2011 International Conference on Computer Science and Information Technology (ICCSIT 2011)
IPCSIT vol. 51 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V51.98

The Research of Using Hash Algorithm to Protect Classified Document

Wang Heng[a,]*, Yu Xingchen, Chang Jingjing, Yao Heng, Wang Xinkai

Computer Science Department, Sichuan University Jinjiang College, Pengshan, 620860, China

Abstract. With the development of computer technology and network, the production management of each industry is more and more information-based, it goes without saying that information security is very important. In this article we put forward a new solution which uses Hash Algorithm, Digital Watermarking and Data Transfer Technology comprehensively.

Keywords: Information Security, Classified Document, Hash Algorithm, Digital Watermarking.

1. Introduction

At present, a website named Search Security has made a survey on information security of companies, it shows that 30% to 40% commercial secrets disclosure is caused by disclosure of electronic documents, the companies which are top thousand on <Fortune> will lose 4 millions dollars because of disclosure of commercial secrets each time.

2. Current Situation of Protecting Classified Document

With the development of information-based production management of every industry, computer disclosure is also on the rise. The greatest feature of computer disclosure is that it is more subtle and harmful. A malicious leak of trade secrets will lead to a serious consequence which will cost huge sum of money to compensate, or even put the enterprise to death. According to the authoritative data, almost no methods are taken by Chinese enterprises to protect electronic documents, even if the secret electronic documents are protected, they are just protected by a traditional encryption methods.

3. The limitation of traditional encryption methods

The leakage of secret documents usually occurs when unauthorized users operate secret documents which are not protected. Even if the business or individual has take the encryption method on secret documents, hackers can also decrypt it in a short period of time. When the leakage was brought to light, it's too late to compensate. As computing power continues to improve, traditional encryption method are facing an unprecedented challenge.

With the development of hacking technology, traditional encryption methods gradually expose shortcomings, in order to better protect secret document, user has to increase the key length, but with the growth of key length, how to remember such a long key becomes a problem. Encryption also has a fatal draw back: A bunch of gibberish or a message box which tells user to input key will be shown to the user, which equals to telling the illegal invaders that this is a very important document, then the hacker will be devoted to cracking your encrypted document.The result of this method is that people will easily know this is a very important document, regardless of whether hackers are able to break your encrypted documents, which would tend to cause immeasurable loss!

* *E-mail address:* jcokeh@gmail.com.

4. Using Hash Algorithm to Protect Secret Document

4.1. Build A Hash Table

Use Digital Watermarking technology to hide n(refers to a number) non-classified documents(general documents) in a file under a directory, which will proceed antomatically while installing the software. We define the document which is hidden in a file as hw(HiddenWord) document and define the classified document which needs to be protected as tw(TransferrededWord) document. No matter whether the document is tw or not, system will not tell the user the information of the document, then the document which is hidden through this method looks as the same as the general one.

When user creates a new document, the default property is tw document, and user can also modify the document property to general document. If it is tw document, a Hash Table will be established in order to associate this tw document with a hw document. If it is a general document, any operations(Delete, Copy, Edit) can be accepted without authority.

4.2. Certification Authority

Rights certification process will be solidified in the USB authentication device, other processes will be stored in PC. When user opens a document, rights certification process will start secretly,if user has inserted the USB authentication device and system has recognized this device, system will ask user to enter the authentication code, if the code is correct, tw document will be opened, that is to say user has opened the document which needs to be protected, and the mapping between tw and hw document will be canceled at this moment, so user can delete, copy, edit this tw document. When user closes this tw document, process will automatically build a Hash Table again.

4.3. Data Transfer

If the system has not recognized the USB authentication device or the system has recognized the USB authentication device but the authentication code is false, system will transfer the data, therefore users can not read and modify the tw document, instead a general document will be demonstrated to users by system through Hash Table.

5. Conclusion

With the development of computer network and the information technology in management of industry, it’s no doubt that information security is very important. In this article, we propose a solution, which has integrated the use of the Hash Algorithm, Digital Watermarking and Data Transfer technology. When we use it to protect documents, attacker can not read the real secret documents when unauthorized, and the document attacker can read is a general one which is opened through a Hash Table, so attacker will give up attacking. If attacker copies all documents, only hw documents can be taken by attacker, we believe this solution will play a positive role in protecting secret documents.

6. Acknowledgements

Wang Heng (1991-), male,from Bazhong, Sichuan Province, undergraduate of Sichuan University Jinjiang College.

Yu Xingchen (1989-), male,from Chengdu, Sichuan Province, undergraduate of Sichuan University Jinjiang College.

Chang Jingjing (1989-), female,from Chaohu, Anhui Province, undergraduate of Sichuan University Jinjiang College.

Yao Heng (1989-), male, from Suining, Sichuan Province, undergraduate of Sichuan University Jinjiang College.

Wang Xinkai (1990-), male,from Bazhong, Sichuan Province, undergraduate of Sichuan University Jinjiang College.

7. References

[1] YAN WANG, PENG SUN, SHUWANG LU, *A Distribution Mechanism of Enterprise Secret Documents*[J]. Computer Engineering, 2004, 22(09): 173-179.

[2] DALI ZHU, *New Application of Digital Watermarking Technology In Information Security*[A]. Academic Research, Information Security and Communication Security,2009.2: