A Review of Chaos Based Image Encryption Techniques

Manasi Hazarika
Department of Computer Science & Engineering and Information Technology,
Assam Don Bosco University
Guwahati, Assam 781017, India

***Abstract*—Information Security is a primary concern of communication. Increasing rate of Image applications demands a good cryptosystem for image security. Unfortunately traditional cryptosystem is not very suitable for multimedia applications due to their statistical property while sensitivity to initial condition makes chaos very popular for image encryption. A variety of methods for image encryption based chaos have been developed in recent years. In this paper we are trying to discuss some of the chaos based algorithm for image encryption.**

Keywords—Chaos, Cryptography, Image encryption, Entropy, Image Correlation.

I. INTRODUCTION

Multimedia data transmission over internet is increasing day by day but at the same time information security is also important especially in case of highly confidential information. Applications of military affairs, multimedia messaging system, confidential video conferencing and many such applications demand highly secure system for storage and as well for transmission of multimedia information like digital images. As a result multimedia information security has become a very popular area of research. Unfortunately traditional cryptosystem like AES, DES are not suitable for Image or video encryption [1] because of some properties of images or videos like spatial redundancies, file size etc. Recently researchers are more attracted towards chaos based encryption systems for image encryption. This concept is not new and instance of it can be traced from Shannon's Classic paper which was published in 1952[2]. The idea behind the use of chaos in cryptography is that chaos has got some characteristics like highly sensitive to initial condition and control condition, ergodicity, pseudo-randomness [3]. These characteristics are very essential for good confusion and diffusion. A good cryptosystem should have a good confusion and diffusion methods. Confusion aims to reduce the correlation between pixels without altering the values while diffusion aims to change values of all the pixels of the image by making tiny changes. Butterfly affect of chaos makes diffusion effective.

In the year 1989 Mathews first derived a chaotic map and suggested to use for cryptography [4]. Since then many image encryption schemes based on chaos has been developed. Chaos based encryption techniques are gaining popularity amongst the researchers as they provide high security, efficiency in speed and complexity.

II. IMAGE ENCRYPTION BASED ON CHAOS

Like conventional encryption schemes Chaos based encryption also involves in both confusion and diffusion phase. A variety of chaotic maps have been used by the researchers to for both the confusion and diffusion stage. Choosing a chaotic map is very important. A chaotic map with robust chaos, good mixing property and a large parameter set only should be chosen [5]. Some of the popular chaotic maps are listed as below.

A. Logistic Maps

Logistic maps are polynomial maps of degree 2. It was popularized after a seminar presented by a biologist Robert May in year 1979 [6]. It is characterized by the equation [7]

$$x_{n+1} = rx_n\,(1 - x_n) \qquad (1)$$

Where $x_n \in$ [0-1], *n* is the number of iterations and r =4.

B. 2D Cat Map

In 1960s Vladimir Arnold had discussed a chaotic map using an image of cat [8]. The two dimensional transformation is carried out using the following equation.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mathrm{mod}1 \qquad (2)$$

C. Tent Map

It is a one dimensional, non linear map defined by the equation

$$\mathrm{x}_{n+1} = \mathrm{f}_{\mu}(\mathrm{n}) = \mathrm{f}(\mathrm{x}) = \begin{cases} \mu \mathrm{x}_n, & \mathrm{x}_n < \frac{1}{2} \\ \mu(1 - \mathrm{x}_n) & \mathrm{x}_n \geq \frac{1}{2} \end{cases} \qquad (3)$$

Where, xn ∈ [0-1] and μ is a real positive number.

A Tent map shows a range of dynamical behavior ranging from predictable to chaotic depending on the value of μ [9].

D. Baker Map

The "Baker" has come from the kneading process that a baker applies to dough. It is another form of chaotic map which comes from the unit square into itself. The unit square is divided into two parts, then they are stacked one another and then is stretched. The general equation for 2D folding map is as follows.

$$\begin{bmatrix} x_b \\ y_b \end{bmatrix} = f(x) = \begin{cases} \left(2x, \frac{y}{2}\right) \; for \; 0 \le x \le \frac{1}{2} \\ (\left(2 - 2x, 1 - \frac{y}{2}\right) \; for \frac{1}{2} \le x \le 1 \end{cases} \qquad (4)$$

E. Standard Map

It is an area-preserving map for two canonical dynamical variables, momentum and coordinate (p,x) which is also known as Chirikov standard map [10] . It is described by the equations:

$$p^{'} = p + Ksinx \qquad (5)$$
$$x^{'} = x + p \qquad (6)$$

Where, K is a dimensionless parameter that influences the degree of chaos and $p^{'}$ and $x^{'}$ are resultant vaules.

III. ANALYSIS OF DIFFERENT CHAOS BASED IMAGE ENCRYPTION TECHNIQUES

In the paper, A new chaotic algorithm for image encryption, Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li presented a new non linear chaotic algorithm (NCA) [11]. To overcome the limitations of one dimensional logistic map like small key space, weak in security NCA uses power function and tangent function instead of linear function. In the algorithm once the key is set then chaotic map is iterated 100 times. The encrypted image is then sent through public communication channel while the encryption key is sent though a secure channel. At receiving site same method is used for decryption as that of encryption. Key space size is 1045 which is much larger than that of 56 DES Algorithm:256. It satisfies the characteristics of traditional cryptosystem like zero- correlation, balanced 0–1 ratio and ideal nonlinearity. It can resist statistic attack and grey code attack.

Daniel Socek, Shujun Li, Spyros S. Magliveras and Borko Furht have introduced an Enhanced 1-D Chaotic Key-Based Algorithm (ECKBA) for Image Encryption [12]. In their work, they have enhanced an already existing algorithm Chaotic-Key Based Algorithm (CKBA) [13] by changing 1-D chaotic logistic map to a piecewise linear chaotic map to improve the balance property and to increase the key size. In the proposed system the target image is transformed using SP network generated by a one-dimensional Zhou's map and a 128-bit secret key. They have used double precision (64 bit) floating point output mapped to 32 bit integer whereas in original CKBA 16-bit precision was used. ECKBA has a very high key space of 128 bits and is secure to known/chosen plaintext attack.

N.K. Pareek, Vinod Patidar, K.K. Sud have presented an image encryption algorithm by using a1D chaotic logistic map[14].In the an 80 bit long encryption key is used which is further divided into 10 blocks, known as session keys. By providing different weightages to all its bits, the initial conditions for both the logistic maps are derived using the external secret key. In the algorithm, the first logistic map is used to generate numbers ranging from 1 to 24 (numbers may be repeated). Using the numbers generated from the first logistic map the initial condition of the second logistic map is modified. To encrypt a pixel, based on the outcome of the logistic map a operation is chosen out of eight different types of operations. To make the cipher more robust, the secret key is modified after encrypting each block pixels of the image. The method has low time consumption. But the major drawback is its key space, which is very low for brute-force attack. The method was cryptanalyzed in [14] and found that is insecure against chosen plaintext attack and also it was showed that the method has some invalid, weak and partial keys which further reduces key space.

A novel chaos-based image encryption scheme using affine modular maps has been proposed by Ruisong Ye and Haiying Zhao in their work [15]. They used affine maps for both confusion and diffusion. Separate key have been used for confusion and diffusion. Two affine modular maps are used for permutation process to yield two index order sequences for shuffling of pixel positions of the, while in diffusion process another two affine modular maps are used to get two pseudo-random gray value sequences for a two-way diffusion of gray values. The algorithm has the advantages such as large key space which is more than 10191, highly sensitivity to the cipher keys and plain-images, almost zero pixel correlation in case of the encrypted image, entropy of the encrypted image of 8 bit Lena image is found as 7.9965 bits, has high NPCR and UACI and can resists chosen/known plaintext attack.

Using bit level permutation a chaos based symmetric image encryption scheme has been proposed by Zhi-liang Zhu, Wei Zhang , Kwok-wo Wong and Hai Yu in [16]. Arnold's cat map is utilized for bit level permutation and for diffusion logistic map is used for diffusion. For the confusion phase the image is divided into a group of images based on bit position of the pixels, for example for an 8-bit image will have 8 different images according to the bit position of each pixel. Since the higher order bits carry more information than the lower order, the first four higher order bits viz, 7th to 4th are permuted individually using the same chaotic map but with different coefficients and the remaining four bits are permuted as a whole to reduce the execution time. The result of permutation in bit level not only alters the locations of the pixels but also alters the value of each pixel. For diffusion, the pixels are scanned horizontally from the left top corner to the right bottom corner to get a sequence. Then using a logistic map each pixel value is altered sequentially in pixel level. The advantages of this algorithm are a high NPCR, UACI and entropy. So this can resist known plaintext attack and differential attack. Key space of this algorithm is 1042.

A fast image encryption and authentication scheme based on chaotic maps has been proposed by Huaqian Yang, Kwok-Wo Wong, Xiaofeng Liao, Wei Zhang, Pengcheng Wei. The encryption key is generated by applying a hash function to the plain image. This is done using a tent map. In case of an 8-bit grey-scale plain-image, pixels are scanned row wise to form a one dimensional sequence and then padded with zeros to make the length of the sequence a multiple of 4 pixels. After that it is divided into blocks of 4 pixels. To generate the hash key four initial secret keys within the range 0-1 are chosen randomly. Secret keys are then mixed with the pixels and the tent map is iterated several times to get the final hash key. In their proposed scheme they employed standard map for permutation. Since in case of standard map the corner pixels are not permuted at all they included a random scan couple so that the corner pixels are also gets permuted along with the other pixels. Logistic map has been employed for the diffusion process. In this phase pixel values are modified sequentially and encrypted a value of a pixel is dependent on the accumulated effect of all the previous pixel values. The proposed algorithm has a key space of 128-bits and is sensitive to the key even for a difference as small as 10-10. It has a high NCPR and UACI. So it can resist differential attack and known plaintext attack. [17]

In the paper [18], a chaos-based image encryption algorithm using alternate structure is proposed by YiWei Zhang, YuMin Wang, and XuBang Shen. In the proposed scheme a grey image with size N×2N (height×width), which can be denoted by an N×2N matrix in domain Z256 is chosen. Each part is encrypted using different keys. So combination of both keys composite the encryption key. In the algorithm, for both the permutation and diffusion general cat-map is used and one way coupled map lattice is applied for substitution. In every round of encryption these two methods are used alternatively. This was cryptanalized in [19] and the major defect they found are firstly the actual key-space is 232 only which is very less to resist brute force attack, secondly the cipher image is insensitive to the changes of the plain image and also insecure against differential attack when an important integer parameter is odd.

In [20], an Improved Image Encryption Algorithm based on chaotic System has been proposed. The main part of the proposed scheme is a chaos-based pseudo-random keystream generator (PRKG) based on a couple of chaotic systems. In PRKG, two logistic chaotic systems are used with different initial values. Parameters of second logistic systems are updated based upon the random numbers generated from the first. At first plain-image is converted into binary data stream. Before encryption, the random keystream generated by PRKG is used to mask these binary data stream. The key size of the algorithm is 2196 if 10-15 precision is used. Experimental result shows almost pixel correlation coefficient in the cipher image [20].

An image encryption based on a new total shuffling algorithm has been proposed in [23]. For shuffling the positions of image pixels, a total shuffling matrix has been introduced. This matrix has been generated by iterating logistic map several times and then transposing the matrix. Using Lorenz chaotic system and Chen's chaotic system the final cipher has been obtained. This scheme has been cryptanalyzed in [22] and has found several defects. These are low sensitivity to the change of plain-image, small key space, vulnerability to chosen plaintext attack and most importantly low speed. So it is not applicable for practical scenario as speed is a very essential factor for real time application.

A novel image encryption algorithm based on a 3D chaotic map has been presented by A. Kanso and M. Ghebleh in [21]. The proposed algorithm is divided into three phases. In phase I pixel blocks of the original image are shuffled based upon the output of a 3D chaotic map cat map using a search rule, CR. In phase II, a random like sequence is generated by iterating 3D cat map. Based on this sequence the shuffled data stream is scrambled and mixed again to achieve sensitivity to the plain image under a mixing rule, MR. The resulting pixels of phase II are masked in phase III based on the output of a 3D cat map under a particular search rule, DR. The algorithm has a very high key space, which is at least 21392; thereby making brute force attack impossible. The algorithm is also resistant to differential attack.

Ji Won Yoon and Hyoungshick Kim have proposed an image encryption scheme with a pseudorandom permutation based on chaotic maps in [24]. In the proposed scheme for both encryption and decryption, a common process is suggested to build a large permutation matrix by combining several small matrices generated nonlinearly by a chaotic map. According to the proposed scheme an application developer can choose any chaotic map for implementation. Authors have used logistic map for the implemented the proposed algorithm.

IV. CONCLUSION

Confidentiality is a very important criterion for information security. So far many algorithms have been designed for digital image encryption and researchers have found chaos based approach more suitable for digital image encryption due to some intrinsic properties of digital images. The algorithms are basically analyzed based on technique, key space and susceptibility to different types of attacks. Along with resistance against different types of attacks, speed is also very essential requirement for real time applications. Keeping these things in mind we can conclude that chaotic based algorithms are very much suitable for real time applications and each technique.

REFERENCES

[1] Schneier, B., Cryptography: Theory and Practice, Boca Raton, CRC Press, 1995.

[2] Jiri Fridrich,"Symmetric Ciphers Based On Two Dimensional Chaotic Maps" in International Journal of Bifurcation and Chaos, Vol. 8, No. 6, 1998, pp. 1259-1284

[3] A. SENGUPTA, "TOWARD A THEORY OF CHAOS", in International Journal of Bifurcation and Chaos, Vol. 13, No. 11, 2003, pp. 3147-3233

[4] Matthews, R., "On the derivation of a chaotic encryption algorithm", Cryptologia, 1989, 8: 29-41.

[5] M. S. Baptista, "Cryptography with chaos", Phys. Lett. A, Vol. 240, pp.50-54, 1998.

[6] R.M.May, "Simple mathematical models with very complicated dynamics", Nature, 26: 459-467, 1976.

[7] www.http://en.wikipedia.org/wiki/Logistic_map

[8] Arnold V and Avez A., "Ergodic problems of classical mechanics", Benjamin; 1968.

[9] http://en.wikipedia.org/wiki/Tent_map

[10] B.V.Chirikov, "Research concerning the theory of nonlinear resonance and stochasticity", Preprint N 267, Institute of Nuclear Physics, Novosibirsk , 1969

[11] Haojiang Gao , Yisheng Zhang, Shuyun Liang, Dequn Li, "A new chaotic algorithm for image encryption", Chaos, Solitons and Fractals 29, pp. 393–399, 2006

[12] Daniel Socek, Shujun Li, Spyros S. Magliveras and Borko Furht , "Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption", in First International Conference on Security and Privacy for Emerging Areas in Communications Networks, pp. 406-407, 2005

[13] J.-C. Yen and J.-I. Guo, "A new chaotic key-based design for image encryption and decryption", in IEEE International Conference on Circuits and Systems, Vol. 4, 2000, pp 49–52

[14] Chengqing Li, Shujun Li, Muhammad Asim, Juana Nunez, Gonzalo Alvarez and Guanrong Chen, "On the security defects of an image encryption scheme", in Image and Vision Computing 27, pp. 1371–1381, 2009

[15] Ruisong Ye and Haiying Zhao, "An Efficient Chaos-based Image Encryption Scheme Using Affine Modular Maps", I. J. Computer Network and Information Security, Vol. 7, pp. 41-50, 2012

[16] Z.-l. Zhu, W. Zhang, K.-w. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation", Information Sciences, vol. 181, pp. 1171-1186, 2010.

[17] Huaqian Yang, Kwok-Wo Wongb, Xiaofeng Liao, Wei Zhang, Pengcheng Wei , "A fast image encryption and authentication scheme

based on chaotic maps," Commun Nonlinear Sci Numer Simulat 15, pp. 3507–3517, 2010

[18] Zhang, Y., Wang, Y., Shen, X., A chaos-based image encryption algorithm using alternate structure. Science in China Series F-Information Sciences 50, pp. 334–341, 2007.

[19] Cryptanalyzing a chaos-based image encryption algorithm using alternate structure,Leo Yu Zhanga,b, Chengqing Li, Kwok-Wo Wongd, Shi Shua, Guanrong Chend, The Journal of Systems and Software 85, pp. 2077– 2085, 2012

[20] Shubo Liu, Jing Sun, Zhengquan Xu and Zhengquan Xu1, "An Improved Image Encryption Algorithm based on Chaotic System", JOURNAL OF COMPUTERS, VOL. 4, NO.11, 2009

[21] A. Kanso and M. Ghebleh , "A novel image encryption algorithm based on a 3D chaotic map", Commun Nonlinear Sci Numer Simulat 17, 2012

[22] David Arroyo, Chengqing Li, Shujun Li, Gonzalo Alvarez and Wolfgang A. Halang "Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm", JOURNAL OF COMPUTERS, VOL. 4, NO. 11, 2009

[23] T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm",Chaos, Solitons and Fractals 0, 2007

[24] Ji Won Yoon a, Hyoungshick Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps", C ommun Nonlinear Sci Numer Simul, 15,pp.3998–4006, 2010.