Image Encryption Based on Embedded ARM System and Lorenz Chaotic Algorithm

Qi ZHANG[1], Hao-ran SUN[2,] and Qun DING[3,*]

Electronic Engineering College, Heilongjian-g University

Xuefu Road 74,Harbin, China

ljittss@163.com,qunding@aliyun.com

Keywords: Embedded ARM, Lorenz, QT GUI, Image encryption.

Abstract. This paper proposed an image encryption method based on embedded ARM system and chaos algorithm. It can ensure the security and confidentiality of the image information on the embedded device. It used the three-dimensional Lorenz chaotic system encryption algorithm, due to the special nature of the chaotic system and the characteristics of the suitable method, it can ensure the reliability of the encryption algorithm. The algorithm part and the image processing part are realized on the embedded device, and the final result is the result of the image encryption and decryption through the embedded QT programming. Realize the combination of chaos encryption algorithm and image encryption on embedded devices. The results show that this method can ensure the image security on the embedded device.

Introduction.

With the rapid development of information technology, image as an important carrier of information gradually replace the text information, as it contains important private information in image information, so the security of the image transmission process should pay more and more attention. And a large number of embedded terminal devices, such as mobile phones, satellite, medical equipment, and a variety of handheld devices, the image security on these embedded devices is particularly important. These embedded ARM devices have a screen display function, and the display function is achieved by QT programming. Image encryption algorithm is numerous, and chaos is widely used in the field of information encryption because of its important and prominent cryptographic properties[1].In this paper, the image encryption is implemented on the embedded ARM device, the image encryption algorithm is Lorenz chaotic algorithm[2-3].

Firstly, the chaotic sequences generated by the three-dimensional Lorenz chaotic equations are used to encrypt and decrypt the image. The paper introduces some basic knowledge of digital image chaotic[4], due to the special nature of chaos can reach good effect of encryption, and the main features of this encryption algorithm is fast and easy to implement in embedded devices[5].Secondly it introduced an embedded operating system based on Qt interface, Qt/Embedded interface built on embedded system development environment based on hardware and software[6], and implement the Qt/Embedded interface ported to S3C2440 development board. Among them, including the Qt/Embedded installation and settings, embedded Linux operating system library file transfer, boot loader, Linux kernel, root file system and the corresponding application. Completion of the Qt interface based on the embedded ARM Linux development platform for debugging, transplantation. Verify the encryption and decryption algorithm in the S3C2440 development board, and achieve the image encryption and decryption. Development board experimental results show that digital image encryption is reliable, the future is bound to become a trend.

Principle and Properties of Lorenz Chaotic System

Lorenz Chaotic System Equation

Lorenz chaotic system is a continuous chaotic system[7], and its system equation is three dimensional differential equations as follows:

$$\begin{cases} \bar{x} = -10(x-y) \\ \bar{y} = -xz + 28x - y \\ \bar{z} = xy - 8z/3 \end{cases} \tag{1}$$

If we want to obtain a pseudo random sequence of chaos by Lorenz equation, first of all, we should discrete the continuous chaotic equations, here we use Euler method, it can transform the continuous equation into difference equations. Although the accuracy is not high enough, but the operation is simple and it has little effect on the nature of the final sequence. The discretization differential equations with Euler method is as follows:

$$\begin{cases} x_{n+1} = x_n + 10(y_n - x_n)h \\ y_{n+1} = y_n + (28x_n - y_n - x_n z_n)h \\ z_{n+1} = z_n + (x_n z_n - 8z_n/3)h \end{cases} \tag{2}$$

Discrete equations can produce discrete numerical values. These arrays into a discrete sequence, if you want to use these sequences for image encryption, you should quantify them, it is converted into a 0-1 two value sequence. Quantitative method is reserved for the last digit of these numbers, these numbers are approximate random, take the average value of these values as a quantitative standard, if it is greater than the number of the average, take ‘1’,else,take ‘0’.Finally we get the three-dimensional 0-1 two value sequence for image encryption.

Properties of Lorenz Chaotic System

The Lorenz chaotic system is adopted because of its good encryption property, which guarantees the realization of the encryption and the security of the encryption result.

Bounded Property: Chaos is bounded. Its motion trajectory is always confined to a certain region, which is called chaos attraction region. So the chaotic system is determined. It is suitable for encryption and decryption.

Random-like Property: The randomness generated within the system is called the random nature of the system[8].Although the whole system is determined, the trajectory of the system is chaotic and unpredictable, so the iterative result is a kind of random characteristic.

Initial Value Sensitivity: The initial value of chaotic system is changed slightly, will cause the difference of the trajectory is obvious, which showed the initial value of chaotic system is extremely sensitive, which is very important in the application of chaotic system in secure communication.

Positive Lyapunov Index: The initial value sensitivity of chaos is precisely because of its positive Lyapunov index[9], and Lyapunov index is one of the criteria to test whether the chaotic system is in the chaotic state. Chaotic systems have attractors[10]. The phase diagram of Lorenz chaotic system is shown in Figure 1:

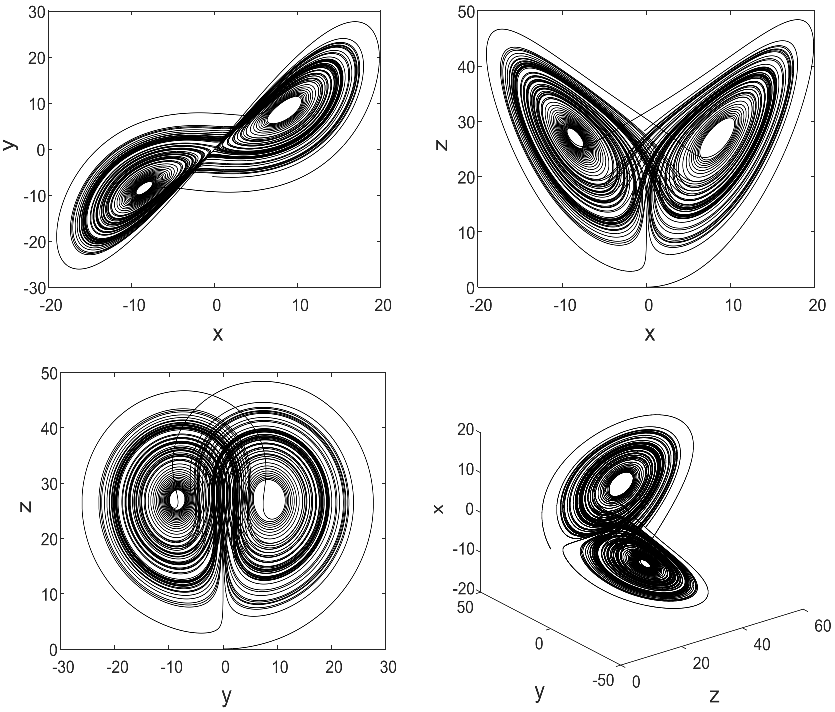


Figure 1.Lorenz chaotic attractors

Image Encryption Based on Lorenz Chaotic Algorithm

Firstly, we will deal with a digital image, and generate the gray matrix of the image. Color images will be generated R,G, B three color gray matrix values, and each matrix is converted into 0-1 two value matrix. The quantized 3D 0-1 pseudo-random sequence XOR respectively with these three matrices. And then synthesize it into a digital image, this is the encrypted image. Decryption is the XOR again, is the reverse process of encryption, the encryption flow chart as shown below:

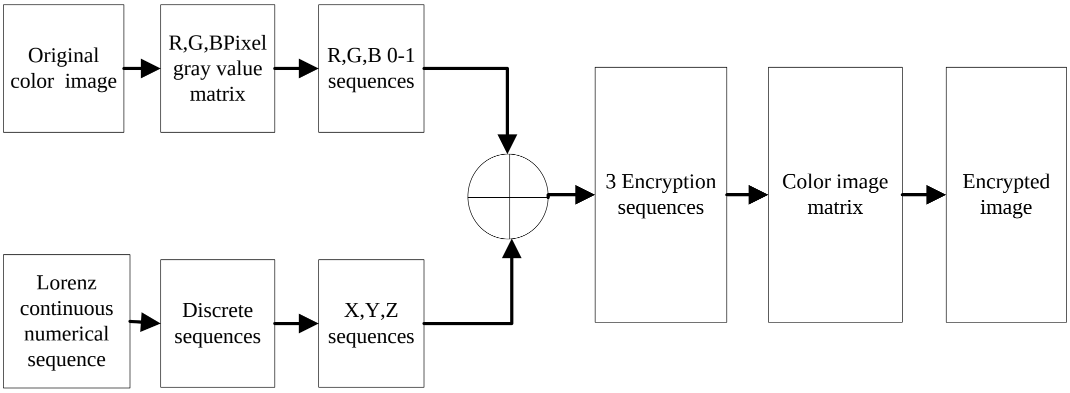
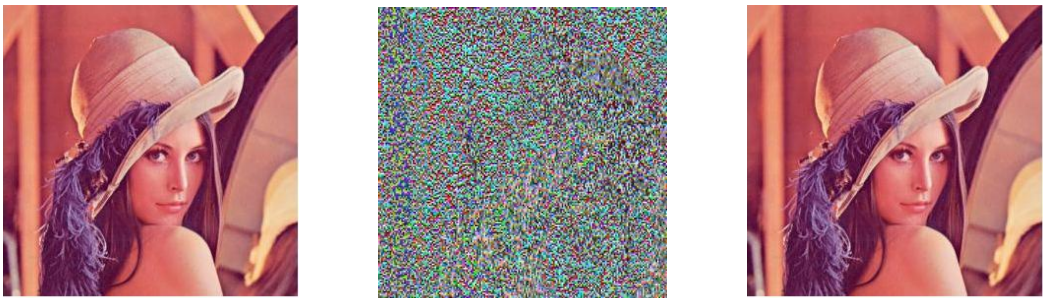


Figure 2.Encryption flow chart

In accordance with the above encryption process, the image is processed in the MATLAB, and to achieve the image encryption, the encryption and decryption results as shown Figure 3:



a).Original image b).Encrypted image c).Decrypted image

Figure 3.Encryption and decrypted results

Implementation of Image Encryption Based on Embedded ARM System

Firstly, we use the embedded development board with the Samsung Corp's ARM9 as the core chip of the S3C2440 architecture, with a color touch screen. Also equipped with NorFlash and NANDFlash as memory. The hardware architecture of the system is shown in figure 4:

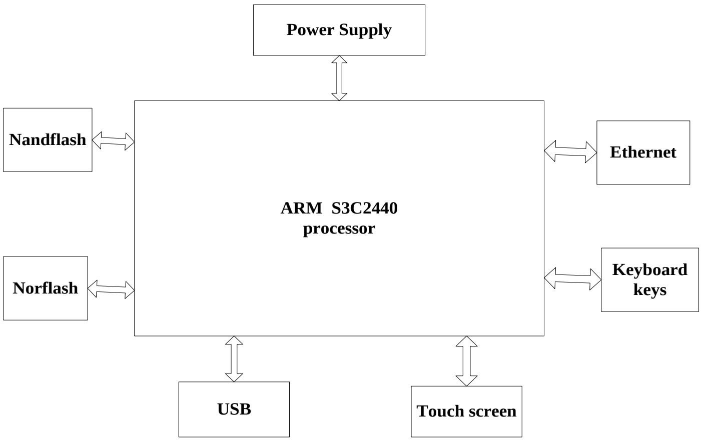
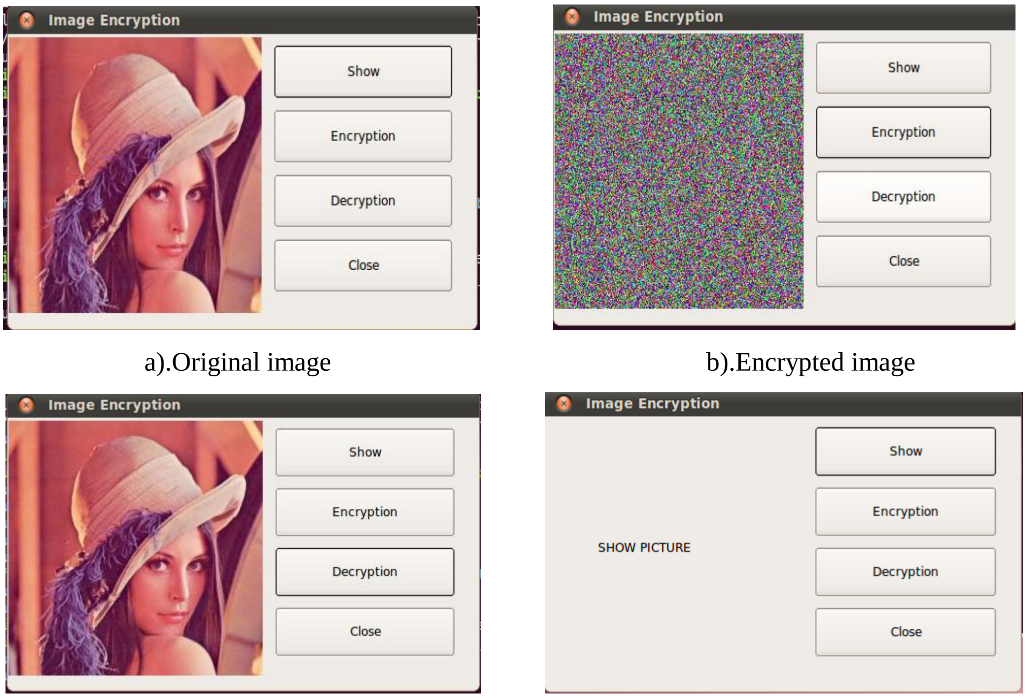


Figure 4.Hardware architecture diagram

If you want to achieve image encryption results on the embedded screen display, here we use QT programming technology. QT/Embedded system will be transplanted to the embedded development board, in which to achieve the encryption algorithm and image processing part of the Linux environment we use C language programming. In the Linux side of the PC environment, the first interface design of the program in the QT Creator environment, using multiple threads, an encryption button generates an interrupt. Call the encryption algorithm and the results of the encrypted image, and then displayed in the embedded screen, press the decryption button to achieve image decryption. In the PC side of the simulation encryption and encryption and decryption results as shown below:



a).Original image

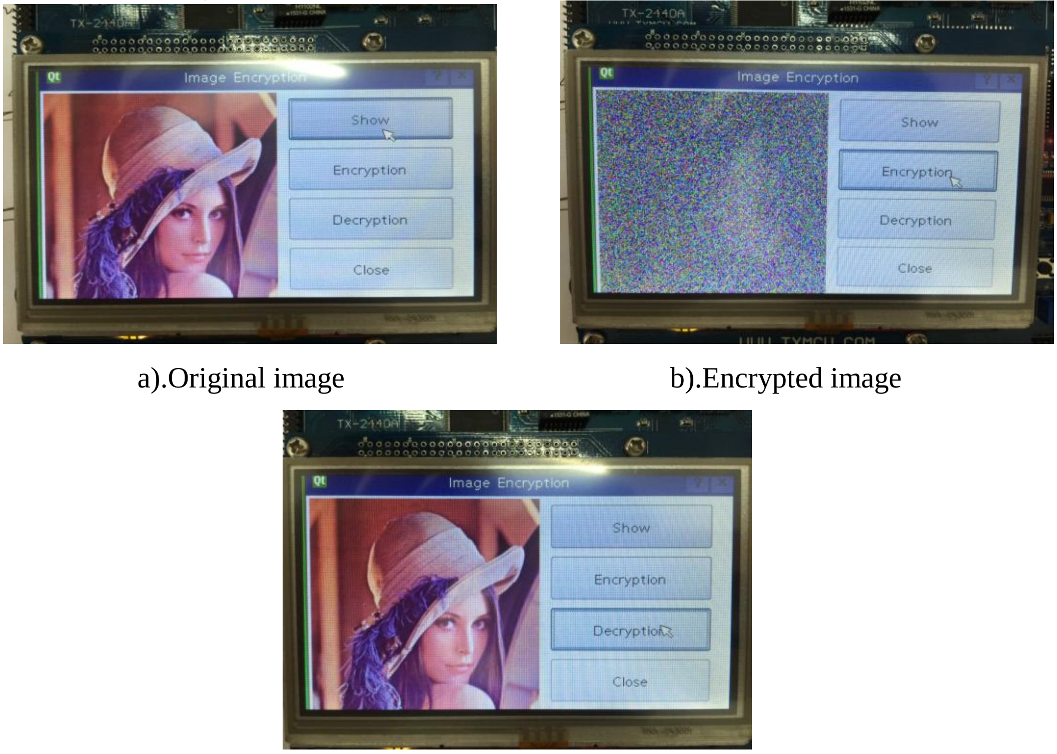
b).Encrypted image

c).Decrypted image

d). Initial interface

Figure 5.Simulation results

Then the QT and C programs are compiled to complete the embedded development board to achieve the results of image encryption and decryption of embedded devices. As shown in the figure below:



a).Original image

b).Encrypted image

c).Decrypted image

Figure 6. Embedded ARM implementation results

Summary

This paper presents an image encryption method based on embedded ARM, which makes it possible to encrypt the image on the embedded system, and promote the security of the information transfer of the embedded device. The encryption algorithm of Lorenz chaotic system used in this paper has high security and confidentiality, and is a kind of system which can be applied to cryptographic algorithms. After the simulation and the final system transplant, as well as the final results show that this method can achieve the encryption and good encryption effect. To effectively promote the progress of image encryption and security of embedded devices, the future development is limitless.

Acknowledgement

This paper is supported by Innovated Team Project in colleges and universities of Heilongjiang Province(No. 2012TD007) and Institutions of Higher Learning by the Specialized Research Fund for the Doctoral Degree (No.20132301110004).

References

[1] K. J. Persohn, R. J. Poxinelli. Analyzing Logistic Map Pseudorandom Number Genearators for Preiodicity Induced by Finite Precision Floating-Point Representation [J]. Chaos Solitons & Fractals, 2012,45(3):238-245.

[2] Pan J,Qi N,Xue B B,Ding Q 2012 .Filed Programmable Gate Array-Based Chaotic Encription Systerm Design and Hardware Realization of Cell Phone Short Message.. Acta Electronica Sinica. Vol.61,No.18,2012,180504.

[3] Y. C. Zhou, L. Bao, C. L. P Chen. Image Encryption Using a New Parametirc Switching Chaotic System[J]. Signal Processing, 2013,93(11):3039-3052

[4] J. H. Lu, G. R. Chen. A new chaotic attractor coined[J].Bifurc Chaos,2002,12 (3) :659-661.

[5] X. Y. Wang, Y. X. Xie. Cryptanalysis of a chaos based on cryptosystem with an embedded adaptive arithmetic coder[J] .Chin Phys. B. 2011, 20 (8) :80-85.

[6] M. Johnson, K. Hawick. Porting the Google Qt Mobile Operating System to Legacy Hardware[J]. OACTA Press,201,724-727.

[7] Y. S. Liu. A video conference solution and achievement based on chaotic encryption algorithms [J]. Computer & Digital Engineering,2011,39(1):104-109.

[8] G. C. Wu, D. Baleanu. Jacobian Matrix Algorithm for Lyapunov Exponents of the Discrete Fractional Maps[J]. Communications in Nonlinear Science and Numerical Simulation, 2015,22(1-3): 95-100.

[9] H. Yang, H. Xia. Histogram modification using gray-level co-occurrence matrix for image contrast enhancemen [J]. Image Processing, IET,2014:782 - 793

[10]J. H. Lu, G. R. Chen. A new chaotic attractor coined[J].Bifurc Chaos,2002,12 (3) :659-661.