CE-TEC

Chaotic Encryption and Turbo Error Correction

Akash Shah,Bhavin Patel, Palak Mehta,Vatsal Mewada
Prof.Sumita Chandak
vatsalmewada@gmail.com
palakmehta7@gmail.com
Dept. of Information Technology
Atharva College of Engineering, Malad(W),
Mumbai, India.

***Abstract*—The cryptographic algorithms in the recent years have suggested some new and efficient and also effective ways for developing image encryption techniques that are secure, these cryptographic algorithms are mostly chaos based. It has been proven that chaos maps and chaotic systems are very useful and effective for cryptography. Here in this paper we use Two-Dimensional Logistic Map with other complicated structures for Encryption of Image. Also here we have used the Permutation and Substitution methods for imbibing properties of Confusion and Diffusion which are a major part of secure cipher. Thus proposed system basically does the work of encrypting image into a random form of structure which is visually does not mean anything to human eyes and also statistically randomizing the image structure.**

***Keywords*- Chaotic Encryption,Logistic Map,Permutation Substitution, Diffussion, Error Correction,Turbo code.**

I. INTRODUCTION

In recent years the Government and Public have shown much concern of Image Security. Image Security is a concern for Military and Government Organizations and also for Public Domain when Private Images are exposed without having authority. In today's world we can send or copy and image form one device to other or sent it over internet to anyone, but without any security this would be a serious damage of privacy to the owner of the data, In this case Images.

There are various Technologies concerning Image Security and most important one being Encryption which is also very straightforward which has the Original/Source Image as Plaintext and the Encrypted Image as Cipher-text.[1][2]. The early encryption techniques were the Digital Encryption Standard (DES) [3], the Advanced Encryption Standard (AES) [4], the Two Fish cipher [5] and the Blow Fish cipher [6] here the Image was Treated as a Stream of bits and encrypted is that manner either bit-by-bit or block-by-block , but these Ciphers or Standards were One-Dimensional in nature which sacrificed the Two- Dimensional nature of the Image. Also it is inefficient in the sense it takes long bit streams form the image usually 8 to 16 bits per pixel to encrypt image data thus high risk and easily exploitable by error and check method.

II. The Two-dimensional Logistic Map

The Two-Dimensional Logistic Map is very complicated in behavior and has evolved to be the best in class when the test for chaos is scaled on the concept of Attractors and Basins[20]. Obviously it has more dynamic, complex and chaotic behavior than One- Dimensional Logistic Map.

A. *Mathematical Definition*

This 2D logistic map is as defined as Eq. (1), where the variable r is the system parameter and (xi; yi) is the two dimensional point making a pair at the i'th iteration.

2D Logistic Map:

$$x_{i+1} = r(3y_{i+1} + 1)x_i(1\text{-}x_i) \quad ...(1)$$

$$y_{i+1} = r(3x_{i+1} + 1)y_i(1\text{-}y_i) \quad ...(2)$$

B. *Chaotic Behaviors*

The Two-Dimensional Logistic Map which is defined in Eq. (1) is a very complex and dynamic system. Depending on the values of the system parameter r, the map evolves from one kind of dynamics to another.

Since a (x;y) trajectory in the context ofthe chaotic behavior is random like but is completely predictable when r and (x0;y0) are both known this works as a pseudo number generator for cryptography being a major security issue.

C. *Complexity*

Obviously the 2D logistic map defined in Eq. (1) has a higher complexity compared to the conventional logistic map[9], i.e. One-Dimensional Logistic Map defined in Eq. (3), here r is the parameter that controls the chaotic behaviors. Below is the One-Dimensional Logistic Map equation.

1D logistic Map:

$$x_{i+1} = rx_i(1 - x_i) \quad ...(3)$$

There are various means by which the complexities of the One-Dimensional and Two-Dimensional Logistic Maps and the Henon Map can be Measured, these are measured for the randomness that could be achieved and for the entropy results. Complexity Comparisons between these chaotic maps using entities like Information Entropy, Lyapunov Exponent and Lyapunov Dimension with the input by various pairs of initial values. As we know Two-Dimensional Logistic Map will have a higher score of Information Entropy than its predecessor One-Dimensional Logistic Map, which implies the greater Randomness effect on the Encryption. Same case is with the Lyapunov exponent and this implies that Two-Dimensional Logistic Map is more Dynamic.

III. Image Encryption using the 2D Logistic Map

In order to deal with the problems faced during 1-d chaotic encryption we use 2-d chaotic maps.

Fig. 1 shows the flowchart of the image encryption method using the 2D logistic map. And the internal working is composed of 2D Logistic Permutation, 2D Logistic Diffusion and 2D Logistic Transposition where each phase itself is an image cipher and they together form the permutation-substitution network. The encryption procedure, the decryption procedure is nothing but reverse the order of processing using the decryption key. The encryption process can be written as C = Enc(P;K), and the decryption process is P = Dec(C;K).The block diagram

.

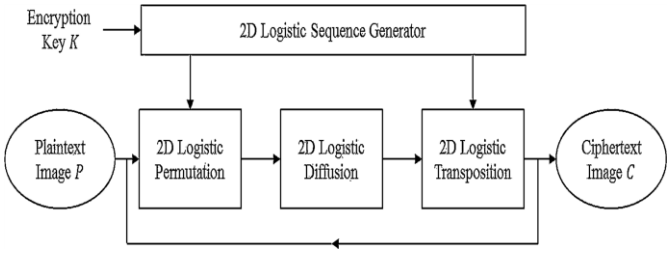


Fig.No.1.Block Diagram of Chaotic encryption using 2D-Logistic map

IV. Key Schedule and 2D Logistic Sequence Generator

We define our encryption key K as a 256-bit string composed of five parts x0; y0; r,T, and A1….A8 where (x0; y0) and r are the initial value and A and T are the parameters of the linear-Congruential-generator .

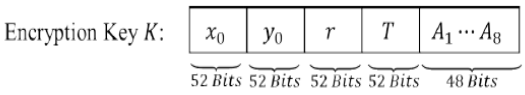


Fig.No.2Encryption Key K Bifurcation.

Here in this, we calculate a fraction value v from a 52-bit string {b-1; b-2; b-52}
using the IEEE 754 double-precision binary floating-point format for the fraction part.
Consequently, x0, y0, r and T can be found. For coefficients A0;A1;… ;A7, each of which is composed of 6-bit string {b0; b1;….; b5}, we translate these 6-bit strings to integers and obtain the required coefficients.

V. 2D Logistic Permutation

Permutation is Mathematically used for many years for use of properties like Confusion and Diffusion for secure Image Transmission. Our Methodology has been explained below.

Permutation Working Step Wise:
Input : Secret Key (values to be assigned by 2D logistic Map)
Output : Generate M x N - 2D Logistic Sequence

$$x_{i+1} = r(3y_{i+1} + 1)x_i(1\text{-}x_i)$$
$$y_{i+1} = r(3x_{i+1} + 1)y_i(1\text{-}y_i)$$

Create permutation map for each row using X matrix

$$X = \begin{pmatrix} 0.1253 & 0.4521 & 0.3714 & 0.8563 \\ 0.7801 & 0.2486 & 0.5743 & 0.4521 \\ 0.6703 & 0.2719 & 0.7641 & 0.5681 \\ 0.9105 & 0.4501 & 0.4902 & 0.8609 \end{pmatrix}$$

Elements in row 2
0.7801,0.2486,0.5743,0.4521

Reorder of elements in row 2
0.2486,0.4521,0.5743,0.7801
Permutation map for row 2

$$e_x^{r=2} = \begin{pmatrix} 0.7801 & 0.2486 & 0.5743 & 0.4521 \\ 0.2486 & 0.4521 & 0.5743 & 0.7801 \end{pmatrix}$$

Row permutation

$$U^x = \{e_x^{r=1}, e_x^{r=2}, \ldots, e_x^{r=M}\}$$

Column permutation

$$U^y = \{e_y^{c=1}, e_y^{c=2}, \ldots, e_y^{c=N}\}$$

Below show is the result of Permutation

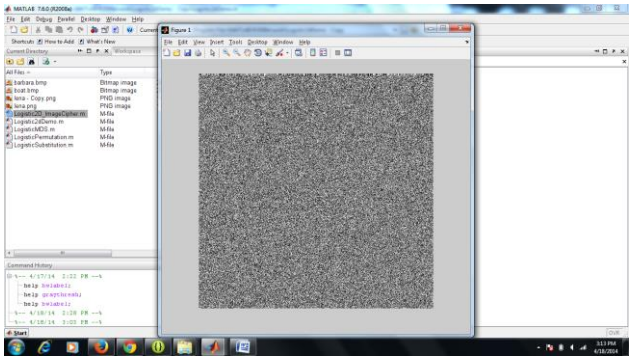


Fig.No.3 Result of Permutation.

VI. 2D Logistic Diffusion

In order achieve good diffusion properties [6], we apply the logistic diffusion for every S X S image block Pb within the plaintext image P over the finite field GF(28) as shown in Eq.(4), where S is the block size variable determined by the plaintext image format, and Ld is the maximum distance separation matrix [4] found from 4X4 random permutation matrices defined in Eq. (4).

$$C_i^{(1)} = (L_d . P_i^{(1)} . L_d mod 256) \qquad \ldots(4)$$

It worthwhile to note that if the plaintext image P is of 8-bit grayscale or RGB colour types, both of which code an image pixel as a byte (1 byte = 8 bits), then the image block Pb is of size 4 X 4; while if the plaintext image is a binary image, then Pb is of size 32 X32 in bits(equivalent to a 4 X 4 image block in bytes).
In the case that the plaintext image P with a size M X N which is not dividable by S, the processing block size of Pb, we then only apply this process with respect to the

region S[M/S] X S[N/S] and [.] is the rounding function towards to zero. Since the 2D logistic diffusion process is applied to every SXS image blocks in the plaintext image for each cipher iteration, any one pixel change in plaintext image then causes a change for S X S pixels in each round.

After sufficient number of cipher rounds , any slight changein a plaintext image leads to significant changes in ciphertext and thus attains the diffusion properties. Fig. 8 shows the results of 2D logistic diffusion. It can be seen that after two-rounds of diffusion, the plaintext image P becomes completely unintelligible.

VII. 2D Logistic Transposition

Transposition process changes pixels values with respect to the reference image I, which is dependent on the logistic sequence generated from the previous stage. First, X and Y , which the matrix version of Xseq and Yseq by arranging a sequence elements in a matrix, are added together to be Z via Eq. (5).

$$Z = X + Y \quad \ldots(5)$$

Next, each 4X4 block B in Z is then translated to a random integer matrix using the block function f(B), where B is a 4 X 4 block, and the subfunction gN(), gR(), gS() and gD() are defined. The function T (d) truncates a decimal d from the 9th digit to 16th digit to form an integer,

$$I^k = f(Z^k) =$$

$$\begin{pmatrix} g_N(Z^k_{1,1}) & g_R(Z^k_{1,2}) & g_S(Z^k_{1,3}) & g_D(Z^k_{1,4}) \\ g_R(Z^k_{2,1}) & g_S(Z^k_{2,2}) & g_D(Z^k_{2,3}) & g_N(Z^k_{2,4}) \\ g_S(Z^k_{3,1}) & g_D(Z^k_{3,2}) & g_N(Z^k_{3,3}) & g_R(Z^k_{3,4}) \\ g_D(Z^k_{4,1}) & g_N(Z^k_{4,2}) & g_R(Z^k_{4,3}) & g_S(Z^k_{4,4}) \end{pmatrix};$$

$$\boldsymbol{g_{N(x)=T(x)mod256}} \quad \ldots(8)$$

$$\boldsymbol{g_{S(x)=T(x^2)mod256}} \quad \ldots(9)$$

$$\boldsymbol{g_{R(x)=T(\sqrt{x})mod256}} \quad \ldots(6)$$

$$\boldsymbol{g_{R(x)=T(2x)mod256}} \quad \ldots(7)$$

A random integer matrix I is obtained, where each 4X4 block in I is actually mapped from a corresponding 4X4 block in Z with the function.

Thus we have achieved the 2D logistic transposition by moving every pixel to the plaintext image, a fixed amount of random integer Image I is used over the integer space (0;F-1), i.e. cipher text image of 2D logistic map C is shown in Eq. (12), If, F = 256 for a 8-bit grayscale image.

$$C = (P + I) \bmod F \quad \ldots(8)$$

[F:- The number of allowed intensity scales of the plaintext image ; Eg. , F = 256 for a 8-bit grayscale image]

For Decryption as above we can similarly define equation as shown in Eq. (9)

$$P = (C - I) \bmod F \quad \ldots(9)$$

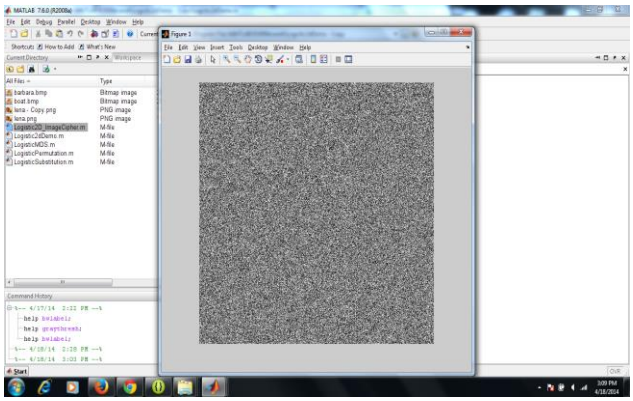


Figure 4: 2D logistic transposition results.

VIII. ERROR CORRECTION

Coding each individual block for getting encoded as an independent entity is a traditional process of error correction coding. However in this brings what we consider for error correction code is: Convolutional codes. It encode bits based upon a state which is determined by summing a fixed set of previously bits. In this every input bit is manipulated in different ways to produce several outputs bits. Resulting each output bit convey the combined information of several different input bits. Initially a key is passed from encoder to decoder. Keys plays role in the decoding process due to the integral part , these codes are used for cryptography.

For encoding data there are many different algorithms, but all this algorithms are dependent upon two variables, the rate is decided in the basis of, how many bits in the state and how many output bits are produced per input bit.

The codes can be further subdivided as systematic and recursive codes.

i. Systematic code:-A systematic code has an output that is the input;

ii. Recursive code:- A recursive algorithm uses a prior output as part of the new input.

Figure 6 shows three diagrams of convolution encodings. They all use a rate of 1(or 1 input, 2 outputs) and have a state that is dependent upon seven inputs. The top image depicts a systematic nonrecursive, the middle a non-systematic nonrecursive, and the bottom a systematic recursive.

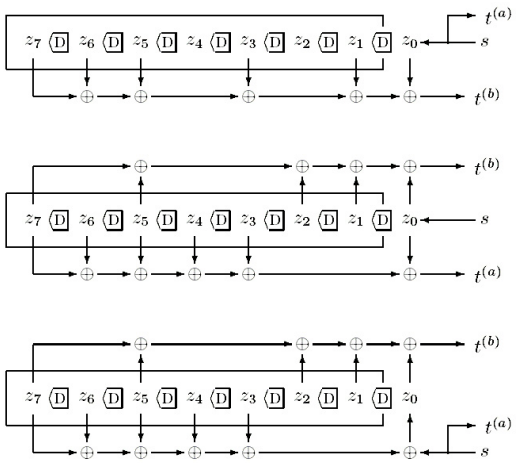


Figure 5: Different methods of generating

convolution codes. Convolution codes also allow for the addition of other checksums. A form of common practice for checking the parity in the code before convoluting it is possible. This gives double error-protection, however a compromise with the speed factor associated with encoding and decoding convolution codes.

A. *4.1 Turbo Codes*

Turbo codes is the recent innovation being first documented in 1993. They use a many previously discovered codes mixture or combined together, also known as hibernation of codes.

The most simple turbo codes technique is of working through a series of simultaneous steps. The input is split into as many copies as desired. Then a copy is sent directly through a convolution code. Simultaneously another copy is permuted and sent through a potentially different convolution code. This process is repeated using different permutations and potentially different convolution codes until all the copies are sent. Then it appends/sums mod 2 certain combinations of outputs and that is the message that is sent

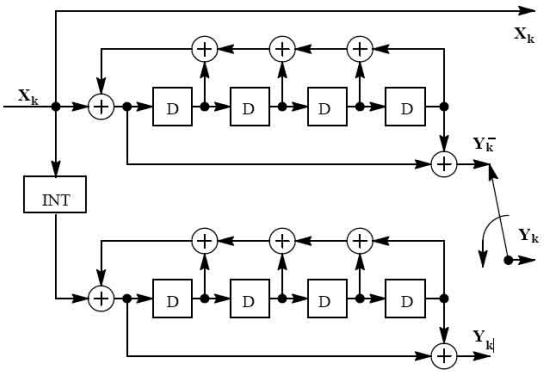


Figure 6: Rate 1 , systematic recursive turbo code.
2

Some turbo codes use a combination of parallel and series configurations. There are various factors that create the most effective turbo codes by using more convolutions, using recursive convolutions, using ”softer” decoders; and, rather non-intuitively, using convolutions. Turbo codes are most effective on longer code words.

I. CONCLUSON

Thus our efforts are to build a secure and reliable image transmission scheme that combine turbo coding based on error correction code and 2D chaotic map based encryption functionality into one single step and try to reduce the overall processing cost. The advantages of our scheme will be for achieving better security by utilizing 2D chaotic map instead of 1D chaotic map and improving the throughput of an image transmission system by using turbo coding.

The Results of our Project have been shown stepwise in above diagrams through screen shots. Finally the Statistical Results of our Project and its output is shown using histograms.

The Figure 7 shows four images on the top-left is the original Image and on the top-right is the encrypted output image.

The first histogram on the left is the Original or Plaintext Image's Histogram and the right hand side histogram is the equalized histogram of the encrypted image as shown in Fig 7.

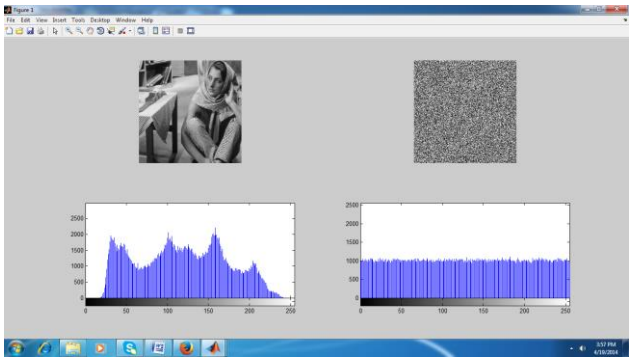
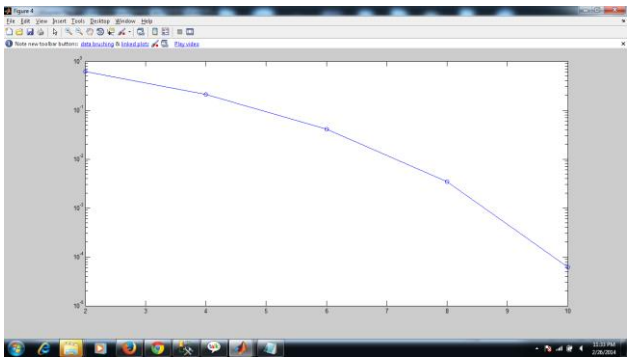


Fig No.7.Result Of Implementing 2D-Chaotic Logistic Encryption

Next we want to Test how successful was our turbo coding, for that we use a graph to plot the error bursts found in the decrypted image after transmission is done via simulation on Matlab. We notice gradually the Error bits vanish from the transmission. Only Initial values are Erroneous when transmitting the Image on Simulation.



FigNo.8 Result Of Implementing Turbo Coding For Error Correction in Encrypted Image Transmission

II. REFRENCES

[1] M. Yang, N. Bourbakis, and S. Li,\Data-image-video encryption," in IEEE Potentials 23(3),28{34 (2004).

[2] D. R. Stinson, Cryptography: theory and practice, Chapman and Hall CRC (2006).

[3] FIPS PUB 46, Data Encryption Standard (1977).

[4] FIPS PUB 197, Avdanced Encryption Standard (2001).

[5] B. Schneier, The two sh encryption algorithm: a 128-bit block cipher, J. Wiley (1999).

[6] R. Anderson and B. Schneier, \Description of a new variable-length key, 64-bit block cipher(Blowsh)," in Lecture Notes in Computer Science, 191{204, Springer Berlin Heidelberg (1994).

[7] Y. Wu, J. P. Noonan, and S. Agaian, \Shannon entropy based randomness measurement and test for image encryption," in CoRR abs/1103.5520 (2011).25

[8] B. Hennelly, and J. T. Sheridan, \Optical image encryption by random shifting in fractional fourier domains," in Opt. Lett. 28, 269{271 (2003).

[9] W. Chen, and X. Chen, \Space-based optical image encryption,"in Opt. Express 18, 27095{27104 (2010).

[10] B. Zhu, S. Liu, and Q. Ran, \Optical image encryption based on multifractionalfourier trans-forms," in Opt. lett. 25(16), 1159{1161 (2000).

[11]YueWua, GelanYangb, HuixiaJinb and Joseph P. Noonana;"Image Encryption using the Two-dimensional Logistic Chaotic Map"Department of Electrical and Computer Engineering, Tufts University Medford, Massachusetts 02155, United StatesDepartment of Computer Science, Hunan City University Yiyang, Hunan 413000, China.

[12]Claude Berrou,IEEE member , and Alain Glavieux ,"Near Optimum error Correcting and Decoding :Turbo Code",IEEE transaction on communication vol.44 no.10 Ocober1996

