BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **13**, No 2

Sofia • 2013

Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2013-0016

A Combined Encryption Compression Scheme Using Chaotic Maps

Bhagwati Prasad, Kunti Mishra

Department of Mathematics, Jaypee Institute of Information Technology, A-10, Sector-62, Noida, UP-201307 INDIA
Emails: b_prasad10@yahoo.com kuntimishra@gmail.com

Abstract: *The intent of this paper is to propose an encryption compression scheme using multiple chaotic maps along with the concept of Galois field. This method improves the security of the encrypted data and a significant compression is also achieved. The obtained high security architectures are ideal for many real life applications such as medical images, legal documents and military and other operation.*

Keywords: *Encryption scheme, data compression, security architectures.*

2010 Mathematics Subject Classification: 68P25, 68Q30, 94A60.

1. Introduction

In the era of information revolution digital communication has become one of the most important parts of our daily life. The information and communication technology is at the backbone of all kinds of developments of human activity. A fast and secure transmission of the data from the transmitter to the receiver is required for an efficient communication system, which can be achieved using an efficient compression and encryption algorithm. A number of compression and encryption methods are proposed in literature see, for example [1-2, 4-5, 7, 9-11, 17-23] and several references thereof. In general, there are two research directions in this area. One embeds the key-controlled confusion and diffusion in source-coding while in the other compression is included in the cryptographic algorithms. It is well known that images are different from texts in many aspects, such as high redundancy and correlation.

The main obstacle in designing efficient image compression algorithms is the difficulty of shuffling and diffusing such image data by traditional cryptographic

tools (see [16, 19]). In most of the natural images, the value of any given pixel can be reasonably predicted from the values of its neighbours. The operation of encryption and compression consists of two parts, namely, encoding and decoding. Encoding is a process in which the original image is represented in a different form, so that it becomes secure and requires less storage than the original image, while decoding recovers the original image from the encoded information. In many real life applications we need to recover the original image exactly, for which lossless decoding is required. The lossless decoding is of particular importance in case of medical images, military and legal documents. In this paper we propose a method to be used in conjunction with multiple chaotic maps which performs encryption and compression together.

2. Preliminaries

M a y [12-13], in 1976, recognized the importance of the logistic model introduced by Verhulst (see [14]) and observed that the continuous time model may not be suitable to reflect the realities in most of the cases and constructed a discrete version of this model. It is represented by the following equation:

$$x_{n+1} = a\, x_n(1-x_n),\ a \in (0, 4),\ x_n \in (0, 1),\ n = 0, 1, 2, \ldots \tag{1}$$

When the value of parameter a is within a certain range, an arbitrary initial value, $x_0 \in (0, 1)$ can generate a chaotic sequence $\{x_1, x_2, \ldots, x_n\}$. For different values of parameter a, the logistic sequence shows different characteristics. The importance of this model lies in the fact that a minute change in the initial condition may cause a drastic change in the behavior of the function. This extreme sensitivity to the initial condition is the most fascinating aspect of chaotic maps which makes chaotic systems ideal for various applications. For details regarding these maps, one can refer to D e v a n e y [6], P r a s a d and K a t i y a r [15, 16] and several references thereof. It is to be noticed that the sequence $\{x_n\}$ generated by (1) appears to have typical chaotic characteristics when a has a value greater than or equal to 3.5699456.

The chaotic sequences generated by a continuous chaotic system are not safe enough, because the chaotic equation can be reconstructed by getting a short burst continuous set of the sequences, if it is in the form of a finite polynomial (see [3]). In order to guarantee the security of the algorithm we consider two logistic chaotic maps with different parameters in the cryptosystem. The chaotic system $\boldsymbol{x} = \{x_1, x_2, \ldots, x_n\}$ is engaged to generate the confusion matrix, while the chaotic system $\boldsymbol{y} = \{y_1, y_2, ..., y_n\}$ is used to keep the property of the chaotic sequence.

3. Algorithm

We use the following proposition of G i l b e r t [8].

Proposition 3.1. Let Z_x be the set of all non-negative integers less than x, this set along with two operations of addition modulo x and multiplication modulo x is a Galois field if and only if x is prime.

The following theorem is of prime importance for our algorithm.

Theorem 3.2. Let $P(x)$ be a polynomial of degree m (a natural number) in variable x with coefficients from Z_x, where x is a prime number, i.e.,

$$a_0 x^m + a_1 x^{m-1} + \ldots + a_m x^0 = P(x). \tag{2}$$

Then the coefficients a_i, $i = 1, \ldots, m$, can be uniquely determined as follows:

$$\begin{aligned} a_0 &= \text{int}\,(p(x)/x^m) \\ R_1 &= p(x) \bmod (x^m) \\ a_1 &= \text{int}\,(R_1/x^{m-1}) \\ R_2 &= R_1 \bmod (x^{m-1}) \\ &\vdots \\ a_{m-1} &= \text{int}\,(R_{m-1}/x) \\ a_m &= R_{m-1} \bmod (x) \end{aligned} \tag{3}$$

P r o o f. It follows easily using the principle of mathematical induction.

First the following two matrices are created as given:

(a) Confusion Image Matrix: A chaotic sequence is used to construct an $n \times 1$ matrix M, where the sequence $\{x_n\}$ is constructed using equation (1). The position matrix P is created from M by sorting it in ascending order, all the values of P denote the index values of the original matrix, which are not being sorted. At last, the image matrix E is turned into a confusion image matrix I according to the position matrix P.

(b) Matrix with Chaotic Properties: In order to keep the property of chaotic sequences, we operate XOR between the confusing image matrix I and the chaotic matrix C to obtain the matrix N, i.e., $N = I \oplus C$, where the chaotic matrix C can be obtained as

$$C = \text{int}(y.10^{15}) \bmod 256, \tag{4}$$

and the sequence $y = \{y_1, y_2, \ldots, y_n\}$ is formed using the chaotic map $y_{n+1} = by_n(1-y_n)$, $b \in [3.5699456, 4)$, $y_n \in (0, 1)$, $n = 1, 2, \ldots$

Now we describe the main part of the algorithm in seven steps as given.

Step 1. Choose the initial value and the system parameter for creating the chaotic sequences x and y.

Step 2. Create a position matrix P by sorting the chaotic sequence x in ascending order. All the values of P denote the index values of the original matrix, which are not being sorted.

Step 3. Turn the original image matrix E into a scrambling image matrix I according to the position matrix P.

Step 4. Turn the chaotic sequence y into a chaotic matrix C according to equation (4).

Step 5. Obtain a ciphered image N by using XOR operation between the image matrix I and the chaotic matrix C, i.e., $N = I \oplus C$.

Step 6. Choose an appropriate m and a prime number x. Divide the ciphered image N obtained in the last step into units of length m and turn each unit into a single value using (2).

Step 7. Combine all single values obtained in Step 6, in this way we get a ciphered image M of length x/m.

The decryption process is the inverse process of encryption. The original image can be obtained with correct key combinations and using (3).

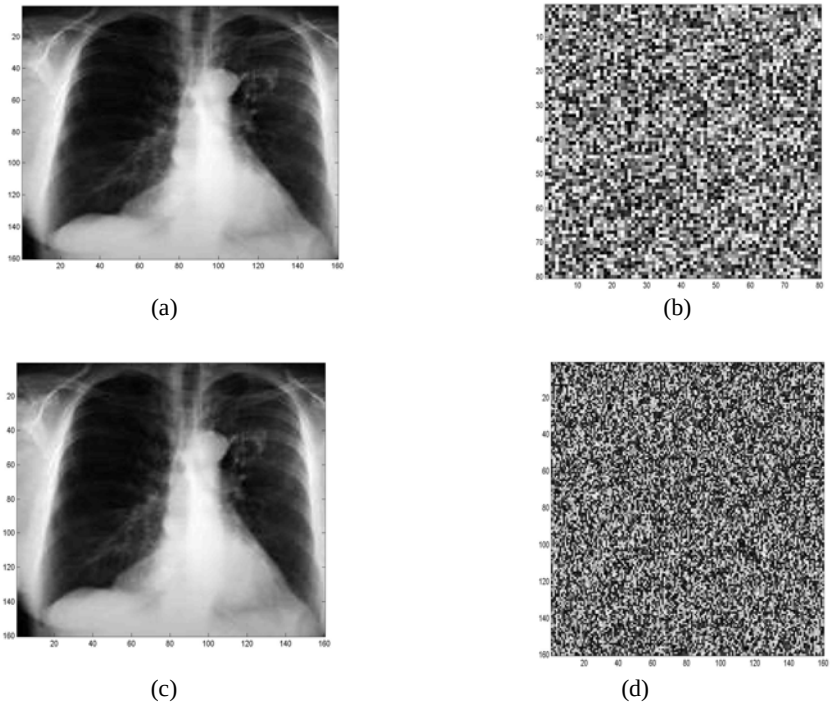
4. Simulation and analysis

A good cryptosystem must have several features, such as high sensitivity to keys and plaintext, that is that any minimal change of a key or plaintext will cause quite different ciphertext (see [17]). The map from the plain text to ciphertext is random, that is the ciphertext does not have any fixed pattern and therefore the adjacent ciphertexts are not correlated. Thus there exists a large key space with sufficient resistance towards brute force search.

4.1. Key sensitivity analysis

We take an original X-ray image of pixel size 170×166 for the study of the sensitivity of our algorithm. The chaotic sequences are generated by taking $x_0 = 0.0978888878777567$, $a = 3.678988867777798$, $y_0 = 0.0987878777788898$, $b = 3.8567877776666777$, $x = 619$, $m = 4$ for encryption purpose.

Now, if we decrypt it using $x_0 = 0.0978888878777568$ instead of 0.0978888878777567, we get Fig. 1(d). It is also noticed that the same sensitivity is achieved for other parameters of the chaotic systems.



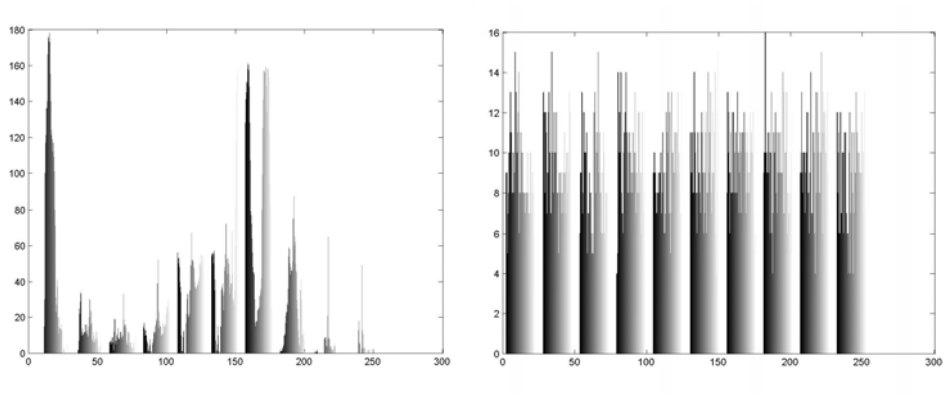
(a) (b)

(c) (d)

Fig. 1. Original image (a); encrypted image (b); correct decrypted image (c); error decrypted image (d)

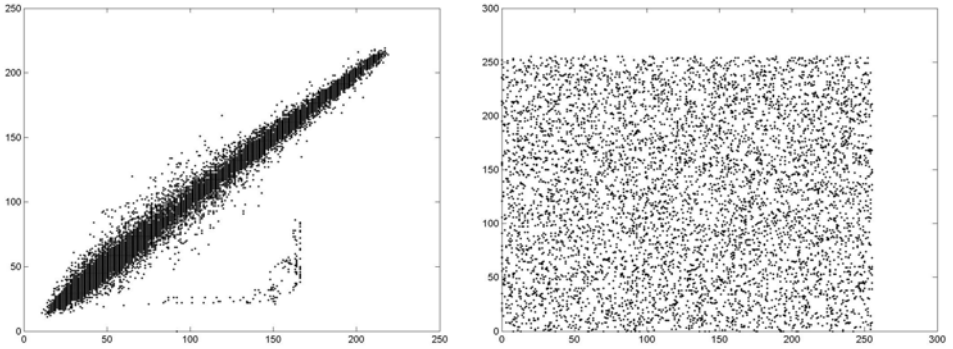
4.2. Statistical analysis

a. Statistical histogram: The original image and its histogram are shown in the figure. It is clear that after encoding the image, using the proposed algorithm, the histogram of the ciphered image is uniformly distributed (see Fig. 2 (a) and (b)). The statistical correlation between the plain text and cipher text is very small, which shows that the cipher text has good confusion performance and it can efficiently resist a statistical attack.



(a) (b)

Fig. 2. Histograms of images: Plain image (a); Ciphered image (b)



(a) (b).

Fig. 3. The correlation distribution of two horizontally adjacent pixels in images: original image (a); ciphered image (b)

b. Correlation of adjacent pixels: The correlation coefficient between the adjacent pixels is obtained by the following formula:

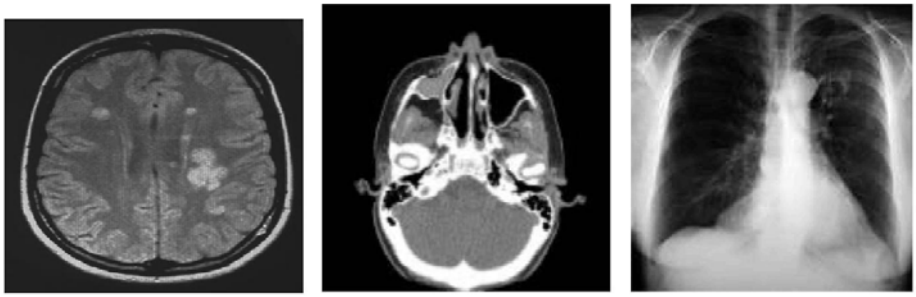
$$\text{The coefficient of correlation } r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{\operatorname{var}(x)}\sqrt{\operatorname{var}(y)}} \ .$$

Table 1. Correlation coefficients of two adjacent pixels

Position of pixels	Plain image	ciphered image
Vertical	0.9954	–0.04787225
Horizontal	0.9651	0.00330860
Diagonal	0.9870	–0.00926613

4.3. Compression analysis

We study the compression analysis of three images, i.e., MRI scan image, CT scan image and X-ray image (see Fig. 4) using the proposed algorithm and found an appreciable compression ratio (see Table 2).



(a) (b) (c)

Fig. 4. Original images: MRI scan image (a); CT scan image (b); X-Ray Image (c)

Table 2. Ratio of original gray scale medical images to the ciphered image

Medical image	Size of a plain image (bits)	Size of a ciphered image (bits)	Ratio achieved
CT	491520	261120	1.8824
MRI	1180032	626892	1.8824
X-Ray	225760	112880	2

5. Conclusion

In the proposed method the concept of Galois field is used along with the multiple chaotic maps to achieve high security along with compression. We have implemented our method on gray scale medical images. The distinct advantage of lossless compression and encryption makes the methodology very useful in some applications, such as medical imaging, multimedia applications and military applications.

References

1. Al-Saidi, N., G. Rushdan, M. Sd. Using IFS as an Encryption Method. – In: ICET'2009, 275-278.
2. Behnia, S., A. Akshani, H. Mahmodi, A. Akhavan. A Novel Algorithm for Image Encryption Based on Mixture of Chaotic Maps. – Chaos Solitons and Fractals, Vol. **35**, 2008, No 2, 408-419.
3. Celika, M. U., G. Sharma, A. M. Tekalp. Gray-Level-Embedded Lossless Image Compression. – Signal Processing: Image Communication, Vol. **18**, 2003, No 6, 443-454.
4. Chen, G., Y. Mao, C. K. Chui. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps. Chaos, Solitons and Fractals, Vol. **21**, 2004, No 3, 749-761.
5. Chen, Y., L. Zhang, Y. Wang. A Data Encryption Algorithm Based on Dual Chaotic System. – In: International Conference on Computer Application and System Modeling, IEEE, 2010, 431-435.

6. D e v a n e y, R. L. A First Course in Chaotic Dynamical Systems: Theory And Experiment. Addison-Wesley, 1992.
7. D i k b a s, S., F. Z h a i. Lossless Image Compression using Adjustable Fractional Line-Buffer. – Signal Processing, Image Communication, Vol. **25**, 2010, No 5, 345-351.
8. G i l b e r t, J. W. Modern Algebra with Applications. John Wiley and Sons, 1976.
9. G r a n g e t t o, M., E. M a g l i, G. O l m o. Multimedia Selective Encryption by Means of Randomized Arithmetic Coding. – IEEE Trans. Multimedia, Vol. **8**, 2006, No 5, 905-917.
10. H u a n g, J., M. L o n g. A Novel Image Cryptosystem with Multiple Chaotic Maps. – In: Proc. of 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009, 4573-4576.
11. K i m, H., J. W e n, J. V i l l a s e n o r. Secure Arithmetic Coding. – IEEE Trans. Signal Process., Vol. **55**, 2007, No 5, 2263-2272.
12. M a y, R. M. Simple Mathematical Models with Very Complicated Dynamics. – Nature, Vol. **261**, 1976, No 459, 459-475.
13. M a y, R. M., G. F. O s t e r. Bifurcations and Dynamic Complexity in Simple Biological Models. – The American Naturalist, Vol. **110**, 1976, 573-599.
14. P a s t i j n, H. Chaotic Growth with the Logistic Model of P.-F. Verhulst. – In: The Logistic Map and the Route to Chaos: From the Beginnings to Modern Applications. M. Ausloos, M. Dirickx, Eds. Springer-Verlag, 2006.
15. P r a s a d, B., K. K a t i y a r. A Comparative Study of Logistic Map through Function Iteration. – In: Proc. Of the Int. Con. Emerging Trends in Engineering and Technology, Kurukshetra, India, 2010, 357-359.
16. P r a s a d, B., K. K a t i y a r. Fractals via Ishikawa Iteration. – In: ICLICC2011, P. Balasubramaniam, Ed. Vol. **140**. CCIS. Heidelberg, Springer, 2011, 197-203.
17. W a n g, Y., K. W. W o n g, X. L i a o, T. X i a n g, G. C h e n. A Chaos Based Image Encryption Algorithm with Variable Control Parameters Chaos. Chaos Solitons and Fractals, Vol. **41**, 2009, No 4, Elsevier, 1773-1783.
18. W o n g, K. W., C. H. Y u e n. Embedding Compression in Chaos-Based Cryptography. – IEEE Trans. Circuits Syst. II, Exp. Briefs, Vol. **55**, 2008, No 11, 1193-1197.
19. W u, C. P., C. C. J. K u o. Design of Integrated Multimedia Compression and Encryption Systems. – IEEE Trans. Multimedia, Vol. **7**, 2005, No 5, 828-839.
20. X i a o, H., S. Q i u, C. D e n g. A Composite Image Encryption Scheme Using AES and Chaotic Series. – In: First International Symposium on Data, Privacy and e-Commerce, 2007, 277-279.
21. Y o o n, J. W., H. K i m. An Image Encryption Scheme with a Pseudorandom Permutation Based on Chaotic Maps. – Common Nonlinear Sci Numer Simulate, 2010, 3998-4006.
22. Y o o n, J. W., H. K i m, J. V i l l a s e n o r. Binary Arithmetic Coding with Keybased Interval Splitting. – IEEE Signal Process. Lett., Vol. **13**, 2006, No 2, 69-72.
23. Z h a n g, L., X. L i a o, X. W a n g. An Image Encryption Approach Based on Chaotic Maps. – Chaos, Solitons and Fractals, Vol. **24**, 2005, No 3, 759-765.