Advances in Intelligent Systems Research, volume 147

International Conference on Network, Communication, Computer Engineering (NCCE 2018)

Chaos Encryption Algorithm Based on Kent Mapping and AES Combination

Yong Wang, Shuo Chen [a)], Ying Wang

School of computers, Guangdong University of Technology, Guangzhou 510003, China

[a)] Corresponding author: 386817263@qq.com

Abstract. Aiming at the application of a class of image encryption algorithm based on chaotic system, a chaotic image encryption algorithm based on Kent mapping and AES (Advanced Encryption Standard) encryption algorithm is proposed. Firstly, an initial condition is defined and a parameter related to plaintext pixel value is extracted as a key. The chaotic sequence generated by Kent is used as the target key of the AES encryption algorithm. Then, the plaintext and the target key are XOR-processed Finally, the target key is substituted into the algorithm to perform several AES encryption algorithms to obtain the ciphertext. The experimental results show that the proposed algorithm can resist the differential attacks and analyze the statistical characteristics well, but also can effectively resist the plaintext attack and the encryption effect is better.

Key words: chaos system; image encryption; Kent mapping; AES encryption algorithm;

INTRODUCTION

The network has brought a lot of conveniences to people's work and life, but also the network information security problems are followed one after another, therefore the digital image encryption technology has become a hot spot in the field of information security nowadays. This paper uses AES combined with chaotic sequence method for image encryption. Advanced Encryption Standard has been multi-analyzed and widely used all over the world [1]. The algorithm is a bit handy, efficient and consistently good performance across different hardware and software environments. However, the key given by the AES algorithm is that the algorithm has poor resistance in the face of exhaustive attacks. In order to improve this feature, this paper introduces a chaotic system. In recent years, the image encryption algorithm based on chaos is the mainstream of image encryption. Kent mapping is a chaotic system with good performance, so this paper uses it to generate chaotic sequences.

In [2], Logistic mapping is used to generate chaotic sequence as the initial key of AES encryption. It not only retains the excellent characteristics of AES as a conventional encryption algorithm, but also facilitates the generation and management of keys. As pointed out in [3], Kent mapping is logically isomorphic to Logistic mapping. Kent mapping can also be used to generate stochastic new solutions in stochastic optimization algorithms. Kent mapping has a better uniformity than Logistic Mapping Ergodicity, the iterative process is also suitable for programmatic operation, we can statistically describe the Kent mapping Logistic mapping good ergodic. In [4], a chaotic system is used to implement chaos stream cipher as the AES initial key to encrypt AES algorithm, which makes full use of the advantages of the two encryption systems and improves the security of the algorithm.

In view of the advantages and disadvantages of the above algorithm, the invariance of the initial key of the AES encryption algorithm is analyzed. Each wheel key generated during the key expansion is also invariant, and the S box produced by the encryption algorithm is fixed, It is easy to be cracked. The chaotic sequence generated by Kent mapping can be used as the target key to encrypt the AES algorithm. This will greatly enhance the security of the AES algorithm. However, the S-box transform and shift in the AES encryption algorithm Bit box confusion has a very perfect encryption, the combination of the two can greatly improve the image encryption security [5].

ALGORITHM PRINCIPLE

Kent Mapping

Kent mapping is a chaotic system with good performance. Therefore, this paper uses it to generate chaotic sequence, and its mapping is as follows:

$$F(x)=\begin{cases} x/a, x\in(0,a] \\ (1-x)/(1-a), x\in(a,1] \end{cases} \tag{1}$$

Where a is a control parameter of the chaotic system. When $x \in (0,1)$, $a \in (0,1)$, Equation (1) has a positive Lyapunov exponent, so that Kent is in a chaotic state. Therefore, a sequence generated by the initial condition in Kent's map is non-periodic and does not converge Pseudo-random sequence. The Kent mapping is very sensitive to the initial conditions, and when the initial values change slightly, two completely different pseudo-random sequences will be generated [6,7].

AES Encryption Algorithm

The paper uses multiple round robin AES encryption method, each round of cycle is divided into four stages: (1) S box transformation: each value of the first 4 binary as the line coordinates, the last 4 binary as column coordinates query S box (3) Column obfuscation operation: replacing a new column obtained by XORing a set of matrices with the ciphertext; (4) Round key operation: ciphertext and key XOR.

Encryption and Decryption Principle

In order to facilitate the discussion of the algorithm, A is used to represent a grayscale image of size 256×256, t is the number of iterations of the chaotic sequence generated by the chaotic system, avg is the average of the pixels, and sum is used as the value of all the pixels in the image Sum, s as the number of AES cycles, encryption steps are as follows:

The plaintext image A is converted into a matrix L of size 256×256 in order of row priority, with values in the range [0,255].

Summing all the pixel values of the plaintext image to obtain the sum sum of the pixel values, obtaining the pixel average avg from the formula (2), and determining the Kent control parameter a from equation (3) Determine the number of iterations chaos system t.

$$\mathrm{avg} = sum/(m \times n) \tag{2}$$

$$a = \frac{\mathrm{mod}(sum \times 100, m \times n)}{(m \times n)} \tag{3}$$

$$t = m + n + \mathrm{mod}(avg \times 10^8, m + n) \tag{4}$$

Set the initial value of Kent mapping to x_0, and substitute a in x_0 and the above step into (1), and then use Kent mapping to iterate t times to remove the influence of transient effect, extract t times and later Of the chaotic data and the chaotic data is rounded and divided by 256 to obtain the value obtained as the target key.

Extract the t to the t+256×256 target key Generate a matrix and clear the text for an exclusive OR bit processing, the target key is 0-256, the binary digit does not exceed 8 bits, and the plain text XOR processing will not Exceeded 8-bit binary range.

Transforms the S-box, extracts the matrix of 256 data at the beginning of t+256×256×(s+1) into 16×16 matrix, numbers the matrix in ascending order of 0-255, and uses the number as the original value of the target key of the segment As the S box, the first four bits of each element value of the ciphertext are extracted as the number of rows of the S box, the last four bits are used as the number of columns of the S box, and the value of the element is replaced with the value of the corresponding position of the S box.

Perform AES shift and column blending.

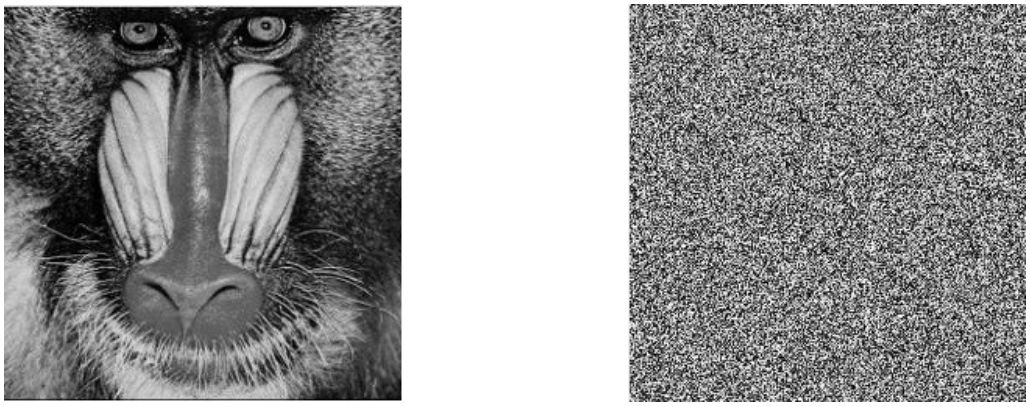
Perform round key addition operation of the AES algorithm, and extract the target key of the data starting t+256×256×s from 256×256 and the ciphertext for XOR operation.

loop (2) - (7) s times, and the matrix into images, to complete the encryption operation.

The decryption operation is the reverse of the encryption operation.

SIMULATION RESULTS

In this paper, the gray image of Lena with size 256×256 is used as plaintext, but it is also suitable for image encryption of other sizes. The initial key in the experiment is $x_0 = 0.3141592650$ in the Kent chaotic system, in which Kent's control parameter a is determined by the image itself, and the experiment can obtain the encryption effect as shown in FIG. 1.

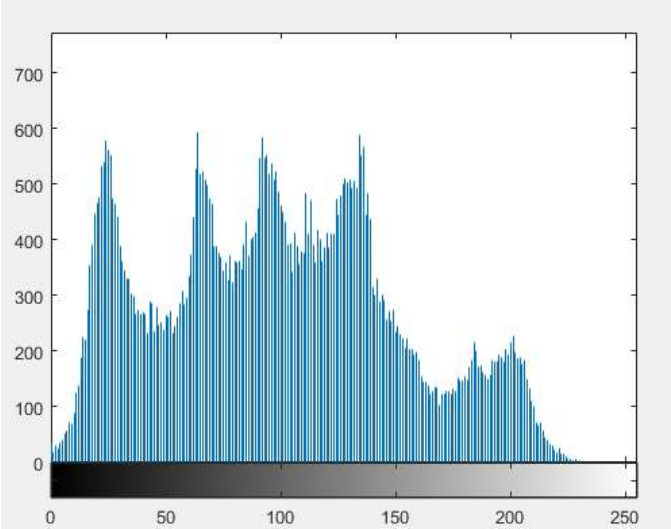


(a)Clear text images (b)Encrypt the image

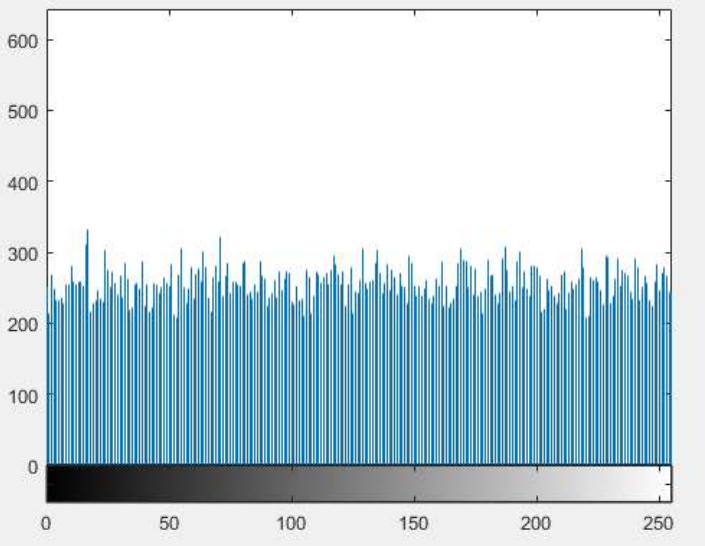
FIGURE 1. Plain text images and encrypted images

Histogram Analysis

The histogram of the gray image is the frequency of each gray level pixel in an image. The grayscale is the horizontal axis and the vertical axis is the gray level. The relationship between the gray frequency and the gray frequency is plotted. The important features Is a reflection of the image gray distribution. From the histogram before and after the encryption to observe, as shown in Fig.2, the plaintext prior to the encryption of the histogram is not uniform, clearly exposing the distribution of image pixel values, and the ciphertext encrypted image gray the histogram is uniform, well-hidden plaintext image information.



(a) Plaintext of plaintext



(b)Ciphertext grayscale image histogram

FIGURE 2. Plaintext and ciphertext gray histogram

Algorithm Statistical Analysis

Each point is selected horizontally, vertically and diagonally to calculate their respective correlation coefficients. From Table 1, the correlation coefficient of the plaintext image is close to 1, indicating that the adjacent pixels of the plaintext image are highly correlated. The adjacent elements of the encrypted image basically have no relationship that is to achieve a better encryption effect, making cipher text has a good anti-statistical analysis of the ability to attack.

TABLE 1. Before and after image encryption adjacent pixels correlation coefficient

Pixel Direction	Horizontal Direction	Vertical Direction	Diagonal Direction
The Original image	0.9650	0.8951	0.9232
Encrypt the Image	-0.0032	-0.0518	-0.0469

CONCLUSION

Aiming at some problems existing in chaotic image encryption algorithms, a new image encryption algorithm is proposed in this paper. The algorithm has the following two main features: First, the use of plaintext parameters as the chaotic sequence value location, with the plaintext image can be different and effectively resist plaintext (ciphertext) image attacks; Second: the algorithm introduced Kent maps the generated hyperchaotic sequences as the target key of the AES algorithm. Combining the advantages of the two algorithms, Kent solves the shortcomings of the target key space of the AES encryption algorithm and greatly enhances the encryption cracking difficulty. Experiments show that this algorithm not only has better encryption effect, but also has higher security.

ACKNOWLEDGMENTS

First of all, we want to thank Professor Wang. The teacher gave careful guidance in the selection of the thesis, the determination of the research plan and the specific implementation process. His rigorous attitude and systematic research ideas have given me a lifetime benefit. At the same time, I would also like to thank all the teachers who have given me great care and support during my studies as well as my classmates and friends who care about me.

REFERENCES

1. Computer Engineering and Science, 2012,34 (05): 1-6. Zhang Xiaoqiang, Wang Mengmeng, Zhu Guiliang. Recent Advances in Image Encryption Algorithms [J].
2. Xiao Huijuan, Qiu Shusheng, Deng Chengliang. Image Encryption Scheme Based on Chaos Mapping and AES Algorithm [J]. Computer Engineering, 2007 (23): 154-155 + 172.
3. Liu Jianjun,Shi Dingyuan, Wu Guoning.A Hybrid Chaos Optimization Algorithm Based on Kent Mapping[J].Computer Engineering and Design,2015,36(06):1498-1503.
4. Wang Yong, Li Jinyang, Wang Ying. Hyperfield neural network and AES combined with hyperchaotic image encryption algorithm [J]. Computer Engineering and Applications [2018-03-06].
5. Wang Yong, Zhu Guang, Wang Ying. Chaophobal networks and improved AES based hyperchaotic image encryption scheme [J]. Computer Engineering and Applications: 1-9 [2018-03-06].
6. Xie Guo-Bo, Wang Tian.A new chaotic image encryption algorithm based on bit scrambling [J]. Microelectronics and Computers, 2016,33 (7): 28-32.
7. XIE Guo-Bo, WANG Tian. Chaotic Image Encryption Algorithm Based on Pixel Scramble and Bit Replacement [J]. Microelectronics and Computers, 2016,33 (3): 80-85.