DOI: 10.21917/ijivp.2020.0329

A NOVEL APPROACH TO IMPROVE IMAGE STORAGE AND SECURITY BY USING CHAOTIC IMAGE ENCRYPTION METHOD AND LOSSLESS COMPRESSION METHOD

Pradheep Manisekarana, Prachi Dhankhar, and Parveen Kumar

Department of Computer Science and Engineering, NIMS University Rajasthan, India

Abstract

In present day life, even common men share confidential information among themselves through social media. This research work could be developed as a plug-in module which performs encryption and decryption and added to those presently available apps. This ensures a high-level end to end encryption. Besides the encryption performed in Adhoc networks where local nodes are interconnected to establish a communication, this research proposal could be added into the existing encryption layer. Such embedded encryption would increase the security levels in industries whose processes are controlled and operated via WIFI networks. Even RFID reader and tags could enjoy this encryption scheme. In chaotic based systems, usually logistic maps are used and the lattice values are modified through several iterations and finally forms a spatio-temporal system. Since linear coupling of lattices results in easy guessing of pixels, non-linear coupling is getting popular among chaotic based encryption systems. Such non-linear spatio-temporal chaotic systems are able to provide sufficient amount of security to the host image. However, intruders have their own way to decrypt either using 'Trial and Error' methods or through mathematical analysis of the encrypted images. So, the task of the researcher is to improve the chaotic metrics ideally by realizing the key space (to be of infinite size) and zero amount of information to be stolen except the encrypted pixels in the hands of intruders. Further decryption by the intended users is still a challenge even though the keys are known because; the quality of the host image should be preserved. Another challenge to the researcher is, to perform compression in order to save the storage area in concerned servers. Naturally compression and decompression are considered to be a valid attack on encryption methods. But in our Case, compression is done intentionally for saving storage area and bandwidth.

Keywords:

Chaotic Systems, ACGLML, Bifurcation Diagram, Arnold's Cat Map, Lattice Variation

1. INTRODUCTION

Chaos systems characterized by its ergodicity, quasi randomness, dependency on initial conditions have been originally popular and under research since 1970. By basic nature of encryption systems, it is understood that conventional encryption methods work on finite set of integers or fractions, whereas chaotic systems work with infinite set of numbers which could be used as a better key space. Hence data undergoes proper shuffling and diffusion is considered to be strongly encrypted content. Linear chaotic systems always suffer from periodic windows and hence non-linear chaotic systems are introduced in order to impose difficulty in guessing the pixel values. Encryption of images has been shown with two maps taken into account. Arnold's cat map (permutation phase) and Chirikov map (diffusion phase).

In this world of digital era, human life and all the luxuries of modern life fully depends on multimedia content and its sharable nature via various social websites and social apps. This has pushed the people to use more amounts of multimedia data and transmit via internet channels. This sharing of multimedia data is expected to be a prime source of revenue for corporates (in the order of several billion USD). Hence, it is essential for them to protect and maintain the present communication environment and the foremost role would also to improve the present scenario in various aspects such as storage required and time for uploading and downloading the information. A standard method of compression and decompression is shown in Fig.1.

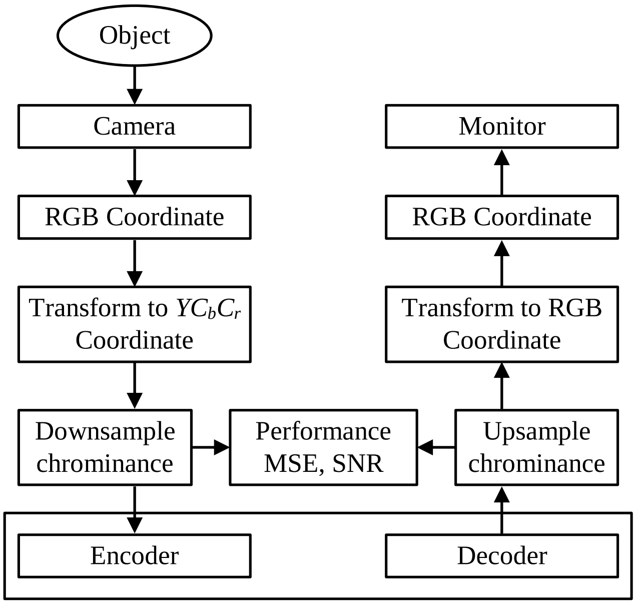

Fig.1. Image Storage System

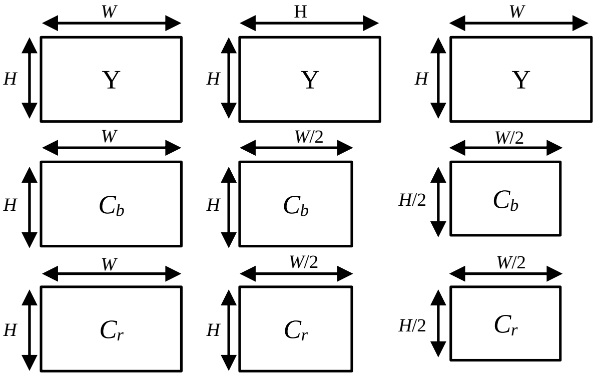

Fig.2. Chrominance Down Sampling Formats

An image acquired from conventional camera is of RGB format. The same is converted into YC_bC_r format. Since the chrominance components less affects the visual quality, down sampling is done on it. Finally encoding is done and stored in the HDD (Hard Disk Drive). While decompression is done, the data stream from the hard disk is taken in serial format and decoded and only chrominance components are further up-sampled. In order to visualize the image after decompression, it is transformed into RGB format and seen on the monitor display. Most of the popular applications including Microsoft paint works on this concept. While saving the image in a computer system it is converted into relevant format and stored in Hard disk through serial binary format. Similarly, when the image is clicked to open it, full decoding algorithms are performed from the binary stream obtained from the hard disk. However, the types of algorithms are based on the compression standards and image formats.

The color components Y, C_b and C_r of color image are defined in YUV format, where Y is the luminance and C_b, C_r are called as chrominance components. The color format conversion from RGB to YC_bC_r co-ordinates is done as per the equation given below.

$$\begin{pmatrix} Y \\ C_b \\ C_r \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.334 & -0.500 \\ 0.500 & -0.419 & -0.081 \end{pmatrix}\begin{pmatrix} R \\ G \\ B \end{pmatrix} + \begin{pmatrix} 0 \\ 128 \\ 128 \end{pmatrix}$$

The same equation is rearranged and used again to transform in reverse into its corresponding RGB components. Three different types of down-sampling the YC_bC_r are shown in Fig.2.

Image compression could be explained in an easy way. An image in its original format is first converted into a series of binary stream. This binary stream is encoded using some standard formats and stored in hard drives. Whenever needed, the same is decoded and displayed on the monitors. If the number of encoded bits is less the total number of bits in the original format, then it is understood that the image is compressed.

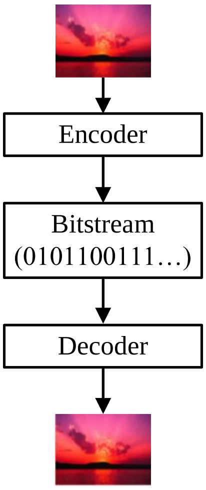

Fig.3. Compression flow

The Compression ratio is defined as follows:

$$Cr = n_1/n_2 \tag{1}$$

where n_1 is the data rate of original image and n_2 is that encoded bit-stream.

The performance of the compression is evaluated based on the following metrics, namely Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

$$MSE = \sqrt{\frac{\sum_{x=0}^{W-1}\sum_{y=0}^{H-1}\left[f(x,y)-f'(x,y)\right]}{WH}} \tag{2}$$

where $f(x,y)$ is the original image and $f'(x,y)$ is the decompressed image.

$$\text{PSNR}=20\log_{10}255/\text{MSE} \tag{3}$$

It is understood that if $PSNR$ (in dB) is less, then the reconstruction is very poor. In Case if both the images are same, then it would lead to an infinite dB, as MSE in denominator is zero. Encoding scheme of an image compression system is shown in Fig.4.

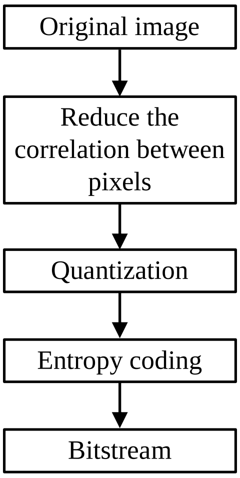

Fig.4. Typical encoding process

In order to reduce the correlation among the pixels of the original image, predictive coding, orthogonal transform and sub band coding methods are popularly used.

1.1 COMPRESSION METHODS

In compression process, few factors to be analyzed and considered to maintain the effectiveness of compression. The major task being the redundancy in original image, it needs to be eliminated.

- *Psycho-Visual Redundancy*: This is related to the visual experience of human beings. Normally in images, some portion of the image would least attract the viewers. So removing some part of the information in those relevant areas would not affect the visual experience of the human beings when the image is reconstructed.
- *Inter-Pixel Redundancy*: This type redundancy is very difficult to reduce. This involves complex mathematical operations to find the statistical relationship among the neighboring pixels.
- *Coding Redundancy*: This is removed using some variable length code schemes such as Huffman coding and arithmetic coding.

Broadly speaking compression methods are of two types namely: Lossy compression and Lossless compression. In lossy compression methods a compression ratio of more than 50:1 is achieved as it allows some amount of information to be lost. But in lossless compression schemes 2:1 is commonly available compression ratio. The block diagram of lossy compression method has been shown in Fig.4.

1.1.1 Lossy Compression Methods:

Generally, most lossy compressors are three-step algorithms, each of which is in accordance with three kinds of redundancy mentioned above.

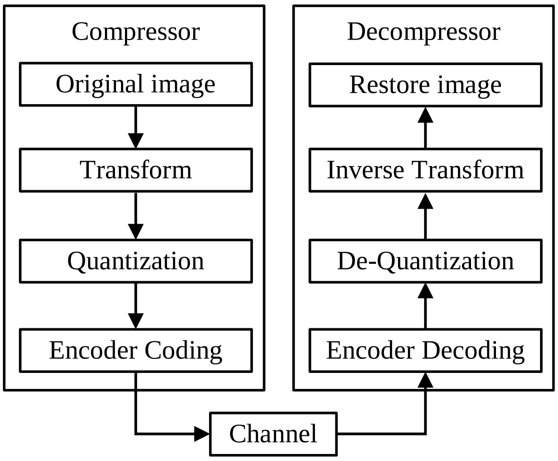

Fig.4. Simplified flow of Lossy Compression

- *Quantization*: Many to one mapping is called as quantization which is of two basic types namely Scalar and vector quantization. Scalar quantization performs mapping on each value of the pixel, whereas Vector quantization performs mapping on block of pixels with the index is maintained in a code book. At the decoder end, original pixels are retrieved by simply verifying the codebook.
- *Transform Coding*: This is realized using numerous transforms such as KLT (Karhunen-Loeve transform), Discrete Fourier transform, Discrete wavelet transform. Many earlier works have used these transforms to attain a better compression standard.

1.1.2 Lossless Compression Methods:

These methods involve two steps process. The first step takes care of reducing the inter-pixel redundancy and the second step performs entropy encoding which removes the coding redundancy. Decompression is just a reverse process of compression. The schematic of the compression and decompression is shown in Fig.5. Usually non-commercial images such as medical images are compressed using these methods. Any loss in image data is very serious and it would lead to misinterpretation of image information. Anyhow, up to 50% compression is possible under this lossless scheme.

Many researchers have investigated the lossless compression schemes and could get bit rate of about 4 to 6 BPP through various entropy coding methods. Lossless compression methods too need measurements to evaluate the performance. Since the loss is zero, PSNR obtained would be unquestionably infinite. Hence only parameter to be measure is its compression ratio. A convenient method is to express it in terms of BPP which is independent of data storage format.

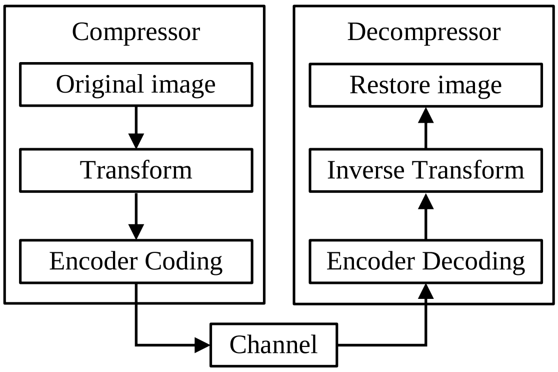

Fig.5. Lossless image compression

This paper has given an idea on two categories of compression, lossy and lossless. Basic terminologies in compression have been defined. Basic schemes of compression have been diagrammatically shown for a better understanding. The compression scheme fully relies on reducing the redundancy in pixels in such a way it does not affect the visual quality of the images. As on time, most popular compression method followed worldwide is JPEG 2000 standard. The working concepts of JPEG and JPEG 2000 have been pictorially shown. Filter bank structures of discrete wavelet transforms have been analyzed in detail. It is understood that discarding the high frequency features during the reconstruction of the image is the main cause for image compression.

2. LITERATURE REVIEW

Earlier researches have always been inspiring and motivating to improve the existing methods of encryption and compression. This section presents a review of various literatures related to our problem statement. In order to clearly analyze the literatures, an expanded survey has been conducted based on titles given the following subsections.

Since color images are the commonly acquired image capturing process, it is valuable to transmit the full color information without missing any information of it. Earlier methods were used to convert the color image into gray and reproduce as gray image at the receiver end. This is not a fully satisfactory image correspondence. Hence works done in paper uses a logistic map and LSB concealing algorithm. Three chaotic sequences are used for standard three layers of R, G and B. After performing this, a bearer image is used to carry the encrypted image using LSB concealing algorithm. This method could offer a good integrity with high speed and key space to achieve this was found very less [3].

Here logistic maps were applied in two stages. First step is to permute the pixel values of the raw image. In the second step, the logistic equation was used for diffusion. A correlation coefficient of 0.0013 was achieved with a small key space and provided good security against diverse attacks.

At this moment, it is necessary to discuss on linear and non-linear coupling of lattices in chaotic systems. In linear coupling, the lattices are coupled with neighborhood lattices and this gives an easy way to predict it by the attackers. This happens because of periodicity introduced in linear coupling. Due to this periodicity, mutual information among the lattices also increased which is a Fig.of demerit in encryption. So some researchers have worked towards non-linear coupling of the lattices and both diffusion and permutation were used. Each color layer first undergoes both single pixel and block pixel diffusion. After diffusion process, the three layers are permuted with interdependency between the pixels of three layers. This was robust and faster than the existing AES algorithm. This method was highly suitable to transmit and preserve the complex images, as any misinterpretation in image information would lead to lethal effects [4].

A simple algorithm was proposed where the color image is partitioned into various blocks in each layer of color component. These blocks are further changed by performing exclusive OR operation on this pixel values. A key of maximum 2120 had been used. Anyhow this method suffers from less security and less key space [5].

Shifting of rows and columns using hash function in an image was proposed to encrypt the image. But the consistency obtained was less from outsider point of view and it is well understood from the correlation value of -0.0078. All the operations were performed after partitioning the image into 3×9×3 pixels [6].

Almost similar work was also done which is still another modified work of AES. Hash function is used to create a shift table to alter the image blocks. These shifted blocks further undergo AES encryption algorithm. NPCR and UACI values obtained are 99.6689 and 27.7599% respectively [7].

In order to attain confidentiality while transmitting high end images such as satellite images, medical images etc., confusion based methodology has been widely recommended. Among plethora of works done, permutation-diffusion methodology also utilized the same structural planning for efficient encryption [8]. Differential attacks were well managed using this methodology. It also presents an optical color image cryptosystem based on spatial multiplexing system and stage truncation operation is proposed. The proposed method could maintain the non-linear characteristics and hence it could mitigate the different types of existing attacks especially iterative attack [9].

Few papers used DWT (discrete wavelet transform) and logistic map for the purpose of encryption. The wavelet coefficients obtained in low pass band were sorted using PWLCM. Once the image was transformed to spatial domain using IDWT, 2D logistic map was used to diffuse the content and further 'XOR'ed in spatial domain. The method was highly suitable for remote sensing image such as satellite images, which holds high end information [10]. This method was found resistant to brute force, differential and statistical attacks along with large key space.

A combination of genetic algorithm and chaotic function has been used for a betterment in image encryption scheme. This method is just like using a conventional genetic algorithm where the initial population was constructed using the encrypted image [11]. The last stage of better encryption stage was obtained by means of optimizing the quality metrics by using traditional optimizing procedure carried over in GA. Entropy and correlation coefficient obtained by using this method are 7.9978 and −0.0009 respectively.

The method as explained below was used to perform a better encryption. Initially the image is portioned into blocks of 8x9x8 pixels. Next, each block is converted into frequency domain by applying Discrete Cosine Transform. Thirdly, quantization is performed using Zigzag scan and then by applying AES encryption method. This method could give a key space of 2128 and it was very sensitive to even a small change in the key [12].

3. PROBLEM STATEMENT

The biggest challenge in presenting its purpose is to solve the latest ineffective methods of cryptography. The following are the main threats to this field of study: key space, approaches to discourage the intruders, image rebuilding quality obtained after decrypting the image and storage space needed to handle the bulk volume of data.

It is also known that the principle reasons for this study is an effective approach that consecutively performs encryption and compression. Instead of a hybrid algorithm, also a serial step-by - step encryption and compression system is also adequate, given that the total security standard for digital data access has been improved as the cloud environment has expanded. There are two types of compression and decompression processes, respectively, Lossy and Lossless. In the case of satellites and hospital images, lossy compressions are less essential. Lossy compressions are actually linked to various frequency transformations which discard information at high frequencies for better compression. Hence a recommendation to use classification methods to distinguish features that are less meaningful and more important in the image, which will reduce the losses that occur in current compression methods. In addition to the chaotic metrics, the compression ratio and image reconstruction quality is important and hence retrieved image could be used by legitimate users. This work has been focused mainly towards the encryption process, along with a lossless compression.

Yet another problem exists in the observation of the Space-Amplitude diagram. The dynamic variation of lattice values over several iterations and their ranges are very important in Space-Amplitude diagram. As a first step in encryption 100 lattice values are initialized randomly and then iterated using logistic map. Each lattice value for example, a random value of 0.4876 is an i^{th} lattice value and then it is modified as per the logistic equation followed in encryption scheme. The dynamic range is between 0 and 1. But, the effectiveness of the algorithm is fully based on the variation between the two extreme ends. Most of the algorithms fail to give this extreme dynamic range. In fact, this problem has never been addressed elsewhere. More the range, more the haze is a basic understanding. If the number of iterations performed using a logistic equation tends to infinity, the ranges are wide. However, by the nature of equations, the range could not be obtained in ACLML method.

In order to evaluate this performance based on the larger range, a new metric is to be introduced. From the visual appearance, it is difficult to catch the complete turbulence towards vertical axis. Calculating the Standard deviation of the i^{th} lattice value could be a proper choice.

4. MATERIALS AND METHODS

Arnold's cat map named after Vladimir Arnold who did researches since 1960 by using a cat image, to modify its original content. The Fig.6 shown below is a simple example to show how chaos theory is applied to images for encryption. Original image shown in iteration 1 is modified after shuffling the image pixel locations. After the iterations, 3,132, 211, 240, 275 and 299 the image attains its original view. This variation in various iterations between 1 and 300 appears to be random when a mathematical equation given below is followed. But is should be emphasized that the image is always predictable when a one knows the size of image and number of iterations. During some initial iteration, the image seems to be sheared and wrapped, but after some considerable number of iterations, the pixels in the image appear to be random by visual experience. The Fig.6 shows how the cat image is modified based on the number of shuffling iterations.

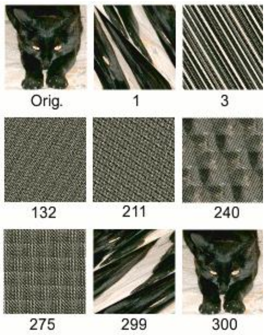

Fig.6. Permutation results of cat image

The permutations are carried out as per the following steps:

Step 1: $T^0(x,y)$ = initial image(x,y); n=0,

Step 2: $T^1(x,y) = T^0$(mod($2x+y$, N), mod($x+y$, N)); $n=1$,

Step 3: $T^k(x,y) = T^{k-1}$(mod($2x+y$, N), mod($x+y$,N)); $n=k$,

Step 4: Output image(x,y) = $T^m(x,y)$

It is seen that the determinant of Arnold map matrix should be equal to one. In such a way the values of x and y are chosen. Also, it is found that the maximum number of iterations to restore the original image never exceeds 3N.

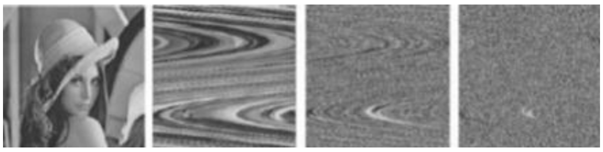

Fig.7. Encryption of Lena image (permutation alone)

It is seen that the original ‘Lena’ image is fine without any iterations. When it is iterated based on the permutation steps mentioned above, the correlation among the pixels slowly get reduced as seen in Fig.4.2. Unfortunately, the histogram obtained for the gray level ‘Lena’ image is same even when it is shuffled to any number of iterations. This is because; only the pixel locations are modified and not the values of the pixel intensities. So diffusion becomes mandatory now.

Yet another way of explaining chaos in diffusion process is presented below. It is a global phenomenon which is present in non-linear systems which are sensitive to initial conditions and have random like performance. One dimensional chaotic map is represented as

$$X_{n+1}= f(X_n) \tag{1}$$

where f is a continuous map in the interval 0 to 1. Chaotic maps are iterated with some initial values are coupled to neighborhood and non-neighborhood lattices. The performance not only depends on the initial values but also on the coupling parameter. Fig.8 shows pictorially, how the image stream values are modified.

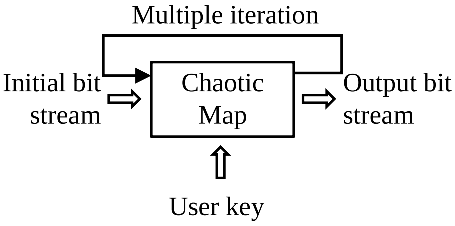

Fig.8. Iterations using Chaotic map

Every image encryption system has following two stages: Image transformation and encryption as mentioned in [13]. The method given in [14] uses Chirikov mapping

$$a_{i+1}=(a_i+b_i)\text{mod } 2\pi \tag{2}$$

$$b_{i+1}=(b_i+K \sin (a_i+b_i))\text{mod } 2\pi \tag{3}$$

where K is the control parameter satisfying $K > 0$, and the ith states a_i and b_i both take real values in [0, 2π) for all i. For $K = 0$, the map is linear and only periodic and quasi-periodic orbit exist. Nonlinearity of the map increases with K and ensures the possibility to observe chaotic dynamics for appropriate initial conditions. For a satisfactory performance K should be kept higher.

In order to incorporate Chirikov standard map for encryption purpose operated on a finite set, initially it should be a discrete function. The discretized version Chirikov standard map can be obtained by changing the range of (x,y) from the [0,2π]*[0,2π] to discrete lattice N×N.

$$x_{i+1}=(x_i+y_i)\text{mod } N \tag{4}$$

$$y_{i+1}=(y_i+K \sin (2\pi x_{i+1})/N)\text{mod } N \tag{5}$$

where N is the width of the square image and K is a positive integer.

Inverse Ciphering is also done easily by following the following equations

$$x_{i+1}=(x_i-y_i)\text{mod } N \tag{6}$$

$$y_{i+1}=(y_i-K \sin (2\pi x_{i+1})/N)\text{mod } N \tag{7}$$

Table.1. NPCR and UACI for various images

Images	**Expected (%)**	**Bit level encrypted image (%)**	**Pixel level encrypted image (%)**
NPCR			
Camera man	99.6093	90.3289	99.5376
Onion	99.6093	98.6914	99.4567
Elaine	99.6094	97.9690	99.5308
UACI			
Camera man	33.4635	26.8856	8.073
Onion	33.4635	28.7962	11.088
Elaine	33.4635	30.2466	15.074

A key space of $2^{448} \simeq 7.26\times10^{134}$ was gained while using Colpitts and Duffing oscillators to encrypt the standard images of Lena, Mandrill and Clown**.** The basics of such oscillators have been well presented in [15] and their Lyapunov exponents obtained on pictorially shown in Fig.9 and Fig.10. The Duffing's and Colpitts equations are non-linear, non-autonomous equations. They exhibit Chaos properties verified by their bifurcation diagrams and Lyapunov exponents.

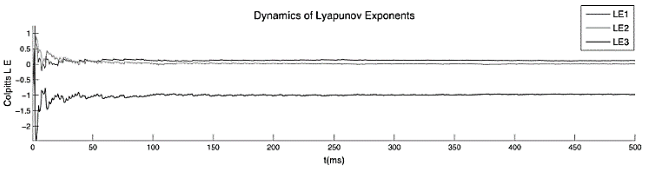

Fig.9. Dynamics of Colpitts Lyapunov Exponents

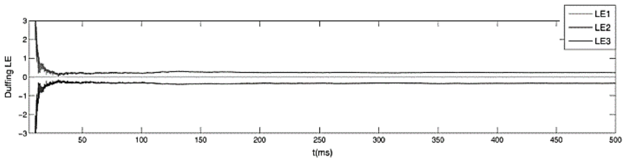

Fig.10. Dynamics of Duffing Lyapunov Exponents

The concept of chaos is applied in encryption as seen in various earlier works. It is essential to show how exactly the chaos theory is applied. Iterative modification in the pixel values as seen in Fig.4.3 whose logistics equations reach chaos for particular values of coupling coefficients and other keys. This is the significant factor to apply chaos for encryption. This chapter provides a sufficient proof that how chaos theory could be to encrypt images with different logistic equations which are the choices of interest of the system designer.

5. PROPOSED MODEL

As the problem is very clear, further progress is to work on a novel proposal implemented in this research work. Chaotic metrics and image quality metrics are dealt separately to prove the ability of the proposed algorithm. Further analysis relies on key sensitivity. To show the results properly, two types of images, gray and color have been considered and various parameters are evaluated in the following subsections. The metrics evaluated for color image are average of three different layers R, G and B.

5.1 CHAOTIC METRICS

Basic metrics are related to the calculation of time consumed for encryption, decryption, compression, decompression. Compression and decompression time include the classification time while doing feature selection. In addition, the following are the metrics to be evaluated and improved in our proposal to find the suitability of the proposed encryption and compression algorithm in real time.

5.2 MUTUAL INFORMATION

In chaotic based systems, the keys are considered as lattice values and based on those lattice values, original image encrypted based on logistic maps. The chaotic behavior of logistic maps depends on the lattice values in the range of 0 to 1, λ and ε. After successful number of iterations, when the lattice values are modified to new values which have been originated from its initial lattice values, it is essential to calculate the mutual information among the lattices. When the total number of lattices are taken as 100, then the mutual information value between most of lattices in [16] is zero except for 10 lattices, which indicates that time series of most lattices in [16] are independent. This feature is suitable for encryption because the chaotic series in a lattice cannot be recovered by other lattices. The mutual information is given in Eq.(8) as given below:

$$I(x(i);x(j)) = H(x(i))-H(x(i)|x(j)) \tag{8}$$

where

$$x(i)=(x_1(i), x_2(i), x_3(i),\dots,x_n(i)),$$

$$x(i)=(x_1(j), x_2(j), x_3(j),\dots,x_n(j))$$

i, j are the different lattices ($1\leq i,j\leq L$). It is essential to reduce the mutual information in any pairs of lattices to zero.

5.3 IMAGE QUALITY METRICS

- *Peak Signal to Noise Ratio (PSNR)*: It is defined as the ratio of the maximum possible power of the signal to the power of intruding noise which affects the fidelity of the system. *PSNR* needs Mean Square Error (*MSE*) to be calculated first. Given an original monochrome image *I* and its reconstructed approximation *K* then, *MSE* is calculated as given in Eq.(9).

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j)-K(i,j)\right]^2 \tag{9}$$

The *PSNR* (in dB) is shown in Eq.(10) and steps to calculate it is given below.

$$PSNR = 10\log_{10}\left(\frac{(MAX_I)^2}{MSE}\right)$$

$$= 20\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

$$= 20\log_{10}(MAX_I)-10\log_{10}(MSE) \tag{10}$$

- *Compression Ratio*: It is given by the ratio of size of uncompressed image to the size of compressed image.

Compression Ratio = (*Uncompressed Size*)/(*Compressed Size*)

Thus, an image with original size of 20 MB and when compressed to 2MB would result in a compression ratio of 20/2=10, expressed as a ratio, 10:1.The metric is not applicable to check the encryption performance but only to the compression performance. So total memory space saved can be defined as the reduction in size relative to the uncompressed size:

Space savings = 1-(*Compressed Size*)/(*Uncompressed Size*)

Thus, a representation that compress a 20 MB file to 2MB would be a space of 1-(2/20) = 0.9 expressed in percentage as, 90%.

In chaotic encryption schemes, the important downside is the key space. Although the chaotic nature in the bifurcation diagrams is disturbed by the periodic windows at particular λ values in Eq.(11).

$$x_{n+1} = \lambda x_n(1-x_n) \tag{11}$$

where θ is the number of iterations θ =1,2,…,n. and $0\leq\lambda\leq 4$. When $3.57\leq\lambda\leq 4$, the system behavior is chaotic. But in generalized logistic map, the chaotic behavior span is expanded to $0.5\leq\lambda\leq 4$.

$$x_{n+1} = \frac{4\lambda^2 x_n(1-x_n)}{1+4(\lambda^2+1)x_n(1-x_n)} \tag{15}$$

The generalised logistic map provided in Eq.(12) is utilized throughout the diffusion process in our hypothesis and while the permutation process n iterated 2D Arnold cat map was used. The suggested method would be referred to in further explanation as Arnold Coupled Generalized Logistic Map Lattices (ACGLML). A generalised logistic map eliminates the Lyapunov exponent's negative values in the LE map and removes the periodic windows in the bifurcation diagram. In order to minimise mutual information between the lattices, the generalised logistic formula has been used with several formulations of the Arnold cat map in the diffusion process. Kolmogorov-Sinai (KS) entropy analysis has still not been undertaken for generalised logistic functions, to the best of the author's understanding. Here is a technique for using a 2D Arnold cat map.

$$x_{n+1}(i) = (1-\varepsilon)f[x_n(i)]+0.5\varepsilon\{f[x_n(j)]+f[x_n(k)]\} \tag{13}$$

where $f(x)$ is a second order difference equation as given in Eq.(14):

$$\begin{bmatrix} j \\ k \end{bmatrix} = \begin{bmatrix} 1 & p_1 \\ q_1 & p_1q_1+1 \end{bmatrix}\begin{bmatrix} i \\ i \end{bmatrix}(\mathrm{mod}\,L) \tag{14}$$

where p_1 = 12, during the diffusion process, q_1=7 and L=100. The matrix's determining factor value using p_1 and q_1 is considered to be 1. These qualities are appropriate to be used in chaotic frameworks. In our proposed algorithm values p_n and q_n of are kept same for an ease of understanding. However, these values are free to be chosen by the user so as to ensure a wide key space. But the user has to ensure the determinant value to be 1 is the minimum criteria.

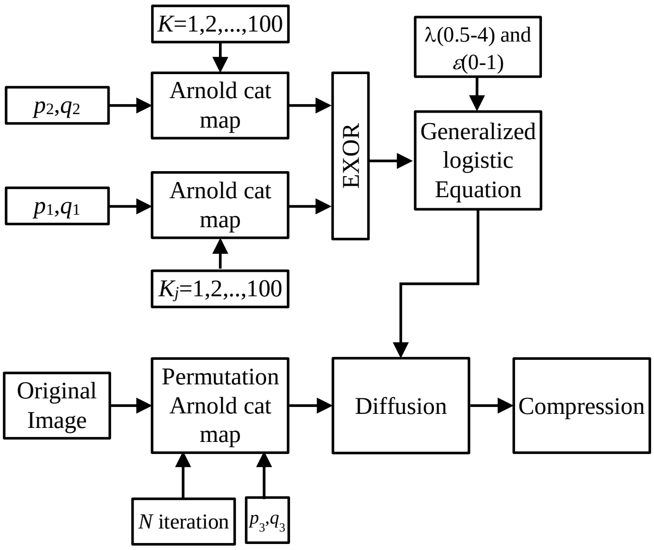

Fig.11. Proposed encryption and compression method

The block diagram shown above in Fig.11 gives a picture of flow of encryption and compression process. For simplicity only forward process is shown, however the decryption and decompression is simply the reverse process of it and original image is reconstructed provided the keys are known correctly.

- *Compression Scheme*: This research has been focused only towards the encryption part of correspondence. Hence, less importance has been shown in compression part of the work. However, the encrypted image should pass through compression algorithms in the practical Cases. To show the robustness of the proposed encryption algorithm, compression and decompression in a lossless method is adopted. It is seen in the earlier chapters that wavelet transforms could give good compression ratio as followed in JPEG 2000 standards. Brief idea on wavelets has been presented below.

Two dimensional wavelet transforms have been applied on encrypted image using two dimensional Symlet waveforms. Wavelet tool box available in matlab version 2016a has been used to perform compression and decompression. Since communications are done in compressed format, encrypted image is first compressed at the transmitter end and then decompressed at the receiver end before the content is applied for decryption process. A compression ratio of around 8:1 is obtained which is of lossless type.

6. RESULT

6.1 BIFURCATION DIAGRAM

The bifurcation diagram shown in Fig.12 is the one obtained by considering the λ value from 0.5 to 4. This bifurcation plot clearly reveals that the range of chaotic behavior is from λ value of 3.57 to 4. In order to view the chaotic region properly, a zoomed version has been shown in Fig.13. However there exists periodicity at λ =3.63 and few other values of λ within 3.57 and 4. A blank vertical line is the evidence of this periodic property. Whereas in Fig.14 obtained from the proposed ACGLML system, the chaotic behavior is from 0.5 to 4. However, in both ACLML and ACGLML the periodic windows have been reduced. Difference between the existing and proposed bifurcation could be well understood by comparing the Fig.12- Fig.15. It is seen in bifurcation of the proposed method that, periodic windows have been completely eliminated. Moreover the range of lattice value's variation is from 0.01 to 1 and the range is maintained for all the values of λ in chaotic region.

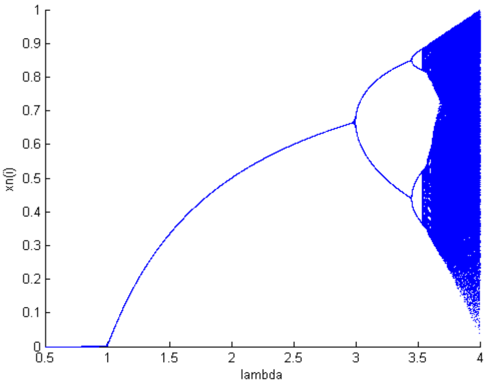

Fig.12. Bifurcation diagram obtained in ACLML (0.5<λ<4)

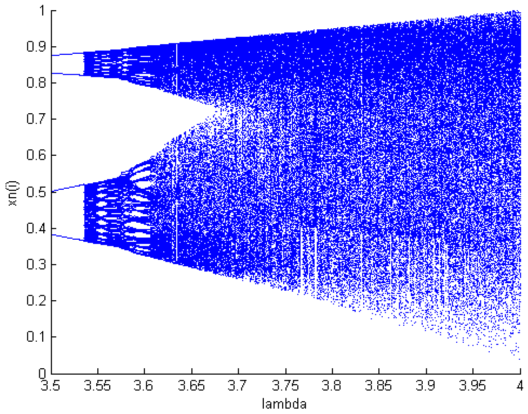

Fig.13. Bifurcation diagram obtained in ACLML (3.5<λ<4)

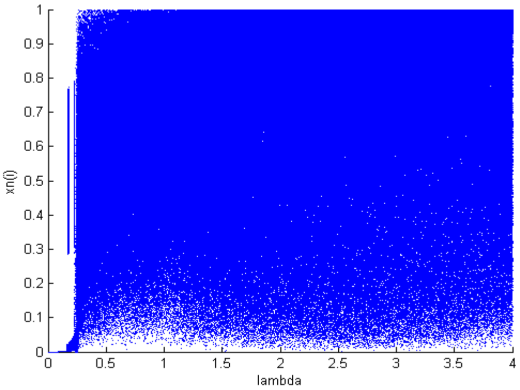

Fig.14. Bifurcation diagram obtained in ACGLML (0.0<λ<4)

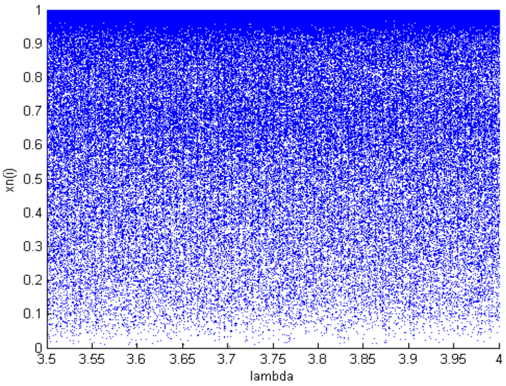

Fig.15. Bifurcation diagram obtained in ACGLML (3.5<λ<4)

It should be seen that the lattice values covers the entire amplitude of 0.01 to 1 for all the values of λ where it is in chaotic region. But in existing ACLML systems, this occurs only at λ=4. The variations in the lattice values of existing system is obtained when ε=0.5 when iterated for 500 times.

In the novel proposed method, compromising results are obtained as listed below. The results obtained nourish the valid users with the following advantages against existing works.

- Standard deviation σ of lattice variation is of average 0.3 which is higher than the existing σ of 0.2.
- Range of λ has been increased from 3.57<λ<4.0 to 0.5<λ<4.0
- Periodicity has been completely eliminated as seen in the obtained bifurcations diagrams.
- Key space has been increased to 28000 against an existing key space of 24000.
- Mutual information for all the 10000 lattices have been brought near to zero against 1% of lattices with higher mutual information in existing works.
- Key space has been increased without any additional encryption time, except the time to perform EXOR operation of lattices K_i = 1,2,..,100 and K_j =1,2,..,100.
- KS entropy density and generality shows that lattices are in chaos for more number of λ and ε pairs.

7. CONCLUSION AND FUTURE SCOPE

7.1 CONCLUSION

This research work has presented the complete process flow of the encryption. Prior to that, chaotic metrics and image quality metrics have been defined. It is shown that how key space has been increased by introducing additional 100 lattices. Further novelty is introduced by iterating the image pixels for multiple times in permutation phase using Arnold Cat map. In all the previous works, multiple numbers of iterations in Arnold map is not done. Hence 1% of 100×100 lattices have more mutual information nearly 0.15. To avoid this, multiple iterations in Arnold cat map has been proposed. Also, while in diffusion phase, the number of iterations N=1012 is better higher value. In order to reduce the time consumed for encrypting the image, the lattices mapped to the new values are applied and final encrypted image is obtained.

7.2 FUTURE SCOPE

Related to the further extensions following ideas are suggested to:

- Introduce contourlet transformations for image compression which would be replace wavelet based compression in proposal.
- The speed of encryption and decryption is a major factor and algorithms could be optimized to reduce it.
- Instead of using 2D Arnold cap map, multidimensional map is a valid enhancement but associated tradeoffs should be properly considered. 8D Arnold cat maps have been used in existing works. But various combinations of logistic maps with different dimension Arnold cap map could reveal new era in the encryption systems.
- Key space obtained is very compromising in the proposed work. Further researches to increase the key space are always encouraged as it troubles the attackers more.

REFERENCES

[1] P. Manisekaran, M.R.A. Dhivakar and P. Kumar, “Enhanced Image Encryption using Multiple Iterated Arnold Coupled Logistic Map Lattices”, *Proceedings of International Conference on Computing Methodologies and Communication*, pp. 514-521, 2020.

[2] P. Manisekaran, M.R.A. Dhivakar and P. Kumar, "On the Analysis of Space-Amplitude Diagram in Chaotic based Image Encryption", *Proceedings of International Conference on Electronics and Sustainable Communication Systems*, pp. 295-301, 2020.

[3] Z. Aihong, L. Lian and Z. Shuai, "Research on Method of Color Image Protective Transmission based on Logistic Map", *Proceedings of International Conference on Computer Application and System Modeling*, pp. 266-269, 2010.

[4] J.M.K. Mastan, G.A. Sathishkumar and K.B. Bagan, "A Color Image Encryption Technique based on A Substitution-Permutation Network", *Advances in Computing and Communications*, Vol. 4, pp. 524-533, 2011.

[5] K.K.S. Pareek, K. Narendra and V. Patidar, "A Symmetric Encryption Scheme for Colour BMP Images", *International Journal of Computer Applications*, Vol. 3, No. 4, pp. 42-46, 2011.

[6] A.B. Abugharsa and H. Almangush, "A New Image Encryption Approach using Block-Based on Shifted Algorithm", *International Journal of Computer Science and Network Security*, Vol. 11, No. 12, pp. 123-130, 2011.

[7] R.S. Yadav, M.H.D.R. Beg and M.M. Tripathi, "Image Encryption Techniques: A Critical Comparison", *International Journal of Computer Science Engineering and Information Technology Research*, Vol. 3, No. 1, pp. 67-74, 2013.

[8] G. Zhang and Q. Liu, "A Novel Image Encryption Method based on Total Shuffling Scheme", *Optics Communication*, Vol. 284, pp. 2775-2780, 2011.

[9] X. Ding and G. Chen, "Optical Color Image Encryption using Position Multiplexing Technique based on Phase Truncation Operation", *Optics and Laser Technology*, Vol. 57, pp. 110-118, 2014.

[10] X. Zhang, G. Zhu and S. Ma, "Remote-Sensing Image Encryption in Hybrid Domains", *Optics Communications*, Vol. 285, pp. 1736-1743, 2012.

[11] P. Shubhangini, S.S. Nichat and M.E. Sikchi, "Image Encryption using Hybrid Genetic Algorithm", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, No. 2, pp. 427-431, 2013.

[12] Y. Ou, C. Sur and K.H. Rhee, "Region-Based Selective Encryption for Medical Imaging", *Proceedings of International Conference on Computing Methodologies and Communication*, Vol. 4427, pp. 62-73, 2007.

[13] Hiral Rathod, Mahendra Singh Sisodia and Sanjay Kumar Sharma, "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)", *International Journal of Computer Technology and Electronics Engineering*, Vol. 1, No. 3, pp. 28-40, 2017.

[14] M.G. Avasare and V.V. Kelkar, "Image Encryption using Chaos Theory", Proceedings of International Conference on Communication, Information and Computing Technology, pp. 15-19, 2015.

[15] G. Kenfack and A. Tiedeu, "Chaos-Based Encryption of ECG Signals: Experimental Results", Journal of Biomedical Science and Engineering, Vol. 7, No. 2, pp. 368-379, 2014.

[16] Ying-Qian Zhang and Xing-Yuan Wang, "Spatiotemporal Chaos in Arnold Coupled Logistic Map Lattice", *Nonlinear Analysis: Modelling and Control*, Vol. 18, No. 4, pp. 526-541, 2013.

[17] A. Sinha and K. Singh, "Image Encryption using Fractional Fourier Transform and 3D Jigsaw Transform", Available at: http://pdf-world.net/pdf-2013/Imageencryption-using-fractional-Fourier transform-and-3DJigsaw- transform-pdf, Accessed at 2013.

[18] N. Zhou, Y. Wang, L. Gong, X. Chen and Y. Yang, "Novel Color Image Encryption Algorithm based on the Reality Preserving Fractional Melling Transform", *Optics and Laser Technology*, Vol. 44, No. 7, pp. 2270-2281, 2012.

[19] M.R. Abuturab, "Securing Color Information using Arnold Transform in Gyrator Transform Domain", *Optics and Lasers in Engineering*, Vol. 50, No. 5, pp. 772-779, 2012.

[20] Y. He, Y. Cao and X. Lu, "Color Image Encryption based on Orthogonal Composite Grating and Double Random Phase Encoding Technique", *Optik*, Vol. 123, No. 17, pp. 1592-1596, 2012.

[21] H. Chen, X. Du, Z. Liu and C. Yang, "Color Image Encryption based on the Affine Transform and Gyrator Transform", *Optics and Lasers in Engineering*, Vol. 51, No. 6, pp. 768-775, 2013.

[22] Z. Yu, Z. Zhe, Y. Haibing, P. Wenjie and Z. Yunpeng, "A Chaos-Based Image Encryption Algorithm using Wavelet Transform", *Proceedings of 2nd International Conference on Advanced Computer Control*, pp. 217-222, 2010.