International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.229-240
http://dx.doi.org/10.14257/ijsia.2013.7.6.23

Design and Analysis of Fast Image Encryption Algorithm based on Multiple Chaotic Systems in Real-time Security Car

Shuai Wang[1,2], Wei Sun[1,*], Yinan Guo[1], Haiqun Yang[1] and Shuming Jiang[2]

[1] *School of Information and Electrical Engineering, China University of Mining & Technology, Xuzhou 221008, China*
[2] *Information Research Institute, Shandong Academy of Sciences, Jinan 250014, China*
***Corresponding author: Wei Sun**
E-mail:wangsh@sdas.org

Abstract

This paper takes intelligent security car as the research background, aiming to find a image encryption algorithm to realize the car in the image secure transmission of wireless transmission network based on open protocols, with good safety and high real-time. this passage is based on the analysis of the existing encryption algorithms of traditional and new image, select the digital image encryption technology based on chaotic system, And put forward a Multiple chaotic image encryption method which is fit for this project, After analysis and test, the algorithm satisfies the requirements of safety and real-time.

Keywords*: image encryption; scrambling; spread; safety; Encryption efficiency*

1. Introduction

In the public security field, because the security car has the advantages of fast deployment, acquiring the image characteristics flexible, remote real-time security .In recent years have received wide attention. The security car involved in the project can be flexibly deployed in the airport, bank, prisons and other classified area, In view of the staff is difficult to reach narrow low space (*e.g.*, Vehicle chassis, pipeline, box, unidentified objects etc.) to collect images for remote real-time safety inspection.

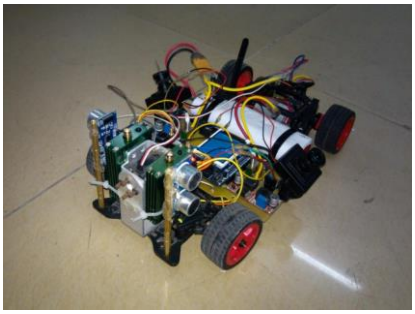


Figure 1. The Intelligent Security Car

As is known to all, digital image has large quantity of data. If we use traditional principle of cryptography encryption will cause long encryption cycle, low efficiency, and difficult to meet the real-time requirement, But the properties of chaotic system can make up for the traditional principle of cryptography, provides a more effective way for digital image encryption.

In 1989 Matthews first clear point out "chaotic cipher" in his article, which is using chaos encryption as the core and describes a chaotic stream cipher scheme deformation in

ISSN: 1738-9976 IJSIA

detail based on Logistic map. His expound about chaotic cryptography attracted the attention of all fields, brought the research upsurge of chaotic cryptography. With further research, strange attractor, bifurcation, Lyapunov index theory have been proposed, chaotic theory has gradually improved, the rule and the potential application has been discovered. Considering the chaotic system with ergodicity, randomness and initial-value sensitivity, chaotic systems have become increasingly used in data encryption.

With the deepening of the study, theory and technology of chaotic system based on image encryption have a greatly development [1-6]. In considering the equilibrium between the encryption security and encryption efficiency, the related techniques are needed to further improve and perfect. Li F Y, and Xu 's article on the proposed image encryption algorithm and Hash function based on chaotic systems [7], The literature describes construct chaotic sequence for pixel scrambling by using Hash function, grayscale image diffusion by using Logistic chaotic system, the security of the algorithm is strong, but the efficiency is not high. Zhang Yudong proposed an image encryption algorithm based on hybrid optical holography [8], The algorithm uses the Arnold mapping to achieve pixel scrambling, and the use of a random number generation algorithm based on the twist method to change gray, finally to realize the image encryption using optical hologram, By experimental verification, the algorithm security is better, but for the 256 * 256 image, the encryption time close to 1s, efficiency is not high. Gao *et. al.*, proposed an image encryption algorithm based on hyperchaos [9], The algorithm uses the Logistic Chaotic Mapping Iterative get different sequence values, then Separately on the plaintext matrix row and column directions of scrambling, Followed by using the value which is generated by the chaotic iteration to change the scrambling image's pixel gray scale. Because this algorithm only uses key stream to realize the independent encryption of pixel, because the lack of mutual influence and restriction in the process of pixels encryption, against differential attack ability is low In order to further improve the security and encryption efficiency, Zhu and his colleagues improved the algorithm, to ensure the security and the 256 * 256 image encryption time was reduced to 0.047s.

Due to security car system have to deal with a lot of image information in a short time, and the image encryption is a necessary step for the normal operation of the system, so the executing efficiency directly affects the whole system's efficiency. In view of this, Encryption algorithm not only need to ensure the safety, but also need to maximize efficiency, obtain the efficient solution. In this paper proposed the encryption algorithm of multiple chaotic fast image based on a large number of research results, to ensure the security and reduce the encryption time, also to improve the algorithm efficiency.

2. Fast Image Encryption Algorithm based on Multiple Chaotic Systems

2.1. Chaotic Maps

(1) the Logistic mapping

Logistic mapping is a typical representative of the chaotic mapping. Although it is one dimensional mapping, the control effect is very good. The Logistic equation is shown as follows:

$$x_{n+1} = \lambda x_n (1 - x_n) \quad (n = 0,1,2,\cdots) \quad (1)$$

In the formula, x_n is the variable, as well as λ is the system parameter in which $\lambda \in (0,4], x_n \in [0,1]$. When $1 \le \lambda < 3$, the solution of the system is fixed point. When $\lambda = 3$ the formula starts the transition state, when $\lambda = 3.5699456$, the system enters a chaotic state. When we set $\lambda = 3.9$, the initial value of x_n is 0.6, the results below

reflect the chaotic sequence values of Logistic mapping in the iteration process of 200 times.

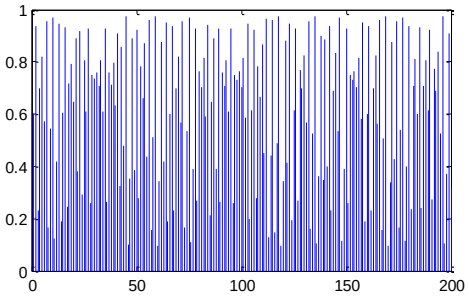


Figure 2. Iterative Sequence Value of Logistic Mapping

(2)Kent mapping

Kent mapping is also a kind of common chaotic map, the map has the feature of short-term predictable and unpredictable for a long time, at the same time has a high sensitivity on initial value, The Kent equation is shown as follows:

$$x_{n+1} = \begin{cases} x_n / a & 0 < x \le a \\ (1 - x_n)/(1 - a) & a < x < 1 \end{cases} \qquad (2)$$

In the formula, x_n is the variable, as well as a is the system parameter in which $a \in (0,1), x_n \in [0,1]$. When we set $a = 0.6$, the initial value of x_n is 0.6, the results below reflect the chaotic sequence values of Logistic mapping in the iteration process of 200 times.

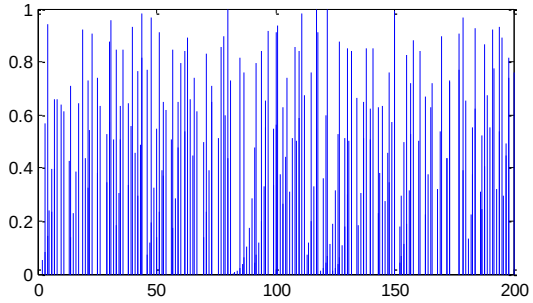


Figure 3. Iterative Sequence Value of Kent Mapping

2.2 scrambling of image pixels

Digital image scrambling algorithm is commonly used in image processing .Image scrambling is to change the original sequence of image pixels[10], so that the third party can not distinguish image information. In practical application, the pixels order is more confusion, the image information is more difficult to identify, and encryption effect is better. However, the process of scrambling is not irregular, but according to the corresponding algorithm is implemented. At the same time, with the corresponding algorithm, the image can restoration.

The widely used scrambling technology including Arnold mapping, standard map and magic transformation, in which Arnold mapping is the most typical[11], and its

scrambling effect is good. Arnold mapping is also called the cat map, as shown in expression (3):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod} \quad N) \qquad (3)$$

Among them, $x, y \in \{0,1,\cdots,N-1\}$, and (x, y) is the initial position of the pixels , and (x', y') is the position after the pixels transform, N is one side of rectangular image (square). In practical applications, the Generalized two-dimensional Arnold mapping is as shown in (4):

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} (\text{mod} \quad N) \qquad (4)$$

p and q are the control parameters of the chaotic equation. (x, y) is the position of image pixels, N represents length for the image. Control parameter in equation is produced by Logistic mapping, Logistic map as shown on the type (5) :

$$x_1(n+1) = \lambda x_1(n)[1 - x_1(n)] \qquad (5)$$

In order to realize the chaotic state, we set 3.8≤□≤4 (encryption can choose a floating-point type data in this range), the calculation process of the control parameters are as follows:

< 1 > Iterate 200 times in the Logistic mapping, in order to eliminate the influence of initial value.

< 2 > Get the parameters of scrambling by type (6), which $\lfloor x \rfloor$ represents the largest integer no greater than x:

$$\begin{cases} p = \lfloor x_1(200) \times 2^{12} \rfloor \bmod N \\ q = \lfloor x_1(200) \times 2^{10} \rfloor \bmod N \end{cases} \qquad (6)$$

In the formula, $x_1(200)$ represents the value after Iterating 200 times.

After testing, no matter how many rounds of scrambling, the position of the image (0, 0) remains unchanged, which provides possibility for the ciphertext crack. In order to prevent the crack from (0, 0) as the breakthrough point to analyze the ciphertext, we need to adopt additional measures to change the position of pixel (0, 0). So we swap position (0, 0) and (m, n) to reduce the ciphertext risk.

2.3. Diffusion of Image Pixels

Just using scrambling operation cannot avoid cracked through the analysis method of the plaintext attack[12]. You tend to choose a specific point, and study its position to find changes in the transformation of scrambling. Confidentiality is not high only using scrambling. But by using diffusion algorithm each pixel value changes well, avoiding the plaintext attack , and further improving the confidentiality.

Diffusion algorithm is generally performed using modular arithmetic and adding operation. Modular algorithm can make the calculation results in the normal range ,and add operation can make the different gray values of the pixels interrelated, increasing interaction between pixels; on the other hand, the distribution of pixel gray value is more uniform. In order to enhance the effect of diffusion, according to chaos pseudo randomness and ergodicity, chaos factor can be introduced into the algorithm. Diffusion

formula using modular arithmetic, add operation and chaotic sequence is shown in expression (7):

$$C(k) = S(k) \oplus \{[P(k) + S(k)] \bmod M\} \oplus C(k-1) \quad (7)$$

In the formula, we set P (k) and C (k) as the current plaintext and ciphertext value. C (k-1) represents the last ciphertext value, where C (0) defined as constants (100), M represents gray level(256). S (k) represents the controlled parameter the control parameters, which obtained by mapping. Kent mapping is a commonly used chaotic mapping, which is shown in expression (8).

$$x_2(n+1) = \begin{cases} x_2(n)/\mu & 0 < x \le \mu \\ (1 - x_2(n))/(1-\mu) & \mu < x < 1 \end{cases} \quad (8)$$

We set 0<μ<1 (we can choose a floating-point type data in this range).We can get the parameters of diffusion in the follow way:

<1> Iterate 200 rounds using the Kent mapping, in order to eliminate the influence of initial value.

<2> Get scrambling the parameters of diffusion by the following formula:

$$S(k) = \lfloor x_2(200) \times 2^{16} \rfloor \bmod M \quad (9)$$

In the formula, $x_2(200)$ represents the value after Iterating 200 times.

2.4. Procedures of Image Encryption and Decryption

To achieve image encryption the algorithm use the methods of scrambling and diffusion. In order to increase the security of the system, the control parameters of scrambling and diffusion are produced by Logistic and Kent mapping. By the above analysis, we can see image encryption algorithm of scrambling and diffusion based on multiple chaotic systems is more useful than the traditional algorithm.

Flowchart of Multiple chaotic fast image encryption algorithm is shown in Figure 4:

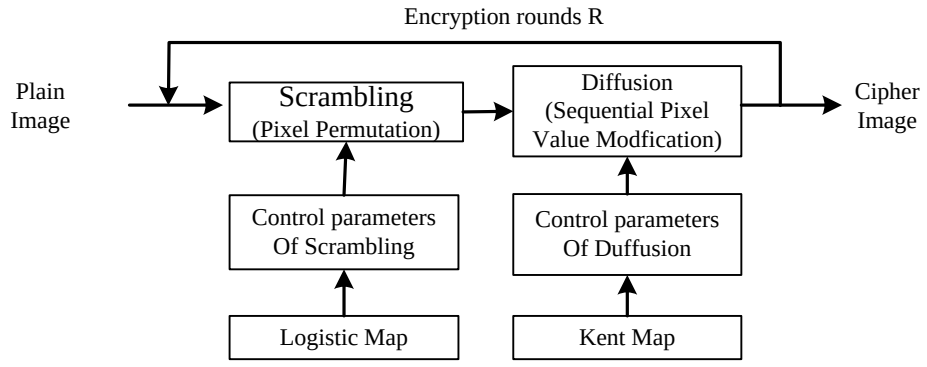


Figure 4. Image Encryption Process

Encryption steps are shown as follows:

Step 1: Set the values of and x1(0), generate the parameters of scrambling by Logistic mapping requirements.

Step 2: Generate the Arnold chaotic scrambling equation according to the control parameters, and we implement one scrambling transformation.

Step 3: exchange position between (0, 0) and (m, n) after scrambling.

Step 4: Set the values of and x2(0), generate the parameters of diffusion by Kent mapping.

Step 5: according to the formula (7) implemented a pixel scrambling transformation.

Step 6: implement scrambling and diffusion process repeatedly, until meeting the requirements of encryption system.

Decryption is the reverse process of encryption process, the main steps are as follows :

Step 1: Set the values of and x2(0), generate the parameters of diffusion by Kent mapping requirements and we implement one inverse diffusion transform, transform formula is as shown in formula (10).

$$P(k) = \{S(k) \oplus C(k) \oplus C(k-1) + M - S(k)\} \bmod M \quad (10)$$

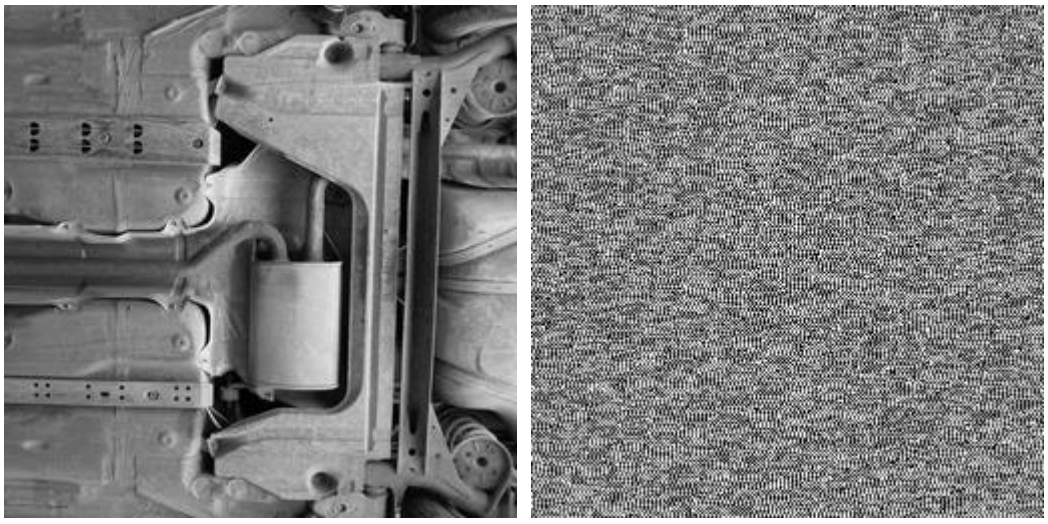
Step 2: exchange position between (0, 0) and (m, n).

Step 3: Set the values of □ and x1(0), generate the parameters of scrambling by Logistic mapping requirements. and generate the Arnold chaotic scrambling equation according to the control parameters, and we implement one inverse scrambling transformation.

Step 4: return to Step 1, until decrypting the original image.

3. The Experimental Results and Analysis

Experimental simulation software is Matlab2007a, the image is " Vehicle chassis photo.jpg". Its size is 512 * 512, and encryption keys are □、□、x1(0)、x2(0)、m、n. We set □=3.95、□=0.6、x1(0)=0.987654321、x2(0)=0.123456789、m=100、n=100. Encryption image is shown in figure 5.



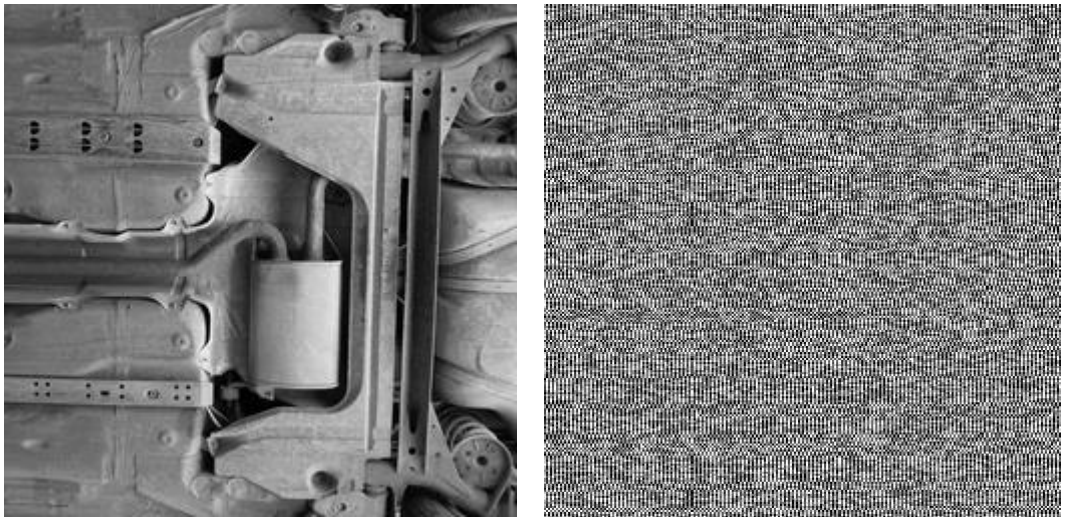
a **b**

Figure 5. (a) Plain Image; (b) Cipher Image using Multiple Chaotic Systems

3.1. Key Analysis

(1) Key space. Encryption keys are □、□、x1(0)、x2(0)、m、n. In formula 3.8≤□≤4、0< □ <1、0< x1(0)<1、0< x2(0)<1,and values of m and n can chose any integer between 1 to N. Due to floating point data accuracy is 1015 , the key space of the algorithm is 2×N2×1059. Thus, the algorithm has enough key space.

(2) key sensitivity analysis. Key sensitivity is mainly refers to small changes on encryption key will lead to great difference of ciphertext, so tiny differences will lead to complete failure of decryption. In decryption experiment, we set x1(0)=0.987654321,x2(0)=0.123456789 ,decrypting correctly .When we set x1(0)=0.987654322,x2(0)=0.123456789 , decryption is failure. Contrast diagram of image decryption effect is shown in Figure 6. In the experiment we can see this algorithm has better security, small difference of the key will cause the image decryption failure.



a **b**

Figure 6. (a) Correctly Decrypting Image; (b) Failure Decrypting Image

3.2. Statistical Analysis

(1) Gray histogram. The histogram depicts the statistical characteristics of gray of pixels. in digital images, the feature can be related to the statistical analysis on the image, providing means for the correct interpretation of image. We can see the gray distribution of the pixels of the image in the gray histogram of image, in which abscissa represents gray value of the pixel (an integer range is 0 to 255), and ordinate represents the number of pixels. Figure 5-5 shows the histograms of two images encryption. By comparing the two gray histograms we can see the distribution of pixel gray value is more uniform in gray interval 0-255, masking characteristics of the gray statistical of the original image well, reaching the expected requirements.

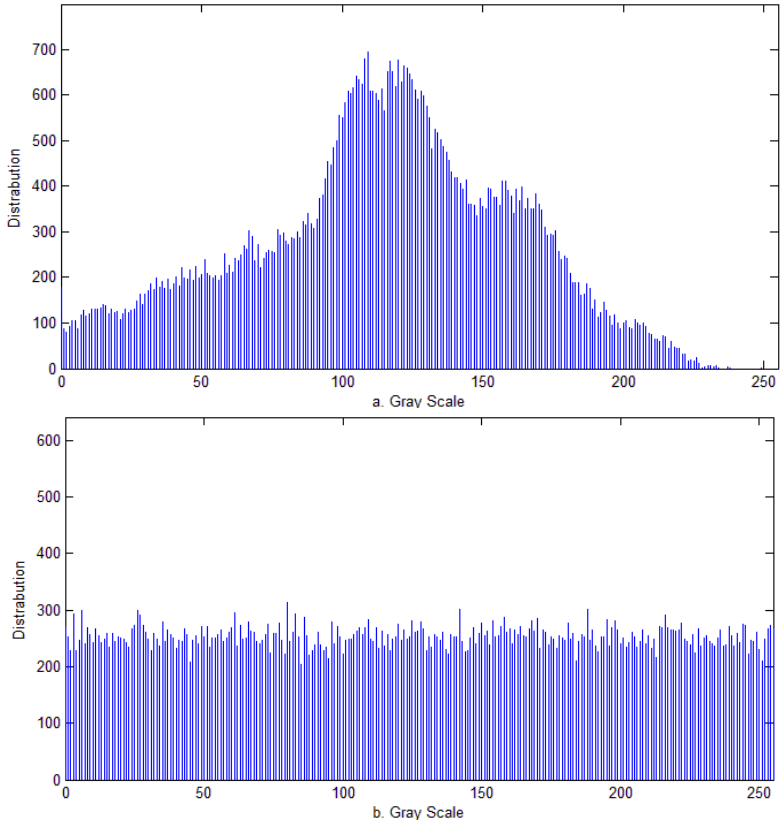


Figure 7. (a) Gray histogram of the Image before Encryption; (b) Gray histogram of the Image after Encryption

(2) Correlation of adjacent pixels. Correlation of adjacent pixels refers to levels of correlation near pixels of image. General correlation of adjacent pixels of the normal image is very strong, but the correlation between encrypted ciphertext in horizontal, vertical and diagonal directions of the adjacent pixels is greatly reduced and the correlation coefficient is very low. The correlation coefficient of the encrypted ciphertext can directly reflect the encryption effect: if the correlation coefficient is smaller, and the pixel correlation is lower, the ability against statistical analysis is stronger, encryption effect is better. In order to test the pixel correlation in the horizontal direction, vertical direction and diagonal directions, we chose more than one thousand groups of adjacent pixels from these three directions randomly. Definition of correlation coefficient is as follows:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{11}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{12}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{13}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{14}$$

In the formula, r_{xy} is correlation coefficient, $\mathrm{cov}(x, y)$ is covariance, $D(x)$ is variance, $E(x)$ is covariance, and x, y mean gray value of adjacent pixels.

The correlation coefficient in the horizontal direction, vertical direction and diagonal directions are respectively 0.9479, 0.9574 and 0.9143 after testing by Matlab. The experimental results show that the correlation of neighboring points are very small. At the same time the chart of the pixels correlation of plaintext and ciphertext plaintext shows, encryption adjacent pixel gray has no relevance after encryption. The secrecy of ciphertext is very good.

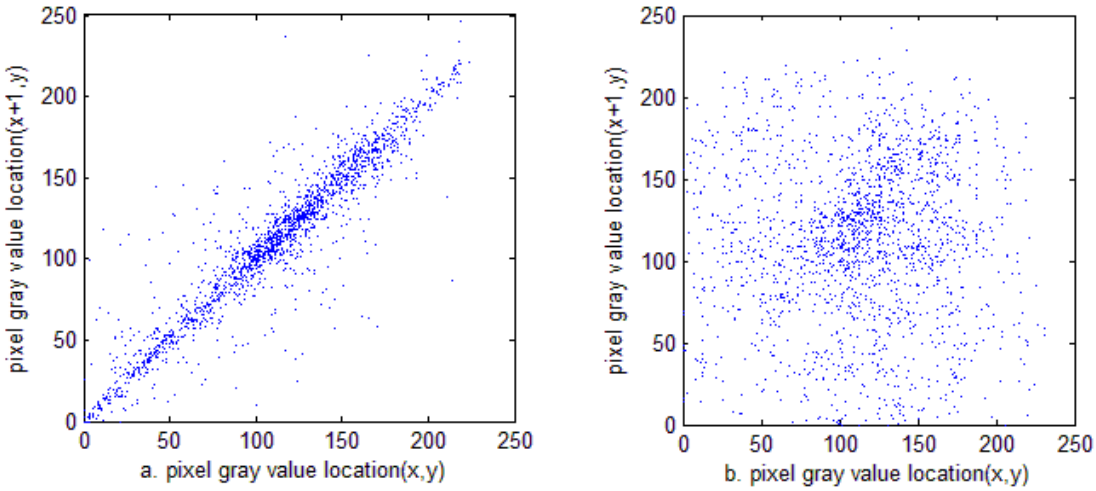


Figure 8. Correlations of Tow Horizontally Adjacent Pixels in (a) the Plain Image; (b) the Cipher Image

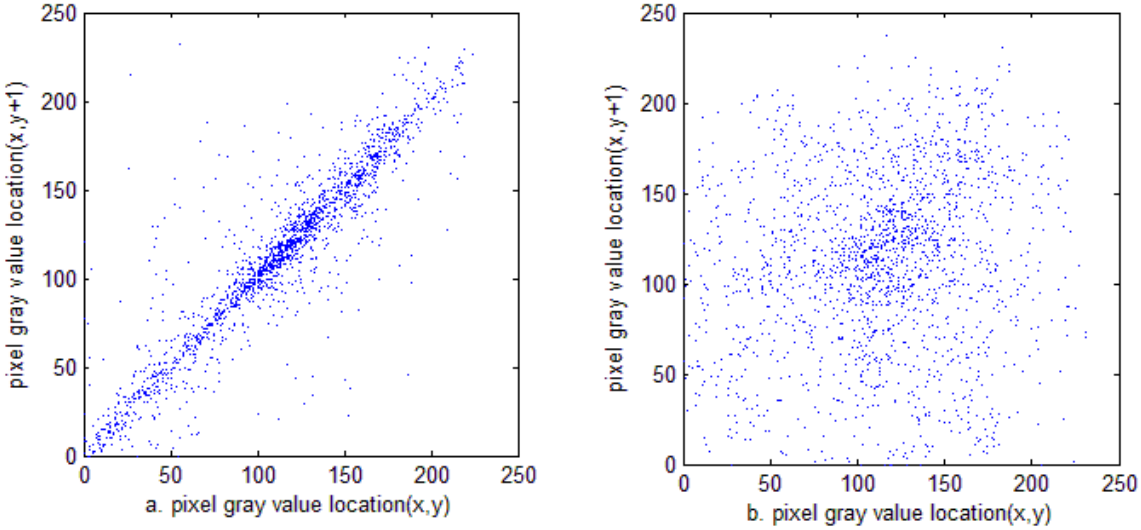


Figure 9. Correlations of Tow Vertically Adjacent Pixels in (a) the Plain Image; (b) the Cipher Image

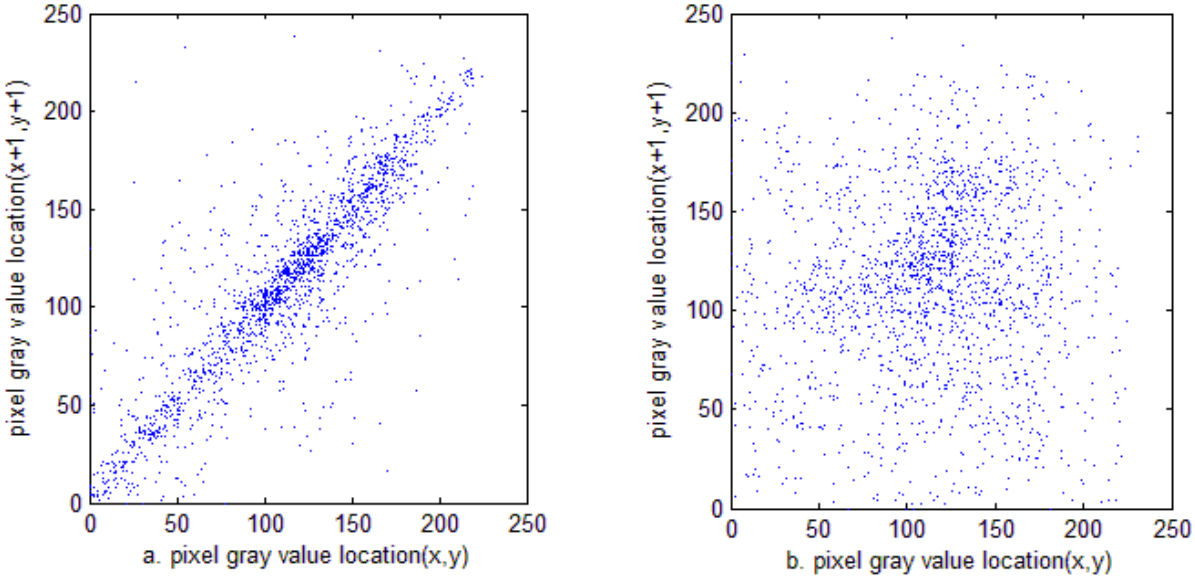


Figure 10. Correlations of Tow Diagonal Adjacent Pixels in (a) the Plain Image; (b) the Cipher Image

3.3. Differential Attack

Differential attack is a plaintext chosen attack. Attackers often use differential analysis to crack the ciphertext. They usually change one or several pixels of the image, by comparing the two ciphertext to find encryption rules.

There are two evaluation indicators testing ability to resist differential attack which are NPCR and UACI. NPCR refers to changes in the number of pixels of the ciphertext after a pixel gray image changed and UACI refers to change of gray of ciphertext after one pixel change in gray. NPCR and UACI are shows as formula (15) and (16).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \qquad (15)$$

$$UCAI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \qquad (16)$$

In the experiment, modify the gray value of (10, 10) in the matrix of the image whose name is "bottom photo.jpg".NPCR and UACI values are shown in which 5-1.The number in the first line means encryption rounds. After the test, when the encryption rounds is greater than or equal to 2 can meeting the conditions: NPCR>99.6%, UACI>33.3%. Ability of algorithm against differential attack is good.

Table 1. Connection of the Value of NPCR and UACI with the Rounds of Encryption

Encryption rounds R	1	2	3	4	5
NPCR	26.95%	99.63%	99.67%	99.61%	99.63%
UACI	13.53%	33.78%	33.75%	33.46%	33.60%

3.4. Analysis of Encryption Speed

The test software of this algorithm is Matlab7.1, the hardware is a computer with the CPU of 2.0GHZ, memory of 2G.When R=2 (algorithm with ability resist differential attack), image encryption with the size of 512 × 512 only use 0.13S, image encryption

with the size of 256 × 256 only use 0.032S. By comparing the document 5, document 6 and document 9 we can get results in table 2 and which shows that the method in this paper guarantees the security of encryption at the same time, encryption speed is fast, so it is the best encryption in the system.

Table 2. The Time Result on Different Encryption Algorithm

	Ref 5	Ref 6	Ref 9	Proposed
Encryption time（s）	1.128	0.995	0.047	0.032

4. Algorithm Summary

After experimental analysis we can see key space is large and key sensitivity is very strong. The algorithm can resist analysis attack effectively; the statistic of pixel gray is a uniform distribution statistic, correlation of adjacent pixels is weak, so it can resist statistical attack well; NPCR and UACI can achieve the ideal values when encryption rounds is greater than or equal to 2 .At the same time, ability of the algorithm for resisting differential attack is very strong; image encryption is fast and can meet the needs of online encryption and decryption with the current size.

In summary, the algorithms has good performance when R=2, which can meet the requirement image secure transmission of system of car in security and real-time.

References

[1] H. Zhu, C. Zhao and X. Zhang, "A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem", Image Communication, vol. 28, **(2013)**, pp. 670-680.
[2] Y. Zhang, D. Xiao, Y. Shu and J. Li, "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations", Image Communication, vol. 28, **(2013)**, pp. 292-300.
[3] S. Behnia, A. Akhavan, A. Akhshani and A. Samsudin. "Image encryption based on the Jacobian elliptic maps", Journal of Systems and Software, vol. 86, **(2013)**, pp. 2429-2438.
[4] C.-H. Lin, T.-H. Chen and C.-S. Wu, "A batch image encryption scheme based on chaining random grids", Scientia Iranica, vol. 20, **(2013)**, pp. 670-681.
[5] A. Bakhshandeh and Z. Eslami. "An authenticated image encryption scheme based on chaotic maps and memory cellular automata", Optics and Lasers in Engineering, vol. 51, **(2013)**, pp. 665-673.
[6] A. A. Abd El-Latif, L. Li, N. Wang, Q. Han and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces", Signal Processing, vol. 93, **(2013)**, pp. 2986-3000.
[7] F. Li and J. Xu, "Image encryption algorithm based on Hash function and multiple chaotic systems", Computer Engineering and Design, vol. 31, **(2010)**, pp. 141-144.
[8] Y. Zhang, L. Wu and S. Wang, "Improved ant colony algorithm based on membership cloud models", Computer Engineering and Applications, vol. 47, **(2011)**, pp. 201-205.
[9] T. Gao and Z. Chen, "A new encryption algorithm based on hyper-chaos", Phys. Lett, vol. 372, **(2008)**, pp. 394-400.
[10] C. He, L. Chen and Z. Wang, "Chaotic image scrambling algorithm based on magic cube", Computer System Applications, vol. 19, **(2010)**, pp. 50-53.
[11] W. Hou and C. Wu, "Image encryption and sharing based on arnold transform", Journal of Computer Applications, vol. 31, **(2011)**, pp. 2681-2686.
[12] J. Liu, C. Zhu and Y. Wang. "Image scrambling effect evaluation method based on position correlation", Computer Engineering, vol. 36, **(2010)**, pp. 208-210.

Authors

Shuai Wang. He received his B.E in Qingdao Technological University (2006) and M.Sc. in Control Theory and Engineering (2009) in China University of Mining & Technology, Now he is a Ph.D. candidate in Information and Electrical Engineering School, China University of Mining & Technology, Xuzhou, Jiangsu. His major fields of study are image processing, pattern recognition and information security.

Wei Sun. He received his M.Sc. in Computer Application (1988) in Beijing University of Aeronautics and Astronautics and Ph.D. in Information and Electrical Engineering School (1994), China University of Mining & Technology, Xuzhou, Jiangsu. Now he is full professor of Automation Department, China University of Mining & Technology. His current research interests include different aspects of Artificial Intelligence and Image Processing.

Yinan Guo, Directed PhD program in China University of Mining & Technology, She received her Ph.D. in Information and Electrical Engineering School (1994), China University of Mining & Technology, Xuzhou, Jiangsu. Now she is full professor of Automation Department, China University of Mining & Technology. The main research direction: evolutionary computation, machine learning, network control system, the multi-agent technology and intelligent control theory and application.

Haiqun Yang. He received his B.E in China University of Geosciences (2012), Now he is a M.Sc. candidate in Information and Electrical Engineering School, China University of Mining & Technology, Xuzhou, Jiangsu. His major fields of study are image processing.

Shuming Jiang. Now he is a associate professor in Shandong Academy of Sciences, Jinan China. His current research interests include different aspects of Image Processing and Pattern Recognition.

