



(51) International Patent Classification:
G06F 1/00 (2006.01)

(21) International Application Number:
PCT/CN2013/088087

(22) International Filing Date:
28 November 2013 (28.11.2013)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: THOMSON LICENSING [FR/FR]; 1-5 rue
Jeanne d'Arc, F-92130 Issy-les-Moulineaux (FR).

(72) Inventors: YU, Qianlong; 8th Floor, Building A, Techno-
logy Fortune Center, No.8 Xueqing Road, Haidian District,
Beijing 100192 (CN). WEI, Zhengdong; 8th Floor, Build-
ing A, Technology Fortune Center, No.8 Xueqing Road,
Haidian District, Beijing 100192 (CN). DING, Qijun; 8th
Floor, Building A, Technology Fortune Center, No.8
Xueqing Road, Haidian District, Beijing 100192 (CN).

(74) Agent: LIU, SHEN & ASSOCIATES; 10th Floor, Build-
ing 1, 10 Caihefang Road, Haidian District, Beijing
100080 (CN).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM,
ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: METHOD AND DEVICE FOR PROTECTING USER INPUT

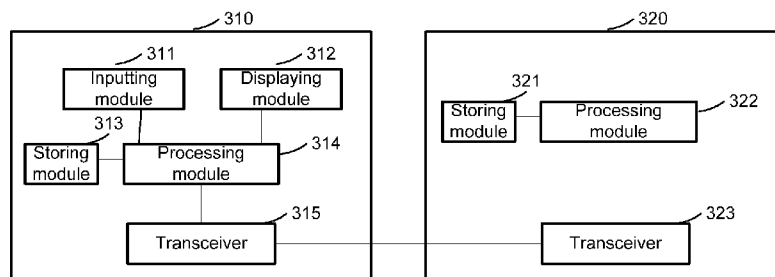


Figure 3

(57) Abstract: It is provided a method for protecting at least one character, wherein at the side of a user device comprising the steps of: receiving at least one inserting character and at least one inserting position for the at least one inserting character; receiving the at least one character; determining at least two characters consisting of the at least one character with the at least one inserting character inserted into the at least one inserting position; and transmitting the at least two characters.

METHOD AND DEVICE FOR PROTECTING USER INPUT

TECHNICAL FIELD

The present invention relates to data processing, and more particularly
5 relates to a method and a device for protecting user input.

BACKGROUND

A password is a secret word or string of characters used for user authentication to prove identity or access approval to gain access to a resource
10 (example: an access code is a type of password), which should be kept secret from those not allowed access.

In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs),
15 etc. A typical computer user has passwords for many purposes: logging into accounts, retrieving e-mail, accessing applications, databases, networks, web sites, and even reading the morning newspaper online. In the context of computer, a character refers to any sign or symbol that is able to be outputted by the keyboard, including alphabetic symbol (e.g. A, a, B, b, C ...etc.), digital
20 symbol (e.g. 1, 2, 3, and 4 ...etc.) and other type of symbols (e.g. @, \$, %, & ...etc.).

It is desired a secure way to protect user input.

SUMMARY

25 According to an aspect of the present invention, it is provided a method for protecting at least one character, wherein at the side of a user device comprising the steps of: receiving at least one inserting character and at least one inserting position for the at least one inserting character; receiving the at least one character; determining at least two characters consisting of the at least

one character with the at least one inserting character inserted into the at least one inserting position; and transmitting the at least two characters.

Further, the method comprises: presenting an inputting area, in which the at least one inserting character is entered automatically in the at least one inserting position and vacant positions are left for receiving the at least one character;
5 and presenting the at least one character in the vacant positions sequentially upon reception of the at least one character.

Further, the method comprises: masking the at least one inserting character and the at least one character with a same character.

10 According to another aspect of the present invention, it is provided a method for protecting at least one character, wherein at the side of a server comprising the steps of: generating at least one inserting character and at least one inserting position for the at least one inserting character; receiving at least two characters; if determining character of the at least two characters located in
15 the at least one inserting position is identical to the at least one inserting character, obtaining the at least one character from the remaining positions of the at least two characters.

Further, in the method, the at least one inserting character and the at least one inserting position vary each time the generating step is carried out.

20 According to another aspect of the present invention, it is provided a user device for protecting at least one character, wherein comprising an inputting module for receiving input of characters; a transceiver for transmitting and receiving data; a processing module for 1) receiving at least one inserting character and at least one inserting position for the at least one inserting
25 character via the inputting module or the transceiver; 2) receiving the at least one character via the inputting module; 3) determining at least two characters consisting of the at least one character with the at least one inserting character inserted into the at least one inserting position; and 4) transmitting the at least two characters via the transceiver.

Further, the user device comprises a displaying module for presenting information; wherein, the processing module is further used for instructing the displaying module to present an inputting area, in which the at least one inserting character is entered automatically in the at least one inserting position and vacant positions are left for receiving the at least one character; and to present the at least one character in the vacant positions sequentially upon reception of the at least one character.

Further, in the user device, the processing module is further used for masking the at least one inserting character and the at least one character with a same character.

According to another aspect of the present invention, it is provided a server for protecting at least one character, wherein comprising a transceiver for transmitting and receiving data; a processing module for generating at least one inserting character and at least one inserting position for the at least one inserting character; receiving at least two characters via the transceiver; and if determining character of the at least two characters located in the at least one inserting position is identical to the at least one inserting character, obtaining the at least one character from the remaining positions of the at least two characters.

Further, in the server, the processing module is further used for generating at least one different inserting character and at least one different inserting position.

It is to be understood that more aspects and advantages of the invention will be found in the following detailed description of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this application, will be used to illustrate an embodiment of the invention, as explained by the description. The invention is not limited to the embodiment.

In the drawings:

Fig. 1 is a diagram showing a form for a user to input his account information according to the prior art;

Fig. 2 is a diagram showing the resulting string of characters after insertion
5 of scrambling characters according to an embodiment of the present invention;

Fig. 3 is a diagram showing a system for protecting user input according to the embodiment of the present invention;

Fig. 4 is a flow chart showing a method for protecting the user input according to the embodiment of the present invention;

10 Fig. 5 is a diagram showing the returned web page after the user sends the request for signing in according to the embodiment of the present invention;

Fig. 6 is a diagram showing the returned web page after the user sends the request for signing in according to the embodiment of the present invention; and

Fig. 7 is a diagram showing that the present invention is applied for
15 protecting characters of the user name according to the embodiment of the present invention.

DETAILED DESCRIPTION

The embodiment of the present invention will now be described in detail in
20 conjunction with the drawings. In the following description, some detailed descriptions of known functions and configurations may be omitted for clarity and conciseness.

In some existing password-protection solutions, the password is transmitted as plain text without encryption. So the password becomes apparent when it is
25 intercepted or snooped. Even if the password is encrypted, the encrypted code is still able to be decrypted to plain text by using a same or corresponding decryption algorithm. Fig. 1 is a diagram showing a form for a user to input his account information according to the prior art. Normally, the inputted characters in the text box of the password are masked with a unified symbol, e.g. asterisk.
30 But the characters are still capable of being detected with some techniques.

In the present invention, the password is scrambled by inserting random characters in random positions. So the password is still kept secret even if the content in the text box of the password is intercepted by other people. Specifically, one or more scrambling characters are randomly generated and assigned with randomly generated positions. The random positions indicate the insertion positions in the password for the scrambling characters. Fig. 2 is a diagram showing the resulting string of characters after insertion of scrambling characters according to an embodiment of the present invention. For the convenience of description, 1) the password is "123456789"; 2) all scrambling characters are "a", "b", "c", "d" and "e"; and 3) characters in the text box of the password are not masked with asterisk. As can be seen from the diagram, the random positions for "a", "b", "c", "d" and "e" are 3, 5, 6, 8 and 9, and the resulting string of characters are "12a34b5c67d8e9". Even if the resulting string of characters is intercepted, the hacker can't recover the password of the user.

Fig. 3 is a diagram showing a system for protecting user input according to the embodiment of the present invention. The system comprises a server 320 and a client device 310.

The client device 310 comprises the following components:

--an inputting module 311: it is used to receive user inputs. It is implemented by using at least one of the following: keyboard, remote controller, touch pad and touch screen.

--a displaying module 312: it is used to display or prompt information to the user. It is implemented by using at least one of the following: display or touch screen.

--a storing module 313: it is used to temporarily or permanently store data. It is implemented by using at least one of the following: volatile storage and non-volatile storage.

--a processing module 314: it is used to process data, access data on the storing module 313, receive data from the inputting module 311 and instruct the

displaying module 312 to display data. It is implemented with Central Processing Unit (CPU). And

--a transceiver 315: it is used to transmit and receive data. It is implemented by using at least one of the following: wired interface, e.g. cable and wireless interface, e.g. Wi-Fi, WiMAX etc.

The server 320 comprises the following components:

--a storing module 321: it is used to temporarily or permanently store data. It is implemented by using at least one of the following: volatile storage and non-volatile storage.

--a processing module 322: it is used to process data, access data on the storing module 321. It is implemented with Central Processing Unit (CPU). And

--a transceiver 323: it is used to transmit and receive data. It is implemented by using at least one of the following: wired interface, e.g. cable and wireless interface, e.g. Wi-Fi, WiMAX etc.

Fig. 4 is a flow chart showing a method for protecting the user input according to the embodiment of the present invention. Because the method is described in the context of signing in operation of a user account in a web site, a person skilled in the art knows that some steps below are redundant when the present invention is implemented in other context. The method comprises the following steps.

In the step 401, the processing module 314 of the user device transmits a request for a signing in web page to the server 320 via transceiver 315. Upon receiving the request, the processing module 322 of the server generates at least one scrambling characters and the same number of positions for all scrambling characters, and transmits the scrambling characters and positions to the user device 310. Meanwhile, the processing module 322 of the server stores the scrambling characters and positions into the storing module 321 for the requesting user device. Besides, the processing module 322 stores the correspondence relationship between the user device and the information about scrambling characters and positions. As an exemplary implementation, it is a

table having two fields. One field is identifier of the user device that uniquely identifies the user device, e.g. device ID, combination of IP address and port number etc. The other field is the scrambling characters and their positions.

In the step 402, the processing module 314 of the user device receives the scrambling characters and their positions via the transceiver 315. It stored the received information in the storing module 313.

In the step 403, the processing module 314 of the user device receives the resulting string of characters, i.e. characters of user password with the scrambling characters inserted into the predetermined positions. Below shows two approaches for inputting the resulting string of characters. The first one is that the information about the scrambling characters and their positions is shown in the signing in web page. Fig. 5 is a diagram showing the returned web page after the user sends the request for signing in. Then the user uses the inputting module 311 to input the resulting string manually. The other one is that the scrambling characters are inserted into their predetermined positions before the user inputs the password. Fig. 6 is a diagram showing the returned web page after the user sends the request for signing in. The vacant positions are left for the user to input the password. As can be seen from the diagram, two vacant positions before "a", two vacant positions between "a" and "b", one vacant position between "b" and "c", two vacant positions between "c" and "d", one vacant position between "d" and "e" are reserved. In the above example, the scrambling characters are in the plain text form. In a variant, they are masked with asterisk.

In the step 404, the processing module 314 of the user device transmits the resulting string to the server. Upon receiving the resulting string, the processing module 322 of the server determines the characters of password based on the resulting string and the stored information about the scrambling characters and their positions. For example, the server compares the generated scrambled characters with characters located in the generated positions in the resulting string. If all comparisons indicate identical, then the server obtains characters in

the remaining positions in the resulting string. Taking the Fig. 5 for example, the server compares characters located in the 3rd, 5th, 6th, 8th and 9th positions in the resulting string with the scrambling characters. If the characters located in the 3rd, 5th, 6th, 8th and 9th positions in the resulting string are "a", "b", "c", "d" and "e" (which means identical), then the server obtains the remaining characters located in the remaining position so as to generate the string that is protected.

According to the present embodiment, the present invention is described in the context of password. However, the present invention is not limited to password. It can be used to protect other kinds of character strings by scrambling them with randomly generated characters and positions. Fig. 7 is a diagram showing that the present invention is applied for protecting characters of the user name.

According to the present embodiment, the random positions indicate the positions associated with the characters of the password. In a variant, the random positions indicate positions in the resulting string of characters. Referring to the Fig. 6, positions of the scrambling characters "a", "b", "c", "d" and "e" in the resulting string are 3, 6, 8, 11 and 13.

Below shows a source code in C programming language for generating the scrambling characters and positions.

```
20      [0001]    /*  
      [0002]        This is a C example code to demonstrate password protection  
      [0003]    */  
      [0004]  
      [0005]    #include "stdio.h"  
25      [0006]    #include "stdlib.h"  
      [0007]    #include "string.h"  
      [0008]  
      [0009]    /*The range of user password length is predefined. The length of  
      user password must inside this range*/  
30      [0010]    #define MIN_PASSWORD_LENGTH 8
```

```

[0011]  #define MAX_PASSWORD_LENGTH 16
[0012]
[0013]  int main(int argc, void* argv)
[0014]  {
5    [0015]      char *position_array;
[0016]      unsigned int max_position_length, random_position_length;
[0017]      unsigned      int      i,available_random_position,random_data,
random_position;
[0018]
10    [0019]      printf("\nPassword          Protection          DEMO
(%s,%s).\n\n",__DATE__,__TIME__);
[0020]
[0021]      max_position_length = 25;
[0022]      if(max_position_length<MAX_PASSWORD_LENGTH){
15    [0023]          printf("ERROR!      max_position_length      must      >=
MAX_PASSWORD_LENGTH\n");
[0024]      }
[0025]
[0026]      /*The redundant positions between max position length and max
20    user password
[0027]      length can be used as max random position length safely*/
[0028]      srand( time(NULL) );
[0029]      random_position_length      =      rand()%(max_position_length-
MAX_PASSWORD_LENGTH);
25    [0030]
[0031]      printf("MIN_PASSWORD_LENGTH
= %d.\n",MIN_PASSWORD_LENGTH);
[0032]      printf("MAX_PASSWORD_LENGTH
= %d.\n",MAX_PASSWORD_LENGTH);

```

```

[0033]     printf("MAX_POSITION_LENGTH
= %d.\n",max_position_length);
[0034]     printf("RANDOM_POSITION_LENGTH
= %d.\n\n",random_position_length);
5   [0035]     printf("Generate random position with random character:\n");
[0036]
[0037]     position_array = malloc(max_position_length);
[0038]     memset(position_array,0,max_position_length);
[0039]
10  [0040]     available_random_position  =  random_position_length  +
MIN_PASSWORD_LENGTH;
[0041]     if(available_random_position>max_position_length)
available_random_position=max_position_length;
[0042]
15  [0043]     srand( time(NULL) );
[0044]     for(i=0; i<random_position_length; i++){
[0045]         for(;;){
[0046]             random_position
=
rand()%available_random_position;
20  [0047]             if(position_array[random_position]==0){
[0048]                 for(;;){ /*Generate a random character*/
[0049]                     random_data = rand()%126; /* In ASCII table, 126='~'
is the max printable ASCII*/
[0050]                     if(random_data>=33) break; /* In ASCII table, 33='!' is
25  the min printable ASCII(except space)*/
[0051]                 }
[0052]                 position_array[random_position]  =
(char)random_data;
[0053]                 break;
30  [0054]             }

```

```

[0055]         }
[0056]     }
[0057]
[0058]
5   [0059]     for(i=0;i<max_position_length;i++){ printf("_____");}
[0060]     printf("_____\\nRESULT: ");
[0061]
[0062]     for(i=0;i<max_position_length;i++){
[0063]         if(position_array[i]){
10  [0064]             printf("[%c]",position_array[i]);
[0065]         } else {
[0066]             printf("[ ],",position_array[i]);
[0067]         }
[0068]     }
15  [0069]     printf("\\nINDEX : ");
[0070]
[0071]     for(i=0;i<max_position_length;i++){ printf(" %02d",i+1);}
[0072]     printf("\\n");
[0073]
20  [0074]     for(i=0;i<max_position_length;i++){ printf("----"); }
[0075]     printf("-----\\n");
[0076]
[0077]     free(position_array);
[0078]
25  [0079] }

```

Below is the explanation of the source code.

1. Normally the min (minimum) and max (maximum) length of user password are predefined by the web site (lines 10 and 11 in C code).
2. We need define the max position length(line 21 in C code).

The max position length must large than the max user password length.

3. Then we can generate the random position length(line 29 in C code).

5 The redundant positions between max position length and max user password length can be used as random position length safely.

4. We can allocate a character array as the data structure to store the random position and random character(line 37 in C code).

5. Then we can generate the random position(line 44/45/46/47/52 in C code).

10 5.1 Generate a random number(line 46 in C code).

5.2 Get the modulus of the random number and the random position length. (line 46 in C code).

Then we can get a number between 0 and random position length, and we can take this number as the random position.

15 5.3 Check if the new position generated is available(line 47 in C code).

5.4 If the new position is not available, repeat from 5.1(line 45 in C code).

5.5 If the new position is available, generate a random character and fill this position(line 48/49/50/52).

20 6. Generate the random character(line 48/49/50)

6.1 Generate a random number(line 49 in C code).

6.2 Get the modulus of the random number and number 126. (line 49 in C code).

Number 126 is the number of max printable ASCII.

25 We can get a number between 0 and max printable ASCII number in this step.

6.3 Check if the new number generated is equal or large than 33 (line 50 in C code).

30 If it is equal or large than 33, that means we find an available random character, otherwise we need repeat from 6.1.

Number 33 is the number of min printable ASCII.

According to a variant of the present embodiment, the present invention is applied to other technical fields, for example, in electric security token, mobile
5 phone short message validation etc.

According to another embodiment of the present invention, it is used in electric security token.

Traditionally, the electric security token works in the following manner.

1. A server and the token generate a pseudo random key (consisting of
10 characters) independently.
2. The token provides the random key to a user.
3. The user is required to input their password as well as the random key.
4. The server checks the random key first. If it is ok, then the server checks the user password.

15 In the above process, the user password input in step 3 is in plain text form.

The process is improved by applying the present invention in the following manner.

1. A sever and a token generate pseudo random positions and key independently.
- 20 2. The token provides the positions and random key to a user.
3. The user is required to input their password in the format provided by token.
4. The server checks the positions and key first. If it is ok, then the server filters out and checks the user password.

25 In the process, the user password input in step 3 is scrambled.

According to another embodiment, the present invention is applied to short message validation.

Currently the application of short message validation code is in this process:

1. A sever generates a random key.
- 30 2. The sever delivers the random key to a user by a short message.

3. The user is required to input their password together with the random key.
4. The server checks the random key and the user password.

In this process, the user password input in step 3 is in plain text form.

The improved process after applying the present invention is as follow.

- 5 1. A sever generate positions and random key.
2. The server delivers the positions and random key to a user by a short message.
3. The user is required to input the password in the format provided by the short message.
- 10 4. The server checks the positions and random key first. If it is ok, then the server filters out and checks the user password.

In this process, the user password input in step 3 is scrambled.

A number of implementations have been described. Nevertheless, it will be understood that various modifications may be made. For example, elements of
15 different implementations may be combined, supplemented, modified, or removed to produce other implementations. Additionally, one of ordinary skill will understand that other structures and processes may be substituted for those disclosed and the resulting implementations will perform at least substantially the same function(s), in at least substantially the same way(s), to achieve at
20 least substantially the same result(s) as the implementations disclosed. Accordingly, these and other implementations are contemplated by this application and are within the scope of the invention as defined by the appended claims.

CLAIMS

1. A method for protecting at least one character, wherein at the side of a user device comprising:
- 5 receiving at least one inserting character and at least one inserting position for the at least one inserting character;
- receiving the at least one character;
- determining at least two characters consisting of the at least one character with the at least one inserting character inserted into the at least one inserting
- 10 position; and
- transmitting the at least two characters.
2. The method of the claim 1, wherein further comprising
- presenting an inputting area, in which the at least one inserting character is
- 15 entered automatically in the at least one inserting position and vacant positions are left for receiving the at least one character; and
- presenting the at least one character in the vacant positions sequentially upon reception of the at least one character.
- 20 3. The method of the claim 1, wherein further comprising
- masking the at least one inserting character and the at least one character with a same character.
4. A method for protecting at least one character, wherein at the side of a server
- 25 comprising:
- generating at least one inserting character and at least one inserting position for the at least one inserting character;
- receiving at least two characters;

if determining character of the at least two characters located in the at least one inserting position is identical to the at least one inserting character, obtaining the at least one character from the remaining positions in the at least two characters.

5 5. The method of the claim 4, wherein the at least one inserting character and the at least one inserting position vary each time the generating step is carried out.

6. A user device for protecting at least one character, wherein comprising
an inputting module for receiving input of characters;
10 a transceiver for transmitting and receiving data;
a processing module for 1) receiving at least one inserting character and at least one inserting position for the at least one inserting character via the inputting module or the transceiver; 2) receiving the at least one character via the inputting module; 3) determining at least two characters consisting of the at least one
15 character with the at least one inserting character inserted into the at least one inserting position; and 4) transmitting the at least two characters via the transceiver.

7. The user device of the claim 6, wherein further comprising
a displaying module for presenting information;
20 wherein, the processing module is further used for instructing the displaying module to present an inputting area, in which the at least one inserting character is entered automatically in the at least one inserting position and vacant positions are left for receiving the at least one character; and to present the at least one character in the vacant positions sequentially upon reception of the at least one character.

25 8. The user device of the claim 6, wherein the processing module is further used for masking the at least one inserting character and the at least one character with a same character.

30 9. A server for protecting at least one character, wherein comprising

a transceiver for transmitting and receiving data;

a processing module for generating at least one inserting character and at least one inserting position for the at least one inserting character; receiving at least two characters via the transceiver; and if determining character of the at least two
5 characters located in the at least one inserting position is identical to the at least one inserting character, obtaining the at least one character from the remaining positions in the at least two characters.

10. The server of the claim 9, wherein the processing module is further used for
10 generating at least one different inserting character and at least one different inserting position.

User Name:

Password:

Figure 1 (Prior Art)

User Name:

Smith

Password:

1

2

a

3

4

b

5

c

6

7

d

8

e

9

Figure 2

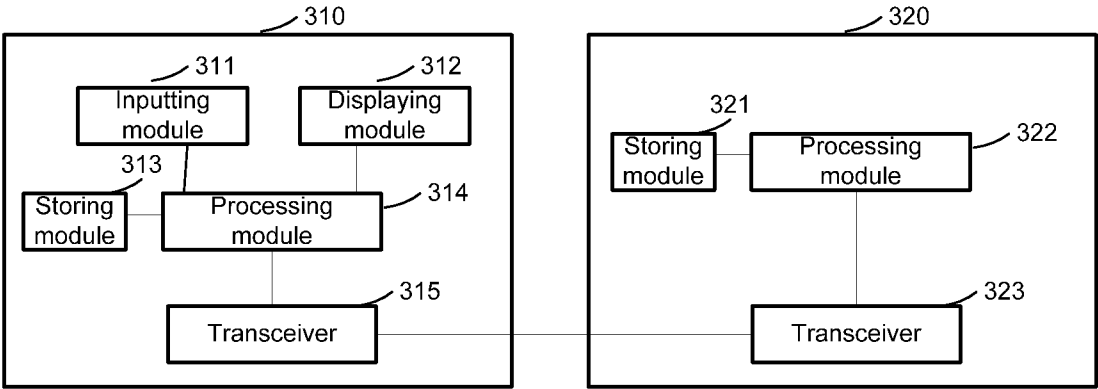


Figure 3

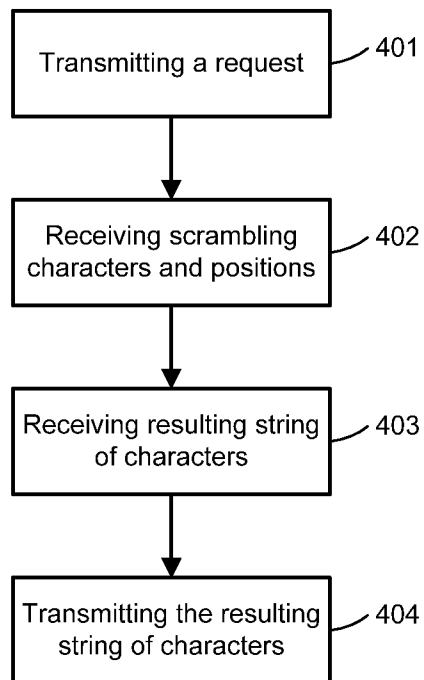


Figure 4

User Name:	
Password:	

Positions of scrambling characters “a”, “b”, “c”, “d” and “e” are 3, 5, 6, 8 and 9

Figure 5

User Name:																					
Password:	<table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;">a</td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;">b</td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;">c</td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;">d</td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;">e</td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;"></td> <td style="width: 15px; height: 20px;"></td> </tr> </table>			a			b		c			d		e							
		a			b		c			d		e									

Figure 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/088087

A. CLASSIFICATION OF SUBJECT MATTER

G06F 1/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 1/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

VEN;CPRSABS;CNABS: password, copher, character, encrypt, insert+, plug+, protect+, secure, scramble, interference, mix

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 1719370A (CHINA MINSHENG BANK CO., LTD.) 11 January 2006 (2006-01-11) description, page 3 paragraph 5 to page 4 paragraph 6	1-10
Y	CN 101702191A (ZHEJIANG DESSMANN MECHANICAL & ELECTRICAL CO., LTD.) 05 May 2010 (2010-05-05) description, paragraphs 9 to 13	1-10
Y	CN 101123454A (UNIV. BEIJING JIAOTONG) 13 February 2008 (2008-02-13) description, page 2 paragraph 7	3, 8
A	CN 1848726A (WANG, YUE) 18 October 2006 (2006-10-18) the whole document	1-10
A	US 2008077978A1 (REPASI, ROLF ET AL.) 27 March 2008 (2008-03-27) the whole document	1-10

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

“A”	document defining the general state of the art which is not considered to be of particular relevance	“T”	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“E”	earlier application or patent but published on or after the international filing date	“X”	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“L”	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“Y”	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“O”	document referring to an oral disclosure, use, exhibition or other means	“&”	document member of the same patent family
“P”	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search

27 June 2014

Date of mailing of the international search report

01 August 2014

Name and mailing address of the ISA/

STATE INTELLECTUAL PROPERTY OFFICE OF THE
P.R.CHINA(ISA/CN)
6,Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088 China

Authorized officer

LI, Yandong

Facsimile No. (86-10)62019451

Telephone No. (86-10)62411735

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/CN2013/088087

Patent document cited in search report		Publication date (day/month/year)	Patent family member(s)		Publication date (day/month/year)
CN	1719370A	11 January 2006	CN	100345078C	24 October 2007
CN	101702191A	05 May 2010	None		
CN	101123454A	13 February 2008	CN	101123454B	20 April 2011
CN	1848726A	18 October 2006	None		
US	2008077978A1	27 March 2008	None		