Journal of Theoretical and Applied Information Technology
15th December 2012. Vol. 46 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN IMPROVED INFORMATION HIDING ALGORITHM

[1, 2] QIAN ZOU, [1]HUAJUN WANG, [1, 2*] WEI HUANG, [2]JIN PAN

[1]Department of Information, Chengdu University of Technology, Chengdu 68, Shichuan, China

[2]Department of Computer, Guiyang University, Guiyang 550005, Guizhou, China

* Corresponding author

ABSTRACT

Hiding technology is a newly developed discipline that concludes many subjects and covers many fields, and it hides the transferring information in the carrier, which greatly increases the safety of information transmission. In order to hide and transfer information more effectively, the paper researched the cloud algorithm in the model of information hiding. It also studied the model of information and improvement of the algorithm. With experiments, the algorithm proved to be applicable and could improve the safety and reliability of information hiding.

Keywords: *Information Hiding, Cloud Computing, Formation Model*

1. INTRODUCTION

Modern information hiding technology is a new science, which includes information theory [1], cognitive science, cryptography etc., and covers new disciplines such as extended communication, signal and information processing technology. The characteristic of information hiding is to put the important information into certain carriers that can be readable and understandable. We hide the important information by carriers during the transmission in order to protect the information without being pirated.

We compared the information hiding technology with cryptograph and then found some shortcomings of traditional encryption method. Firstly, attackers can get clear clues and then detect where the important information is, which increases the possibility of being decoded. Secondly, if the encrypted documents are decoded, the encrypted information is fully transparent. Lastly, if the attacker failed to decode, he could destroy the information and the legal receiver couldn't get the right encrypted information [2-4].

2. FORMS OF CLOUD COMPUTING

2.1 SaaS (Soft Ware as a Service)

This kind of cloud computing adopts multiple user architecture, which provides a single software through the browser to thousands of customer. Google Docs of Google is one of the typical SaaS[5].

2.2 PaaS(Platform as a Service)

This kind of clouding computing is in fact another SaaS, of which the developing environment is provided as a service. Enterprises can develop the application based on basic architectures through the server established by the provider. Applicable platform of Face book and Force.com of Sales force are examples of this kind of cloud computing.

2. 3 In-cloud Web Service

This kind of clouding computing enables developers to use the API given by providers to develop the applicable software without developing all the function themselves [6]. Google Maps and Google Earth of Google is one typical example.

2. 4 Manage Service Provider (MSP)

This kind of computing is the oldest form of clouding computing (it is in fact an in-cloud service). With this form, service management is an application actually provided to the IT user but not to the end user, such as E-mail virus scanning and monitoring. The examples include the services provided by Secure Works, IBM and Verizon, and anti-span service of Google based on cloud computing.

2.5 Utility Computing

This kind of cloud computing enables users to use the storage and virtual computers according to their needs . The examples are S3(storage) and EC2 (virtual computers) of Amazon[3].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. ADVANTAGES OF CLOUD COMPUTING

3. 1 Virtualization

The virtual management, adjustment and application are carried out by cloud computing through software. The maintenance cost and utilization ratio of resources can be greatly decreased by the virtualization in the cloud computing [4].

3. 2Dynamic Scalability

With more people surfing on the Internet, the number of access to the information service center increases rapidly. In the cloud computing system, the server can be added into the present server cluster to improve the processing ability of cloud computing center. If there is anything wrong with the node, the node should be abandoned, and the task is transferred to another node, it can join in the present cluster after the problem is solved.

3.3 High Reliability and Security

If the computer's configuration is relatively low, the data would be easily lost if the computer is destroyed under the traditional mode. As a result, there would be great troubles and economic damages. However, under cloud computing mode, large amount of data is stored in the cloud, and the application procedure is operated in cloud computing center, so the computing is carried out through cloud computing center. All the services are distributed over the different servers. If any node goes wrong, it would be ended up and transferred to another procedure or node. The failed node is automatically dealt, which ensures the normal operation of computing and application. This means it is not necessary to prepare backup at the user end and the checkpoint recovery is ready at any time.

3. 4 Data and Software in the Cloud

Under the traditional mode, the software we use is generally installed by the professionals when we bought the computer. It is not convenient for us to install and update the software when using it. If a computer gets infected by virus which we cannot deal with, we could just let it spread and lost our data; while it will cost too much to ask professionals to solve the problem. Under the cloud computing mode, all users' data is saved in the cloud and one can get it at anytime he wants from the cloud. The users' software is directly managed by the facilitator, who is in charge of the updating and maintenance. Our data will not be lost and doesn't need to be backed up, and the software can update by itself.

3.5 Powerful Computing and Storage Ability

Under the traditional mode, the PC's size is too large, and sometimes it computes too slowly. Additionally, the storage space is not enough if the computer is not renewed. Under the cloud computing mode, we can login at anytime and anywhere we want to get the computation service without carrying the computer of large size. At the same time, users don't need to worry about the processing speed and storage space because the service is provided by thousands of servers [5],

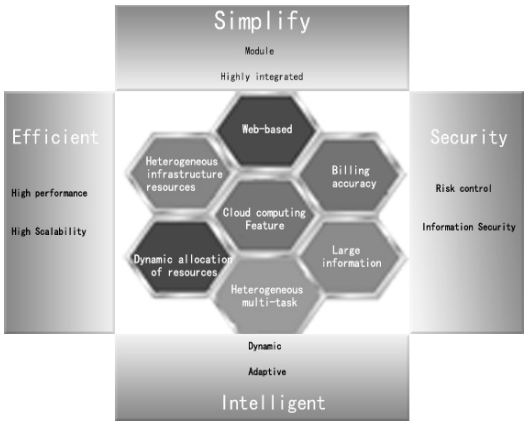

Figure 1: Cloud computing Feature

3. 6 Low Cost and Green Energy-saving

In the large amount of data processing circumstance, PC cluster distributed processing method of cloud computing instead of the central processing method of minicomputers and disc arrays, which lowered the construction cost. In the fierce competition, making a profit is of course the most important while saving the cost is also another way of earning a profit [6]. The former President of Google in China mentioned that Google would spend 64 billion dollars if they didn't adopt the cloud computing technology, and that the real cost was 1.6 billion dollars. That is to say, Google only spends 1/40 of the amount his rival spends. Many IT companies have encountered the hard disk damage. When the company wanted to buy a new disk, they find that the disk with the unique interface has been extinct. Even if the disk has been found, the data has to be transferred, which costs a lot of money and time. With the cloud computing, the storage of documents doesn't need to be compatible with read and write function of other disks, which increases the life expectancy of disks and decreases the cost.

Journal of Theoretical and Applied Information Technology
15th December 2012. Vol. 46 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. MODE DESIGN OF INFORMATION HIDING SYSTEM

Given A is going to send some information to B, A needs to randomly distract some unimportant information from the random information source. When the information is publicly transferred, it cannot be suspected, which is called the carrier. Integrating the secret information M into the carrier C, and the carrier C is changed to the stego-object C'. The embedding of secret information needs a key, which is called stego-key.

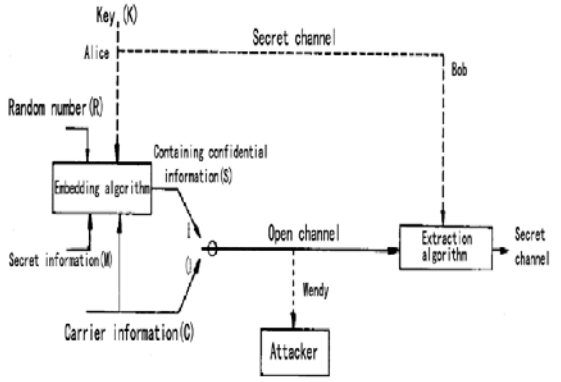

Figure 2: Information Hiding Model

In this model, Alice and Bob are the sender and the receiver separately. The guarder Wendy is the analyst, that is, the attacker, existing in the system channels. The sender Alice transfers the secret information to the receiver Box by a system, which makes the guarder Wendy cannot find out the secret information in the whole information. In order to transfer the secret information to Bob, the system should be robust. Alice can choose two methods when communicating. One is that the sender directly transfers the carrier information C to Bob through open communication channels and the switch is on "0". The other one is that the sender, using random digit R and key K, embeds the secret information into the carrier information C, which becomes the secret information S and then transfers it to Bob through open communication channels and the switch is on "1". Bob distracts the secret information M' through the key K which is obtained through the secret communication channels, hoping to get Alice's secret information as soon as possible .

The security of this model depends on whether the passive attacker Wendy can detect there is secret information M in the data which is obtained through the secret communication channels.

They have the following features:

A: Imperceptibility: By making use of redundancy existed in human feelings (feeling redundancy) and digital signals (data redundancy), information hiding uses digital media and digital files as carriers, and then hides the secret information with some algorithms to get the objective of hiding communication without changing the carriers' basic features and application value.

B: Capacity of embedding information: more information is required to be hidden in carriers.

C: Robustness: Not highly required.

The chart: the relationship between imperceptibility, robustness and capacity.

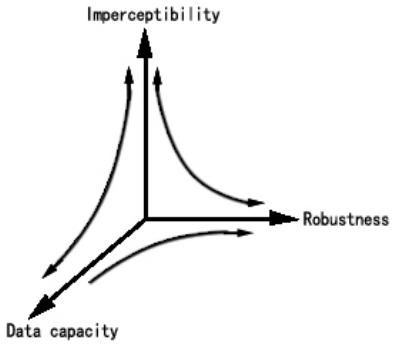

Figure 3: The Relationship Between Imperceptibility, Robustness And Data Capacity

5. ALGORITHM IMPROVEMENT OF INFORMATION HIDING

Any probability distribution can be decomposed as a sum of many normal distributions, which is proved in mathematics. Similarly, considering the universality of the normal cloud, gray frequency distribution of images can be regarded as the superposition of many normal clouds, by changing from quantitative data to qualitative concept. The so called cloud transform is to automatically generate many superpositions of C clouds (Ex, En, He) with different particle sizes according to frequency distribution function of certain data attribute X in the given universe. Each cloud stands for a discrete and qualitative concept, and then the conceptive transform will be changed from successive numerical interval. Its mathematical expression is:

$$f(x)y = \sum_{i=1}^{n}(a_i C(E_{x_i}, E_{N_i}, H_{E_i})) \quad (1)$$

Where ai is the amplitude coefficient;n is transformed to generate the number of discrete concepts. A series of different sizes consisting of normal cloud model cloud base set is obtained after cloud transform.

$$C\{C_1(E_{x_1}, E_{n_1}, H_{e_1}), C_2(E_{x_2}, E_{n_2}, H_{e_2}),,, C_m(E_{x_m}, E_{n_m}, H_{e_m})\} \quad (2)$$

Where, (C_1 , C_2 … C_m)is represented by the atomic cloud model concept.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

There are many methods of information hiding. Now the author uses the improved LSB to hide information. The process includes a subset of the carrier element { j_1 , • • • , $j_{l(m)}$ },and the substitute operation is carried on the subset, that is, c_{ji} is replaced by m_i (m_i =1or 0). In the process of extraction, we extract the LSB (the hiding carrier) and reorder it to reconstruct the secret information.

The embedding algorithm:

for （i=1;i<=VGA series numbers ;i++） do;

$s_i \longleftarrow ci_i$;

end for ;

for （i=1;i <=length of secret information ;i++） do ;

//randomly selected by the computer unimportant positions to store secret information

$s_{ji} \longleftarrow c_{ji} <=> m_i$;

end for

for （i=1;i <=length of secret information ;i++） do;

$m_i \longleftarrow LSB(c_{ji})$;

end for;

//VGA series of carrier image selected by the computer

Sec Addr= 0x00;

FileSecbmp . Seek (SecAddr , CFile,begin) ;

/ / operate each of the bitmap file which is ready for hiding and the first seven bytes of each byte in the source file with XOR. The result is then written as the last one of each byte of the source bitmap file data.

/ / while (fileSecbmp. Read (BufferSecbmp, size of (BufferSecbmp)) = = 1)

{

for (int i= 0; i< 8; i+ +)

{

//set each byte in the bitmap file which is ready for encryption and the corresponding mask to bitwise AND, and the result is stored in the array block SecBit

SecBit[i]= Buffer Secbmp[0] & SecMark[i] ;

// place the indicator aiming at source bitmap at the beginning position of the actual bitmap data

fileResbmp. Seek(ResAddr , CFile,begin);

//write the bytes aimed at by the source bitmap file into array clock BufferResbmp

fileResbmp. Read (BufferResbmp,size of(BufferResbmp));

//extract the result of each byte from the source file and change it into the hexadecimal system, and XOR the high seven bits and get K result for(int j= 0; j< 8; j+ +)

{

if ((((unsignedint) BufferResbmp [0]) &ResMark[j])> 0)

ResBit[j] = 1;

else

ResBit[j] = 0;

}

6. ANALYSIS OF THE EXPERIMENTAL RESULTS

The research of the hiding algorithm put forward in this article developed a kind of applied software of information hiding (Figure 4). The detected information hiding effect through the software is shown in the following parts.

First, choosing the image used for carrier through data selection, and input the data through input/load information module. In order to make the effects comparable, an image comparison model is set, through which the effects before and after the hiding can be examined. Either word, image or text documents can be chosen to hide all kinds of secret document contents. To extract secret information, blind extraction is adopted. Setting a code input in this program, and then we can extract the document information from the carrier inform by correct orders. This software characterizes information security model and it can decrease the possibility of information exposition. Furthermore, it helps enhance the information security management and improve security standards. If secret information is revealed, we can get the revealing proof through secret information and prevent the internal stuff from revealing information deliberately.

When selecting the data from the data source, the program will indicate the user to select the picture as original carrier. The information to be embedded is operated in “embedding data input”. After the program popup menu, we cam input the information to be hidden. We can also find out that the effect of the picture does not change after being hidden (Reported in Figure 5.). As a result, we achieve our final goals.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

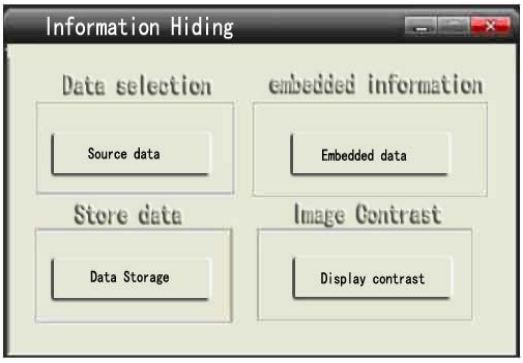

Figure 4: Software Interface

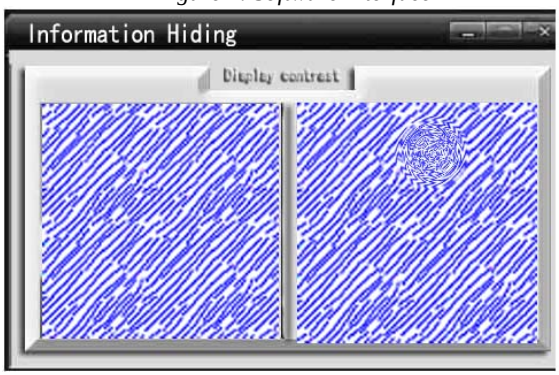

Figure 5: the Picture Effect

The image format that we use is BMP form provided by Microsoft, composed of three parts: BMP title, BMP information and BMP array information.

BMP(Bitmap) title is composed of 14 bytes; BMP information is made of BMP title and palette, of which BMP information is composed of 40 bytes and the size of palette depends on colors. BMP information includes the width, height and size etc. of images.

BMP array information records successively every image data of each image count according to the order of rows.

Table 1 : Table Bitmap Array Information

Compare	Before camouflage	After camouflage
Appearance (no change)		
File Size	264,310 Byte	491,312 Byte
Header of file	Length of the file 0x30431	Length of the file 0x66058
End of file	After the end of the image data file	Office document image data to increase data

For example, given a BMP document with 24 bytes:

01100110, 00111101, 10001111, 00011010, 00000000, 10101011, 00111110, 10110000,

It's odd-even sorting is 0,1,1,1,0,1,1,1. Now 79 is required to be hidden and it is changed into a binary code number 01001111. Comparing with the two sequences, it is found that the third, fourth and fifth number is not consistent. Then we adjust the odd and even byte of the BMP document data and make it consistent with the binary code number of 79.

The third number: change 10001111 into 10001110, and the odd byte is changed into even one.

The fourth number: change 00011010 into 00011011, and the odd byte is changed into even one.

The fifth number: change 00000000 into 00000001, and the even byte is changed into odd one.

After adjustment, the parity of this BMP document is the same as the binary number of 79. As a result, these 8-number bytes hide the information of one byte.

To sum up, the procedure of embedding information into BMP document is as this:

Change the information ready for being hidden into binary data flow. Compare the parity of each byte of BMP document image data with the binary data flow mentioned before. Change the parity of the byte through adjusting the lowest position "0" or "1" to make it consistent with the binary data flow, that is, to embed information into 24-digit BMP images. Information extracting is to extract the hidden information from the impersonation media, which is just the opposite of information embedding:

Firstly, judge the parity of each byte of the BMP document image data. If the number of "1" is even, then output "0"; if the number of "1" is odd, then output "1". To make up a binary number from an 8-digit number every time when 8 bytes are detected (the first output is the highest one). Secondly, obtain a series of 8-digit binary numbers with the above mentioned methods. The numbers are the code of hiding information. If the code is transferred into text, image and sound, the hidden information is obtained.

After the original 24-digit BMP image document is hidden, its byte numerical value's variation is at most 1 (because it is added or subtracted "1" at the lowest number), and the represented color density only varied at most 1/256.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

7. CONCLUSION

With the increasing research in information hiding system and methodology, it is vitally necessary to further estimate the performance of information hiding system and to discuss the basic tests, etc. Reasonable evaluation and basic test of information hiding play an important role in the improvement of the system and its performance. Current research in information hiding technology mainly focuses on information hiding algorithm, which satisfies visual imperceptibility.

From the above analysis, it is proved that the information model based on the information hiding technology can prevent the secret information from leakage, which is helpful for the inside work staff to enhance their management, and to reinforce the safety awareness. The paper is about the research of information hiding technology, which will be of great significance in the future information and network warfare. We firstly need to study information capacity, which decides the application value of the technology, and then enhance the storing capacity on certain carriers. We also need to improve the information hiding algorithm, the study capacity of information embedding and the positioning accuracy. In addition, we also study measurement performance so that we can enlarge information storing capacity.

ACKNOWLEDGEMENTS

This work was supported by Foundation of Guizhou Province Science and Technology . Item Number: J [2012]2020.

REFERENCES

[1] Niculescu D, Nath B, "Ad hoc positioning system (APS) using AOA", *IEEE Computer and Communications Societies*, Vol. 3, No.11, 2003, pp. 1734-1743.

[2] Yaman, R., Gethin, D.T., and Clarke, M.J., "Effective sorting method for facility layout construction", *International Journal of Production Research*, Vol. 31, No. 2, 1993, pp. 413-427.

[3] Balakrishnan, J., Cheng, C.H., and Conway, G., "An improved pair-wise exchange heuristic for the dynamic plant layout problem", *International Journal of Production Research*, Vol. 38, No.13, 2000, pp. 3067-3077.

[4] Baykosoglu, A. Gindy, N.N.Z., "A simulated annealing algorithm for dynamic facility layout problem", *Computers and Operations Research*, Vol. 28, No.8, 2001, pp. 1403-1426.

[5] Dorigo, M., Maniezzo, V., Colorni, "The Ant System: Optimization by a Colony of Cooperating Agents", *IEEE Transactions on Systems, Man, and Cybernetics-Part B*, Vol. 26, No. 1, 1996, pp. 29-41.

[6] Rajagopal Iyengar, Biplab Sikar, "Scalable and distributed GPS free positioning for sensor Networks", Proceeding of IEEE Intel Conference, IEEE Computer Society, February 10-15, 2003, pp. 338-342.

[7] J. T. Brassil, S. Low, N. F. Maxemchuk , "Copyright protection for the electronic distribution of text documents", *Proceedings of IEEE*, Vol. 12, No. 12, 1999, pp. 1181-1196.

[8] D. Huang, H. Yan, "Inter word distance changes represented by sine waves for watermarking text images", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 3, No. 11, 2001, pp. 1237-1245.

[9] V. RodoPlu, T. H. Ming, "Minimum Energy Mobile Wireless Networks", *IEEE Journal of Selected Areas in Communications*, Vol. 17, No. 8, 1999, pp. 1333-1344.