International Journal of Trend in Research and Development, Volume 4(6), ISSN: 2394-9333
www.ijtrd.com

# Image Encryption Using Chaotic Process

[1]G. Naga Raju, [2]Dr.P V Rama Raju, [3]R.L V S SSubbarayudu, [4]K.Maa Lakshmi, [5]R. S SVidyaSagar and [6]T.Parimala
[1]Asst. Professor, [2]Professor & HOD, [3, 4, 5, 6]BTech Students
[1, 2,3,4,5,6]Department of Electronics and Communication Engineering, Sagi Ramakrishnam Raju Engineering College (A), Bhimavaram, India

***Abstract*:** In modern era, digital image transmission over the internet and storage in databases has become very wide. Security is required to prevent unauthorized access to these. This is achieved by encryption-decryption mechanism. In this paper, a chaos based encryption scheme was proposed which consists of an efficient permutation-diffusion mechanism in which permuting the image pixel positions follows with diffusion i.e., changing the gray value of image pixels so that the relation between original image and cipher imageis confused. Original image is obtained from cipher image at the other end through exact reverse process to encryption, called as decryption.

***Keywords:*** *Encryption, Cipher, Chaos, Permutation, Diffusion.*

## I. INTRODUCTION

Data need to be transmitted from one place to another. For this purpose a channel is required, the channel may be secure or insecure. For secure channel, the channel itself has the capacity of protecting the data whereas for insecure channel, there is a real need to follow a separate mechanism at the transmitter and receiver end for securing the data from unauthorized access [1]. There are several data protection techniques [2] like NULL`ing out, masking data, watermarking, encryption etc. out of which encryption is the most widely used technique.Data can be of several forms like text, image, audio, video etc.. Here, we deal with image form of data. An image can be composed into pixels and can be easily processed with various systems available as of now.From [3], it can be understood that several forms of data like text, audio etc. can also be hidden in image which is one form of cryptographic process. G.NagaRaju, James Vijay proposed an algorithm [4] of hiding data in an encrypted image which shown better results for data hiding in an image.

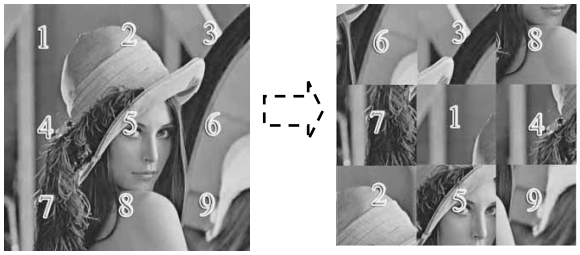
Image encryption is the process of converting original image to a cipher form which is used for transmitting over the insecure channel. A cipher image is the image in which information in original image is contained but in a form which cannot be understood by unintended persons. At the receiver end, the exact reverse process of encryption, called decryptionis performed to get original image from cipher image. The original image can also be called as plain image, from here on and the cipher image and encrypted image refers to the same.

There are several different encryption algorithms are proposed [5] till now like Image compression and encryption using scan, using secret-key images [6], using digital signature, using chaotic maps, random scrambling, Advanced encryption algorithm [7] etc

There are several encryption schemes and for our consideration, Chaotic and Non-Chaotic are two major classifications. It is found that chaotic process is advantageous [8] and is used here.

Chaos, technically can be defined as that when the present determines the future but the approximate present does not approximately determine the future [9]. Chaos has been introduced in cryptography because of ergodicity, sensitive dependent on initial condition, pseudo-randomness, structural complexity and control parameters. Chaos also has greater advantage over noise. In 1987, Edward Lorenz proposed butterfly effect; a small change in initial condition causes great changes at output [10]. There are several chaotic maps available [11] as Logistic map, Tent map, Quadratic map, Bernoulli map, Arnold map etc.. Bernoulli map is used here. These maps provide large key space, randomness in cipher image, and a good sensitivity values for initial conditions.

A chaotic based encryption scheme composed of two processes as permutation process and diffusion process [12]. Permutation is the process in which image pixels are shuffled i.e., each pixel is rearranged randomly. It is the process of clipping and splicing that realign the pixel matrix of digital image. The randomness of shuffling depends on the type of mapping function used and the initial and control parameters used in the mapping function. Permutation can be certainly understood from the figure1.




(a) (b)

Fig1: Images before (a) and after (b) permutation

In diffusion process, each pixel is processed and its gray value is changed according to a function. The randomness of diffusion depends on several factors like the mapping function, diffusion transformation, number of iterations of the function, generated keystream which also depends on plain image etc. The diffusion can also be understood as Linear Feedback Shift Register etc. as in [13]. Comparing various encryption techniques [14], it is found that chaotic scheme and that too Bernoulli shift mapping is better of all and the same is used here.

The paper is organized as follows. In section II, methodology was proposed clearly. Section III shows the obtained results after simulation for various images. Thereby concluded and the future scope given in section IV. The set of references are cited in section V.

## II. METHODOLOGY

The methodology for this chaotic encryption and decryption can be understood from the block diagram shown in figure2.The entire process can be mainly classified as encryption and decryption. The encryption process can be subdivided as permutation and diffusion. Permutation can be further be divided into blocks as iteration, sorting, permutation, reshaping. Diffusion is further divided into blocks as initialization, quantization, diffusion transformation, cipher

image. Decryption has exact reverse alignment. The blocks are clearly explained later on.

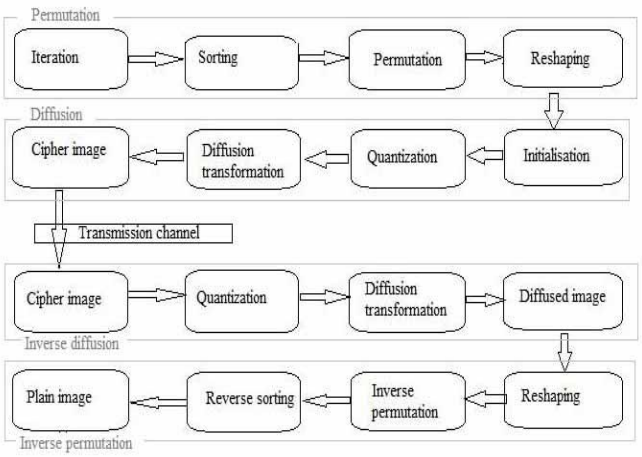



Figure 2: Block diagram for proposed chaotic encryption and decryption

The process consists of first loading or extracting the required image to be encrypted. The process for encryption can be broadly classified into two parts as Permutation and Diffusion.

**Permutation:**

In permutation phase, image is shuffled i.e., position of pixels are changed according to a procedure as follows.

1.*Iteration:*The initial values and control parameters for the mapping function are first initialized. Bernoulli shift map is used here and the function is iterated on image to obtain a truncated orbit. Bernoulli map can be illustrated from the function.

$$x_{i+1}=(a.x_i))\text{mod}(1)$$

where a is initial value and $x_1$ is the control parameter.

2.*Sorting:* The orbit obtained from iteration is sorted(in ascending order) to find out the index order sequence

3.*Permutation:* Firstly, the plain image is converted into a vector i.e., a single row one and then it is permuted. Permutation here means that the vector is rearranged according to index order obtained after sorting.

4.*Reshaping:* The permuted image is converted into 2 dimension according to row (or column) to get shuffled image.

**Diffusion:**

In diffusion phase, for the permuted image, the value for each pixel is changed. The procedure for diffusion consists of following

1. Initialisation: The initial values and control parameters used for diffusion process are assigned.

2.Quantisation: Each pixel is selected and for the pixel, quantization formula is applied to get the random gray value ( of 8 bit length) i.e., the pixel gray value rounded off to a random number according to the quantization formula. The quantizatin formula is

$$d(i) = \text{floor}(l.y_i).$$

where$y_i$ is the initial value for quantization and l indicates color level.

3.Diffusion transformation: A two point diffusion transformation is applied i.e., the permuted image and diffusion parameters compared according to a function (xor) to obtain gray value i.e., diffusion for the pixel. The diffusion transformation formula is

$$C(i+1) = S_i\text{xor}[(d_i+C_i)\text{mod}256].$$

Where the initial value $C_i$ can be copied from $d_i$ and $S_i$ indicates gray value of $i^{th}$ index in vector converted form to the permuted image

The Bernoulli map for $t_i$ with b as control parameter and $t_1$ as initial value is iterated j ($j=1+[C_{i+1} \text{ mod } 2]$) times to generate key stream which depends on plain image. The above steps are repeated for all the pixels of the image.

4. Cipher image: A cipher image or the encrypted image is thus obtained.

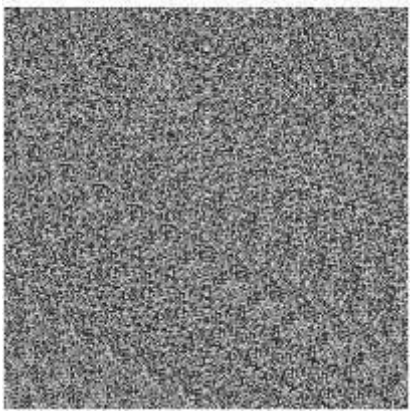
The Cipher image is used for transmission over the channel. Decryption is the reverse process of encryption.The exact reverse steps for encryption process are followed with same key , initial values and control parameters must be used to correctly decrypt the encrypted image or to get original image.

## III. RESULTS

The results obtained are shown in figure3 and figure4 when the two images lena image and cameramanimage are simulated using the mentioned scheme with values as a=1.16, b=5.93, $x_1$=0.61, $y_1$=0.26. The results shown are for specific inputs of initial conditions and control parameters only and the output will vary with variation in these parameters.

Plain image

Permuted image



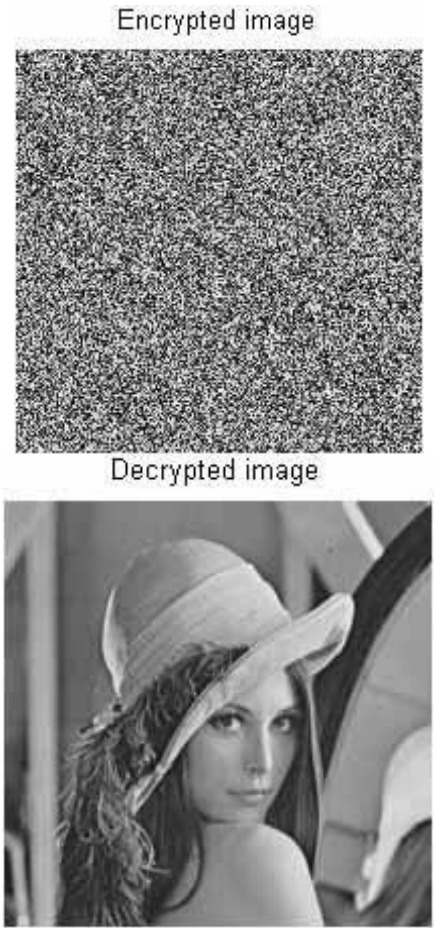



Fig3: Results for lena image

The proposed scheme when applied for cameraman image, the results are as shown in figure 4.

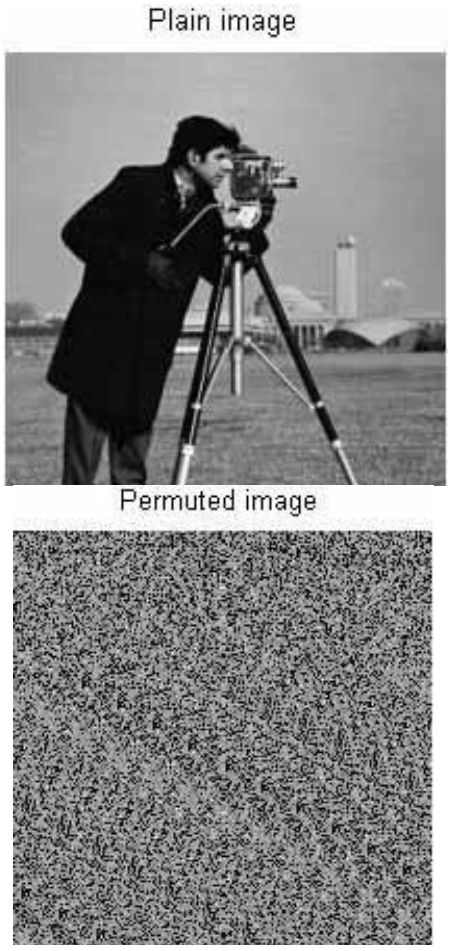




Figure 4: Results for cameraman image

## IV. CONCLUSION& FUTURE SCOPE

Thus, an efficient image encryption scheme is presented here with various advantages of large keyspace, good statistical property, secret key sensitivity etc. and can be used whenever security is required. However, if security is not in concern like for broadcast applications, it is not recommended to use any of the encryption techniques as that is an extra requirement of equipment and algorithms.The process can be further developed so that several parameters we enter manually i.e., initial and control parameters etc., can be obtained through a process from a shortened single key which includes efficient number of intakes.

### *References*

[1] Willian Stallings, Cryptography and Network security principles and practices.: Prentice Hall, 2010
[2] B.Schneier, Applied Cryptography, USA, 1996
[3] M.S. Baptista, Phus. Let. A 240
[4] G. Naga Raju, James Vijay, "Secret-key based Separable Reversible Data-Hiding in Encrypted image,"National Conference on VLSI, Signal processing & Communications NCVSComs-2011.
[5] Rinkipakshwar, "A survey in different image encryption and decryption techniques", International journal of computer science and information technologies, Vol. 4 (1) , 2013, 113 – 116
[6] G. Nagaraju and T. V. Hyma Lakshmi, "Image encryption using secret-key images and SCAN patterns",International Journal in Advances in computer, Electrical,& Electronics Engg., Vol. 02, 2012, pp. 13-18
[7] Ramaraju PV, Nagaraju G, Chaitanya RK. Image Encryption and Decryption using Advanced

EncryptionAlgorithm. Discovery, 2015, The International Daily journal, ISSN 2278 – 5469 EISSN 2278 – 5450, 29(107),Pp:2-28
[8] Behrouz A Forouzan, Cryptography and Network security. California, USA: tata McGraw Hill Education Private Limited, 2011
[9] Christopher M Banforth, Mathematics of Planet Earth, April 2013
[10] J. gleick, Chaos Making a New Science., 1987
[11] G.A.Sathishkumar, Dr.K.Bhoopathybagan, 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
[12] Ruisong Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism" Springer-Verlag Berlin Heidelberg, pp. 32-39,2011
[13] Rohit S, K N Haribatt, A nandini Sharma, "Image encryption and decryption using chaotic key sequence generated", Advances in electronics, computers and communications(ICAECC) pg.1-6, October 2014
[14] M Bin Younas, Jawad Ahmad, "Comparative Analysis of Chaotic and Non-chaotic Image Encryption Schemes." Dept. of EEE, HITEC University.

**ABOUT AUTHORS:**

**Dr. P. V. RAMA RAJU**

Presently working as a Professor and HOD of Department of Electronics and Communication Engineering, S.R.K.R. Engineering College, AP, India. His research interests include Biomedical-Signal Processing, Signal Processing, Image Processing, VLSI Design, Antennas and Microwave Anechoic Chambers Design. He is author of several research studies published in national and international journals and conference proceedings

**G. Naga Raju**

Presently working as assistant professor in Dept. of ECE, S.R.K.R. Engineering College, Bhimavaram, AP, India. He received B.Tech degree from S.R.K.R Engineering College, Bhimavaram in 2012, and M.Tech degree in Computer electronics specialization from Govt. College of Engg., Pune university in 2004. His current research interests include Image processing, digital security systems, Signal processing, Biomedical Signal processing, and VLSI Design.

**R. L V S SSubbarayudu**

Presently pursuing Bachelor of Engineering degree in Electronics & Communication engineering at S.R.K.R. Engineering College, AP, India

**K. Maa Lakshmi**

Presently pursuing Bachelor of Engineering degree in Electronics & Communication engineering at S.R.K.R. Engineering College, AP, India

**R. S. S.Vidyasagar**

Presently pursuing Bachelor of Engineering degree in Electronics & Communication engineering at S.R.K.R. Engineering College, AP, India

**T. Parimala**

Presently pursuing Bachelor of Engineering degree in Electronics & Communication engineering at S.R.K.R. Engineering College, AP, India