ISSN:2320-0790

An International Journal of Advanced Computer Technology

A Novel DNA based Encryption Algorithm for Multimedia information

Shima Ramesh Maniyath[1], Thani kaiselvan V[2]

[1]Asst. Professor, MVJ College of Engineering, Bangalore
[2]Asso. Professor, Vellore Institute of Technology, Vellore

Abstract: DNA cryptography is another field of cryptography emerging with the examination of DNA processing. As of late, different DNA based cryptographic calculations have been proposed to create secure picture encryption systems yet at the same time huge numbers of them have low processing and require sending long key. In such manner, this paper proposes another technique for content, image, and video encryption taking into account DNA calculation innovation. The first information is encoded utilizing DNA calculation and DNA correlative principle. In this paper, an encryption plan is composed by utilizing the advancements of DNA synthesis, DNA Digital coding and additionally the hypothesis of conventional cryptography. The customary encryption strategy and DNA computerized coding are utilized to preprocess to the plaintext. Organic troublesome issues and cryptography registering challenges give a twofold security protection to the plan. The primary reason for this calculation utilized for a picture and video is to decrease the enormous picture encryption time. This calculation is executed by utilizing the common DNA groupings as fundamental keys. The main part is the procedure of pixel scrambling. The first picture is befuddled in the light of the scrambling arrangement which is produced by the DNA grouping. The second part is the procedure of pixel substitution. The pixel dim estimations of the new picture and the one of the three encryption formats produced by the other DNA succession are XORed a tiny bit at a time thusly. The fundamental extent of this paper is to propose an augmentation of this calculation to recordings and making it secure utilizing advanced Biological innovation. A security investigation for the proposed framework is performed and presented. Here we demonstrated the legitimacy of the calculation through recreation and the hypothetical examination on the parameters, for example, affectability to plaintext, key affectability, histogram investigation, connection examination including bio-security and math security. What's more, the security investigation demonstrates that the encryption plan has high secret quality.

Keywords: DNA Cryptography, DNA Digital coding, Arnold Cat map, PCR, Image Encryption, DNA computing

I. INTRODUCTION

DNA cryptography [1], [2] is a new born cryptographic field emerged with the research of DNA computing, in which DNA is used as information carrier and the modern biological technology is used as implementation tool. The vast parallelism [3] and extraordinary information density inherent in DNA molecules are explored for cryptographic purposes such as encryption, authentication, signature, and so on . The research of DNA cryptography is still at the initial stage, and there are many problems to be solved. 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. DNA cryptography benefits from the research of DNA computing, DNA cryptography profits by the exploration of DNA processing, yet the DNA figuring is not equivalent to DNA cryptography, and there is the vital distinction between them. In DNA processing, DNA innovation is utilized to take care of troublesome computational issues. While in DNA cryptography, distinctive troublesome natural issues are utilized as the security premise of DNA cryptosystems [4]. The procedures of cryptography can be viewed as calculation. Be that as it may, not all DNA calculations identify with cryptography.

Advanced 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 color intensity. As indicated by the capacity of human visual perception in distinguishing different levels of intensity, the entire range of intensity is divided into 256 levels. Along these lines, the level of intensity in each pixel has a value between 0 and 255. This range is demonstrated by a byte (8 bits). In this way, each pixel is equal to one byte. On the other hand, due to large data size and real time requirement, it is not

reasonable to use conventional encryption methods. In this way, 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 [5] 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. In addition, these algorithms require more than the usual expected computation time and power while performing image encryption. Plain text encryption algorithm.in our study, an encryption plan is composed by utilizing the advances of DNA Synthesis, PCR Amplification and DNA computerized coding and the hypothesis of customary cryptography. The customary encryption system (DES or RSA) and DNA Digital coding innovation are utilized to preprocess to the plaintext. We can get totally diverse ciphertext from the same plaintext through this preprocess operation, which can adequately keep assault from a conceivable word as PCR ground works. The security investigation demonstrates this plan is protected by scientific and trial obstructions. The encryption plan proposed in this paper has high secret quality

II. DIFFICULT BIOLOGICAL PROBLEMS USED IN THIS SCHEME

DNA is the germ plasm of all ways of life. In a twofold helix DNA string, two strands are corresponding as far as grouping that is A to T and C to G as per Watson-Crick rules, which is one of the best investigative revelations in the twentieth century. The cutting edge cryptography depends on troublesome mathematic issues, for example, the Non-Deterministic Polynomial Time Complete (NP-C) issue [6]. Quantum cryptography depends on the Heisenberg unverifiable guideline, which can likewise be viewed as a troublesome physical issue. Along these lines, we believe that DNA cryptography ought to additionally be founded on troublesome natural issues. Some uncertain troublesome organic issues in DNA science may have exceptional quality in cryptography and can be utilized to accomplish new encryption plan. There are numerous troublesome natural issues, which may more troublesome than numerous troublesome mathematic issues. In any case, the trouble is that not these organic issues are applicable to the standard of DNA cryptography. This is completely not quite the same as all around examined troublesome numerical issues. Here in our study, we chose a regular troublesome science issue to add to an encryption plot and attempted to talk about the security of this plan.

The difficult biological problem referred to here is “It is extremely difficult to amplify the message-encoded sequence without knowing the correct PCR two primer pairs”. Polymerase Chain Reaction (PCR) is a fast DNA amplification technology based on Watson-Crick complementarity, and is one of the most important inventions in modern biology. Two complementary oligonucleotide primers are annealed to double-stranded target DNA strands [7], and the necessary target DNA can be amplified after a serial of polymerase enzyme. The PCR is a very sensitive method, and a single target DNA molecule can be amplified to 10^6 after 20 cycles in theory. Thus one can effectively amplify a lot of DNA strands within a very short time. Thinking about the highly stability of PCR, each PCR primer (20-27)-mer nucleotides long is a comparatively perfect selection. In this study, we selected each PCR primer 20-mer nucleotides long. It is a special function in PCR amplification that having the correct primer pairs. It would still be extremely difficult to amplify the message-encoded sequence without knowing the correct two primer pairs. If an adversary without knowing the correct two primer pairs wants to pick out the message-encoded sequence by PCR amplification, he must choose two primer sequences from about 10^{23} kinds of sequences (the number of combination taking 2 sequences from 4^{20} candidates). So, we believe that this biological problem is difficult and will last a relatively long time.

III. DNA DIGITAL CODING TECHNOLOGY

In the data science, the most crucial coding system is twofold advanced coding [8], which is anything can be encoded by two state 0 or 1 and a mix of 0 and 1. There are four sorts of bases, which are adenine (An) and thymine (T) or cytosine (C) and guanine (G) in DNA grouping. The least difficult coding examples to encode the 4 nucleotide bases (A, T, C, G) is by method for 4 digits: 0(00), 1(01), 2(10), 3(11). Clearly, there are 4!=24 conceivable coding designs by this encoding position. As we all know, in a twofold helix DNA string, two DNA strands are held together correlative as far as succession, that is A to T and C to G as per Watson-Crick complementarity principle. Consider DNA advanced coding, it ought to mirror the organic attributes of 4 nucleotide bases, the reciprocal decide that (~0)=1, and (~1=0) is proposed in this DNA computerized coding. As per this reciprocal manage, that is 0(00) to 3(11) and 1(01) to 2(10). So among these 24 designs, just 8 sorts of examples (0123/CTAG, 0123/CATG, 0123/GTAC, 0123/GATC, 0123/TCGA, 0123/TGCA, 0123/ACGT, 0123/AGCT) which are topologically indistinguishable fit the correlative principle of the nucleotide bases. It is proposed that the coding design as per the arrangement of atomic weight, 0123/CTAG, is the best coding design for the nucleotide bases. This example could idealize mirror the natural attributes of 4 nucleotide bases and have a certain organic essentialness.

The paired computerized coding of DNA successions beats the character DNA coding with the accompanying preferences: (1). To decrease the redundancy of the information coding and improve the coding efficiency compared to the traditional character DNA coding. (2). The digital coding of DNA sequence is very convenient for mathematical operation and logical operation and may give a great impact on the DNA bio-computer. (3). The DNA sequence after preprocessing by DNA digital coding

techniques is able to do digital computing and adapt to the existing computer-processing mode, which facilitates the direct conversion between biological information and encryption information in the cryptography scheme. (4). By using the technology of DNA digital coding, the traditional encryption method such as DES or RSA could be used to preprocess to the plaintext in the cryptography scheme.

IV. SYSTEM DESIGN OF ENCRYPTION SCHEME

Presently, for trading message securely just between particular two persons. We might call the sender Alice, and the proposed beneficiary Bob. Most importantly, we augment the meaning of this encryption plan as takes after. We will portray the framework configuration of encryption plan, whose security on the plan is for the most part in view of the troublesome natural issues and troublesome numerical issues. We will demonstrate the method Assume there is a sender Alice who possesses an encryption key K_A, and a proposed beneficiary Bob who claims an unscrambling key K_B ($K_A = K_B$ or K_A K_B). Alice utilizes K_A to make an interpretation of a plaintext M into ciphertext C by an interpretation E. We have utilizes K_B to make an interpretation of the ciphertext C into the plaintext M by an interpretation D .

The encryption procedure is: C = EKA (M)

The decoding procedure is: DKB (C) = DKB (EKA (M)) = M

It is hard to acquire M from C unless one has KB. We call interpretation E as encryption procedure and C as ciphertext. Here,K_A, K_B and C are not constrained to computerized information, but rather can be any system, material, information, and so forth, for example, DNA succession. E and D are additionally not constrained to numerical calculations.The planned collector Bob has a couple of keys (E,D).We will portray the general procedure of the encryptions plan as takes after.

A. *Key Generation*

The message-sender Alice plans a DNA grouping which is 20-mer oligo nucleotides long as a forward groundwork for PCR intensification and transmits it to planned recipient Bob over a safe channel. The message-beneficiary Bob likewise plans a DNA succession which is 20-mer oligo nucleotides long as an opposite groundwork for PCR enhancement and transmits it to Alice over a protected channel. After a couple of PCR preliminaries is individually planned and traded over a protected correspondence channel, we can get an encryption key K_A that is a couple of PCR groundworks and Bob's open key E, and in addition an unscrambling key K_B that is a couple of PCR groundworks and Bob's mystery key D.

B. *Encryption*

First of all, the sender Alice will translate the plaintext M into hexadecimal code by using the built-in computer code.Then hexadecimal code is translated into binary plaintext M by using third-party software. Finally, Alice translates the binary plaintext M into the binary ciphertext C by using Bob's public key E. We call this preprocess operation is pretreatment data process (data pre-treatment). Through this preprocess operation; we can get completely different ciphertext from the same plaintext, which can effectively prevent attack from a possible word as PCR primers. Then, Alice translates the binary ciphertext C into the DNA sequence according to the DNA digital coding technology. After coding, Alice synthesizes the secret-message DNA sequence which is flanked by forward and reverse PCR primers, each 20-mer oligo nucleotides long. Thus, the secrete-message DNA sequence is prepared. The last process of this encryption is that Alice generates a certain number of dummies and puts the secrete-message DNA sequence among them. It is necessary that each dummy has the same structure as the secrete-message DNA sequence. After mixing the secrete-message DNA sequence with a certain number of dummies, Alice sends the DNA mixture to Bob using an open communication channel.

C. *Decryption*

After the proposed collector Bob gets the DNA blend, he can without much of a stretch discover the emit message DNA grouping. Since the expected collector Bob had gotten the right PCR two preliminary sets through a protected way, he could open up the discharge message DNA grouping by perform PCR on DNA mixture. After Bob increases the emit message DNA succession, he could recover the plaintext M sended from Alice from the converse preprocess operation utilizing his mystery key d. This unscrambling procedure is a mathematic calculation, as well as a natural procedure. The pretreatment information stream diagram is portrayed in Fig 1.

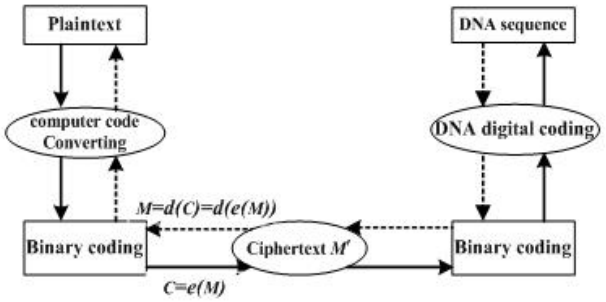


Figure 1: Data pre(post) treatment flow chart

In the following part of this section, we thoroughly discuss details of this encryption scheme with an example shown in fig. 2. The result of the PCR amplification is shown in fig. 3.

Step 1: Key Generation. The message-sender Alice and the message-receiver Bob respectively design and exchange a pair of PCR primers over a secure communication channel. The encryption and decryption keys are a pair of PCR primers. In this scheme, the intended PCR two primer pairs was not independent designed by sender or receiver, but

respectively designed complete cooperation by sender and receiver. This operation could increase the security of this encryption scheme, because even if an adversary somehow caught one of a primer pair, the amplification was not efficient when one of a primer pair is incorrect, only when both of the primer sequences were correct, the amplification could be successful.

Step 2: Data pretreatment. Here we choose "GENECRYPTOGRAPHY" (gene cryptography) as plaintext to encrypt. We first convert this sentence into hexadecimal code by using the built-in computer code, that is: "47 45 4E 45 43 52 59 50 54 4F 47 52 41 50 48 59". Then we translate hexadecimal code into binary plaintext M by using third-party software, that is:

01000111 01000101
01001110 01000101
01000011 01010010
01011001 01010000
01000001 01010000
01001000 01011001

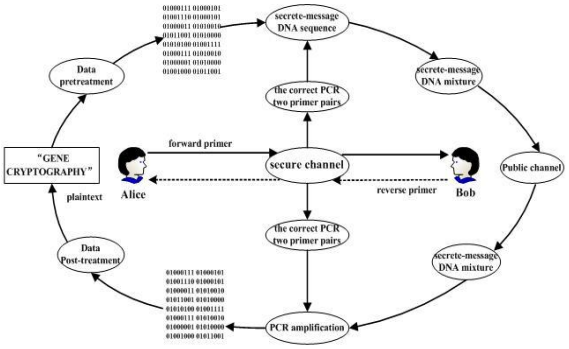


Figure 2: Flow chart of Encryption scheme system

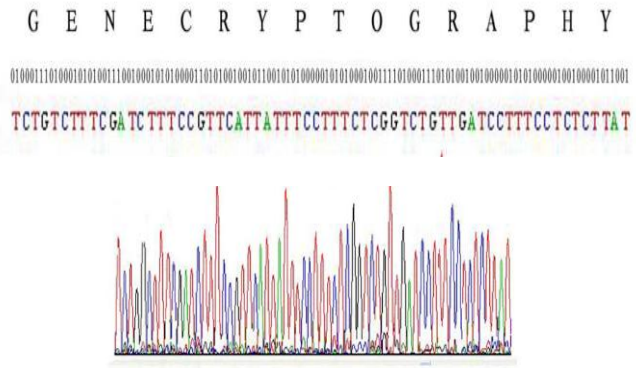


Figure 3 Result of PCR Amplification

Step **3:** Encryption. Alice will encrypt the binary plaintext M into the binary ciphertext C by using Bob's public key E .After that, Alice converts the binary ciphertext C into the DNA sequence by using the DNA digital coding technology. Finally, a secret-message DNA sequence containing an encoded message 64 nucleotides long flanked by forward and reverse PCR primers. Thus, the secrete-message DNA is prepared. After mixing the secrete-message DNA sequence with a certain number of dummies, Alice sends the DNA mixture to Bob using an open communication channel, such as DNA book.

Step 4: Decryption. After the intended receiver Bob gets the DNA mixture, he can easily pick out the secret-message DNA sequence by using the correct primer pairs. Bob translates the secret-message DNA sequence into the binary ciphertext C by using the DNA digital coding technology. Then, Bob can decrypt the binary ciphertext C into the binary plaintext M by using his secret key E.

Step 5: data post-treatment. After the binary plaintext M has been recovered, Bob can retrieve the plaintext M, "GENECRYPTOGRAPHY" from the binary plaintext M by using data post-treatment.

V. Image Encryption Algorithm

A. The Introduction of Algorithm

Despite the fact that a ton of more develop encryption calculations have been proposed, they are not really fit for scrambling the enormous couldn't be packed discretionarily, for example, the guide (bmp).If it is compacted, a great deal of imperative picture. In the practice, there are numerous enormous pictures that should be transmitted through an Internet which data will be unequipped for distinguishing proof. So a picture encryption calculation for the enormous picture that possesses the low encryption time and the high security is important.

B. Arnold Cat Map

Arnold cat map [9] is a typical chaotic map[10], 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 [11] is as in (1).

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

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 [12] 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 [13]; 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 [14] 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 I
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.

C. The Flow of the Encryption Algorithm

In this paper, the first picture is befuddled by Arnold Cat Map [15], for that recurrence worth is created by utilizing the normal DNA succession. At that point, the new picture and the three DNA layouts that are produced by other DNA arrangement are XORed thus. Fig.4 is the stream diagram of this calculation. The picture encryption calculation is as take after:

Step1: Input the first picture A0 is N×N in size, where N and N are lines and segments of the picture separately.

Step2: Gain the picture A1 by befuddling the first Image A0 in the light of the scrambling arrangement which is increased by first regular DNA succession, trailed by Arnold Scrambling

Step3: The DNA layout B 1 is produced by the second DNA arrangement. At that point, the DNA layout B 1 and the picture A1 are XOR ed, and the picture A2 is produced. In this calculation, we plan that a dark worth is comprised of four bases. One base speaks to two twofold digits, in which A, C, G and T are supplanted by 00, 01, 10 and 11.

Step4: According to Fig.5 (b) and Step3, the DNA layout B2 is produced by the DNA format B1 and the picture A2 are XORed, and the picture A3 is created.

Step5: According to Fig.5 (c) and Step3, the DNA layout B3 is produced by the DNA format B2 and the picture A3 are XORed, and the picture A4 is created.

Step6: Gain the scrambled picture A1, where A1 = A4.

As per Step 3, we are utilizing DNA Digital Coding Technology for coding the DNA groupings into a parallel stream. For any pixel, the scope of its dark worth is 0-255, in particular 00000000-11111111. We utilize four bases rather than a dim quality, in which 00, 01, 10 and 11 are supplanted by A, T, C and G.

Table II DNA Digital Coding

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

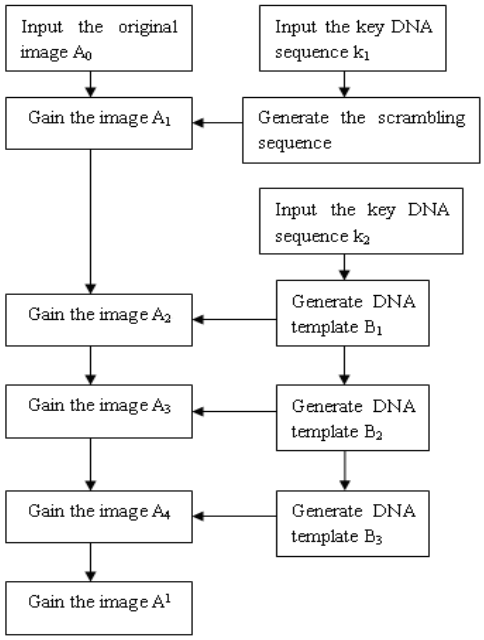


Fig 4 Flow chart of image Encryption Algorithm

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

(a)

1	6	11	16	21
2	7	12	17	22
3	8	13	18	23
4	9	14	19	24
5	10	15	20	25

(b)

25	24	23	22	21
20	19	18	17	16
15	14	13	12	11
10	9	8	7	6
5	4	3	2	1

(c)

Figure 5 The Matrices of the Location

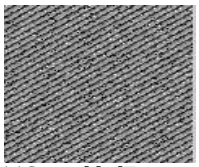
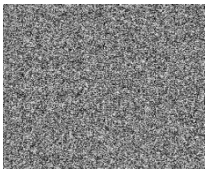
VI. Extension of Secure Algorithm to Videos

A video comprises of single edges which are transiently requested in a steady progression. A solitary video casing might again comprise of a few edges. Since the quantity of casings in a video is extensive, we require a scrambling system that takes less time. The local methodology for video encryption is to regard video information as content and encode it utilizing standard encryption calculations like AES (Advanced Encryption Standard) or DES (Data Encryption Standard). The essential issue [16] with these encryption calculations is that they have high encryption time. They additionally bring about immeasurable increment in size of the video, making them inadmissible for continuous applications like PAY-TV, Pay-Per View and Video on Demand (VOD) and so forth. An interesting normal for video information is that, despite the fact that data rate is high, data quality is low


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

Fig 6 Example for Test Videos along with Frame Numbers

The test videos are shown in Figure 6 along with the frame number. The results of scrambling and XORing the test videos are shown in Figure 7 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.

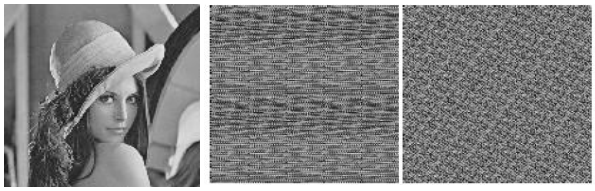



(a)ScrambledFrame **(b) Encrypted Frame**

Fig. 7. Frames from Encrypted Test Videos

VII. Experimental Results

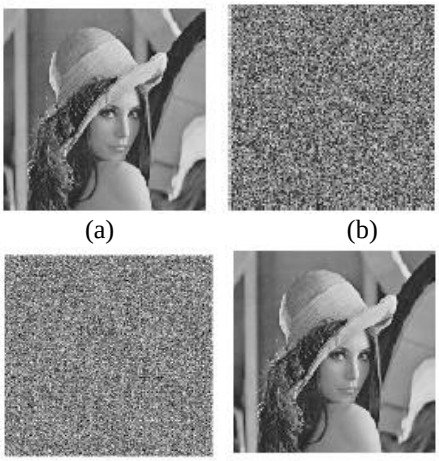
In this paper, we select the classical image of 256×256 Lena.bmp with 256 gray levels as the original image and adopt the discretized Arnold cat map to be the encryption algorithm. We use Matlab 2010 to simulate the experiment. Make the parameter in the Arnold cat secret, the images which are iterated 33 times and 21 times in a period are showed as figure 8(b) and figure8(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)**

Fig 8.The scrambling results of cat map.

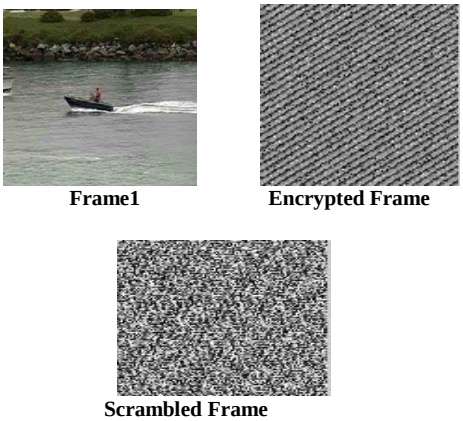
Fig.8 in the experimental result shows the encrypted image and decrypted image. Fig8 (a) shows the original image and Fig.8(b) is the scrambled image gained by the Arnold scrambling process. Fig.8(c) is the encrypted image that is different from the original image absolutely. The encryption processes 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.8(d) is gained. From the experimental results, the image encryption algorithm is feasible and satisfactory.



(a) (b)

(c) (d)

Fig.8 Experimental Results for an image



Frame1 **Encrypted Frame**

Scrambled Frame

Fig 9 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 9.

VIII. 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 peformed 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.

A Key's Security Analysis

An extensive key space is imperative; since we must be accepted that everything is known by the assailant with the exception of the keys in the light of the theory is proposed by Kirchhoff [17]. So it could repulse the comprehensive assaults just when the key space is sufficiently huge. In this paper, we utilize the common DNA groupings as principle keys. In the nature, DNA arrangements are different, and the length has the impressive distinction. If there should arise an occurrence of the same DNA grouping, subsequent to the distinction of the length and the beginning position, a portion is very unique in relation to others. Thusly, the key space is sufficiently substantial to oppose thorough assaults. Keeping in mind the end goal to encourage break down affectability, we test the calculation under the wrong unscrambling keys. A proficient encryption calculation ought to be delicate to mystery key i.e. a little change in mystery key amid unscrambling process results into a totally distinctive decoded picture. So here we are utilizing two keys for picture encryption, one is for scrambling the data picture. The second key is the DNA succession, which will be diverse for distinctive persons.

In this we rolled out an improvement in single piece of the mystery key, which was utilized to control pseudorandom era of DNA succession utilized for scrambling the first picture by Arnold feline guide. Again we test the calculation with distinctive DNA arrangements for unscrambling.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.

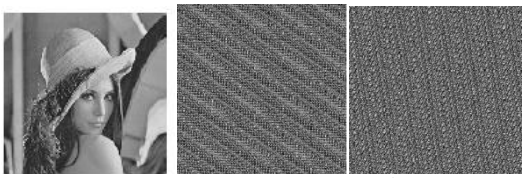


Fig 9 Decrypted images using Wrong Keys for scrambling

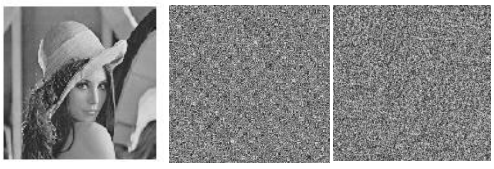
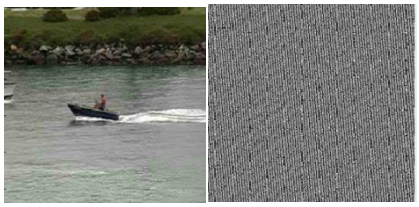


Fig 10 The Decrypted images using Wrong DNA Keys



(a) (b)

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

B *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 III
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

C 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)).

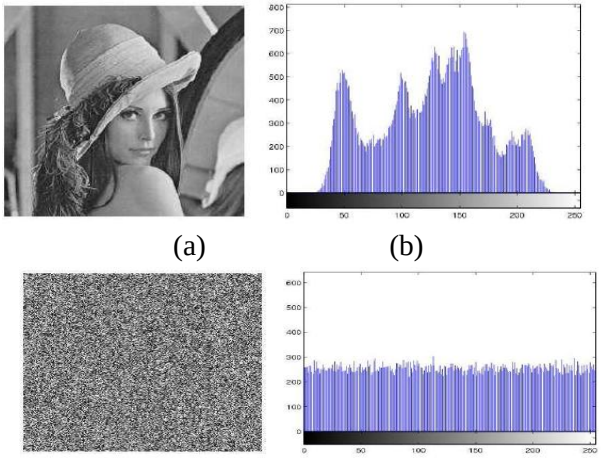


Fig.11 Histograms of the plain-image and the encrypted image

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.

D. Correlation Coefficient Analysis

In the proposed algorithm, the correlation coefficient Analysis [18] 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 IV. Correlation analysis

Adjacent Pixels	Correlation coefficients	
	Original image Fig 12(a)	Encrypted image Fig 12(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.

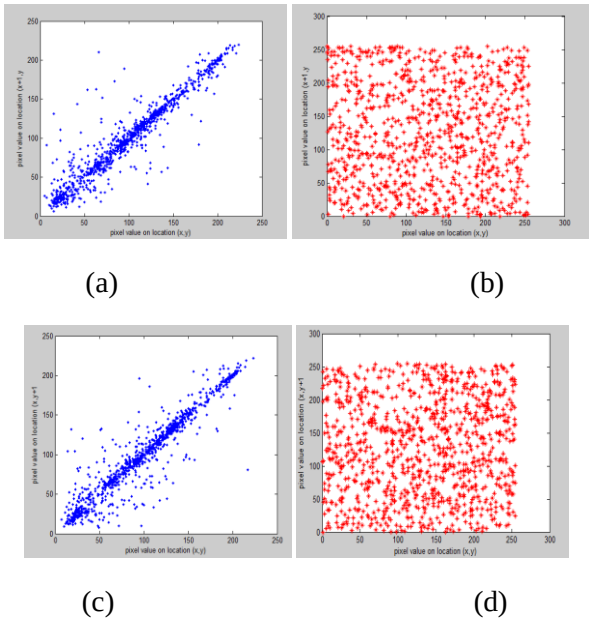


Fig 12 Correlations of two adjacent pixels: Fig (a) and (b), show the distribution of two horizontally adjacent pixels and Fig (c) and (d), show the distribution of two vertically adjacent pixels in the plain and encrypted images shown in Fig. 11 (a) and Fig. 11(c).

E .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 V. 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

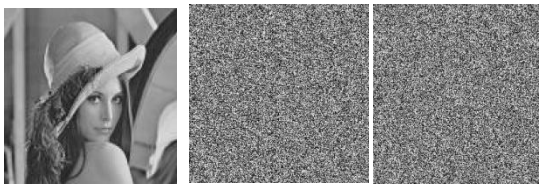
Table VI .Time analysis of the algorithm for video per frame

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

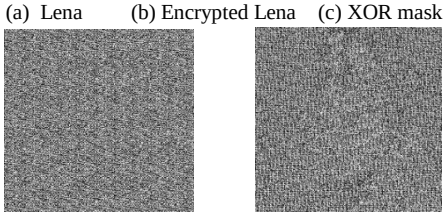
IX. Cryptanalysis

A. Known-Plaintext and chosen plaintext attacks

Chosen/Known-plain text attacks are such attacks [19] 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

B. 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)

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

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 differential resistive against attack.

Table .VII NPCR and UACI of proposed method

NPCR	UACI
0.0015%	**0.004%**

X. Conclusions

In this paper, we composed an encryption plan by utilizing the innovations of DNA combination, PCR intensification and DNA computerized coding and additionally the hypothesis of customary cryptography. The expected PCR two preliminary sets was utilized as the key of this plan not freely outlined by sender or collector, but rather separately planned by the complete participation of sender and beneficiary. This operation could expand the security of this encryption plan. Then again, the customary encryption system and DNA advanced coding are utilized to preprocess to the plaintext. Through this preprocess operation we can get totally diverse ciphertext from the same plaintext, which can successfully keep assault from a conceivable word as PCR preliminaries. The multifaceted nature of organic troublesome issues and cryptography figuring challenges give a twofold security shields to the plan. Also, the security investigation demonstrates that the encryption plan has high classified quality. Also, the expense of this encryption plan will be cut enormously with the advancement of organic advances later on.

This paper we planned an encryption plan by utilizing the advancements of DNA union, PCR intensification and DNA computerized coding and additionally the hypothesis of customary cryptography, a picture encryption calculation for the huge picture that is to utilize the DNA arrangements to create the scrambling succession and encryption format so that the encryption time of the huge picture is diminished as it were. The fundamental keys are the normal DNA successions in this paper, so the key space is sufficiently vast to oppose comprehensive assaults. The investigation exhibits that the picture encryption calculation is effective and very secure. All parts of the

proposed encryption framework were recreated utilizing MATLAB. Relationship investigation demonstrated that connection coefficients between nearby pixels in the plain-picture are altogether diminished in the wake of applying encryption capacity. To evaluate the contrast between scrambled picture and comparing plain-picture, two measures were utilized: NPCR and UACI. The plan can oppose most referred to assaults, for example, measurable investigation and animal power assaults. All the trial examinations demonstrate that the proposed encryption calculation:

(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

XI. ACKNOWLEDGEMENT

We creators might want to pass on our earnest appreciation to Vellore Institute of Technology, Vellore for giving an amiable workplace and consistent backing in finishing our undertaking.

XII. REFERENCES

[1] L. M. Adleman, "Molecular computation of solutions to combinational problems," *Science*, vol. 266, pp. 1021–1024, 1994.

[2] R. J. Lipton, "Using DNA to solve NP-complete problems," *Science*, vol. 268, pp. 542–545, 1995.

[3] L. M. Adleman, "On applying molecular computation to the date encryption strands in DNA based computers," in *Proc. of the 2ed Annu*., 1996, pp. 28–48.

[4] C. T. Celland, V. Risca and Bancroft C. "Hiding messages in DNA microdots," *Nature*, vol. 399, pp. 533–534, 1999.

[5] M. Amosa, G. Paun and G. Rozenbergd. "Topics in the theory of DNA computing," *Theoretical Computer Science*, vol. 287, pp. 3–38, 2002.

[6] G. Z. Xiao, "New field of cryptography: DNA cryptography," *Chinese Science Bulletin*, vol. 51, pp. 1139–1144, 2006.

[7] L. Kari, "DNA Computing: Arrival of Biological Mathematics," *The Mathematical Tntelligencer*, vol. 19, pp. 9–22, 1997.

[8] 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.

[9] 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

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

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

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

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

[14] 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

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

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

[17] 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'*

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

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