Research Journal of Applied Sciences, Engineering and Technology 5(22): 5308-5313, 2013
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: November 08, 2012 Accepted: December 28, 2012 Published: May 25, 2013

Image Encryption Algorithm based on Chaos Mapping and the Sequence Transformation

Honge Ren, Linlin Dai and Jian Zhang
Institute of Information and Computer Engineering, Northeast Forestry University, Harbin 150040, China

Abstract: According to the existing problems like that the algorithm is very complex, the quantity of operation is large and safety is not advanced in the present digital image encryption, this study has put forward a new chaotic system based on Logistic generation and transformation to realize the sequence image encryption, the algorithm gave the traditional chaotic series a new purpose. It used two kinds of ways on the comprehensive encryption for the same image that is respectively from the alternative operating on image pixel grayscale value and the confusion of the pixel position in the specific operation method. The experiment results show that the algorithm has good encryption effect and can withstand statistical analysis and attack operation, the amount of the key is large with high safety, in line with the requirements of modern technology to image encryption.

Keywords: Chaotic system, logistic, image encryption, series transformation

INTRODUCTION

With the rapid development of science and technology, information technology has been used widely in people's daily life (Nur *et al*., 2011; Cai-Hua *et al*., 2011). Therefore, today the network information exchange is particularly important, in the meantime, the perfect combination of network technology and multimedia technology makes network application has been further widened scope, a large number of multimedia information is used to exchange through the internet. Consequently, information safety has been vividly portrayed (Rengarajan *et al*., 2012; Mei-Lei and Zhe-Ming, 2011). Digital image is as an important carrier of the multimedia information and for the safety of image information transmission security problems are as the one of the important direction. In recent years, experts and scholars in this field have also concluded many research results; to improve color image encryption and decoded quality of the images the scholars preceded the more extensive studies (Banerjee, 2012; John, 2012). It is thus clear that based on all kinds of visible field, a variety of methods has been put forward. According to the characteristics of digital image information people has put forward a lot of digital image encryption algorithm based on chaotic system encryption technology since it has good effect and speed of encryption got an extensive use of research (Ercan, 2009; Narendra, 2009). David (2010) has used the characters of chaotic system to comment on image encryption with chaotically coupled chaotic maps. The watermarking has also used the information hiding technology (Minghui *et al*., 2012; Cai-Hua *et al*., 2011; Akram *et al*., 2011). Omid and Subariah (2011) have put the information security technology upon the adaptive image. Even though the results of these studies achieved for image encryption algorithm, but there are still some disadvantages that algorithm thought is complex or the operation time is long and so on. This study proposed a new algorithm aimed at the existing problems, because of the advantages that Logistic mapping has strong randomness and good balance, it realized the image encryption based on the mapping to constitute the sequence and give the new transformation.

ALGORITHM THEORY

Chaotic sequence: The characteristics of the chaotic motion that neither has periodicity nor convergence, the dots on the motion locus cover the whole area, the motion locus continue flex and fold that makes the system export to be similar to random noise, the system motion is extremely sensitive. Any long-term motion approaching two dots can not be forecasted and make chaotic sequence to be fit for the digital information encryption. So we can use the chaotic system to produce chaotic sequence what is large, unrelated and random and confirmed to regeneration for chaotic encryption through digital image.

Logistic mapping is used widely, so we can define the model as the Eq. (1):

$$x_{n+1} = \mu_0 * x_n * (1 - x_n) \quad (1)$$

where, $0 < \mu_0 \leq 4$, $0 < x_n < 1$, $n \in N$, μ_0 is called bifurcation parameter, x_n is ergodic on the region [0, 1].

Corresponding Author: Honge Ren, Northeast Forestry University, Institute of Information and Computer Engineering, Harbin 150040, China

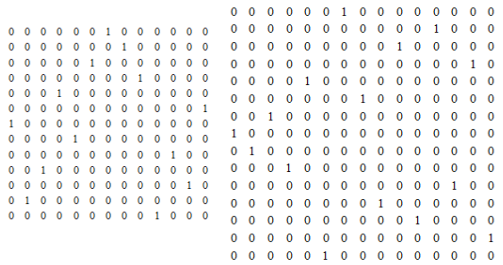
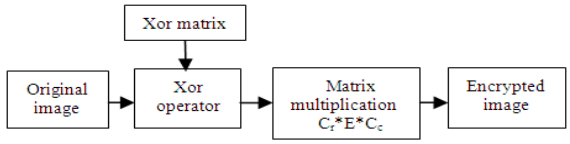
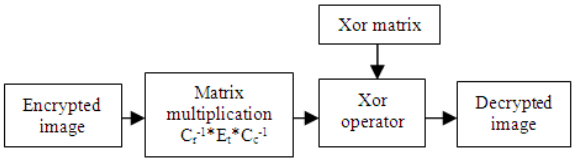


Fig. 1: The 13*13 row matrixes and 15*15 column matrixes



(a) Encryption Process



(b) Decryption process

Fig. 2: The system of the image processing

From the study, we can see that when 3.569945.....$<\mu_0\leq 4$, the mapping is in the chaotic status. value is extremely tiny, when n is greater than some value, the x_n will become prodigious different.

The matrix transformation based on chaotic sequence: As digital image can be regarded Under this circumstance that the distinction of original as a two dimension matrix, we can use the chaotic sequence from Eq. (1) to achieve the grayscale value encryption and position chaos on the whole image. Firstly, we need aim at the grayscale value transformation on the specific pixel (the grayscale value is between 0 and 255), due to the values from this chaotic system are all between 0 and 1. So we need to enlarge every one and then get the modulus to 256. Doing this can ensure the random sequence can be ranged from 0 to 255 and transform the sequence to the two dimension integer sequence based on the size of image, the method for calculating like the Eq. (2):

$$y_n = (x_n * 1000) \bmod N \tag{2}$$

where

x_n = From the Logistic transformation

y_n = The element value which we need on the exclusive or matrix

N = The grey value range, here N is 256

Through the transformation from the Eq. (2), we can make sure that every value can between 0 and 255 and then take the new sequence to structure a matrix.

Secondly, if we want to disorder the two dimension digital image which size is m*n, we need permute the position to every row and column. Suppose C_r and C_c are the row matrix and column matrix we need, so let define these two matrixes, they are shown as Eq. (3) and Eq. (4), where m and n are the subscripts of the transformed matrix:

$$C_r(m,n) = \begin{cases} 1 & (n=X_m) \\ 0 & (n\neq X_m) \end{cases} \tag{3}$$

$$C_c(m,n) = \begin{cases} 1 & (m=X_n) \\ 0 & (m\neq X_n) \end{cases} \tag{4}$$

To give an example, Fig. 1 express the row and column transformed matrix of a 13*15 image, this is according the Logistic sequence that original value is 0.72, μ_0 is 3.8 and we can get the 13*13 row matrix and 15*15 column matrixes.

Encryption algorithm base on the digital image: This study put forward a encryption algorithm which has two steps: the first step, exclusive or every pixel dot on the original image and the element from the matrix base on the Eq. (2), if the size of the original image A is m*n, exclusive or matrix is W, t (m, n) represents the image pixel value after the exclusive or.

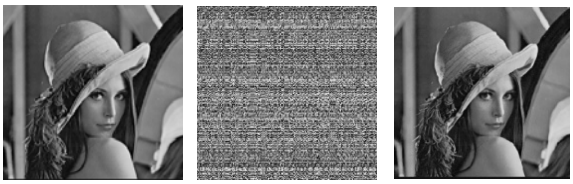
The second step: making a position chaos to the image after exclusive or, also the size of the original image A is m*n, the transformed matrixes are C_r and C_c, their sizes are respectively m*m and n*n, E represents the encryption image after this step, E_t represents the matrix made up by t (m, n) though the Eq. (5), then this transformation encryption process is like the Eq. (6):

$$t(m,n) = p(m,n) \oplus q(m,n) \quad (p(m,n) \in A, q(m,n) \in W) \tag{5}$$

$$E = C_r * E_t * C_c \tag{6}$$

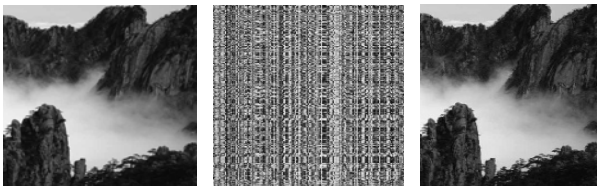
Thus E is the final encryption image. Then the decryption has also contained two steps and this is the inverse operation of encryption algorithm. In the first place take the image E into the transformation of the position, the matrix E_t' has the same position as the original image, based on the properties and characters of the determinant and there is a inverse operation among the matrix multiplication, such as Eq. (7) shows:

$$E_t` = C_r^{-1} * E * C_c^{-1} \tag{7}$$



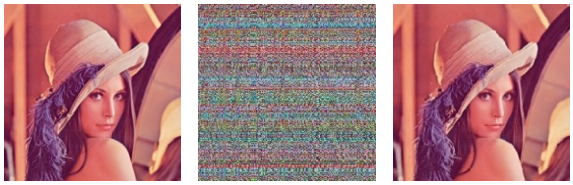
(a) (b) (c)

Fig. 3: The simulation experiment on lenna image



(a) (b) (c)

Fig. 4: The simulation experiment on M * N type image



(a) (b) (c)

Fig. 5: The simulation experiment on RGB image

This moment we can get the original image if we do the exclusive or operation, where u (m, n) is the pixel dot by restoring like Eq. (8):

$$u(m,n)=v(m,n)\oplus q(m,n)\ \ (v(m,n)\in E_t^{'},q(m,n)\in W) \quad (8)$$

In addition, the processes of image encryption and decryption are symmetrical and reversible; the whole process can be concluded as a disposing of image like the Fig. 2.

SIMULATION RESULTS

To prove the feasibility of this algorithm, this study is used the software of MATLAB as the tool for developing and achieving the algorithm for the digital image encryption based on the transformation of Logistic mapping sequence through programming. The experiments among this study aim at the different images consist of different sizes and shapes, thus, the color image also obtained the certification, the Fig. 3, 4 and 5 list the consequences of experiment to 256*256 lenna image, 533*400 scenery image and RGB image. In these experiments, the sequence used the Logistic chaos input μ_0 is 4 and x_0 is 0.68, in the three images, (a) express the original images, (b) express the images after encryption, (c) express the decrypted image. From these consequences, we can find out, this algorithm is suitable for the different sizes, gray image and color image and the efficiency is favorable, can not distinguish the original image from the Encrypted image. Besides, from (c) we can summarize that the inverse operation can successfully restore the original image and the decrypted image are distinct.

ATTACK OPERATING AND COMPARISON

Statistics attack analysis: The ability of resisting statistics attack analysis is one of the standards to judge the superior or inferior of an algorithm. Mention from literary above for the purpose of exclusive or the grayscale value is used to prevent the statistics attack.

From the consequence of this experiment we can see it obviously on the Fig. 6, after exclusive or, the distribution of gray statistics has happened evident changes that the image after disposing has a very good uniformity on gray distribute, so that the image is able to resist the statistics attack over the gray analysis.

Data cutting attacks: During the process of transfer on image information, if the images got the data loss attacks, the restored image always would not be distinguished as the deficiency of the original image, the consequence below just give the data loss attacks to the encrypted image, as the Fig. 7, the top row shows the encrypted images after a 80*80 center or edge cutting attack on different image. The bottom row shows the images reconstructed by the method above. As they contain most of the original images visual information, so these reconstructed images are visually acceptable, even though some distortions are apparent.

Noise attacks: There are many different types of noise existing in public multimedia channels such as internet and wireless communication networks. And the noise belongs to a kind of attack which has no intentions; they would lead to the descending of image quality. The common noise is Salt and pepper noise and Gaussian noise and so on; they are different kinds of image noise. The experimental results in Fig. 8 and 9 shows the performance of the algorithm after it has been subjected to noise attack. The consequence of this experiment is like the Fig. 8 and 9, the top row shows the encrypted images after a Salt and pepper and Gaussian attack on different image. The bottom row shows the images reconstructed by the method above. Even though being affected by noise, these reconstructed images contain most of the original images' visual information. The experimental results demonstrate that the algorithm demonstrates a good

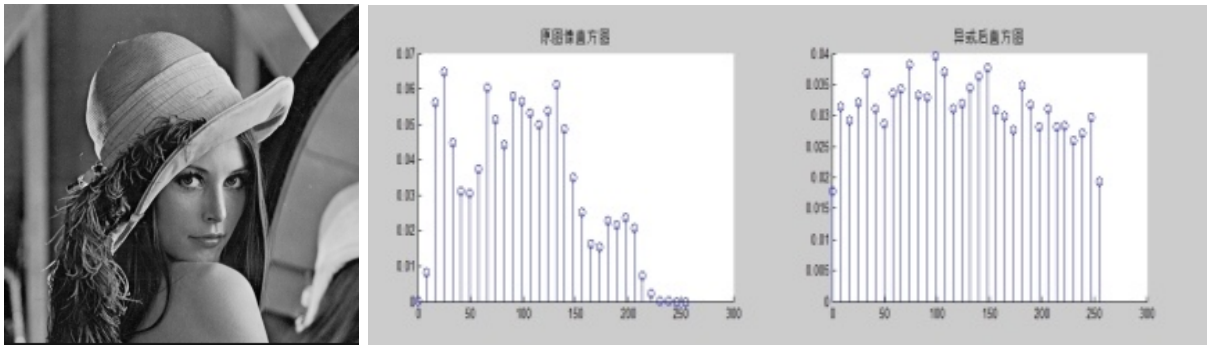
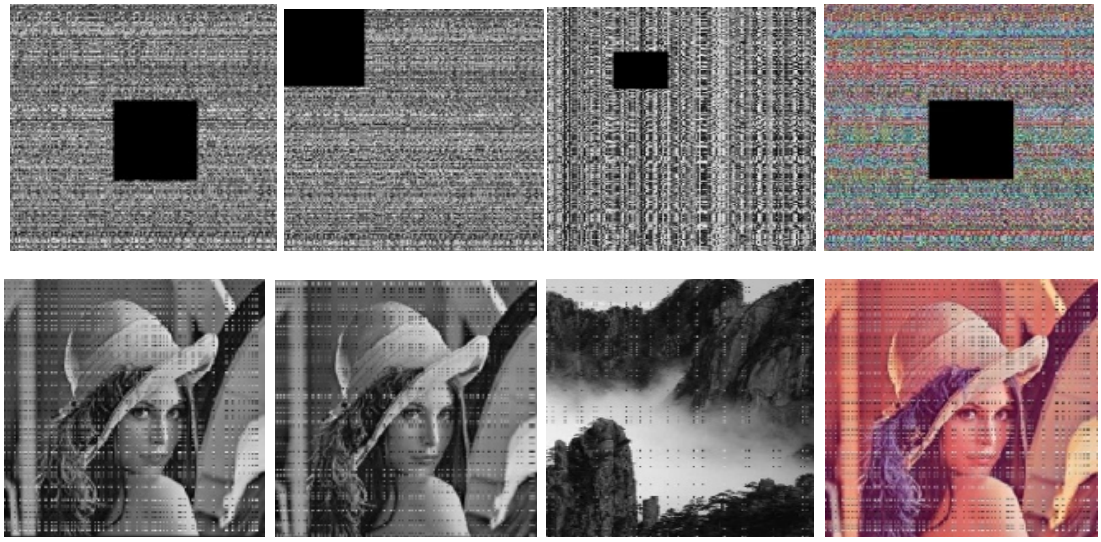
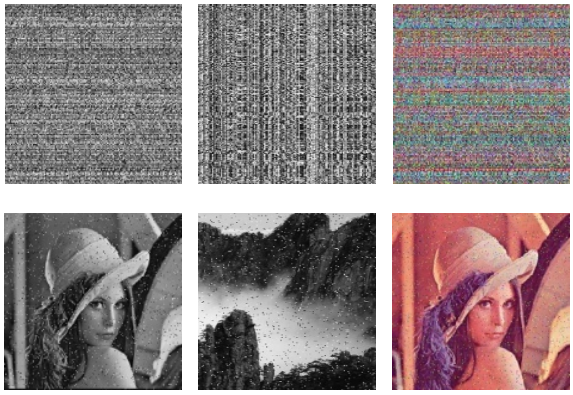


Fig. 6: Grey statistics on lenna image



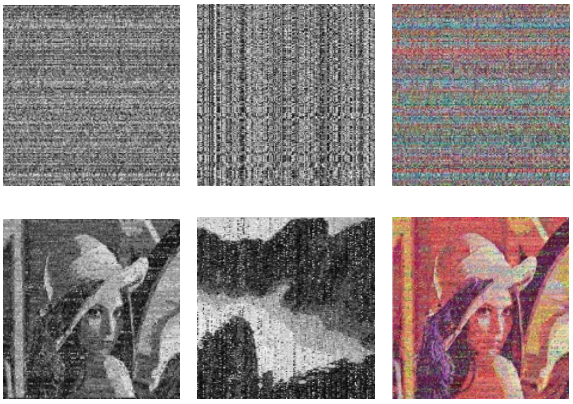
(a) (b) (c) (d)

Fig. 7: Data loss attacks to the encrypted images



(a) (b) (c)

Fig. 8: Salt and pepper noise attack

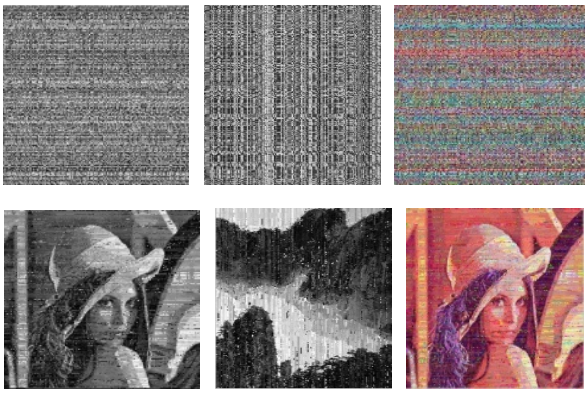


(a) (b) (c)

Fig. 9: Gaussian noise attack

performance against noise attacks as well. The original images can be completely reconstructed even though they are subject to a noisy environment.

Low pass filter attacks: Filtering are common ways of image attacks. Applying these attacks deliberately



(a) (b) (c)

Fig. 10: Gaussian low pass filter attack

helps to verify the ability of the encrypted multimedia data to tolerate possible distortions that may occur in public media transmission channels. Actually Gaussian low pass filter is a kind of signa l filter using at the smooth processing, as we know digital image has a important problem which is the noise in later stage, so this low pass filters are widely used for it to avoid accumulative errors. Figure 10 gives examples of low pass filter attacks. The images were encrypted by the algorithm using the chaotic sequences transformation. These encrypted images were filtered by a 3*3 Gaussian low pass filter. The images shown in the bottom row were reconstructed from these filtered images. These reconstructed images are obviously recognizable. These experimental results demonstrate that algorithm retains its excellent performance in the face of low pass filter attacks.

SECURITY AND EXECUTION TIME ANALYSIS

The space of security keys analysis: In this encryption, the security key has consisted of two parts, part one is the original value of x_0 and μ_0 of the Logistic sequence. Another security key is a formation of the image size, if the row or column matrix is needed the n*n size, while this situation the security keys space is N. Combined of two security keys space, the large number of keys can absolutely withstand the exhaustively attack, so this algorithm has high level security in the applying area.

Execution time analysis: The execution time can demonstrate how efficiently the encryption algorithms encrypt image. This feature is designed to show whether the encryption algorithm can meet the requirements of low computation and high processing speed in real-time applications.

Table 1 gives the execution time. The result was measured on a computer running the Windows 7 operating system with 2GB memory and with a CPU using Intel (R) core (TM) 2 Duo CPU T5750. The time of encryption process was measured when the Logistic sequence was applied individually to image. The results has shown that there is a familiar relation with the size of images and the running time of this method is short, encryption and decryption time can meet the requirements of the normal operation.

Table 1: Algorithm running time statistics

Running time (s)	Lenna (256*256)	Image (533*400)	RGB (256*256)
Encryption	0.031	0.218	0.140
Decryption	0.094	0.499	0.296

CONCLUSION

This study gave a new use about the Logistic chaotic sequence based on the characters of the chaos system and defined a new transformation, the transformation make the chaotic sequence to a two dimension array. Through the relation between the numerical order and the value, making the sequence into a matrix we need. This matrix has well function on substitution; it can carry the pixel dots through substitution so that achieving the chaotic effect. Simultaneously the study has taken the sequence to form an exclusive or matrix to resist statistics attack. Bonding the two methods finished the encryption from two angles of substitution and chaos.

Because the two steps of this algorithm both have inevitability, thus we can use this character to finish the decryption. During the attack experiments, the simulation results and comparisons demonstrated their encryption performance that they are able to withstand common attacks. The original image can be completely reconstructed by this algorithm even though the reconstructed images are slightly different from the original image. Through the security keys space analysis which it has a large keys space, we learned that its security is very well, so the attacking by method of exhaustion can be resist fairly prominent and it has high level safety. What's more, the operating by this algorithm is fleet and uncomplicated; the efficiency can meet the requirements during the normal applying.

ACKNOWLEDGMENT

The authors would like to thank the helpful comments and suggestions from my teachers and colleagues in the laboratory of image recognition and intelligent control. This study is supported by the national '948' Project (2010-4-05).

REFERENCES

Akram, M.Z., A.M. Azizah and S.M. Shayma, 2011. High watermarking capacity based on spatial domain technique. Inform. Technol. J., 7: 1367-1373.

Banerjee, S., 2012. Synchronization of spatiotemporal semiconductor lasers and its application in color image encryption. Optic. Commun., 9: 17-23.

Cai-Hua, L., L. Zhe-Ming and S. Yu-Xin, 2011. Reversible data hiding for btc-compressed images based on bitplane flipping and histogram shifting of mean tables. Inform. Technol. J., 7: 1421-1426.

David, A., 2010. Comment on image encryption with chaotically coupled chaotic maps. Physica, 12: 1002-1006.

Ercan, S., 2009. Cryptanalysis of a chaos-based image encryption algorithm. Phys. Lett. A, 2009(15).

John, F.B., 2011. Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality. Optic. Commun., 284(19): 4350-4355.

Mei-Lei, L. and L. Zhe-Ming, 2011. An image hashing scheme based on mean-removed vector quantization for multiple purposes. Inform. Technol. J., 1: 120-126.

Minghui, D., Z. Qingshuang and L. Sibo, 2012. The watermarking algorithm against shearing based on dopplerlet-radon transformation. Inform. Technol. J., 3: 349-353.

Narendra, S., 2009. Gyrator transform-based optical image encryption, using chaos. Optic. Laser. Eng., 2009(5).

Nur, M., S. Xingming and Y. Hengfu, 2011. An excellent image data hiding algorithm based on BTC. Inform. Technol. J., 7: 1415-1420.

Omid, Z. and I. Subariah, 2011. Adaptive Image steganography based on optimal embedding and robust against chi-square attack. Inform. Technol. J., 7: 1285-1294.

Rengarajan, A., Q. Jiaohua and B.B.R. John, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 5: 566-576.