An Analysis and Comparison Performance of DNA and Chaotic Method Combination for Image Encryption

V Saputra¹, D R I M Setiadji² and E H Rachmawanto³

¹, ², ³ Department of Informatics Engineering, Dian Nuswantoro University, 207 Imam Bonjol Street, Semarang 50131, Indonesia.

Abstract. There is a variety of important and personal information stored in an image that is often shared via the internet. Cryptography is one way to protect these image files, so that private information cannot be read by malicious third parties. The DNA and Chaos methods are one of the cryptographic methods that are widely proposed and combined. Some previous research proposes a combination of these two methods with a sequence of different methods and different testing techniques where all the research claims the results are very good. This research aims to analyze and compare the performance of two methods namely DNA-Chaos and Chaos-DNA with more complete measurement tools such as PSNR and SSIM to measure results visually, there is also entropy to measure the probability of encryption results can be solved, NPCR and UACI to find out encryption strength from differential attacks and image histogram analysis. From the test results, it appears that both methods have their own strengths and weaknesses. Chaos-DNA is superior in entropy, and UACI, while DNA-Chaos is superior in PSNR, SSIM and NPCR values, but the difference is not significant, so it can be said that the performance of the two methods is quite identical. The results of the histogram analysis also showed that the shape of the histogram generated from the encrypted image was also quite similar.

1. Introduction
In an era with the development of computer technology that is very fast at this time, the storage of files in physical form turned into file storage in digital form. Multimedia files such as images, audio, and video are also increasing and are stored in the cloud through the internet network. Advances in internet technology have a negative effect because of openness and network sharing so that the security of digital files against serious threats during the transmission process [1]. As a result, we need a system that can secure the confidentiality of multimedia information. Among various methods of protection, image encryption techniques are one of the most efficient and common methods for protecting digital file information especially images [2].

One popular cryptographic algorithm is Chaos Map [3], where this algorithm performs randomization with certain patterns in a system. Chaotic systems have properties where and their initial values are sensitive, aperiodic, and non-convergent [4,5]. Properties in chaotic systems can be used to generate random sequences. Research on chaos-based cryptography has been widely implemented before on digital images. However, in these studies it is said, many encryption algorithms use a single chaotic function, making it vulnerable to interpretation [6]. Another cryptographic algorithm, Deoxyribonucleic Acid (DNA), this algorithm can be combined with chaotic algorithms to increase its safety. The workings of the DNA method is inspired by how the DNA of living things works.

Information stored in DNA is stored as a code consisting of four elements namely adenine (A), guanine (G), cytosine (C) and thymine (T). In binary form, 0 and 1 are a complement, 00 and 11 are also
complement, 01 and 10 are also complement. From this basis the DNA algorithm is concluded as A is 00, C is 01, G is 10 and T is 11[7–9]. Each DNA element is paired with each other where A is paired with T and C is paired with G. These pairs will form a unit called the base pair, where each base pair will complement one another.

In some research predecessors like [2] and [6] proposed a hybrid encryption technique that combines Chaos and DNA methods to improve image encryption security. This encryption is also called super encryption because it combines two different methods[10]. The difference is the order in which the methods are used, such as in research [2] DNA is done first then followed by chaos method, while in research [6] have the reverse method sequence. In research[2] the DNA-Chaos method has been tested and proven that this method is resistant to exhaustive attacks and has good test results. In more detail, in research [2] the stages of the research are started from an original image that is converted into a binary number matrix which is then translated into DNA language and the addition of chaotic maps, where chaotic maps are used are 2D Logistic Maps. However, the trial results are only measured using PSNR, although the results are very good at 7,988 dB. However, because the measuring instrument used is still incomplete, more detailed testing is needed.

Just as in research [2], research [6] also concluded that the Chaos-DNA method is also a good combination of encryption and resistance to attack, where the encryption results are measured using entropy and PSNR. The results are also very good where the resulting PSNR values range from 7.86 to 9.59 dB and entropy values of 7.98 to 7.99 bits. In this study, a comparison of the two methods, DNA-Chaos and Chaos-DNA, will be carried out with various types of measurements aimed at analyzing the results more accurately, so that the best formula for the combination of these methods is known.

2. Literature Review

2.1. Deoxyribo Nucleic Acid (DNA) Cryptography

DNA must be possessed by all living things ranging from the smallest creatures such as viruses to complex living things like humans. DNA carries a lot of information from a living thing. DNA is also a long polymer of a small unit called nucleotides[11]. DNA is a kind of molecule that forms a genetic sequence. DNA pieces containing the genetic code are known as genes. The information contained in genes is stored in DNA [12]. In DNA there are basic forms of DNA structure that are shaped like two helices that form hydrogen bonds, namely Cytosine (C), Thymine (T), Adenine (A) and Guanine (G)[8]. There is a principle called Watson-Crick base complementary principle which is the relationship between several pairs, namely A (adenine) with T (thymine) and C (Cytosine) with G (guanine) so that they form a series of the double helix. This principle is then implemented in a cryptographic method called DNA cryptography. You do this by changing bases A, C, T, and G into bases 00, 11, 10 and 01. Furthermore, 24 conditioning patterns are made which are presented in Table 1.

Table 1 shows 24 encoding forms of the DNA algorithm, which are divided into 8 combinations of encoding patterns. The number 11001001(2) is the same as 20110(10) if it is coded into a form of DNA in combination with column 8 is ATGC. The results of the coding will make a different interpretation when they want to be returned to the form of binary numbers when someone uses the combination form[12]. For example, by using a combination of column 7, the result of the ATGC encoding should be 20110(10) to 1100011(2) = 198(10).

Table 1. Form of DNA Encoding.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| A | 00 | 00 | 01 | 01 | 10 | 10 | 11 | 11 |
| T | 11 | 11 | 10 | 10 | 01 | 01 | 00 | 00 |
| C | 01 | 10 | 00 | 11 | 00 | 11 | 01 | 10 |
| G | 10 | 01 | 11 | 00 | 11 | 00 | 10 | 01 |
In general, in the process of encrypting images with the DNA method, the original image will take the bit value in each pixel to be used as a key, then the key is converted to hexadecimal which is then used as a binary number matrix. After that, the value of R, G, B in the picture is taken its bit value then translated into a DNA code that is A, T, G, C. Then the formation of mRNA comes from the opposite of the DNA code that was formed earlier. The final step is to perform an XOR operation using a key that has been obtained with mRNA to form an encrypted image.

2.2. Chaos Map

Chaos Map is a polynomial mapping that shows a pattern of irregular chaotic maps [13], where the encryption technique used in chaos maps is diffusion or pixel scrambling [14]. Equations in the chaotic map can be seen in the formula (1).

\[ X_{n+1} = \mu X_n (1 - X_n) \]  

In the encryption process, later pixels that have been encrypted are randomized using a logistic function to make images more complicated to decrypt.

3. Proposed Method

In this research, the method to be proposed is two methods to be compared, namely the DNA-Chaos method which will be explained in Scheme 1 and Chaos-DNA in Scheme 2. Both of these schemes will be measured, analyzed and compared to find out if there are differences in performance and if there can be which schema performance is better. Each scheme will consist of encryption and decryption processes.

3.1. Scheme 1

![Scheme 1](image)

**Figure 1. DNA-Chaos Encryption Process**

The schematic of the scheme 1 encryption process in Figure 1 is detailed as follows:

1) For the key generation process, the key is taken from a plain image byte array and converted to a byte array that is encrypted with the SHA 256 function.
2) Plain image is set to RGB pixel value, then the pixel value is converted to bits.
3) The bits are converted into arrays and then translated into messages in DNA cryptography.
4) The array that has been translated then converted into its opposite to form mRNA.
5) After the array value has become mRNA, then the array is randomized with chaotic sequences and produces a new DNA code.
6) Then with the XOR operation, an encrypted image is formed.
Furthermore, the decryption process for Scheme 1 presented in Figure 2 can be explained in more detail as follows:

1) The encrypted image will be taken by the RGB value first.
2) The RGB values that have been obtained are then operated on with XOR, then the DNA code that has been obtained is randomized with chaotic sequences to their original form.
3) Then the encrypted DNA code is rewritten in reverse from before then the decryption image will be obtained.

### 3.2. Scheme 2

Figure 3. Chaos-DNA Encryption Process
The schematic of the scheme 2 encryption process in Figure 3 is as follows:

1) Plain image is taken RGB values from the matrix and then randomized with chaos sequences then performed XOR surgery.
2) Then the image that has been formed, the bit value is taken and converted to an array. Arrays that have been formed are translated into codes in the DNA algorithm.
3) The key formation process is taken from the bit value of the original image into an array and changed with the SHA 256 function.
4) The array that has been translated then converted into its opposite to form mRNA.
5) New encrypted images are formed.

![Figure 4. Chaos-DNA Decryption Process](image)

Furthermore, the decryption process for scheme 2 presented in Figure 4 can be explained in more detail as follows:

1) From the encrypted image, the RGB value is taken, then translated into the DNA code.
2) After that, the DNA code obtained will be translated again with the opposite to produce mRNA. Then it was scrambled back like everything with chaos sequences.
3) After that, it is operated on with XOR so that the decrypted image is obtained.

4. Implementation and Testing

| Table 2. Plain image used. |
|-----------------------------|
| Image | Car | Lady | House and Car | House | Girl |
| ![Car Image](image) | ![Lady Image](image) | ![House and Car Image](image) | ![House Image](image) | ![Girl Image](image) |
| Resolution | 200×200 | 256×256 | 512×512 | 256×256 | 640×854 |
| Extension | .jpg | .tiff | .tiff | .tiff | .jpg |
In this study, the proposed image encryption method will be implemented in color images in RGB format. So that the test results are better, the images used are quite diverse where each image has a different size and extension. All processes in this research use the Python programming language 3.7.3. The image used is presented in Table 2.

In the first stage, encryption with scheme 1 and scheme 2 with key input and the original image is performed, resulting in an encrypted image which is presented in Table 3. In table 3 also a PSNR value is calculated from the difference between the original image and the encrypted image. PSNR value can be calculated from the MSE value, where if the greater the MSE, the PSNR value will be smaller, and vice versa. In cryptography, the target PSNR value is as small as possible because the smaller the PSNR the more different the encryption results. In addition, SSIM values are also presented. SSIM is a well-known quality metric that is relatively newer than PSNR, where the SSIM is measured measuring the degree of similarity between two images. SSIM has a value between 0-1, which means that if the value is getting closer to 1 then the image has a high level of similarity, and if getting closer to the number 0 then the similarity level of the two images is small. While the formula used to calculate SSIM and PSNR can be seen in research [15].

### Table 3. Encryption Results.

| Image         | Scheme 1 (DNA-Chaos) | Scheme 2 (Chaos-DNA) |
|---------------|----------------------|----------------------|
|               | PSNR         | SSIM         | PSNR         | SSIM         |
| Car           | 27.9051   | 0.0154   | 27.9211   | 0.0155   |
| Lady          | 27.9080   | 0.0188   | 27.9134   | 0.0197   |
| House and car | 27.9091   | 0.0189   | 27.9112   | 0.0190   |
| House         | 27.9025   | 0.0237   | 27.9079   | 0.0238   |
| Girl          | 27.8975   | 0.0188   | 27.9152   | 0.0190   |
The results shown in table 3 show that the visual difference is not much different, but the DNA-Chaos method is slightly superior where the average PSNR produced is 27.9044 dB while the Chaos-DNA method produces a PSNR value of 27.91376 dB, as well as the SSIM method DNA-Chaos yields 0.0191 while the Chaos-DNA method produces values 0.0194. It can be concluded that visually the difference is very small and not as significant. In the next measurement the entropy, UACI, and NPCR values are tested. Entropy is a possible value that a file contains information about the key so that the file that has been mathematically encrypted can be decrypted[16]. Entropy can be calculated with equation (2).

\[ T(x; y) = H(x) - H_y (x) = H(y) - H_x (y) = H(x) + H(y) - H(x,y) \]  

The NPCR and UACI first appeared in 2004 by Yaobin Mao and Guanrong Chen. Since then NPCR and UACI have become two of the most widely used methods of security analysis in encrypting images for differential attacks. The NPCR is centered on an exact number or an absolute number that indicates the value of how much the pixel's value changes. Whereas UACI focuses on the difference between the original image and the encrypted image[17]. NPCR has a distance between 0-1. If the NPCR shows the number 0 then all the pixels in picture A are the same as in picture B. And if the NPCR shows the number 1, then all the pixels in picture B change totally compared to picture A. The value in UACI also has a distance between 0-1 which indicates when the greater the value the difference in intensity between the two encryption images. Where in the case of image encryption, image A is the original image and image B is the encrypted image. The formula for calculating NPCR and UACI can be seen in research [17]. Whereas in Table 4 presents the value of Entropy, UACI, and NPCR.

| Image         | Scheme 1 (DNA-Chaos) | Scheme 2 (Chaos-DNA) |
|---------------|----------------------|----------------------|
|               | Entropy | NPCR | UACI | Entropy | NPCR | UACI |
| Car           | 7.6988  | 0.9960 | 0.3047 | 7.7155  | 0.9958 | 0.3048 |
| Lady          | 7.7262  | 0.9948 | 0.2597 | 7.7315  | 0.9947 | 0.2560 |
| House and car | 7.7254  | 0.9953 | 0.2476 | 7.7293  | 0.9953 | 0.2478 |
| House         | 7.7259  | 0.9949 | 0.2049 | 7.7694  | 0.9948 | 0.2050 |
| Girl          | 7.7257  | 0.9962 | 0.3247 | 7.7357  | 0.9960 | 0.3247 |
| Average       | 7.7204  | **0.9954** | 0.2683 | **7.7363** | 0.9953 | **0.2677** |

Based on Table 4 it can be seen that the method in scheme 1 is superior to the NPCR value while for entropy and UACI it is superior to the method contained in scheme 2.

A histogram is a graphical representation of the color distribution of a digital image. This graphic consists of two axes namely Y or Vertical axes and X or Horizontal axes. The Y-axis represents the number of pixels of a gray level value, while the X-axis represents the gray level. The results of the histogram generated from the encrypted image are presented in Table 5. Where this histogram is a combination of all layers R, G, and B.

| Image | Original | DNA-Chaos | Chaos-DNA |
|-------|----------|-----------|-----------|
| Car   | ![Histogram](car.png) | ![Histogram](dna-chaos.png) | ![Histogram](chaos-dna.png) |
Based on the results of the histogram presented in Table 5 it appears that the histograms of the two scheme schemes are quite similar. However, both of these methods also succeeded in significantly changing the shape of the image histogram.

5. Conclusions
Preliminary research claims that the combination of the two methods has good performance, where each research proposes using a different method sequence, namely DNA-Chaos and Chaos-DNA. This research aims to make sense and compare the performance of a combination of DNA and Chaotic methods in image encryption with more complete testing methods and measuring instruments such as PSNR, SSIM, Entropy, NPCR, UACI and histogram analysis. The results show that each method has its own advantages and disadvantages. DNA-Chaos is superior to PSNR, SSIM and NPCR values, whereas Chaos-DNA is superior to entropy, and UACI. But the difference in value is very thin, so it can be said that the performance of the two methods is similar. The results of the histogram analysis also show that the shape of the histogram generated from the encrypted image is also identical.

6. References
[1] Ardy R D, Indriani O R, Sari C A, Setiadi D R I M and Rachmawanto E H 2017 Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5) Proceeding of 2017 International Conference on Smart Cities, Automation and Intelligent Computing Systems,
[2] Zhang Q and Guo L 2010 Image encryption using DNA addition combining with chaotic maps *Math. Comput. Model.* **52** 2028–35

[3] Irawan C, Setiadi D R I M, Rachmawanto E H, Sari C A and Doheir M 2019 Hybrid Encryption using Confused and Stream Cipher to Improved Medical Images Security *J. Phys. Conf. Ser.* **1201** 012022

[4] Kadhim O N and Hussain Z M 2018 Information Hiding using Chaotic-Address Steganography *J. Comput. Sci.* **14** 1247–66

[5] Alawida M, Samsudin A, Teh J Sen and Alkhawaldeh R S 2019 A new hybrid digital chaotic system with applications in image encryption *Signal Processing* **160** 45–58

[6] Suryadi M, Satria Y and Fauzi M 2018 Implementation of digital image encryption algorithm using logistic function and DNA encoding *J. Phys. Conf. Ser.* **974** 012028

[7] Singh K and Kaur K 2011 Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it *Int. J. Comput. Appl.* **23** 17–24

[8] Ahgue A O, De Nkapkop J D, Effa J Y, Franz S, Adelis P and Borda M 2018 A DNA-based chaos algorithm for an efficient image encryption application 2018 International Symposium on Electronics and Telecommunications (ISETC) (IEEE) pp 1–4

[9] Ahmed R K and Mohammed I J 2017 Developing a New Hybrid Cipher Algorithm using DNA and RC4 *Int. J. Adv. Comput. Sci. Appl.* **8** 171–6

[10] Setyaningsih E, Iswahyudi C and Widayastuti N 2012 Image Encryption on Mobile Phone using Super Encryption Algorithm *TELKOMNIKA (Telecommunication Comput. Electron. Control.)* **10** 815–24

[11] Pramanik S and Setua S K 2012 DNA cryptography 2012 7th International Conference on Electrical and Computer Engineering (Dhaka: IEEE) pp 551–4

[12] Zhang Y, Fu B and Zhang X 2012 DNA Cryptography Based on DNA Fragment Assembly (Jeju: IEEE)

[13] Zhang X and Cao Y 2014 A novel chaotic map and an improved chaos-based image encryption scheme. *ScientificWorldJournal.* **2014** 713541

[14] Kusuma E J, Sari C A, Rachmawanto E H and Setiadi D R I M 2018 A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography *J. ICT Res. Appl.* **12** 103

[15] Hore A and Ziou D 2010 Image Quality Metrics: PSNR vs. SSIM 2010 20th International Conference on Pattern Recognition (Istanbul: IEEE) pp 2366–9

[16] Tsai D-Y, Lee Y and Matsuyama E 2008 Information entropy measure for evaluation of image quality. *J. Digit. Imaging* **21** 338–47

[17] Wu Y, Noonan J P and Agaian S 2011 NPCR and UACI Randomness Tests for Image Encryption *Cyber Journals Multidiscip. Journals Sci. Technol. J. Sel. Areas Telecommun.* 31–8