Secure Image Encryption Scheme Based on DNA and New Multi Chaotic Map

Roayat Ismail Abdelfattah¹, Hager Mohamed and Mohamed E Nasr
Department of Electronics and Electrical Communications, Faculty of Engineering
University Tanta, Tanta 31111, Egypt

E-mail: royat_esmaeel@f-eng.tanta.edu.eg
E-mail: hager_saqr@yahoo.com
E-mail: mohamed.nasr@f-eng.tanta.edu.eg

Abstract. Encryption of medical image is very important subject especially in wireless body area networks (WBAN) applications where the devices have many limitations in memory size, energy and computation capabilities. In this paper an image encryption scheme is introduced to be suitable for this limitations. The scheme consists of two phases. Firstly, the patient information (as name, age, ..etc) is hidden in the patient medical image (as x-ray, MRI, ..etc) using Least Signification Bit technique to reduce the capacity of data encrypted and make this information visually unavailable to unauthorized personnel. Secondly, the patient's medical image is encrypted using DNA coding rules and a new multi chaotic map system. DNA coding improves computational speed and provides large capacity for data transmission while the new multi chaotic map consists by merging Henon, Sin and Ten map (HST) to produces pseudo random sequences with more chaotic characteristics. Results show that this scheme has a good peak signal to noise ratio, low correlation, huge key space, key-dependent pixel value replacement and can resist statistical and differential attacks.

1. Introduction
The wireless network of the body area is one of the most important modern health care technologies. Through it we can monitor the health condition of the patient continuously without disrupting his daily life. For WBAN, patient data transmission has to be safe without losing patient privacy and data integrity. Because any change in data may lead to incorrect diagnosis and treatment. There are many challenges in WBAN such as limitation of memory, computation, mobility and scalability [1].

DNA cryptography is a promising technique for WBAN due to its many advantages [2]. Firstly, it has large parallelism which helps to improve computational speed. Secondly, it has large capacity to store information by DNA molecules and low power consumption. So DNA cryptography is a new technology for unbroken data and provides high security in WBAN compared to traditional cryptography such as DES and AES [3, 4]. Chaotic encryption technology has been widely used for image encryption due to its properties like initial conditions sensitivity, pseudo randomness and non-periodicity, which conform to the required characteristics of encryption [5, 6]. Due to the advantages of both DNA coding and chaotic system, scientists use both of them in images cryptosystem to produce more powerful and safe system difficult to be penetrated or broken [7-9].

¹ Corresponding Author.
Our Contribution
In the proposed scheme, DNA is used with a new one dimension (HST) map system which has more advantages than the simple chaotic system (henon map, sin map, ten map, …) such as larger parameter space, high randomization and many chaotic sequences. So it is hard to prophesy the chaotic series generated by (HST). In the medical image, the patient's information is usually printed in the corner of the medical image for presentation. As a result, it is easily available for anyone and may be intercepted by authorized user. So in this paper, the patient information is hidden in medical image which is then encrypted using the proposed encryption algorithm. This provides a more secure algorithm that can resist any attack types.

2. Related Work

2.1. DNA Encoding
DNA refers to Deoxyribonucleic acid is a nucleic acid which carries the genetic information of living organisms. In a DNA sequence there are four different nucleic acid bases adenine (A), thymine (T), cytosine(C), guanine (G), where C and G, T and A are pairs complementary. If four bases A, T, C, G are encoding to 00,11,10,01 we can get 24 types of encoding schemes. Because of the complementary relationship between DNA bases, there are eight types of coding groups that meet the principle of base complementarity, which are shown in table 1. This technique is used in the image encryption to obtain the image diffusion. As a result of the existence of eight types of DNA coding rules, there are also eight types of XOR for DNA bases. For example, The XOR rule for the DNA encoding rule 5 is shown in table 2.

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

Table 1. For DNA Encoding and Decoding rules.

Table 2. The XOR operation for DNA Sequence.

| A  | C  | G  | T  |
|----|----|----|----|
| A  | C  | A  | T  |
| C  | A  | C  | G  |
| G  | T  | G  | C  |
| T  | G  | T  | A  |

2.2. Chaotic System
Chaotic maps are dynamical systems with high sensitivity to control parameter and initial conditions. Any slight change in the initial conditions causes a remarkable deviation. This sensitivity has placed a strong limit on our ability to predict the performance of chaotic systems over a long period of time. Encryption schemes based on chaos use initial conditions as a cryptographic key. The chaotic maps are divided into one-dimensional and high dimensional chaotic maps. The one-dimensional map commonly has one variable and little parameters. The one dimension maps as Sine map and Tent map, indicated as: Sine map: \( S(n+1) = r \times \sin(\pi \times S(n)) \), Ten map: \( T(n+1) = r \times |1-2T(n)| \) and One-dimension decomposition henon map: \( h(n+1) = 1- a \ h(n) ^2 + b \ h(n-1) \).

2.3. Steganography
Steganography is a technique of hiding important information in ways that prevent it for being detect. The purpose of steganography is to deliver a message in a manner that no one other than the sender and the intended recipient doubts or feels the existence of the message. These messages are moved through cover carriers like text, audio, images. The simplest method to hiding data in image is called least significant bit insertion (LSB). In LSB algorithm, data is hidden in the least significant bits of the cover
image that cannot be observed by human. In grayscale image each pixel is representing in eight bit as figure 1. The bit of the secret message is put in some or all 8th bit of the bytes inside an image. The following equation illustrates the idea of the Steganography process:

\[
\text{Stego-image} = \text{cover image} + \text{information}
\]

Information maybe text OR image etc. In our scheme the secret message is the information of patient which is hidden in the patient medical image using LSB steganography.

Figure 1. Least significant bit.

3. Proposed Encryption Scheme

3.1. General description of proposed algorithm

3.1.1. Proposed multi chaotic map (HST). In our scheme, the Sin map and Ten map are combined with Henon map as show in figure 2 to get new one dimensional chaotic system with simple structure and more variables, parameters and more random behavior than single one dimensional map.

\[
Z(n+1) = 1 - a \times \sin[\pi \times Z(n)] + b \times r \times |1 - 2Z(n-1)|
\]

Where \(a, b, r\) is the chaotic system parameter and \(Z(n), Z(n-1)\) is initial value.

3.1.2. Statistical tests for (HST) map. The randomness of the proposed HST map is tested by the NIST test suit which consists of 16 statistical tests. These tests are defining if the generated sequence is random or not. The basic dependence within these tests is on the probability value (p-value). The p -value is compared by the significance level \(\alpha\) which is the threshold between rejection and non-rejection region. In NIST the significant level equal 0.01. For p-value less than 0.01 this means that the sequence is not random and reject and for p-value greater than 0.01 this means that the sequence is random and accepted. The result of sequence generated from the proposed map is shown in figure 3.

Figure 3. Proposed HST map randomness tests.
According to this result, the proposed HST chaotic map sequence is perfect random and suitable for being used.

3.2. Key Generation
In our scheme, SHA_256 hash function of the input image is used to get a 256-bit secret key K. So a single bit change in the plain image will produces a completely different hash value. The secret key K is divided to 8-bit blocks as in equation (2) and the initial values are obtained by equation (3),(4).

\[ K = k_1, k_2, k_3, \ldots, k_{32} \]  
\[ Z_0 = Z_0' + \left \lfloor \frac{(k_1 + k_2 + k_3 + \ldots + k_{16})}{256} \right \rfloor \]  
\[ Z_1 = Z_1' + \left \lfloor \frac{(k_{17} + k_{18} + k_{19} + \ldots + k_{32})}{256} \right \rfloor \]

Where \( Z_0' \) and \( Z_1' \) are Initial values given.

3.3. Encryption Algorithm
- Step1: The patient information is hiding in medical image \( I(m, n) \) (\( m, n \) is image dimensions) using LSB steganography and get the embedded image \( E(m, n) \).
- Step 2: Embedded image \( E \) is hashed to get the initial value of HST chaotic system according to section 3.1 and then by using crossover a new crossover image \( H(m, n) \) is generated.
- Step 3: \( H(m, n) \) matrix is transformed to binary sequence by represent each pixel in 8 and then encoding with chosen DNA encoding rules 5 \( H_{dna} \).
- Step 4: Generating chaotic sequence \( P \) using the proposed HST map whose length is \( m \times n \) with parameter \( a, b, r \) and initial value \( Z_0, Z_1 \).
- Step 5: Using chosen DNA encoding rule 5 again to encode chaotic sequence \( P \) The result is named as \( P_{dna} \).
- Step 6: According to XOR operation Table 2, \( P_{dna} \) is xored with \( H_{dna} \) and the result is decoding with another DNA chosen rule 7 to get cipher image \( V \).

Figure 4. Encryption algorithm.

3.4. Decryption Algorithm
- Step1: Cipher image is encoding according to chosen DNA rule 7 using in encryption algorithm getting \( V_{dna} \).
- Step2: Repeat step 4, 5 as in encryption algorithm.
- Step3: According to DNA XOR operation Table 2, \( V_{dna} \) is xored with \( P_{dna} \) to get \( H_{dna} \).
- Step4: Decoding \( H_{dna} \) with DNA chosen rule 5 and get \( H \).
- Step5: Inverse crossover to get embedded image \( E \).
- Step6: By using LSB steganography, patient information is extracted and get original medical image \( I \).
4. Experimental Simulation Result

4.1. Tools

In this paper, the proposed algorithm was implemented on a multiple image. the experiment is performed on a personal computer with Intel ®, core ™i7-8550u, CPU@1.80GH, and 8GB laptop running windows 10 using Wolfram Mathematica11.3 and MATLAB R2016a. The secret keys are $a=1.4$, $b=0.3$, $r=0.399$, $Z_0'=0.1$, $Z_1'=0.25$. The encryption and decryption images are plotted in figure 6. It is clear that there is no relationship between the original and encrypted images which indicates that this algorithm has achieved visual security performance testing. The other security performance tests such as key space, key sensitivity, entropy, peak signal to noise ratio, correlation, uaci, npcr and noise added test are illustrating in next section (4.2).
4.2. **Security Analysis and performance tests**

4.2.1. **Key space analysis.** For a good encryption scheme, the key space has to be big enough to stand against the brute force attack. In our scheme, the keys are the initial values $Z_0'$, $Z_1'$ and the parameter $a$, $b$, $r$ and 256 bit for hash value. For $a$, $b$, $r$, $Z_0'$, $Z_1'$, the computational precision of the 64-bit dual resolution number is about $10^{-15}$ according to the IEEE standard [10], the security of SHA256 with complexity of the best attack as $SHA256 = 2^{128}$, So that the total key space = $2^{128} \times 10^{75} \approx 3.4028 \times 10^{113}$ which is bigger than the maximum key space ($2^{256}$) of practical symmetric encryption of AES [11]. So it is big enough to resist brute-force attack.

4.2.2. **Key sensitivity analysis.** Key sensitivity means that the encrypted image can only be decrypted by the correct key and any attempt to decrypt it with other keys will fail. If it is decrypted by the wrong key, no information about the image can be obtained. Figure 7, illustrates the decryption process for the correct key and the decryption process using the wrong key. It is clear that the decryption process using the wrong key does not give any features to the original image.

4.2.3. **The gray histogram analysis.** The histogram is a chart that reflects the frequency or distribution of pixel values in grayscale image. the histogram of the encryption image has to be sufficiently flat. Figure 8 plots the histograms of both original image and encrypted image of Lena. It is clear that the histogram of the two images is quite different and histogram of encrypted image is uniform which makes it capable of confronting the statistical attack.

4.2.4. **Entropy analysis.** Information entropy is the hallmark of randomness. Here, the information entropy is considered to evaluate the amount of randomness in the image. For the ideal grayscale image the maximum value of the information entropy is 8 according to the following equation.

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \log_2 \frac{1}{p(m_i)}$$ (5)
where \( m, P (m_i) \) is denotes to information source and the probability of symbol \( m_i \) respectively. Table 3 provides a comparison of the entropy of Lena image while Table 4 provides the entropy of other tested medical images.

| Test image | CT | Reference[18] | MRI-1 [18] | MRI-2 | MRI-3 | MRI-4 | MRI-5 | MRI-6 |
|-----------|----|----------------|-----------|-------|-------|-------|-------|-------|
| Plain image | 3.9854 | 3.9854 | 5.6047 | 5.6047 | 7.1252 | 6.6276 | 6.7585 | 6.9311 | 3.6270 |
| Cipher image | 7.9974 | 7.9973 | 7.9975 | 7.9974 | 7.9974 | 7.9974 | 7.9974 | 7.9971 | 7.9973 |

4.2.5. Correlation analysis. Correlation coefficient is used to calculate the relation between two neighboring pixels in an image. For a good encryption, there should be no correlation between two neighboring pixel of the encrypted image. For our scheme, the correlation coefficients were calculated according to the equation (6) using randomly 4000 pairs of neighboring pixels from original and cipher image and the result is show in Table 5.

\[
R_{xy} = \frac{\text{Cov}(x,y)}{\sqrt{\text{D}(x)\text{D}(y)}}, \quad \text{Cov}(x,y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))
\]

\[
E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i, \quad D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2
\]

From these results, we can see that the correlation coefficients in the original image are close to 1 while the encrypted image coefficients are approximately 0. This means that our scheme succeeded in eliminating the relation between neighboring pixels in the image, which makes it able to prevent statistical attacks as show in figure 9.
Figure 9. Correlation of Two Neighboring Pixels.
Table 5. Correlation of two neighboring pixels of the plain-images and cipher-images.

|                        | Horizontal | Vertical | Diagonal |
|------------------------|------------|----------|----------|
| Original Lena image    | 0.9421     | 0.9662   | 0.9150   |
| Encrypted Lena image   | 0.0025     | 0.0011   | 0.0019   |
| Original CT image      | 0.9753     | 0.9744   | 0.9955   |
| Encrypted CT image     | 0.0001     | 0.0041   | 0.0029   |
| Original MRI-1 image   | 0.9635     | 0.9655   | 0.9412   |
| Encrypted MRI-1 image  | 0.0071     | 0.0034   | 0.0015   |
| Original MRI-2 image   | 0.9688     | 0.9893   | 0.0694   |
| Encrypted MRI-2 image  | 0.0073     | 0.0041   | 0.0019   |
| Original MRI-3 image   | 0.9933     | 0.9867   | 0.9929   |
| Encrypted MRI-3 image  | 0.0033     | 0.0060   | 0.0011   |
| Original MRI-4 image   | 0.9952     | 0.9874   | 0.9889   |
| Encrypted MRI-4 image  | 0.0047     | 0.0031   | 0.0018   |
| Original MRI-5 image   | 0.9235     | 0.9566   | 0.8956   |
| Encrypted MRI-5 image  | 0.0024     | 0.0036   | 0.0019   |
| Original MRI-6 image   | 0.9761     | 0.9806   | 0.9632   |
| Encrypted MRI-6 image  | 0.0040     | 0.0038   | 0.0011   |

4.2.6. PSNR analysis. Peak signal to noise ratio is used in image quality assessment, which is defined arithmetically by the mean square error (MSE) by the following equation.

$$PSNR = 20 \log_{10}(Max(I) / \sqrt{MSE})$$

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (G_0(i,j) - G_1(i,j))^2$$ (7)

Table 6 reports MSE and the PSNR values for the encrypted images using our scheme. The results show that the PSNR values between the encrypted and original image using our scheme is small and the MSE value between the encrypted and the original image is large. This means that the scheme has a good performance and more security.

Table 6. MSE & PSNR.

|         | MSE   | PSNR |
|---------|-------|------|
| Lena    | 9131.17 | 8.56 |
| CT      | 15144.68 | 6.36 |
| MRI-1   | 12819.64 | 7.09 |
| MRI-2   | 12077.12 | 7.35 |
| MRI-3   | 13623.49 | 6.82 |
| MRI-4   | 11670.33 | 7.49 |
| MRI-5   | 12558.48 | 7.18 |
| MRI-6   | 16817.41 | 5.91 |

4.2.7. Resistance to differential attack. The sensitivity of an encrypted image to the few changes in the original image is one way of measuring the resistance of image encryption algorithms to differential analysis. The two measures used are NPCR and UACI, which are calculated by the following equations.

$$NPCR = \frac{1}{M \times N} \left( \sum_{i,j} D(i,j) \right) \times 100\%$$

$$UACI = \frac{1}{M \times N} \left( \sum_{i,j} \left| \frac{c_1(i,j) - c_2(i,j)}{255} \right| \right) \times 100\%$$

$$D(i,j) = \begin{cases} 0 & c_1(i,j) = c_2(i,j) \\ 1 & c_1(i,j) \neq c_2(i,j) \end{cases}$$ (8)

In our scheme one pixel was changed in the original image and both NPCR and UACI are measured and the results are shown in table 7 and 8. It is clear from the results that the values that our scheme is capable of facing differential attacks.
Table 7. UACI & NPCR of Lena.

|                  | Proposed algorithm | Reference[7] | [13] | [14] | [15] | [16] | [17] |
|------------------|--------------------|--------------|------|------|------|------|------|
| UACI             | 33.571             | 28.71        | 32.212| 33.347| 33.49 | 33.419| 33.457|
| NPCR             | 99.613             | 99.60        | 98.475| 99.621| 99.62 | 99.6041| 99.6077|

Table 8. UACI & NPCR of Tested medical images.

| Test image | CT   | MRI-1 | MRI-2 | MRI-3 | MRI-4 | MRI-5 | MRI-6 |
|------------|------|-------|-------|-------|-------|-------|-------|
| UACI       | 33.483| 33.587| 33.423| 33.489| 33.487| 33.481| 33.447|
| NPCR       | 99.589| 99.609| 99.584| 99.568| 99.587| 99.609| 99.586|

4.2.8. Noise added analysis. The encrypted image is exposed to noise during transmission in a noisy channel. The strength of the algorithm is measured by noise resistance and the ability of reliable receiver to recognize the image after decoding it. The proposed scheme is tested by adding Gaussian noise with variance 0.01 and mean zero and pepper and salt noise with density 0.05 to cipher image and then decrypt it with correct key. The cipher image is shown in figure 10.

Figure 10. (a),(b) cipher and decrypted image with Gaussian noise, (c), (d) cipher and decrypted image with salt & pepper noise respectively.

4.2.9. Complexity computation. A good encryption algorithm needs to have a fast encryption time and low computation complexity. In the proposed algorithm, patient information is hiding in his medical image and then encrypted embedded image so the encoding time for embedded image is less than the encoding time for text and images on their own. The computation complexity of the proposed algorithm is calculated as follows for embedded image matrix m x n time complexity is \(O(m \times n)\) then the complexity time for encoding image to DNA is \(O(4 \times m \times n)\). also the complexity for chaotic map sequence is \(O(m \times n)\) then the complexity time for encoding chaotic to DNA is \(O(4 \times m \times n)\) and DNA xor operation complexity time is \(O(4 \times m \times n)\) and the time of decoding DNA sequence is \(O(8 \times m \times n)\). Thus the total time of complexity is almost equal \(O(8 \times m \times n)\). The complexity time can also be reduced if the proposed algorithm is applied in parallel mode.

5. Conclusion
In this paper, the steganography and cryptography technique has been used for image encryption. Firstly, the patient’s information is concealed in his / her medical image using LSB steganography. Secondly, the medical image is encrypted using the proposed encryption scheme which achieves the process of the confusion and diffusion by using DNA encoding rules and new HST map which combines henon, sin and ten map to produce chaotic series with high degree of randomness. Finally, the cipher image is tested and the results prove that it has low correlation, high entropy value, low PSNR value and uniform
histogram. Security analysis shows that our scheme has a high level of security, large key space and can resist all type of attacks, compared with other schemes.

6. References

[1] Omala A A, Robert N and Li F 2016 Aprovably-secure transmission scheme for wireless body area networks *Journal of medical systems*. 40 p 247.

[2] Raj B B and Vijay J V 2016 Securing data transfer through dna cryptography using symmetric algorithm *International Journal of Computer Applications*. 133 pp 19–32.

[3] Poriye M and Upadhyaya S 2016 Improved security using dna cryptography in wireless sensor networks *International Journal of Computer Applications*. 155 pp 323–5.

[4] Hossain S, Alam R, Biswas R and Morimoto Y 2016 A dna cryptographic technique based on dynamic dna sequence table *International Conference on Computer and Information Technology (ICCIT)*. 51 pp 270–275.

[5] Teng L, Wang X and Meng J 2018 A chaotic colour image encryption using integrated bit-level permutation *Journal Multimedia Tools and Applications*. 77 pp 6883–6896.

[6] Dagadu J C, Li J, Aboagye E O and Ge X 2017 Chaotic medical image encryption based on arnold transformation and pseudo randomly enhanced logistic map *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*. 4 pp 8096–8103.

[7] Cui G, Wang L, Zhang X and Zhou Z 2018 An image encryption algorithm based on dynamic dna coding and hyper-chaotic lorenz system *International Conference on Bio-Inspired Computing: Theories and Applications*. 952 pp 226–238.

[8] Zhang X, Han F and Niu Y 2017 Chaotic image encryption algorithm on bit permutation and dynamic dna encoding *Computational Intelligence and Neuroscience*. ID 63 6519675 p 11.

[9] Paul S, Dasgupta P, Naskar P K and Chaudhuri C 2017 Secured image encryption scheme based on DNA encoding and chaotic map *International Information and Engineering Technology Association*. 4 pp 70–75.

[10] F. W. Group and others 1985 IEEE Standard for Binary Floating-Point Arithmetic. *ANSI IEEE Std.754–1985*.

[11] Joan D, Vincent R 2002 The design of rijndael AES - the advanced encryption standard. (berlin heddberg : springer).

[12] Sujarani R and Manivannan D 2017 Anon linear two dimensional henon_sine chaotic map based image cryptosystem *International Journal of Pure and Applied Mathematics*. 115 pp 215–221.

[13] Sathishkumar G A, Bagan K B and Sriraam N 2011 Image Encryption Based on Diffusion and Multiple Chaotic Maps *International Journal of Network Security & Its Applications*. 3 pp 181–194.

[14] Liu Y, Lin T, Wang J and Yuan H 2018 Bit image encryption algorithm based on hyper chaos and dna sequence *Journal of Computers*. 29 pp 43–55.

[15] Gan G, Lu Y, Chen Y and Han D 2017 A novel image encryption algorithm based on the chaotic system and dna computing *International Journal of Modern Physics C*. ID 28 1750069.

[16] Yu Zhang L, Hu H, Liu Y and Wong K 2014 A chaotic image encryption scheme owning temp-value feedback *Communications in Nonlinear Science and Numerical Simulation*. 19 pp 3653–3659.

[17] Hu T, Liu Y, Gong L and Ouyang C 2016 An image encryption scheme combining chaos with cycle operation for dna sequences *An International Journal of Nonlinear Dynamics and Chaos in Engineering Systems*. 87 pp 51–66.

[18] Dagadu J C, Li J, Aboagye E O and Deynu F K 2019 Medical image encryption scheme based on multiple chaos and dna coding *International Journal of Network Security*. 21 pp 83–90.