Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2015, 7(3):506-510

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

The application study of image processing in control system

Tong Chun-ya[1], Shao Shi-wei[2,3*], Zhong Qiu-bo[1*],Yu Hua[1], Shi Jing-jing[1], He Ke-jia[1] and Zhang Hong-mei[1]

[1]School of Electronic and Information Engineering, Ningbo University of Technology, China
[2]School of Resource and Environmental Sciences, Wuhan University, No.129, Luoyu Road, Wuhan, China
[3]Wuhan Land Resource and Urban Planning Information Centre, No.13, Sanyang Road, Wuhan, China

---

ABSTRACT

Image measure technology and automatic control theory are combined to design and realize an encryption control system based on image processing. The equipment of video capture and image processing technology are used to replace traditional image encryption methods. The image processing result is used as S-DES image encryption algorithm to control experimental system in real time. The simulated results show that the proposed algorithm is a good spatial design algorithm for chaotic keys, and possesses a large space of keys, fairly well encryption effect and excellent security to statistic analyses and different attacks.

Key words: Methane detection; Maintenance-free; Auto-calibration; Visualized calibration; WSN

INTRODUCTION

Image processing has been applied in many fields. In control system, image encryption is one of applications. With the rapid development of the internet and the multimedia technology, digital image is becoming important carrier of information communion for people. With the advance of information security requirement, the encryption technology of digital image is applied widely to multimedia communications. Conventional encryption arithmetic (e.g. DES) has many disadvantages, such as the structure complexity, the secret key singleness and the encryption speed slowly, and it is difficult to satisfy the encryption requirement of the image that has lots of data. So using the conventional encryption solely is not enough. Chaotic mapping can be applied to image encryption, because it has the sensitivity of initial value and the randomness [1-4]. The method which adopting combined conventional encryption technology with the chaotic mapping can overcome the single conventional encryption's disadvantage effectively. The pixels' values in original image can be changed ultimately via encrypting, in order to realize the aim of encryption.

For advancing the quality of encryption effectively, the method of position scrambling can be used before encrypting. The classical algorithms are Arnold cat map[5], affine transformation, magic square transformation, and knight-tour transformation. etc. Through these transformations, it can realize the change of the image pixels' position, and by keeping secret the parameters and the iteration times to reach the aim of encryption. A method which based on Arnold cat map and S-DES is proposed in this paper, by using the particular character of Logistic chaotic map, the key numbers of S-DES are increased and the key can be changed in real-time. The experiment result shows that the method realizes the image encryption and decryption effectively, it has well security and fast operation speed.

S-DES ENCRYPTION ALGORITHM

Cat mapping is from Arnold, and it is named because of demonstrating it with a cat's face usually, the expression of Arnold cat map is shown as Eq.1.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(N) \qquad (1)$$

Where（x_n, y_n）is pixels position in an N×N image;（x_{n+1}, y_{n+1}）is the transformed position after cat map; a and b are the system parameters and must be the plus integers. The determinant value is 1, so cat map is a map which keeping area (no attractor). At the same time, the cat map is one-to-one mapping, each point in matrix can be transformed to another point uniquely. Cat map has two typical factors, which bring chaotic movement: tension (multiply matrix in order to enlarge x, y) and fold (taking mod in order to bring x, y in unit matrix). In fact, cat map is a chaotic map.

Image position can be scrambled via the iteration of cat map, consequently realizing the image encryption. With the difference of the iteration times, the relevant result of scrambling is also different. For a 256×256 gray image, it is hard to find out the trace of original image after iterating 30 times, reaching the effect of scrambling; the image after iterating 64 times is the same as the original image, so cat map has the periodicity [6]. With the differences of the parameter and the image's size, the periodicity is different. Image can be scrambled via keeping the value of a, b secret, but the periodicity will bring some insecure factors, so applying cat map solely can not meet the demands of encryption; and cat map only transforms the original image's position, however the pixels' values have not been changed. The original image can be recovered via the method of exhaustion, so on the base of scrambling, it is necessary to modify the pixels' values to realize double encryption.

The data encryption standard DES which is designed by U.S. National Bureau of Standard is a well-known block cipher, and it adopts Feistel structure to iterate [7]. But the complex structure and slow speed aren't satisfied with the encryption requirement of images, which have large data. Although the key quantities achieve 56 bits, using the only key in an encryption is not safe obviously. Professor Edward Schaefer in university of Santa Clara proposed S-DES, namely the simplified DES algorithm, also adopts Feistel structure. The plaintext and cryptograph block are both 8 bits, and it is consistent with the bits, which the value of pixel has, its structure is shown as Fig.1. Comparing with DES, the structure of S-DES is simple and the execution speed is fast. But the security will be reduced. Therefore depending on S-DES merely cannot meet the encryption requirement. Combining the chaotic map with S-DES system can enhance the security of system by using the characteristic of sensibility of original value and randomness in chaotic map.

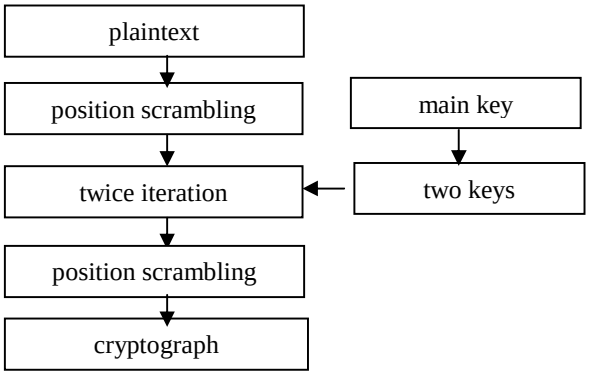


Fig.1 S-DES structure

The chaos is a process of definite pseudo-random sequence produced by nonlinear dynamics system. It's non-periodic, non-astringe and sensitive to the original value. Logistic map is a typical chaotic map and its expression is showed as Eq.2.

$$X_{n+1} = bX_n(1 - X_n) \qquad (2)$$

Where $X_n \in [0, 1]$, when the value of parameter b is between (3.569, 4), the system has the chaotic characteristics, and then the sequence produced by Logistic map is random and sensitive to original value. It is possible to realize the position scrambling of S-DES structure by collating the sequence of the chaotic map. Operating the sequence can produce the enough long keys, and it achieves the purpose that the information can be encrypted each time. It is obvious that combing the chaotic map with the S-DES encryption system can enhance the random, and also increase the key quantity of system further.

THE S-DES STRUCTURE BASED ON LOGISTIC MAP

The encryption structure which combined the Logistic map with S-DES system is showed as Fig.2.

Where the value of pixel is the value of gray image, its range is between (0~255); it still needs two iteration; the sequence produced by Logistic map is used for the S-DES key to ensure the different key in every encryption. The concrete encryption steps are as follows:

Presents the parameter value b of Logistic map and initial value x0. Under the double precision value circumstance, it makes the map iterate several times to produce a sequence（X1, X2, X3,……）. The specific times is decided by the image size.

Inputting an image, and changing the pixel value of each point to 8 bit binary; Taking the first 8 numbers of the sequence, and collating the 8 numbers according to the size, then replacing 8 numbers according to the corresponding positions. Namely completing the operation of positions replacement one.

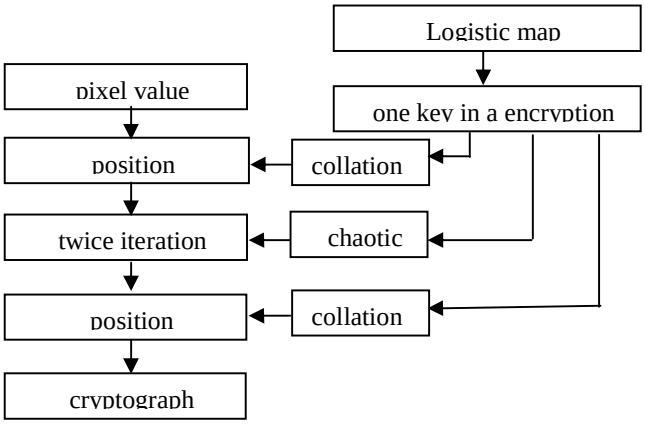


Fig.2 The encryption structure of Logistic map and S-DES

Taking subsequent 16 values in the sequence respectively. Putting the last bit of each value together, and then it will become two keys which both have 8 bits. Using it to iterate twice in S-DES.

Taking eight bits of the sequence to use in the position replacement two, and the method is consistent with the step 2. Then it completes image encryption of one point.

Applying the sequence produced by step 1, and repeating the step 2~4 until all points of image were encrypted.

Making the sequence produced by chaotic map as the source of collating and the iterative keys are the characteristic using sensitivity of initial value and randomness in chaotic map. The method overcomes the disadvantage that key is difficult to manage in the traditional method, and makes the key change in real-time. Therefore it brings great challenge to the attacker.

EXPERIMENTAL SECTION

The original gray image of 256×256 is shown as Fig.3.

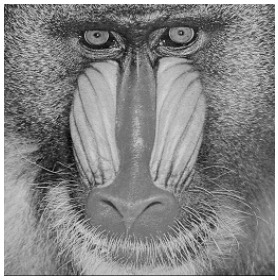
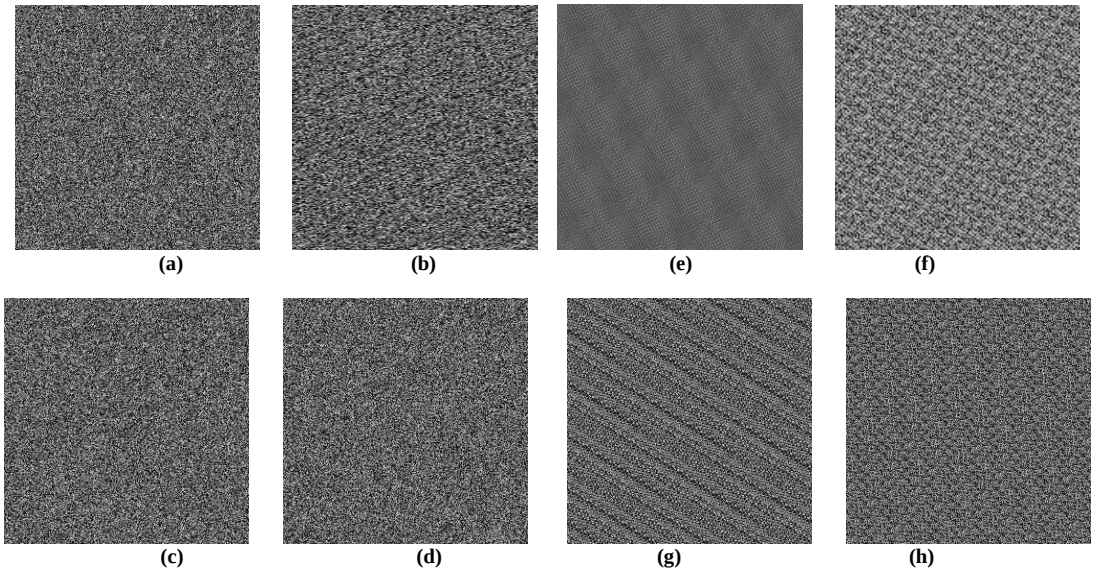


Fig.3 The original image

The initial values are a=1, b=1, x0=0.142, y0=0.258. When the iterative times are n1=n2=1, n1=n2=40, n1=n2=50, n1=n2=192, the corresponding results of encryption are shown as Fig.4(a)-(d). Results of the same image scrambled by using the traditional Arnold transformation are showed as Fig.4(e)-(h).



(a) **(b)** **(e)** **(f)**

(c) **(d)** **(g)** **(h)**

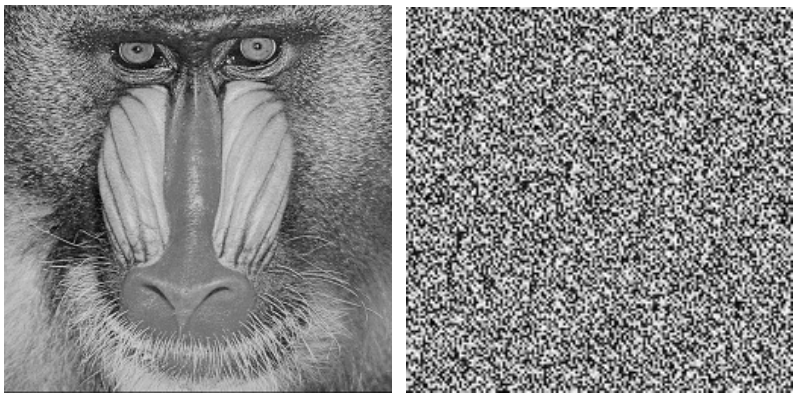
Fig.4 Comparative analysis of scrambling effect

The results of Fig.4 show that the encryption algorithm is better than the original Cat map. The effect is always better no matter iteration times.

The design of the algorithm is simple and effective, programming is also very easy to implement, and the speed of its implementation is quick too. In order to detect the time expense of algorithm, we carried many encryption and decryption experiments on different sizes of 8-bit and 24-bit BMP image. The hardware system used in the experiments is Pentium4 2.8G CPU, 2G DDR memory; the software system is the windows XP operation system, the MATLAB platform. In the experiment, for 256 × 256 BMP image which data size is192k, encryption cost approximately 0.026s and decryption cost approximately 0.037s. So the efficiency of the algorithm is quite high.

Set the parameter value of Logistic b=4, the initial value X0=0.8. Under double precision circumstance, it iterates 32 ×120 × 120= 460800 times. According to the steps of Fig.4, encrypting Fig.4(c) two times and its result. Then the pixel value and the position of the pixel both are changed, and realized the dual encryption The Logistic map and the S-DES are combined, which its safety is based on the sensitivity of the initial value. A small change of the initial value will cause the huge variety in the result. The image of Fig.5(a) is the image of the exact decryption, and

Fig.5(b) is the decrypted image which its initial value of Logistic map X0=0.80000001. From these images, we can see puny change cannot recovery the original image, so the safety of encryption system gains the further enhancement.



(a) (b)

Fig.5 The decrypted image

Analyzing from the quantities of the key, the parameters of the Arnold cat and the number of iteration may be regarded as the key, and the parameter and the initial value of the Logistic map also can be regarded as the key, then the total quantities of the key can reach at least 1017 so that the exhaustion method is very difficult.

Analyzing from the relativity, the relativity of the adjacent pixel in original image is bigger. But the relativity through position scrambling and pixel changing hardly exists, so it is very difficult to attack by using statistics method.

CONCLUSION

An encryption method based on S-DES and chaotic map is proposed. Through applying the sensitivity of initial value and randomness in chaotic map, the system has larger key quantities and the key is real-time. Through the simulation analysis in MATLAB, the method has the quick computing speed because of its simplified DES structure, and has the ability of anti-statistics attack and exhaustion attack.

Acknowledgements

This material is based upon work funded by Zhejiang Provincial Department of education research project under Grant No.Y201327098, Natural Science Foundation of China under Grant No.61203360, Zhejiang Provincial Natural Science Foundation of China under Grant No.LQ12F03001, LQ12D01001, LY12F01002, Ningbo City Natural Science Foundation of China under Grant No.2012A610009, 2012A610043, State Key Laboratory of Robotics and System (HIT)Foundation of China under Grant No.SKLRS-2012-MS-06, China Postdoctoral Science Foundation under Grant No.2013M531022.

REFERENCES

[1] Joung-Youn Kim, Lee-Sup Kim, and Seung-Ho Hwang, *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 11, no. 4, pp. 475-484, **2001**.
[2] Scharinger J **1998** *J.Electron Imageing* 7 318-25
[3] Soong-Der Chen and A. R. Ramli, *IEEE Transactions* on, vol. 49, no. 4, pp. 1310-1319, **2003**.
[4] Lu J, Chen G R **2002** *J. Bifurcation and Chaos*.12 659-61.
[5] K. A. Panetta, E. J. Wharton, and S. S. Agaian, *IEEE Transactions on Systems, Man, and Cybernetics*, Part B: Cybernetics, vol. 38, no. 1, pp. 174-188, **2008**.
[6] Ni R R, Ruan Q Q and Cheng H D **2005** *J. Pattern Recognition* 38 357-68.
[7] Yoo S M, Kotturi D,Pan D W and Blizzard J **2005** *J. Microprocessors and Microsystems*. 29 317-26.