Analysis of Statistical Properties of Chaos based Image Encryption by Different Mappings

Leyla Roohi
University Technology Malaysia (UTM)

Subarih Ibrahim
University Technology Malaysia (UTM)

Rezza Moieni
University Technology Malaysia (UTM)

ABSTRACT

Chaos mappings attracted a lot of research in recent years because of good properties of chaos maps in terms of continuous broad band power spectrums, sensitivity to initial conditions and similarity to random behavior. Many different scheme and algorithms have proposed in image encryption by chaos maps as well as different mappings. Not only can the structure of algorithm effect on statistical properties of image encryption, but also different chaos maps can, because of different dynamical properties. PWLCM has attracted a lot of research on recent years regarding good dynamical properties. In following sections, the statistical properties of Yoon algorithm [7] will analysis with PWLCM to conclude better statistical properties and better key space.

Keywords

chaos map, PWLCM, image encryption

1. INTRODUCTION

In recent years chaos based algorithms have become an important field of cryptography. Scharinger [1] introduced chaos theory to encryption. After that, Fridrich [2] showed a general framework for using discrete chaotic maps for encrypting images. This framework has been utilized many times and for image encryption, for example the works which was done by [3]. In this framework the analog chaotic map is first discretized and then it is generalized by the entry of some parameters. The parameters of the map serve the purpose of the key for encryption system. This discrete generalized parameterized map is used in the encryption algorithm.

Chaos-based image encryptions have been categorized by their architecture and their mapping. Due to chaos-based image cryptosystems architecture, they can be categorized in these three different categories as follows [4]: Permutation, Diffusion, and Permutation-Diffusion.

Different architecture can utilize different chaos mapping for permutation and substitution. There are analog and discrete maps and also, linear and non-linear ones that can be classified by the number of strings to make: One dimensional, two dimensional, Three dimensional and multi-dimensional.

The algorithm has implemented with logistic map that has some problems should be considered and it conducts the crypto systems to utilize an alternative like piece wise linear map (PWLCM) [5] , [6].

PWLCM is a one dimensional map that has better balance property and a wider range of control parameter choices in comparison to logistic map. PWLCM is a one dimensional map and this category is easy to implement because it uses a non-complex equation as compared to two or three dimensional maps. The following sections describe.

2. PREMUTATION-DIFFIUSION SCHEME

A permutation-diffusion algorithm was proposed by [7]. The algorithm is based on a large pseudorandom permutation which is produced from tiny permutation matrices that are based on chaos-based maps. This algorithm proposed a new image encryption algorithm with a large pseudorandom permutation which is computed from chaotic maps combinatorially. Since a pseudorandom sequence is securely extended by a permutation matrix, the proposed encryption algorithm shows secure statistical information with relatively short pseudorandom sequences compared to other encryption algorithms.

There are five steps in this algorithm as follows and for better security step (iv) and (v) are repeated K times**:**

(i) Key generation
(ii) Small matrix generation
(iii) Permutation matrix construction
(iv) Permutation
(v) Masking

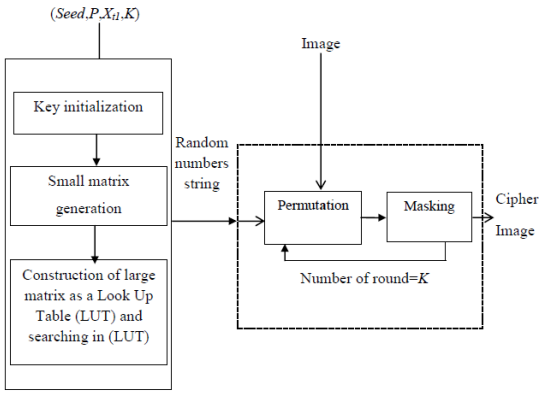


Figure 1: Diagram of Yoon [7] scheme

The first three steps are for enhancing Logistic map. Steps (iv) and (v) are for shuffling of image and masking it. The steps are as depicted in Figure 1.

After key initializing small matrices are built by PWLCM and become ready for creating the Look Up Table (LUT) in the next step. In the third step of algorithm searching is done in

LUT to find random number without creating of LUT. In the fourth step with random number string that is created in the third step the image pixels shuffle. After that the shuffled image XOR with random string that is created in third step.

3. Development phase: Small Matrices Generation

One dimensional defines the simplest forms of a chaotic process. One iteration operation of one dimensional map can produce one arbitrary stream. One dimensional chaotic map has the advantages of high level efficiency and simplicity in comparison to two and three dimensional maps. Many one dimensional chaotic maps introduces in recent years.

Piecewise linear chaotic map (PWLCM) is an attractive research trend in applying the chaos theory and techniques to cryptography recently, in which many new cryptosystems and algorithms have been proposed. PWLCM is a map composed of multiple linear segments. This mapping is proposed by Zhou [8]. PWLCM has perfect dynamical properties and can be realized simply in both hardware and software. PWLCM are widely used in digital chaotic ciphers [9], [10]. Awad showed that PWLCM has better statistical properties than Logistic map[11]. Especially, Logistic map has poor balance properties in comparison to PWLCM. Socek [12] examined that PWLCM has better statistical properties in comparison to Logistic map. It shows balance (uniformity) is better in PWLCM for proving these 10000 samples from 100 set of sequence in 32 and 16 bit resolution chose and percentage of zeroes and ones calculated. According to this, the percentage of zeroes and ones was very close in PWLCM and this means better balance property in this mapping. Equation 1 shows PWLCM.

$$x(n) = F[x(n-1)] = \begin{cases} x(n-1)x\dfrac{1}{p} & if\ 0 \le x(n-1) < p \\ [x(n-1)-p]x\dfrac{1}{0.5-p} & if\ p \le x(n-1) < 0.5 \\ F[1-x(n-1)] & if\ 0.5 \le x(n-1) < 1 \end{cases}$$

Where the positive control parameter and the initial condition are respectively p ϵ (0; 0.5] and x(n) ϵ [0; 1].

However, all of digital chaotic iterations are constrained in a discrete space with 2N elements where N is the length of precision, it is obvious that every chaotic orbit will finally be periodic and will go to a cycle with limited length not greater than 2N. Short period of chaos maps after implementation can degrade the dynamical properties of chaos maps. [13] Studied series of dynamical indicators, which can quantitatively reflect the degradation effects on a digital PWLCM. He also categorized the remedies of the dynamical degradation of computerized chaos maps. Cascading multiple chaotic systems as a remedy introduced by [14], two cascaded chaotic systems are used to increase the cycle length of the generated digital chaotic orbits in a spread spectrum communication system, where one chaotic system is used to initialize another one every N iterations. Such a remedy can increase the length of the controlled pseudo-orbit to O (N) times. In this paper we use two PWLCM by cascading method to overcome dynamical degradation of PWLCM and to reach larger key size as well.

For development of step two of Yoon algorithm PWLCM is used for shuffling Small matrices that are generated based on seed value. In this algorithm we chose the seed as a 24 bit value [7]. Then every 4 bits are assumed as one number. For example if the seed value is [0011 1001] =0 39 the two values for this seed are 3 and 9. The matrix size is calculated by adding the values by 2 because matrix sizes of 0 and 1. Matrices size 0 and 1 are not suitable values for small matrices because 0 means no matrix and 1 means just a single number in a matrix, thus cannot be considered as a matrix. Hence, the size of small matrices are m1= 5 and m2= 11 after adding 2. Small matrices are created as follows:

(i) Without losing generality, if the size of small matrices derived from Seed are {m1,m2,mi,…mn} where i=1 to n and mi is the size of small matrices, each small matrices is built as follows:

$$Mi = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 2 & 2 & & 2 \\ \vdots & & \ddots & \vdots \\ mi & mi & \cdots & mi \end{bmatrix} \quad (2)$$

(ii) Shuffle the values of Mi by using new map and then use Knuth shuffling Equation 3.

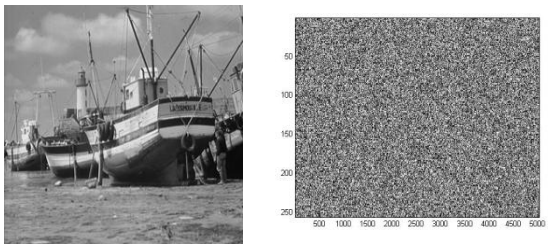
$$Mi(t) \leftrightarrow Mi\ (mod(Fp(Xt)*103, mi) \quad (3)$$

According to Knuth shuffling each column of small matrix shuffles separately by the random string that is generated by cascaded PWLCM. At the end of this step all small matrices are built. At the next step creating big matrix as a Look Up Table (LUT) is done by using small matrixes. If each column is assumed as a vector and Hamming distance between every two vectors is d. The Hamming distance should be at least mi-1. Hence, there is no same element in each row and each column as well. Hence, if the numbers are chosen from column or row a string with long Period is created to permute plain image.

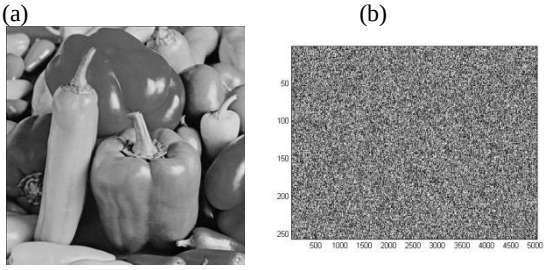
SECURITY ANALYSIS

A good encryption scheme should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. In this section, we will discuss the security characteristics of the improved encryption scheme by means of statistical analysis, key space analysis and information entropy analysis.

In this section, results of Yoon algorithm with new chaos map on test images Fishing boat and peppers 256*256 are shown. Different number of rounds is evaluated in this algorithm and results as well. Correlation coefficients (vertical, horizontal and diagonal) for two adjacent pixels and entropy of mentioned rounds are measured. Initial value for seed= [101110011101011011010011] in following sections.



(a) (b)



(c) (d)

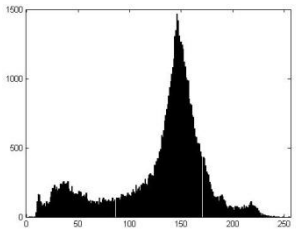
Figure2: (a),(b) Fishing boat Plain Image and Its cipher (k=2), (c), (d) Peppers Plain Image and its cipher Image (k=2)

4.1 Statistical Analysis

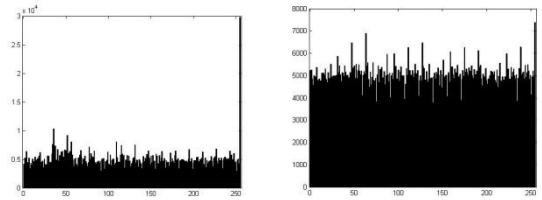
To prove the improved cryptosystem against any statistical attack, the histograms and the correlations of two adjacent pixels in the encrypted images are analyzed in this part.

4.2 Histogram

A widely used measurement for reconstructed images for an n x m size image is the histogram. The histogram can tell, whether or not an image has been properly exposed or not. In other words, an image-histogram demonstrates how pixels in an image are distributed by graphing the number of pixels at each color or grey scale intensity level. Fig 3 and 4 (a) shows histogram of Fishing boat and Peppers, (b) and (c) shows histogram of cipher image with Logistic map and PWLCM. As we can see, the histograms of the cipher images are significantly different from that of the original image in both images. Better results are obtained with PWLCM as the different gray levels of the image are almost equally distributed over pixels (Logistic map scale is 104 while 103). It means the encrypted image with new map provide better security features that can strongly resist against statistical attacks.

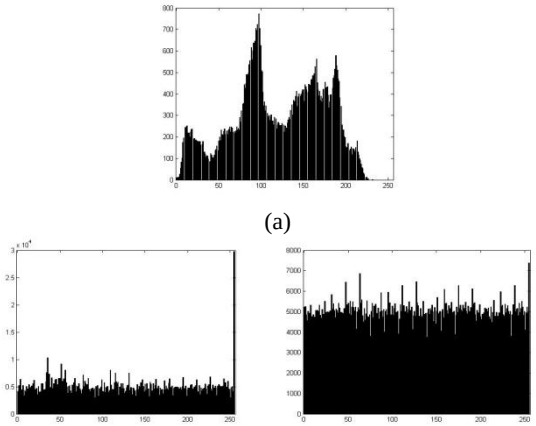


(a)



(b) (c)

Figure 3: (a) Histogram of Plain Image Fishing boat (K=2), (b) Histogram of Fishing boat Cipher Image with Logistic map,(c) Histogram of Fishing boat Image with PWLCM.



(a)

(b) (c)

Figure 4: (a) Histogram of Plain Image Peppers (K=2), (b) Histogram of Fishing boat Cipher Image with Logistic map,(c) Histogram of Peppers Cipher Image with PWLCM.

4.3 Correlation Coefficient

The correlation is a metric which shows the correlation between two adjacent pixels in encrypted images. The ideal correlation tends to be zero in cryptography. The correlation coefficients of vertical, horizontal and diagonal two adjacent pixel measurements for Logistic map and PWLCM are shown

In Table1 to Table 6, it can be seen that correlation coefficient of different rounds for both test pictures are reduced significantly with new map. In Fig 5 and 6 we can also see a good distributed pattern of cipher images in comparison to plain images. Better distributed pattern can be seen for Yoon algorithm with PWLCM in figure 5(b) and 6(a).

Table1: Vertical Correlation Coefficients for Different Rounds with PWLCM

Vertical	K=2	K=4	K=8	K=10
Boat	-0.0025	0.0226	-0.0023	0.0019
Peppers	-0.0076	0.0268	-0.0292	-0.0028

Table2: Vertical Correlation Coefficients for Different Mapping

Vertical	K=2	K=4	K=8	K=10
Boat	-0.0236	-0.0466	-0.0027	0.0257
Peppers	-0.0199	-0.0529	-0.0108	0.0359

Table3: Horizontal Correlation Coefficients for Different Rounds with PWLCM

Horizontal	K=2	K=4	K=8	K=10
Boat	-0.0096	0.014	-0.0127	0.0316
Peppers	-0.0004	-0.0145	-0.0001	0.0253

Table 4: Horizontal Correlation Coefficients for Different Rounds with Logistic map

Horizontal	K=2	K=4	K=8	K=10
Boat	0.0168	0.0335	-0.0053	0.025
Peppers	0.0158	0.0292	0.0068	0.0142

Table 5: Diagonal Correlation Coefficients for Different Rounds with PWLCM

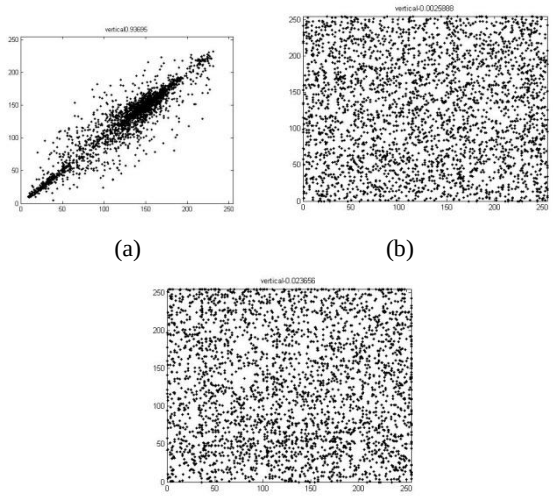
Diagonal	K=2	K=4	K=8	K=10
Boat	-0.0161	-0.0006	0.003	-0.0064
Peppers	-0.0151	0.001	0.0071	0.0003

Table 6: Diagonal Correlation Coefficients for Different Rounds with Logistic map

Diagonal	K=2	K=4	K=8	K=10
Boat	0.0136	0.0134	0.0239	0.0172
Peppers	0.0072	0.0023	0.0163	0.012

3.4 Key Space Analysis

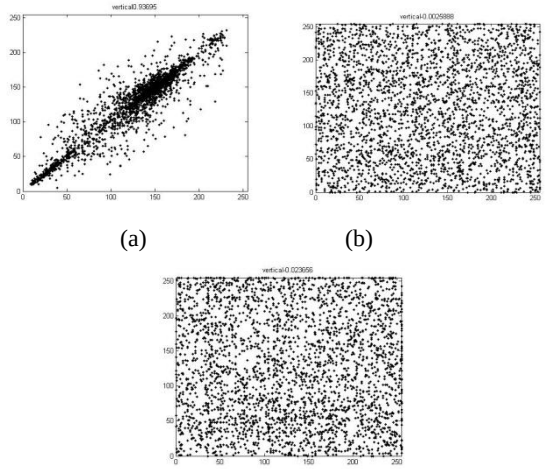
For resisting against the brute-force attack the key size should be large enough to keep the system secure. In Yoon algorithm 'seed' as the size of small matrices, number of rounds besides initial conditions of Logistic map considered a keys. With new mappings for this scheme the initial condition increased to four instead of two. x1, x2 and p1 and p2 as initial conditions of new map . PWLCM has also wider choices than Logistic map practically. Hence, the key size with new map can reach $(2^{32})^4 * 2^{24} * 2^6 = 2^{158}$ at least with 16 bit precision that makes the system secure against various attacks.



(a) (b)

(c)

Figure5: (a) Vertical Correlation Coefficients of plain Image Fishing Boat,(b) Vertical Correlation Coefficients of Cipher Image with PWLCM, (c) Vertical Correlation Coefficients of Cipher Image with Logistic map



(a) (b)

(c)

Figure 6: (a) Vertical Correlation Coefficients of Plain Image Peppers,(b) Vertical Correlation Coefficients Of Cipher Image with PWLCM, (c) Vertical Correlation Coefficients of Cipher Image with Logistic map

3.5 Entropy

Entropy is a measure of randomness in cryptography and in cryptography, a greater change in entropy is more desired as it means more complexity in encrypted message.

The ideal value of entropy is 8. The entropy *H(m)* of a message source *m* can be calculated as :

$$H(m) = \sum_{i=0}^{2^N - 1} p(m_i) \log_2 \frac{1}{p(m_i)}$$

The entropy of encrypted image for Pepper test image and with new map is 7.9666 in round 4 that is closer to 8 in comparison to cipher image in same round with Logistic map.

It means that information leakage in encrypted image is insignificant and the system is more secure against entropy attack with new map.

Table7: Entropy of Pepper Test Image

Entropy	K=2	K=4
PWLCM	7.9576	7.9666
Logistic	7.9017	7.9325

4. CONCLUSION

We proposed an image encryption algorithm based on the previously proposed method by Yoon [7] with new mappings that consists two PWLCM. PWLCM has better dynamical properties and using two as cascade method can overcome dynamical degrading of this chaos map after computerizing. Hence, better statistical properties and larger key space can be obtained to conduct the Yoon algorithm to more secure system.

There are other techniques for improving dynamical properties of chaos maps like perturbation technique that can be tested by Yoon algorithm to study how this algorithm behaves. Besides, Yoon algorithm itself can be considered as a random generator for further study

5. REFERENCES

[1] Scharinger, J. 1994. Fast encryption of image data using chaotic Kolmogorov.ows. J Electron Imaging 1998;7(2):318–25 Schuneier. Applied Cryptography. New York: John Wiley, 347~374.

[2] Fridrich, J. 1998. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurc Chaos, 8(6):1259–84.

[3] Mao, Y and Chen, G,. and Lian, S. 2004. A Novel Fast Image Encryption Scheme based on 3D Chaotic Baker maps. Int J Bifurc Chaos, 14(10):3613–24.

[4] Fu, C., Lin, B., Miao, Y., Liu, X., & Chen, J. (2011). A Novel Chaos-Based Bit-level Permutation Scheme for Digital Image Encryption. Optics Communications, 284(23), 5415–5423. doi:10.1016/j.optcom.2011.08.013

[5] Arroyo, D., Alvarez, G., Fernandez, V., & May, C. D. (n.d.). On the inadequacy of the logistic map for cryptographic applications, 1–6.

[6] Lasota, A. and Mackey, M.C. 1997. Chaos, fractals, and noise. Stochastic aspects of dynamics. Springer-Verlag, New York, 2nd Ed., 1997.

[7] Yoon, J. W., & Kim, H. 2010. An image encryption scheme with a pseudorandom permutation based on chaotic maps. Communications in Nonlinear Science and Numerical Simulation, 15(12), 3998–4006. doi:10.1016/j.cnsns.2010.01.041

[8] Zhou, H. 1996, "A Design Methodology of Chaotic Stream Ciphers and the Realization Problems in Finite Precision," phd thesis, department of electrical Engineering, Fudan university, Shanghai China, 1996.

[9] Li, S., Mou, S. , Cai ,J., Z. Ji, J. and Zhang, 2003. On the Security of a Chaotic Encryption Scheme: Problem with Computerized Chaos in chaos computerized precision . Comput. Phys. Commun. 153. 52.

[10] Huang, F, Guan, F.Z.,2005. A Modified Method of a Class of Recently Presented Cryptosystems. Chaos Solitons Fractals 23 1893.

[11] Awad, A., & Saadane, A. 2010. New Chaotic Permutation Methods for Image Encryption, (November).

[12] Socek, D., Shujun Li, Magliveras, S.S. And Furht, B. 2005. Short Paper: Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption. First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 406-407.

[13] Li, S., Chen, G., & Mou, X. 2005. on the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps. International Journal of Bifurcation and Chaos, 15(10), 3119–3151. doi:10.1142/S0218127405014052

[14] Heidari-Bateni, G. & McGillem, C. D. 1994 "A chaotic direct-sequence spread-spectrum communication system," IEEE Trans. Communications 42, 1524–1527.