http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (18): 4687-4692, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.4687.4692

Content-oriented Multi-level Security Authorization of Remote Sensing Images

[1]Yuan Ye, [1]Tu Chunxia and [2]Liu Xiaojun
[1]Schoo of Mathematics and Computer Science,
[2]School of Physics and Electronic Information, Huanggang Normal University,
Huanggang, 438000, Hubei, China

Abstract: In this study, on the basis of the characteristics of Large Quantity of Remote Sensing Data and application requirements on security, a scheme of authorizing the use of remote sensing images based on multi-level secrurity is put forward. We propose multi-region and multi-level confidential information of remote sensing images encryption algorithm based on content. The same remote sensing 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 Remote Sensing Data on security and secrecy.

Key words: Remote sensing images, multi-region selection, multi-level encryption, multi-level authorization based on content

INTRODUCTION

We need to take security measures to protect these spatial data by the explosion of the value of space remote sensing data and the use in some important fields. At present the research on remote sensing image security problems mainly focus on digital watermarking (Barni *et al*., 2001; Wang *et al*., 2005; Barni *et al*., 2002), information hiding (Min, 2005; Wang *et al*., 2005) and encryption technology based on traditional image (Liu, 2010). Digital watermarking technology of remote sensing image mainly deals with the problem of copyright protection but haven't achieved the protection of remote sensing image data itself. Generally Information hiding hides confidential information in the non confidential image data. The hidden data capacity is limited because of some characteristics like the huge amount of data of the remote sensing image. Also, it's not functional that it may affact the compression, analysis and other application of remote sensing image after inserting remote sensing image secret information into non confidential image data.What's more,the efficiency of encryption is lower in traditional technology due to not considering the characteristic and security requirement of remote sensing image.

Research on multilevel security authorization mainly lies in the file information multi-level authorization based on whole.As we all know, there is a classification in each the file information.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.

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 study, the characteristics of remote sensing image were combined and embedded thought of multi-level authorization into the security process of the remote sensing image. While those data were ensured to be encrypted speedy, different classes of users would get those confidential information with different degree of importance (Wu *et al*., 2011).

REMOTE SENSING IMAGE CONTE -NT OF THE MULTI-LEVELAUTHOR-IZATIONREQUIREMENTS

Select the region of the remote sensing image data encryption: It will take a great deal of time and strength and influence the application of remote sensing image if those all data are encrypted without distinguishing process. Among the most of remote sensing images, the secret areas only occupied a small proportion of the whole remote sensing image. For example, A frame of image includes area {R1, R2, R3, R4, ... Rn}, s is the Confidential region set, /s is nonconfidential region set. if:

Corresponding Author: Tu Chunxia, Schoo of Mathematics and Computer Science, Huanggang Normal University, Huanggang, 438000, Hubei, China

$$S = \{R1, R2, R3\}$$
$$/S = \{Ri|3<i<n,i?N\} = \{R4, R5, \ldots Rn\}$$

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 study. that region R1, R2, R3 are in different position of each piece of remote sensing image can help to selct fast and describe accurately of course, it can reduce the amount of data required in security areas at the meantime.

Partition multi-domain security authorization: Application of remote sensing image contains not only the military applications, but also extended to ordinary civil field. If the remote sensing 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. 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 remote sensing 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:

$$\{U1, Key\_U1\} \rightarrow \{R1, R2, R3, R4, \ldots Rn\}$$
$$\{U2, Key\_U2\} \rightarrow \{R2, R3, R4, \ldots Rn\}$$
$$\{U3, Key\_U3\} \rightarrow \{R3, R4, \ldots Rn\}$$

In order to achieve multi-level authorization by letting different users access different level of data information of remote sensing images,those data should be encrypted hierarchically according to the degree of importance of confidential information in remote sensing image.

Remote sensing image encryption based on content: In order to keep the use value of the rest remote sensing image, encryption method of remote sensing image based on content is required in the process of regional encryption. Codings of remote sensing image are organized in accordance with Uniform protocol standard which is expressed by fixed grammar information.

The grammatical structure of information benefits indicating semantic information in image format and protocol standard and plays an important role in decoding the identification and extraction of image compression code stream. Encryption special code is easy to cause the known plaintext attack, therefore grammatical structure information cannot be protected by encryption. It's Used to indicate the image of information color, texture, structure, content and so on and the encryption can achieve secure content information and reduce the secret region resolution effect. The encryption of this part of the data can guarantee the encrypted stream still meet the standards and no illegal code. In a word, it can realize the encryption protection based on content.

MULTILEVEL SECURITY AUTHORIZ-ATION ALGORITHM ORIENTED CON-TENT

Algorithm combined remote sensing 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.

Description and extraction method of confidential region: Description and extraction of remote sensing image secret area is segmentation of remote sensing image. The image is segmented into regions with different characteristics and extract the object of interest (Wen *et al*., 2002). But this process cannot be conducted by completely reliable model for the complexity of remote sensing image itself.

In this study, methods the features of remote sensing image of delamination and classification will be included such as point, line, 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.

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 study for "one encryption, multistage decryption ". The basic framework of multilevel secure encrypted is shown in Fig. 1.

After segmentation and extraction of the original remote sensing image, we can get N secret images and 1 residual image. All the secrets of regional image are

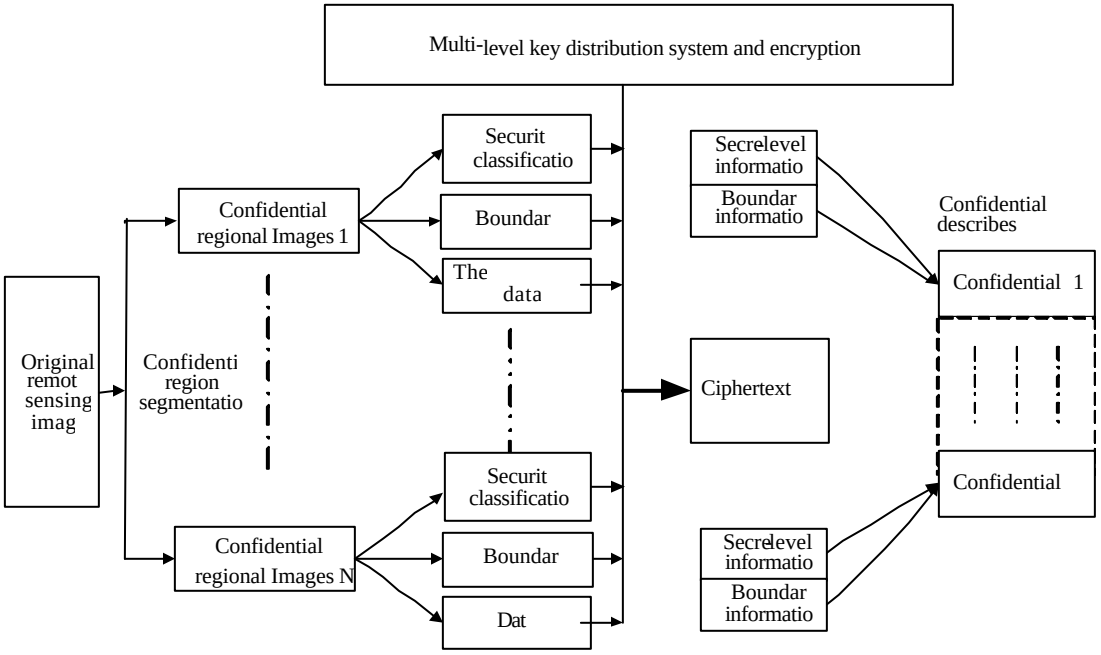

Fig. 1: Content-oriented multi-level encryption framework of remote sensing images

separately specified categories. The specified key will be got by Multilevel key distribution system. The ciphertext 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 remote sensing 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 remote sensing image data is simplified because all the users will get the same data.

Key generation method of multilevel security authorization: This study 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 remote sensing image distribution system can be devided into collections of disjoint classes of customers according to security levels like $A = \{U_1, U_2, \ldots, U_n\}$. Each user has a corresponding security level. We use the partial order relation "<" to show different security levels." $U_i = U_j$" indicates that the level of U_i isn't higher than U_j. therefore, formed A partially ordered set.

Remote sensing 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 : $U_1 = U_2 = \ldots = U_n$. The multi-level security of this method can be realized by trapdoor one-way function. The user U_j only needs to keep the key U_j. only when $U_i = U_j$, the user can calculate K_i from K_j. If $U_i = U_j$, K_j cant be got by K_j. Figure 2 is for the Multilevel key diagram.

Multilevel secure key generation module takes a random number Key0 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 D_{PK}. For example, high level permissions users can using their keys(Key3) to get primary key by repeatedly using one-way decrypt function D_{PK}. Key2 = D_{PK} (Key3), Key1 = D_{PK} (Key2).

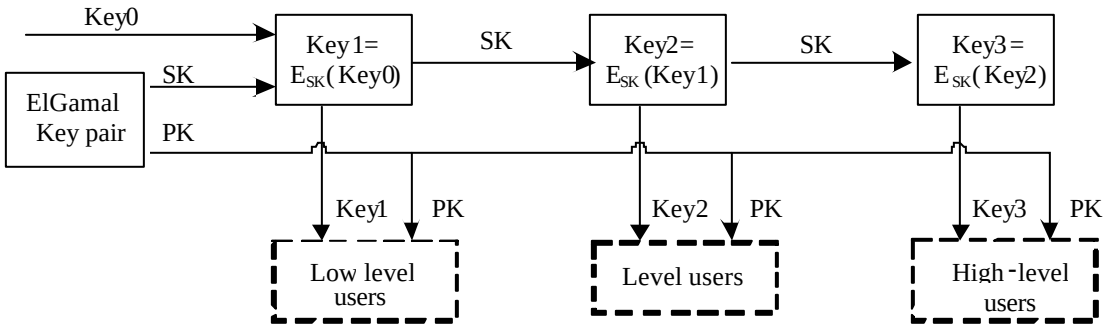

Fig. 2: The architecture of the production of multi-level key

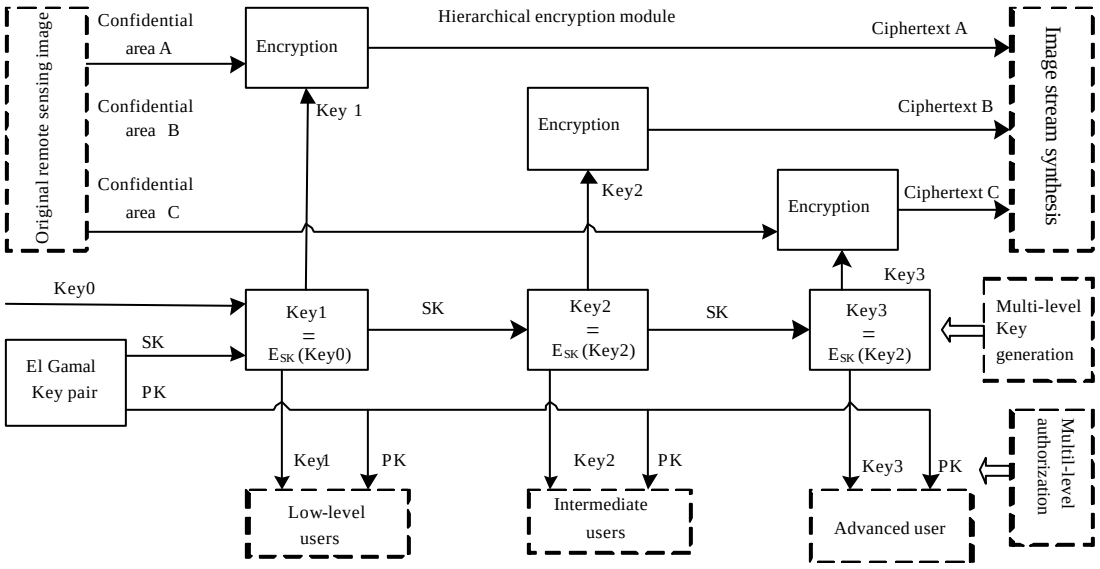

Fig. 3: The architecture of multi-level security authorization

Basic framework of multilevel security authorization: In remote sensing image encrypted authorization system, different levels of users to obtain the same image data and different access key. Due to users' different key permissions, remote sensing 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 (Amini and Jalili, 2010). 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 remote sensing 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 ciphertext will return to the prior remote sensing 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.

EXPERIMENT AND ANALYSIS

Mockup experiment: The satpics from GeoEye (the world's largest commercial satellite remote sensing images provide company) are employ to test authorization method of multilevel security. It can provide 50 cm image data accuracy.

Fig. 4: Experiment of Remote Sensing Images

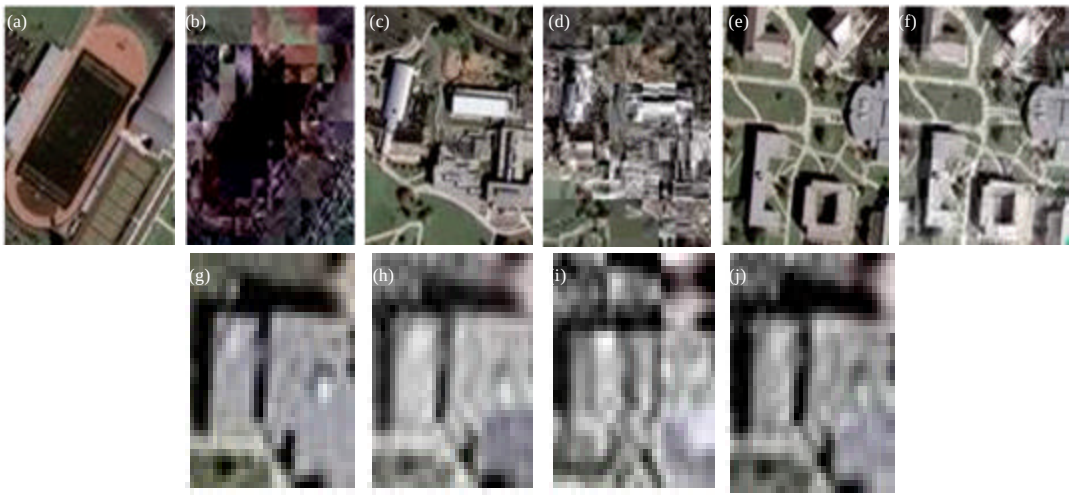

Fig. 5(a-j): Results of multi-level region encryption images

For selecting the multi-level authorization method in the secret area, basing the enclosing rectangle and the point, line, surface two ways are carried out In this study.

- 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 Fig. 5(82×100) (a), (c), (E) extracted from remote sensing image in Fig. 4. As for selecting boundary, Fig. 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 5b, d, f is graph (a), (c), (e) of the different levels of encryption. As we can tell from the impression image, encryption strength of Fig. 5b, d, f image decreases gradually but the definition rises. Fig. 5 H, I, J is g of the different levels of encryption and definition becomes high.

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):

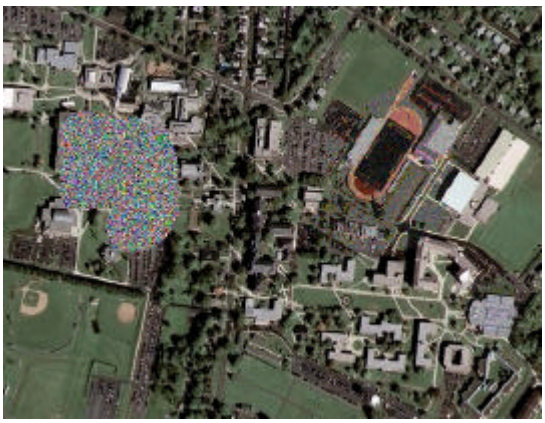

Fig. 6: Security regions multi-level encryption based on the point, line and plane selection

- 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 (Hsu *et al*., 2011).

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

To the method presented in this study, 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.

CONCLUSION

The Content-Oriented multi-level security authorization of remote Sensing images method is put forward in this study which is about segregating, abstracting the confidential areas first, 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 remain 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 remote sensing image solved.

ACKNOWLEDGMENTS

The project was supported by the Scientific Research Program of Huanggang Normal University (Grant No. 2012009303) and the Teacher Program of Electrical and Electronic Experimental Teaching Demonstration Center (Grant No. zj201257).

REFERENCES

Amini, M. and R. Jalili, 2010. Multi-level authorisation model and framework for distributed semantic-aware environments. IET Inform. Sec., 4: 301-321.

Barni, M., F. Bartolini, E. Magli and G. Olmo, 2002. Watermarking techniques for electronic delivery of remote sensing images. Opt. Eng., 41: 2111-2119.

Barni, M., F. Bartolini, V. Cappellini, E. Magli and G. Olmo, 2001. Watermarking-based protection of remote sensing images: Requirements and possible solutions. Proc. SPIE, 4475: 191-202.

Hsu, C.L., L.P. Chang and and T.C. Wu, 2011. A supervising authenticated encryption scheme for multilevel security. Int. J. Innovative Comput. Inform. Control, 7: 1087-1095.

Liu, D., 2010. A new scheme for pervasive computing-oriented dynamic multi-level security access control. Microelectr. Comput., 27: 102-105.

Min, L.Q., 2005. The security transmission model of image based on LSB. Eng. Surveying Mapping (Chin.), 14: 11-14.

Wang, X.M., Z.Q. Guan and C.H. Wu, 2005. Information authorized hiding algorithm for remote sensing image based on image fusion. J. Remote Sensing (Chin.), 9: 576-582.

Wang, X.Y., H.Y. Yang and J. Wu, 2005. Content based adaptive discrete cosine transform domain watermarking algorithm for remote sensing image. Acta Geodaetica Et Cartographic Sinica, 34: 324-330.

Wen, J.T., M. Severa, W.J. Zeng, M.H. Luttrell and W.Y. Jin, 2002. A format-compliant configurable encryption framework for access control of video. IEEE Trans. Cir. Syst. Video Technol., 12: 545-557.

Wu, C.X., X. Lv and J.Q. Li, 2011. Geological data access security mechamism based on grid-GIS. Proceedings of the 19th International Conference on Geoinformatics, June 24-26, 2011, Shanghai, pp: 1-5.