AN ENHANCED CHAOTIC IMAGE ENCRYPTION

Mintu Philip

Department of Computer Engineering, Rajagiri School of Engineering and Technology
mintu.philip@gmail.com

ABSTRACT

The paper proposes a new image encryption scheme based on chaotic encryption. It provides a fast encryption algorithm based on coupled chaotic map. The image is encrypted using a pseudorandom key stream generator. The image is partially encrypted by selecting most important components of image. To obtain most important components of an image, discrete wavelet transform is applied.

KEYWORDS

Chaos Theory, wavelet, logistic map,, image encryption.

1. INTRODUCTION

Chaos theory has been established since 1970s. The distinct properties of chaos, such as ergodicity, quasi-randomness, sensitivity dependence on initial conditions and system parameters, have granted chaotic dynamics as a promising alternative for the conventional cryptographic algorithms.

A new way of image encryption scheme has been proposed which utilizes a chaos-based cryptographic scheme using the logistic map. A combined image compression and encryption scheme is proposed. The model is achieved by using discrete wavelet transform and RLE for compression. Chaos based system is used for encryption. This algorithm encrypts image pixel by pixel taking consideration the values of previously encrypted pixels. This system is robust against cryptanalytic attacks. Also a simple implementation of image encryption achieves high encryption rate on general purpose computer. In mobile bandwidth constraints and power saving are needed for which the proposed algorithm is suitable.

2. PROPOSED IMAGE ENCRYPTION ALGORITHM

The image is encrypted pixel by pixel using logistic maps. The advantage of logistic map is that it has a very complex dynamics. Use of two logistic map increases the complexity of algorithm. Only the first few coefficients are encrypted since energy is concentrated in these values. This will save the execution time. The algorithm uses a coupled logistic map. It has a pseudorandom key stream generator that generates a binary stream which used in chaotic encryption. The first logistic map whose initial parameters are taken from the KEY generated during user authentication process provides the initial parameters for second logistic map.

Following are the logistic maps:

DOI : 10.5121/ijcseit.2011.1507

$$x_{n+1} = \mu x_n(1 - x_n) \quad (3)$$

$$y_{n+1} = \mu y_n(1 - y_n) \quad (4)$$

The steps involved in pseudorandom key stream generator are:

1. $x_{i+1} = \mu 1 x_i(1 - x_i)$ (5)
   $y_{i+1} = \mu 2 y_i(1 - y_i)$ (6)
2. Convert real number x_i to binary equivalent X_i.
3. Divide X_i into three parts and XOR the three parts to obtain X_i'.
4. Perform above steps for value of 'i' starting from 1 to n.
5. Convert X_n to real value x_n.
6. The value x_n is given as initial value μ2 to second logistic map.
7. Above steps are repeated for second logistic map.
8. The final value y_n is multiplied by 10^{18} and is converted to binary, stored in s1.
9. Multiply the value of μ2 by 10^5 and convert to binary and store in s2.
10. Take first 56 bits of s1 and 5th to 15th bits of s2 and combine it to form the key to encrypt.
11. Perform XOR operation of pixels with the key to obtain the cipher.
12. At receiver side perform XOR of cipher with the key to decrypt data.
13. Decompress the data using inverse DWT to obtain the pixels of the image.
14. Write the pixels to a new image file.

The binary sequence generated by pseudorandom key stream generator is XORed with the pixel values of the image to obtain the cipher image.

3. STATISTICAL ANALYSIS

The encrypted images should possess certain random properties in order to resist the statistical attack. Statistical analysis is done by calculating the histograms, the correlations of two adjacent pixels in the encrypted images and the correlation coefficient for several images and its corresponding encrypted images of an image database. A detail study has been undergone and the results are summarized as followings. Different images have been tested, and similar results are obtained. However, due to the page limit, only the results for the Lena. The advantage of partial encryption is that only very few coefficients are encrypted so that encryption time is reduced. This is helpful in mobile application where bandwidth and power is constrained. It also helps to increase the security of image since the intruder does not know which all coefficients are encrypted.

3.1. Difference between the original and the permuted images

NPCR (Number of Pixels Change Rate) is used to test the difference between the original image *P1* and the permuted one *C1*. *NPCR* stands for the number of pixel change rate. Then, if *D* is a matrix with the same size as images *P1* and *C1*, *D (i,j)*is determined as follows:

$$D(i,j) = \begin{cases} 1 & if\ P1 \neq c1(i,j) \\ 0 & else \end{cases} \quad (7)$$

NPCR is defined by the following formula:

$$NPCR = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{D(i,j)}{M \times N} \times 100 \quad (8)$$

The NPCR of the new system is found to be 99.42.

3.2. Correlation coefficients of intra and inter - color –components

To quantify the dependence between two images, Pearson's correlation coefficient is commonly used. Given by equation, this coefficient is obtained by dividing the covariance between the two images (eq. 13) by the product of their standard deviations (eq. 12 and eq. 11). E in eq.11 is the expected value operator. P1 (i, j) and C1 (i, j) are respectively the pixels gray values of the first and the second images.

$$E(x) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} P1(i,j) \quad (9)$$

$$D(P1) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[P1(i,j) - E(P1(i,j))]^2 \quad (10)$$

$$Cov(P1,C1) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[P1(i,j) - E(P1(i,j))] \times [C1(i,j) - E(C1(i,j))]$$

$$r_{P1C1} = \frac{Cov(P1,C1)}{\sqrt{D(P1)}\sqrt{D(C1)}} \quad (11)$$

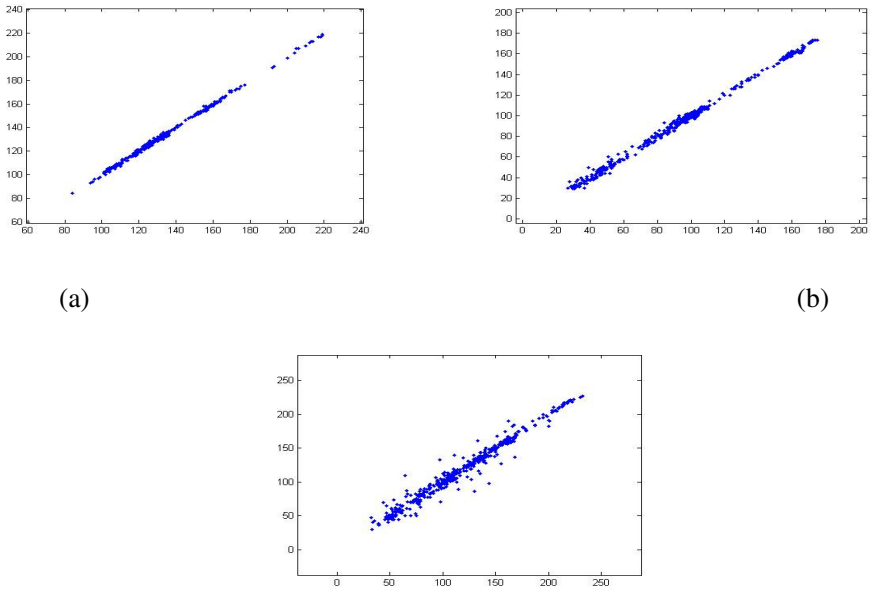
Following results for found for various standard images:

Image	Correlation coefficient
Lena	0.00099
Pepper	0.002
Cameraman	0.0017

Table 1: correlation coefficient of encrypted image.

3.3. Distribution of two adjacent pixels

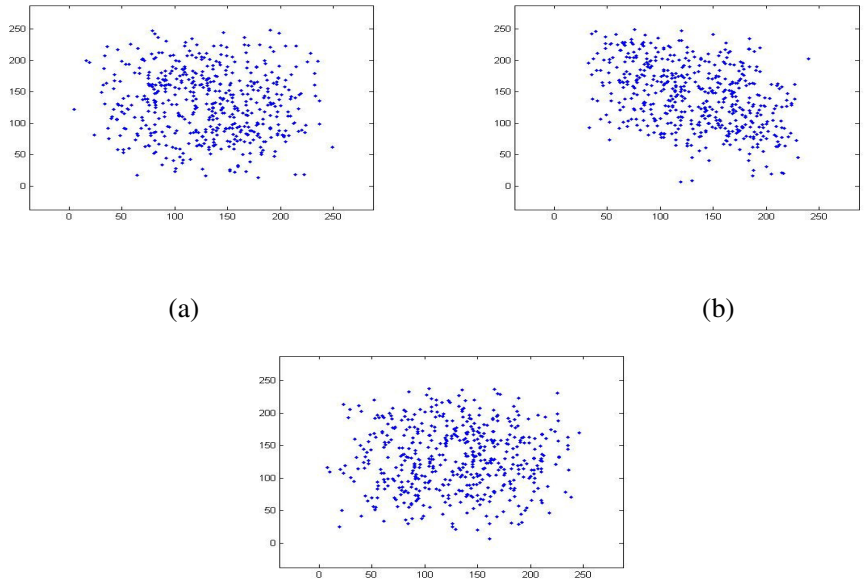
Statistical analysis on large amounts of images shows that on average, 8 to 16 adjacent pixels are correlated.In this section, some simulations are carried out to test the correlation distribution between two horizontally, vertically and diagonally adjacent pixels, in the original and permuted images. Fig. 5 shows the correlation distribution of two horizontally, vertically and diagonally adjacent pixels in the first component of the original image and the encrypted images. Then, we plot the pixel value on location (x,y+1) over the pixel value on location (x, y), location (x+1,y) over the pixel value on location (x, y) and location (x+1,y+1) over the pixel value on location (x, y).



(a) (b)

(c)

Fig 1: (a) horizontal, (b) vertical and (c) diagonal correlation matrix of original image



(a) (b)

(c)

Fig 2: (a) horizontal, (b) vertical and (c) diagonal correlation matrix of encrypted image

It is clear from Fig 2 that there is negligible correlation between the two adjacent pixels in the encrypted image.

3.4. Histogram analysis

An image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. We have calculated and analyzed the histograms of the encrypted image as well as the original colored image.

As we can see, the histogram of the encrypted image is significantly different from that of the original image. Also the histogram of complete and partially encrypted image are same. Moreover, one can observe that the coupled map improves the uniformity of the histogram for encryption method.

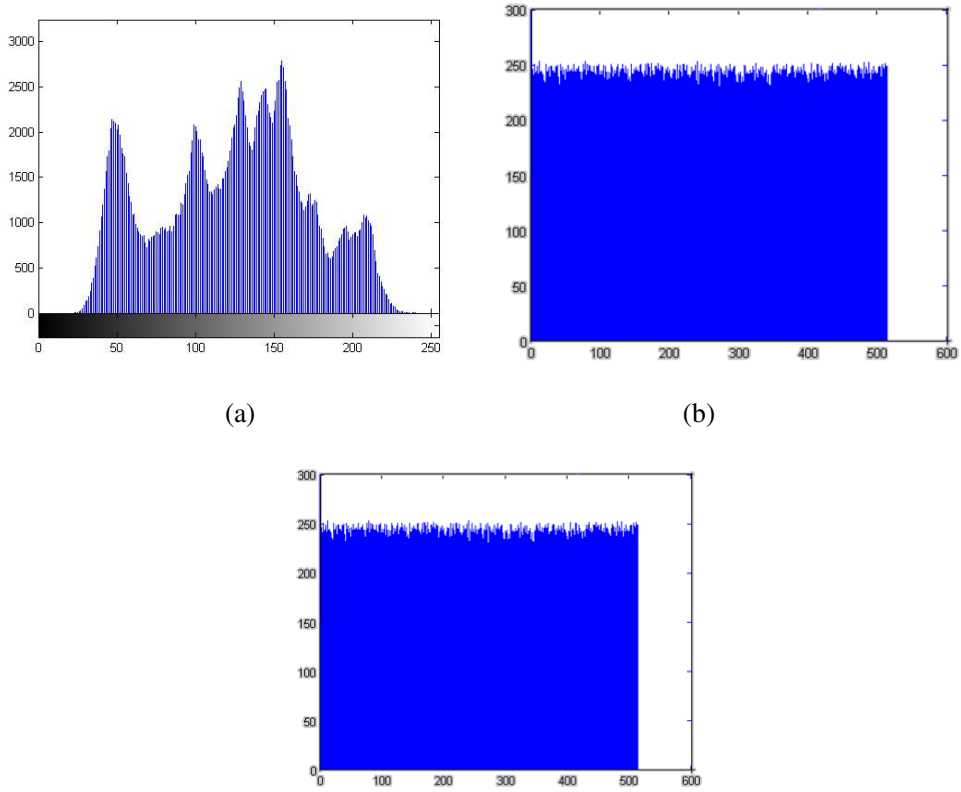


Fig3: Histogram of (a) original image and (b) encrypted image and (c) partially encrypted image

3.5. Information Entropy analysis

Entropy is a statistical measure of randomness that can be used to characterize the texture of an image. It is well known that the entropy *H(m)* of a message source *m* can be calculated as :

$$H(m) = \sum_{i=0}^{2^N-1} p(mi)\ \log_2 \frac{1}{p(mi)} \qquad (12)$$

Where *p(mi)* represents the probability of message *mi*.

When an image is encrypted, its entropy should ideally be 8. If it is less than this value, there exists a certain degree of predictability which threatens its security. The entropy of partially and complete encrypted images are found to be different by 0.2%.

Image	Entropy(original)	Entropy(Encrypted)
Lena	6.95	7.7719
Pepper	6.775	7.7
Cameraman	6.775	7.762

Table 2: Information Entropy

The obtained results are very close to the theoretical value. This means that information leakage in the encryption process is negligible.

3. CONCLUSIONS

The proposed algorithm was found to be very fast and secured which can be applied for real time applications which have bandwidth and power constraints. This is because it requires less time to encrypt and decrypt image since they are partially encrypted. This will also help to improve security since the intruder does not know which all coefficients are partially encrypted. Application of chaos theory helps to achieve complex dynamics. The encryption scheme can be extended to videos.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] Jui-Cheng Yen, and Jiun-In Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption", IEEE International Symposium on ISCAS 2000, Geneva, pp. IV-49-IV-52, May. 2000.

[7] Po-Han Lee,Soo-Chang Pei and Yih-Yuh Chen, "Generating Chaotic Stream Ciphers Using Chaotic Systems", Chinese Journal Of Physics Vol. 41 , No. 6, 2003.

[8] Socek, D., Shujun Li, Magliveras, S.S. and Furht, B, "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, 2005:406-407.

[9] Deergha Rao and K. Gangadhar, "Modified Chaotic Key-Based Algorithm for Image Encryption and Its VLSI Realization", International Conference on Digital Signal Processing, 2007.

[10] H.E.H. Ahmed, H.M. Kalash, and O.S.F. Allah, "An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption", presented at Informatica (Slovenia), 2007, pp.121-129.

[11] Shubo Liu, Jing Sun, Zhengquan Xu "An Improved Image Encryption Algorithm based on Chaotic System", journal of computers, vol. 4, no. 11, 2009, pp.1091-1100.

[12] Abir Awad, Abdelhakim Saadane, "Efficient Chaotic Permutations for Image Encryption Algorithms", Proceedings of the World Congress on Engineering Vol I, 2010.

[13] Ai-hongZhu, Lia Li, "Improving for Chaotic Image Encryption Algorithm Based on Logistic Map", 2nd Conference on Environmental Science and Information Application Technology, 2010.

[14] G. Chen, Y. Mao, C.K. Chui, "A symmetric image encryption based on 3D chaotic maps", Chaos Solutions Fractals, vol. 21, pp. 749–761, 2004.

[15] S. E. Borujeni, M. Eshghi1, "Chaotic Image Encryption Design Using Tompkins-Paige Algorithm", Hindawi Publishing Corporation, Mathematical Problems in Engineering, Article ID 762652, 22 pages, 2009.

[16] Mazleena Salleh, Subariah Ibrahim, Ismail Fauzi Isnin, "Image encryption algorithm based on chaotic mapping", Journal Teknologi, 2003, pp: 1–12.

[17] Shubo Liu, Jing Sun, Zhengquan Xu, "An Improved Image Encryption Algorithm based on chaotic system", Journal of Computers, vol. 4, no. 11, November 2009, pp: 1091-1100.

[18] Noura, H. El Assad, S. Vladeanu, C, "Design of a fast and robust chaos-based crypto-system for image encryption", 8th International Conference on Communications (COMM), 2010, pp: 423 – 426.

Author

Mintu Philip is currently working as a faculty in Department of Computer Science at Rajagiri School of Engineering and Technology. She received B.Tech degree in Computer Science from Rajagiri School of Engineering and Technology, Kerala on April 2008. She completed M.tech in Computer Science with Specialization in Data Security under CUSAT, Kerala on 2011.