A Multilevel Image Encryption based on Duffing map and Modified DNA Hybridization for Transfer over an Unsecured Channel

P. Naga Srinivasu[1], Ch. Seshadri Rao[2]
[1,2]Assistant Professor, Department of Computer Science and Engineering
Anil Neerukonda Institute of Technology and Sciences

ABSTRACT
It was known to us from decades it is been a factual challenge for us to transfer the privileged data specially images to transfer over a unsecured channel. In this paper we propose a novel image encryption technique using DNA interwearing based Hybridization along with chaotic maps to transfer image data over a unsecured channel. In the early stages we apply Duffing map(chaotic map) on the original image, the resultant image we obtain will be the scrambled original image, where pixel position will be scattered over the image plain. And in the next phase we apply the technique of modified DNA hybridization based on the interwearing on the resultant image. Finally encrypted using a modified hill cipher.By doing so we attain chaotic behavior(Butterfly effect with small change in initial condition leads to big change in resultant outcome) by using Duffing map and we achieve highely security with less processing by using DNA Hybridization based image encryption. The security analysis of proposed techniques has achieved satisfactory outcome and results were presented.

Keywords
Duffing map, DNA NucleoBase, Interwearing, DNA Hybridization, cipher

1. INTRODUCTION
In the present day scenario with ever increasing transfer of data over the network, encryption of data plays a vital role to ensure the integrity, accuracy and sustainability of data. It our aim to transfer the image data in a unsecured data in a secured way. There were many techniques used in image encryption such as DES,3DES, AES,IDEA,BLOWFISH[1] these suffer with a few flaws like DES whose key size is 56-BIT which could be easily broken in very less time which is practically proved and 3DES is computationally not feasible much time for encryption at perform normal DES operation trice. AES is competitively better but I requires more computations. Blowfish is other traditional block cipher relatively better than the rest three but while using with images or videos comparatively less performance as it is block cipher sometimes it is required to do padding and every time we have to segment the image to multiple blocks and have to reassemble them. And the other method of image encryption is through pixel permutation where the image pixels were scrambled basing on some criteria which requires very less computation but this pixel permutation alone can't provide high security to transfer image over a unsecured channel.

Here in our encryption technique we propose a multi-level encryption where in the early phase we use Duffing map which exhibit the dynamic behavior of chaotic maps and in the next phase we perform the modified DNA hybridization which provides the high security to the image data with less computation and finally encrypted to cipher. The paper was arranged as follow in the first section we discuss about Duffing map and in the second section about DNA Hybridization and in third section we discuss about modified hill cipher based encryption and following by the results and conclusion.

2. DUFFING MAP BASED PIXEL PERMUTATION
Basically Duffing map is also sometimes called as Holmes Map is a type of chaotic map which exhibit chaotic behavior which is discrete over time domain with a dynamic nature. Basically when we pass pixel coordinates(X,Y) as the input for the Duffing equation it will derive the new coordinates (X+1,Y+1).By which we achieve better shuffled pixels which was easy to perform and invertible in nature.

Here is the equation to compute new coordinates of pixels from old coordinates

Binary Value	Replaced With
00	**C(Cytosine)**
01	**A(Adenine)**
10	**T(Thymine)**
11	**G(Guanine)**

$$X_{i+1} = Y_i$$

$$Y_{i+1} = -q(X_i) + p(Y_i) - y_i^3$$

Where

P and q were two constants. We had chosen p=2.75 and q=0.2 to exhibit chaotic behavior.

3. DNA ENCODING AND INTERWEARING BASED HYBRIDIZATION
DNA Hybridization is a technique in which we have to convert the image bit sequence to DNA sequence basing on nucleic acid bases[2]. As we know that every DNA sequence is build by four natural nucleic i.e Adenine(A),Thymine(T),Cytosine(C) and Guanine(G) following the complementary condition that Adenine(A) is opposite/complimentary to Thymine(T) and Cytosine(C) is opposite/Complimentary to guanine(G).It is common in DNA sequencing where the binary data was replaced by the nucleic acid bases .Where the binary sequence 01 is replaced by A and its complementary 10 is obviously replaced by T similarly 00 is replaced by Cytosine(C) and 11 is replaced by Guanine.

Here while doing the DNA hybridization based on interwearing by considering an random DNA sequence. If we

consider a grey scale image and the pix intensity as the pixel value. It obvious that the pixel value lies between 0(full dark) and 255(full bright).This requires 8 bits for representation of the pixel.so this 8 bits were converted to some DNA sequencing before performing DNA hybridization on them.

So let us consider the image of size M x M where M is a even number, and the pixels values were represented in matrix format and in case if the matrix consist of odd number of rows or columns we are going to perform padding to the original data which adds more security to the data.

Take other matrix with same size as M x M with random sequence of DNA, which will be used to perform hybridization of the original DNA sequence based on some interwearing rules. Here is the way way how we perform hybridization.

Original data

$$\begin{bmatrix} p_{11} & p_{12} & \cdot & \cdot & p_{1m-1} & p_{1m} \\ p_{21} & p_{22} & \cdot & \cdot & p_{2m-1} & p_{2m} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{m-11} & p_{m-12} & \cdot & \cdot & p_{m-1m-1} & p_{m-1m} \\ p_{m1} & p_{m2} & \cdot & \cdot & p_{mm-1} & p_{mm} \end{bmatrix}$$

Random DNA matrix for hybridization

$$\begin{bmatrix} R_{11} & R_{12} & \cdot & \cdot & R_{1m-1} & R_{1m} \\ R_{21} & R_{22} & \cdot & \cdot & R_{2m-1} & R_{2m} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ R_{m-11} & R_{m-12} & \cdot & \cdot & R_{m-1m-1} & R_{m-1m} \\ R_{m1} & R_{m2} & \cdot & \cdot & R_{mm-1} & R_{mm} \end{bmatrix}$$

Here by following the interwearing rules for performing the DNA hybridization. Here we perform the substitution of random DNA matrix in the original matrix.

Step 1: In first step each element of the columns in both original data and random data matrix is moved up by one row with the elements in first row circularly follow the last.

Step 2: In the second step all the rows divisible by four in the original matrix were performed exclusive OR(XOR) with the corresponding rows in the random data matrix.

$$\boldsymbol{Q = P \oplus R}$$

Step 3: In this step we rotate the columns of both the original data matrix and random data matrix were shifted by one step left in circular manner(rotate left circular).

Step 4: Now in the last step we will replace all the columns divisible by four in the original matrix were performed exclusive OR with the corresponding columns in the random matrix.

So the resultant matrix will be hybridized for of the original pixel matrix. The resultant matrix will as follows

Resultant Matrix

$$\begin{bmatrix} p_{22} & p_{23} & Q_{24} & \cdot & \cdot & p_{2m} & p_{21} \\ p_{32} & p_{33} & Q_{34} & \cdot & \cdot & p_{3m} & p_{31} \\ R_{42} & R_{43} & P_{44} & \cdot & \cdot & R_{4m} & R_{41} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{m2} & p_{m3} & Q_{m4} & \cdot & \cdot & p_{mm} & p_{m1} \\ p_{11} & p_{13} & Q_{14} & \cdot & \cdot & Q_{1m} & p_{11} \end{bmatrix}$$

4. ENCRYPTION OF RESULTANT MATRIX

Once after obtaining the resultant matrix after performing the hybridization we are going to convert the DNA based data to hexadecimal data based on the following table.

DNA Sequence	Hexadecimal Value
AA	0
AT	1
AC	2
AG	3
TA	4
TT	5
TC	6
TG	7
CA	8
CT	9
CC	A
CG	B
GA	C
GT	D
GC	E
GG	F

Once after converting the resultant matrix to the hexadecimal format. we are going to perform hill cipher on the data for final round of encryption. Here we are going to take some random matrix as the key and we are going to perform the matrix multiplication to generate the cipher text.

$$\begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \\ k_{41} & k_{42} & k_{43} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix} = \begin{bmatrix} \boldsymbol{c_1} \\ \boldsymbol{c_2} \\ \boldsymbol{c_3} \\ \boldsymbol{c_4} \end{bmatrix}$$

Here we are going to perform the operation with mod F(16) as we are performing the operation with hexadecimal data, Here were the linear equations

$$\boldsymbol{C_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_2) Mod\ F}$$
$$\boldsymbol{C_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_2) Mod\ F}$$
$$\boldsymbol{C_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_2) Mod\ F}$$

$$C_4 = (k_{41}p_1 + k_{42}p_2 + k_{43}p_2) Mod\ F$$

While decryption the receiver end the same process will be done in reverse order to get back the resultant matrix.

5. SECURITY ANALYSIS

It is common that many active or passive attacks were possible on the cipher text[3], there were basically three major attacks that are against the proposed technique of image encryption: Cipher text attack, Chosen Cipher text attack, adaptive chosen cipher text attack. But in our technique it's very difficult because of multiple level of encryption and the key we had taken. At the beginning we had performed a chaotic map based pixel shuffling and then we make use of DNA interwearing based hybridization followed by the modified hill cipher based encryption had enriched the security at multi-levels.

5.1 Combat against Exhaustive Attacks

Our proposed technique of image encryption is highly resistant against exhaustive attacks like brute force attack because of multiple keys we are using at multiple levels. In both the stages we use a random matrix of M X M and M X N which is not possible for crypt analyst to decode the original image data in polynomial time.

5.2 Combat against Statistical Attack

In the play fair based encryption algorithm we are going to modify the actual pixel intensity of the resultant image and inerwearing based hybridization makes difficult for the statistical attack to identify the actual pixel values and positions.

5.3 Information Entropy

Information entropy will tell you the availability of amount of information a particular event or message depending on the context, by which we can calculate the degree of uncertainty. The information of entropy can be calculated based on the distribution of the grey scale over the image and degree of scrambling of pixels in the image.

$$\mathrm{I(n)} = -\sum_{i=0}^{m} P(n_i)\log 2\ P(n_i)$$

Where ni is the ith grey value for m level grey image, P(n) is the emergence probability of ni ,so $\sum_{i=0}^{m} P(n_i)$ is 1. We can say for a well encrypted image the value if I(n) should be something around 7 in our experimental result we got it upto 6.879 which is very close to the expected value.

The degree of the correlation among the pixels after shuffling is calculated by

$$I_{xy} = \frac{\frac{1}{\mathrm{r}*\mathrm{c}}\sum_{i}^{r}\sum_{j}^{c}(X_{ij}-X)(Y_{ij}-Y)}{\sqrt{\frac{1}{\mathrm{r}*\mathrm{c}}\sum_{i}^{r}\sum_{j}^{c}(X_{ij}-X)^2 \frac{1}{\mathrm{r}*\mathrm{c}}\sum_{i}^{r}\sum_{j}^{c}(Y_{ij}-Y)^2}}$$

X_{ij} and Y_{ij} are the pixels in the ith row and jth column of X and Y respectively and 'r' and 'c' represent the number of rows and columns in the image.

6. RESULTS

The results of the work show the encrypted images after DNA encryption using a Duffing Map.

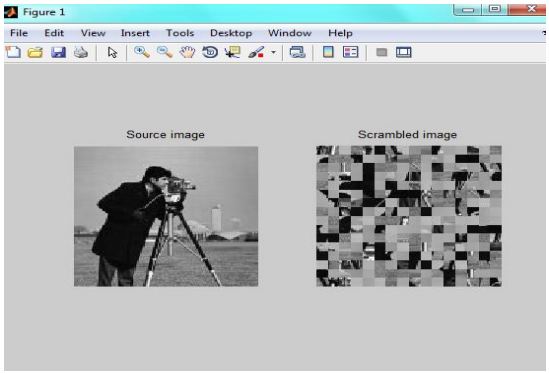

Fig 1. Resultant image after 30 iterations using duffing map algorithm,we get a scrambled image

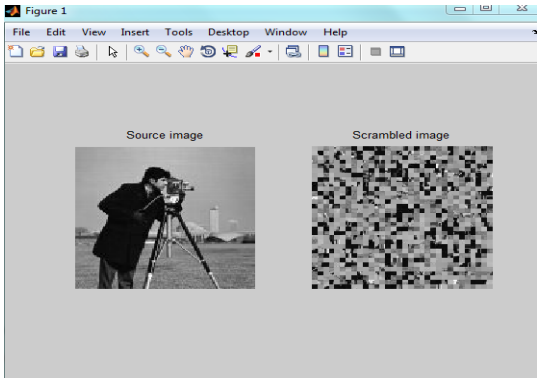

Fig 2. Resultant image after 70 iterations using duffing map algorithm,we get a better scrambled image than 30 iterations

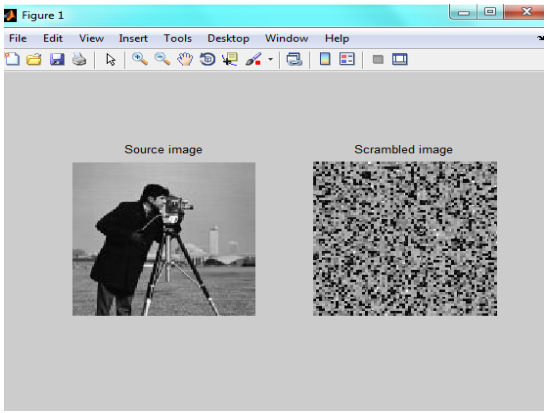

Fig 3.Resultant image after 120 iterations using duffing map algorithm,we get better scrambled image than 70 iterations

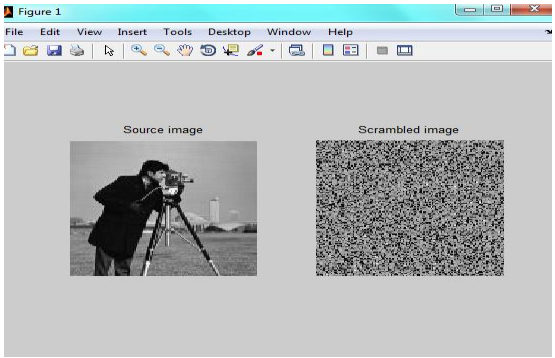

Fig 4:Resultant image after 175 iterations using duffing map algorithm,we get a better scrambled image than 120 iterations

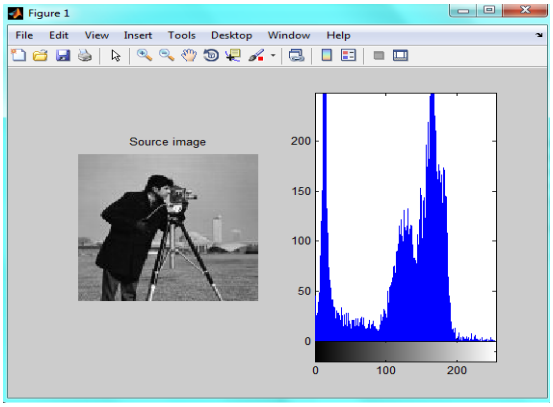

Fig 5:It shows the histogram of the original image

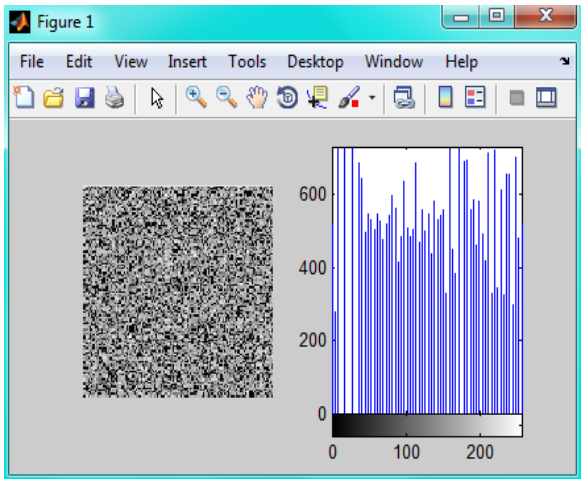

Fig 6:It shows the histogram of the resultant encrypted image

7. CONCLUSION AND FUTURE WORK

The fundamental idea behind this technique of encrypting an image is to effectively use the less computation based methodology to achieve better security over the traditional approach. DNA based encryption or chaotic maps alone could not give a better result. So in this technique we use a modified way of DNA hybridization and chaotic maps for better security.

Our future work is to apply the same with different sorts of data and measure the performance and to do comparative study to decide where this technique suites well.

8. REFERENCES

[1] Milind mathur, ayush kesarwani,"comparision between des,3des,rc2,rc6,blowfish and aes"proceedings of national conference on new Horizons in IT-NCNHIT-2013

[2] Jangid, R.K. Mohmmad, N. ; Didel,A ; Taterh, S," Hybrid approach of image encryption using DNA cryptography and TF Hill Cipher Algorithm",April 2014,ICCSP,IEEE.

[3] Shima Ramesh Maniyath,supriya M ,"An uncompressed Image Encryption Algorithm Based on DNA Sequencing".

[4] Jun peng, Shangzhu Jin,Liang Lei,Qi Han ,"Research on a novel image encryption algorithm based on the hybrid of chaotic maps and DNA encoding",july 2013,IEEE.

[5] Qiang Zhang, Ling Guo , Xianglian Xue , Xiaopeng Wei ,"An image encryption algorithm based on DNA sequence addition operation"oct 2009,IEEE.

[6] Rithu Guptha,Anchal Jain," A New Image Encryption Algorithm based on DNA Approach", International Journal of Computer Applications,volume 85,Issue 18.

[7] Borislav stoyanov,krasimir kordov,"Novel Image Encryption Scheme Based on Chebyshev Polynomial and Duffing Map",march 2014, The Scientific World Journal

[8] AL.Jeeva,Dr. V. palanisamy, K.Kangaram "Comparative analysis of performance efficiency and security measures of some encryption algorithms",june 2012,International journal of engineering research and applications.

[9] Som, S. , Kotal, A. ; Chatterjee, A. ; Dey, S. "A colour image encryption based on DNA coding and chaotic sequences."sept. 2013,IEEE.

[10] Xiaoling Huang, Guodong Ye ,"An image encryption algorithm based on hyper-chaos and DNA sequence",Dec 2012,Springer.

[11] Lili Liu,Qiang Zhang, Xiaopeng Wei," A RGB image encryption algorithm based on DNA encoding and chaos map,feb 2012,Science Direct.