Content-Oriented Multi-Level Security Authorization of Images

Liu Xiaojun
School of Electronic & Information
Huanggang Normal University
Hubei Huanggang, China
whutliuxiaojun@126.com

Peng Chong
School of Electronic & Information
Huanggang Normal University
Hubei Huanggang, China
whutliuxiaojun@126.com

Abstract—*The technology of digital watermarking and information hidden of image cannot solve the security problem of confidential regional data, and thus the research of the high-performance encryption technology of confidential data of Large Quantity of image has a important theoretical value and practical significance.In this paper, on the basis of the characteristics of Large Quantity of Image and application requirements on security, a scheme of authorizing the use of image based on multi-level secrurity is put forward. We propose multi-region and multi-level confidential information of image encryption algorithm based on content. The same images after encryption are distrtbuted to different level users, such as authorized user, partly authorized user, unauthorized user, but different authorization users acquire different importmant degree information after decryption through their own decryption keys. The scheme has the high confidentiality and high computing efficiency encryption algorithm and solve the difficult problems of Large Quantity of Image on security and secrecy.*

Keywords- images; multi-region selection; multi-level encryption; multi-level authorization based on content

I. INTRODUCTION

As we all know, there is a classification in each file. so whether the classification of the user is correspond with the that file is the key of judging the users' access right .But the research on multi-level authorization based on content is rare .Some confidential information in image regions involved in most related to military security and political stability. Confidential information contained in the images may be gained by the hostility. So the image data can only be applied by small range of users then the value of it couldn't be embodied entirely[1-3]. In order to make full and safe use of those data, the confidential part of them must be encrypted before being transferred or released .In this paper, the characteristics of image were combined and embedded thought of multi-level authorization into the security process of the image. While those data were ensured to be encrypted speedy, different classes of users (military/Defense Department, government agencies, research institutes, ordinary people.) would get those confidential information with different degree of importance.

II. IMAGE CONTENT OF THE MULTI-LEVEL AUTHORIZATION REQUIREMENTS

A. Select the region of the image data encryption

It will take a great deal of time and strength and influence the application of image if those all data are encrypted without distinguishing process. Among the most of image, the secret areas only occupied a small proportion of the whole image. For example, A frame of image includes area {R1， R2， R3， R4， …Rn}, s is the confidential region, /s is no confidential region.

Ordinary users can't get the information of set S, but /S. therefore, it's not necessary to have all the data encrypted. the selective for content encryption method which only encrypted image data from important region like set S will be in this paper . that region R1 R2 R3 are in different position of each piece of image can help to select fast and describe accurately . of course , it can reduce the amount of data required in security areas at the meantime .

B. Partition multi-domain security authorization

Application of image contains not only the military applications, but also extended to ordinary civil field. If the image data user groups are {U1，U2，U3，U4…，Un} which include military / defense department, government agencies, research institutes and ordinary people etc. Those groups belong to different levels[4-5]. If U1>U2>U3>U4, The corresponding military / defense department, government agencies, research institutes and ordinary people user groups. Different levels of user group can access different range, while the military and defense departments can access all the confidential area of images, government agencies and research institutes could visit some area with no national security in it. However, any confidential area shouldn't be got by ordinary people. If R1>R2>R3>R4>…Rn, after partition multi-domain security encrypted process , different levels of user groups have been deciphered ,accessible areas are as follows:

{U1，Key_U1} →{R1，R2，R3，R4，…Rn}
{U2，Key_U2} →{R2，R3，R4，…Rn}
{U3，Key_U3} →{R3，R4，…Rn}
……

In order to achieve multi-level authorization by letting different users' access different level of data information

of image those data should be encrypted hierarchically according to the degree of importance of confidential information in image.

III. MULTILEVEL SECURITY AUTHORIZATION ALGORITHM ORIENTED CONTENT

Algorithm combined image format and encryption technology of multi region and levels. To achieve Multi-level security authorization, we can adopt different levels of cipher code corresponding to importance of confidential information.

A. Description and extraction method of confidential region

Description and extraction of image secret area is segmentation of image. The image is segmented into regions with different characteristics and extract the object of interest[6]. But this process cannot be conducted by completely reliable model for the complexity of image itself.

In this paper, methods the features of image of delimitation and classification will be included such as point, line, and surface. Surface features can be divided into civil buildings, airports, military bases etc. Then analysis of the information in the corresponding layer or object category will approach according to the spatial properties and spectral characteristics of confidential information encrypted. No matter what is the shape of the object of confidential information, they could be selected by the minimum enclosing rectangle or point, line, surface tool directly. Therefore, description and extraction of the confidential surface features will be done.

B. The basic framework of multilevel secure encrypted region

In order to reduce the number of encryption and decryption and improve the efficiency of the system, a multilevel secure encryption system is designed in this paper for "one encryption, multistage decryption"[7]. The basic framework of multilevel secure encrypted is shown in Fig 1.

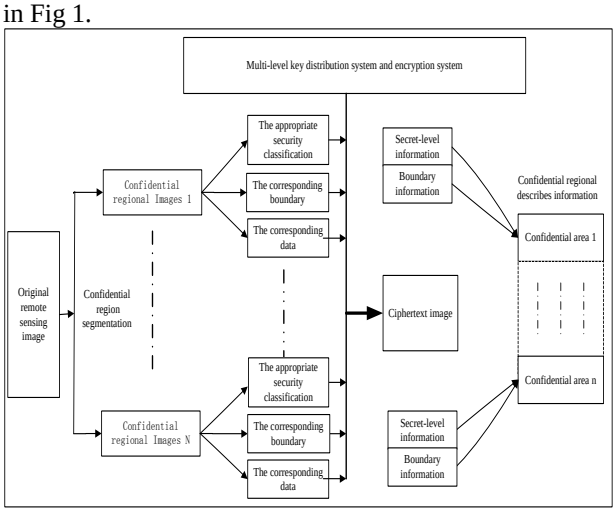

Figure 1. Content-oriented multi-level encryption framework of images

After segmentation and extraction of the original image, we can get N secret images and 1 residual image. All the secrets of regional image are separately specified categories. The specified key will be got by Multilevel key distribution system. The cipher text will form according to the Security encryption system. Each secret regional image block classified information, edge information is used as a structure and filled in the secret area finally received a description file. Therefore, we can get encrypted images and a certain number of Secret area description information. They will be distributed to users of different levels after arranged by system. Thus the management of image data is simplified because all the users will get the same data.

C. Key generation method of multilevel security authorization

This paper realizes secure access control in multilevel and the design of high, middle, low three security level users and general users. Confidential region of each classified users use their key can decrypt the secret .Meanwhile; high level users can calculate the low-level key according to the respective key.

The users of image distribution system can be divided into collections of disjoint classes of customers according to security levels like A={U1，U2，…，Un}. Each user has a corresponding security level. We use the partial order relation "<" to show different security levels." Ui≤Uj" indicates that the level of Ui isn't higher than Uj. therefore, (A，≤) formed A partially ordered set.

Image in this method user groups including high, low, three categories of users and the general public. The authority relationship between users is a totally ordered set : U1≤U2≤…≤Un. The multi-level security of this method can be realized by trapdoor one-way function. The user Uj only needs to keep the key Uj. only when Ui≤Uj , the user can calculate Ki from Kj . If Ui≥Uj , Kj cant be got by Kj . Fig 2 is for the Multilevel key diagram .

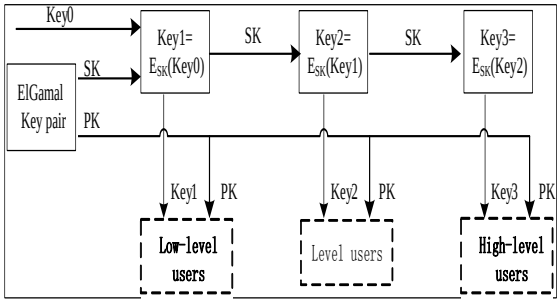

Figure 2. The architecture of the productionof multi-level key

Multilevel secure key generation module takes a random number Key0 (with checking the random characteristics) as the initial key. We can achieve the calculation of the multistage data encryption key using ElGamal public key cipher algorithm. ElGamal, the private key of the pair of SK as one-way encryption function of ESK operation key, The encryption key SK on the initial key Key0 repeatedly used one-way encryption function of ESK were generated from low to high multilevel data encryption keys Key1, Key2 and Key3. The private key SK generated by multilevel security key module. Any level of the users cannot gain access to the SK, and the PK public key will be distributed to all levels of users. Similarly in the decryption end, high level data encryption key can generate low-level data encryption key with the

corresponding decryption function DPK[8-10]. For example, high level permissions users can using their keys(Key3) to get primary key by repeatedly using one-way decrypt function DPK . Key2=DPK(Key3)，Key1=DPK(Key2)

D. The basic framework of multilevel security authorization

In image encrypted authorization system, different levels of users to obtain the same image data and different access key. Due to users' different key permissions, image information in different degree will be got. Each user can only obtain the corresponding information. For example, government agencies and research institutes can visit all the confidential area which nothing to do with national security. The basic framework of encryption multi-level authorization is shown in Fig 3.In order to describe simple and considering the diagram layout , encryption levels are divided into high, middle and low three levels. There are three confidential regions of the original image. The data of these 3 regions will be encrypted by Key1, Key2 and Key3 from low to high after analysis and extraction. Symmetric encryption algorithm can make it (Symmetric encryption algorithm is of high encryption and decryption speed and high data throughput rate). Such as AES, the the cipher text will return to the prior image through the following code, and then publish it. At the same time , data decryption keys of the corresponding level Key1,Key2,Key3 and ElGamal, public key decryption key PK are given to the appropriate level of the users.

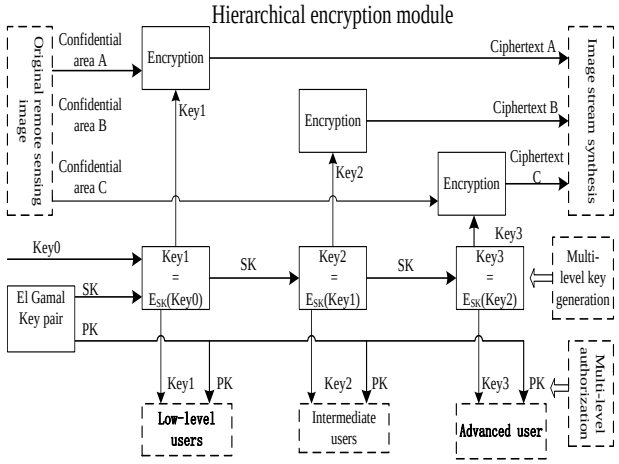

Figure 3. The architecture of multi-level security authorization

IV. EXPERIMENT AND ANALYSIS

A. experiment

Multi-level authorization method of enclosing rectangle: The minimum bounding rectangle of surface features of any shape can describe the outer boundary. Confidential features can be extracted by rectangle from sensing remote images. To larger confidential area, generally high resolution rectangle area will be selected . Three large rectangular area images In Figure 5（82×100） (a), (c), (E) extracted from image in Figure 4. As for selecting boundary, figure 5 （ 24×24 ） or smaller resolution rectangle will be adopted.

After secret areas of different levels are done, Different levels of keys will be produced by multilevel key distribution management module. Then encrypt The rectangular area(Including internal and external regional features) data hierarchically by Symmetric encryption algorithm with those keys. Finally publish the encrypted image . Figure 5 (b), (d), (f) is graph (a), (c), (e) of the different levels of encryption. As we can tell from the impression image, encryption strength of Figure 5 (b), (d), (f) image decreases gradually but the definition rises. Figure 5 (H), (I), (J) is (g) of the different levels of encryption and definition becomes high .

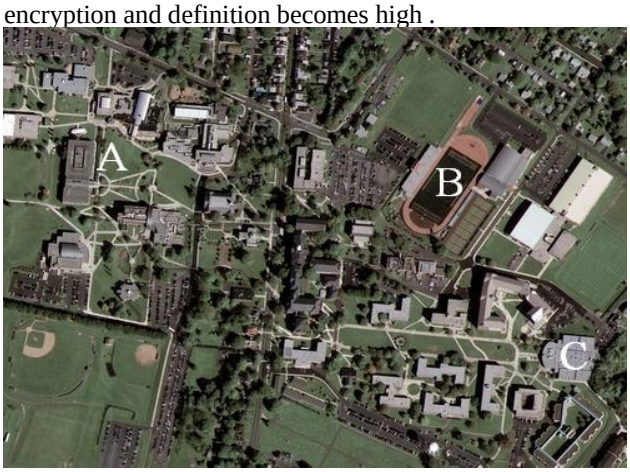

Figure 4. Experiment of Remote Sensing Images

High level users can get respective encryption key of confidential area by calculating with their own keys then decipher the encrypted image of area (b),(d)and (f) to get complete information . By the same method ,secondary users can get information of area (d)、(f) but (a) while the ordinary users cannot get any keys of confidential area but the indistinct image of area (b),(d)and (f)

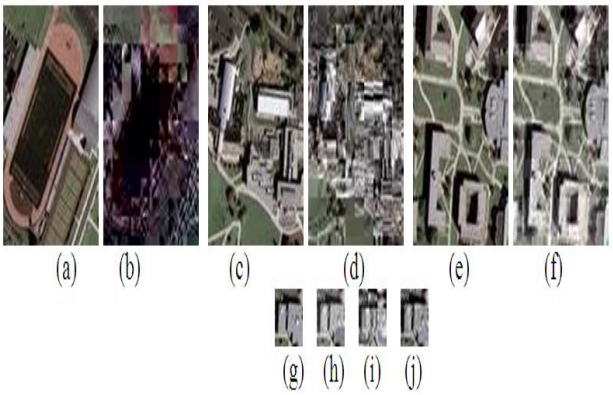

Figure 5. Results of multi-level region encryption images

Multi-level authorization method by point, line, surface tool to select confidential area: We can select A, B ,C three areas of Fig.4 (confidential level A>B>C) to encrypt with different levels then publish as shown in Fig.6.

From the processed images, it's obviously that they have been damage to different degree. To area A, we can get no information from it. The resolution ratio of B and C decreased and B became worse. Then give out the image after processing to different users. High level users can get complete information of area A, B and C while the secondary users can obtain from B and C but A. what's more, ordinary users cannot encrypt any area.

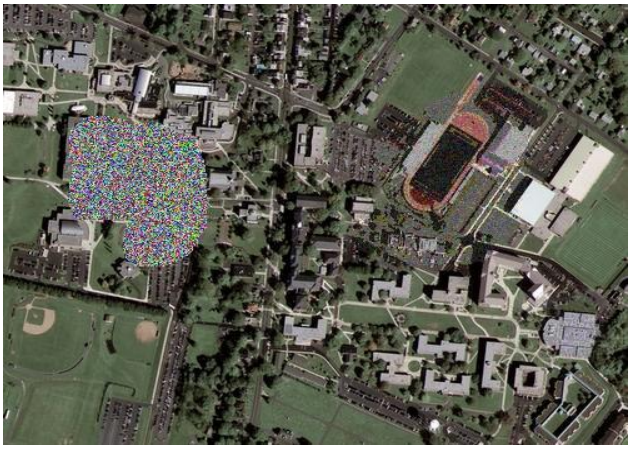

Figure 6. Security regions multi-level encryption based on the point, line and plane selection

B. function analysis

The safety of image multi-level authorization algorithm brought up in this paper refers to symmetric encryption algorithm and multilevel key generation module safety management. AES encryption algorithm is adopted and ElGamal, the Public-key encryption algorithm defends for multilevel key generating module. Both of them are away from any attack currently.

To the method presented in this paper, full encryption does not require partial image. In the general case with not large amount of data, symmetric encryption algorithm is of high calculation efficiency which can meet the requirements of practical applications.

V. CONCLUSION

The Content-Oriented multi-level security authorization of image method is put forward in this paper which is about segregating, abstracting the confidential areas first, and then encrypting with different levels of key according to the degree of secrecy confidential area. Users with high level keys can encrypt high-grade encryption area while the image format remains compatible. Moreover, high level keys can encrypt confidential area encrypted by low level keys after calculation. Safety testing and test results indicate that this kind of multi-level security authorization is of little calculation, low complexity and high reliability. The contradict between popularizing and security of high resolution image solved

ACKNOWLEDGMENT

The project was supported by the Doctoral Scientific Fund Project of Huanggang Normal University (Grant No. 2013031103), and the Scientific Research Program of Educational Commission of Hubei Province of China (Grant No. 20142905).

REFERENCES

[1] Amini, M, 2010 Multi-level authorisation model and framework for distributed semantic-aware environments [J], IET Information Security, v4, n4:301-321. DOI: 10.1049/iet-ifs.2009.0198

[2] Barni M, BartoliniF, 2001. Watermarking-based protection of remote sensing images:Requirements and possible solutions[A].Proceedings of SPIE v4475:191-202. DOI: 10.1117/12.449582

[3] Barni M, Bartolini F, 2002. Watermarking techniques for electronic delivery of remote sensing images [J]. Optical Engineering, 41(9):2111-2119. DOI: 10.1117/1.1496787

[4] Hsu,Chien-Lung,Chang, Liang-Peng; 2011, A supervising authenticated encryption scheme for multilevel security [c],International Journal of Innovative Computing, Information and Control, v7, n3:1087-1095, March

[5] LIU Ding. 2010， A New Scheme for Pervasive Computing-Oriented Dynamic Multi-Level Security Access Control [J], Microelectronics & Computer, V27(1):102-105

[6] Min Lianquan. 2005, The Security Transmission Modelof Image Based on LSB [J]. ENGINEERING OF SURVEYING AND MAPPING, (Chinese),V 14(3):11-14.

[7] WANG Xian-min, GUAN Ze-qun, WU Chen-han. 2005, Information Authorized Hiding Algorithm for Remote Sensing Image Based on Image Fusion[J]. Journal of Remote Sensing(Chinese), V9(5):576-582.

[8] WANG Xiang-yang, YANG Hong-ying, WU Jun. 2005, Content based Adaptive Discrete Cosine Transform Domain Watermarking Algorithm for Remote Sensing Image [J]. V,34(4):324-330

[9] Wen J T, Severa M, Zeng W J, etal. 2002. A format-compliant configurable encryption framework for access control of video. IEEE Transactions on Circuits and Systems for Video Technology, V12(6): 545-557. DOI: 10.1109/TCSVT.2002.800321

[10] Wu, Chunxia, Lv, Xia; Li, Jianqiang 2011,Geological data access security mechanism based on Grid-GIS,[C] Proceedings-19th International Conference on Geoinformatics . DOI: 10.1109/GeoInformatics.2011.5981019