International Journal of Security and Its Applications
Vol. 10, No. 3 (2016), pp.205-214
http://dx.doi.org/10.14257/ijsia.2016.10.3.19

Color Digital Image Encryption Technology and Software Implementation based on Chaotic Map

Pei Wang

Zhengzhou University of Aeronautics, Henan, 450005, China
hongqi1958@126.com

Abstract

Digital image information security, is accompanied by the rapid development of computer network and multimedia technology and the emergence of new problems. In recent years, the image information on the Internet more and more popular, but for some image information relating to personal privacy and national security, we must take the secret transmission mode, the image encryption technology more and more attention, research has important image encryption technology practical significance. Based on MFC and Matlab7.0 development tools, the paper design color image based on coupling chaotic encryption algorithm developed into an application software that fully implements all the performance of the proposed design of the cryptographic algorithm, and a beautiful interface, easy operation intuitive algorithm evaluation function and so on. In this paper, a digital color image encryption algorithm based on chaotic mapping. It was proposed based on color image encryption algorithm disaster and chaos mapping combined color image encryption algorithm based on logistic mapping, and two encryption algorithms performance comparison and analysis.

Keywords*: Digital image; color image encryption; information security encryption; advanced encryption standard*

1. Introduction

With the rapid development of network technology and multimedia technology, multimedia messaging has become an important means of access to information, it has become an important part of people's lives: the digital information in various forms of portable rapid transmission on the network, e-commerce, e-government through the network it provides a variety of services for us, but at the same time also brought the issue of information security risks [1]. According to statistics, almost every 20 seconds around the world together hacker intrusion incident, According to FBI investigation, only the US annual economic loss due to information security problems caused by it more than 17 billion US dollars [2]. Now, information security technology not only related to personal communications privacy issues related to a company's trade secrets and even the survival of the enterprise, but also issues related to the safety of a country [3, 4]. Therefore, the information security technology is more and more common concern of the whole society [5].

With the multimedia technology, the rapid development of information storage technology and network bandwidth limitations relax, more and more digital images to be transmitted over the network, and gradually become an important means of access to information [6-9]. The images on the network some irrelevant information, some of it is critical, which may relate to individual privacy interests of the company and military secrets, national security. On the other hand, the popularity of the network, development of Internet technology makes it easily accessible to the network and collect information these images, whether such collection is well or ill, legally or illegally, security image

ISSN: 1738-9976 IJSIA

transmission gradually became public concern problem, the image transmitted reliably safe handling also become an important direction of current research [10, 11].

Up to image encryption technology research is in the same space for image re-encoding, which is the image scrambling encryption technology. The general growth of key lengths and encrypt multiple cycles of ways to improve the ability of anti-decipher. Another way is to encrypt the next graph, density map and key are stored in a different space, which is based on secret sharing secret image segmentation and encryption technology. From the current study, this encryption algorithm is present, effective and difficult to decipher. In this paper, a digital color image encryption algorithm based on chaotic mapping. It was proposed based on color image encryption algorithm disaster and chaos mapping combined color image encryption algorithm based on Logistic mapping, and two encryption algorithms performance comparison and analysis.

2. Digital image encryption technology and password system

A. Password System

Image encryption passwords originated in the early classical theory, the theory of the development of modern cryptography has an important role in image encryption password system is often referred to as cryptography, and its block diagram shown in Figure 1, which consists of five parts [12]:

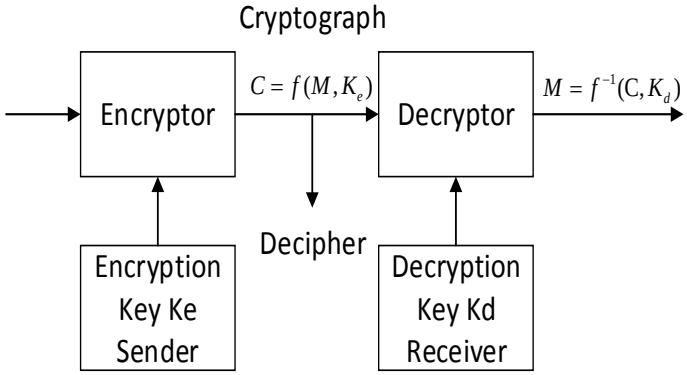


Figure 1. Block Diagram of Password System

(1) Plainiext space M, which is a collection of all plaintext;
(2) The ciphertext space c, which is a collection of all the ciphertext;
(3) Key space K, which is a collection of all keys, key K usually consists of the encryption key Ke and the decryption key Kd composition;
(4) The encryption algorithm E, which is composed of M to e encryption transform, which is called encryption functions f (.);
(5) The decryption algorithm D, which is decrypted by the transformation C to M, where $M=f(c, k_d)$ is the decryption function, which requires f (.) The presence of reversible function.

B. Digital image and its mathematical representation

From a visual perspective, the picture is observing systems with a variety of different forms and means of observation of the objective world and obtained an indirect effect on the human eye to generate visual perception of an entity directly or objective reflection nature scenery or something [13]. It people from birth to appreciate the most important and most abundant information for maximum object [14].

First, the most intuitive to use a two-dimensional matrix to represent a digital image, where the elements of the matrix of rows and columns, that is, the value of the various

elements of the digital image is displayed on a computer screen coordinate pixel point, the matrix is digital image corresponding to the position of the pixel gray scale value (usually 256) or color values [15-17]. for example, a Ge x pixels of a digital image, which pixel gray scale value or color values from the row-column matrix Ge F represented, shown in Figure 2:

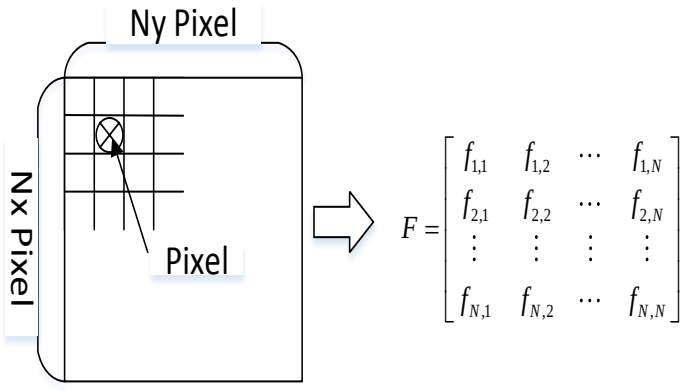


Figure 2. Pixel Gray Scale Value from the Row-column Matrix

C. The basic statistics of the digital image

(1) Image information

An image if there are q gray scale value, and the probability respectively p1, p2, p3 ,,, pi, according to Shannon theorem, the amount of information of this image by equation (1):

$$H = -\sum_{i=1}^{q} p_i \log_2 p_i \tag{1}$$

H is usually called entropy, when the probability of each image appear gray value equal to each other, the image of the maximum entropy for example, an 8-bit digital image represented by the amount of information available in the formula (2):

$$H = -\sum_{i=0}^{255} p_i \log_2 p_i \tag{2}$$

(2) Image average gray

Means the arithmetic mean of the average gray in an image pixel gray value of all, it reflects the average reflection intensity images of different objects, the general formula (3):

$$S = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[f(i,j) - \overline{f}]^2}{MN} \tag{3}$$

(3) Image gray variance

Variance reflects the total value of the discrete level grayscale image average gray value of each pixel, which is a measure of the entropy of an image information as the size of the main metrics, the statistical characteristics of the image of one of the most important statistic variance the larger the amount of information of the image, is calculated as (4)

$$\overline{f} = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} f(i,j)}{MN} \tag{4}$$

Range is the difference between the minimum and maximum grayscale value image gray values, namely

$$f_{range}(i,j) = f_{\max}(i,j) - f_{\min}(i,j) \tag{5}$$

3. Color Image Encryption Algorithm based on Chaotic Mapping

A. Chaotic Map Model

One Dimensional Chaos polynomial model can be expressed by the following ratio of N degree:

$$x_N(n+1) = \frac{\alpha^2 (T_N(\sqrt{x(n)}))^2}{1+(\alpha^2-1)(T_N(\sqrt{x(n)})^2)} = \frac{\alpha^2 T_N^2 x(n)}{1+(\alpha^2-1)T_N x(n)} \tag{6}$$

Take the model range is [0,1], there is a control parameter α, which is written as a polynomial Chebyshev type, n represents the time, N is an integer greater than one.

$X_n(N+1)$ is N-1 order model mapping, because poles having N-1 in the interval [0,1]. According Shwarzian derivative theorem, we can see X (n + l) up to N + 1 cycles attract tracks. This mapping has a most stable fixed point in a single period, or that it is ergodic.

Invariant measure formula of the mapping is as follows:

$$\mu(x,\beta) = \frac{1}{\pi}\frac{\sqrt{\beta}}{\sqrt{x(1-x)}(\beta+(1-\beta)x)}, \beta > 0 \tag{7}$$

Equation (7), (n + 1) of the parameter α can be expressed as follows:

$$\alpha = \frac{\sum_{k=0}^{[\frac{(N-1)}{2}]} C_{2k+1}^N \beta^{-k}}{\sum_{k=0}^{[\frac{N}{2}]} C_{2k}^N \beta^{-k}} \tag{8}$$

This paper presents a new color image encryption algorithm disaster co Chaos Model:

$$\Phi_{3,3,2}(\tilde{x}_1,\tilde{x}_2,\tilde{x}_3) = \begin{cases} \tilde{x}_1(n+1) = \frac{1}{\alpha_1^2}\tan^2(3\arctan\sqrt{x_1(n)}), \\ \tilde{x}_2(n+1) = \frac{1}{\alpha_2^2}\tan^2(3\arctan\sqrt{x_2(n)}), \\ \tilde{x}_3(n+1) = \frac{1}{\alpha_3^2(f(x_1(n),x_2(n)))}\tan^2(2\arctan\sqrt{x_3(n)}) \end{cases} \tag{9}$$

B. AES encryption algorithm, decryption algorithm

AES encryption algorithm, decryption flow chart was shown in Figure 3. Visible when decryption, simply reverse the inverse transform all operations carried out and reverse scheme can use a key schedule. The AES algorithm has its own peculiarities, namely the decryption and encryption have essentially the same structure, so there is an inverse equivalent password, this is equivalent to the inverse code through a series of inverters transform the original exchange AES algorithm to achieve solution, these inverse transformation press and AES encryption algorithm in the same order.

Just key expansion is different, which is to extend the application of the original key, then applied to all round keys except the first one and the last round outside. This is called direct decryption algorithm decryption algorithm In this algorithm, only the steps different encryption itself, but does not appear in the same order of the steps, in order to

facilitate implementation, usually the only nonlinear step placed in the first round of transformation step 1, the structure makes it possible to define an equivalent decryption algorithm, wherein the order of steps used with the same encryption, except that each step into its inverse, and changing the key layout scheme.

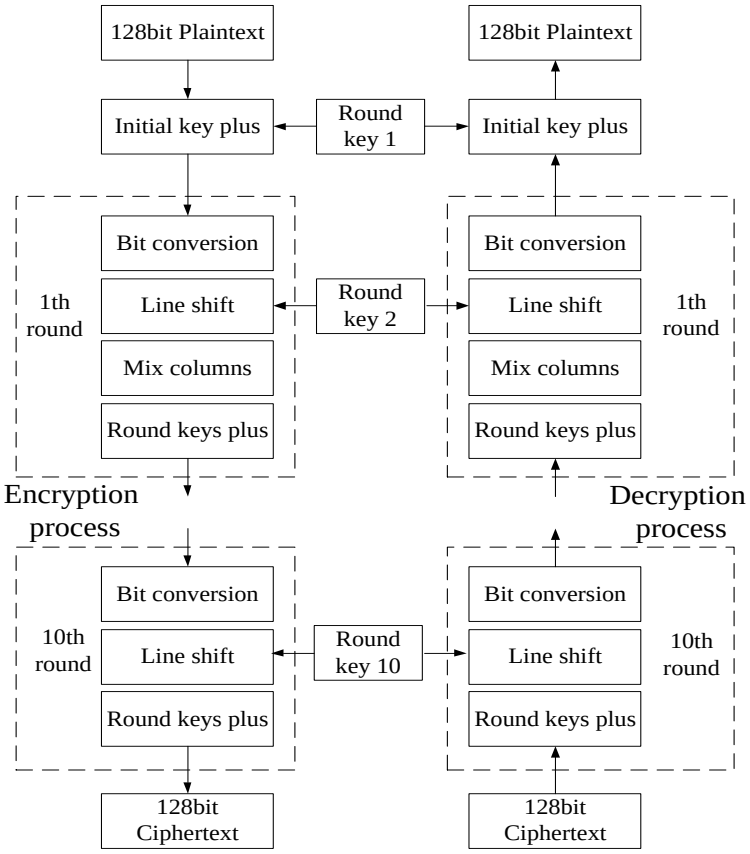


Figure 3. AES Encryption and Decryption Algorithm Flowchart

Birth differential and linear cryptanalysis laid the theoretical foundation iterated block cipher design. Currently, for a new block cipher, only to fight only when given evidence of differential and linear analysis may be carefully considered. Of course, the differential and linear analysis can be implemented not only in attack. A block cipher should be able to fight against all kinds of conceivable cryptanalysis. However, in most cases, the fight against differential and linear analysis has been a major criterion block cipher, while other known means of attack makes key consideration, and usually only a slight modification to the original design to resist.

4. Experiment and Analysis

A. Key Sensitivity Analysis

Sensitivity analysis to calculate the key was taken only different initial values, different control parameters, a different iteration values. Different key value $x_2(0)$ = 0.03600660015037, μ_2= 3.90153455419664, N_2 = 3001. The results were shown in Figure 4.

50 digital color images with different content with different key groups are key sensitivity analysis of the two types of data and analysis results in Figure 4 and Figure 5 Results similar to the above described two figures data is objectively true. It can be seen, the correlation coefficient of the encryption algorithm key sensitivity analysis obtained is

minimal or even negative, which demonstrates the encryption algorithm proposed in this paper is extremely sensitive keys, high security, is an excellent encryption algorithm.

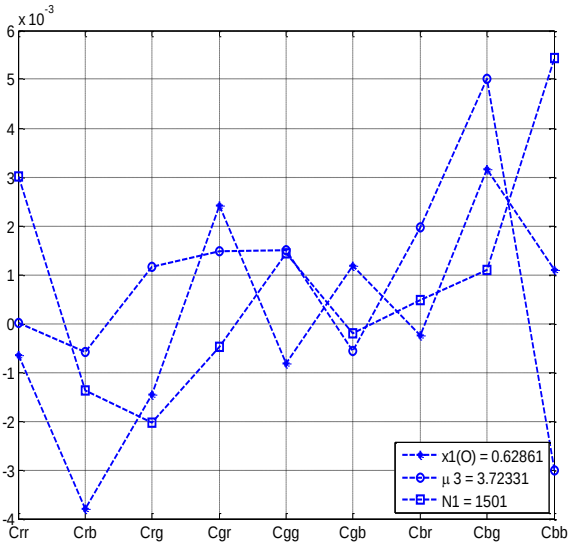


Figure 4. Type a Key Sensitivity and the Correlation Coefficient

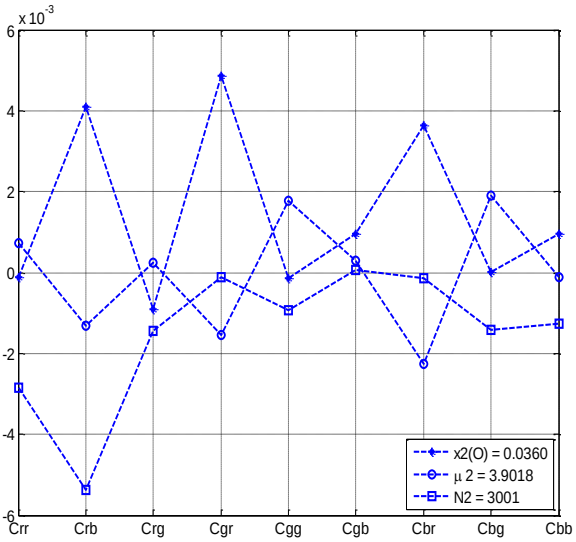


Figure 5. Type Two Key Sensitivity Analysis

B. Security analysis

Safety analysis of standard lot, this section mainly security analysis elect the following items: key space analysis, subtraction dense velocity analysis, histogram analysis, correlation analysis plaintext ciphertext, key sensitivity analysis, adjacent pixel correlation analysis, differential attacks.

If the target image is a color image, a color image because there are R, G, B three-channel component, so we a color image, you need to draw each R, G, B, three channels three histograms. Formula is as follows:

$$p(z)_{(R/G/B)} = \frac{1}{s} \iint_{D(R/G/B)} p_{(R/G/B)}(z', x, y)dxdy \tag{10}$$

R, G, B represent color images of red, green, and blue channels. For a good image encryption algorithm, the encrypted image histogram is smooth, statistical analysis can

not draw a pixel distribution of the encrypted image. Thus, a color image to be encrypted, must meet encrypted color image histogram three channels are smooth. Using the above formula, we can draw a histogram of the original map and encryption lena lena diagram shown in Figure 6:

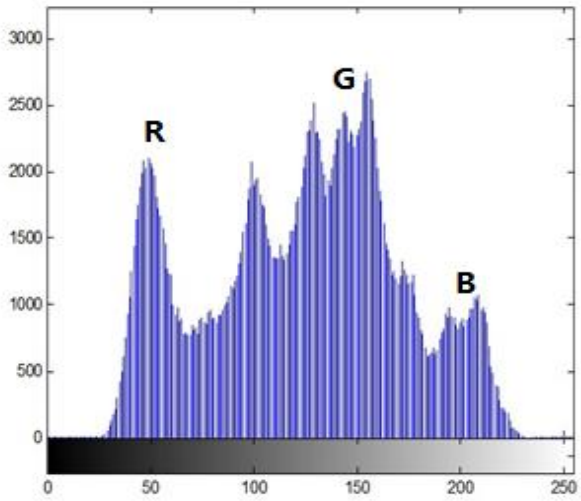


Figure 6. Three-channel RGB Histograms

After drawing 20 different content of over 20 different key set of histograms encrypted digital color chart, draw results found exactly like Figure 7, the encrypted secret all distribution histogram, smooth. The correlation coefficient plaintext and ciphertext lena lena diagram between graphs shown in Table 1.

Table 1. The Correlation Coefficient Plaintext and Ciphertext Lena Lena Diagram between Graphs

Plaintext/ciphertext	Red channel	Blue channel	Green channel
Red channel	0.0078	-0.0015	-0.0016
Blue channel	0.008	-0.002	-0.003
Green channel	0.007	-0.003	0.002

The contents of a completely different color images with digital encryption algorithm used in this paper and the 50 different sets of keys encrypted ciphertext image of nine correlation coefficients, which can be found in 50 sets of data on the correlation coefficient table data similar to a number of correlation coefficients for each group are very small, can be said to be close to zero, so the use of encryption algorithms can be drawn in this article encrypted digital color image is almost random images.

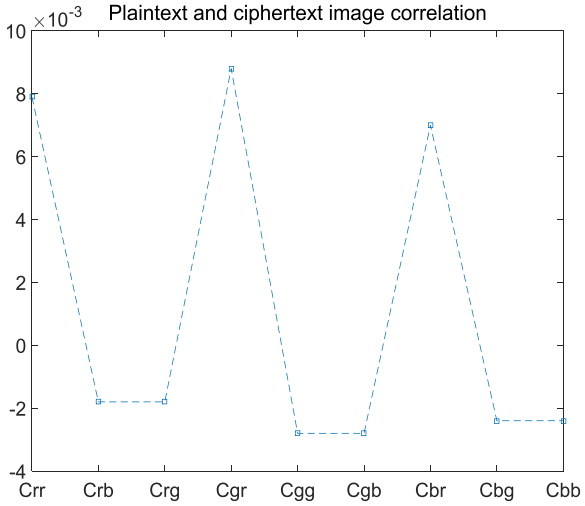


Figure 7. Plaintext Ciphertext Image Correlation Diagram

5. Conclusions

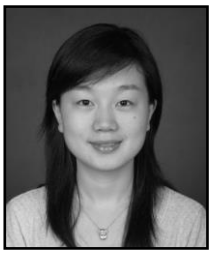
With the rapid development of Internet technology and digital multimedia technology, the public can be very quick access to a variety of digital multimedia information images, video transmission over the network you want, which including individuals, businesses, medical institutions, military, country, etc actors, all of which subject might want to transfer the image information is stored in secure, non-threatening, which the integrity of the information and save the time of image transmission, privacy, and reliability of the higher requirements. In this paper, simulation experiments show that the algorithm can balance plus relationship decryption algorithm speed and security, with high security and fast algorithm encryption and decryption speed, suitable for real-time video communications and secure communication, and proposed two species were compared and analyzed color image encryption algorithm based on chaotic mapping performance.

References

[1] T. F. Lee, C. Y. Lin and C. L. Lin, "Provably secure extended chaotic map-based three-party key agreement protocols using password authentication", Nonlinear Dynamics, **(2015)**, pp. 1-10.
[2] D. Mishra, J. Srinivas and S. Mukhopadhyay, "A secure and efficient chaotic map-based authenticated key agreement scheme for telecare medicine information systems", Journal of medical systems, vol. 38, no. 10, **(2014)**, pp. 1-10.
[3] S. Zhang, H. Yao and X. Sun, "Sparse coding based visual tracking: Review and experimental comparison", Pattern Recognition, vol. 46, no. 7, **(2013)**, pp. 1772-1788.
[4] K. Cannons, "A review of visual tracking", Dept. Comput. Sci. Eng., York Univ., Toronto, Canada, Tech. Rep. CSE-2008-07, **(2008)**.
[5] Q. Jiang, J. Ma and X. Lu, "Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems", Journal of medical systems, vol. 38, no. 2, **(2014)**, pp. 1-8.
[6] C. Chang and R. Ansari, "Kernel particle filter for visual tracking", Signal processing letters, IEEE, vol. 12, no. 3, **(2005)**, pp. 242-245.
[7] H. Grabner and H. Bischof, "On-line boosting and vision", Computer Vision and Pattern Recognition, IEEE Computer Society Conference, IEEE, vol. 1, **(2006)**, pp. 260-267.
[8] H. Grabner, C. Leistner and H. Bischof, "Semi-supervised on-line boosting for robust tracking", Computer Vision–ECCV, Springer Berlin Heidelberg, **(2008)**, pp. 234-247.
[9] S. Stalder, H. Grabner, L. Van Gool, "Beyond semi-supervised tracking: Tracking should be as simple as detection, but not simpler than recognition", Computer Vision Workshops (ICCV Workshops), IEEE 12th International Conference IEEE, **(2009)**.
[10] X. H. Han, L. Quan and X. Xiong, "A modified gravitational search algorithm based on sequential quadratic programming and chaotic map for ELD optimization", Knowledge and Information Systems, vol. 42, no. 3, **(2015)**, pp. 689-708.

[11] B. Babenko, M. H. Yang and S. Belongie, "Visual tracking with online multiple instance learning", Computer Vision and Pattern Recognition, CVPR IEEE Conference, IEEE, **(2009)**.
[12] N. Dalai and B. Triggs, Histograms of oriented gradients for human.
[13] Q. Chen, N. D. Georganas, E. M. Petriu, "Real-time vision-based hand gesture recognition using haar-like features", Instrumentation and Measurement Technology Conference Proceedings, MTC IEEE, **(2007)**.
[14] J. Chen, Y. He and J. Wang, "Multi-feature fusion based fast video flame detection", Building and Environment, vol. 45, no. 5, **(2010)**, pp. 1113-1122.
[15] T. H. M. Soliman, F. F. Yang and S. Ejaz, "A Polar Coding Scheme for Secure Data Transmission Based on 1D Chaotic-Map", International Conference on Computer Information Systems and Industrial Applications. Atlantis Press, **(2015)**.
[16] W. Yao and S. Qin, "Aircraft diagnosis by solving map exactly", Review of Computer Engineering Studies, vol. 2, no. 1, **(2015)**, pp. 1-8.
[17] R. Jin, C. Kou and R. Liu, "Biclustering algorithm of differential co-expression for gene data", Review of Computer Engineering Studies, vol. 1, no. 1, **(2014)**, pp. 7-12.

Author



Pei Wang, She received her M.A. in Art and Design (2006) from Donghua University. Now she is lecturer of landscape design at Art and Design Department, Zhengzhou University of Aeronautics. Her current research interests include different aspects of Environment Design and Landscape Design.