B.SC. 3Year Degree Honours Part – III Examination

Computer Science (Honours)

Registration No: 016062

Session: 2016 -2017

Roll No: 213-17117-0197

College: Kalyani Mahavidyalaya

Project Report on:

“A Lossless Image Encryption Method based on DNA Substitution and Chaotic Logistic Map”

**ACKNOWLEDGEMENT**

**I**t is easily understandable that research based project is not easy to develop without any sort of help or suggestions from anybody. I have successfully done my project “**A Lossless Image Encryption Method based on DNA Substitution and Chaotic Logistic Map**” taking a lot of valuable tips and suggestions from a no. of individuals. I would like to pay my sincerest gratitude to that particular person Mr.Shouvik Chakraborty.

I would like to thank  **Smt. Sampa Rani Bhadra  (Head of the Deperatment )** for her guidance as well as her special care to me . She was along with me through the whole project to solve critical problems whenever I faced. I am highly grateful to her.

**Signature of Student Signature of Guide**

**Date: Date:**

**CERTIFICATE**

**T**his is to certify that project / dissertation entitled “**A Lossless Image Encryption Method based on DNA substitution and Chaotic Logistic Map”** is a bonafide work done by **Raja Swarnakar** for 3rd Year Examination has been carried out under the supervision and guidance of **Smt. Sampa Rani Bhadra(Head of the Department)**.

I found him conscientious and vigilant in his project work and completed the project successfully.

I wish him for bright future.

Dr. Runu Das

Principal Signature

External Signature

Smt. Sampa Rani Bhadra 1.

HOD(Computer Science) Signature

     2.

**Contents**

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **Topic** | **Page number** |
|  | [**Introduction**](#_1.Introduction:) | **1-3** |
|  | [**Objective**](#_2.Objective:) | **3** |
|  | **[Chaotic Logistic](#_3.Chaotic_Logistic_Map:)**  **[Map](#_3.Chaotic_Logistic_Map:)** | **4-6** |
|  | [**DNA Substitution**](#_4._DNA_Substitution) | **7** |
|  | [**Proposed Algorithm**](#_5._Proposed_Algorithm) | **8-11** |
| **5.1** [**Encryption Algorithm**](#_5.1_Encryption_Algorithm) | **8-10** |
| **5.2** [**Decryption Algorithm**](#_5.2_Decryption_Algorithm:) | **10-11** |
|  | [**Experimental Result**](#_6._Experimenatal_Result:) | **12-16** |
| **6.1** [**Correlation Coefficient**](#_6.1_Correlation_Co-Efficient) | **12** |
| **6.2** [**PSNR**](#_6.2_PSNR:) | **13** |
| 6.3 [**Differential Attacks: NPCR and UACI**](#_6.3_Differential_Attacks:) | **14** |
| **6.4** [**Histogram**](#_6.4_Histogram) | **15** |
|  | [**Coding Snapshot**](#_7.Coding_Snapshot/////) | **17-19** |
|  | [**Conclusion**](#_8._Conclusion) | **19** |
|  | [**References**](#_References:) | **20** |

A Lossless Image Encryption Method based on DNA substitution and Chaotic Logistic Map

# 1.Introduction:

With the growing interest of internet in this world, the most concerned thing arise is security of information. Everyday a lot of information flowing around the globe through internet and at the same time security threat increasing exponentially. It has become essential to protect information from unauthorized access. Many application like military image databases, private video conferencing, medical imaging system ,cable TV etc. require fast and robust security system to store and transmit digital images. As someone said, "Necessity is the mother of invention" and this security crisis led to develop good encryption techniques . Encryption works by jumbling up the information data into unreadable form and then uses a key to extract the original data .In the past, several image encryption techniques have been proposed in the literature based on different principles. Traditional image encryption techniques are generally not suitable for real-time processing for their slow speed and also handling different image formatting. Many chaos-based image encoding algorithms have been suggested in recent time. [2] The concept of chaos is mostly used for its excellent cryptographic characteristics. Chaos-based encryption techniques provide a good combination of speed, high security, complexity, reasonable computational overheads and computational power etc. The digital images have certain characteristics such as: redundancy of data, strong correlation among adjacent pixels, being less sensitive compared to text data i.e. a tiny change in the attribute of any pixels of images does not drastically degrade the quality of the image and bulk capacity of data etc.

The traditional ciphers like AES, DES, IDEA, RSA etc. are not suitable for real-time image encryption as these ciphers require large computational time and high computing power. For real time image encryption only those ciphers are preferable which takes lesser time and at the same time without compromising the security.[1] Various encryption algorithms provide different degree of security and it is based on how hard they are to break. If the cost required to break an algorithm is more than the value of the encrypted data then the algorithm probably is thought to be safe. Modern high quality image encoding techniques have several errors and are exposed to heavy attacks by expert cryptanalyst. Through study and analysis between these techniques are needed to ensure performance and to choose the better one for the intended application. There are three types of encoding schemes namely substitution, transposition and permutation and techniques which include both substitution and transposition. Substitution schemes change the pixels while permutation just shuffles the pixels based on the algorithm. In some cases both the methods are combined to improve security.

In this paragraph we will briefly discuss a few chaos based image encryption scheme. In [3] author has shown to construct a symmetric block encryption technique based on two-dimensional standard baker map. Yen et al.[4] proposed an encryption technique known as BRIE based on chaotic logistic map. Further, authors [5] have proposed an encryption technique called as CKBA (Chaotic Key Based Algorithm) in which a binary sequence as a key is generated using a chaotic system. In [6] authors proposed a chaos based method using bit level permutation. Permutation at bit level changes the value. Authors [7] illustrated a new method on total shuffling. In [8] combinations of two logistic maps are used for improving the security. In [9] authors have combined the diffusion and confusion operation and uses spatial-temporal chaotic system for generating the key. This increased security but its time consuming.

The remaining of this project organized is as follows. **Section** 2 describes the objective of this project, **section** 3 describes the chaotic logistic map, **section** 4 describes the DNA substitution ,**section** 5 describes proposed encryption method ,**section** 6 describes experimental result, **section** 7 illustrated a few snap of coding and **section** 8 conclude the project.

### 2.Objective:

The aim is to propose an image encryption algorithm that is fast and secure in real-time processing. This chaos-based algorithm is fast and productive. Applying the DNA substitution provides another layer of security.

The output encrypted image reveals that the proposed method is quite reliable and robust.

This method is so sensitive to the initial values and input image so that the small changes in these values can lead to significant changes in the encrypted image.

The proposed algorithm is resistant to the differential attack.

It has been tested and various parameters are checked like correlation coefficient analysis, NPCR and UACI values, histograms analysis, PSNR value analysis.

# 3.Chaotic Logistic Map:

Chaos is a ubiquitous phenomenon existing in deterministic nonlinear systems which exhibit high sensitivity to initial conditions and have random behaviour. It was discovered by Edward N.Lorenz in 1963. To create a chaotic stream cipher, a random bit stream is to be generated using chaotic system. Pseudo Noise (PN) Sequences : A pseudo random bit generator [10] (PRBG) is a deterministic algorithm, which uses a truly random binary sequence of length k as input called seed and produces a binary sequence of length l>>k, which is called pseudorandom sequence. This pseudorandom sequence appears to be random. The output of a PRBG is not truly random; in fact the number of possible output sequences is at most a small fraction ( / ) of all possible binary sequences of length l. The basic idea is to take a small truly random sequence of length k and expand it to a sequence of much larger length l in such a way that an adversary cannot efficiently distinguish between output sequence of PRBG and truly random sequence of length.

The logistic map is a polynomial mapping of degree 2, often cited as an archetypal example of how complex, chaotic behaviour can arise from very simple non-linear dynamical equations. Mathematically, the logistic map is written as given in Equation 1.

) (1)

where λ € (0,4) , n = 0,1.....

Response of logistic map for λ=3.16 is given in Figure 1 and for λ=3.985 is given in Figure 2.

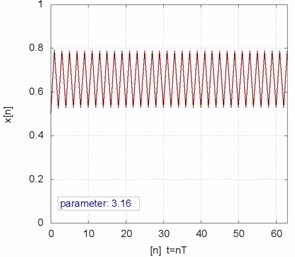


Figure 1: Response of Logistic map for λ=3.16

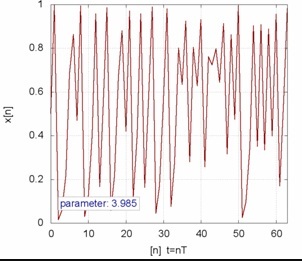


Figure 2: Response of Logistic map for λ=3.985

A bifurcation diagram shows the values visited or approached asymptotically (fixed points, periodic orbits, or chaotic attractors) of a system as a function of a bifurcation parameter in the system. The bifurcation parameter λ is shown on the horizontal axis of the plot and the vertical axis shows the set of values of the logistic function visited asymptotically from almost all initial conditions. The bifurcation diagram shows the forking of the periods of stable orbits from 1 to 2 to 4 to 8 etc. Each of these bifurcation points is a period-doubling bifurcation. The ratio of the lengths of successive intervals between values of λ for which bifurcation occurs converges to the first Feigenbaum constant. The diagram also shows period doublings from 3 to 6 to 12 etc., from 5 to 10 to 20 etc., and so forth. Bifurcation diagram of logistic map is given in Figure 3.

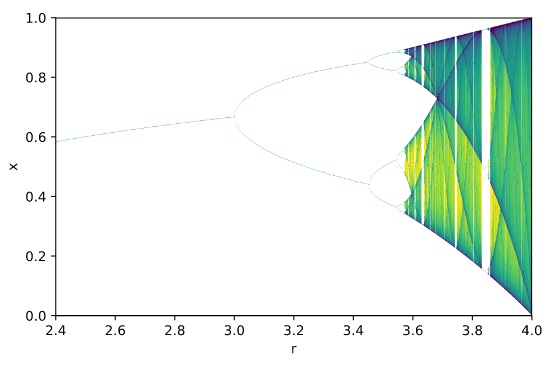


Figure 3: Bifurcation diagram of Logistic map

The pseudo random bit sequence is generated by comparing the outputs of two chaotic logistic maps. The chaotic logistic map produces the binary sequences by comparing the outputs of the piecewise linear chaotic maps in the way as given in Equation 2.

(2)

## 4. DNA Substitution Method:

There are two rules in chaotic DNA substitution:-

• Binary Coding Rule

• Complementary Rule

The binary coding rule transforms letters transforms binary codes into A, T, G, C and vice-versa. In this method the following encoding is adopted A=00, C=01, G=10, T=11. That means A is coded as "00", C as "01" etc. Each pixel value is then transformed into binary sequence using DNA substitution.

In complementary rule , each letter x is assigned to a complement denoted C(x). Here the C(x) represents the complement of x. This is how the complement operation takes place:-

(AT)(TC)(CG)(GA), the complement rule states that C(A)=T, C(T)=C,C(T)=G,C(G)=A. There are six allowable complementary transformations.

(AT)(TC)(CG)(GA)

(AT)(TG)(GC)(CA)

(AC)(CT)(TG)(GA)

(AC)(CG)(GT)(TA)

(AG)(GT)(TC)(CA)

(AG)(GC)(CT)(TA)

## 5. Proposed Algorithm

##### 5.1 Encryption Algorithm

The process proceeds with choosing an image and converting it to grayscale if its color one. Now we initialize DNA\_lookup matrix for DNA substitution. Now we take initial parameters for the logistic map x1 , y1 , r. We generate a pseudo random bit sequence whose length can be calculated using Equation 3.

(3)

**DNA\_lookup matrix** =[0,1;0,0;1,1;1,0]

Taking 100 bits of generated pseudo random bit sequence i.e. PRBS and process it in following procedure 1:

Let us imagine 100 bits as row of 10 bits each means 10 rows of 10bits.

We take 8 bits from each row excluding first bit of each row. Taking 8 bits from each row performing XOR operation with 8 bits of next row to get 8bits sequence and again perform XOR operation with 8bits of next of row and repeat the process until the 100 bits processed to get 8bits sequence that is our first key.

Now we generate a 64 bit binary sequence which will be used as second key. We convert each pixel value of an image to decimal value into 8 bit binary format and reverse it. Then generate a binary sequence of length 8 by performing XOR on corresponding pixel binary sequence generated in previous step with temporary key. Divide this binary sequence in 4 groups containing 2 bits each and reverse each group. Now we substitute each group with the corresponding values obtained from DNA\_lookup matrix. Combine four groups into 1byte and perform XOR operation with the first key. Reverse the obtained sequence and convert it into decimal and assign it as an encrypted image pixel.

The encryption algorithm is given below:

1. Input an image.
2. Convert it into grayscale if it is color image
3. Initialize DNA\_lookup matrix.
4. Initialize x1,y1,r parameter for the logistic map.
5. Generate a PRBS of length calculated using equation 3.
6. We take the 100 bits of PRBS and process it to generate 8 bits binary sequence using procedure 1 and marked as first key (key 1).
7. Generate a 64 bit binary sequence which will be marked as key 2.
8. Extract rest of the PRBS sequence which is obtained in step 5 i.e. after extracting 100bits .
9. Perform XOR operation between key 2 and first 64 bits of PRBS obtained in step 8 and assign it to tempkey.
10. For all pixels repeat the following step:

10.1 Convert each pixel to 8 bits binary sequence and reverse it;

10.2 Divide tempkey into 8 byte and perform XOR 1 byte of tempkey with the binary sequence generated in 10.2.

10.3 Divide the binary sequence obtained in previous step into 4 groups 2bits each . And reverse each group.

10.4 Substitute each group with corresponding value obtained from DNA\_lookup matrix .

10.5 Combine four groups into 1 byte and perform XOR operation with key 1.

10.6 Reverse the binary sequence obtained in previous step and convert it into decimal value and assign it as an encrypted pixel .

10.7 Check if the tempkey is exhausted then

10.7.1 Reverse the current tempkey.

10.7.2 Perform XOR operation between tempkey and remaining extracted PRBS.

##### 5.2 Decryption Algorithm:

The decryption process follows exactly the reverse method of the encryption process.

The Decryption algorithm is given below:

* + - 1. Input the encrypted image.
      2. Initialize DNA\_lookup matrix.
      3. Initialize x1,y1,r parameter for the logistic map.
      4. Generate a PRBS of length calculated using equation 3.
      5. We take the 100 bits of PRBS and process it to generate 8 bits binary sequence using procedure 1 and marked as first key (key 1).
      6. Generate a 64 bit binary sequence which will be marked as key2.
      7. Extract rest of the PRBS sequence which is obtained in step 4 i.e. after extracting 100bits.
      8. Perform XOR operation between key 2 and first 64 bits of PRBS obtained in step 7 and assign it to tempkey.
      9. For all pixels repeat the following step:

9.1 Convert each pixel to 8 bits binary sequence and reverse it.

9.2 Perform XOR operation with key1.

9.3 Divide the binary sequence in four parts obtained in previous step and reverse the binary sequence.

9.4 Substitute each group with corresponding value obtained from DNA\_lookup matrix .Then reverse it.

9.5 Combine the four groups into 1 byte.

9.6 Divide tempkey into 8 byte and perform XOR 1 byte of tempkey with the binary sequence generated in previous step.

9.7 Reverse the binary sequence obtained in previous step and convert it into decimal value and assign it as an decrypted pixel.

9.8 Check if the tempkey is exhausted then

9.8.1 Reverse the current tempkey.

9.8.2 Perform XOR operation between tempkey and remaining extracted PRBS.

#### 6. Experimenatal Result:

The main goal of the image cryptographic algorithms is to produce a image that is difficult to understand. The quality of the image may degrade. The algorithm proposed in this paper degrades the image quality during the encryption technique but at the end of the decryption, the original image is restored. Automated quality measurement methods that are based on mathematical and computational algorithms are necessary because of the variability and inconsistency between human observers. The quality of the image is assessed by some parameters. In the following sections, details of the different parameters along with the results are given.

## 6.1 Correlation Co-Efficient :

Correlation coefficients have been tested in three different direction *i.e*. horizontal, vertical and diagonal. Correlation coefficients are calculated for the selected pairs using Equation 4.

(4)

Where

(5)

(6)

(7)

where x, and y in the above equations are the gray-scale values of the two adjacent pixels in the image, and T is the total pair of pixels randomly selected from the image. Table 1 shows the results obtained from proposed approach on some standard images.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Test Image | Horizontal | | | Vertical | | | Diagonal | | |
| Org | Enc | Dec | Org | Enc | Dec | Org | Enc | Dec |
| Cameraman | 0.9207 | 0.0030 | 0.9207 | 0.9538 | 0.0248 | 0.9538 | 0.8894 | 0.0021 | 0.8894 |
| Boat | 0.8322 | 0.0051 | 0.8322 | 0.9007 | 0.0153 | 0.9007 | 0.8322 | 0.0110 | 0.8322 |
| Mandrill | 0.8764 | -0.0102 | 0.8764 | 0.8852 | 0.0079 | 0.8852 | 0.8245 | 0.00626 | 0.8245 |

Table 1

## 6.2 PSNR:

PSNR is an abbreviation for Peak Signal to Noise Ratio. PSNR is a well-known parameter and can be computed from Equation 8. The PSNR results in an undefined value only if; *i.e*., when the original image is compared to itself. In this case the MSE value in the denominator part of the Equation 8 would result in a zero value, and hence, a division by zero situations occurs).

(8)

Where

(9)

N is the number of pixels in the frame, and xij, yij are the ith and jth pixels in the original and processed frames, respectively. L is the dynamic range of pixel values (L is 0 to 255 for gray-scale images).

Table 2 shows the results obtained from proposed approach on some standard images.

|  |  |  |
| --- | --- | --- |
| Test Image | PSNR | |
| O-D | O-E |
| Cameraman | Undefined | 8.3519 |
| Boat | Undefined | 9.227 |
| Mandrill | Undefined | 9.209 |

Table 2

## 6.3 Differential Attacks: NPCR and UACI

To test the influence of only one pixel change in the plain image over the whole encrypted image, two common measures are used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity(UACI). NPCR and UACI can be defined using Equation 10 and Equation 11 respectively.

(10)

UACI= (11)

Where C1 and C2 are two encrypted images corresponding to two original images with subtle change *i.e*., one pixel difference. w,h are the image width and height , D(i, j) is a bipolar array with the same size as image C1 ,D(i, j) is determined using on Equation 12.

} (12)

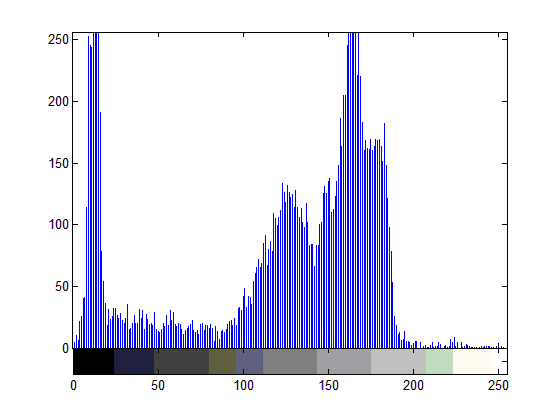
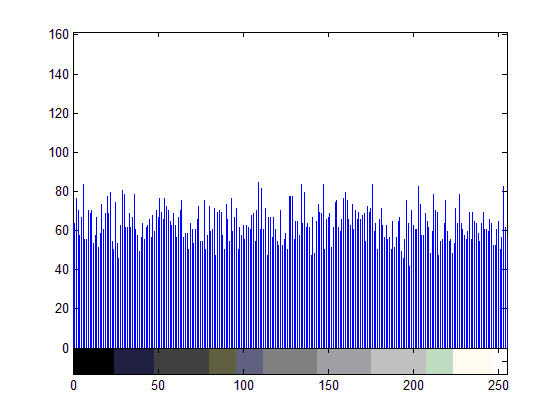
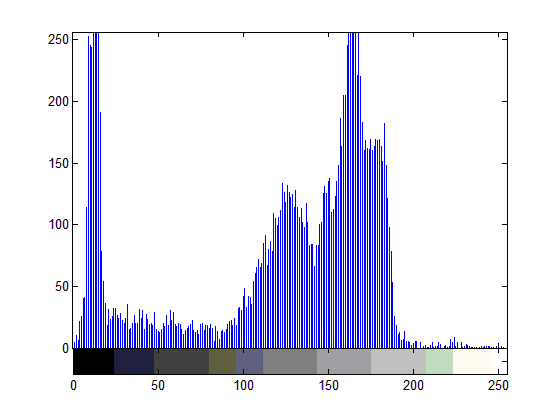
Table 3 shows the results obtained from proposed approach.

|  |  |  |
| --- | --- | --- |
| Test Image | Proposed Approach | |
| NPCR(%) | UACI(%) |
| Cameraman | 99.61 | 31.25 |
| Boat | 95.54 | 28.56 |
| Mandrill | 99.59 | 28.61 |

Table 3

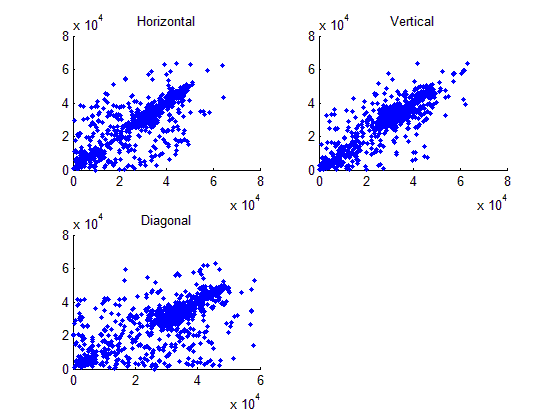
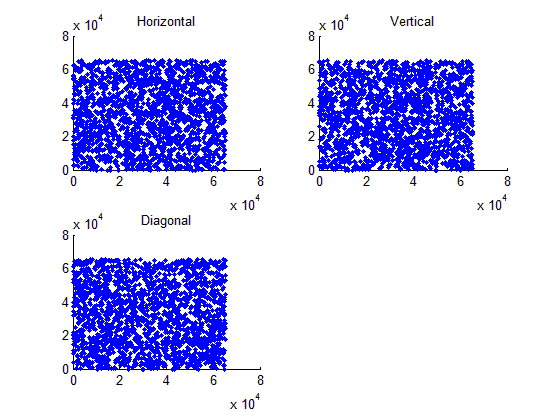
## 6.4 Histogram

The histogram of the encrypted images is significantly different from the histogram of the original images (left-shifted) and hence it does not provide any useful information to perform any statistical analysis attack on the encrypted image. Figure 5 shows an example of plotting the histogram of the original, encrypted, and decrypted along with the correlation coefficients.



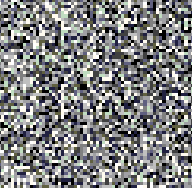
1. (b) (c)

Figure 3: This shows histogram analysis of image Cameraman (a) is original,(b) is encrypted ,(c) is decrypted

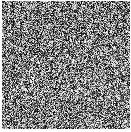
 

(d) (e)

Figure 4: This shows the correlation coefficient analysis of Cameraman(d) and encrypted (e)

(q) (p) (r)

(t) (u) (v)

Figure 5: q ,t are the original image of cameraman and boat respectively, p , u are the encrypted and r, v decrypted image

# 7.Coding Snapshot5 snap.jpg6 snap.bmp4 snap.bmp2 snap.bmp1 snap.bmp

## 8. Conclusion

The proposed work is highly resilient and robust among most other encryption approach. In this approach we have generated key using chaotic logistic map and then we have applied DNA substitution algorithm. We perform various mathematic evaluations using benchmark parameters namely correlation coefficient ,PSNR, UACI etc. and our proposed works has been proven to be quite strong against cryptographic attack. This method is lossless .This makes one of the useful method for image encryption

In future we would like to explore DNA cryptographic approach,its emerging field.

## References:

1. Chakraborty, S., Seal, A., Roy, M., & Mali, K. (2016). A novel lossless image encryption method using DNA substitution and chaotic Logistic map. International Journal of Security and Its Applications, 10(2), 205-216
2. Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. Image and vision computing, 24(9), 926-934.
3. Fridrich Jiri, Symmetric ciphers based on two dimensional chaotic maps, Int. J. Bifurcat Chaos 8 (6) (1998) 1259–1284.
4. J.C. Yen, J.I. Guo, A new image encryption algorithm and its VLSI architecture, in: Proceedings of the IEEE workshop signal processing systems, 1999, pp. 430–437
5. J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52
6. Z-l Zhu, W. Zhang, K-w Wong and H. Yu, “A chaos-based symmetric image encryption scheme using a bit-level permutation”, Elsevier Information Sciences, vol. 181, (2010), pp. 1171–1186.
7. Zhang, G., & Liu, Q. (2011). A novel image encryption method based on total shuffling scheme. *Optics Communications*, *284*(12), 2775-2780.
8. Y. Mao and G. Chen, “Chaos-Based Image Encryption”, in Hand- book of geometric computing, Springer, (2005).
9. Y. Wanga, K-W Wong, Xiaofeng Liaoc and Guanrong Chen, “A new chaos- based fast image encryption algorithm”, in Applied Soft Computing, Elsevier, (2011).
10. N.K. Pareek, V Patidar and K. K. Sud, “A Random Bit Generator Using Chaotic Maps”, vol. 10, no. 1, (2010), pp.32-38