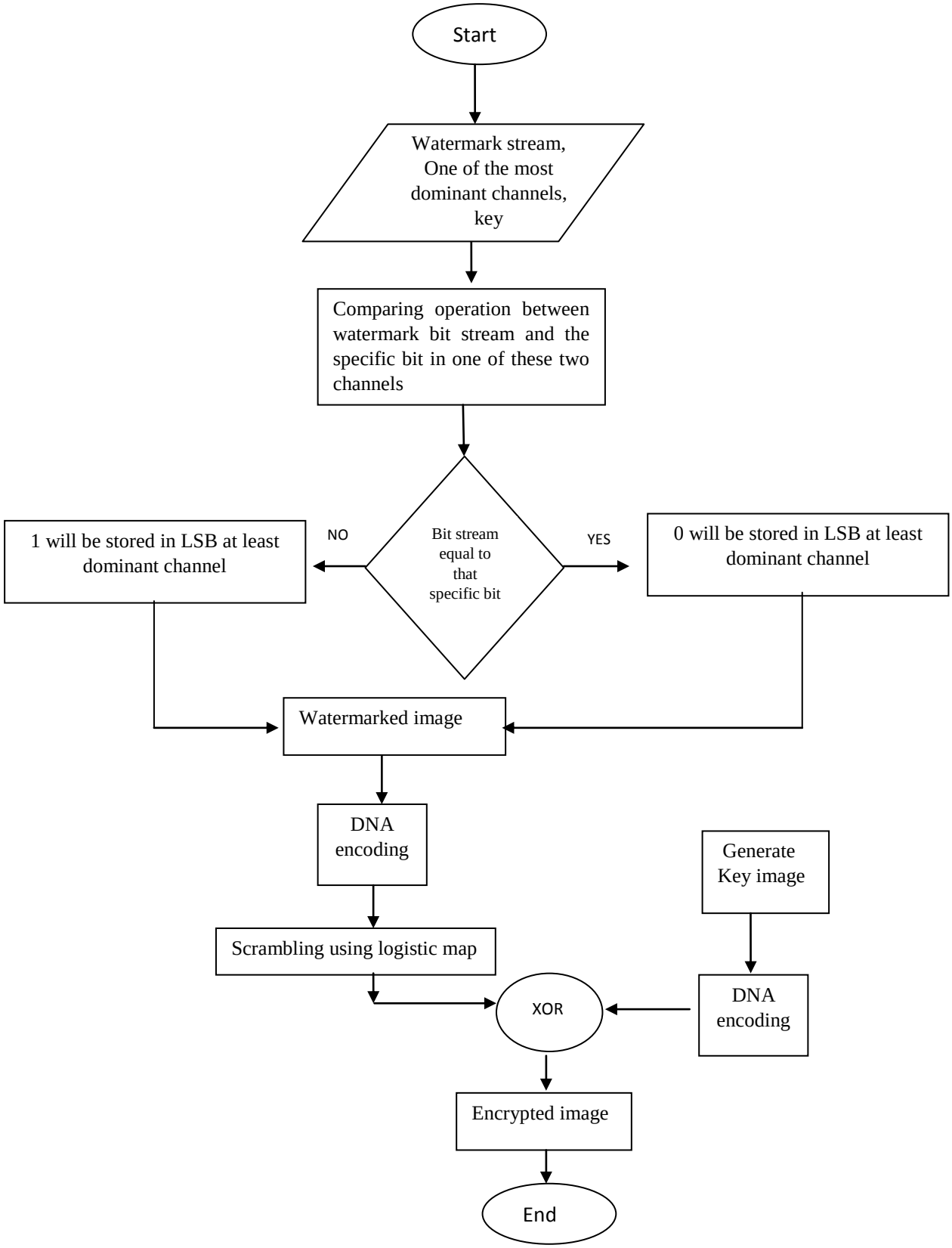


Figure 2- The flowchart of the proposed algorithm.

4. Results and Discussion

It is common that a lot of active or passive attacks were attainable on the ciphertext, there are essentially three major attacks that square measure against the proposed algorithm of image coding: Ciphertext attack, chosen ciphertext attack, improve chosen cipher text attack. However in our algorithm it's terribly troublesome due to multiple level of secret writing and therefore the key that one have a tendency to have taken. At the start one have a tendency to perform a channel variation, so using DNA strategy improve safety at multi-levels.

The proposed algorithm is very resistant against complete attacks like brute force attack attributable to multiple keys that square measure used at multiple levels. In each stages, it had been used a random select of channel that isn't potential for cryptanalysis to rewrite the first image information in polynomial time.

In the proposed algorithm, modifying the actual constituent intensity of the resultant image is done and using DNA rules makes hard for the statistical attack to identify the actual constituent values and positions.

Because of modifying the smallest amount dominant channel in blocks, the embedding method is modified. So, the proposed algorithm separates the watermark in non-stepwise method by finding the most important bit. The watermark is added sequentially on all the extracted blocks in image to increase robustness. Saving the watermark will not added in LSB directly for more security, extend of that the algorithm use a comparison operation to store the watermark bits and also using multiple secret keys.

Using DNA adds a lot of strong to the algorithmic rule quality. Figure-3 gives an example for the original and watermarked image with a small degree of MSE. This is done before adding the encryption operation using DNA rules. Table-2 represents a sample of initial image after adding the watermarked image and its encryption. Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) will be in a good range that maintains image quality. As shown in Table-3, the algorithm provides high PSNR and Low MSE.

Additionally table 4 provides the data entropy of the encrypted image. So, the values of the three different channels are arranged behind 7.6 that has a good value with minimum loss of information.

(a) **(b)**

Figure 3- Original and Watermarked Bird image. (a): Original image, (b): Watermarked image.

Table 2-The watermarked and encrypted image

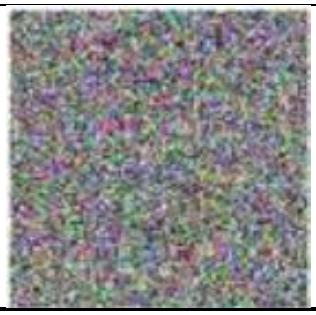
Image number	Watermarked image	Encrypted image
1 (Lena image)		
2 (Pepper image)		
3 (Flower image)		

Table 3-The fidelity criteria on the decrypted image.

Image number	Image size (KB)	MSE	PSNR
1	599	0.002	75.04
2	1176	0.00078	79.35
3	270460	0.0137	69.36

Table 4-The entropy evaluation.

Encrypted image	R Layer	G Layer	B Layer
1	7.6867	7.6877	7.6734
2	7.6894	7.6808	7.6789
3	7.6861	7.6871	7.6753

5. Conclusions

Security plays a controlling role in computer science, the importance of security is further increased because of internet usage. The proposed algorithm provides a high level of security for two reasons. First, the embedded secret message in cover image is not in a sequential fashion to prevent attacker to know that there is even secret message. Second, it depends on similarity principle which gives high quality arrange from 69 and 79 PSNR values on different images. Other feature, it provides high capacity because it embedded a random place bit in each pixel that has similar bits to secret messages.

Also the output of the algorithm provides a good evaluation because it gives good fidelity criteria with MSE (0.002, 0.00078 and 0.0137) on different images. Also, in this algorithm an improvement on the standard LSB approach was done so the serial embedding in LSB is avoided. The embedding operation is done indirectly for high security.

Reference

1. Inderjeet K, Rohini S and Deepak S. **2013**. Transform Domain Based Steganography Using Segmentation and Watermarking. , *International Journal of Computing and Business Research,* 4(1).
2. Grima D and Sumity K. **2013**. Two Layer Provision for Secure Data Transmission. *International Journal of Engineering Sciences Paradigms and Researches*, 03(01).
3. Manish M and Akashdeep S. **2010**. Steganography in Colored Images Using Information Reflector with 2k Correction. *International Journal of Computer Applications*,1(1).
4. Mohammad T and AdnanG. **2008**. RGB Intensity Based Variable-Bits Image Steganography. IEEE Asia-Pacific Services Computing Conference; December 9-12, Yilan, Taiwan.
5. Adnan G. **2010**. Pixel Indicator Technique for RGB Image Steganography. *Journal of Emerging Technologies in Web Intelligence*, 2(1).
6. Namita T and Madhu S . **2010**. Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth. *International Journal of Security and Its Applications*, 4(4).
7. Lip P, Delina B, Tan A, and Sim O. **2013**. An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm. *The International Arab Journal of Information Technology*; 10(1).
8. Lili L, Qiang Z, Xiaopeng W. **2012**. A RGB image encryption algorithm based on DNA encoding and chaos map. *Computers and Electrical Engineering Journal*, 3(6).
9. Samir B and Suman C. **2011**. Image hiding in DNA sequence using arithmetic encoding. *Journal of Global Research in Computer Science*, 2(4).