ISSN 2688-8300 (Print) ISSN 2644-3368 (Online)

NEW INSIGHTS INTO CHAOS BASED IMAGE ENCRYPTION & ITS APPLICATION

Suvam Mukherjee

Department of Mathematics
Muralidhar Girls' College
P-411/14, Gariahat Road, Kolkata-700029
India
Email: suvampu01@gmail.com

Abstract

Nowadays the whole world is upgrading with different innovative technologies. We need to resist any attack during data transfer over insecure networks. Random nature & sensitivity to initial conditions in dynamical maps are highly useful to secure cryptography algorithms. In this paper, structure of different chaotic maps have been reviewed, basis of chaos-based image encryption has mentioned. Finally a new encryption scheme has been proposed using tent & logistic map. Performance analysis of proposed scheme has been discussed. Different coupling of chaotic maps, aspects of elliptical curve can be considered for compressed image, video or audio encryption as future work.

Keywords: *Nonlinear Dynamics, Chaos, Encryption, Tent map*

Introduction

Chaos: Around 1922, French mathematician Jacques Hadamard introduced the system exhibiting sensitive dependence on initial conditions. Edward Lorenz first proposed the idea of chaotic systems in 1963. Lorenz's talk from 1972 conference become very famous - "Predictability: does the flap of a butterfly's wing in Brazil set off a tornado in Texas?" A small change in initial condition produces rapid divergence for a chaotic system. Belgian physicist David Ruelle first coined the term 'strange attractors' around 1971. Around 1975, James A. Yorke introduced the terminology chaos theory. Mitchell Jay Feigenbaum introduced notion of period doubling in the field of chaos. Chaos theory is an important part of nonlinear dynamics. It measures unpredictability of deterministic nonlinear dynamical systems. Chaotic systems exhibit pseudo-randomness due to sensitivity on initial conditions & also show ergodic properties.

Cryptography: With the rapid spike of technological advancement, we have to rely on insecure networks to transmit a wide range of data. Images, videos, audio files are being shared as information carrier in these channels. So, we need to be concerned about confidentiality, integrity, authenticity of transmitted data. Cryptography provides us the support for such issue. Now what Cryptography is?

ISSN 2688-8300 (Print) ISSN 2644-3368 (Online)

Cryptography is the powerful scientific tool which converts the original information into unreadable form and secures the data transmission from unauthorized users. The Greek etymology of Cryptology, i.e. '*kryptos logia'* means the study of secrecy. It has two parts- Cryptography & Cryptanalysis. So, in other words, Cryptography is the study of secrets & of secure communication in presence of eavesdropping adversaries. There are enough documented evidences in favour of use of ciphers in different era - Scytale Cipher used by Greeks, Hieroglyphs of Egypt, Clay tablets from Mesopotamia, Atbash Cipher of Hebrews, Cryptanalysis of poly-alphabetic cipher by Arabics, Caesar Cipher due to Roman emperor Julius Caesar, Enigma machine used by German military force up to 2nd World War, Vernam Cipher, Hill Cipher. In terms of key exchange, encryption techniques can be categorized as follows:

(a) Symmetric Scheme - AES, DES, 3-DES, RC4, QUAD, IDEA

(b) Asymmetric Scheme - RSA, DSA, ECC, DH Key Exchange

PRINCIPLES OF CHAOS-BASED IMAGE ENCRYPTION

Basic principle of chaotic image encryption lies in dynamical systems. Generally different dynamical maps are employed to produce pseudo-random number sequence to encrypt original figure. Sensitivity to initial conditions, large key space, random characteristic, nonlinear complexity of chaotic maps make them perfect candidate for robust encryption schemes. Generally chaos-based image encryption takes place in two stages- confusion & diffusion. Pixel values of original image are permuted in confusion process while diffusion is employed to transform pixel values in a sequential manner. Close connection between chaotic systems & cryptography has been pointed out in the following table-

Dynamic System	*Cryptography Algorithm*
Set of real numbers	Finite set of integers
Control parameter	Secret Key
Several iterations	Several rounds
Sensitive to initial conditions & control parameters	Diffusion
Nonlinear Structural Complexity	Algorithmic Complexity

LITERATURE REVIEW

According to L. Kocarev, chaotic cryptography seems more powerful than the tradition cryptographic protocols. Compression of data plays a vital role in digital communication [4]. Arnold Cat Map has been used for spatial domain in encryption method proposed by Guan et al. Applying Chen system to output signal, it was encrypted with converted image. The result depicts the large key space's necessity for different attacks & sensitivity of encryption algorithm to keys [5]. The following paper proposed a new encryption technique using chaotic logistic map. Pareek et al. used two logistic maps. Using 80-bit external secret key,

ISSN 2688-8300 (Print) ISSN 2644-3368 (Online)

initial conditions for maps were derived [6]. According to Gao et al., one dimensional chaotic map for image encryption is not secure at all. The author used the notion of hyper-chaos.Initially logistic map had been used for pixel shuffling. Further grey pixels were converted using hyper chaotic system [7]. Huang et al. proposed new pixel shuffling process with multi-chaotic systems. FIPS test had been employed, NPCR & UACI had been calculated using four chaotic systems [8]. Famous work of Pareek et al. used idea of cross coupling of two skew tent maps. Basically output of first one was used as initial condition of other & vice-versa. This process is known as cross-coupling. Bassic statistical tests had been performed to generate binary sequences [9]. The following work is not remarkable except addition of two chaotic systems - Rossler & Lorentz systems. The analysis depicts the necessity of high speed, security & large key space [10]. Kanso introduced interesting self shrinking techniques to produce chaotic key flows having good statistical qualities via one dimensional chaotic map [11]. Works of X. Tong & others incorporated Baker map for permuting original pixel values [12]. While the works of Huang proposed encryption techniques incorporating four dimensional chaotic systems with 3 control parameters. Here partial encrypted results from the permutation matrix had been concatenated for cipher image [13]. Further works of Rajinder Kaur et al. used the notion of partial compression of an image & used chaotic Henon map [14]. Similar works of Lalita Gupta et al. used Baker map in encryption techniques. They discussed about pixel shuffling, bit-wise XOR in confusion process with nonlinear noise function [15]. Rather followings are quite useful observations. Using beta chaotic map, pseudo random numbers were generated to permuting pixel positions. Diffusion & substitution techniques were employed in this technique [16]. Patro & Acharya proposed interesting scheme using multistage permutation incorporating super-chaos [17]. Around 2019, bit-plane based scheme was proposed by Sravanthi et al. The scheme used piece-wise linear chaos & logistic sine map [18]. In tele-medicine, cryptographic protocols play a vital role to provide security. The following work by R. Ali & T.S.Ali is very useful, it proposed a novel image signcryption scheme employing Public key cryptography & elliptic curve cryptography. They used chaotic Henon map, logistic & tent maps. Chaos-based symmetric image encryption provided satisfactory results for key space analysis, correlation, entropy & histogram analysis [19]. Recent work by Faragallah et al. investigated efficiency of chaos-based image block ciphering in spatial & Fractional Fourier Transform (FrFT) domains. The scheme used Arnold Cat map, chaotic Baker map & logistic map. They analyzed cyber security & ciphering efficiency using entropy, differential & histogram analysis [20].

METHODOLOGY

In chaos-based image encryption, every input image is represented by matrix structure of pixel values. Using 8 bits pixel we can represent 2^8 different colors of gray. While we need 24 bits for color pixels (Green, red, blue) to represent 2^{24} different choices of colors. Different chaotic maps are used to generate number sequences, which are pseudo-random in nature.

ISSN 2688-8300 (Print) ISSN 2644-3368 (Online)

Commonly Used Dynamical Map	Description
Logistic Map	Robert May proposed this one dimensional map as follows: $x_{n+1} = \alpha x_n(1-x_n), x_n \in [0,1]$, $\alpha \in [1,4]$ is control parameter
Tent Map	$x_{n+1} = \begin{cases} \lambda x_n, x_n < \frac{1}{2} \\ \lambda(1-x_n), x_n \geq \frac{1}{2} \end{cases}$ $\lambda \in (0,2)$
Henon Map	Michel Henon introduced the two dimensional discrete map around 1976, which is defined as follows: $x_{n+1} = 1 - ax_n^2 + y_n$, $y_{n+1} = bx_n$ a, b are control parameters and 1.4, 0.3 are respective values in general.
Arnold Cat Map	Vladimir Arnold proposed this scheme using an image of a cat in 1960. The process depicts the randomization of original image pixels using modulo operation. The map is defined as: $\Gamma \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+b \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } n)$
Sinusoidal Map	$x_{n+1} = \beta {x_n}^2 sin(\pi x_n), \beta = 2.3$
Baker Map	The two dimensional chaotic Baker Map is defined as follows: $B(x,y) = \begin{cases} (2x, \frac{y}{2}), 0 \leq x < \frac{1}{2} \\ (2x-1, \frac{y+1}{2}), \frac{1}{2} \leq x \leq 1 \end{cases}$ The process first breaks the input square unit into identical parts & then two half parts are concatenated along one another.
Chua Generator	This electronic circuit is first chaos generator from a physical system. It is defined as follows: $\dot{x} = \alpha(y - m_1 x - 0.5(m_0 - m_1)[\lvert x+1 \rvert - \lvert x-1 \rvert])$ $\dot{y} = x - y + z$ $\dot{z} = -\beta y - \gamma z$ Where $\alpha = 9, \beta = 14.28, \gamma = 0, m_0 = -\frac{1}{7}, m_1 = -\frac{2}{7}$
Chebyshev Map	This 3D chaotic map is defined by $x_{n+1} = cos(k \cos^{-1} x_n), -1 \leq x_n \leq 1, k \in \mathbb{Z}^*$

ISSN 2688-8300 (Print) ISSN 2644-3368 (Online)

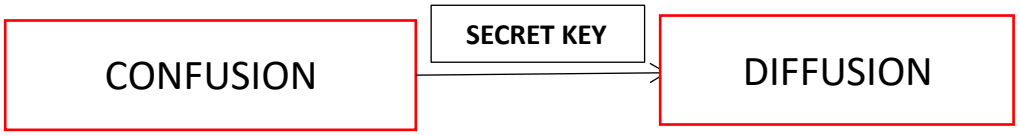

Figure 1: Basic Structure of Chaos-based Image Encryption

In this work, a new encryption scheme is being proposed. Firstly, Tent Map has been used. Depending on initial conditions & control parameters, we can observe the chaotic behavior. Here $\lambda \in (0,2)$ is the control parameter. Pseudo random sequences have been generated using this map. Next, logistic map is used. Figure 2 describes the chaotic behavior of logistic map.

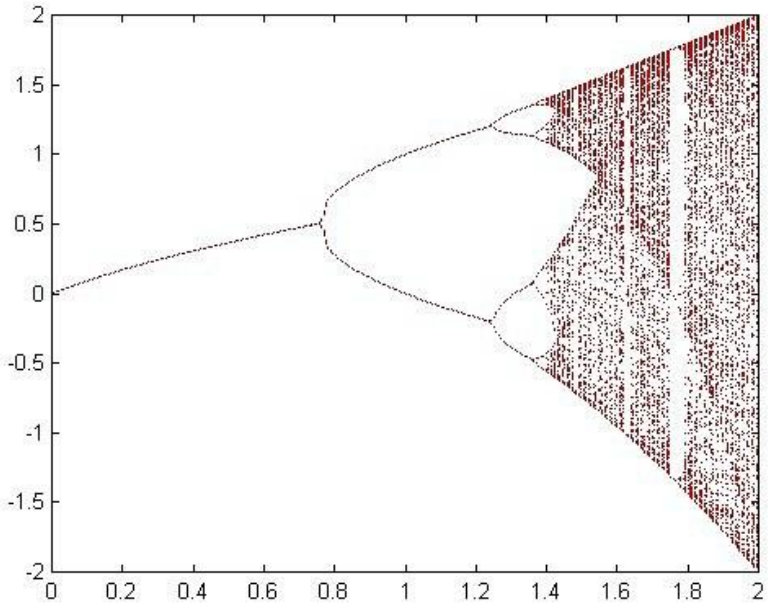

Figure 2: Logistic Map

Output from tent map has been used to generate key using chaotic logistic map. Then bitwise XOR was performed & that XOR output had been stored in secret key matrix. In this case, we have performed NIST proposed statistical tests. The test suit includes frequency test, cumulative sum, entropy, serial, longest run etc. Test results are satisfactory in each case. Original & encrypted images have been shown in figure 3 & 4.

ISSN 2688-8300 (Print) ISSN 2644-3368 (Online)

Figure 3: Original Image

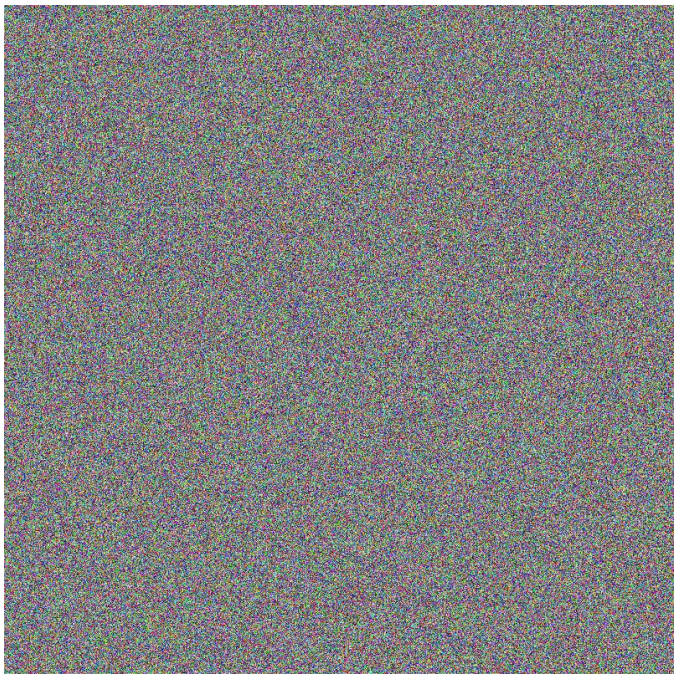

Figure 4: Encrypted Image

PERFORMANCE ANALYSIS

Histogram Analysis:

Histogram analysis is the process of graphical representation of pixels in an image. Pixel distribution over [0, 255] for encrypted image should be uniform. Figure 5 demonstrates uniform characteristic of encrypted image in this work.

ISSN 2688-8300 (Print) ISSN 2644-3368 (Online)

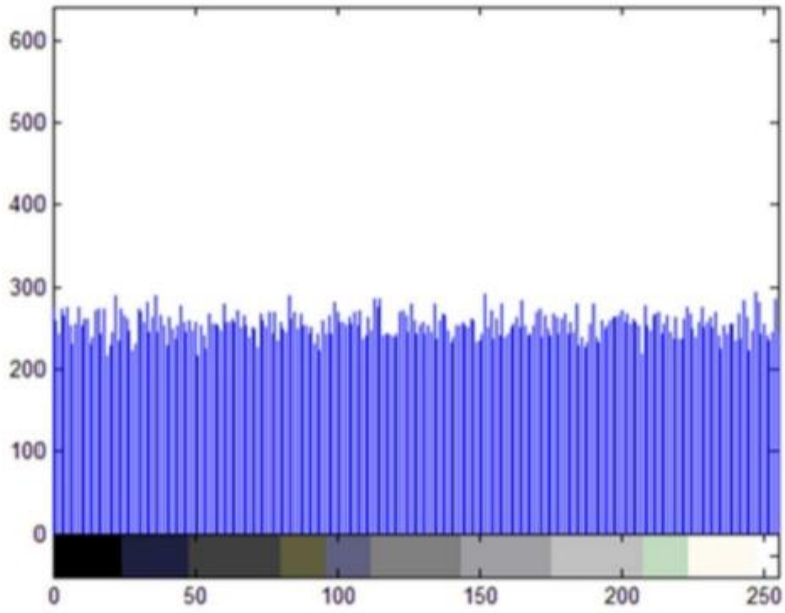

Figure 5: Histogram Analysis of Encrypted Image

Entropy:

Entropy is powerful tool in information theory. In the field of cryptography, it gives the proper insight of encryption scheme. For N number of symbols, entropy of message m is defined as $H(m) = \sum_{k=0}^{N} p(m_i) \log_2 \frac{1}{p(m_i)}$ where $p(m_i)$ denotes the probability of occurrence of symbol m_i.

In this work, calculated entropy values are 6.9505 & 7.9973 for plain-text & cipher images respectively.

Correlation Coefficient:

Correlation between adjacent pixels is vital statistic for image encryption scheme. It depicts the quality of the cryptosystem. To resist cryptanalytic attack, expected correlation coefficient of adjacent pixels in encrypted image is almost zero. It is defined by $\rho_{xy} = \frac{Cov(x,y)}{\sigma(x)\sigma(y)}$ where $\sigma(x)$ is standard deviation of distribution of pixel, x & y be gray-scale values of two pixels at same position in respective original & encrypted images.

In this work, correlational values between adjacent pixels are given by the following table:

Original Image	Encrypted Image
0.9023 (horizontal)	-0.0015 (horizontal)
0.8150 (diagonal)	0.0006 (diagonal)

ISSN 2688-8300 (Print) ISSN 2644-3368 (Online)

UACI (Unified average changing intensity):

Differential attack is important notion in image encryption. UACI is used to compute any difference between original & encrypted image. This intensity is calculated using following relation: $\text{UACI} = \frac{1}{mn}\sum_{i,j}^{m,n}\frac{|P(i,j)-E(i,j)|}{255} \times 100\%$ where m,n are height & width of the image, $P(i,j)\&E(i,j)$ stand for (i,j)th pixel of original image P & encrypted image E respectively. In this work, UACI is 32.4736%.

APPLICATION

- Watermarking is important for image authentication. Discrete wavelet transformation is applied for embedding of watermarking. Chaotic maps are used to encrypt watermark & low frequency parts are extracted. These parts need to embed into that of original figure. This type of scheme is effective for image compression, noise attack etc.
- Signcryption scheme is very interesting & effective scheme for medical imaging encryption during data transmission over insecure channel. The process using number theoretical approach is highly effective in healthcare system.
- Remote sensing is a hot topic nowadays. But due to high computational time, traditional cryptography protocols are not suitable enough. For satellite imagery processing, security issue is highly expected. In this regard, multi- chaos based schemes are being used to produce pseudo random key sequences. Bit wise XOR operation is being performed sequentially for encryption & decryption of images.
- In the field of parallel computing, different advanced softwares are being used. Nvidia introduced GeForce 256 in 1999,first Graphics Processing Unit (GPU). With the advancement of technology, powerful languages like CUDA, OpenCL have been used for GPU. Gradually GPU is being used in various fields- financial markets estimate, Seismography, Machine learning & AI etc. Chaos based encryption schemes play a vital role. Previous values in recursive maps may generate some problem for parallel processing. So we need to encrypt multiple images using single key generation step.

REFERENCES

[1] Strogatz, S.H., "Nonlinear Dynamics And Chaos : With Application to Physics, Biology, Chemistry and Engineering", CRC Press, 1st edition, ISBN-13: 9780738204536 (2000).

[2] Lakshmanan, M., Rajasekar, S., "Nonlinear Dynamics: Integrability, Chaos and Patterns", Springer - Verlag, Berlin, Heidelberg (2003).

[3] Paterson, M., Stinson, D., "Cryptography: Theory and Practice", 4th edition, CRC Press (2018).

[4] Kocarev, L., Chaos-based cryptography: a brief overview, IEEE Circuits and Systems Magazine, 1(3), pp. 6-21 (2001)

ISSN 2688-8300 (Print) ISSN 2644-3368 (Online)

[5] Guan Zhi-Hong, Huang Fangjun, Guan Wenjie, Chaos-based image encryption algorithm, Physics Letters A, 346(1-3), pp. 153-157 (2005)

[6] Pareek, N.K., Patidar, V., Sud, K.K., Image encryption using chaotic logistic map, Image & Vision Computing, 24(9), pp. 926-934 (2006)

[7] Gao, T., Chen, Z., A new image encryption algorithm based on hyper-chaos, Physics Letters A, 372(4), pp. 394-400 (2008)

[8] Huang, C.K., Nien, H.H., Multi Chaotic system based pixel shuffle for image encryption, Optics Communication, 282, pp. 2123-2127 (2009)

[9] Pareek, N.K., Patidar, V., Sud, K.K., A random bit generator using chaotic maps, International Journal of Network Security, 10(1), pp. 32-38 (2010)

[10] Patel, K.D., Belani, S., Image Encryption Using Different Techniques: A Review, International Journal of Emerging Technology and Advanced Engineering, 1(1), November (2011)

[11] Kanso, A., Self-shrinking chaotic stream ciphers, Communications in nonlinear science and numerical simulation, 16(2), pp. 822-836 (2011)

[12] Tong, X.J., Liu, Y, Zhang, M., Wang, Zhu, A Novel Image Encryption Scheme Based on Dynamical Multiple Chaos and Baker Map, 11th International Symposium on Distributed Computing and Application to Business, Engineering & Science (2012)

[13] Hung, X., A new digital image encryption salgorithm based on 4D chaotic system, International Journal of Pure and Applied Mathematics, 80(4), pp. 609-616 (2012)

[14] Kaur, R., Singh, K., Comparative Analysis and Implementation of Image Encryption Algorithms, IJCSMC, 2(4), pp. 170-176, April (2013)

[15] Gupta, L., Gupta, R., Sharma, M., Low Complexity Efficient Image Encryption Technique Based on Chaotic Map, International Journal of Information & Computation Technology, 4(11), pp. 1029-1034 (2014)

[16] Zahmonl, R., Ejbali, R., Zaied, M., Image encryption based on new beta chaotic maps, Opt. Lasers Eng, 1(96), pp. 39-49 (2017)

[17] Patro, K., Acharya, B., Secure multi-level permutation operation based multiple color image encryption, J Inf Secur Appl., 40, pp. 111-133 (2018)

[18] Sravanthi D et al., A secure chaotic image encryption based on bit-plane operation, Soft computing in data analytics, Springer, Singapore, pp. 717-726 (2019)

[19] Ali, Tahir & Ali, Rashid, A novel medical image signcryption scheme using tent-logistic-tent system and Henon chaotic map, IEEE Access, 10.1109/ACCESS.2020.2987615

[20] O.S. Faragallah et al., Investigation of Chaotic Image Encryption in Spatial and FrFT Domains for Cybersecurity Applications, IEEE Access, vol.8, pp. 42491-42503 (2020)

[21] Wang, X., Gao, S., Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory, Information Sciences, vol. 507, pp. 16-36 (2020)