The Design and Implementation of Encryption and Decryption Methods Based on Dynamic Conversion Table

Xiangzhen He, Xianghe Meng, Junsheng Xiao, and Fucheng Wan

***Abstract*—With the development of computer network technology, the security network information has been subject to widespread concern, and selecting the encryption of certain information has become a method frequently used. In this paper, there is a kind of encryption and decryption strategy of character replacement based on dynamic conversion table. The video path on the website as an example to carry on the analysis, and the result is the show of the browser address bar are the path information encrypted, when the user to watch video. This can effectively improve the security of the video resource in website.**

***Index Terms*—Encryption, decryption, dynamic conversion table.**

I. Introduction

The Internet technology and the Internet users in the rapid development, at present, the people use a variety of methods to ensure the security of network information [1]. The information encryption, decryption process become one of the most commonly means. There are displacement method and shift method in the common information encryption and decryption method. This paper puts forward methods is a kind of displacement method, where it use dynamic conversion table in the character displacement. There are the following three characteristics: the number of groups randomly determined in the table; the characters randomly determined in the group; the corresponding operand number randomly determined in each group [2]. How to deal with the specific information for encryption and decryption, this paper is going to elaborate.

II. The Algorithm Principle

The algorithm is characters displacement encrypting and deciphering algorithm based on a dynamic conversion table. The algorithm principle will be generated and maintained a dynamic conversion table, when the software restarts every time [3]. In the encryption of string, the software traverse each character of the plaintext and find the group of Numbers and the corresponding operation number in the dynamic conversion table. Finally it selects a kind of operator to process the operand and achieves encryption of string.

The specific steps of encryption:

1) The initialization of character array and operand array. The data in the array can be ordered, also can be disordered in their initialized state;

2) To determine the number of the group in the dynamic conversion table;

3) According to the array of characters and operands, the software dynamically generates the two sets of random sequence;

4) Using two sets of random sequences generated by the last step, the software respectively read the corresponding data from the array of characters and operands, and generates a dynamic conversion tables. The format of the dynamic conversion table is shown in Table I.

TABLE I: The Dynamic Conversion Table

The number of group	The characters in group	The operand
group 1	char11, char12, … , char 1m	operand 1
group 2	char21, char22, … , char 2m	operand 2
group 3	char31, char32, … , char 3m	operand 3
…	…	…
group n	charn1, charn2, … , char nm	operand n

5) This is a process about encryption process of relative path. Reading the string of the original path, namely "plaintext", and removing path every character in turn, then the algorithm perform the following operation: First the algorithm will traverse every character of the “The characters in group” column in the dynamic conversion table and record the number of the group where the current character. Then to get the operand related the group through the number of group and to select an operator combined with the decided operand to encrypt the current character. Finally, it will combine the encrypted character, which can generate an encrypted string, called "ciphertext".

This is a process about decryption process of relative path. In essence, the process is the inverse operation of the encryption process. The methods used in this paper will sequentially record each the number of the group where operand in each character of the encrypted path, in the realization path encryption. Then, the software traverses each character in the ciphertext, and makes the following operation: to get the operand corresponding group to execute the inverse operation of the encryption process with the current characters, and then to combine every character of the decryption. After the end of the process, you can get string of the original path (plaintext).

Manuscript received October 5, 2012; revised January 9, 2013. This work was supported in part by the National Key Technology R&D Program (Grant No.2009BAH41B01), the project of Central College Scientific Research Fund of Northwest University for Nationalities (Grant NO. ZYZ2011099) and Key Lab of Chinese National Linguistic Information Technology Open Projects in Northwest University for Nationalities (Grant NO. 2012KF005).

The authors are with Key lab of China’s National Languages Information Technology, Northwest University for Nationalities,730030, Lanzhou Gansu, China (e-mail: 5967148@qq.com, mxh1114@163.com, 1033763620@qq.com, 306261663@qq.com).

III. The Analysis of Specific Instance

When the network users to browse the video site, if the address bar of browser shows relative path stored in the server about the current video, it will lead to the video stored in the web server will be free to download. Here, this paper takes relative video path of address bar in the browser as an object of study. The hypothetical premise conditions: this relative video path are not included Chinese. (Such as: … / Users/Desktop / 1. mp4).

By analysis, to determine parameters of the following types:

1) The first is the type and number of the elements in the character array, wherein including elements: "a to z", "A to Z", "0 to 9", "." and "/". The statistics draw that the number of elements is 64;

2) The second is the number of groups in the conversion table, here determines 16. At the same time also can be determined 4 that each group contains the number of characters. Here, the user can customize the number of groups, but due to the changes in the number of group will lead to changes in the number of elements in the group, and changes in the number of operands and the operator;

3) The third is the type and number of the elements in the operand array, wherein including elements: -11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3 and 4. Here a total of 16. Here to determine the range of elements according to the type of operator.

4) The forth is the select of mathematical operator. The selection in the present instance is "+". The selection of the mathematical operator can be combined with the selection of operand.

The dynamic conversion table that generated in the encryption process shows in Table II. The string of relative video path before the algorithm encrypt is "…/Users/Desktop/1.mp4", while the string of the path after the algorithm encryption: 22RUshgsR@hscpieR ×2pe.

TABLE II: The Dynamic Conversion Table in Specific Instance

The number of group	The characters in group				The operand
1	k	v	A	9	-8
2	Z	8	a	1	-7
3	M	Y	/	w	-10
4	f	C	6	R	1
5	m	e	i	B	3
6	h	0	d	g	-1
7	L	O	E	P	-3
8	N	4	o	I	-6
9	s	U	z	X	0
10	b	c	x	2	2
11	r	u	T	p	-11
12	n	5	H	W	-5
13	l	3	G	V	-2
14	D	t	y	F	-4
15	j	K	J	.	4
16	Q	q	7	S	-9

Here is the source code in encryption function:

```
private String encryptHandle(String tem){
   String sc="";
   //record the string after the encryption
   int operate=0;//record the current operator
   int lc=0;      //record the current character
   char [] ch=new char[tem.length()];
   //record all the characters
   for(int i=0;i<tem.length();i++){
      ch[i]=tem.charAt(i);
   }
   for(int i=0;i<ch.length;i++){
      operate=0;
      lc=ch[i];
      for(int m=0;m<16;m++){
      //m is the number of group
         for(int n=0;n<4;n++){
            if(table1[m][n]==lc){
            //table1 is character array
               operate=table2[m];
               //table2 is operand array
               break;
            }
         }
      }
      lc=lc+operate;
      //realize encryption of character displacement
      sc+=String.valueOf((char)lc);
       //combined the character after encryption
   }
   return sc; //return the ciphertext string
}
```

The section of the code gives a framework of encryption algorithm, and each key statement has a corresponding comment. It can be seen that the one core section of the code is two kinds of character array: table1 and table2, the other one core section is the encryption process for the character. The above code segment use "+" which is a kind of relatively simple operation mode. Here, the user can use the more complex operator, according to actual situation.

IV. The Scalability of Algorithm

The algorithm proposed in this paper has good scalability. The multi-level encryption is a specific extension application in all of application. The processes that the original strings use this algorithm to execute multi-level encryption show in Fig. 1. The principle of encryption is that the algorithm will take the last-level output string after encryption as the next-level input string before encryption and perform the next-level encryption. In this process, the algorithm will only need to maintain a respective dynamic conversion table in every level of encryption stage. The encryption process is consistent in every level. The string after multi-level encryption in the difficulty of deciphering will higher, therefore this algorithm also has a higher security [4].

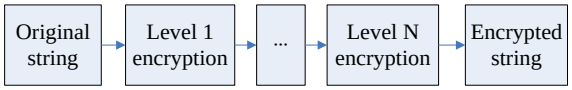

Fig. 1. The process of multi-level encryption

In addition, the method mentioned in this paper applied to string sequence of character variables which consist of letters, numbers and other characters; it can also be extended and applied this encrypted thinking of the algorithm to other string sequence, such as pure Chinese characters string, a mixed string of Chinese characters and letters.

V. Conclusion

At present, this paper proposed encryption method has the following features: the first is the dynamic conversion table in this algorithm, not only each element and the number of groups in the table are randomly determined, but the operand and operator also can be randomly selected. It is randomness that is very strong. The second is that this dynamic conversion table can be dynamically updated. It will produce and maintain a new conversion table in the software each run, and realize real-time update. The realization of the above two points can greatly reduce the opportunity of success by using the dictionary data matching. It is play better protection role in the security of network information. People often use treatment, storage, and the data of the complexity to measure encryption/decryption performance of the algorithm [5]. If decoding an algorithm cost is greater than the value of the data itself or decoding algorithm need time than the encrypted data security for a long time, etc., it prove that the algorithm is secure.

References

[1] T. Wade and L. C. Washington, *The Cryptography Introduction*, Beijing: People's Posts and Telecommunications Press, 2004, pp. 56-59.
[2] X. J. Li, "The pure software encryption method for a web application system," *Information Security and Confidentiality of Communications*, vol. 6, pp. 25-27, 2008.
[3] M. Z. Xu and L. Yu, *The Information Security and Cryptography*, Beijing: Tsinghua University Press, 2007, pp. 121-132.
[4] B. J. Zhang, *The Computer Security and Protection Technology*, Beijing: China Machinery Press, 2005, pp. 112-118.
[5] M. X. He and P. Z. Fan, "The new generation of private key encryption standard AES advances and comments on computer applications," *Application Research of Computers*, vol. 10, pp. 4-6, 2001.

Xiangzhen He was born in 1977. He mainly engaged in the Tibetan language information processing and Internet application development since 2000, currently working for the China national information technology institute in the Northwest University for Nationalities, with many years of computer teaching and practice experience, and has published more than 10 articles on Tibetan information processing till date.