Modified Algorithm of Encryption and Decryption of Images using Chaotic Mapping

A.Anto Steffi[1], Dipesh Sharma[2]

[1]Department of Computer Science & Engg.RIT Raipur, Chhattisgarh, India
aantosteffi@gmail.com

[2] Department of Computer Science & Engg.RIT Raipur, Chhattisgarh, India
download.dks@gmail.com

Abstract: In recent years, the chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques. In this paper a new approach for image encryption is based on chaotic baker map and chaotic Lorenz map in order to meet the requirements of the secure image transfer. In the proposed image encryption scheme, an external secret key of 128 bit and two chaotic maps are employed. The initial conditions for both maps are derived using the external secret key by providing different weight age to all its bits. The results of experiment show that the proposed image encryption scheme provides an efficient and secure way for real time image encryption and transmission.

Keywords: Image encryption, chaotic maps, Lorenz map, Baker map, AES**.**

1. Introduction

Security of multimedia information is used to protect the multimedia content from unauthorized access. Image information is different from the text data, it has larger amount of data, higher redundancy and stronger correlation between pixels. Traditionally developed encryption algorithm such as RSA, AES, and DES is suitable for text encryption but not suitable for image encryption directly because of two reasons. One is that the image size is larger than that of text, so the traditional cryptosystems take much time to directly encrypt the image data. The other reason is that the decrypted text must be equal to the original text. However this requirement is not necessary for image, a decrypted image containing small distortion is acceptable due to human perception [1]. Chaos signals are considered good for practical use because they have important characteristics such as they are highly sensitive to initial conditions and system parameters, they have pseudorandom property and non periodicity as the chaotic signals usually noise like etc. Consequently, the combination of chaotic theory and cryptography forms an important field of information security. The characteristics of chaotic signals make chaos system an excellent and robust cryptosystem against any statistical attacks. Lot of image encryption algorithms based on chaotic systems has been proposed. There have been many image encryption algorithms based on chaotic maps like the logistic map, the baker map, cat map etc. In order to improve the security performance of the image encryption algorithm, the concept of shuffling the positions of pixels in the plain image and then changing the gray values of the shuffled pixels is used. In this paper, two chaotic maps are used to enforce the security of the proposed encryption process.

2. Chaotic Mappings Used

- BAKER SYSTEM

Let $X = [0, 1)^2 = [0, 1) \times [0, 1)$ be the unit square. Consider the following two dimensional map $F: X \to X$

$$F(x,y) = \begin{cases} (2x, \frac{y}{2}) & \text{if } 0 \le x < \frac{1}{2}, \\ (2x-1, \frac{y+1}{2}) & \text{if } \frac{1}{2} \le x < 1. \end{cases}$$

Geometrically, F is obtained by cutting $[0, 1)^2$ into two vertical rectangles R0 = [0, 1/2) × [0, 1) and R1 = [1/2, 1)×[0, 1), stretching and compressing each to obtain an interval of horizontal width 1 and vertical height 1/2 and then putting them on top of each other. The name baker's map comes because these mimic the movement made by a baker to prepare the bread dough. Similar maps are often use in industrial processes since, as we will see formally later, they are very effective in quickly mixing.

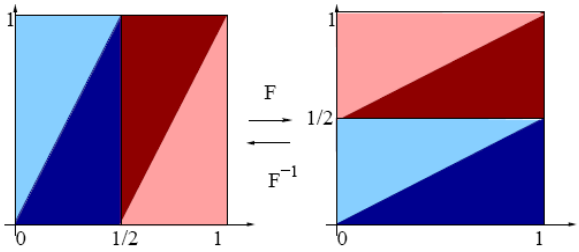

Figure 2.1: the action of baker's Map

- LORENZ SYSTEM

The equation of Lorenz chaotic system is described as following:

$$\begin{cases} dx/dt = \sigma(y-x) \\ dy/dt = rx - xz - y \\ dz/dt = xy - bz \end{cases}$$

Where, б, r and b are parameters. When б=10, r>24.74, b=8/3, the system is chaotic. The trajectory of Lorenz system can be obtained by the fourth order Runge-Kutta algorithm,

and choosing suitable step is also very vital to the pseudo-random performance of the sequence. We can get the above conclusion by a lot of tests: When step *h* is 0.1, the Lorenz sequence has better performance. Take the example of *x*, we choose the same parameters: x_0=10, y=20, z=30, б=10, r=28, b=8/3, n=6000 and different steps: 0.01 shown by Fig 2.2 and 0.1 shown by Fig 2.3

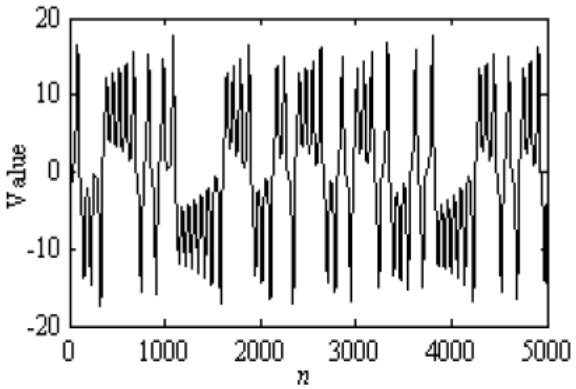

Figure 2.2: The x sequence where h is 0.01

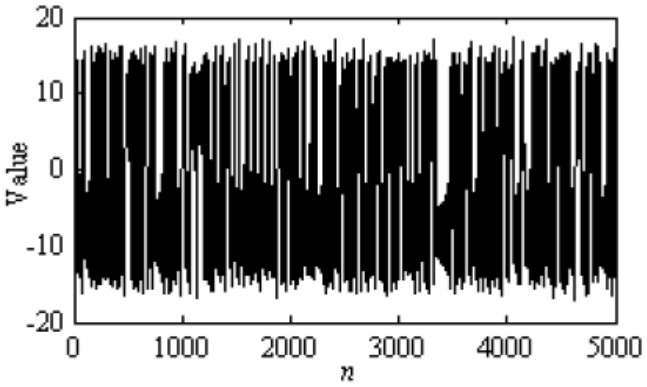

Figure 2.3: The x sequence where h is 0.1

According to Fig 2.2 and Fig 2.3 the sequence shown by Fig 2.3 has smaller blank window and better chaotic pseudorandom performance under the condition of the same iteration than the sequence shown by Fig 2.2

3. Proposed Image Encryption Algorithm

3.1 Architecture of chaos based image cryptosystem

The chaos-based image cryptosystem mainly consists of two stages. The plain image is given at its input. The typical architecture of the chaos-based image cryptosystems is depicted in Figure 3.1. There are two stages in the chaos based image cryptosystem

The confusion stage is the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels and the image becomes unrecognizable. Therefore these initial conditions and control parameters serve as the secret key. It is not very secure to have only the permutation stage since it may be broken by any attack. To improve the security, the second stage of the encryption process aims at changing the value of each pixel in the whole image. The process of diffusion is also carried out through a chaotic map which is mainly dependent on the initial conditions and control parameters. In the diffusion stage, the pixel values are modified sequentially by the sequence generated from one of the two chaotic systems selected by external key. The whole confusion-diffusion round repeats for a number of times to achieve a satisfactory level of security. The randomness property inherent in chaotic maps makes it more suitable for image encryption.

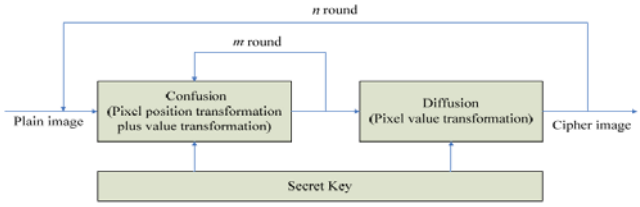

Figure 3.1: Architecture of chaos based image cryptosystem

3.2 Encryption Algorithm

The proposed scheme is shown in Figure 3.2. Different chaotic systems are employed in confusion and diffusion stages. Also complex chaotic maps are chosen rather than the simple ones to further enhance the complexity of the algorithm and thereby improving the security. The input to the cryptosystem is the plain image which is to be encrypted. The cryptosystem consists of two stages.

The first stage is the confusion stage and the second one is the diffusion stage. Among the two chaotic dynamic systems namely Lorenz and Baker one is selected by the system parameter which is obtained from the key and it is applied to the digital color image encryption because of higher secrecy of high-dimension chaotic system. The second step of the encryption process is to encrypt the shuffled image by changing its pixel values based on one of the two high-dimensional chaotic systems (Lorenz, and Baker). This is referred to as the diffusion stage. The initial conditions and the control parameters used to generate the chaos sequence in both the stages serve as the secret key in the two stages. The resulting image is the Cipher image. Separate key is used for permutation and diffusion stages of the encryption process to improve security of the algorithm.

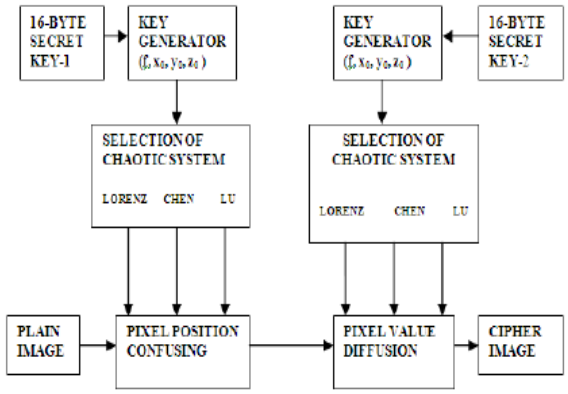

Figure 3.2: Chaos based encryption cryptosystem

3.3 Decryption Algorithm

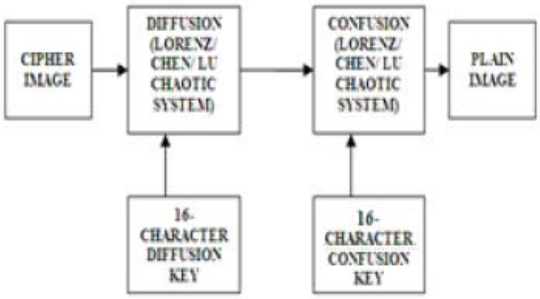

Figure 3.3: Chaos based decryption cryptosystem

The decryption system is illustrated in the Figure 3.3. The first stage in the decryption process is the diffused image decryption stage. In the encryption process, the pixel value diffusion was carried out with any one of the two chaotic systems. Therefore, in the decryption process to retrieve the original pixel values, again any one of the chaotic system (Lorenz, Baker) is employed in the first stage of decryption. The first stage of decryption process uses the three dimensional sequence generated by any one of the chaotic system .It is a kind of high-dimensional maps and complex enough.

The initial conditions that were used in the encryption process should be used here and this serves as the decryption key for the first stage. Second, in the encryption process, the pixel position permutation was carried out with any one of the chaotic system. The initial conditions and control parameters for generating the chaos-sequence were used as the confusion key. Therefore in the decryption process, the same chaotic systems with same confusion key are used to get the original position of the image. The output of the decryption system gives the original image.

4. Experimental Results

The proposed encryption algorithm is implemented in MATLAB for computer simulations. We take a grayscale "lena" image of 128x128 in size for experimental purposes.

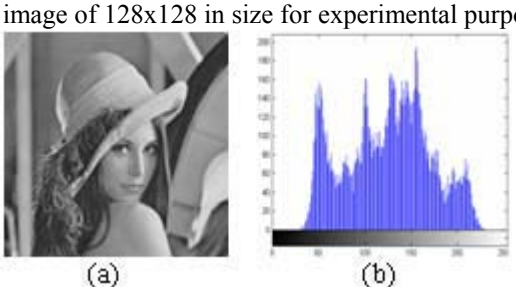

Figure 4.1: Plain-image and its histogram

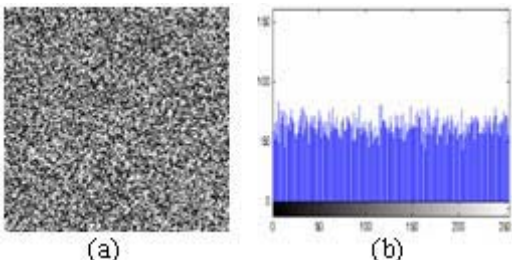

Figure 4.2: Encrypted image and histogram of encrypted image

4.1 Key Space Analysis

Key space is the total number of different keys that can be used in the cryptographic system. A cryptographic system should be sensitive to all secret keys. It require 2^k operations to succeed. Here 128 bit key is used. So 2^{128} operations, which is extensively large enough to resist the attack.

4.2 Key Sensitivity Analysis

A good cryptosystem should be sensitive to a small change in secret keys i.e. a small change in secret keys in decoding process results into a completely different decoded image.

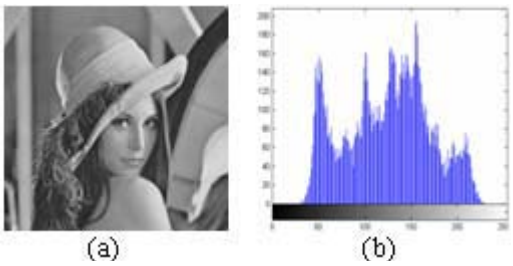

Figure 4.3: Decrypted-image and its histogram

To evaluate the key sensitivity property of the proposed cryptosystem, the same key is employed in decryption except that the value of x_0 is slightly changed to 0.30000001 and the decrypted image is shown in fig 4.4

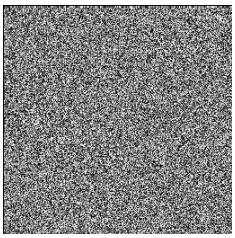

Figure 4.4: Decrypted-image with wrong key

This shows the high key sensitivity of the proposed encryption scheme. This guarantees the security of the proposed scheme against brute force attacks to some extent.

4.3 Correlation Coefficient Analysis

A useful measure to assess the encryption quality of any image cryptosystem is the correlation coefficient between pixels at the same indices in the plain and the cipher images. This metric can be calculated as follows:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

Where, x and y are the gray-scale values of two pixels at the same indices in the plain and cipher images. In numerical computations, the following discrete formulas can be used:

$$E(x) = \frac{1}{L}\sum_{l=1}^{L} x_l$$

$$D(x) = \frac{1}{L}\sum_{l=1}^{L} (x_l - E(x))^2,$$

$$\mathrm{cov}(x, y) = \frac{1}{L}\sum_{l=1}^{L} (x_l - E(x))(y_l - E(y)),$$

Where, L is the number of pixels involved in the calculations. The closer the value of *x, y r* to zero is, the better the quality of the encryption algorithm.

Table 4.1: Correlation Coefficients of two adjacent pixels in two images

		Correlation coefficients		
		Red	Green	Blue
Horizontal	Plain Image	0.9508	0.9707	0.9579
	Cipher Image	-0.005	0.0018	0.0002
vertical	Plain Image	0.9718	0.9754	0.9818
	Cipher Image	0.0032	-0.0063	0.0018

According to Table 4.1, we can remark that the correlation coefficients of the plain image are equal to 1, implying that high correlation exists among pixels, while the correlation coefficients of the cipher image are equal to 0, implying that no detectable correlation exists among pixels. Therefore the proposed algorithm can protect the cipher image from statistical attacks.

4.4 Information Entropy Analysis

Illegibility and indeterminateness are the main goals of image encryption. This indeterminateness can be reflected by one of the most commonly used theoretical measure - information entropy. Information entropy expresses the degree of uncertainties in the system and defines as follow.

$$H(m) = -\sum_{i=0}^{2^N - 1} P(m_i)\log_2[P(m_i)]$$

Where $P(m_i)$ is the emergence probability of m_i. If every symbol has an equal probability, i.e $m=\{m_0,m_1,m_2,\ldots m_2^{8}{}_{-1}\}$ and $P(m_i)=1/2^8 (i=0,1,\ldots 255)$, then the entropy is $H(m)=8$ which corresponds to an ideal case. Practically, the information entropies of encrypted images are less compared to the ideal case. To design a good image encryption scheme, the entropy of encrypted image close to the ideal case is expected.

For the three matrices R, G and B of the image, the corresponding entropies are 7.99758, 7.99708 and 7.99749 and H (m) is equal to 8, which is the ideal situation. So these results mean that the cipher images are close to random source and the proposed algorithm is secure against entropy attack.

5. Conclusions

In this paper, we presented a new algorithm of encryption and decryption of images. All the simulation and experimental analysis show that the proposed image encryption system has very large key space, high sensitivity to secret keys, has information entropy close to ideal value 8 and has low correlation coefficients close to the ideal value 0. Hence, we can say that all the analysis prove the security, effectiveness and robustness of the proposed image encryption algorithm.

References

[1] Fridrich, J., Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos, 1998, 8: 1259–1284.

[2] Zhang Han, Wang Xiu Feng, Li Zhao Hui, Liu Da Hai, Lin You Chou, "A New Image Encryption Algorithm Based on Chaos System", Proceedings of the 2003 IEEE International Conference on Robotics, Intelligent Systems and Signal Processing, Changsha, China, pp.778-782, October 2003.

[3] Chen, G. R., Mao, Y. B., Chui, C. K., A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 2004, 21: 749-761.

[4] Y.B. Mao, G. Chen, S.G. Lian, "A novel fast image Encryption scheme based on the 3D chaotic baker map", Int. J. Bifurcate Chaos, vol. 14, pp. 3613–3624, 2004.

[5] Kristina Kelber , Wolfgang Schwarz , "General Design Rules for Chaos-Based Encryption systems", Proceedings of 2005 International Symposium on Nonlinear Theory and its Applications(NOLTA2005) Bruges, Belgium, October 18-21, pp.465-468, 2005.

[6] Peng Fei, Shui-Sheng Qui, Long Min, "An Image Encryption Algorithm based on Mixed Chaotic Dynamic Systems and External Keys", Proceedings of 2005 International Conference on Communications, Circuits and Systems,,Vol. 2, pp.1139, 27-30 May 2005.

[7] Guang ZH, Huang FJ, Guan WJ, "Chaos-based Image Encryption Algorithm", Physics Letters A, Vol.346, pp.153 – 157, 2005.

[8] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," Chaos, Solutions &Fractals, vol. 29, no. 2, pp. 393–399, 2006.

[9] Alvarez, G., Li, S.: Breaking an encryption scheme based on chaotic baker map. Physics Letters A 352, 78—82(2006).

[10] Huang Yuanshi, Xu Rongcong, Lin Weiqiang, "An Algorithm for JPEG Compressing with Chaotic Encrypting", Proceedings of the International Conference on Computer Graphics, Imaging and Visualisation (CGIV'06), 2006.

[11] Chengqing Li, "On the security of a class of Image Encryption Scheme", IACR's Crytology ePrint Archive: Report 2007/339, August 2007.

[12] Wong, K. W., Kwok, B., Law, W. S., A fast image encryption scheme based on chaotic standard map, Physics Letters A , 2008, 372: 2645–2652. Wong, K. W., Kwok, B., Law, W. S., A fast image encryption scheme based on chaotic standard map, Physics Letters A , 2008, 372: 2645–2652.

[13] Su Su Maung, and Myitnt Myint Sein, "A Fast Encryption Scheme Based on Chaotic Maps", GMSARN International Conference on Sustainable Development: Issues and Prospects for the GMS, 2008.
[14] Musheer Ahmad and M. Shamsher Alam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", Musheer Ahmad et al /International Journal on Computer Science and Engineering, Vol.2(1), 2009, 46-50.
[15] Patidar, V., Pareek, N. K., Sud, K. K., A new substitution–diffusion based image cipher using chaotic standard and logistic maps, Commun. Nonlinear Sci. Numer. Simulat., 2009, 14: 3056-3075.
[16] Fengjian Wang, Yongping Zhang and Tianjie Cao "Research of chaotic block cipher algorithm based on Logistic map", 2009 Second International Conference on Intelligent Computation Technology and Automation, 2009**:** 678 – 681.
[17] Wang Y, Wong KW, Liao XF, et al, "A Chaos-based Image Encryption Algorithm with Variable Control Parameters", Chaos Solitons & Fractals, vol. 41, no. 4, pp.1773-1783, 2009.
[18] Wong KW, Kwok BSH, Yuen CH, "An Efficient Diffusion Approach for Chaos-based Image
Encryption" Chaos Solitons & Fractals, vol. 41, no. 5, pp.2652-2663, 2009.
[19] Borujeni SE, Eshghi M, "Chaotic Image Encryption Design Using Tompkins-Paige Algorithm", Mathematical Problems in Engineering, 762652, 2009.
[20] Ye, R., A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Opt. Commun. 2011, 284: 5290-5298.

Author Profile

Dipesh Sharma Currently, he is faculty in the Department of Computer Science Engineering, RIT, Raipur, Chhattisgarh, India. His area of interest includes Cryptography, encryption techniques, ad-hoc networks.

A. Anto Steffi Currently, she is pursuing Master of Technology in the Department of Computer Science Engineering, RIT, Raipur, Chhattisgarh, India. Her area of interest includes Cryptography, image encryption techniques.