An Uncompressed Image Encryption Algorithm Based on DNA Sequences

Shima Ramesh Maniyath[1] and Supriya M[2]

Department of Computer Science & Engineering,
Amrita Vishwa Vidyapeetham ,School Of Engineering, Bangalore Campus, India
ramesh.shima86@gmail.com
m_supriya@blr.amrita.edu

ABSTRACT

The rapid growth of the Internet and digitized content made image and video distribution simpler. Hence the need for image and video data protection is on the rise. In this paper, we propose a secure and computationally feasible image and video encryption/decryption algorithm based on DNA sequences. The main purpose of this algorithm is to reduce the big image encryption time. This algorithm is implemented by using the natural DNA sequences as main keys. The first part is the process of pixel scrambling. The original image is confused in the light of the scrambling sequence which is generated by the DNA sequence. The second part is the process of pixel replacement. The pixel gray values of the new image and the one of the three encryption templates generated by the other DNA sequence are XORed bit-by-bit in turn. The main scope of this paper is to propose an extension of this algorithm to videos and making it secure using modern Biological technology. A security analysis for the proposed system is performed and presented.

.

KEYWORDS

Arnold cat map, image encryption, DNA sequences, big image

1. INTRODUCTION

ENCRYPTION is a common technique to uphold image security. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication. To achieve the above purpose researchers look for more secure cryptography incessantly [I]. Since the vast parallelism, exceptional energy efficiency and extraordinary information density is inherent in DNA molecules, DNA cryptography [2,3] is a new born one has become an important direction. DNA cryptography benefits from the research of DNA computing, but the DNA computing is not equal to DNA cryptography, and there is the essential difference between them. In DNA computing, DNA technology is used to solve difficult computational problems. While in DNA cryptography, different difficult biological problems are used as the security basis of DNA cryptosystems. The processes of cryptography can be regarded as computation. But not all DNA computations relate to cryptography.

In recent years, as the rapid development of the social and technology of science, produce a large amount of data calculation and NP problem. But DNA computer has excellent characteristics to

D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, pp. 258–270, 2011.

DOI: 10.5121/csit.2011.1224

solve these problems (such as, efficient parallel and mass storage capacity). In 1994, Dr Adleman solve directed Hamilton path problem by DNA computing [4], expand the study area. DNA encryption [5] [6] is the forefront field of DNA computing. Different from traditional encryption methods,

Digital image is a massive two-dimensional data. The smallest unit of an image is a pixel. In a digital image, each pixel represents a different level of colour intensity. According to the capacity of human visual perception in distinguishing different levels of intensity, the entire range of intensity is divided into 256 levels. Thus, the level of intensity in each pixel has a value between 0 and 255. This range is demonstrated by a byte (8 bits). Therefore, each pixel is equal to one byte. However, due to large data size and real time requirement, it is not reasonable to use conventional encryption methods. Thus, a major recent trend is to minimize the computational requirements for secure multimedia distribution. There are a number of encryption algorithms available such as DES, AES, International Data Encryption Algorithm (IDEA) and RSA (developed by Rivest, Shamir and Adleman).These traditional encryption algorithms have shortcomings and they are not considered as ideal for image applications, mainly because of low level of efficiency when dealing with large and redundant blocks of image data. Moreover, these algorithms require more than the usual expected computation time and power while performing image encryption.

2. Related Works

An image encryption algorithm based on DNA sequences for the big image is presented in this paper. We don't use DNA biological operation to implement image encryption, yet the first DNA sequence is used to generate the scrambling sequence to accomplish pixel scrambling using Arnold cat map, and the second DNA sequence is used to generate the three DNA templates to accomplish pixel replacement. This algorithm is further fit for encrypting the big image as a result of its principle. Moreover we are extending this Algorithm for videos in order to prove that our image Encryption Algorithm is efficient. Since the main keys are the natural DNA sequences, this algorithm has higher security and is robust against all kinds of attacks.

In this paper Section 3 talks about algorithm for image encryption and Section 4 extension of this algorithm to videos, Section 5, Experimental Results, Section 6, Algorithm Performance Analysis and Section 7, Cryptanalysis.

3. Image Encryption Algorithm

3.1. The Introduction of Algorithm

Although a lot of more mature encryption algorithms have been proposed, they are hardly fit for encrypting the big image. In the practice, there are many big images that need to be transmitted through an Internet which could not be compressed arbitrarily, such as the map (bmp). If it is compressed, a lot of important information will be incapable of identification. So an image encryption algorithm for the big image that owns the low encryption time and the high security is necessary.

3.2. Arnold Cat Map

Arnold cat map [8] is a typical chaotic map, it is a discrete system that stretches and folds its trajectories in phase space. Vladimir Arnold discovered the ACM in the 1960s and he used the image of a cat while working on it, its expression is as in (1).

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(N) \qquad (1)$$

Where x_n, y_n are the pixel position of $N \times N$ image, a, b are the parameters which are positive integers. The (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. The period T of the Arnold cat map depends on the parameters a, b and the size N of the original image. The determinant [11] value is 1, so cat map is a map which keeping area (no attractor). At the same time, the cat map is one-to-one mapping [9]; each point in matrix can be transformed to another point uniquely. Cat map can replace the position of the image pixel points in order to get the purpose of encryption. For the same image, the iterative times are different [12] when the value of a and b are different. So Image can be scrambled via keeping the value of a, b secret After iterating m (m > 1) times, the correlation among the adjacent pixels can be disturbed completely.

Table 1
Iterative Period

a **b**	**a=1** **b=1**	**a=1** **b=4**	**a=4** **b=6**	**a=8** **b=14**	**a=20** **b=12**	**a=28** **b=28**	**a=30** **b=40**
Period	**192**	**256**	**128**	**128**	**64**	**64**	**128**

Through the table.1 we can see that the different a, b value will generate different period of repeating the original image.

3.3. The Flow of the Encryption Algorithm

In this paper, the original image is confused by Arnold Cat Map, for that frequency value is generated by using the natural DNA sequence. Then, the new image and the three DNA templates that are generated according to the other DNA sequence are XORed in turn. Fig.1 is the flow chart of this algorithm. The image encryption algorithm [1] is as follow:

Step1: Input the original image A_0 is N×N in size, where N and N are rows and columns of the image respectively.
Step2: Gain the image A_1 by confusing the original Image A_0 in the light of the scrambling sequence which is gained according to the first natural DNA sequence, followed by Arnold Scrambling

Step3: The DNA template B_1 is generated by the second DNA sequence. Then, the DNA template B_1 and the image A_1 are XORed, and the image A_2 is generated. In this algorithm, we design that a gray value is made up of four bases. One base represents two binary digits, in which A, C, G and T are replaced by 00, 01, 10 and 11.

Step4: According to Fig.2 (b) and Step3, the DNA template B_2 is generated by the DNA template B_1 and the image A_2 are XORed, and the image A_3 is generated.
Step5: According to Fig.2 (c) and Step3, the DNA template B_3 is generated by the DNA template B_2 and the image A_3 are XORed, and the image A_4 is generated.
Step6: Gain the encrypted image A^1, where $A^1 = A_4$.

According to Step 3, we are using DNA Digital Coding Technology [1] for coding the DNA sequences into a binary stream. For any pixel, the range of its gray value is 0- 255, namely 00000000-11111111. We use four bases instead of a gray value, in which 00, 01, 10 and 11 are replaced by A, T, C and G.

Table 2
DNA Digital Coding

DNA Bases	Binary Value
A	00
T	01
C	10
G	11

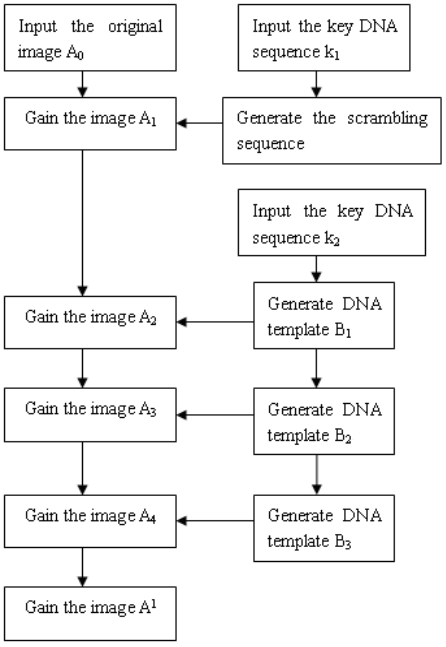


Figure 1 The Flow Chart

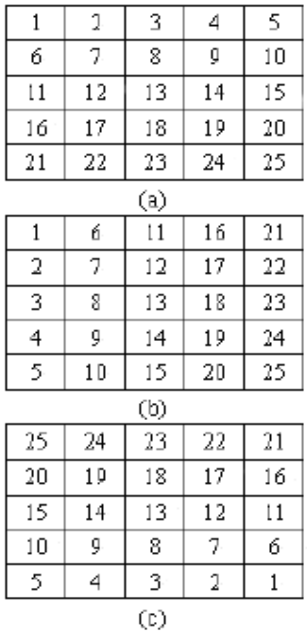


Figure 2 The Matrices of the Location

4. Extension of Secure Algorithm to Videos

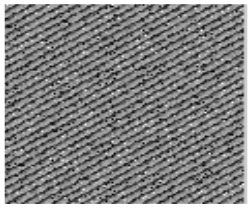
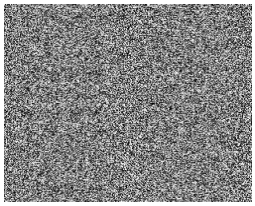
A video consists of single frames which are temporally ordered one after the other. A single video frame may again consist of several frames. Since the number of frames in a video is large, we need a scrambling method that takes less time.

The native approach for video encryption is to treat video data as text and encrypt it using standard encryption algorithms like AES (Advanced Encryption Standard) or DES (Data Encryption Standard). The basic problem [10] with these encryption algorithms is that they have high encryption time. They also result in vast increase in size of the video, making them unsuitable for real-time applications like PAY-TV, Pay-Per View and Video on Demand (VOD) etc. A unique characteristic of video data is that, even though information rate is very high, information value is very low


(a) Xylophone (141) (b) boat (149)

Fig 3 Example for Test Videos along with Frame Numbers

The test videos are shown in Figure 3 along with the frame number. The results of scrambling and XORing the test videos are shown in Figure 4 Visual details in the video are almost lost after the first step of encryption, but still a very low-quality image can be seen. The details are completely lost after XORing the Scrambled videos.

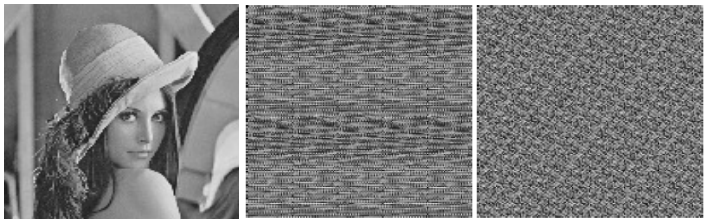



(a)Scrambled Frame (b) Encrypted Frame

Fig. 4. Frames from Encrypted Test Videos

5. Experimental Results

In this paper, we select the classical image of 256×256 Lena.bmp with 256 gray levels as the original image and adopt the discretized Arnold cat map to be the encryption algorithm. We use Matlab 2010 to simulate the experiment. Make the parameter in the Arnold cat secret, the images which are iterated 33 times and 21 times in a period are showed as figure 5(b) and figure5(c) The number of times may be selected according to visual effect. From the figure, we can see the result of 21 times is better than the 33 times. The image iterative quality is also different to the same size image. Through the cat map, it realizes the scrambling and attains the purpose of encryption. Its safety mainly is to keep the secret of the parameters and the iteration times, but the attacker can also attract through the method of statistics analysis and exhaustion. So we still need to change the pixel value to encrypt further.

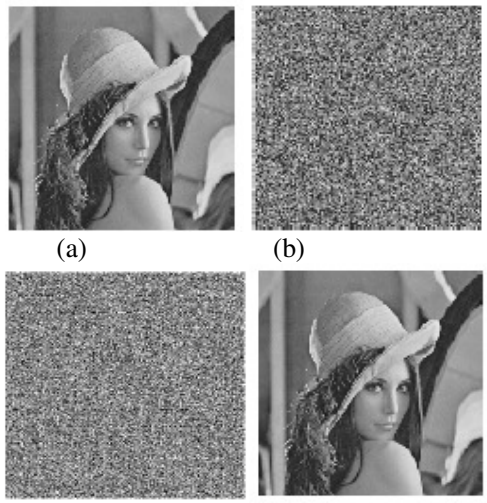


a. Original image b. Scrambled images (33 & 21 times)

Figure 5.The scrambling results of cat map.

Fig.6 in the experimental result shows the encrypted image and decrypted image. Fig.6 (a) shows the original image and Fig.6 (b) is the scrambled image gained by the Arnold scrambling process. Fig.6(c) is the encrypted image that is different from the original image absolutely. The encryption processes contain three XOR operations. The decryption processes are similar to the encryption ones. If and only if the true keys are obtained, the encrypted image is executed on the

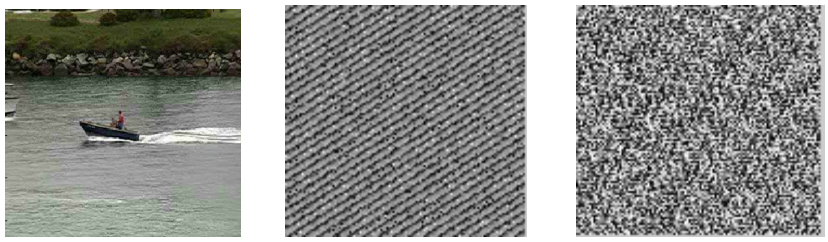
basis of the decryption algorithm and the decrypted image Fig.6 (d) is gained. From the experimental results, the image encryption algorithm is feasible and satisfactory.



(a) (b)

(c) (d)

Figure. 6 Experimental Results for an image



Frame1 Scrambled Frame Encrypted Frame

Figure 7 Video Encryption using the proposed algorithm

Here every frame of the video is taken one after the other in order and the pixels of each frame is taken as the input to the encryption algorithm. Results obtained on encrypting frames of video after scrambling are shown in Figure 7.

6. Algorithm Performance Analysis

An image encryption algorithm is satisfactory only when it is robust against all kinds of cryptanalytic, statistical and brute-force attacks. Here, some security analysis has been performed on the proposed one, including some important ones like key space analysis, statistical analysis, etc. The security analysis demonstrates that the algorithm owns the high security.

6.1. Key's Security Analysis

A large key space is very important; since we must be assumed that everything is known by the attacker except the keys in the light of the hypothesis is proposed by Kirchhoff. So it could repel the exhaustive attacks only when the key space is large enough. In this paper, we use the natural DNA sequences as main keys. In the nature, DNA sequences are various, and the length has the

considerable difference. In case of the same DNA sequence, since the difference of the length and the initial position, a segment is quite different from others. Therefore, the key space is large enough to resist exhaustive attacks.

In order to further analyze sensitivity, we test the algorithm under the wrong decryption keys. An efficient encryption algorithm should be sensitive to secret key i.e. a small change in secret key during decryption process results into a completely different decrypted image. So here we are using two keys for image encryption, one is for scrambling the input image. The second key is the DNA sequence, which will be different for different persons.

In this we made a change in single bit of the secret key, which was used to control pseudorandom generation of DNA sequence used for scrambling the original image by Arnold cat map. Again we test the algorithm with different DNA sequences for decrypting.

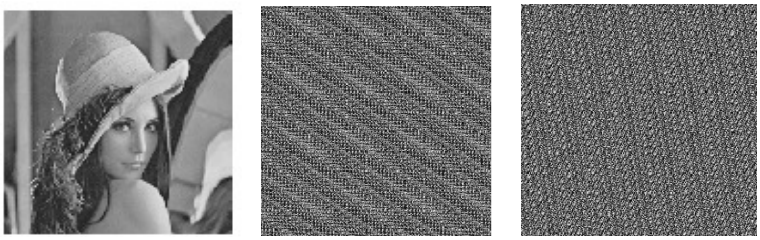


Figure 8 Decrypted images using Wrong Keys for scrambling

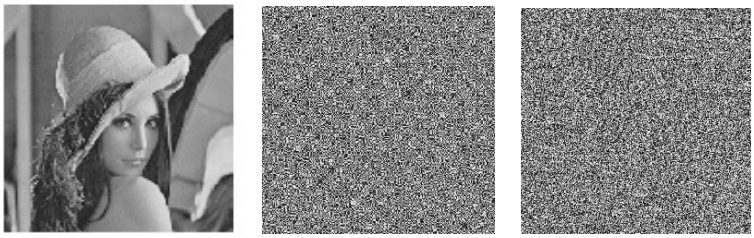
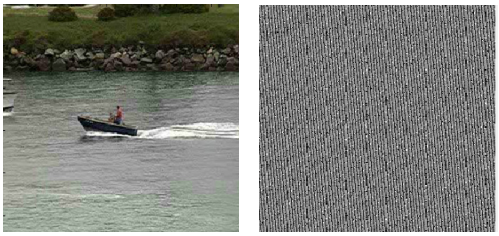


Figure 9 The Decrypted images using Wrong DNA Keys



(a) (b)

Figure.10 Key Sensitivity Test for videos: (a) shows the decrypted frames using correct key and (b) shows the decrypted frames using wrong key

6.2 A Key's Sensitivity Analysis

Testing the key sensitivity of the proposed image encryption procedure, we have performed the following method. Assume that the encryption key used is k0, first, a 256×256 Lena plain-image is scrambled by using the test key and the resultant encrypted image is obtained .Next, the same plain image is again scrambled and encrypted with four slightly different keys described in Table 2. In order to see the influence of changing a single pixel in the original image on the encrypted image with the proposed algorithm distinctly, we have also introduced the number of pixels change rate (NPCR). The NPCR measure the percentage of different pixel numbers between the two images. The NPCR is defined as follows:

$$NPCR = (1 - \frac{\sum_{ij} D(i,j)}{wh}) \times 100\%$$

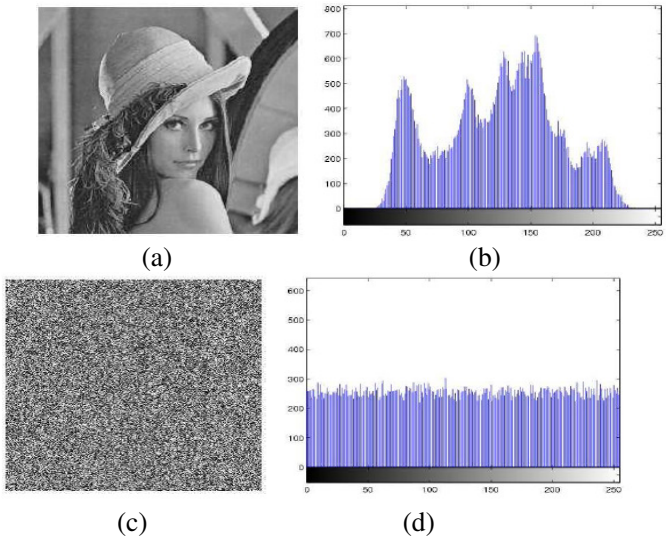
Where D is a two-dimensional array. For two encrypted images of the same original image with two different keys $C_1(i,j)$ and $C_2(i,j)$, D(i,j) is determined from $C_1(i,j)$ and $C_2(i,j)$, if $C_1(i,j) = C_2(i,j)$,then D(i,j)=1 otherwise D(i,j)=O. In Table 3 we have given the results of NPCR with different keys in the proposed scheme. From table 3, we can easily find that although there is a slight difference between two keys, the change rates are higher; NPCR are over 99%. It means that the proposed encryption scheme is very sensitive with respect to small changes in keys

Table 3
NPCR Results

Test item	Test result between images scrambled with tiny changes in the key			
	K1	K2	K3	K4
NPCR (%)	99.85	99	99.9	99.78

6.3 The Gray Histogram Analysis

An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each colour intensity level. We compare the gray histograms of the lena.bmp before and after encryption (Fig.11) to analyze the statistical performance, and we can see that the gray histogram of the encrypted image (Fig.11 (d)) is fairly uniform and significantly different from the one of the original image (Fig.11 (b)).



(a) (b)

(c) (d)

Fig.11 Histograms of the plain-image and the encrypted image

This shows that the encrypted image doesn't provide any information regarding the distribution of gray values to the attacker. Hence, the proposed algorithm can resist any type of histogram based attacks and strengthen the security of encrypted images significantly.

6.4 Correlation Coefficient Analysis

In the proposed algorithm, the correlation coefficient Analysis of 1000 randomly selected pairs of vertically, horizontally adjacent pixels is determined. In most of the plain-images, there exists high correlation among adjacent pixels, while there is a little correlation between neighbouring pixels in the encrypted image. It is mainstream task of an efficient image encryption algorithm to eliminate the correlation of pixels. Two highly uncorrelated sequences have approximately zero correlation coefficient. Then the correlation coefficient is calculated. Correlation coefficient can be given by:

$$C_r = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{(N\sum_{j=1}^{N} x_j^{\,2} - (\sum_{j=1}^{N} x_j)^2) \times (N\sum_{j=1}^{N} y_j^{\,2} - (\sum_{j=1}^{N} y_j)^2)}}$$

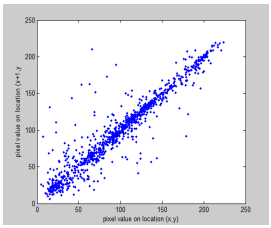
Where x and y are the gray-scale values of two adjacent pixels in the image and N is total number of pixels selected from the image for the calculation.

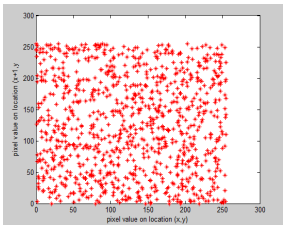
Table 4 Correlation analysis

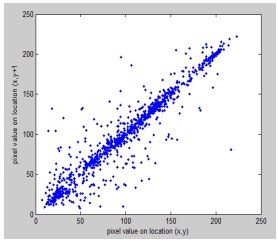
Adjacent Pixels	Correlation coefficients	
	Original image Fig 10(a)	Encrypted image Fig 10(b)
Horizontal	0.9489	-0.0041
Vertical	0.9473	-0.0089

An extensive study of the correlation between image and its corresponding encrypted image by using the proposed encryption algorithm is also done and the following results obtained are shown in table 4.

So here we have depicted the distributions of two horizontally and vertically adjacent pixels in the original and encrypted images. It is clear from the Fig. 12 and Table 4 that there is negligible correlation between the two adjacent pixels in the encrypted image. However, the two adjacent pixels in the original image are highly correlated.


(a)


(b)


(c)

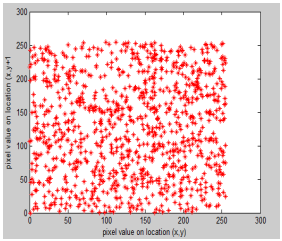

(d)

Figure .12 Correlations of two adjacent pixels: Fig (a) and (b), show the distribution of two horizontally adjacent pixels and Fig (c) and (d), show the distribution of two vertically adjacent pixels in the plain and encrypted images shown in Fig. 11 (a) and Fig. 11(c).

6.5 Encryption speed analysis

The main purpose of this algorithm is to reduce the big image encryption time. For images of different sizes, we have recorded the time taken by our algorithm to perform the encryption, decryption, scrambling and descrambling of images.

Table 5. Time analysis of the algorithm for image

Image size (in pixels)	Key Generation (s)	Scrambling (s)	Encryption (s)	Decryption (s)	Descrambling (s)
256×256	0.009	0.001	1.07	2.04	0.01
512×512	0.011	0.004	1.1	2.1	0.07
1024×1024	0.015	0.012	1.5	2.25	0.12

Table 6 .Time analysis of the algorithm for video per frame

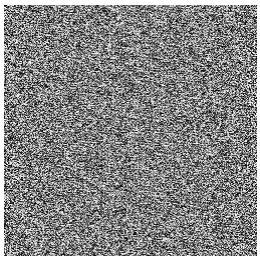
Frame size	No of Frames	Key Generation (s)	Encryption (s)	Decryption (s)
288×352	149	0.004	1.02	2.05
288×384	183	0.06	1.02	2.06
240×352	299	0.042	1.009	1.85
512×512	49	0.078	1.1	2.22

7. Cryptanalysis

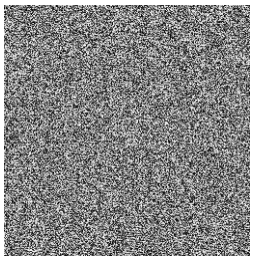
7.1 Known-Plaintext and chosen plaintext attacks

Chosen/Known-plain text attacks are such attacks [13] in which one can access/choose a set of plain texts and observe the corresponding cipher texts. In today's networked world, such attacks occur more and more frequently. For a cipher with a higher level of security, the security against both known-plaintext and chosen-plaintext attacks are required. Apparently, even when the secret key is changed for each plaintext, these methods are insecure against chosen/known-plaintext attacks. The mask image I_m is obtained by simply XOR-ing the plain image I with its corresponding cipher image I'. XOR-ing the mask I_m with unknown cipher image J', obtained by encrypting J by the same key. If we get the unknown plain image J then the algorithm fails in Chosen/Known-plaintext attack, otherwise the algorithm safe against Chosen/Known-plaintext attack. Fig.13 demonstrates an unsuccessful chosen/known-plain text attack in the proposed algorithm.

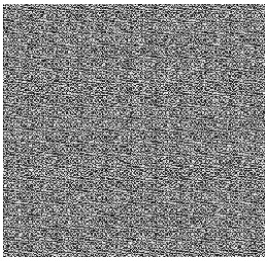
(a) Lena



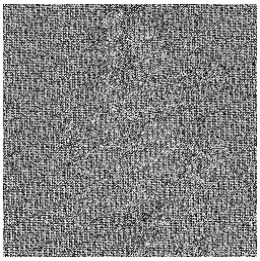
(b) Encrypted Lena



(c) XOR mask



(d) Unknown Cipher Text



(e) Failed attempt to crack the Unknown Cipher text

Fig.13 Unsuccessful chosen/Known-plaintext attack on proposed algorithm

7.2 Differential Attack

Attacker tries to find out a relationship between the plain image and the cipher-image, by studying how differences in an input can affect the resultant difference at the output in an attempt to derive the key. Trying to make a slight change such as modifying one pixel of the plain image, attacker observes the change of the cipher-image. To test the influence of one pixel change on the whole encrypted image by the proposed algorithm, two common measures are used: NPCR & UACI means the number of pixels change rate of ciphered image while one pixel of plain-image is changed. UACI which is the unified average changing intensity, measures the average intensity of the differences between the plain-image and ciphered image.

1) Number of Pixels Change Rate (NPCR)

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%,$$

2) Unified Average Changing Intensity (UACI)

$$\mathrm{UACI} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\%,$$

C_1 and C_2: two ciphered images, whose corresponding original images have only one-pixel difference. C_1 and C_2 have the same size. C_1 (i, j) and C_2 (i, j): grey-scale values of the pixels at grid (i,j). D(i, j): determined by C_1 (i, j) and C_2 (i, j), if C_1 (i, j) = C_2 (i, j), then, D(i, j) = 1; otherwise, D(i, j) = 0. Wand H: columns and rows of the image.

Tests have been performed on the proposed scheme on a 256-level gray scale image of size 256×256 shown in Fig. 13(a). The NPCR and UACI test results are shown in table 6. Results obtained from NPCR show that the encryption scheme's sensitivity to small changes in the input image is under 0.01%. The UACI estimation result shows that the rate influence due to one pixel change is very low.

The results demonstrate that a swiftly change in the original image will result in a negligible change in the ciphered image. So the proposed algorithm is highly resistive against differential attack.

Table .7 NPCR and UACI of proposed method

NPCR	UACI
0.0015%	0.004%

8. Conclusions

This paper presents an image encryption algorithm for the big image that is to use the DNA sequences to generate the scrambling sequence and encryption template so that the encryption time of the big image is reduced to a great extent. The main keys are the natural DNA sequences in this paper, so the key space is large enough to resist exhaustive attacks. The analysis demonstrates that the image encryption algorithm is efficient and highly secure. All parts of the proposed encryption system were simulated using MATLAB. Correlation analysis showed that correlation coefficients between adjacent pixels in the plain-image are significantly decreased after applying encryption function. To quantify the difference between encrypted image and corresponding plain-image, two measures were used: NPCR and UACI. The scheme can resist most known attacks, such as statistical analysis and brute-force attacks. All the experimental analyses show that the proposed encryption algorithm:
(i) has high level of security with less computation; (ii) is highly robust towards cryptanalysis; and (iii) can be applied practically for the protection of digital images over open channels

9. ACKNOWLEDGEMENTS

We authors would like to convey our sincere gratitude to Amrita School of Engineering, Bangalore for providing a congenial working environment and constant support in completing our project.

10. REFERENCES

[1] Shihua Zhou, Qiang Zhang, Xiaopeng Wei ‘Image Encryption Algorithm Based on DNA Sequences for the Big Image’2010 International Conference on Multimedia Information Networking and Security

[2] G. Z. Xiao, M. X. Lu, L. Qin and X. 1. Lai, "New Field of Cryptography: DNA Cryptography" Chinese Science Bulletin, vol. 51, pp.1413-1420, 2006.

[3] A.Leier, C. Richter, W. Banzhaf and H. Rauhe, "Cryptography with DNA Binary Strands" Bio Systems, vol. 57, pp.13-22, 2000.

[4] D. Heider and A. Bamekow, "DNA-based Watennarks Using the DNA-Crypt Algorithm" BMC Bioinfonnatics, vol. 8, pp.176-185, 2007.

[5] L. Adleman, "Molecular Computation of Solutions to Combinatorial problems," Science, vol. 226, pp. 1021-024, Nov. 1994

[6] G. cui, L. Qin, "Information Security Technology Based on DNA Computing", IEEE International, 2007

[7] G. Xiao, M. Lu, L. Qin, X. Lai, " New field of cryptography: DNA cryptography," Chinest Science Bulletin, vol. 51(\0), pp. 1139-1144, Jun. 2006.

[8] Chen G R, Mao Y B and Chui C K. "A symmetric image encryption scheme based on 3D chaotic cat maps". *Chao s, Solutions and Fractals*,.vol. 21, pp. 749-761, 20

[9] Yuanzhi Wang , Guangyong Ren, Julang Jiang , Jian Zhang, Lijuan Sun, "Image Encryption Method Based on Chaotic Map" 2007 IEEE

[10] Rustam Rakhimov Igorevich, Hanmaro Yong, Dugki Min, Eunmi Choi, "A Study on Multimedia Security Systems in Video Encryption"

[11] Peizhen WANG, Huixin GAO, Mutian CHENG, Xiaosan MA, 'A New Image Encryption Algorithm Based on Hyper chaotic Mapping', *2010 International Conference on Computer Application and System Modelling*

[12] D. Chattopadhyay, M. K. Mandal1 and D. Nandi,' Symmetric key chaotic image encryption using circle map', Indian Journal of Science and Technology.

[13] *Shujun Li, Xian Zheng* **"**CRYPTANALYSIS OF A CHAOTIC IMAGE ENCRYPTION METHOD"

Author Profiles:

Shima Ramesh Maniyath received the Bachelor's Degree in Electronics and Communication Engine ering from Kannur University, in 2009 and Master's Degree in Embedded System Design from Amrita School of Engineering, Bangalore in 2011.Research Interest includes: Cryptography, Network Security, Image Processing.

Supriya M received Bachelor's degree in Computer Science and Engineering in Tamil Nadu College of Engineering under Bharathiyar University in 1999 and Master's Degree in Computer Science Engineering under Dr. M.G.R University. She is pursuing PhD in Security under the Topic Distributed Storage. Research interest includes: Compiler Design, Cryptography, Operating Systems.