# Digital Image Encryption Based On Advanced Encryption Standard(AES) Algorithm

Qi Zhang
Electronic Engineering College, Heilongjiang University
Harbin, China
ljittss@163.com

Qunding*
Electronic Engineering College, Heilongjiang University
Harbin,China
qunding@aliyun.com

*Abstract*—**With the rapid development of network and communication technology, digital image communication has become an important way of information transmission.Therefore, much more attention has been paid to the development of the digital image encryption technology.In this paper ,we propose a digital image encryption technology based on AES algorithm,and the algorithm implementation in MATLAB.Then,we perform digital image processing,obtain the date that can use the AES encryption algorithm,combine both approaches.Then,the digital image can be encrypted,and the algorithm is realized in MATLAB simulation.Through the comparison of the histogram analysis and the analysis of the key,the result has showed that the method can better realize the effect of encryption and decryption.**

***Digital image; encryption; AES; MATLAB***

## I. INTRODUCTION

Information technology today, driven by technological development, the transfer of image information security has become the most concern, since the transfer process, the contents of the information may be intercepted by others to attack, so it is easy to send the information they storm drain, people's privacy would be threatened. These are related to the computer network has a close relationship. Thanks to the Internet there are some loopholes in the transfer of information security is already perilous. Belgium cryptographers Joan Daemen and Vincent Rijmen proposed encryption standard AES algorithm [1].As the AES encryption algorithm is fast and has the advantages of strong ability to resist attacks [2]-[3],so this kind of algorithm is widely used in data encryption.Therefore, in this paper I design a kind of image encryption based on AES algorithm.Through the digital image processing to get the AES encryption standard data,encrypt the date in packet.Eventually put all the data together,reduction of encrypted image, achieve the desired encryption effect.

## II. AES ALGORITHM PRINCIPLE

### A. AES algorithm principles and summarize

Advanced Encryption Standard(AES),also called Rijndael encryption[4].It is the block encryption standard which set by the United States Federal Government lately.AES is used instead of DES.After several rounds of screening that AES was widely used [5].On November 26, 2011 the NIST released the latest encryption standard screening after five years,and took effect in May 2002.After four years of precipitation and the test,AES became one of the most popular symmetric encryption algorithm [6].

AES encryption system is symmetric in group,there are three kinds of key length in this way of encryption:128 bits,196 bits and 256 bits,packet size is all 128 bits,the algorithm has good flexibility.So it is widely used in the software and hardware.In the three key length of AES algorithm,the 128 bits key length is frequently used.When under the key length, 10 times of iterative computation in internal algorithm.In addition to the final round,each round consists of five parts:SubBytes, S-box,ShiftRows,MixColumns,AddRoundKey.

Exclusive between plaintext and key expansion blocks of [7].In AES,five date unit of measurement can be used:bits, bytes, characters, groups,states.Each round of AES consists of byte replace (SubBytes), the line displacement transformation(ShiftRows),mixed column transformation (MixColumns) key transformation (AddRoundKey) and so on.From one phase to another phase of the data packet transform,in the whole encryption start and end stage,the concept of AES using data grouping.AES algorithm design should meet three criteria:

(1) Can resist all known attacks.

(2) Fast and coding compaction.

(3) Simple in design.

Around this kind of design thought,the data packet is prominent in AES algorithm and the key length is variable.The iteration round of number is controlled by the key and the block length. Process of AES Encryption and Decryption is shown as Fig.1.

The left and right of the figure respectively are: encryption algorithm and decryption algorithm,the middle is the key expansion algorithm.The encryption algorithm is composed of N round of iterations,each round has four different process,byte replace (SunBytes),the line displacement transformation (ShiftRows), mixed column transformation(MixColumns),key transformation(AddRoundKey).The final round is slightly different,it has not mixed column transformation.The decryption algorithm is the reverse of encryption algorithm[9],but the keys with the same,inverse byte

978-1-4673-7723-2/15 $31.00 © 2015 IEEE
DOI 10.1109/IMCCC.2015.261

substitution (InvSubBytes), retrograde displacement transform (InvShiftRows), inverse mixed column transform (InvMixColumns).

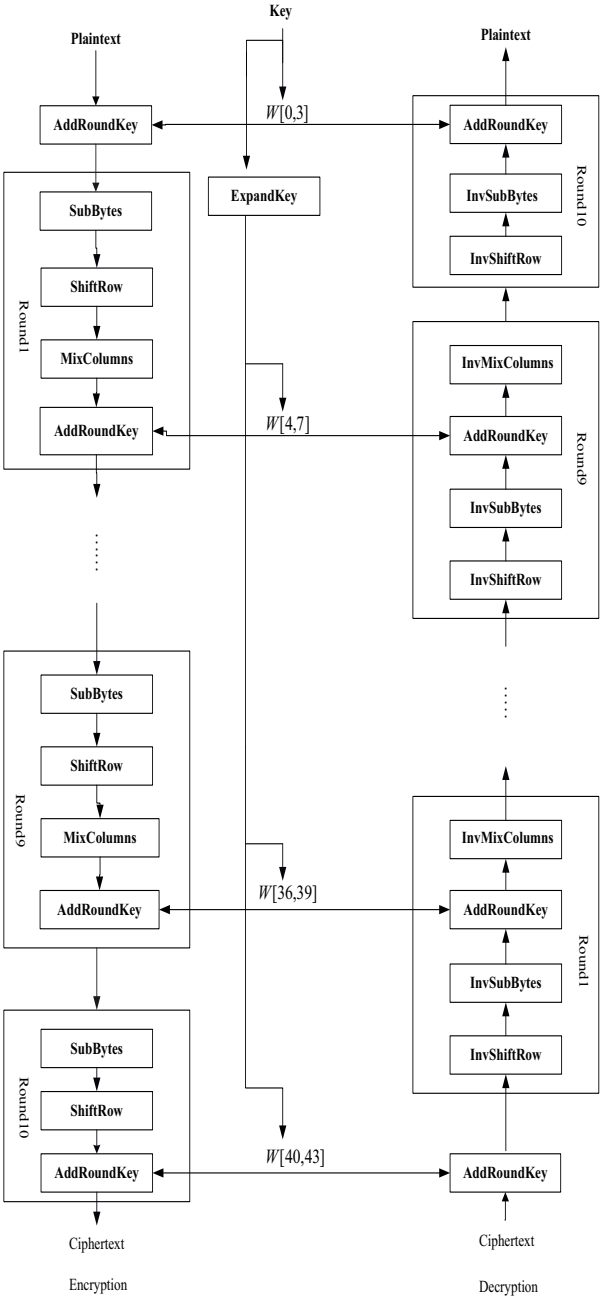



Figure 1. Process of AES Encryption and Decryption

## B. *The process of AES encryption on MATLAB*

This paper designs the process of AES encryption and decryption algorithm on MATLAB.Respectively defined S-box function, byte replace function and displacement function, mixed column transformation function and the key transformation function.At the same time,design their inverse transformation,then the decryption process is obtained.Call the defined function respectively,compose the AES encryption program,AES-demo.Below is the main program of AES-demo.This program used 32 hexadecimal number as plain text input(128 bits binary number).

```
[s_box, inv_s_box, w, poly_mat, inv_poly_mat] = aes_init;
plaintext_hex = {'32' '43' 'f6' 'a8' '88' '5a' '30' '8d' ...
                 '31' '31' '98' 'a2' 'e0' '37' '07' '34'};
plaintext = hex2dec (plaintext_hex);
ciphertext = cipher (plaintext, w, s_box, poly_mat, 1);
re_plaintext=inv_cipher(ciphertext,w,inv_s_box, inv_poly_mat, 1);
```

Plaintext:32,43,f6,a8,88,5a,30,8d,31,31,98,a2,e0,37,07,34

Key:00,04,08,0c,01,05,09,0d,02,06,0a,0e,03,07,0b,0f

Ciphertext:89,05,81,e2,ed,ca,35,1c,5e,76,08,40,6a,33,5f,bd

The initial situation of the running program is showed as Fig.2.

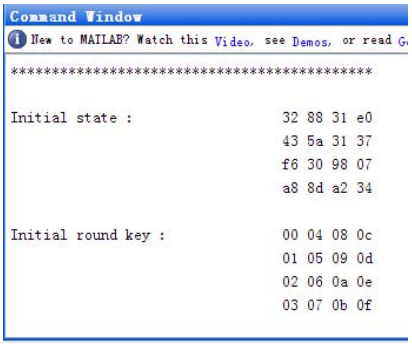



Figure 2. AES encryption plaintext and initial key

The results of AES encryption algorithm after the program is showed as Fig.3.

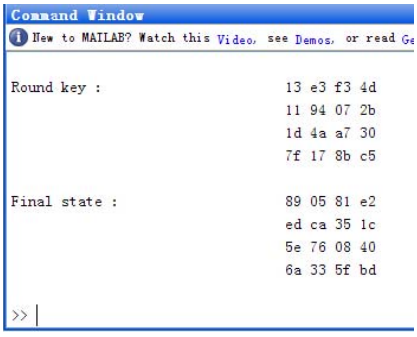



Figure 3. The result of AES encryption result and round keys

## III. DIGITAL IMAGE ENCRYPTION BASED ON AES ALGORITHM

### A. *Principle of image encryption based on AES algorithm and MATLAB simulation*

When encrypt the digital image based on the AES algorithm,first of all, we can convert a digital image into a binary matrix[8].The elements of the matrix in rows and columns,they are the coordinates of the point that the image has shown on the screen.The value of the elements are the gray levels of pixels(Usually 256 grades, from 0 to 255).

Because the state matrix of AES algorithm is based on a unit of 4×4 matrix that each element contains 8 bits.The value of the matrix element is between 0 to 255.It is usually coincide with the gray level of the image.Therefore, for a digital image,we can get a matrix after it's digitization.To deal with this matrix in block based on the AES algorithm.Starting at the upper left of the image,each 4×4 matrix in block encrypts by AES encryption algorithm,then make all the block together.Then you can get a matrix which number is totally different from the original numerical matrix. Consequently we changed the original image pixel gray value,to achieve the effect of encryption.Decryption process is the inverse of the encryption process,so we do not talk here.The process of image encryption based on AES is shown as Fig.4.

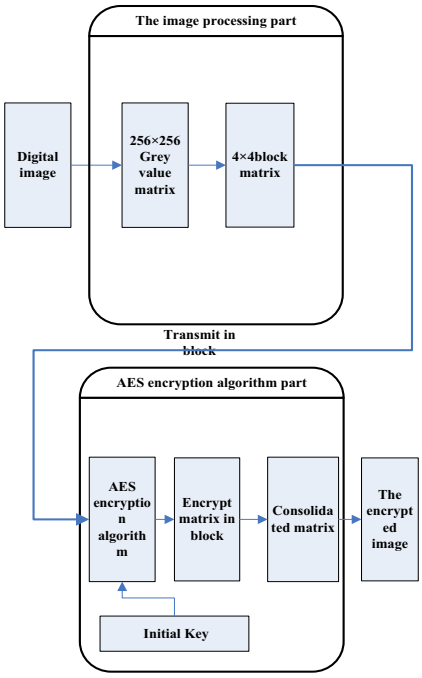



Figure.7. The process of image encryption based on AES

The specific process of AES algorithm of digital image encryption.First of all, a picture of a digital image gray value matrix is given,This we choose 256 ×256 standard Lena image,then we can get the gray value matrix.The matrix can be divided into 4×4 matrix for each unit of 8 bits, set an initial key before encryption,it's digits should be the same as the plain text of the AES encryption algorithm.Then use an AES encryption algorithm for each matrix,put all the new matrix together,it is the encryption matrix,then we can transform this matrix into a gray digital image,this image is the final encrypted image.We can deal with the digital image based on AES encryption algorithm on MATLAB,then get the original image and encrypted image,and the image is shown as Fig.5. and Fig.6.

Figure 5. The original image

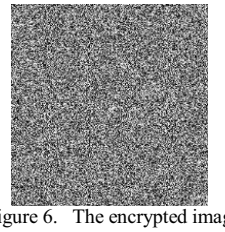


Figure 6. The encrypted image

After the image has been encrypted,we can see clearly that the we could not get any information of the original image.From this we can see the AES encryption algorithm can achieve the result of image encryption.Here we also do image decryption through the MATLAB,then we can see the image after decryption baaed on AES decryption algorithm which are shown as Fig.7. and Fig.8.

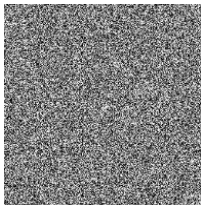


Figure 7. The encrypted image

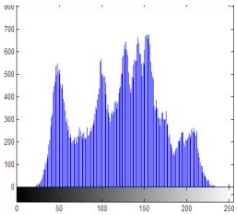
Figure 8. The decrypted image

We can find out that the decrypted image is nearly the same as the original image.Therefore we can see the decryption with AES is well.It can also prove the maneuverability of AES algorithm for image encryption.

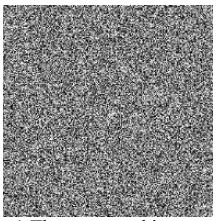
### B. *UnitsThe analysis of the result of decryption*

The general feature of the image can be described through gray histogram of the image[9],that is the number of occurrences of different pixel values.If a image with a low contrast,then the histogram is narrow and focused on the middle of the gray scale.If the pixel of an image occupies all possible gray scale and it is uniform distribution,then the image has high contrast and various gray color.Thus it can analyze the effect of image encryption through the contrast of the digital image histogram.The analysis of the contrast of the histogram of the original image and the encrypted image are shown as Fig.9.

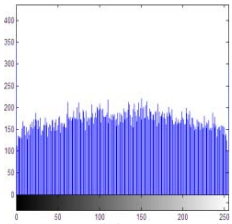
a）The original image



b) Histogram of the original image



c) The encrypted image



d)Histogram of the encrypted image

Figure 9. Histogram analysis of AES image encryption

From the histogram we can see that there is obvious change between the encrypted image histogram and the original image histogram.There are great changes from the distribution of pixels and the pixels.And the histogram pixel values of encrypted image are more evenly distributed.Then the encrypted image approximation for a picture of a random noise image.From this result we can see that the AES algorithm has good effect for image encryption.It also suggests that this kind of algorithm had a high security.In the process of the image transmission it will be not susceptible to tampering or eavesdropping.

### *C. The text of decryption and key sensitivity*

A good encryption algorithm should be sensitive to plaintext,and also be sensitive to the key[10].First of all, we know that the key of AES algorithm has the same length with the plaintext,they all have 128 bits.Then the key has128 times the power of 2 possibilities,It shows that this key can resist brute force attack.In order to test the sensitivity of the key, used respectively:

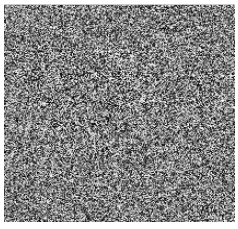
Correct key:

I={00,04,08,0c,01,05,09,0d,02,06,0a,0e,03,07,0b,0f}

Wrong key:

P ={01,04,08,0c,01,05,09,0d,02,06,0a,0e,03,07,0b,0f}

We can see that there is only 1 bit of difference between the correct key and the wrong keys.Respectively using the two key to decrypt the image,the result are shown as Fig.10.



a)The decrypted image with correct ke b)The decrypted image with wrong key

Figure 10. Test of key sensitivity

The results show that even if we use the wrong key with a litte difference with the correct key,at the time of decryption.There is a big difference between the original image and encrypted image,that is the wrong image, it has been unable to restore the original image,lead to complete failure to decryption.So this AES encryption algorithm is sensitive to plaintext.

## IV. CONCLUSION

This paper puts forward the method that use the AES algorithm with the key control to encrypt the image.This method incorporates a variety of characteristics,and with simple design.As the MATLAB has powerful numerical calculation function,especially for arrays and matrix calculations,and the infrastructure of the AES algorithm uses the matrix as the basic unit.So to implement the image encryption based on AES algorithm in the MATLAB environment is easy.From the above experimental results and analysis,coupled with the histogram and key sensitivity analysis,this method can achieve very good effect on image encryption.And the decryption essence has the same structure with the encryption,so it can easily restore the original image.Due to the AES algorithm is easy to implement in software and hardware,it has laid a good foundation for subsequent image encryption in the transmission encryption on software and hardware.So we have reason to believe that use this method to encrypt the image will have a very good prospect in the future.

## ACKNOWLEDGMENT

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] J. Daemen and V. Rijmen, The Design of Rijndael: AES‑ The Advanced Encryption Standard J. Springer-Verlag. 2002:55-56 )

[2] M. Zhang, G. Shao and K. Yi. T-matrix and Its Applications in Image Processing J. Electronics Letters. 2004, 40(25): 1583-1584

[3] L. Y. Fan, J. J. Luo, H. L. Liu. Data Security Concurrent with Homogeneous by AES Algorithm in SSD Controller J. Ieice Electronics Express, 2014, 11(13): 115-118.

[4] Y. J. Li, W. L. Wu. Improved Integral Attacks on Rijndael C. Journal of Information Science and Engineering, 2011, 27(6): 2031-2045.

[5] Y. W. Zhu, H. Q. Zhang, Y. B. Bao. Study of the AES Realization Method on the Reconfigurable Hardware C. 2013 International Conference on Computer Sciences and Applications, 2013: 72-76.

[6] K. Stevens, O. A. Mohamed, Single-Chip FPGA Implementation of a Pipelined, Memory-Based AES Rijndael Encryption Design C. 2005 Canadian Conference on Electrical and Computer Engineering, 2005: 1296-1299.

[7] J. Tpldinas, V. Stuikys, R. Damasevicius. Energy Efficiency Comparion with Cipher Strength of AES and Rijndael Cryptographic Algorithms in Moble Devices J. Elektonika IR Elektrotechnika, 2011, 2: 11-14.

[8] A. Grediaga, F. Brotons, B. Ledesma. Analysis and Implementation Hardware and Software of Rijndael Encryption ]. IEEE Latin America Transactions, 2010, 8(1): 82-87.

[9] J. T. Zhou, A. C. Oscar, G. T. Zhai. Scalable Compression of Stream Cipher Encrypted Images Through Context-Adaptive Sampling J. IEEE Transactions on Information Forensics and Security, 2014, 9(11): 1857-1868.

[10] D. Das, M. Mukherjee, N. Choudhary, A. Nath, J. Nath. An Integrated Symmetric Key Cryptography Algorithm Using Generalised Modified Vernam Cipher Method and DJSA Method: DJMNA Symmetric Key Algorithm C. 2011 World Congress on Information and Communication Technologies, 2011: 1199-1204.