Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2018, 5(1):106-112**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Secure Image Retrieval System Based on Cloud Computing

Qin wang[1], Hongxin Lu[2], Jun Ye*[3]

[1]School of Automation & Information Engineering, Sichuan University of Science & Engineering, Zigong, China
[2]School of Computer Science, Sichuan University of Science & Engineering, Zigong, China
[3]School of Mathematic and Statistics, Sichuan University of Science & Engineering, Zigong, China

Abstract With the rapid adoption and application of cloud computing and mobile technology, Baidu cloud service, 360 cloud antivirus, Jinshan cloud platform etc, which security has become more and more attention in the convenience of people's lives at the same time. The security threat exists in cloud computing including data lost, date disclosed, hacking etc. To solve the above problems, a secure image retrieval system based on cloud computing is proposed in this paper. The core technology is that the images in the whole operation of the system are ciphertext interactions. The system realizes the user to encrypt the image on the client side, in the server side adopts the ciphertext storage, while achieving the protection of user image confidentiality, security and retrieval of fast and accurate needs. Not only has a high theoretical value, in practice, there is a higher value to promote the use of it.

Keywords Cloud computing; Image encryption; image retrieval

1. Introduction

Cloud computing [1-5] is an information technology paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources. Cloud computing is useful. It can be used to save the storage space.

The disclosure of network information has seriously endangered the national economic, social development and personal privacy. For information security [6-11], the state has increased the security of information into a national strategy. February 27, the central network security and information leading group was established. General Secretary of the CPC Central Committee, State President, Central Military Commission Chairman Xi Jinping personally served as head,Li Keqiang, Liu Yunshan as deputy head. This is another major step in the spirit of the Third Plenary Session of the Eighth Central Committee of the Communist Party of China. Not only shows the network information security is currently facing the situation complex and the status of the important, but also marks the Chinese information technology and network information security has been included in the national development of one of the highest strategic direction. So the face of such a big environment, network information security is imminent.

2. Model Establishment

2.1. Eigenvalue extraction

(1)Shrink size: Start with a small picture, but the picture is greater than 8*8,32*32 is the best.

(2)Simplify color: Transform the image into a grayscale image, further simplifying the calculation.

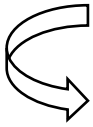
(3) Calculate DCT: Calculate the DCT transform of the picture to obtain a 32 * 32 DCT coefficient matrix.

(4) Reduce DCT: Although the result of DCT is a 32 * 32 size matrix, but we only need to retain the upper left corner of the 8 * 8 matrix, this part of the picture shows the lowest frequency.
(5) Calculate the average: Like the same as the hash, Calculate the average of DCT.
(6) Calculate the hash value:This is the most important step, set the hash value of 0 or 1 for 64 bits based on the 8 * 8 DCT matrix. Greater than or equal to the DCT value set to "1", less than the DCT mean set to "0". Combined these together to form a 64-bit integer, this is the fingerprint of this picture.

2.2. Image encryption

Data encryption is performed using the AES algorithm.

0	1	2	4	5	6	7	8	9	10	11	12	13	14	15



0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

Figure 1: The organization of plaintext and key

Separately processing each byte: Find the multiplication inverse of the byte on the finite field GF (28),"0" is mapped to itself, $\alpha \in GF(28)$ $\beta \in GF(28)$;

$$\alpha \cdot \beta = \beta \cdot \alpha = 1 \bmod (x8 + x4 + x2 + x + 1)。$$

The multiplicative inverse affine transformation obtained in the previous step

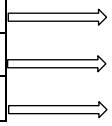
$$yi = xi? + x(i+4) \bmod 8? + x(i+6) \bmod 8? + x(i+7) \bmod 8? + ci$$

(ci is 6310,and that is the xth bit of 011000112),Matrix is expressed as:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

Declare a local variable array in the constructor and initialize it, and then use memcpy, (The member variable is named x, the local variable name y) row shift transformation to complete the line-based cyclic shift operation, the transformation method shown in Figure 2:

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15



0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

Figure 2: (Line-based cyclic shift operation)

That is, the row shift transformation on the line, the first 0 line unchanged, the first line cycle left shift 1 byte, the second line of the left shift 2 bytes, the third line of the left shift three bytes. And then mixed column by column, the method shown in Figure 3

$$b(x) = (03 \cdot x3 + 01 \cdot x2 + 01 \cdot x + 02) \cdot a(x) \bmod (x4 + 1)$$

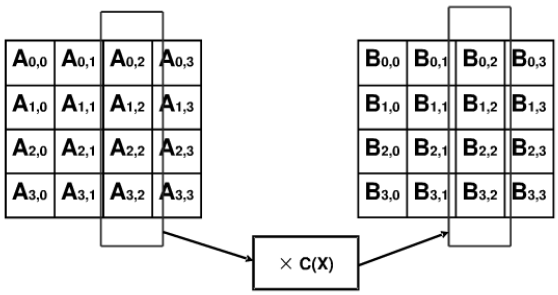


Figure 3: Mixed column by column

Matrix representation:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

he standard algorithm should be looped 8 times.(a and b each bit multiplication results are added together), But here only use the lowest 2, the inverse column of the decryption is used only with the low 4 bit. So here the high 4-bit operation is redundant, only the lower 4 bits. Simply add byte by byte, the addition of the finite field GF (28) is modulo 2 addition, namely the XOR Key Expanse on (Key extension).Key extension .Extend the input key to 11 groups of 128-bit key groups, in which group 0 is the input key itself, and then the *i*-th row of the nth group is the sum of the n-1th group of the *i*-th column and the nth group of the *i*-th column.(Modulo 2 addition, 1<= i <=3).

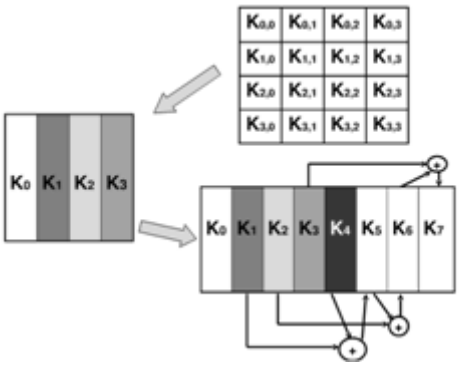


Figure 4: (key extension)

For each group of the first column that i = 0, there is a special deal.

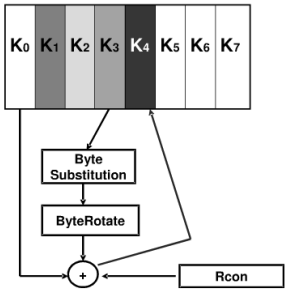


Figure 5: (key extension processing result)

The last column that is the n-1th group third column 4 bytes cycle left 1 byte. And each byte are substituted by other bytes. SubBytes. The first row (the first byte) is added to the round constant, and finally added to the previous set of columns.

3. Application

3.1 Test environment

3.1.1 Set up the test environment

Client	server
Windows7 intelcorei5-4210M@2.6GHz 8GMemory ADATASP900128GB java1.8	CentOS6.564 bit CPUSingle Core, Memory2G, bandwidth1M, system disk40G Java1.8 (Ali cloud server)

step：installJava JDK：

①http://www.oracle.com/technetwork/

java/javase/downloads/index.html, Log in to the website to download the latest jdk, and it is recommended to use version 1.8.

②And then double-click to open, enter the default open, has been the default click on the next step until the completion.At this point jdk has been installed successfully.

③Configure the environment variable, right click on my computer, select Properties -> Advanced System Settings -> Select System Environment Variables -> New System Environment Variables.(The variable value is the lib folder path under the Java installation path)

④In the system environment variables, click on the "path" editor, put the "%JAVA_HOME%/bin" to the front, click OK to complete.

⑤At this point, jdk has been installed, we have to verify whether the installation is correct, press the key "win + R" or click Start -> run the input "cmd", open the system command prompt box, enter "java -version", as shown , indicating successful installation.

3.2. Testing

3.2.1. Upload pictures

Click on the picture and upload the picture button as shown in Figure 5.

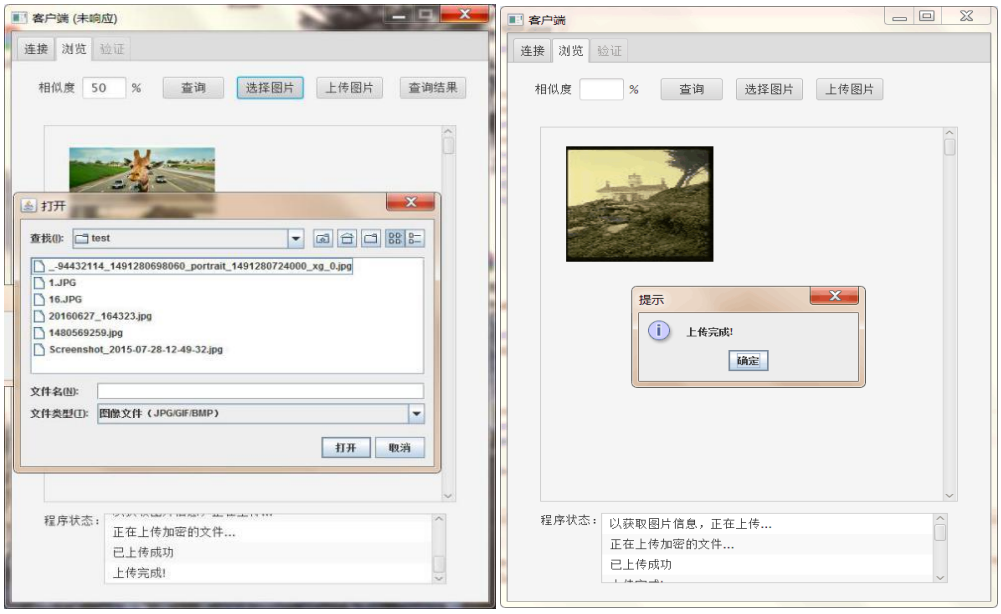


Figure 5

Picture plaintext and ciphertext comparison chart Figure 6:

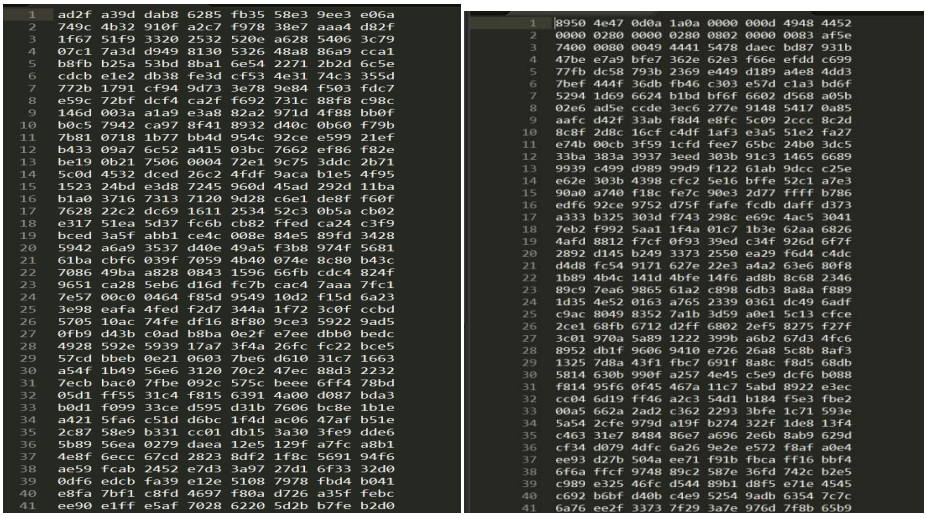


Figure 6: Ciphertext Comparison

Figure 7: Upload successful

3.2.2. Retrieve the picture

The query function of the system is to use the eigenvalues of the picture to retrieve the picture library of the server so as to achieve the purpose of quick retrieval and to set the similarity of the picture before executing the query.

After the success of the query interface shown in Figure 8:

Figure 8: query pictures

4. Conclusion

The system is mainly for the safe transmission of the image. Products in the realization of the function is mainly through the client on the image AES and a series of encryption algorithm processing. The system needs to transfer the image into a ciphertext, which greatly enhanced the image in the network transmission process of security. Because the data in the transmission process is a ciphertext, even in the transmission process, "hacker" intercepted the system information, "hackers" will not know what the data is transmitted which also greatly guarantees the privacy of the images transmitted by the system. Completely guaranteed the user's privacy, will not cause the disclosure of user information. Not only that, after the user uploads the image to the server store, the server doesn't save the most original image of the user, but the ciphertext after the client encrypts. As a result, there will not be the phenomenon of server information theft. The system uses the such encryption and encryption of cloud storage mode to maximize the maintenance of user privacy. This paper describes the cloud image security image retrieval system and the use of technology, greatly improving the cloud computing data service platform security performance.

Acknowledgement

This work was supported by the Undergraduate innovation and entrepreneurship project of Sichuan Province (20170622037).

Reference

[1]. Ostermann S, Iosup A, Yigitbasi N, et al. A performance analysis of EC2 cloud computing services for scientific computing. International Conference on Cloud Computing. Springer, Berlin, Heidelberg, 2009: 115-131.

[2]. Armbrust M, Fox A, Griffith R, et al. A view of cloud computing. Communications of the ACM, 2010, 53(4): 50-58.

[3]. Moreno-Vozmediano R, Montero R S, Huedo E, et al. Cross-Site Virtual Network in Cloud and Fog Computing. IEEE Cloud Computing, 2017, 4(2): 46-53.

[4]. Wang Y, Li J, Wang H H. Cluster and cloud computing framework for scientific metrology in flow control. Cluster Computing, 2017: 1-10.
[5]. Fiandrino C, Kliazovich D, Bouvry P, et al. Performance and energy efficiency metrics for communication systems of cloud computing data centers. IEEE Transactions on Cloud Computing, 2017, 5(4): 738-750.
[6]. Cavusoglu H, Cavusoglu H, Son J Y, et al. Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. Information & management, 2015, 52(4): 385-400.
[7]. Ifinedo P. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, 2014, 51(1): 69-79.
[8]. Ab Rahman N H, Choo K K R. A survey of information security incident handling in the cloud. Computers & Security, 2015, 49: 45-69.
[9]. Safa N S, Von Solms R, Futcher L. Human aspects of information security in organisations. Computer Fraud & Security, 2016, 2016(2): 15-18.
[10]. Safa N S, Von Solms R. An information security knowledge sharing model in organizations. Computers in Human Behavior, 2016, 57: 442-451.
[11]. Xu L, Jiang C, Wang J, et al. Information security in big data: privacy and data mining. IEEE Access, 2014, 2: 1149-1176.