[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200610046226.0

[43] 公开日 2006 年 8 月 30 日

[11] 公开号 CN 1825796A

[22] 申请日 2006.3.29
[21] 申请号 200610046226.0
[71] 申请人 刘大扬
地址 117000 辽宁省本溪市平山区溪园街 B 座三单元五楼一号
[72] 发明人 刘大扬

[74] 专利代理机构 大连智慧专利事务所
代理人 周志舰 刘 琦

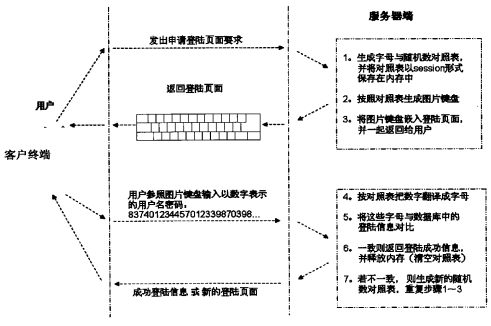
权利要求书 2 页 说明书 6 页 附图 3 页

[54] 发明名称

基于图片键盘的网络加密系统及其操作方法

[57] 摘要

公开了一种实现客户端以身份验证方法加密注册或登陆的系统，以及系统中实现加密、验证的方法。 本发明基于图片键盘的网络加密系统，其操作方法包括，客户终端申请注册或登陆；服务器应答并随机生成每一按键字符与输入码的对照表；根据对照表生成图片格式的软键盘或图片格式的对照表；服务器将图片与注册或登陆页面发送到客户终端；客户终端显示页面，用户根据键盘图片或对照表图片录入注册或登陆验证信息；客户终端将注册或登陆验证信息传送到服务器；服务器参照对照表校验。 本发明能有效防止键盘监听，使被窃取的用户名和密码无效，而且支持短密码，减轻了用户背密码的负担，并且密码无法被机器自动破译，从而提高了现有登陆方式的安全性。



1．一种基于图片键盘的网络加密系统的操作方法，所述系统包括网络互联的服务器以及客户终端，所述客户终端包括显示器和键盘；其特征在于，包括如下步骤：

（S1）所述客户终端通过网络向所述服务器发送申请注册或登陆页面请求;

（S2）所述服务器应答客户终端申请注册或登陆页面的请求，随机生成每一按键字符与输入码的对照表，将对照表存储于存储器中；

（S3）所述服务器根据对照表生成图片格式的软键盘或图片格式的对照表；

（S4）所述服务器将（S3）中的图片以及注册或登陆页面发送到客户终端；

（S5）所述客户终端将注册或登陆页面在所述显示器上显示；所述注册或登陆页面显示所述图片格式的键盘或按键对照表并要求输入包括用户名和密码的注册或登陆验证信息；

（S6）用户根据图片格式的键盘或按键对照表录入注册或登陆验证信息后；所述客户终端将注册或登陆验证信息传送到所述服务器；

（S7）所述服务器对客户终端返回的注册或登陆验证信息参照所述对照表校验；校验的步骤包括：服务器收到客户终端传来的字符串后，按位数分解，在所述对照表中查找对应字符，而后在登陆情况下对比原始注册信息校验。

（S8）根据校验结果，服务器向客户终端发送成功或失败页面或者重新登陆的页面，并删除所述存储器中的所述对照表。

2．根据权利要求 1 所述的操作方法，其特征在于，所述对照表中每一按键字符所对应的输入码为 1 至 8 位，所述输入码为数字、字母、符号或三者的组合。

3．根据权利要求 2 所述的操作方法，其特征在于，所述对照表中每一按键字符所对应的输入码为 2-5 位。

4．根据权利要求 1-3 任一所述的操作方法，其特征在于，所述存储器为内存或硬盘或闪存。

5．一种基于图片键盘的网络加密系统，包括网络互联的服务器以及客户终端，所述客户终端包括显示器和键盘；其特征在于，

所述客户终端还包括一个注册、登陆中央处理模块，通过网络向所述服务器发送申请注册或登陆页面请求，并将注册或登陆页面显示在所述显示器上，

以及将注册或登陆验证信息传送到服务器；所述注册或登陆页面要求输入包括用户名和密码的注册或登陆验证信息以及显示一个图片格式的键盘或按键对照表；

所述服务器包括一个注册、登陆响应中央处理模块，应答客户终端申请注册或登陆页面的请求，随机生成每一按键字符与输入码的对照表；根据对照表生成图片格式的软键盘或图片格式的对照表；将所述图片以及注册或登陆页面发送到客户终端；对客户终端返回的注册或登陆验证信息参照所述对照表校验；向客户终端发送注册或登陆成功、注册或登陆失败或者重新注册或登陆的页面。

基于图片键盘的网络加密系统及其操作方法

技术领域

本发明涉及一种包括服务器端和客户端互联的网络系统，更具体地说，涉及一种实现客户端以身份验证方法加密注册或登陆的系统，以及系统中实现身份加密、验证的方法。

背景技术

在软件尤其是网络安全领域中公知的身份验证方法是使用用户名和密码登录的方法。目前人们采用的一对一的用户名/密码存储与调用机制。但由于密码过短，反破译性不强等原因，经常造成用户的用户名和密码在网上传输过程中被窃取，或被计算机破译。例如使用的密码过短(8 位以下单纯的数字或字母)，计算机使用字典式排查法，通常可以在短时间内试出正确的用户名和密码。一些木马程序也可以通过监听键盘敲击获取密码。

目前解决上述问题的方法如下：

1、使用 8 位以上数字和字母组合的密码。虽然现在的计算机需要长时间来破解这种密码，但随着计算机硬件和并行计算技术的飞速发展，这个时间会越来越短，而且八位以上无规则密码由于较长，用户本人也较难记忆。

2、 密码学家采用一些加密算法(例如: 对称加密, 非对称加密)对网上传输的用户名和密码加密。这些算法只是在一定时间没有找到反推方法时有效，随着研究的进一步深入，每种算法都有被破解的可能。 一旦加密方法被攻击者掌握，这些用户名和密码也就因此被破解。而且研究这些算法需要大量数学尖端人才的投入，耗时耗力，使开发周期和成本增大，而且服务器端、客户终端的计算量较大，增加了设备负担。

3、 一些大型网站采用附加图形码的方法，如验证码方式。此种方法虽可以防止恶意计算机不断验证用户名和密码，但却无法保证被传出的用户名以及密码信息不被截获并破译。

4、一些软件选择了软键盘， 让用户通过鼠标输入的方式， 以避免键盘被监听。但因使用鼠标输入用户名和密码效率太低， 这种方法也不被人们普遍接

受，而且同样无法在传输过程中保护用户名、密码。

发明内容

本发明针对上述问题，提供了一种网络加密系统，该系统由服务器端随机生成图片格式的软键盘发送到客户终端、用户根据图片中的键盘键位输入身份验证信息从而实现加密。该系统及该系统的操作方法解决了如下问题：

1、密码的网上窃取问题——由于服务器传给客户端的是图片， 恶意计算机无法自动从中读取信息。 客户端传回服务器的是字符串， 没有真正的密码，即使这些数字被截取， 由字符也无法推断出密码的内容。

2、字典式攻击问题——由于每次尝试登陆时所采用的对应关系（即二维数组）都是随机生成的， 所以攻击计算机无法采用暴力破解、 字典式攻击等手段对密码进行逐个排查。

3、键盘监听问题——由于用户通过键盘输入的是随机的字符串，这就使键盘监听失去了作用。

4、由于对照表采取的是一个键对应一位或多位随机字符串的原理。以 4 位随机字符串为例，2 位密码通过对应后成为了 8 位密码。这让用户使用短密码保护个人信息成为了可能。

为了解决上述问题，本发明实现了一种基于图片键盘的网络加密系统，包括网络互联的服务器以及客户终端，客户终端包括显示器和键盘；客户终端还包括一个注册、登陆处理模块，通过网络向所述服务器发送申请注册或登陆页面请求，并将注册或登陆页面显示在所述显示器上，以及将注册或登陆验证信息传送到服务器；注册或登陆页面要求输入包括用户名和密码的注册或登陆验证信息以及显示一个图片格式的键盘或按键对照表。服务器包括一个注册、登陆响应处理模块，应答客户终端申请注册或登陆页面的请求，随机生成每一按键字符与输入码的对照表；根据对照表生成图片格式的软键盘或图片格式的对照表；将所述图片以及注册或登陆页面发送到客户终端；对客户终端返回的注册或登陆验证信息参照所述对照表校验；向客户终端发送注册或登陆成功、注册或登陆失败或者重新注册或登陆的页面。

本发明还实现了上述基于图片键盘网络加密系统的加密、验证操作方法，系统包括网络互联的服务器以及客户终端，客户终端包括显示器和键盘；操作方法包括如下步骤：客户终端通过网络向所述服务器发送申请注册或登陆页面

请求；服务器应答客户终端申请注册或登陆页面的请求，随机生成每一按键字符与输入码的对照表，对照表存储于存储器中；服务器根据对照表生成图片格式的软键盘或图片格式的对照表；服务器将所述图片以及注册或登陆页面发送到客户终端；客户终端将注册或登陆页面在显示器上显示，其中，注册或登陆页面显示图片格式的键盘或按键对照表并要求输入包括用户名和密码的注册或登陆验证信息；用户根据图片格式的键盘或按键对照表录入注册或登陆验证信息后；客户终端将注册或登陆验证信息传送到所述服务器；服务器对客户终端返回的注册或登陆验证信息参照对照表校验，校验步骤包括：服务器收到客户终端传来的字符串后，按位数分解，在对照表中查找对应字符，而后在登陆情况下对比原始注册信息校验。而后服务器向客户终端发送成功或失败页面或者重新登陆的页面。该方法由于在服务器随机生成按键与输入码的对应关系，在登陆信息返回后，根据该对应关系校验，从而在服务器端实现双重校验的要求。并采用无规则的“图片键盘”，在一定程度上杜绝了密码的泄漏和破解问题。

优选方式下，在本发明基于图片键盘的网络加密系统的操作方法中，对照表中每一按键字符所对应的输入码为 1 至 8 位，输入码为数字、字母、符号或三者的组合。最优的是，对照表中每一按键字符所对应的输入码为 2-5 位。输入码过多，不便于用户的输入；当输入码为 1 位时，又需要用户牢记较长位数的密码，不便于记忆；因此输入码的位数根据需要确定，优选 2-5 位为益。

在本发明基于图片键盘的网络加密系统的操作方法中，存储对照表的存储器可以是内存或硬盘或闪存以及其他类型实现存储功能的设备。优选内存的方式实现。

通过上述技术方案，本发明具有如下特点：首先采用的是每次登录生成“图片键盘”，用无规则字符去对应密码内容的方法在网上传递数据。 数字与密码的对应关系动态存在于服务器的内存当中，每次客户端重新访问、 超时或关闭客户端， 都会导致服务器端的密码对照表从新生成。由于在客户端与服务器之间传输的是图片和无规则字符，这就从根本上杜绝了密码的泄漏和破解问题。本技术不限于在网络应用程序上应用，单机应用程序也可以采用此方法， 以防止键盘监听。该技术的推广使用将会给网民生活、电子商务、银行信用、网络办公、数据管理、金融结算、网站维护、机要传递、身份确认、国防通讯等带来可靠的安全保证。

本发明不仅可以应用于网络应用程序，也可用于单机程序。不仅能让被窃

取的用户名和密码无效，支持用户原始的短密码，无需牢记冗长的无规则密码，不怕键盘监听，而且密码无法被机器自动破译。从根本上克服了现有的密码在加密和传输过程中易被窃取和破译的问题， 同时也减轻了用户背密码的负担，提高了现有登陆方式的安全性。另外本方法由于从客户终端到服务器的消息无需加密，再配合其它加密方法的前提下，可以提高工作效率，减轻服务器和客户终端的负担。

附图说明

图 1 是本发明基于图片键盘的网络加密系统中的操作流程示意图；

图 2 是本发明基于图片键盘的网络加密系统中的登陆页面示意图；

图 3 是本发明网络加密系统中生成基于图片格式随机软键盘实施例的示意图；

图 4 是本发明网络加密系统中生成另一种基于图片格式随机软键盘实施例的示意图。

具体实施方式

本发明基于图片键盘的网络加密系统，在物理结构上，包括网络互联的服务器以及客户终端，客户终端至少设置了显示器和键盘以及中央处理器、存储器模块。通常情况下，本发明的系统可以基于现有互联网实现的，客户终端为个人电脑。客户终端的处理器是能够执行注册、登陆程序的中央处理模块，它的功能是：通过网络向服务器发送申请注册或登陆页面请求，并将注册或登陆页面显示在显示器上，以及将注册或登陆验证信息传送到服务器；而上述的注册或登陆页面要求用户输入包括用户名以及密码的注册或登陆验证信息以及显示一个图片格式的键盘或按键对照表。而服务器端包括执行注册、登陆响应程序的中央处理模块，其功能是：应答客户终端申请注册或登陆页面的请求，随机生成每一按键字符与输入码的对照表；根据对照表生成图片格式的软键盘或图片格式的对照表；将图片以及注册或登陆页面发送到客户终端；对客户终端返回的注册或登陆验证信息参照对照表校验；向客户终端发送注册或登陆成功、注册或登陆失败或者重新注册或登陆的页面。

参考图 1 所示本发明网络加密系统的操作流程，其过程大致为：

1、客户终端通过网络向所述服务器发送申请注册或登陆页面请求。

2、服务器应答客户终端申请注册或登陆页面的请求，随机生成每一按键字符与输入码的对照表。将对照表存储于存储器中，存储器可以是内存、硬盘或闪存等。该对照为二维对照表，最好以 session 形式存于内存，在具体实现过程中，该 session 可以设定时间限制参数。

该对照表中每一按键字符所对应的输入码为 1 至 8 位，输入码采用数字、字母、符号或三者的组合。参考图 2 所示，上半部显示键盘符号，下半部显示随机数字，对照表的按键对照关系可以是 1 个按键对应 4 位数字，如 Q 对应 8594，W 对应 2281……。当然也可采用图 3 所示一个按键对应 2 位字母与数字的组合，如 Q 对应 a1， W 对应 c3……。还可以是图 4 所示的一一对应关系，如 Q 对应 a， W 对应 c……。在对应关系上，最好一个按键对应 2-5 位字符组合，对应位数过多，不便于用户输入。

3、服务器根据对照表生成图片格式的软键盘或图片格式的对照表。

4、服务器将所述图片以及注册或登陆页面发送到客户终端。

5、客户终端将注册或登陆页面在所述显示器上显示，注册或登陆页面显示图片格式的键盘或按键对照表并要求输入包括用户名和密码的注册或登陆验证信息，如图 2 所示。在注册时通常仅要求用户按照对照表输入用户名、密码，其它注册信息一般无需按输入码输入，同时用户名也无法支持中文。

6、用户根据图片格式的键盘或按键对照表录入注册或登陆验证信息后；客户终端将注册或登陆验证信息传送到服务器。如用户在收到图 2 所示的登陆页面后，在“图片键盘”上查找密码下方对应的随机数字， 将这些数字按顺序输入密码栏，然后提交。

7、服务器对客户终端返回的注册或登陆验证信息参照对照表校验；校验的方法为服务器收到客户终端传来的字符串后，从存储器中找到相应的对照表(由于同时登陆的用户数量不同，对照表的数量有变化，因此需要对照表与要登陆的客户终端相对应)，按位数分解，在对照表中查找对应字符，而后对比数据库的信息校验。例如图 3 所示的，用户输入用户名为 a1c3n5b0 对应真实的用户名为 QWER。而图 4 中，用户输入的密码为 acnbmnpi，则真实密码为 QWERTYUI。随机键盘的对应关系是任意的，每次用户登陆过程中对应输入的按键也就不同，这可以有效的防止键盘的恶意监听。此后，按需要把对应的字符存入数据库(注册时)或与数据库中的数据对比(登录时)，即对比原始注册信息校验。如果对应字符与数据库记录不一致，则返回错误信息提示登陆失败，或者生成新对应关

系的“图片键盘”登陆页面返回客户终端，要求用户重新登陆。当用户名或密码与数据库记录一致时，服务器返回登陆成功的页面并清除存储器中此客户终端相应的对照表信息。

此外，图 1 中显示了服务器响应客户终端请求优选执行的 1-7 步操作，包括：接到客户终端初始请求后生成字母与随机数对照表，并将对照表以 session 形式保存在内存中；按照对照表生成图片键盘；将图片键盘嵌入登陆页面并一起返回给用户。还包括：客户终端返回登陆信息后按照对照表把数字翻译成字母；将这些字母与数据库中的登陆信息对比；一致则返回登陆成功信息，并释放内存（清空对照表）；若不一致，则生成新的随机数对照表，重复客户终端初始请求时的操作。

当然上述图片也可以直接采用对照表形式的图片，应用时随机数可以是数字、字母或数字和字母的组合，只需让用户清楚按键对应关系即可。此外，目前本系统生成的对照表只适用于英文、数字，暂不考虑中文、韩文等其他语言。在网上传递有信息的图片，可以防止恶意计算机自动读取有用信息。在必要情况下，对传输的图片采取水印等图片加密方法，保证图片在传输、显示过程中的安全性。

以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，根据本发明的技术方案及其发明构思加以等同替换或改变，都应涵盖在本发明的保护范围之内。

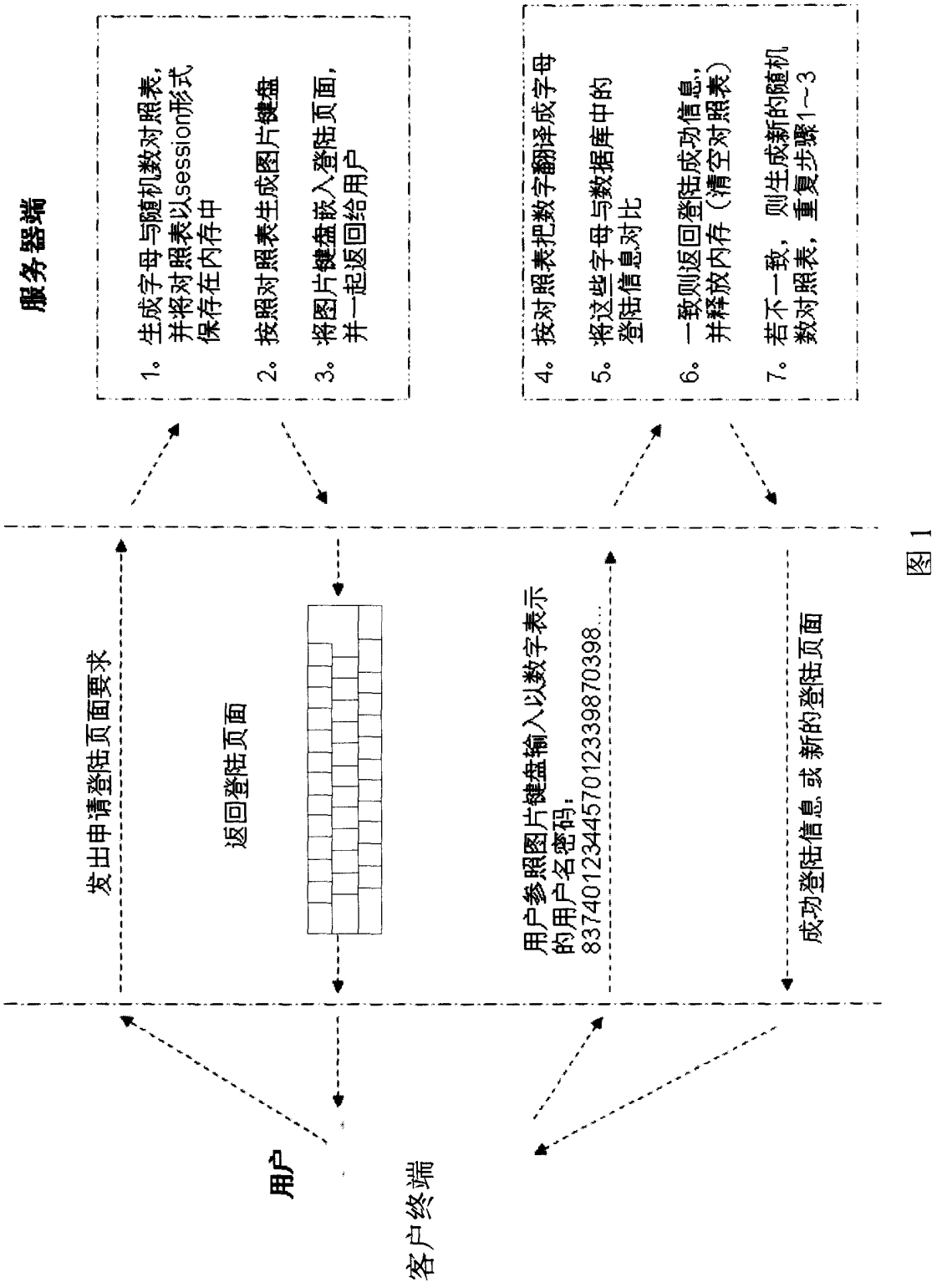

服务器端
1。生成字母与随机数对照表，并将对照表以session形式保存在内存中
2。按照对照表生成图片键盘
3。将图片键盘嵌入登陆页面，并一起返回给用户
4。按对照表把数字翻译成字母
5。将这些字母与数据库中的登陆信息对比
6。一致则返回登陆成功信息，并释放内存（清空对照表）
7。若不一致，则生成新的随机数对照表，重复步骤1～3
发出申请登陆页面要求
返回登陆页面
用户参照图片键盘输入以数字表示的用户名密码：
837401234457012339870398...
成功登陆信息 或 新的登陆页面
用户
客户终端

图 1

登陆页面

Login here
Look at tthe soft keyboard,and enter the number under the key. Username:
837401234457012339870398
Password
447695833987374012344457
Forgot password? Login

Tab	Q 8594	W 2281	E 4628	R 8557	T 7758	Y 4457	U 0293	I 1374	O 9583	P 0498	{ [	}]	
Caps lock	A 0123	S 2843	D 8374	F 3659	G 0398	H 2746	J 2047	K 3374	L 0047	: ;	" '	Enter	
Shift	Z 4906	X 0955	C 4267	V 3048	B 3478	N 3987	M 4476	< ,	> .	? /	Shift	|	

图2

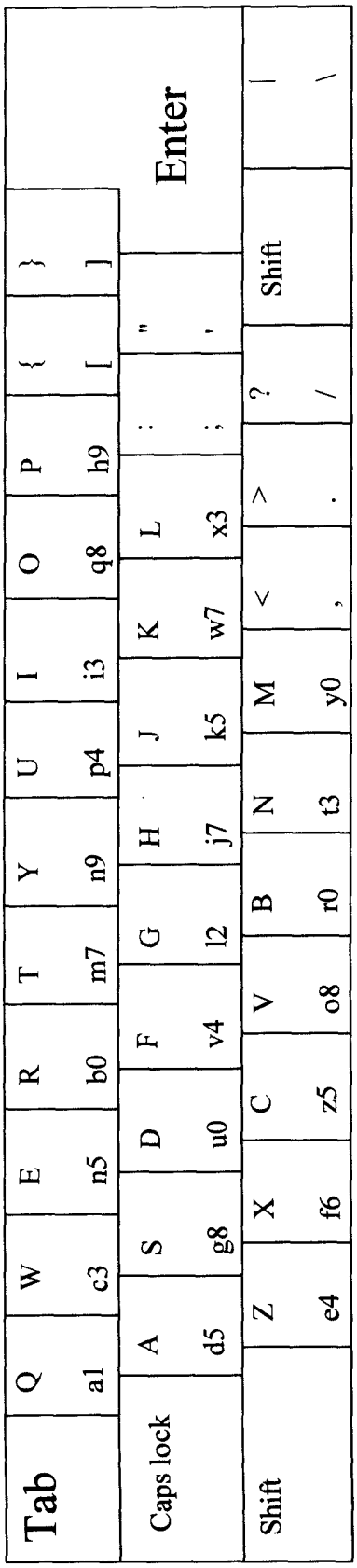

Tab
Q a1
W c3
E n5
R b0
T m7
Y n9
U p4
I i3
O q8
P h9
{ [
}]
Caps lock
A d5
S g8
D u0
F v4
G l2
H j7
J k5
K w7
L x3
: ;
" '
Enter
Shift
Z e4
X f6
C z5
V o8
B r0
N t3
M y0
< ,
> .
? /
Shift
| \

图3

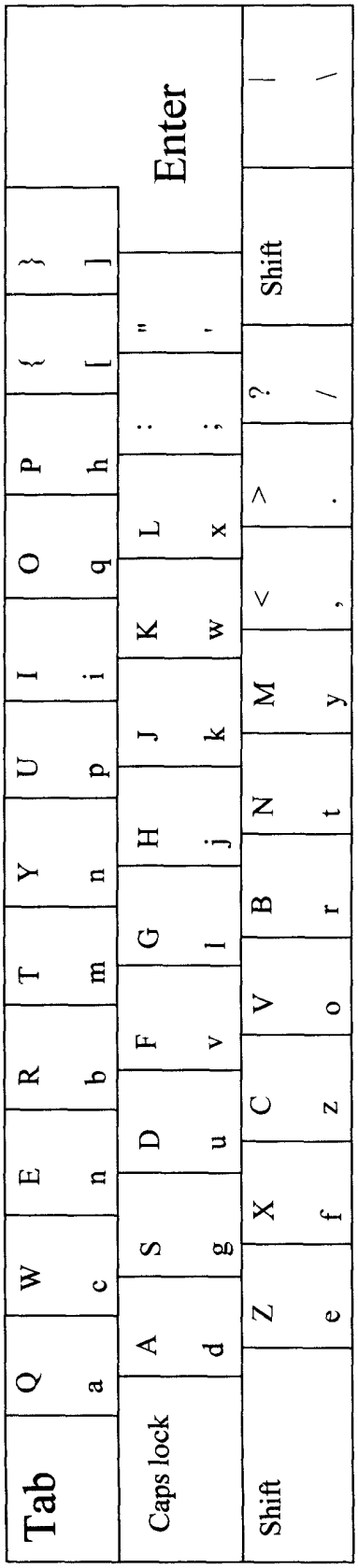

Tab
Q a
W c
E n
R b
T m
Y n
U p
I i
O q
P h
{ [
}]
Caps lock
A d
S g
D u
F v
G l
H j
J k
K w
L x
: ;
" '
Enter
Shift
Z e
X f
C z
V o
B r
N t
M y
< ,
> .
? /
Shift
| \

图4