

PIXIPHER : A Chaotic Maps and DNA Coding Based RGB Image CODEC Framework

Anmol Singh, Sunil Suthar, and Chiranjoy Chattopadhyay

Indian Institute of Technology Jodhpur

Abstract. Researchers in the field of DNA based chaotic cryptography have recently proposed a set of novel and efficient image encryption algorithms. In this paper, we present a comprehensive summary of those techniques, which are available in the literature. The discussion given in this paper is grouped into three main areas. At first, we give a brief sketch of the backbone architecture and the theoretical foundation of this field, based on which all the algorithms were proposed. Next, we briefly discuss the set of image encryption algorithms based on this architecture and categorized them as either encryption or cryptanalyzing techniques. Finally, we present the different evaluation metrics used to quantitatively measure the performance of such algorithms. We also discuss the characteristic differences among these algorithms.

Keywords: keyword1, keyword2

1 Introduction

Digital image has become the defacto standard from information sharing nowadays. Even though, we share a lot of information through that medium, images are vulnerable to illegal access from unauthorized users. Most importantly, for national security projects, health care, visual communication requires special attention. The primary goal of any digital image codec (encryption and decryption) is to fulfill this need of designing a highly secured system to prevent unauthorized use of digital images.

Since its inception [5], researchers have worked designing robust image codecs. Canonical approaches for image encryption fails in several scenarios. Recently, unconventional techniques are applied as a potential alternative for image encryption. Bio-Computing methods had been explored in the past for various other related task, including image encryption. Moreover, deep study of chaotic systems also paved the path for image encryption due the mixing property of a chaotic system is similar to the cryptographic property, which says that a small perturbation to the local area generates huge change in the entire space.

In general, an image encryption technique is divided into two stages: (i) confusion and (ii) diffusion. During the confusion stage, position of the image pixels are scrambled (changed) to make the original image unrecognizable. However, it has to be ensured that the original image can be obtained by performing the reverse

operations. Image pixels are scrambled by at first generating a pseudo-random sequence either using chaos maps or by random number generator. This sequence is used to change the pixel locations and thereby introduce confusion. The next stage is to encrypt the scrambled image, i.e. diffusion. In [3], a RGB image encryption algorithm based on DNA encoding combined with chaotic map is proposed aiming at characteristics of RGB image. A image encryption scheme based on DNA sequence addition operation and chaos was proposed in [1,7]. In [6], a Chaos Based Symmetric Key Encryption of RGB Color Images with DNA Coding and a Chaos based Pseudorandom Binary Number Generator (PRBNG) has been proposed. A proposal was given in [4], where the concept of DNA is being used in the encryption and decryption process with theoretical justification and implementation. In [2] a novel confusion and diffusion method for image encryption was proposed.

The key contributions of PIXIPHER are: (i) Encryption and Decryption of RGB images based on DNA sequence and using various chaotic maps, (ii) Quantitatively measuring performance of the algorithms using different evaluation metrics, (iii) Evaluating algorithm on other parameters such as Robustness, Reliability and Attack proof and cracking of Encrypted Image, (iv) Development a simple open-sourced client based application which can be used to send images directly to other client over the network.

2 Detail Description Of Pixipher

In this Phase Pixipher implemented some popular existing Encryption and Decryption Techniques and tried to observe behavior of these techniques using different chaotic maps and DNA coding techniques.

2.1 Background

Different Image Scrambling Maps

1. Arnold's Cat Map

Arnold Cat Map is used to scramble the image. Arnold mapping is one-to-one mapping, Therefore, there is one-to-one relationship between original image and scrambled image to avoid the coordinate position of conflict. Determinate of this map is 1 so the Arnold mapping is unique.

$$X_{n+1}Y_{n+1} = 1pqpq + 1X_nY_n \text{ Mod } N \quad (1)$$

Where (X_n, Y_n) is the pixel position of $N \times N$ given image, p, q are the parameters which are positive integers and $((X_{n+1}, Y_{n+1}))$ is the new position of the original pixel position (X_n, Y_n) when Arnold cat map is performed once. n is the total no. of iteration performed by map.

2. Pixel Position Shift In Both Horizontal and Vertical Direction (PPSHV)

PPSHV Method is used for scramble the image. PPSHV mapping is one-to-one mapping, Therefore, there is one-to-one relationship between original image and scrambled image to avoid the coordinate position of conflict. In this method pixipher shift pixels with a subsequent number in both horizontal and vertical direction. Complexity of this method is slower than Arnold's Cat Map.

3. Pixel Position Shift Using Binary Shift (PPSBS)

PPSBS Method is used for scramble the image. PPSBS mapping is one-to-one mapping, Therefore, there is one-to-one relationship between original image and scrambled image to avoid the coordinate position of conflict. In this method pixels position are shifted using binary Binary Shift. Complexity of this method is faster than both PPSHV and Arnold's Cat Map.

DNA Coding DNA Coding table is used to convert 8-bit binary number into DNA Sequence.

[HTML]C0C0C0 000	001	010	011	100	101	110	111
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

Table 1. Different Kinds of DNA-Binary Coding

Here in the table-1 4 bases (A,T,C,G) .Total 24 (4!) combinations possible but we are using only 8 such combination because of the complementary relationship between the bases.

Logistic Map The one-dimensional Logistic map is one of the simplest nonlinear chaotic discrete systems that exhibit chaotic behavior, defined as

$$Z_{n+1} = \mu_1 Z_n (1 - Z_n) \quad (2)$$

Where, Z_0 is initial condition with $Z_0 \in [0, 1]$, μ_1 is the system parameter with $\mu_1 \in (3.57, 4]$ and n is the number of iterations.

Pseudo-random Binary Number Generator A Pseudo Random Bit Generator (PRBG) based on two one-dimensional logistic maps run side-by-side and start from random independent initial conditions. The PRBG is based on two logistic maps,

$$X_{n+1} = \mu_1 X_n(1 - X_n) Y_{n+1} = \mu_1 Y_n(1 - Y_n) \quad (3)$$

starting from random independent initial conditions ($X_0, Y_0 \in (0, 1)$, and $X_0 \neq Y_0$), generates bit sequences by comparing the outputs of both the logistic maps as

$$g(X_{n+1}, Y_{n+1}) = \begin{cases} 1 & \text{if } X_{n+1} > Y_{n+1} \\ 0 & \text{if } X_{n+1} \leq Y_{n+1} \end{cases} \quad (4)$$

The set of initial conditions ($X_0, Y_0 \in (0, 1)$, and $X_0 \neq Y_0$) serves as the seed for the PRBG, if we supply the exactly same seed to the PRBG, it will produce the same bit sequence due to the above deterministic procedure.

2.2 Encryption Algorithm

1. First The Original RGB image is decomposed into its RGB components I^R, I^G, I^B . Size of the image is $N \times N$
2. Scramble each component of the plain image using the generalized Arnold Cat Map with given values of p, q and n . Consider the scrambled image at n th iteration to be $I_{scrambled}^R, I_{scrambled}^G, I_{scrambled}^B$
3. Consider $I_{scrambled}^R$ and convert each of its pixels into their 8-bit binary equivalent
4. A pseudo-random binary sequence of size $3 \times N \times N$ is generated with chosen value of the triplet (X_0, Y_0, μ) by the PRBNG, from which 3-bit disjoint and consecutive binary sequences are extracted to choose DNA coding rule as in the DNA Coding Table, and thus each 8-bit binary pixels are converted to their corresponding DNA codes producing DNA coded image $I_{DNA-Coded}^R$. This generates the first level of diffusion for the image component
5. Now use every third (X_n, Y_n) pair generated in Step 4 by the PRBG to decode the DNA coded image binary codes and then into pixel value $I_{DNA-Decoded}^R$. It is 2nd level of diffusion.
6. encryption keys, k_i are generated by the 1D logistic map with chosen value of (μ_1, Z_0) as

$$k_i^{temp} = Z_{n+1} = \mu_1 Z_n(1 - Z_n) k_i = \lfloor \text{mod}(10^{14} X k_i^{temp}, 256) \rfloor \forall i = 1, 2, 3, \dots, (N \times N) \quad (5)$$

7. Each decoded image pixel of $I_{DNA-Decoded}^R$ is encrypted with the key k_i generated in Step 6 to get the encrypted pixel $P_i^{encrypted-R}$.

$$P_i^{encrypted} = \text{Mod}(P_i^{Decoded} \oplus k_i, 256) \quad (6)$$

Where \oplus denotes the exclusive-OR operation

8. Continue Step 3 to 6 for the other components $I_{scrambled}^G, I_{scrambled}^B$ of the original image.
9. The final Encrypted image is generated by recombination of encrypted R,G,B components.

2.3 Decryption

The original image can successfully be recovered by applying the encryption algorithm in reverse order with the parameters p , q and n for generalized Arnold Cat Map for unscrambling the Encrypted image, the initial condition and system parameter for (μ_1, z_0) 1D Logistic map for key generation and the triplet (μ, X_0, Y_0) for pseudo-random binary number generation would be used during decryption which has to be transmitted through secure channel.

2.4 Local Image Encryption And Decryption

As the Image size is increases time complexity for encryption and decryption is also increases gradually so to prevent this Pixipher uses Different type of Encryption technique and call it Local Image Encryption. In local Image Encryption Image divided into sub-images and than do the encryption and decryption of sub-images because complexity for small size sub-images is very low so the whole complexity for a image is also reduces. We can see the time Complexity and performance Analysis of both technique in Section 7

3 Experimental Setup

3.1 Image Data-set

Pixipher perform Encryption and Decryption on different type and size of Images. Table 2 shows the number and size of experimental Images.

3*RGB Images	128 x 128	30
	256 x 256	65
	512 x 512	45
3*Grayscale Images	128 x 128	40
	256 x 256	35
	512 x 512	25

Table 2. Image Data-set for Encryption and Decryption

3.2 Quantitatively Measuring Performance of the Algorithms Using Different Evaluation Metrics

The primary characteristic of a good encryption algorithm is to make changes in the input image in such a manner that the difference between the pixel values of the original and the encrypted images maximizes. Moreover, the final encrypted

image must not reveal any of the features of the original image. Visual inspection is one way of measuring the difference between an original and encrypted image. However, it is not enough to quantitatively measure the differences and thus evaluation metrics are necessary.

Different evaluation metrics available in the literature to measure the performance of an image encryption algorithm using a combination of DNA computing and chaos theory. The metrics can be grouped into three sets, based on: (i) pixel properties, (ii) diffusion quality, and (iii) miscellaneous. In the following subsections we present the fundamental ideas behind each of these metrics.

Metric Based on Pixel Properties The set of metrics in this group evaluates the ability of the encryption algorithm to substitute the original image with an uncorrelated encrypted image. The different metrics under this category are:

1. **Histogram Deviation (HD)**

The HD measures the deviation between the original and the encrypted images. Higher the value of HD reflects better encryption accuracy, where d_i is the amplitude of the absolute difference at the i^{th} gray level.

$$HD = \left(d_0 + d_{255} + 2 \sum_{i=1}^{255} d_i \right) M \times N \quad (7)$$

2. **Correlation coefficient**

A convenient metric to measure the quality of any image encryption algorithm is the correlation coefficient between pixels at the same location in the original and the cipher images. It is desirable that the correlation coefficient value between the original and the encrypted image should be close to zero, indicating that the pair of images is uncorrelated. This ensures that the proposed algorithm is guarded against the pixel correlation statistical attack.

$$CC_{xy} = Cov(x, y) \sqrt{D(x)} \sqrt{D(y)} \quad (8)$$

Where: $D(x) = 1/L \sum_{i=1}^L \left(x_i - 1/L \sum_{j=1}^L x_j \right)^2$, x = Input Image, y = Encrypted Image, L = Number of pixels involved in the Calculation, $Cov(x, y) = 1/L \sum_{l=1}^L \left(x_l - 1/L \sum_{k=1}^L x_k \right) \left(y_l - 1/L \sum_{k=1}^L y_k \right)$

3. **Irregular deviation (ID)**

The irregular deviation (ID) measures the quality of encryption in terms of how much the deviation caused by encryption (on the encrypted image) is irregular. A difference image is calculated by calculating the absolute difference between the input and encrypted image. Histogram analysis is performed on this difference image. Lower value of ID indicates higher encryption accuracy.

$$ID = \sum_{i=0}^{255} |H(i) - M_H| M \times N \quad (9)$$

Where, M_H = Mean Value of Histogram, H = Histogram of the difference Image.

4. **Histogram Uniformity (HU)**

Suppose H_1 be the histogram of the input image and H_2 be the histogram of the encrypted image. Then, H_2 should have the following characteristics: (i) H_2 should be totally different from H_1 , and (ii) H_2 must have a uniform distribution.

Metric based on diffusion quality The set of metrics in this group evaluates the efficiency of the diffusion mechanism. Different metrics in this category are:

1. **Avalanche effect (AE)**

Suppose, a single bit is altered in the original input image I . The resultant image is denoted by I_0 . Now, both I and I_0 are encrypted to give I_E and I_{E0} . The AE metric measures the percentage of different bits between I_E and I_{E0} . An encryption algorithm is said to possess good diffusion characteristics if there exist a 50 percent difference in the bits of I_E and I_{E0} .

2. **Unified Average Change in Intensity (UACI)**

It measures the average intensity of differences between the two images. Like NPCR, higher value of UACI indicates better encryption.

$$UACI = 1MN \left[\sum_{i=1}^M \sum_{j=1}^N C_1(i, j) - C_2(i, j) 255 \right] \times 100\% \quad (10)$$

Where, C_k = Encrypted Images, $k = \{1, 2\}$.

3. **Number of Pixel Change Rate (NPCR)**

The NPCR measures the percentage of different pixels in the two images. Higher the value of NPCR, better is the encryption algorithm.

$$NPCR = \sum_{i=1}^M \sum_{j=1}^N D(i, j) MN \times 100\% \quad (11)$$

Miscellaneous Metrics Members of this category of metrics is used to measure the encryption quality based on a combination of the above mentioned categories.

1. **Key sensitivity and key space analysis**

One of the significant characteristics of chaotic sequence is having a large key space and high sensitivity to initial conditions. A small change in one or more than one of the values of the input parameters will cause a huge change at the output.

2. **Peak Signal to Noise Ration (PSNR)**

This metric measures the robustness of the image encryption algorithm in the presence of noise. PSNR measures the ratio between the maximum possible power of a signal and the power of corrupting noise. Due to the varied

dynamic range of different signals, PSNR is usually expressed in terms of the logarithmic decibel scale.

$$PSNR = 10 \times \log_{10} \left[M \times N \times 255^2 \sum_{m=1}^M \sum_{n=1}^N |f(m, n) - f_d(m, n)|^2 \right] \quad (12)$$

Where, $f(m, n)$ = Original Image, $f_d(m, n)$ = Encrypted Image.

3. Information Entropy (IE)

The information entropy is reacts the degree of uncertainties in the system. The information entropy measures the distribution of gray value in the image. The greater information entropy the more uniform of the distribution of gray value.

$$IE = \sum_{i=0}^{2^J-1} [p(S_i) \cdot \log_2 1/p(S_i)] \quad (13)$$

Where, $p(S_i)$ = Probability of the Symbol S_i , $2^J = 256$.

4. Computation Time

Apart from the security consideration, running speed of the algorithm is also an important aspect for a good encryption algorithm. The processing time is the time required to encrypt and decrypt an image. The smaller value the processing time has, the better the encryption efficiency will be.

4 Results

The experiments have been performed using Matlab 14 with different RGB and Grayscale images. Pixipher plot Encrypted and Decrypted images with Performance Evaluation Metrics.

4.1 Qualitative Analysis

Fig -1 shows the flow chart of Existing Encryption and Decryption Technique and Fig-3 shows the flow chart of local image encryption technique. Encrypted image from both technique can't describe that which one is used but in scramble image we can see the difference between both technique.

Fig- ?? shows decryption of an image using different decryption keys. Image ?? shows that If all the decryption parameters are same as encryption parameter than decrypted images is same as original i.e it will decrypt correctly. Image ?? shows that if Arnold cat map's key is changed than decryption image is not as original but the histogram of decrypted image is same as original image it means that decrypted image is same as original only pixels are scrambled. Image ?? and ?? shows if decryption key or all parameters are changed than decrypted image is not same as original in other word it further encrypted.

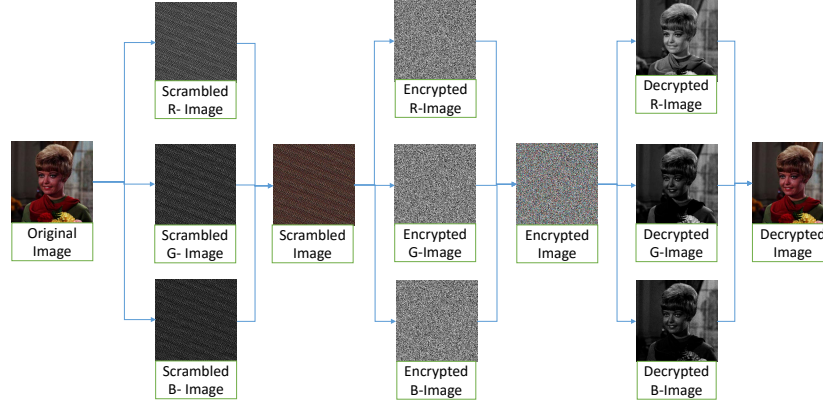


Fig. 1. Simple Image Encryption and Decryption Flow Chart of a RGB Image

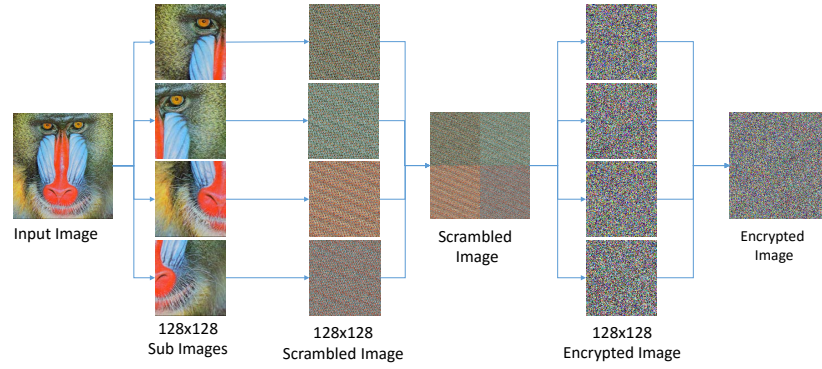


Fig. 2. Local Image Encryption Flow Chart of a RGB Image using Arnold Cat Map For Scrambling

4.2 Quantitative Analysis

The primary characteristic of a good encryption algorithm is to make changes in the input image in such a manner that the difference between the pixel values of the original and the encrypted images maximizes. Moreover, the final encrypted image must not reveal any of the features of the original image. Visual inspection is one way of measuring the difference between an original and encrypted image. However, it is not enough to quantitatively measure the differences and thus evaluation metrics are necessary. As we earlier see that different evaluation metrics available in the literature to measure the performance of an image encryption algorithm using a combination of DNA computing and chaos theory. Here some of evaluation metrics are used to find some Quantitative analysis.

In Fig. 4 different quantitatively measure are performed on different RGB (3 rows for R, G, B) and Grayscale Images and results are shown

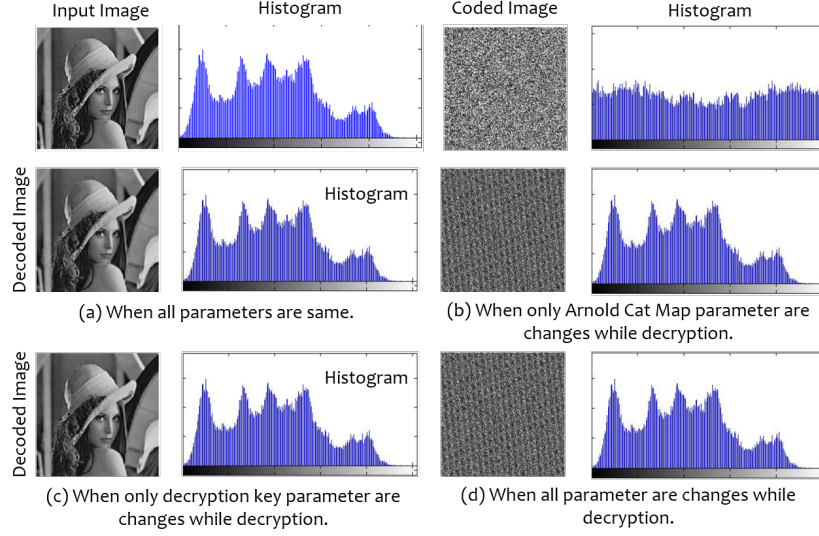


Fig. 3. Local Image Encryption Flow Chart of a RGB Image using Arnold Cat Map For Scrambling

4.3 Signature generation of Images

An images identity can be checked by producing the image signature. We generated the signature by using Existing SHA family of algorithm. Considered initial 10x10 pixel values (can be set as needed) and applied the SHA technique.

4.4 Performance Analysis

Apart from the security consideration, running speed of the algorithm is also an important aspect for a good encryption algorithm. The performance analysis is the time required to encrypt and decrypt an image. The smaller value the processing time has, the better encryption efficiency will be. Table 3 shows processing time for both techniques on different systems. As we can clearly see that Local image encryption techniques performance is way better that existing technique, as the image size is increases.

5 Conclusion

The algorithm was implemented with two major versions. In first version the image was encrypted as whole while the other version divided image into smaller parts. Computation time while encrypting images with sub-division method takes very less time than the normal method. Quantitative Metrics after encryption with sub-division method were either better or same as compared to normal method. Pixipher tool can encrypt/decrypt images with given parameters and can send images over network also.






Images	MO	ME	HD	CC	UACI	NPCR	PSNR	IE (O)	IE (E)
	143.1502 116.8219 106.9607	127.6975 127.3001 126.9125	0.998048 0.998125 0.997978	0.002216 0.003145 -0.00059	30.3031 31.4493 33.5639	99.6096 99.6122 99.5956	8.65281 8.30894 7.72693	7.6571 7.7560 7.8420	7.99780 7.99772 7.99762
	137.3913 128.8587 113.1171	127.3128 127.4455 127.04581	0.99797 0.99811 0.99803	0.00457 0.00447 0.00608	29.9572 28.5697 31.1240	99.5941 99.6219 99.6078	8.7712 9.2501 8.3931	7.70667 7.47443 7.75221	7.99921 7.99931 7.99932
	177.5769 177.8524 190.2139	127.4368 127.4046 127.4344	0.99816 0.99812 0.99806	-0.00035 -0.00095 -0.00288	31.9876 33.1457 32.7700	99.6326 99.6242 99.6135	8.1569 7.8416 7.9416	6.71776 6.79897 6.21377	7.99915 7.99909 7.99901
	225.9149	128.42753	1.000039	-0.0006127	48.4649	99.7406	4.96686	1.54831	7.996463
	123.1771	127.2408	0.99813	-0.00158	27.5555	99.6234	9.6313	7.20100	7.99920

Fig. 4. Signatures of Encryption and Decryption Images Generated using SHA-160 Algorithm

Approach	System	128 × 128	256 × 256	512 × 512	1024 × 1024
Global	4 GB RAM	20	180	1800	-
	16 GB RAM	7	75	540	4200
Local	4 GB RAM	20	84	300	1200
	16 GB RAM	7	30	120	480

Table 3. Computation time, for Encryption and Decryption of different size images with respect to different systems and different Technique

References

1. A novel color image encryption algorithm based on {DNA} sequence operation and hyper-chaotic system. *Journal of Systems and Software* 85(2), 290 – 299 (2012)
2. Liu, H., Wang, X., kadir, A.: Image encryption using {DNA} complementary rule and chaotic maps. *Applied Soft Computing* 12(5), 1457 – 1466 (2012)
3. Liu, L., Zhang, Q., Wei, X.: A {RGB} image encryption algorithm based on {DNA} encoding and chaos map. *Computers Electrical Engineering* 38(5), 1240 – 1248 (2012)
4. Roy, B., Rakshit, G., Singha, P., Majumder, A., Datta, D.: An improved symmetric key cryptography with dna based strong cipher. In: *2011 International Conference on Devices and Communications (ICDeCom)*. pp. 1–5 (2011)
5. Shannon, C.E.: Communication theory of secrecy systems. *The Bell system technical journal* 28(4), 656–715 (1949)
6. Som, S., Kotal, A., Chatterjee, A., Dey, S., Palit, S.: A colour image encryption based on dna coding and chaotic sequences. In: *International Conference on Emerging Trends and Applications in Computer Science*. pp. 108–114 (2013)
7. Zhang, Q., Guo, L., Wei, X.: Image encryption using dna addition combining with chaotic maps. *Mathematical and Computer Modelling* 52(11), 2028 – 2035 (2010)