ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

# IMAGE ENCRYPTION USING CHAOS

**Prachi S. Mankar[*1] & Prof.S.K.Nanda[2]**
[*1]Department of Electronics and Telecommunication Amravati university
[2]HOD, Department of Electronics and Telecommunication, Amravati university

## ABSTRACT

In last few decades, due to the use of internet digital information transmission has becoming the common. But while transmitting the information over the open network, the question comes out, whether it is secure or not. To maintain its security the information should be transmitted into the format which is not recognized by the third person. the process of sending the information into unrecognized form is called as encryption. This particular paper presents the idea of encrypting the image using the chaos theory i.e encrypting in complete noise format, using the theory of logistic map.

***Keywords-*** *Chaotic Map, Logistic Map, Image Encryption, Chaotic Theory, Key Sensitivity.*

## I. INTRODUCTION

A large amount of digital data is being stored on different media and exchanged on the networks. This data contains private and the confidential information. For this the techniques are required to provide the confidentiality, authenticity, integrity. Recently the technologies based on the chaos are preferred over the other technologies for the transmission of the images or data over the distances for preventing its confidentiality and integrity.. The chaos is the word derived from Greek which means the unpredictability and is also defined as the study of complicated dynamic system. Its behavior changes with the change n the initial condition or change in the initial values of the parameters (i.e . key in case of encryption techniques). In last few years the digital information sharing over the internet is the fastest development. The people keeps exchanching the secured and confidential data over the internet on the open network. So while sending the images the question arises that is of the security, where the sent information follows the cryptographic principle or not. Whether it follows integrity,confidentiality or authenticity. Some times there may be the possibility of brute force attack or the possibility of intruder to introduce any data and thus loss the integrity. This will not cause much problem in the day to day life. But this will surely affect in case of military applications. To avoid the attacks and to maintain the confidentiality of the transmitted data it is necessary to send A large amount of digital data is being stored on different media and exchanged on the networks. This data contains private and the confidential information. For this the techniques are required to provide the confidentiality, authenticity, integrity. Recently the technologies based on the chaos are preferred over the other technologies for the transmission of the images or data over the distances for preventing its confidentiality and integrity.. The chaos is the word derived from Greek which means the unpredictability and is also defined as the study of complicated dynamic system. Its behavior changes with the change n the initial condition or change in the initial values of the parameters (i.e . key in case of encryption techniques. In last few years the digital information sharing over the internet is the fastest development. The people keeps exchanging the secured and confidential data over the internet on the open network. So while sending the images the question arises that is of the security, where the sent information follows the cryptographic principle or not. Whether it follows integrity, confidentiality or authenticity. Sometimes there may be the possibility of brute force attack or the possibility of intruder to introduce any data and thus loss the integrity. This will not cause much problem in the day to day life. But this will surely affect in case of military applications. To avoid the attacks and to maintain the confidentiality of the transmitted data it is necessary to send into the coded form called as encrypted form and the process is called as encryption. In the corresponding paper we are encrypting the image into the complete form of noise .for converting the image into the form of noise we are using the chaotic map and chaotic theories. This paper is the review of different encryption process and the chaotic maps

There are different encryption schemes such as Advanced encryption standards (AES) and Data encryption standards (DES) which are the best suited approach for the text encryption. But to encrypt the image this are not suitable. Because the image is the combination of pixels and consist of bulk amount of data. So different encryption techniques need to be used.

ISSN 2348 – 8034
Impact Factor- 3.155

## II. WHAT IS CHAOS THEORY?

The phenomenon which occurs in nonlinear definable systems, which are dynamic in nature and sensitive to the initial condition gives completely random behavior is called as *chaos*. An important characteristic that has caused this phenomenon to take into consideration for many cryptographic systems is being definable despite of its pseudo-random behavior. Due to pseudo-random behavior, the output of the vision system seems random in attackers' view, while in receiver's view, the system can be defined and decryption is possible. one of the main advantages of chaotic system's realization is facilitated key management approach because this method only needs to protect and secure transmission of secret key (parameters and initial values of chaotic system), which has a little volume and therefore not only a little memory is needed to maintain it but also there is more confidence during its transfer. To state as a definition, Chaos theory is the study of complex, nonlinear, dynamic systems. It is a branch of mathematics that deals with systems that appear to be orderly (deterministic)but, in fact, harbor chaotic behaviors. It also deals with systems that appear to be chaotic, but, in fact, have underlying order. Chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions, an effect which is popularly referred to as the butterfly effect. Small differences in initial conditions (such as those due to rounding errors in numerical computation) yield widely diverging outcomes for chaotic systems, rendering long-term prediction impossible in general. This happens even though these systems are deterministic, meaning that their future behavior is fully determined by their initial conditions, with no random elements involved. In other words, the deterministic nature of these systems does not make them predictable. This behavior is known as deterministic chaos, or simply chaos. Nature is highly complex, and the only prediction you can make is that she is unpredictable.

- Pick a number, any number •
- Plug it in for x in .8x + 1 •
- Take the result and plug that back in for x again in .8x + 1 •

Repeat this processAfter some number of iterations, you should notice the list of numbers (the "orbit") convergingon a particular numberStrange attractors are shapes with fractional dimension.

The chaos theory gives the explanation for the completely insignificant factors. Its ts the theory of complicated and disputed mathematical theory. As it gives the idea or explaination about the random or chaotic occurances. Hence the name is given as chaotic theory. Edward Lorenz performed the first experiment on chaos theory in 1960.He was working with the system which gives the information about the weather. In 1961, when he started recreating the past weather sequence he started printing it in midway and printed the first three values instead of full six . this logically gives completely different sequence instead of giving the original sequence for the change of only decimal point value. However Lorenz proved that such a small factor can affect the the oveall outcome. This gives completely chaotic behavior.

## III. PROPOSED METHODS

As image is the combination of pixels so the advanced encryption standard (AES) or data encryption standard(DES) can not be use for the encryption of the image. As image consists of pixels hence it has the large data compared to text. There are different method for implementing the chaotic map. First one is *henon map* The henon map is the two dimensional map which is invertible and iterated map. The state equation is use for the representation of henon map. The state equation in combination with the chaotic attractor is used. The method of generating the pseudo- random sequences can be used to propose the Henon map. second one is *tent map*. Tent map is the iterated function in the mathematics and that is into the form of the shape of the tent and forms the dynamic system which is discrete time in nature. But all this are 1-D maps. Which does not gives the dynamic nature. Hence the 2-D map is proposed. The 2D map is the logistic map. This is the third form the chaotic map.The most simplest and well studied example of a 1D map that exhibits the complicated behavior from interval [0,1]bin to [0,1] can be explained by logistic map. The logistic map can be parameterized by μ. And given by the following equation.

$g_\mu(x) = \mu * (x)$-------(1)
The state evolution is as follows.
$x(n+1)=\mu*x(n)*(1-x(n))$-------- (2)

ISSN 2348 – 8034
Impact Factor- 3.155

Where $0 \leq \mu \leq 4$. This map constitutes a discrete-time dynamical system in the sense that the map $g_\mu$ :[0,1] ® [0,1] generates a semi-group through the operation of composition of functions. In the this map, μ is varied from 0 to 4, a period-doubling bifurcation occurs.

**Mathematical Definition**

The 2D logistic map can be defined by the following equation,where r is the system parameter and $(x_i,y_i)$ is the pair-wise point at the ith iteration.

$X_{i+1}=r(3Y_i+1)X_i(1-X_i)$----------3(a)

$Y_{i+1}=r(3X_{i+1}+1)Y_i(1-Y_i)$----------3(b)

Where r=1.19 and the initial value $(X_0,Y_0)$ at(0.8909,0.3342).

## IV. IMAGE ENCRYPTION USING 2D LOGISTIC MAP

With respect to different system parameters the chaotic map has the different behaviours. In th proposed approach we will take the value of r in the interval [1.1,1.19]. and at this aparticular interval system will behave chaotic. Figure 1 shows the flowchart for the proposed encryption method. This consist of 2D logistic permutation,2D logistic diffusion and 2D transposition.the encryption and decryption processes are inversible to each other. i.e encryption process can be written as C=Enc(P,K) and decryption can be written as P=Dec(C,K).

*1)Key And Sequence Generator*

The encryption key K can be defined into the format of 256 bit stream and has five parts $X_0,Y_0,r,T$ and $A_1,\ldots.A_8$ where ( $X_0,Y_0$)and r are the initial conditions and equation 1 defines the parameter.

*2)Permutation*

Suppose the size of plaintext image is M×N. the condition is generality should not be loss. Hence total number of pixels are MN. ( $X_0,Y_0$) is the initial value used for the round. using 2D logistic map equation 3a,3b a sequence of x and y of length MN is generated. Let the X and y coordinate sequence be Xseq and Yseq respectively. Rearrange the sequences in X and Y format. And perform the the row permutation and column permutation using the matrices

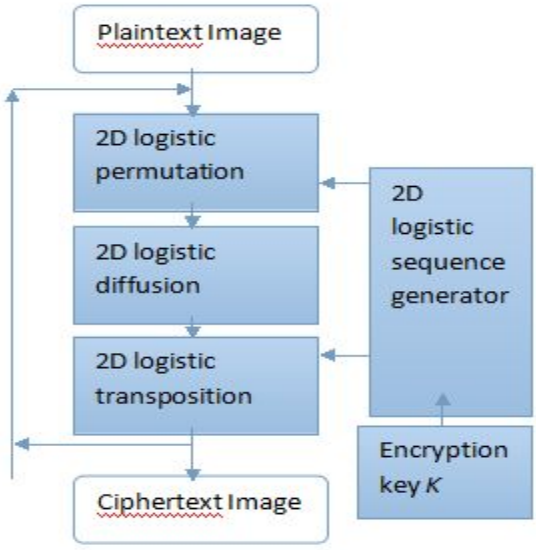


***Fig 1:flowchart for encryption of an image***

ISSN 2348 – 8034
Impact Factor- 3.155

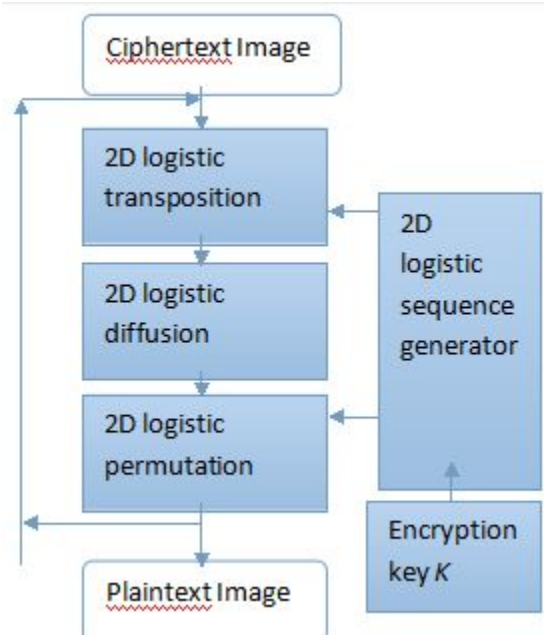


***Fig 2:flowchart for decryption of an image***

*3)Diffusion*

Using the finite Galois field($2^8$) we apply the diffusion S×S to the each block in the plaintext image.where S is the block size variable obatained by the plaintext image.

The total number of cipher rounds can be obtained by following equation

$$\#round_{min}=\log_{s\times s} M\times N=\log_2 MN/2\log_2 S$$

After the diffusion of the image the transposition is performed on the image pixels. The transposition changes the values of the pixels with respect to reference image.

## V. SECURITY ANALYSIS

*1)key sensitivity analysis*

The value of the secure cipher should depend upon the encryption key.the dependence of the cipher on the key is called as sensitivity and this sensitivity depends on two factors

-Encryption : by using the two different encryption keys k1, k2 and generate the two ciphertext images i.e C1,C2 and check out the differences of two ciphertext images by using the same plaintext or refence image.

-Decryption: by using the same ciphertext image and using two different encryption keys k1,k2 how different the two decrypted images d1 and d2 are.

*2) Histogram Analysis*

The histogram analysis is the most important method of estimating the ciphertext image.the histogram is the graph which shows the pixel value distribution. As the ciphertext image is completely chaotic it has the random distribution. Hence the histogram of the plaintext and ciphetext image can gives the analysis of the security of image.

ISSN 2348 – 8034
Impact Factor- 3.155

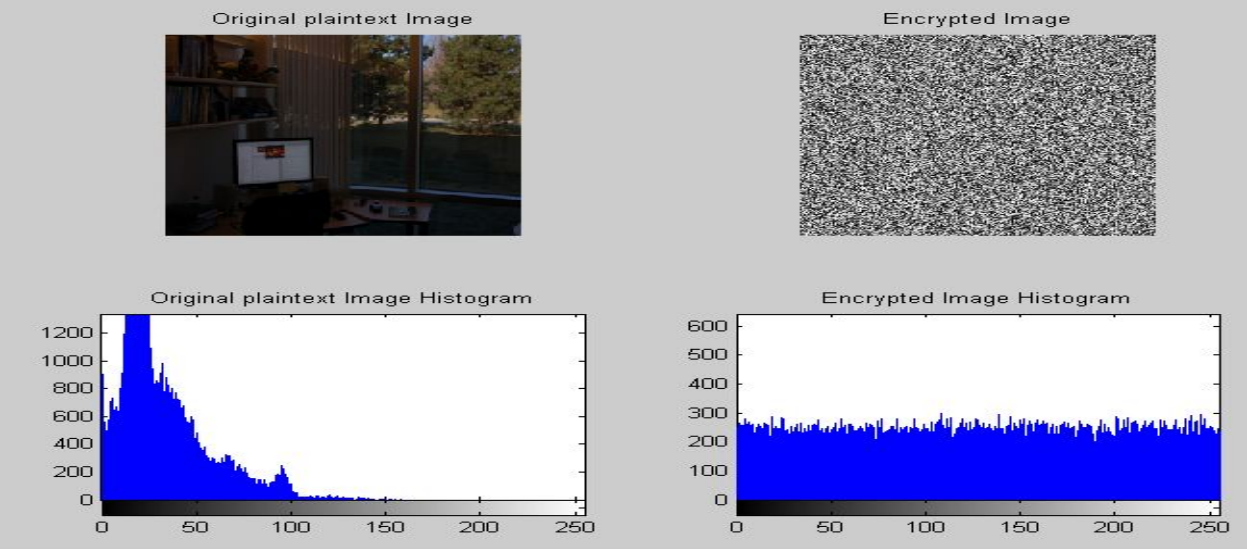


***Fig 3:histogram analysis***

## I. CONCLUSION

Compared with the other chaotic schemes and maps the logistic map gives the best suited result for the secured transmission and for the encryption process. The performed security analysis shows that the method can resist many forms of cryptanalysis.The logistic map converts the simple plaintext image into the ciphertext which is the complete noise. the ciphertext image has the complete random like structure. There is no correlation between the ciphertext and plaintext so its become difficult to analyse the plaintext from ciphertext and vice versa. The best suited result is obtained by using logistic map and AES encryption algorithm.

## *REFERENCES*

1. *G.A.Sathishkumar, Dr.K.Bhoopathy bagan,Dr.N.Sriraam," "Image Encryption based on Diffusion and Multiple Chaotic Maps" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.*
2. *Minal Govind Avasare, Vishakha Vivek Kelkar, "Image Encryption using Chaos Theory", International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, Mumbai, India,2015.*
3. *Danial Roohbakhsh, Mahdi.Yaghoobi, "Color Image Encryption using Hyper Chaos Chen", International Journal of Computer Applications (0975 – 8887) Volume 110 – No. 4, January 2015 .*
4. *Alireza Jolfaei, Abdolrasoul Mirghadri, "An Image Encryption approach using chaos and Stream cipher", journal of theoretical and applied information technology.*
5. *William stallings, ―Cryptography and Network Security: Principles & Practices‖, second edition.*