Chaotic Map and Image Based Cryptosystem

K.Meena [1], Dr.G.A.Sathish Kumar [2]

[1] *PG Student, Department of ECE, Sri Venkateswara College of Engineering, Tamilnadu 602117*

[2] *Professor, Department of ECE, Sri Venkateswara College of Engineering, Tamilnadu 602117*

Abstract- **In this paper, an image encryption scheme based on colour byte scrambling technique is proposed by using Logistic map and Tent map. The proposed scheme is using Logistic map for generating permutation sequence to shuffle the colour bytes (confusion) and Tent map is used for generating masking sequence to change the value of the colour bytes (diffusion) of the 24-bit colour image. The traditional scrambling techniques confusion and diffusion are applied continuously on the test image which leads to producing the cipher image which has good confusion and diffusion properties. Since we are applying Logistic map and Tent map for image encryption, it is very difficult for the cryptanalyst to break the proposed image encryption algorithm. The performance and security of the proposed method are evaluated thoroughly using key space analysis, statistical analysis, sensitivity analysis and so on. Results are encouraging and suggest that the scheme is reliable to be adopted for the secure image communication application.**

Index terms- **Logistic Map, Tent Map, Quadratic Map, Chaos, diffusion process and Stream Cipher**

I.INTRODUCTION

With the rapid developments of computer technology and multimedia industry, the protection of digital information transmitted or stored on the internet becomes more and more important. An effective method is to encrypt the digital information so that only the authorized entities with the key can decrypt it. Since digital image has some intrinsic features such as bulky data capacity, high redundancy and high correlation among pixels, the conventional encryption schemes such as DES, AES and RSA are not considered suitable for image encryption [1]. In recent years, chaos-based image encryption system has been widely investigated because of the fundamental feature of chaotic map such as sensitivity to initial condition, random likebehaviors and aperiodicity [2-8].

A general chaos-based image encryption method is composed of two steps: pixel permutation and diffusion. In the permutation stage, a P-box is usually generated to shuffle the pixel position in order to destroy high correlation of pixels in the image. In the diffusion stage, the pixel values are modified sequentially so that the histogram is totally changed and a tiny change of plain image can spread out to almost all pixels in the cipher image. However, many chaos based image encryption algorithms with permutation diffusion structure are broken recently [9-15]. The main reason is that the key stream used in diffusion step only depends on the key [16]. If the key keeps unchanged, the key streams generated to encrypt different plaintexts are the same. Therefore the attackers can obtain the key stream by known-plaintext attack and chosen-plaintext attack [10, 12-13]. Correspondingly, the encryption scheme degenerates to permutation-only architecture which has already been broken .

To improve the security of encryption algorithm, some researchers recently proposed that the key stream in diffusion should be relevant to the plaintext. They use the plaintext to control the iteration times of chaotic system, so the generated key stream is different if the plaintext is different, even though the key is the same. This scheme is successful to resist the known-plaintext attack and chosen plaintext attack. Nevertheless, there still exist some possible problems. First, it is well known that one-dimensional chaotic map has periodic problem when implemented in finite precision, which may result in consequent degradation in security [16]. And the key space of low dimensional chaotic map is small. Second, the necessary iteration times of chaotic system in diffusion process increases largely. In addition, the P-box in permutation process is irrelevant to the plaintext. In this paper, a novel image encryption scheme based on even-symmetric chaotic maps is proposed. In the permutation process, the iteration time of even-symmetric chaotic map to avoid transient effect is not fixed but relevant to the plaintext so the P-box changes even though the initial value is the same. In the diffusion process, two even symmetric chaotic maps are used to generate the key stream. The pixels in the permuted-image determine which even symmetric chaotic map to iterate for next byte in the key stream each time instead of increasing the iteration times. Meanwhile, the problems of short period and small key space in one-dimension chaotic map are practically avoided by using two chaotic systems. In this paper, we use the even symmetric chaotic map for its good statistical properties [18-19]. Other one-dimension chaotic maps such as skew tent map are also applicable for our scheme. This method can also be extended to other fields such as text encryption since the algorithm treats the image as a vector.

In this paper, a new colour byte scrambling scheme for the colour image encryption using Logistic and Tent map is proposed. The chaotic sequences are generated using these chaotic maps and thereby the position of image pixels and values are changed according to the transformation of chaotic sequences. The chaotic image encryption is done by confusion and diffusion. The confusion is obtained through the change of pixel locations and diffusion is obtained through the alteration of pixel values. In this scheme, the Logistic map is one dimensional which is simple and efficient and used for the generation of permutation sequences for achieving confusion. The two-dimensional Tent map is used for the generation of masking sequences for achieving diffusion. Finally, the outcome of the proposed algorithm is compared with existing results and validated by different cryptanalysis.

II. RELATED WORK

The chaotic logistic map technique has been proposed by Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay and Debashis Nandi [2]. This technique was employed on the gray level where the XOR operations and pixel shuffling of the image are used to confused and diffuse the pixel value and the pixel position. Another technique has been proposed by Jiri Giesl, Ladislav Behal and Karel Vlcek [1] based on Peter de Jong's chaotic map and transformed the image into wavelet domain and performed encryption over this wavelet coefficients. In the above techniques, the entire image is encrypted and decrypted each time, which is a big overhead in case of storage and retrieval of large set of images, in an image database or transmission of images over large an insecure channel. Also the loss of even a small part of the encrypted images results in greater distortion in the decrypted image. This is due to the fact that the part of the encrypted image which is distorted constitutes pixels that will be scattered in the decrypted image.

III. THE PROPOSED ENCRYPTION ALGORITHM

The proposed system is a Chaotic Maps and Image Based Cryptosystem that combines randomness of chaos system into existing Cosine-transform-based chaotic system for image encryption. On analyzing several chaotic maps based on its performance, the logistic, tent maps were compatible with the proposed system. The m*n image pixels is shifted initially and its output is combined with chaotic maps (logistic & tent maps). The output from the chaotic map is then scrambled using high-efficiency scrambling method. Histogram of the final output of scrambled image is also obtained. Hence, the image is encrypted and decrypted using chaotic maps. The proposed modification to the existing chaotic maps for image encryption will enhance the security level in image processing.

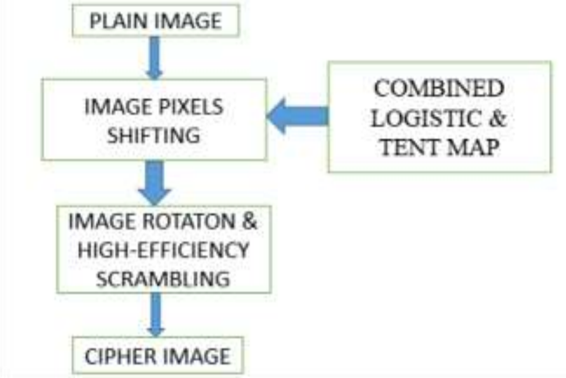

PLAIN IMAGE
IMAGE PIXELS SHIFTING
COMBINED LOGISTIC & TENT MAP
IMAGE ROTATON & HIGH-EFFICIENCY SCRAMBLING
CIPHER IMAGE

Figure 1. Chaotic maps and image based cryptosystem

A. Functionality of Chaotic Maps

Step 1: Initially the input image (eg. cameraman image) is used to study the characteristics of the logistic and tent maps, which produce complex dynamic behaviors.

Step 2: The same input image is taken and its pixels are shifted using circular shift operation and this pixel shifted output is given as input to the logistic and tent chaotic maps. Step 3: Small changed in plain image to all pixels of the cipher image is done using scrambling method. The output of the logistic and tent maps is given as input to image rotation method and rotated output image is obtained.

Step 4: Rotated image is the input image and it is pixels are scrambled randomly to obtain the encrypted image and the same reverse process is used for decryption of image.

Step 5: Histogram of the final output of scrambled image is also obtained. Hence, the image is encrypted and decrypted using chaotic maps.

B. Logistic Map

The logistic map is a polynomial mapping of degree 2, often cited as an archetypal example of how complex, chaotic behavior can arise from very simple non-linear dynamical equations. The relative simplicity of the logistic map makes it a widely used point of entry into a consideration of the concept of chaos. It is a one dimensional and iterative map. Mathematically, the logistic map is written as

$$x_{n+1} = r\, x(1\text{-}x_n)$$

xn is a number between zero and one that represents the ratio of existing population to the maximum possible population. The values of interest for the parameter r (constant, sometimes also denoted μ) are those in the interval [0,4]. This nonlinear difference equation is intended to capture two effects:

1 Reproduction where the population will increase at a rate proportional to the current population when the population size is small.

2 Starvation (density-dependent mortality) where the growth rate will decrease at a rate proportional to the value obtained by taking the theoretical "carrying capacity" of the environment less the current population.

C. Tent Map

The Tent map is known as its tent-like shape .It can be defined by the following equation:

$$x_{i+1} = f\mu(x_i) = \begin{cases} \mu x_i & ,\text{if } x_i < 0.5 \\ \mu(1 - x_i) & ,\text{if } x_i > 0.5 \end{cases}$$

where, μ is a positive real constant. Choosing for instance the parameter μ=2, the effect of the function fμ may be viewed as the result of the operation of folding the unit interval in two, then stretching the resulting interval [0,1/2] to get again the interval [0,1]. Iterating the procedure, any point x0 of the interval assumes new subsequent positions as described above, generating a sequence xi in [0,1]. The μ =2 case of the tent map is a non-linear transformation of both the bit shift map and the r=4 case of the logistic map. The value of μ, the tent map demonstrates a range of dynamical behavior ranging from predictable to chaotic.

D. Circular Shifting

A circular shift is the operation of rearranging the entries in a tuple, either by moving the final entry to the first position, while shifting all other entries to the next position, by performing the inverse operation. A circular shift is a special kind of cyclic permutation, which in turn is a special kind of permutation. Formally, a circular shift is a permutation σ of the n entries in the tuple such that, modulon, for all entries i = 1,..n. The result of repeatedly applying circular shifts to a given tuple are also called the circular shifts of the tuple. Repeatedly applying circular shifts to the four-tuple (a, b, c, d) successively gives, (d, a, b, c), (c, d, a, b), (b, c, d, a), (a, b, c, d) (the original four-tuple). Then the sequence repeats; this four-tuple therefore has four distinct circular shifts. Not all n-tuples have n distinct circular shifts. For instance, the 4-tuple (a, b, a, b) only has 2 distinct circular shifts. In general the number of circular shifts of an n-tuple could be any divisor of n, depending on the entries of the tuple. A bitwise rotation, also known as a circular shift, is a bitwise operation that shifts all bits of its operand. Unlike a logical shift, the vacant bit positions are not filled in with zero but are filled in with the bits that are shifted out of the sequence. Circular shift to left and right figure 2.

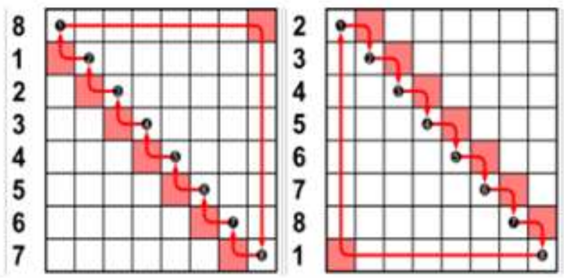


Figure 2 Circular shift to left and right

E. Scrambling technique

Image scrambling is the method of rearranging the pixels randomly to make the image visually unreadable and break the correlation between the neighboring pixels. In general, during scrambling the pixel values remain unchanged. Most of the image encryption algorithms involve two phases, namely confusion and diffusion. In the confusion phase the pixel positions are permuted using some scrambling technique and in the diffusion phase the pixel values are changed by using some inverse-able function. Image pixels are highly correlated with neighboring pixels and a good scrambling algorithm reduces this correlation near to zero. Scrambling of Gray scale Image figure 3.

Bit-plane scrambling is one of the famous image scrambling techniques. In a quantum image gray-code (GB) with bit-plane scrambling is presented. It is used as one of the basic steps in many encryption algorithms. A novel chaos-based bit-level permutation scheme is used, in which the image is extended to bit plane binary image and the rows are permuted according to a random sequences. The columns are shifted using the random sequences. Transforming a plain image into a meaningless noise image. Bit plain permutation based on pseudo random number sequence. This scheme performs the scrambling in two steps, first using a pseudo random sequence. Second scheme is successful in generating a secure scrambled image with good cryptographic effects.

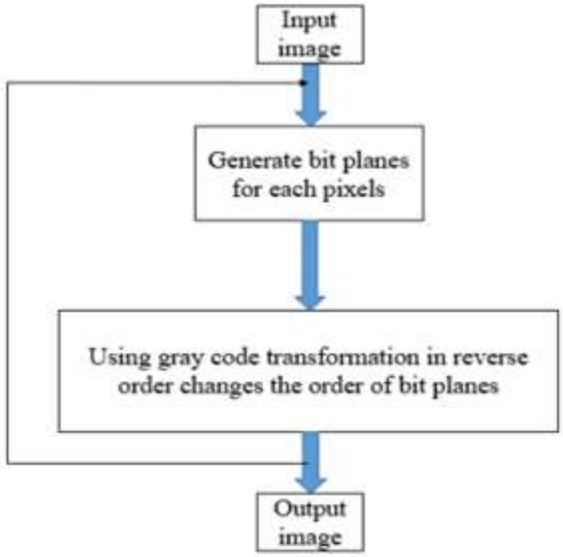

Input image
Generate bit planes for each pixels
Using gray code transformation in reverse order changes the order of bit planes
Output image

Figure 3 Scrambling of Gray scale Image

IV. SIMULATION RESULTS

In this section, few analyses have been done to validate the performance of the proposed scheme. The experimental analysis of the proposed combined chaotic encryption scheme has been done on the colour image shown in Fig. 6 which is downloaded from the benchmark Waterloo image set and the size of the image is 1118×1105 [20]. To initiate the experiment, the control parameters are calculated from the plain image using the generation of control parameters algorithm for Logistic and Tent map. Further the initial parameters for the Logistic and the Tent maps are provided below and the results of the proposed algorithm are validated.

A. Tent Map

Input image with size of (256×256) is given as input to tent map and its output is obtained. Tent Map figure 4

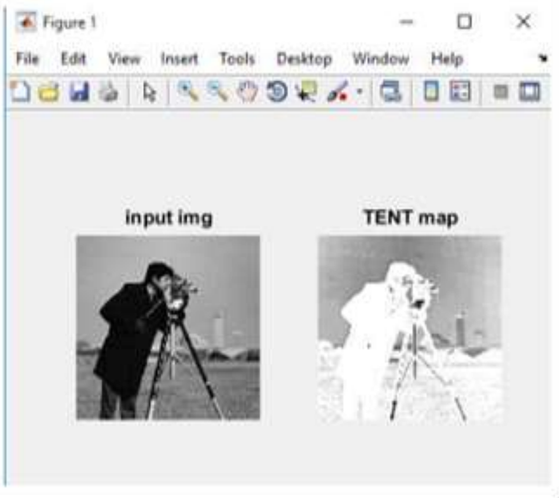


Figure 4.4Tent Map

Histogram of Tent Image

Tent map output is given as input to the circular shifting method and tent map image histogram is obtained. Histogram of Tent Image figure 5.

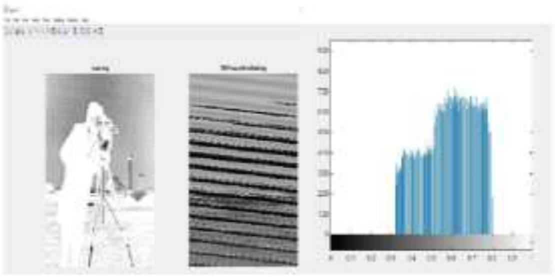


Figure 5 Tent map Shifted image

Histogram of Logistic map

Input image is given to Logistic map and then its output circular shifted and histogram is obtained.

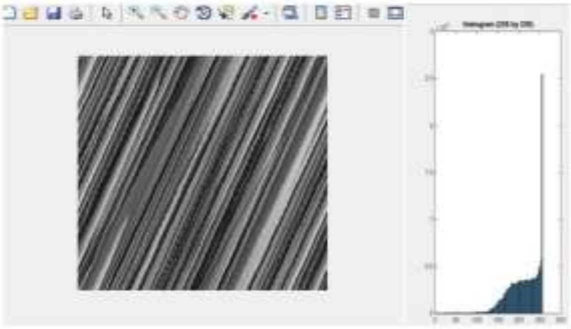


Figure 6 Histogram of Logistic map

Image Rotation and Scrambling

Output of Tent and Logistic map is combined together to obtain the cipher image and this cipher image given as input image to scrambler and reverse process is done to recover the original input image.Image Rotation and Scrambling figure 7

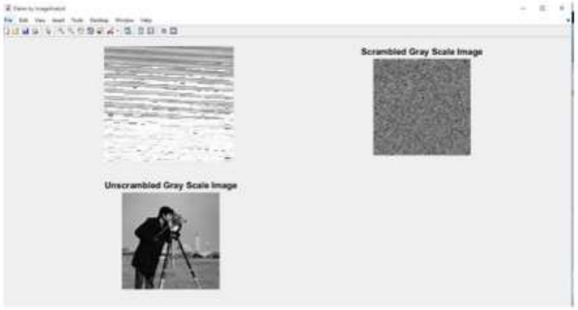


Figure 7 Image Rotation And Scrambling

Histogram of Original Image

Histogram of original cameraman image is show below. Histogram of Original Image figure 8

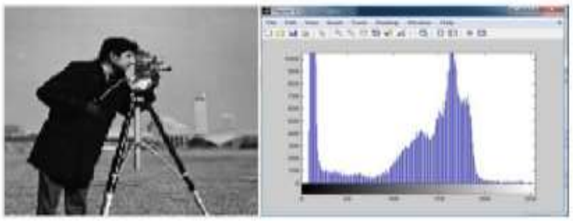


Figure 8 Histogram of Original Image

Histogram of Scrambled Image

Histogram of the scrambled image is shown in the below figure. Histogram of Scrambled Image figure 9

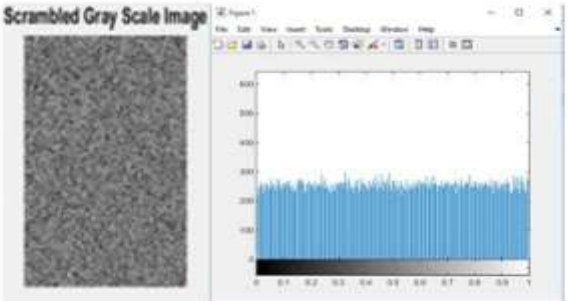
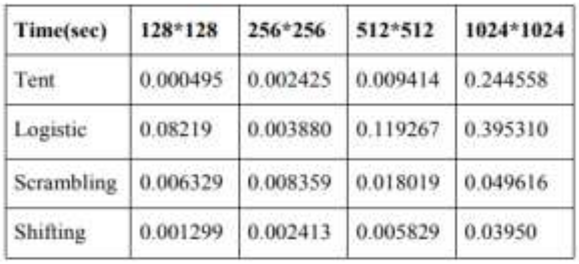


Figure 9 Histogram of scrambled image

Chaotic maps

The following figures show the graphical output of the chaotic maps used (logistic, tent) and tabular column indicates the execution time for each process.

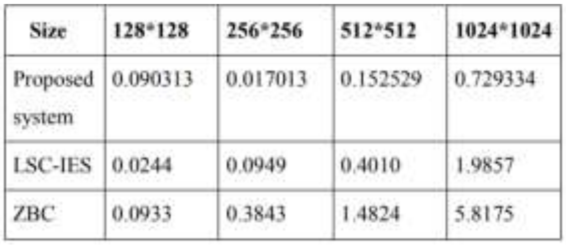


Time(sec)	128*128	256*256	512*512	1024*1024
Tent	0.000495	0.002425	0.009414	0.244558
Logistic	0.08219	0.003880	0.119267	0.395310
Scrambling	0.006329	0.008359	0.018019	0.049616
Shifting	0.001299	0.002413	0.005829	0.03950

Table 1 Time Consumption for each Operation in Proposed Algorithm in seconds

Analysis:

We have implemented the technique in MATLAB 7.10 using a PC equipped with Intel Core2Duo T5550 @ 1.83 GHz, 2 GB RAM, 32±bit Windows 7 Ultimate OS. Theoretically the time taken for both encryption and decryption of the proposed system is low compare than LSC-IES,ZBC. It can be seen from Table. 2



Size	128*128	256*256	512*512	1024*1024
Proposed system	0.090313	0.017013	0.152529	0.729334
LSC-IES	0.0244	0.0949	0.4010	1.9857
ZBC	0.0933	0.3843	1.4824	5.8175

TABLE 7.2 Required time (seconds) for encrypting one image with different sizes using different image encryption algorithms.

V. CONCLUSION

In this day and age, as more and more people share information in the digital format, the amount of data being generated is increasing at a drastic pace. Therefore, cryptography is of utmost importance, however due to the standard structure of most cryptographic functions being used at present, such as data hiding, encryption algorithm the chances of data breaches continues to increase. This project incorporates chaotic characteristics, while satisfying all the properties of both confusion and diffusion, by providing high level of security during image encryption schemes. Future work, would be a combination of chaotic maps will be tested for better security results, which may include sinh map and quadratic chaotic maps.

This project involved the two operations. Firstly, combining the chaotic map and image with chaotic map as a key to the encryption of image. Secondly, incorporating the output of combined chaotic maps in circular shift and scrambling methods in Matlab. In comparison to existing image encryption schemes, the proposed Chaotic Maps and Image Based Cryptosystem has improved randomness and performance, and reduced execution time thereby enhancing the security of the image.

REFERENCES

[1] ZhongyunHua, Yicong Zhou, Hejiao Huang “Cosine-transformbased chaotic system for image encryption”, Information Sciences Journal,Elsevier, Vol.480,2019.

[2] Y. Zhou, L. Bao, C.L.P. Chen “A new 1D chaotic system for image encryption” Signal ProcessingJournal, Elsevier, Vol.172, 2014.

[3] Z. Hua, S. Yi, Y. Zhou “Medical image encryption using highspeed scrambling and pixel adaptive diffusion” Signal Processing Journal,Elsevier, Vol.144, 2018.

[4] C. Pak, L. Huang, “A new color image encryption using combination of the 1D chaotic map”, Signal Processing Journal,Elsevier ,Vol.138, 2017.

[5] Z. Hua, Y. Zhou “Design of image cipher using block-based scrambling and image filtering”, Information sciences Journal,Elsevier, Vol.396,2017.

[6] M. Murillo-Escobar, C. Cruz-Hernndez, F. Abundiz-Prez, R. LpezGutirrez, O. A. Del Campo, “A RGB image encryption algorithm based on 365 total plain image characteristics and chaos”, Signal Processing Journal, Elsevier , Vol.105, 2015. 46

[7] Z. Hua, F. Jin, B. Xu, H. Huang “2D Logistic-Sine-coupling map for image encryption”, Signal Process Journal, Elsevier, Vol.149,2018.

[8] MeysamAsgari-chenaghlu, “Mohammad-Ali Balafar’A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation”, Signal processing Journal, Elsevier, Vol.157,2018.

[9] Wikipedia contributors, “Logistic Map,” http://en.wikipedia.org/w/index.php?title=Logistic_map&oldid=410 48057, 2006.

[10] Meng Ge, Ruisong Ye “A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties”,Egyptian Informatics Journal,Elsevier , Vol.20,2019.

[11] A.-V. Diaconu “Circular inter–intra pixels bit-level permutation and chaos-based image encryption”, Information Science Journal,Elsevier, Vol.355-356,2016.

[12] Kumar, Gelli MBSS, and V. Chandrasekaran, "A Generic Framework for Robust Image Encryption Using Multiple Chaotic Flows", International journal of computational cognition (http://www. ijcc. Us,) vol.-8, no.-3, pp.13, 2010.

[13] Awad, Abir, and AbdelhakimSaadane, "New chaotic permutation methods for image encryption", IAENG Int. J. Comput. Sci, vol.-37, no.-4, 2010.

[14] Yoon, Ji Won, and Hyoungshick Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps", Communications in Nonlinear Science and Numerical Simulation, vol.-15, no.-12, pp. 3998-4006, 2010.

[15] Alvarez, Gonzalo, and Shujun Li, "Some basic cryptographic requirements for chaos-based cryptosystems", International Journal of Bifurcation and Chaos, vol.-16, no.-08, pp. 2129-2151, 2006.

[16] Scharinger J., “Fast encryption of image data using chaotic kolmogorov flows”, J. Electron Imageing, vol.-7, pp. 318-325, 1998.

[17] Fridrich J., “Symmetric ciphers based on twodimensional chaotic maps”, J. Bifurcat Chaos, vol.- 8, pp. 1259-84, 1998.

[18] Li S J, Zheng X, Mou X and Cai Y, “Chaotic encryption scheme for real-time digital video

Proc SPIE on Electronic Imaging", 4666 149-166, 2002.

[19] Lu J and Chen G R, "A new chaotic attractor coined J. Bifurcation and Chaos", vol.-12, pp. 659-661, 2002.

[20] Chen G R, Mao Y B and Chui C KA, "Symmetric image encryption scheme based on 3D chaotic cat maps", J.Chao, Solitons and Fractals, vol.-21, pp. 749-761, 2004.