Industria y Comercio

SUPERINTENDENCIA

Delegatura de propiedad Industrial

División de Nuevas Creaciones

SOLICITUD

PATENTE DE INVENCIÓN

21. **EXPEDIENTE No.** PCT 06-38994

54. **TÍTULO** METODO DE SERVICIO DE CERTIFICACION SEGURA

51. **CLASIFICACIÓN INTERNACIONAL**

71. **SOLICITANTE** SOLMAZE CO., LTD.

DOMICILIO SEOUL - KOREA

74. **APODERADO** JESUS ADELARDO CARDENAS A.

22. **BOGOTÁ, D. C.,** 25-04-06

(FORMA P-10)

PETITORIO

Industria y Comercio
SUPERINTENDENCIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Rad: 08-036994- -00000-0000 Fec: 2005-04-25 15:38:21
Dep: 2020 NUEVAS CREACIONES
Tra: 11 PATENTES II Fol: 378 FABRICACIONAL
Art 411 PRESENTACION Folios: 66

FORMULARIO ÚNICO DE SOLICITUD DE PATENTE
PCT
ENTRADA EN FASE NACIONAL

(1) SOLICITUD DE:

☒ Patente de Invención. ☐ Patente de Modelo de Utilidad.

☒ Capítulo I. ☐ Capítulo II.

(2) SOLICITANTE (71)

Nombre: **SOLMAZE CO., LTD.**

Dirección: **1212, Kolong Digital Tower, 222-7, Guro 3-dong,Guro-gu, Seoul, 152-777**
Nacionalidad o Domicilio: **Seoul**
Lugar de Constitución: **República de Korea**
Teléfono: Fax:

E-mail:

IDENTIFICACION
C.C. ☐ NIT ☐
C.E. ☐ Otro ☐
Cual _____
Número _____

(3) REPRESENTANTE O APODERADO (74)

Nombre: **JESUS ABELARDO CARDENAS A.**

Dirección: **Carrera 7 No. 74-56 Oficina 804**

Teléfono: **3131652, 3132414** Fax: **3131713**
E-mail: **cardenaslaw@etb.net.co**

IDENTIFICACION
C.C. ☒ NIT ☐
C.E. ☐ Otro ☐
Cual _____
No. **19.427.257** TP **38.319**

(4) INVENTOR (ES) (72)

Nombre (1) : **HWANG, JAY-YEOB**
Dirección: **106-dong, 703-ho, 1555, Bunji-joongsan village, Ilsan 2-dong, Ilsan-gu, Goyang-si, Gyunggi-do, 411-728 .**
Nombre (2) :**YANG, KI-HO**
Dirección: **126-26, Daesin-dong, Seodaemun-gu, Seoul, 120-160**
Nacionalidad o Domicilio: **Korea**

(5) PCT (86)
Solicitud Internacional No. **PCT/KR2004/002495** Fecha **25-09-2004**
Publicación Internacional No. **WO2005/029216** Fecha **31-03-2005**

(6) Título (54) **METODO DE SERVICIO DE CERTIFICACION SEGURA**

(7) Clasificación Internacional (51) G06F17/00

(8) Prioridad

SI ☒ NO ☐

(33) País de Origen	(32) Fecha	(31) Número de Solicitud
KR	25-09-2003	10-2003-0066452
KR	08-07-2004	10-2004-0053149
KR	30-08-2004	10-2004-0068356

(9) **Comprobante de pago No.** 06-31.096 y 06-31.097 **Fecha** 24-04-2006

(10) **ANEXOS**

- [x] Comprobante de pago de la tasa de presentación de la solicitud.
- [ ] Documento que acredita la existencia y representación legal cuan el solicitante sea persona jurídica.
- [ ] Poderes, si fuere el caso necesario.
- [ ] Documento de cesión del inventor al solicitante o causante.
- [ ] Declaraciones.
- [x] Copia de la solicitud internacional. (Resumen, descripción, reivindicaciones, dibujos)
- [x] Traducción de la solicitud internacional al castellano. (Resumen, descripción, reivindicaciones, dibujos)
- [ ] Copia del examen preliminar internacional efectuado por la Autoridad Internacional de Examen Preliminar (IPEA).
- [ ] Traducción del examen preliminar internacional efectuado por la IPEA.
- [ ] De ser el caso, copia del contrato de acceso.
- [ ] De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de las comunidades indígenas.
- [ ] De ser el caso, certificado de depósito del material biológico.
- [ ] Arte final 12x12.
- [ ] De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por el mismo titular o su causante, relacionadas parcial o totalmente con la invención de esta solicitud.
- [ ] De ser el caso, modificaciones efectuadas a la solicitud internacional.
- [x] Otros: **Informe de búsqueda internacional, publicación internacional A2 y A3 con traducción extracto para su publicación en medio magnético, tarjeta archivo temático, comprobante de pago de tasas por palabras adicionales para publicación.**

(11) **FIGURA CARACTERÍSTICA:**

(12) **Solicito la concesión de la patente,**

NOMBRE: JESUS ABELARDO CARDENAS ALFARO

FIRMA:

C.C. 19.427.257 Bogotá **T.P. 38.319**

C & R

3

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Rcd: 03-038004- -00000-0000 Fcc: 2003-04-25 16:36:31
Exp: 9580 NUMERACIONES Cns: 378 FABENACIONALI
Tip: 11 PATENTENTE
Act 411 PRESENTACION Folios: 85

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 06 - 31,096
FECHA : ABRIL 24 DE 2006

C O N S I G N A C I O N

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
CARDENAS Y RODRIGUEZ ABOG	CONSIGNACION	BANCO POPULAR	050-00110-6	31587849	24/04/2006	1,817,260.00

C O N C E P T O

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE IN	463,000.00
		TOTAL : $	463,000.00

SON: CUATROCIENTOS SESENTA Y TRES MIL PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No._____

4

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Rad: 03-038084- -00000-0000 Fec: 2003-04-25 16:38:31
Rec: 2003 NULIFICACIONES
Ref: 11 PATENTES EXP: 378 FABENACIONAL!
Act: 411 PRESENTACION Folios: 85

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

CERTIFICACION DE EXCEDENTE : 06 - 31,097
FECHA : ABRIL 24 DE 2006

***** C O N S I G N A C I O N *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
CARDENAS Y RODRIGUEZ ABOGCONSIGNACION		BANCO POPULAR	050-00110-6	31587849	24/04/2006	1,817,260.00

***** C O N C E P T O *****

CANT.	RENTISTICO	CONCEPTO		TOTAL CONCEPTO
1	50005-01-09 OTROS SERVICIOS DE PROPIEDAD I	99	OTROS SERVCIOS ADMINISTRATIVOS	729,960.00
			TOTAL : $	729,960.00

SON: SETECIENTOS VEINTINUEVE MIL NOVECIENTOS SESENTA PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No._____

5

PCT REQUEST

Print Out (Original in Electronic Form)

0	For receiving Office use only	
0-1	International Application No.	
0-2	International Filing Date	
0-3	Name of receiving Office and "PCT International Application"	
0-4	Form PCT/RO/101 PCT Request	
0-4-1	Prepared Using	PCT-SAFE Version 3.50 (Build 0002.175)
0-5	Petition The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	Receiving Office (specified by the applicant)	Korean Intellectual Property Office (RO/KR)
0-7	Applicant's or agent's file reference	auth_maze
I	Title of Invention	The Method of safe certification service
II	Applicant	
II-1	This person is	applicant and inventor
II-2	Applicant for	all designated States
II-4	Name (LAST, First)	HWANG, Jay-Yeob
II-5	Address	1555 Bunji -joongsan village, doosan apartment 108-708 Ilsan2-Dong Ilsan-Gu Goyang411-728 Republic of Korea
II-6	State of nationality	KR
II-7	State of residence	KR
II-8	Telephone No.	82-031-976-6501
II-10	e-mail	jay@foelian.com
II-11	Applicant's registration No. with the Office	419980485480
V	DESIGNATIONS	
V-1	The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.	

6

PCT REQUEST

Print Out (Original in Electronic Form)

VI-1	Priority claim of earlier national application		
VI-1-1	Filing date	25 September 2003 (25.09.2003)	
VI-1-2	Number	10-2003-0066452	
VI-1-3	Country	KR	
VI-2	Priority claim of earlier national application		
VI-2-1	Filing date	08 July 2004 (08.07.2004)	
VI-2-2	Number	10-2004-0053149	
VI-2-3	Country	KR	
VI-3	Priority claim of earlier national application		
VI-3-1	Filing date	30 August 2004 (30.08.2004)	
VI-3-2	Number	10-2004-0068356	
VI-3-3	Country	KR	
VII-1	International Searching Authority Chosen	Korean Intellectual Property Office (ISA/KR)	
VIII	Declarations	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	-	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	-	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	-	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	-	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	-	
IX	Check list	number of sheets	electronic file(s) attached
IX-1	Request (including declaration sheets)	3	✓
IX-2	Description	9	✓
IX-3	Claims	4	✓
IX-4	Abstract	1	✓
IX-5	Drawings	5	✓
IX-7	TOTAL	22	

7

PCT REQUEST

Print Out (Original in Electronic Form)

	Accompanying Items	paper document(s) attached	electronic file(s) attached
IX-8	Fee calculation sheet	-	/
IX-17	PCT-SAFE physical media	-	-
IX-19	Figure of the drawings which should accompany the abstract		
IX-20	Language of filing of the international application	Korean	
X-1	Signature of applicant, agent or common representative	(PKCS7 Digital Signature)	
X-1-1	Name (LAST, First)	Hwang, Jay-Yoob	
X-1-2	Name of signatory		
X-1-3	Capacity		

FOR RECEIVING OFFICE USE ONLY

10-1	Date of actual receipt of the purported international application	
10-2	Drawings:	
10-2-1	Received	
10-2-2	Not received	
10-3	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application	
10-4	Date of timely receipt of the required corrections under PCT Article 11(2)	
10-5	International Searching Authority	ISA/KR
10-6	Transmittal of search copy delayed until search fee is paid	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	Date of receipt of the record copy by the International Bureau	

8

PCT (ANNEX - FEE CALCULATI N SHEET)

Print Out (Original in Electronic Form)

(This sheet is not part of and does not count as a sheet of the international application)

0	For receiving Office use only			
0-1	International Application No.			
0-2	Date stamp of the receiving Office			
0-4	Form PCT/ROI101 (Annex) PCT Fee Calculation Sheet			
0-4-1	Prepared Using	PCT-SAFE Version 3.50 (Build 0002.175)		
0-6	Applicant's or agent's file reference	auth maze		
2	Applicant	HWANG, Jay-Yeob		
12	Calculation of prescribed fees		fee amount/multiplier	Total amounts (KRW)
12-1	Transmittal fee	T	45000	
12-2-1	Search fee	S	225000	
12-2-2	International search to be carried out by	KR		
12-3	International filing fee (first 30 sheets)	I1	1329000	
12-4	Remaining sheets		0	
12-5	Additional amount	(X)	0	
12-6	Total additional amount	I2	0	
12-7	I1 + I2 =	I	1329000	
12-12	Electronic Filing reduction (Full)	R	-285000	
12-13	Total international filing fee (I-R)	I		1044000
12-14	Fee for priority document			
	Number of priority documents requested		0	
12-15	Fee per document	(X)	0	
12-16	Total priority document fee	P		
12-17	TOTAL FEES PAYABLE (T+S+I+P)			1314000
12-19	Mode of payment		cash	

THE METHOD OF SAFE CERTIFICATION SERVICE

Technical Field

The present invention relates to authentication of a user, and more particularly, to technologies capable of preventing fraudulent use of an ID and a password of an individual, which are stolen through keyboard input information, and the drain of a password of a button input type of an entrance door lock device.

Background Art

A variety of security programs for PCs have been commercialized. They provide a function of monitoring illegal invasion for hacking or whether or not a hacking program has been installed, and the like.

Further, lots of Internet websites provide services in which if a user checks a security access option upon logging in, the user's ID and password are encrypted using 128bits SSL (Secure Sockets Layer) of an international standard, which is used in Internet banking, card payment, etc., so that a hacker cannot intercept those information.

Technical Problem

However, the conventional security program for the PCs operates only in a corresponding computer. Thus, if a user tries to open his/her e-mails using other's computers, those

information is exposed to the danger of hacking.

Also, the conventional security access service is helpless in the face of a keyboard input information hacking program installed within a computer.

Further, a current door lock device using a button has a disadvantage in that the password is likely to be exposed to an accompanied person.

Accordingly, it is an object of the present invention to provide an authentication method which enables both a security access in any computer and a safe door lock.

Advantageous Effects

As described above, the present invention is advantageous in that it is very excellent in terms of the security of login information in any computer regardless of whether or not a security program is installed, the security as a door lock device, the prevention of an authentication attempt by third parties, and the security against phishing. Further, the present invention is advantageous in that it can expand the band of a password even in a small-sized keypad such as a mobile phone, and it allows a user to safely report in case of emergence.

Brief Description of Drawings

FIG. 1 is a flowchart illustrating a main process flow of the present invention;

FIG. 2 shows an example that clicks on an image;

FIG. 3 shows an example that reports the past access history upon logging in;

FIGS. 4 and 5 show another embodiments of an authentication method by the input of coordinates.

FIG. 6 shows an embodiment in which numbers are indicated every coordinates not coordinate writing;

FIGS. 7 and 8 show another embodiments of an authentication method by the input of coordinates;

FIG. 9 shows an embodiment of a non-response screen against the manipulation of a direction key;

FIG. 10 illustrates a setting screen for producing a personalization set;

FIG. 11 shows an embodiment in which the present invention is applied to a mobile phone;

FIG. 12 shows an example of a user profile table for an authentication service according to the present invention; and

FIG. 13 shows an example of an interface for registering a main computer according to the present invention.

Best Mode for Carrying Out the Invention

The present invention is composed of four main steps. Each of the steps will now be described.

FIG. 1 is a flowchart illustrating a main process flow of the present invention.

1. Authentication step by text input (S100)

This step is the most common method in which an ID and a password are inputted through the keyboard for authentication.

Thus, detailed description on this step will be omitted.

2. Access location tracking step (S200)

If a user passes through the authentication step using the text input, the process proceeds to a web page for an authentication step through coordinate input. At this time, a JAVA applet that performs an access location tracking function is automatically downloaded into the user's computer, and then reports the user's current access location to a server. The server stores this information.

Description on technology in which JAVA applet tracks an access location can be found in Korean Patent Application No.10-2001-0027537.

3. Authentication step through coordinate input (S400)

If the user's access location is tracked, the user is provided with a screen on which a predetermined image and other images are displayed randomly in order, so that the user clicks on the predetermined image correctly. At this time, the predetermined image can be one or plural. It is determined that authentication is successful only when the user clicks on the predetermined image correctly. Alternately, the user can click on a second password consisting of a character string through a mouse.

At this time, the number of available attempts can be properly limited (S410), so that a hacker is discouraged to make an attempt on hacking with the user's access location exposed (S420).

FIG. 2 shows an example that clicks on an image.

4. Access history report step (S330, S500)

If someone attempts access in a state where a user is being accessed, the location of the person who attempts access, which is obtained in the access location tracking step, and the access location of a current login status of the user are compared (S310). If they are not the same, the user of the current login status is immediately informed of the access location of the person who attempts access (S330). The user can report the access location of the person so that the hacking criminal can be caught.

If they are the same, the obtained positional information of the person who attempts access is always reported to the user in a next login (S500). More particularly, if there is a case where clicking on an image is failed, an alarm of a higher level is provided so that the user can prepare for hacking.

FIG. 3 shows an example that reports the past access history upon logging in.

Of the steps described above, the step of receiving the coordinates of the image is to prevent anyone who steals information inputted through the keyboard from making fraudulent use of others' ID since the conventional login method is mainly depending upon the keyboard. That is, if a person who attempts access does not click on a predetermined image correctly although he has stolen information inputted through the keyboard, he fails in login.

Further, in the access location tacking step, if a user attempts clicking on an image, the user's access location is

exposed. Thus, the user will not dare to make an attempt of he does not know a predetermined image.

Moreover, in the authentication step through the keyboard input, the speed of clicking on the mouse becomes slows only with authontication by clicking on the mouse. Thus, since surrounding person when login is made can easily memorize an image, this step is for preventing a user from attempting hacking only with the memorized image. That is, this employs the fact that since the input of the keyboard is generally made by depressing several keys immediately, it is difficult to perceive the input. That is, a dual security system is implemented by allowing the input to be made through the keyboard and the mouse, separately.

Hereinafter, various embodiments of the authentication method by the input of coordinates will be described.

FIGS. 4 and 5 show another embodiments of the authentication method by the input of coordinates.

This method employs key coordinates and key images. In this method, if a user hits a predetermined key image to a predetermined key coordinate, authentication is successful.

For example, it is assumed that key coordinates of a user are (4, 2), and a key image is a heart pattern 1. (4, 2, heart pattern) is recorded in the user's personal information DB of the server as second authentication information. In the server, all the patterns are randomly mixed and an image table as shown in FIG. 4 is transmitted to the user's terminal. At this time, (2, 3), which is the position of the key image 1 of the image

table in which all the patterns are randomly mixed, is recorded. The user inspects closely where the heart pattern 1 being his the key image shown on the screen is located, and then controls a direction key so that his heart pattern 1 is located in the key coordinates (4, 2). In FIG. 4, since the heart pattern 1 is (2, 3), if the right direction key is pressed twice and a down direction key 1 is pressed once, the entire images are shifted in the direction of the direction key. Thus, the heart pattern 1 located at (2, 3) is located at (4, 2), as shown in FIG. 5. If the enter key is pressed, authentication is successful. According to the manipulation of the direction key, the server continues to shift (2, 3), compares coordinates immediately before the enter key is inputted with the key coordinates, and if they are the same, considers that authentication is successful. In this method, a total of 25 images are shifted together. Thus, it is very difficult to know which image corresponds to which coordinates although others behind sees the screen. Moreover, although manipulation information of the direction key is stolen, authentication will not be successful only with the same method because the key image is located at a different position next time. In this case, the shift rule is a method in which an image located at the end in the traveling direction like 1-2-3-4-5-1 is shifted toward a first position of the direction.

Furthermore, in this method, the key coordinates can be newly designated every time using a second key image.

FIG. 6 shows an embodiment in which numbers are indicated

every coordinates not coordinate writing.

In this embodiment, assuming that the heart pattern 1 is a first key image and a second key image is a clover pattern 4, a fourteenth position 3 where the clover pattern of the second key image is initially located becomes key coordinates. That is, if the first key image is moved to the position where the second key image is initially located, authentication is successful.

In this method, since key coordinates are changed every time, it is easy to memory the key coordinates by attaching the number 3 than coordinates such as (4, 3). A user who receives the image table as shown in FIG. 6 finds a heart pattern 1 being his first key image, finds a clover pattern 4 being a second key image, memorizes the number 14 being its position number, and then manipulates a direction key in order to position the heart pattern 1 at the 14 position. At this time, memorizing the position number of the clover pattern is for not to lose the first position 3 since the clover pattern is also moved when the heart pattern is moved. Therefore, it can be thought that the position 3 designated by the second key image not the second key image is hit. The user can easily memorize the key images using the name of the images, by producing memorizing sentences such as "I love clover" (a heart can be moved to a position where the clover was located), "Carrot to a panda" (a carrot is moved to a position where the panda was located).

For this method, when the server newly produces the image table before transmission, coordinates of each key image can be recorded, and movement of the coordinates can be calculated

according to key manipulation of the user.

At this time, another interesting and useful functions such as a booby trap key 5 and a report key 6 can be thought.

Both the booby trap key and the report key are keys predetermined by a user. In this embodiment, the user sets a carrot 5 as the booby trap key, and a butterfly 6 as the report key. The booby trap key is a key indicating a position through which passage is not allowed when the key image is moved. That is, if the order of a position number 12-13-14 is moved in FIG. 6, a position 13 where the carrot is located is a booby trap key 5. Thus, an alarm is generated from a PC speaker and authentication is thus unsuccessful. That is, it is preferred that a path of 12-11-15-14, 12-7-8-9-14, etc. be used away from the carrot.

Further, if the booby trap key is trapped during the authentication process, the booby trap key transmits an alarm message to a user via SMS or e-mail so that the user can take a proper action. For example, URL, which can receive a report, can be included in the alarm message. If a report is received, a guard can go to a spot in order to catch a criminal.

The report key 6 allows a user to make report without being noticed if a criminal enters a company or a home by threats or when withdraws cash, in the case where the report key 6 is used as an authentication device in a door lock device, a bank cash dispenser, etc. If the user deceives the second key image into considering it to be the butterfly 6 of the report key or directly manipulating it, authentication is successful and thus

sets the criminal at ease. In this case, however, a report is automatically made to the police or a guard company. That is, the report key can be a function in which the report function is added to the function of the second key image.

The booby trap key and the report key further increases the level of a danger that attempts authentication in order for an illegal user to disguise himself as others, thereby maximizing a prevention effect.

Further, a method of assigning a number to each position shown in this method can be applied to the method of FIG. 4. That is, in the method of FIG. 4, you can memorize the heart pattern at the number 19 instead of memorizing that the heart pattern is at the position (4, 2).

FIGS. 7 and 8 show another embodiments of an authentication method by the input of coordinates. This method is a case where key images form a pair such as 21(7) and 11(8).

21 is found in a left image table of FIG. 7, and 11 is found in a right image table of FIG. 7. Then, two key images are overlapped by dragging the right image table using the mouse, and are then dropped. In this case, if there is (21, 11) among various pairs of overlapped images, authentication is successful. Even in this case, the arrangement of the image tables is randomly changed in order every time. Thus, even if manipulation information of the mouse is known, next authentication will be unsuccessful. Further, since several pairs of images are overlapped at a time, others behind will not know which image pair is which key pair. In this method, if

two image tables correspond to the key image pair when the server produces the image tables, others can easily know it since too less pairs of the images are overlapped. Thus, in order to prevent this, the image tables in the case where too less pairs of the images are overlapped are discarded, and new image tables are generated.

The above-described methods of FIGS. 4 and 6 correspond to a method in which the process of hitting the key image is safe although others steal a glance at it. In order to accomplish the object, first, a key image and key coordinates (or a second key image arranged within a second image table) that must correspond to its key image must be known to a user himself. Second, when the position of the key image is manipulated, all other images are manipulated at the same time in the same direction and as long as the same distance. Thus, although others watch it, they do not know which image is manipulated. Since the arrangement of image tables is differently presented every time, authentication is unsuccessful only with the same manipulation value although the manipulation value is known.

Furthermore, even if the direction key is manipulated, the same effect can be obtained although all the images are never moved. In this case, the user can draw a pointer over the key image in his mind, and moves the pointer in his mind together to the key coordinates according to the manipulation of the direction key. That is, if the images are moved, the pointer is also moved, but if the images are not moved, the pointer is not moved. Thus, others who see it from the side do not which image

is manipulated.

FIG. 9 shows an embodiment of a non-response screen against the manipulation of a direction key.

In the embodiment of FIG. 9, if a passage rule is a 2 point passage type starting from a key image, and a key image, a through coordinate image and a terminal coordinate image are beer, a soccer ball and television, a sentence for memorizing can be "Watch a soccer relay while drinking beer". In the example shown in FIG. 9, a distance from beer to the soccer ball is one box downwardly, and a distance from the soccer ball to television is two boxes to the right and one box upwardly. A total manipulation process is "a down direction key once, enter, a right direction key twice, and an up direction key once, enter".

An embodiment of a personalization set that prepares for phishing will now be described.

Description on the personalization set will be made assuming the case of FIG. 9.

The method such as FIG. 9 is advantageous in that a personalization set in preparation for phishing can be easily implemented. That is, since sets to pass are differently registered every person, sets different every person are presented. Thus, others' key image and passage points cannot be known using bogus sets.

FIG. 10 illustrates a setting screen for producing a personalization set.

As shown in FIG. 10, if a user selects his key image and

passage coordinate image from images which is much more than 16 necessary in a set and generates a personalization set including the selected images as shown in FIG. 9, bogus sets are produced so that it is difficult to include all the 3 images of a corresponding person.

Assuming that 3 images among 36 images as in FIG. 10 are selected and the remaining 13 images is randomly selected to produce the personalization set, the probability that specific 3 images are all included when selecting the 16 images from the 36 images is merely 7.8%. That is, the probability that a criminal passes through a bogus set and then steals a target user's key is 7.8%. If specific images are to be selected from 100 images, the probability is further dropped and results in 0.3%.

Furthermore, it is evident that the personalization set can be implemented to support a unique set by uploading images produced by a user.

Also, in order to steal a glance at a personalization set in advance and then attempt a phishing attack using a bogus personalization set, it will be effective to send an alarm message to a person even in an attempt that a criminal sees only the personalization set but does not pass. The alarm message can include an advice sentence reading that it is better to change a key because there is the possibility that the personalization set may be exposed.

Next, a method of preventing an attempt to steal a key by applying a personalization set, which is obtained by installing a hacking tool having an image capture function in others'

computer so as to steal the above-described personalization set, to a bogus site for phishing will be described. Although capture can be prevented through an anti-capture technology, this method is to prepare for a case where a hacking tool that cannot be prevented through the anti-capture technology exists.

FIG. 12 shows an example of a user profile table for an authentication service according to the present invention. In this example, main computer information 14 is recorded every user.

FIG. 13 shows an example of an interface for registering a main computer according to the present invention.

When the personalization set according to the present invention is executed on-line, specific unique information 16 within a computer of a user can be recognized using, e.g., MAC address of a LAN card or the computer of the user can be recognized using cookie. If the computer is recognized as a computer that has not been registered in the user profile, an alarm message is sent to a contact point 15 designated by the user, and the interface for registering the main computer as shown in FIG. 13 is provided so that the user can take an necessary step.

The alarm message notifies the user of the fact that authentication has been attempted by a computer not registered by the user so that the user can prepare for personal information hacking.

Further, the interface for registering the main computer allows the user to register his computer, which is currently

being used, as a main computer. At this time, the registered computer is recognized as the main computer of the user, and is thus treated differently from strange unregistered computers.

What the main computer of the user and the strange computers are differently treated means that keys for passing through authentication are set to be different. For example, a key 12 used in the main computer and a key 13 used in a strange computer can be set to be completely different, or all keys can pass through the strange computer but some of the keys can pass through the main computer. That is, although phishing is successful in the main computer, only the key 12 for the main computer is stolen, which makes it difficult for fraudulent use by an attacker who has to input the key 13 for the strange computer.

Furthermore, the method of confirming keys different every computer is effective in preventing fraudulent use in a strange computer even in authentication by an existing text input as well as authentication by the coordinate input. That is, if a password is 8 positions, 8 positions are all confirmed in the strange computer, but only 4 positions are confirmed in the main computer. It is thus possible to prevent fraudulent use in the strange computer although the password is stolen.

If the present invention is applied to a security access service, it is evident that there is a sufficient hacking-prevention effect although the access location tracking step is omitted. Further, it can be seen that a security effect is sufficient although a dual authentication step is not practiced.

Next, description will be given on a method in which the present invention is applied to devices such as a mobile phone, a door lock and a safe in a built-in manner.

In the mobile phone, the door lock, the safe and so on, there is no need to confirm who is who among numerous people like services on Internet or a bank. It is thus not necessary to confirm an ID and a password.

Therefore, there is less need to perform the above-described first and second authentication steps. Further, in these devices, the keyboard is a compact keyboard not a full keyboard like a computer keyboard. In this keyboard, it is convenient to input numbers, but inconvenient to input characters. For this reason, a password in this device is usually composed of only numbers. This results in a too narrow bandwidth of the password. Furthermore, since there is nothing meaning in numbers, a password related to personal information is used in finding meaningful numbers that can be easily memorized. This password is disadvantageous in that it can be easily analogized by third parties.

FIG. 11 shows an embodiment in which the present invention is applied to a mobile phone.

As shown in FIG. 11, in the case where a text password is first inputted and the input of coordinates is completed by presenting an image table for coordinate authentication without confirming the password, if it is determined whether to allow a passage by confirming the text password and the coordinates at a time, the number of cases is 10 thousands when a number password

is only 4 positions, and if it is a 2-point passage rule in a 16 image table, the number of cases is 210. They are not simply added, but multiplied, resulting in 2.1 millions the total number of cases. This means that assuming that an hour is taken to find one number password, a full month is taken in order to find the full number password if 7 hours are invested a day.

To this end, the process can be programmed to allow a passage only when both the text input and the coordinate input are valid without the process of confirming the text input and the coordinate input intermediately.

The above-described built-in type is very useful in the door lock. This means that not only the bandwidth of a password widens, but also all pertinent persons can use the number password. That is, in an existing number key, since all constituent members uses a single key by, it is inconvenient to inform all the constituent members of a new password. Thus, it is very common to use the key for a long time without changing it. In the present invention, if keys as many as the number of constituent members are registered, each constituent member can manage each key separately. Also, since the bandwidth is sufficiently wide enough to be shared by a plurality of constituent members, it can be safely used in most door locks for an office. Furthermore, there is an advantage in that entrance and exit can be managed on a constituent member basis.

Furthermore, if a door lock to which advanced technologies such as an electronic chip or biomatrics are applied is used, the level of security does not drop to the level of security of

a number key provided as an assistant key.

27

What Is Claimed Is:

1. A security access service method in processing member login in an on-line service, comprising:

an authentication step by the input of text;

an access location tracking step;

an authentication step by the input of coordinates; and

an access history report step.

2. The security access service method as claimed in claim 1, wherein the access location tracking step is performed between the two authentication steps.

3. The security access service method as claimed in claim 1, wherein the access history report step includes the steps of:

if another access is attempted with a user being already accessed, comparing the location of a person who attempts access, which is obtained in the access location tracking step, with the access location of a current login status, and if the location of the user and the access location of the current login status are different, immediately reporting the access location of the person who attempts access to the user of the current login status through a screen, and

if the location of the user and the access location of the current login status are the same, the obtained positional information of the person who attempts access is always reported to the user upon next logging in.

4. The security access service method as claimed in claim 1, wherein the access history report step includes the step of, if the authentication step by the input of the coordinates fails, immediately sending an alarm message through message means that is designated by the user.

5. A security access service method in processing member login in an on-line service, comprising:

an authentication step by the input of text; and

an authentication step by the input of coordinates.

6. The security access service method as claimed in any one of claims 1 to 5, wherein the authentication step by the input of the coordinates comprises the steps of:

transmitting an image table in which a key image is randomly mixed with a plurality of other images to the screen of the user;

manipulating the entire images to have the same value at the same time according to a manipulation value of a keyboard or a mouse of the user;

confirming a position manipulated by the key image; and

if coordinates whose manipulation of a position is confirmed and key coordinates previously designated by the user coincide with each other, determining that authentication is successful, and if they do not coincide with each other, determining that that authentication is unsuccessful.

7. The security access service method as claimed in claim 6, wherein the key coordinates are positions designated using a second key image.

8. The security access service method as claimed in claim 7, further comprising the step of, if a first key image passes through a position designated by a booby trap key image through the manipulation of the user, determining that authentication is unsuccessful, and transmitting an alarm message to a PC of the user or an original owner of an ID.

9. The security access service method as claimed in claim 7, further comprising the steps of, if the user places the first key image at a position designated by a report key image and then confirms the manipulation, determining that authentication is successful, and allowing this fact to be automatically reported through a guard system.

10. A method of safely authenticating a user, comprising the steps of:

transmitting an image table in which a key image is randomly mixed with a plurality of other images to a screen of a user;

manipulating the entire images to have the same value at the same time according to a manipulation value of a keyboard or a mouse of the user;

confirming a position manipulated by the key image; and

if coordinates whose manipulation of a position is confirmed and key coordinates previously designated by the user coincide with each other, determining that authentication is successful, and if they do not coincide with each other, determining that that authentication is unsuccessful.

11. The safe authentication method as claimed in claim 10, wherein the key coordinates are positions designated using a second key image.

12. The safe authentication method as claimed in claim 11, further comprising the step of, if a first key image passes through a position designated by a booby trap key image through the manipulation of the user, determining that authentication is unsuccessful, and transmitting an alarm message to a PC of the user or an original owner of an ID.

13. The safe authentication method as claimed in claim 11, further comprising the steps of, if the user places a first key image at a position designated by a report key image and then confirms the manipulation, determining that authentication is successful, and allowing this fact to be automatically reported through a guard system.

14. The safe authentication method as claimed in any one of claim 1 to 9, further comprising the step of registering a

personalization image table in which a construction image history of provided image tables is differently registered on a user basis.

15. The safe authentication method as claimed in claim 14, wherein the step of registering the personalization image table comprises the steps of:

allowing the user to select a key image and a through coordinate image or a terminal coordinate image from a group of images, which are much more than the number of images that are required in the personalization image table, and then to input the selected images;

allowing a server to randomly extract images as many as the number of images, which is necessary to complete the image table, from the remaining images except for the selected images; and

mixing the images that are selected and inputted by the user and the images that is selected by the server, and registering the personalization image table.

16. The safe authentication method as claimed in any one of claims 10 to 13, further comprising the step of inputting a text password, and

wherein the authentication process step includes determining that authentication is successful only when both the text password and the key coordinate are valid after the input of the text password and the key coordinates has been completed, and determining that authentication is unsuccessful if either

the text password or the key coordinate is not valid.

17. The safe authentication method as claimed in any one of claims 1 to 9, 14 and 15, further comprising:

a key coordinate registration step of providing the interface for allowing the user to differently define key coordinates for a main computer and key coordinates for a strange computer, and registering the inputted information;

a terminal information acquisition step of acquiring recognized information of a computer of the user;

a terminal recognition step of determining the computer as the main computer or the strange computer based on the recognized information on the computer of the user, which is acquired in the terminal information acquisition step;

a main computer registration step of, if it is determined that the computer is the strange computer in the terminal recognition step, registering the computer information to provide a main computer registration interface that can be registered as the main computer, and registering the inputted information; and

a strange computer alarm step of, if the computer is determined to be the strange computer in the terminal recognition step, notifying the user of the alarm message regardless of the authentication result,

wherein the authentication step by the input of the coordinates includes determining whether the coordinates the manipulation of the position of which is confirmed and the key

coordinates previously designated by the user coincide with each other, if the computer is determined to be the main computer in the terminal recognition step, confirming the key coordinates for the main computer, and if the computer is determined to be the stranger computer in the terminal recognition step, confirming the key coordinates for the strange computer.

18. The safe authentication method as claimed in claim 17, wherein the key coordinates are two or more, and all the key coordinates are confirmed in the strange computer, and only some of the key coordinates are confirmed in the main computer.

19. A method of safely authenticating a user, comprising the steps of:

a password registration step of providing the interface for allowing a user to differently define passwords for a main computer and passwords for a strange computer, and storing the inputted information;

a terminal information acquisition step of acquiring recognized information of a computer of the user;

a terminal recognition step of determining the computer as the main computer or the strange computer based on the recognized information of the computer of the user, which is acquired in the terminal information acquisition step;

a main computer registration step of, if it is determined that the computer is the strange computer in the terminal recognition step, registering the computer information to

provide a main computer registration interface that can be registered as the main computer: and

an authentication processing step of, if the computer is determined the main computer in the terminal recognition step, confirming a password for the main computer, and if the computer is determined the strange computer in the terminal recognition step, confirming a password for the strange computer.

20. The safe authentication method as claimed in claim 19, further comprising the steps of:

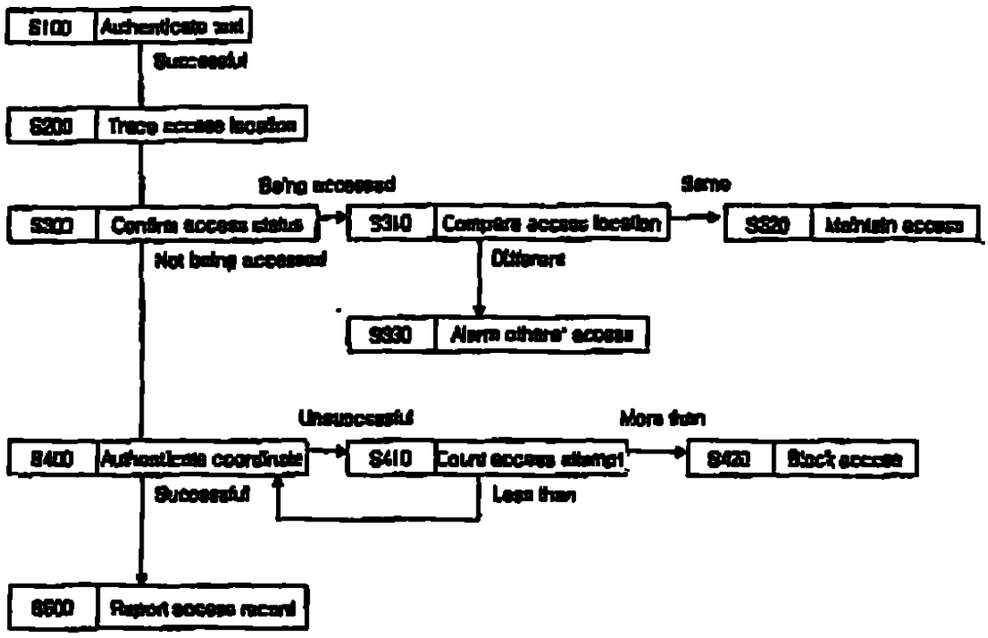
providing the interface for allowing the user to register a contact point where the alarm message is received, and storing the inputted information; and

a strange computer alarm step of, if the computer is determined to be the strange computer in the terminal recognition step, notifying the alarm message to the contact point regardless of the authentication result.

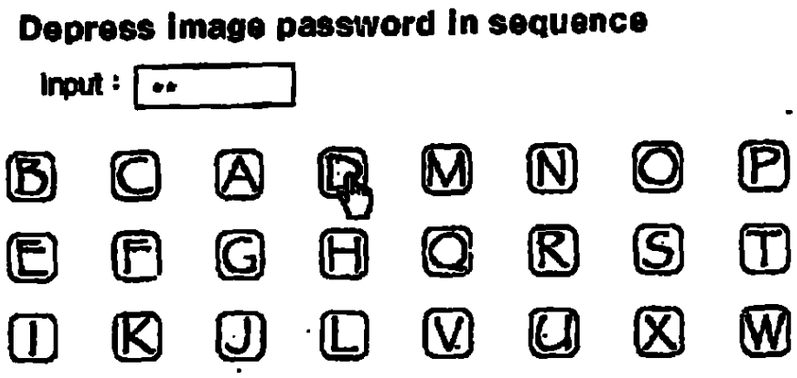
ABSTRACT

The present invention relates to safe authentication. According to the present invention, a security access service method includes an authentication step by the input of text, an access location tracking step, an authentication step by the input of coordinates, and an access history report step.

[Fig.1]


S100
Authenticate card
Successful
S200
Trace access location
Being accessed
Same
S300
Confirm access status
S310
Compare access location
S320
Maintain access
Not being accessed
Differs
S330
Alarm others' access
Unsuccessful
More than
S400
Authenticate coordinate
S410
Count access attempt
S420
Block access
Successful
Less than
S500
Report access record

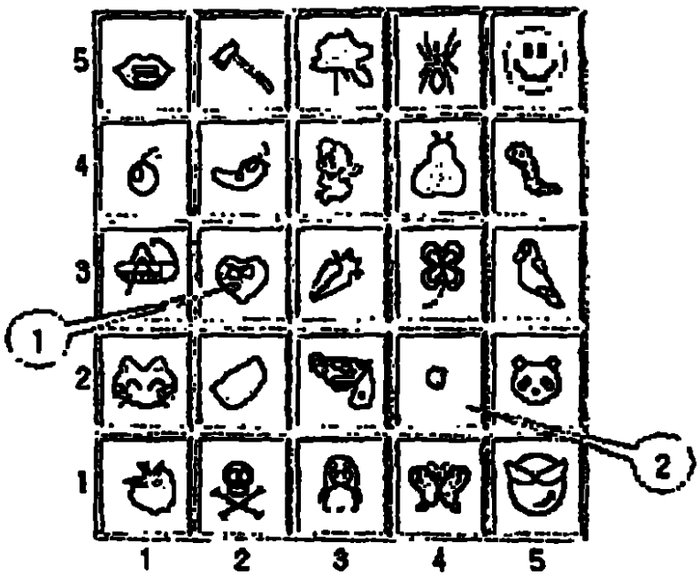
[Fig.2]



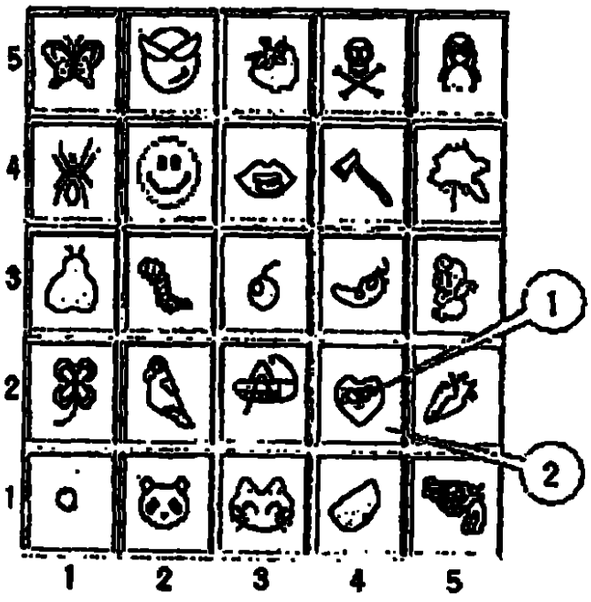
[Fig.3]

Access date	Access location	Authentication result	Access time
9/14 22:02	203.58.101.2	Second authentication unsuccessful	-
9/14 10:37	168.253.66.15	Second authentication successful	12:14
9/13 19:06	168.253.66.15	Second authentication successful	46:06
9/13 09:52	168.253.66.15	Second authentication successful	28:11

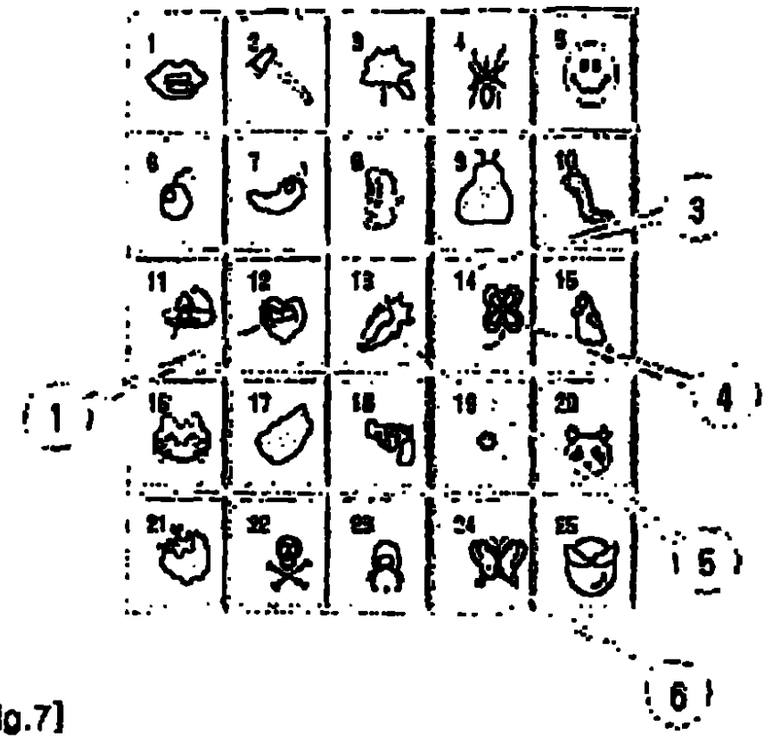
[Fig.4]



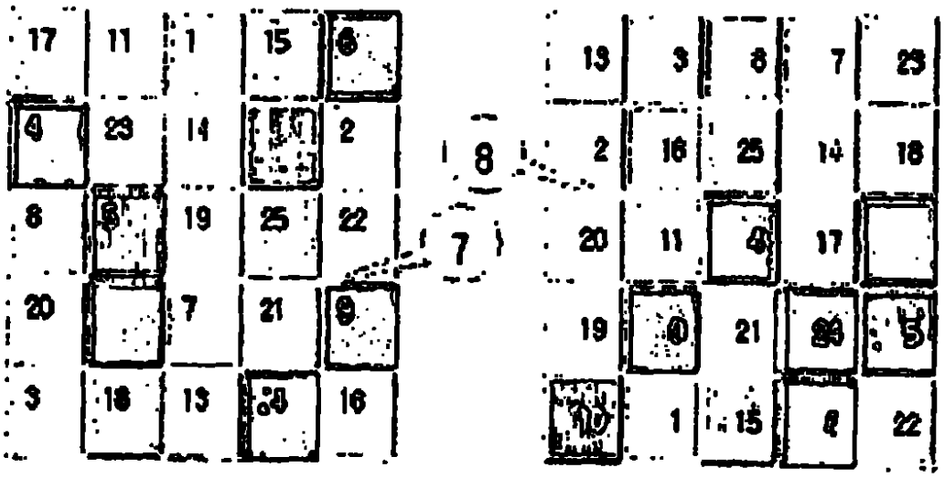
[Fig.5]



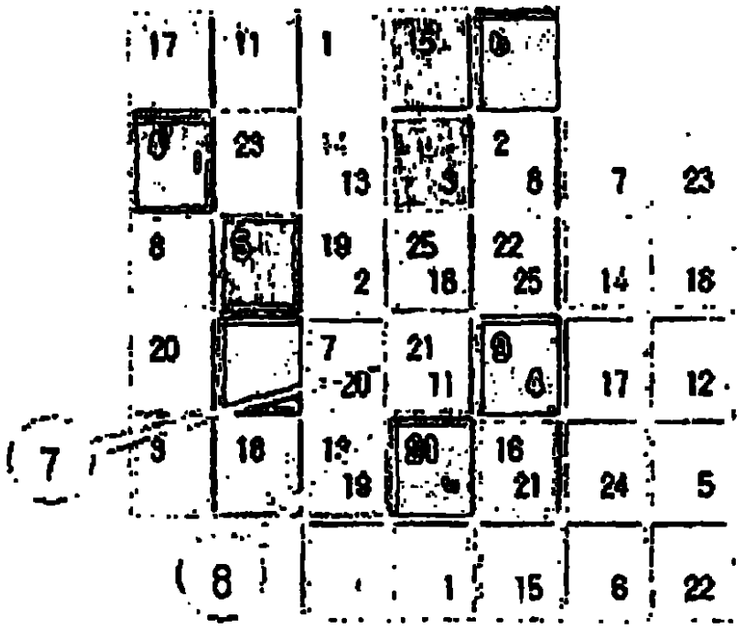
[Fig.6]



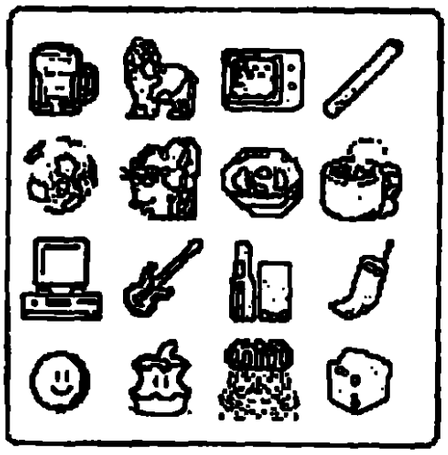
[Fig.7]



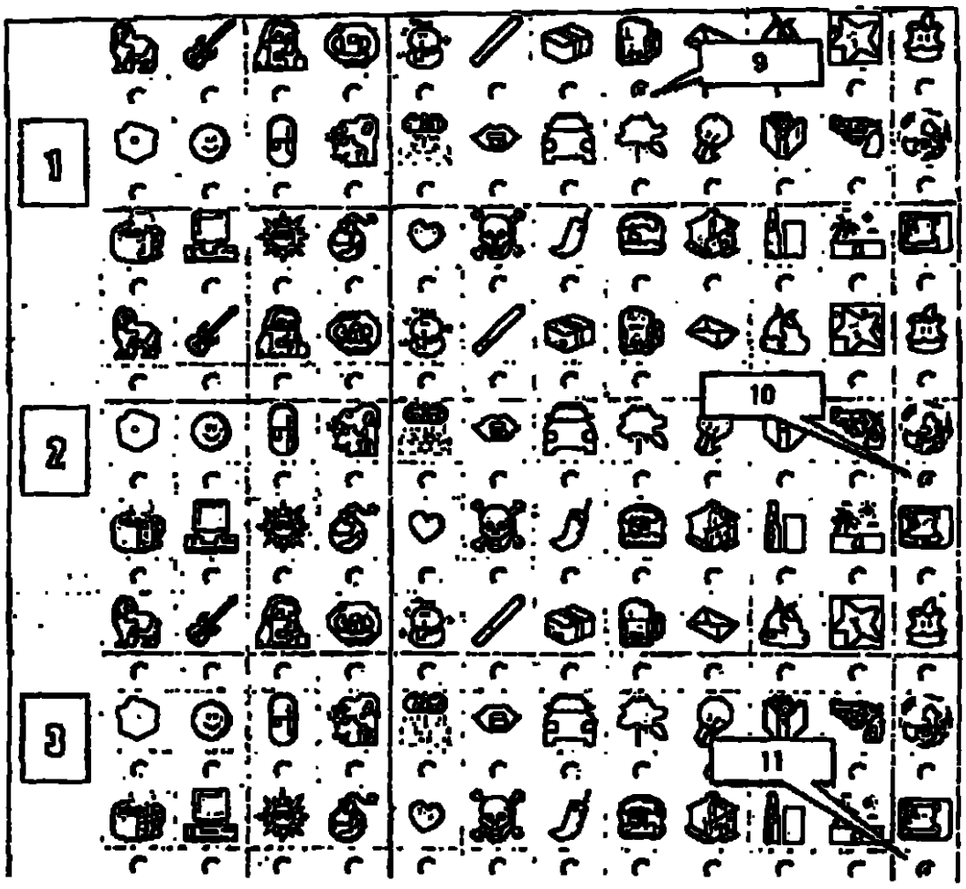
[Fig.8]


17 11 1 15
23 13 2 8 7 23
8 19 2 25 16 22 25 14 18
20 7 20 21 11 17 12
7 16 19 16 21 24 5
8 1 15 6 22

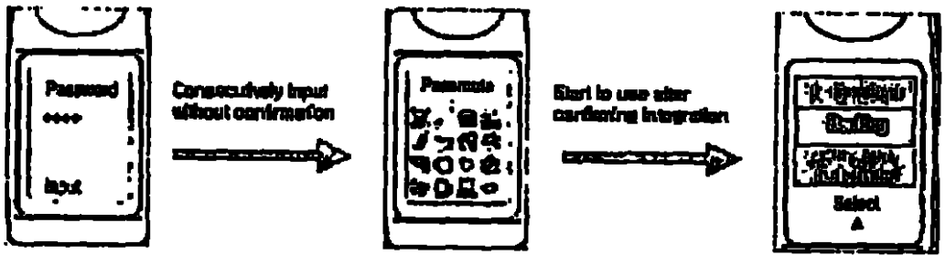
[Fig.9]



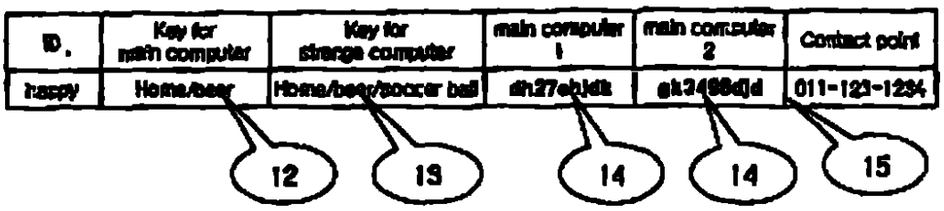
[Fig.10]


9
1
10
2
11
3

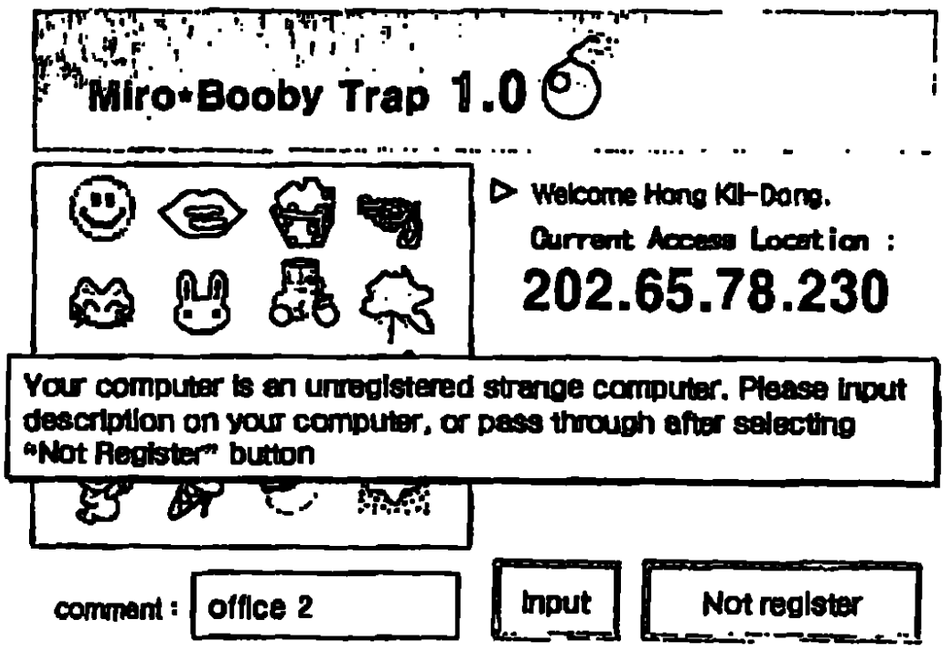
[Fig.11]


Password
Input
Consecutively input without confirmation
Password
Start to use after confirming integration
Select

[Fig.12]


ID.
Key for main computer
Key for strange computer
main computer 1
main computer 2
Contact point
happy
Home/bear
Home/bear/soccer ball
011-123-1234
12
13
14
14
15

[Fig.13]


Miro*Booby Trap 1.0
Welcome Hong Kil-Dong.
Current Access Location :
202.65.78.230
Your computer is an unregistered strange computer. Please input description on your computer, or pass through after selecting "Not Register" button
comment :
office 2
Input
Not register

MÉTODO DE SERVICIO DE CERTIFICACIÓN SEGURA.

Campo Técnico

La presente invención se refiere a la autenticación de un usuario, y en particular, a las tecnologías capaces de prevenir el uso fraudulento de una identificación (ID) y contraseña de un individuo, las cuales son robadas a través de la información ingresada por el teclado, y la fuga de una contraseña del tipo de los que son ingresados a través de botones en un dispositivo de cerradura de puerta.

ANTECEDENTES

Una variedad de programas de seguridad para las computadoras personales (PCs) han sido comercializados. Éstos proveen una función para el monitoreo de invasión ilegal por piratería informática (*hacking*) ó ya sea que un programa de piratería informática (*hacking*) haya sido instalado o no.

Además, muchos sitios de Internet proveen servicios en los cuales si un usuario marca una opción de acceso segura al darse de alta, la identificación y contraseña del usuario son encriptadas utilizando 128 bits *SSL (Capa de sockets segura)* de un estándar internacional, el cual es utilizado por los bancos vía Internet, para el pago de tarjetas de crédito, etc., de tal manera que un pirata informático (*hacker*) no pueda interceptar dicha información.

Sin embargo, el programa de seguridad convencional para las computadoras personales opera solamente en la correspondiente computadora. Por lo que, si el usuario trata de abrir sus correos electrónicos usando otra computadora, esa información queda expuesta al peligro de la piratería informática (*hacking*).

Incluso, el servicio convencional de acceso seguro queda inservible en el caso de que un programa de piratería informática (*hacking*) de ingreso de información por el teclado sea instalado en la computadora.

También, un dispositivo de candado que utilice un botón presenta la desventaja de que la contraseña queda igualmente expuesta que con una persona acompañada.

En tal virtud, es un objeto en la presente invención el proveer un método de autenticación que refuerce tanto al acceso seguro en cualquier computadora como en una cerradura de puerta.

Como se ha descrito anteriormente, la presente invención es de gran ventaja en el sentido de que es excelente en términos para la seguridad de vaciar información en cualquier computadora sin importar si ha sido o no instalado un programa de seguridad, la seguridad como un dispositivo de cerradura de puerta, la prevención de un auténtico ataque por terceras personas, y la seguridad contra el ataque a través de un link fraudulento (*phishing*). Además, la presente invención es de gran ventaja en la medida en la que puede expandir la banda de una contraseña incluso en un teclado de tamaño pequeño como un teléfono móvil, y que permite al usuario reportarse de manera segura en caso de una emergencia.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es un diagrama de flujo ilustrando el flujo del proceso principal de la presente invención;

La figura 2 muestra un ejemplo que hace "*clic*" en una imagen;

La figura 3 muestra un ejemplo que reporta el historial de accesos pasados hasta el registro;

Las figuras 4 y 5 muestran otras personificaciones de un método de autenticación por el ingreso de coordenadas.

La figura 6 muestra una personificación cuyos números que se encuentran indicados no coinciden con los escritos;

Las figuras 7 y 8 muestran otras personificaciones de un método de autenticación por el ingreso de coordenadas;

La figura 9 muestra la personificación de una pantalla de no-respuesta contra la manipulación de una llave de dirección;

La figura 10 ilustra una pantalla establecida para la producción de un juego de personalización;

La figura 11 muestra una personificación en la cual la presente invención es aplicada a un teléfono móvil;

La figura 12 muestra un ejemplo de una tabla del perfil del usuario de un servicio de autenticación en concordancia con la presente invención; y

La figura 13 muestra un ejemplo de una interfaz de registro a una computadora principal de acuerdo con la presente invención.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

La presente invención está compuesta por cuatro pasos principales. Cada uno de los pasos será descrito a continuación:

La figura 1 es un diagrama de flujo ilustrando el proceso del flujo principal de la presente invención.

1. Paso de autenticación por el ingreso de texto (S100):
   Este paso es el método más común en el cual una identificación y una contraseña son ingresadas a través de un teclado para autenticación. Razón por la cual, la descripción detallada de este paso será omitida.

2. Paso de rastreo de ubicación de acceso (S200):
   Si el usuario pasa a través del paso de autenticación utilizando el ingreso de texto, el proceso procede a una página Web para un paso de autenticación a través del ingreso de coordenadas. Al mismo tiempo, una aplicación de JAVA que ejecuta una función de rastreo de ubicación de acceso es bajada automáticamente a la computadora del usuario, y reporta la ubicación de acceso actual del usuario al servidor. El servidor almacena esta información.
   La descripción de la tecnología en la cual la aplicación JAVA rastrea la ubicación del acceso puede ser encontrada el la Solicitud Coreana de Patente No. 10-2001.0027537.

3. Paso de autenticación a través del ingreso de coordenada (S400):

Si la ubicación del acceso del usuario ha sido rastreada, el usuario es proveído con una pantalla en la cual una imagen predeterminada y otras imágenes son desplegadas en orden aleatorio, de tal manera que el usuario de *"clic"* en la imagen predeterminada correctamente. Al mismo tiempo, la imagen predeterminada puede ser una o varias. Es determinante que la autenticación será exitosa sólo cuando el usuario de *"clic"* en la imagen predeterminada correctamente. Alternativamente, el usuario puede dar *"clic"* en una segunda contraseña consistente en un cordón caracterizado a través del ratón.

Al mismo tiempo, el número de atentados disponibles puede ser propiamente limitado (S410), de tal manera que el hacker sea desanimado para realizar un ataque en *hacking* con la ubicación de acceso del usuario expuesta (S420).

La figura 2 muestra un ejemplo que hace clic en una imagen.

4. Paso del reporte del historial de acceso (S330, S500):
Si alguien ataca el acceso en un estado donde el usuario ha sido accesado, la ubicación de la persona que atacó el acceso, la cual es obtenida en el paso de rastreo de ubicación de acceso, y la ubicación de acceso del estatus actual de registro del usuario son comparados (S310). Si no son el mismo, el usuario del estatus actual de registro es inmediatamente informado de la ubicación de acceso de la persona que intento acceder (S330). El usuario puede reportar la ubicación de acceso de la persona de tal manera que el pirata informático (*hacker*) pueda ser atrapado.

Si son el mismo, la información obtenida de la posición de la persona que intentó acceder es siempre reportada al usuario en el siguiente registro (S500). En particular, si existe el caso que cuando se de *"clic"* en una imagen y falle, una alarma de alto nivel es proveída de tal manera que el usuario este preparado para la piratería informática (*hacking*).

La figura 3 muestra un ejemplo que reporta el historial de accesos pasados desde el registro.

De los pasos anteriormente descritos, el paso del recibo de las coordenadas de la imagen es para prevenir que cualquiera que robe información ingresada a través de un teclado la utilice de manera fraudulenta la identificación de otros toda

vez que el método convencional de registro depende principalmente del teclado. Esto es, si una persona que pretende su acceso no da *"clic"* a una imagen predeterminada de manera correcta a pesar de que ha robado información ingresada a través del teclado, falla en su registro.

Además, en el paso de rastreo de ubicación de acceso, si un usuario intenta dar *"clic"* en una imagen, la ubicación de acceso del usuario es expuesta. Por lo que el usuario no osaría en hacer un intento del cual no conoce una imagen predeterminada.

Incluso, en el paso de autenticación a través del ingreso por teclado, la velocidad para dar *"clic"* al ratón se vuelve lenta solo con la autenticación al hacer *"clic"* en el ratón. Por lo que, al acorralar a la persona cuando el registro está hecho puede memorizar fácilmente una imagen, este paso es para prevenir al usuario de un ataque de piratería informática sólo con la imagen memorizada. Esto es, se emplea el hecho de que desde el ingreso por el teclado es generalmente realizado por la presión de varias teclas inmediatamente, es difícil percibir el ingreso. Esto es, un sistema de seguridad dual es implementado al permitir el ingreso hecho a través el teclado y el ratón, separadamente.

En adelante, varias personificaciones del método de autenticación por el ingreso de coordenadas serán descritas.

Las figuras 4 y 5 muestran otras personificaciones del método de autenticación por el ingreso de coordenadas.

Este método emplea teclas de coordenadas y teclas de imagen. En este método, si el usuario teclea una tecla de imagen predeterminada a una tecla de coordenada predeterminada, la autenticación resulta exitosa.

Por ejemplo, se asume que las teclas de coordenadas del usuario son (4,2), y y que la tecla de imagen es el patrón 1. (4,2, patrón) es grabado en la información personal del usuario DB del servidor como una información de autenticación secundaria. En el servidor, todos los patrones son mezclados aleatoriamente y una tabla de imagen como se muestra en la figura 4 es transmitida a la terminal del usuario. Al mismo tiempo, (2,3), la que es la

posición imagen clave 1 de la tabla de imágenes la cual todos los patrones son electoriamente mezclados es grabada.

El usuario inspecciona de cerca el lugar donde el patrón de corazón que se muestra en la pantalla se localiza, y más tarde controla una llave de dirección de manera que el patrón del corazón 1 sea localizado en las coordenadas clave (4,2).

En la figura 4, como el patrón cardíaco 1 es (2,3), si la dirección clave correcta es presionada dos veces y una llave baja de dirección 1 es presionada una vez, las imágenes son giradas en el sentido de la llave de dirección.

Así, el patrón cardíaco 1 localizado a (2, 3) es localizado a (4, 2), como se muestra en la figura 5. Si la tecla "*enter*" es presionada, la autenticación es exitosa.

De acuerdo con la manipulación de la tecla de dirección, el servidor continúa cambiando (2, 3), compara las coordenadas de manera inmediata antes de que la tecla "*enter*" sea registrada con las coordenadas claves, y en caso de ser las mismas, considera la autenticación como exitosa.

En este método, un total de 25 imágenes son movidas juntas. Así, resulta sumamente difícil saber qué imagen corresponde a qué coordenadas a pesar de que otros puedan ver la pantalla por atrás.

Además, a pesar de que la información sobre manipulación de la tecla de dirección es robada, la autenticación no sería exitosa únicamente con el mismo método porque la imagen clave estaría localizada en una posición diferente en la siguiente ocasión.

En este caso, la regla de cambio es un método en el que una imagen ubicada al final en la dirección de viaje 1-2-3-4-5-1 es movida hacia una primera posición de la dirección.

Además, en este método las coordenadas clave pueden ser designadas nuevamente cada vez utilizando una segunda imagen clave.

La figura 6 muestra una presentación en que los números son indicados.

En esta presentación, asumiendo que el patrón cardíaco 1 es la primera imagen clave y una segunda imagen clave es un patrón de trébol 4, una décima cuarta posición 3 donde el patrón de trébol de la segunda imagen clave se localiza inicialmente la autenticación es exitosa.

En este método, como las coordenadas clave son cambiadas a cada momento, es fácil recordar las coordenadas clave al adjuntar el número 3 a las coordenadas como (4, 3). Un usuario que recibe la tabla de imagen como se muestra en la figura 6 se encuentra con un patrón cardíaco 1 siendo su principal imagen clave se encuentra con un patrón de trébol 4 siendo una segunda imagen clave, memoriza el número 14 como su posición y entonces manipula una tecla de dirección para ubicar el patrón cardíaco 1 en la posición del 14.

A este tiempo, memorizar el número de posición del patrón de trébol sirve para no perder la primera posición 3 pues el patrón de trébol también se mueve cuando se mueve el patrón cardíaco.

De esta manera, se puede pensar que la posición 3 designada por la segunda imagen clave es golpeada. El usuario puede memorizar fácilmente las imágenes clave utilizando el nombre de las imágenes o produciendo enunciados para memorizar como "amo al trébol" (un corazón puede movido a una posición en la que se localizó al trébol), "zanahoria a un panda" (una zanahoria es movida a una posición en donde se localizó el panda).

Para este método, cuando el servidor nuevamente produce la tabla de imagen antes de la transmisión, coordenadas de cada imagen clave pueden ser grabadas, y el movimiento de las coordenadas puede ser calculado de acuerdo con la manipulación clave del usuario.

Para este momento, otras útiles e interesantes funciones como una trampa clave 5 y un reporte 6 pueden ser pensados.

Tanto la llave de trampa como la llave de reporte son llaves predeterminadas por un usuario. En esta presentación, el usuario dispone una zanahoria 5 como la trampa clave, y una mariposa 6 como la llave de reporte. La llave de trampa es una llave que indica una posición a través de la que no se permite la circulación cuando la imagen clave se mueve.

Así, si el orden de una posición número 12-13-14 es movido en la figura 6, una posición 13 donde se ubica la zanahoria es una llave de trampa 5. Una alarma es generada de una bocina de computadora y la autenticación no es exitosa. Así, se prefiere un camino de 12-11-15-14, 12-7-8-9-14, etc. sea usada lejos de la zanahoria.

Además, si la llave de trampa es atrapada durante el proceso de autenticación, la llave de trampa transmite un mensaje de alarma a un usuario a través de un mensaje de texto a teléfono celular (sms) o a través de correo electrónico de manera que el usuario pueda tomar las medidas pertinentes.

Por ejemplo, el URL, que puede recibir un reporte, puede ser incluido en el mensaje de alarma. Si un reporte es recibido, un guardia puede ir a un punto para detener a un criminal.

La clave de reporte 6 permite a un usuario hacer el reporte sin ser notificado si un criminal penetra una empresa o casa con amenazas o cuando retira dinero, en caso de que dicha clave de reporte 6 sea usada como un mecanismo de autenticación en un aparato para cerrar puertas, un cajero automático, etc. Si el usuario falsea la segunda imagen clave considerándola la mariposa 6 de la llave del reporte o manipulándola directamente, la autenticación es exitosa y así pone al criminal en una situación vulnerable. En este caso, sin embargo, se elabora un reporte automáticamente para la policía o para una empresa de seguridad. Así, la clave del reporte puede ser una función en la que la función del reporte se añade a la función de la segunda imagen clave.

La clave de la trampa y la clave del reporte también aumentan el nivel de un peligro que intenta autenticación para que un usuario ilegal que quiera hacerse pasar por alguien más, y así se maximice el efecto de prevención.

Más adelante, un método para asignar un número a cada posición que se muestra en este método puede ser aplicado al método de la figura 4. En el método de la figura 4, se puede memorizar el patrón cardíaco al número 19 en lugar de memorizar que el patrón cardíaco se encuentra en la posición (4, 2)

Las figuras 7 y 8 muestran otras presentaciones de un método de autenticación por el ingreso de coordenadas. Este método es un caso donde las imágenes clave forman un par como 21(7) y 11(8).
21 es encontrado en una imagen ubicada a la izquierda de la tabla de la figura 7, y 11 se encuentra en una tabla de imagen ubicada a la derecha de la figura 7. Dos imágenes clave son encimadas al arrastrar la imagen de la derecha de la tabla usando el ratón de la computadora y más tarde se pegan. En este caso, si hay (21, 11) de entre varios pares de imágenes encimadas, la autenticación es exitosa.

Incluso en este caso, el arreglo de las tablas de imagen es cambiado al azar en cada ocasión. Así, incluso si la información sobre manipulación del ratón es conocida, la siguiente autenticación no será exitosa. Considerando que varios pares de imágenes son encimados al mismo tiempo, otros más atrás no sabrán qué par de imágenes es el par clave.

En este método, si dos tablas de imágenes corresponden al par de la imagen clave cuando el servidor produce las tablas de imagen, otras pueden saberlo fácilmente pues muchos menos pares de imágenes se encuentran encimados. Así, para poder prevenir esto, las tablas de imágenes en caso de que muchos menos pares de imágenes estén encimadas son rechazadas y se generan nuevas tablas de imágenes.

Los métodos arriba mencionados de las figuras 4 y 8 corresponden a un método en el que el proceso de presionar la imagen clave es seguro aunque otros pueden mirar de reojo. Para poder alcanzar el objeto primeramente una imagen clave y las coordinadas clave (o una segunda imagen clave arreglada dentro de una segunda tabla de imagen) que debe corresponder a su imagen clave debe también ser conocida para el usuario.

Segundo, cuando la posición de la imagen clave es manipulada, todas las otras imágenes son manipuladas al mismo tiempo en la misma dirección y siempre y cuando se trate de la misma distancia. Así, aunque otros lo vean, no se sabe qué imagen es manipulada. Como el arreglo de tablas de imágenes es presentada de manera diferente en cada ocasión, la autenticación no es exitosa sólo con el mismo valor de manipulación aunque el valor de manipulación sea sabido.

Además, incluso si la tecla de dirección es manipulada, el mismo efecto puede ser obtenido aunque las imágenes no se muevan. En este caso, el usuario puede dibujar una aguja indicadora sobre la imagen clave mentalmente, y mover la aguja junto con las coordenadas clave de acuerdo con la manipulación de la tecla de dirección.

Si las imágenes son movidas se mueve la imagen también, pero si las imágenes no se mueven, la aguja no se mueve. Así, quienes lo ven de lado no saben qué imagen es manipulada.

La Figura 9 muestra una presentación de una pantalla anti-respuesta contra la manipulación de una tecla de dirección.

En la presentación de la figura 9, si una regla de pasaje es un tipo de pasaje de dos puntos que comienza de una imagen clave y ésta una imagen coordenada y una imagen terminal coordenada que son una cerveza, un balón de fútbol y una televisión, una frase para memorizar podría ser "Ve una retransmisión de fútbol mientras tomas cerveza". En el ejemplo mostrado en la figura 9, una distancia de cerveza a balón de fútbol es una caja en dirección descendente, y una distancia del balón de fútbol a la televisión son dos cajas a la derecha y una caja hacia arriba.

Un proceso de manipulación total es "una tecla en dirección hacia abajo en una ocasión, *"enter"*, tecla de dirección a la derecha y una tecla hacia arriba, *"enter"*.

A continuación se describe una presentación de un conjunto de que prepara la personalización de de ataque por medio de un link fraudulento

La descripción del set de personalización será hecha asumiendo el caso de la figura 9.

El método como el mostrado en la figura 9 es ventajoso en el sentido de que un set de personalización en preparación para un ataque de link fraudulento puede ser fácilmente implementado. Así, los sets para pasar son registrados de forma diferente por cada persona.

Así, las imágenes clave y los puntos de pasaje no pueden ser conocidos usando sets falsos.

La figura 10 muestra una pantalla para producir un set de personalización.

Como se muestra en la figura 10, si un usuario selecciona su imagen clave y pasaje de imagen de coordenadas de imágenes que es mas que 16 necesaria en una asignatura y genera una asignatura personalizada incluyendo la imagen seleccionada como se muestra en la FIG. 9, asignaturas falsas son producidos para que sea difícil incluir todas las 3 imágenes de una persona correspondiente.

Suponiendo que 3 imágenes entre 36 imágenes como en FIG. 10 sean seleccionadas y las 13 imágenes restantes sean aleatoriamente seleccionadas para producir la asignatura personalizada, la probabilidad de que esas 3 imágenes específicas sean todas incluidas cuando se seleccionen las 16 imágenes de las 36 imágenes es de escaso 7.8%. Esto es, la probabilidad de que un criminal pase a través un asignatura falsa y luego robe la clave meta del usuario es 7.8%. Si imágenes especificas han de ser seleccionadas de entre 100 imágenes, la probabilidad disminuye considerablemente y resulta en un 0.3%.

Además, es evidente que la asignatura personalizada puede ser implementada para soportar una asignatura única mediante la carga de imágenes producidos por un usuario.

También, para poder dar un vistazo por adelantado a la asignatura personalizada y posteriormente intentar un ataque por medio de link fraudulento (*phishing*) usando una asignatura falsa, sería efectivo enviar un mensaje de alarma a la persona aun y cuando en el caso de que el criminal vea solo la asignatura personalizada pero no pase. El mensaje de alarma puede incluir un enunciado de aviso en el que se advierte que es mejor el cambiar una clave por que existe la posibilidad de que la asignatura personalizada este expuesta.

A continuación, un método para prevenir un intento de robo a una clave aplicando una asignatura personalizada, que es obtenida mediante la instalación de una herramienta para acceder ilegalmente a un ordenador teniendo una función de captura de imagen en otro ordenador para robar la asignatura personalizada antes descrita, hacia un sitio falso para intentar un ataque por medio de link fraudulento (*phishing*) será descrito. Aunque la captura puede ser prevenida por medio de tecnología anti-captura, este método es para prepararse para un caso donde una

herramienta para acceder ilícitamente a un ordenador no puede ser prevenida mediante la tecnología anti-captura exis nte.

La figura 12 muestra un ejemplo de una tabla de perfil de usuario para un servicio de autenticación de acuerdo a la presente invención. En este ejemplo, la información del ordenador principal 14 es grabada en cada usuario.

La figura 13 muestra un ejemplo de una interfase para registrar un ordenador principal de acuerdo a la presente invención.

Cuando la asignatura personalizada de conformidad con la presente invención es ejecutada en línea (*on-line*), información específica única 14 dentro de un ordenador de un usuario puede ser reconocida, ejemplo, dirección MAC de una tarjeta de red de área local (LAN) o un ordenador de un usuario puede ser reconocido utilizando una *cookie*. Si el ordenador es reconocido como un ordenador que no ha sido registrado en el perfil del usuario, un mensaje de alerta es enviado a un punto de contacto 15 designado por el usuario, y la interfase para registrar el ordenador principal como se muestra en la figura 13 es provisto para que el usuario pueda tomar los pasos necesarios.

El mensaje de alarma notifica al usuario del hecho de que la autentificación ha sido intentada por un ordenador no registrado por el usuario para que el usuario pueda estar preparado para el acceso ilegal de su información personal.

Adicionalmente, la interfase para registrar el ordenador principal permite al usuario registrar su ordenador actualmente en uso, como el ordenador principal.

En este momento, el ordenador registrado es reconocido como el ordenador principal del usuario y por tanto es tratado de manera diferente a ordenadores extraños no registrados.

Que el ordenador principal del usuario y el ordenador extraño sean tratados de manera diferente significa que las claves para pasar a través de la autentificación se programan para ser diferentes. Por ejemplo, una clave 12 utilizada en el ordenador principal y una clave 13 usada en un ordenador extraño pueden ser programadas para ser completamente diferentes, o todas las claves pueden pasar a través del ordenador extraño pero algunas de las claves pueden pasar a través del ordenador principal. Esto es, aunque el ataque por medio de link fraudulento (*phishing*) sea

exitoso, solo la clave 12 para el ordenador es robada, lo que lo hace difícil para un uso fraudulento por un atacante quién tiene que ingresar la clave 13 para el ordenador 13.

Además, el método de confirmación de claves, diferente en cada ordenador, es efectivo en prevenir el uso fraudulento en un ordenador extraño aún con la autentificación de un texto existente ingresado y autentificado por el ing so coordinado. Esto es, si una clave de acceso es de 8 posiciones, las 8 posiciones son todas confirmadas en el ordenador extraño, pero solo 4 posiciones están confirmadas en el ordenador principal. Es sin embargo, posible el prevenir uso fraudulento en el ordenador extraño a pesar de que la contraseña sea robada.

Si la presente invención es aplicada a servicios de acceso de seguridad, es evidente que existe un efecto suficiente de prevención para el acceso ilegal a un ordenador a pesar de que el paso de rastreo de ubicación de acceso sea omitido.

Además, puede ser visto que un efecto de seguridad es suficiente a pesar de que un paso dual de autentificación no sea practicado.

A continuación, se dará una descripción respecto al método en el cual la presente invención es aplicada a aparatos tales como teléfonos móviles, un seguro para puertas y una caja fuerte de forma incluida.

En el teléfono móvil, el seguro para puertas, la caja fuerte y así sucesivamente, no hay necesidad de confirmar quién es quién entre numerosas personas como en los servicios de Internet o de un Banco. Por tanto, no es necesario confirmar una identificación de acceso (ID) y una contraseña.

Por lo que, existe menor necesidad de ejecutar el primer y segundo paso de autentificación antes descritos. Además, en estos aparatos, el teclado es un teclado compacto, no un teclado como el utilizado en un ordenador. En este teclado, es conveniente el ingresar números, pero inconveniente ingresar caracteres. Por esta razón, la contraseña en este aparato usualmente solo se compone de números. Este es el resultado de un ancho de bando muy estrecho de la contraseña. Más aún, como no existe ningún significado en los números, una contraseña relacionada con información personal es utilizada para encontrar números significativos que puedan

ser fácilmente memorizados. Esta contraseña es desventajosa pues puede ser fácilmente analogada por terceros.

La figura 11 muestra una personificación en la cual la presente invención es aplicada a un teléfono móvil.

Como se muestra en la figura 11, en el caso donde una contraseña de texto es primeramente ingresada y el ingreso de coordenadas es completado mediante la presentación de una tabla de imagen para coordinar la autentificación sin confirmar la contraseña, si se determina permitir el paso mediante la confirmación de la contraseña de texto y de las coordenadas en un tiempo, el número de casos es 10,000 cuando una contraseña numérica es únicamente de 4 posiciones, y si es una regla de pasaje de 2 puntos en una tabla de imagen 16, el número de casos es 210. No son simplemente sumados, sino multiplicados, resultando en 2.1 millones el número total de casos. Esto significa que asumiendo que tome una hora encontrar un número de contraseña, todo un mes se toma para encontrar el número completo de la contraseña si se invierten 7 horas al día.

A este extremo, el proceso puede ser programado para permitir un pasaje solo cuando ambos, el texto ingresado y la coordenada ingresada, sean válidas sin el proceso de confirmar el ingreso de texto y el ingreso de coordenada intermediariamente.

El tipo incluido antes descrito, es muy útil en los seguros para puertas. Esto significa que no solamente el ancho de banda de una contraseña se amplia, sino también todas las personas pertinentes pueden usar la contraseña numérica.

Esto es, en una clave numérica existente, como todos los miembros que lo constituyen utilizan una sola clave, no es conveniente informar a todos los miembros que la constituyen sobre una nueva contraseña. Entonces es muy común usar la clave por un largo tiempo sin cambiarla. En la presente invención, si se registran tantas claves como número de miembros que la constituyen, cada miembro puede manejar cada clave separadamente. También, como el ancho de banda es suficientemente amplio como para ser compartido por una pluralidad de miembros que la constituyen, puede ser usada de manera segura en la mayoría de seguros para puerta en una oficina, mas aún, existe una ventaja en que la entrada y salida pueda ser administrada en una base de miembros que la constituye.

Adicionalmente, si se usa un seguro para puerta al cual se le aplican tecnologías avanzadas tales como un chip electrónico o biométrico, el nivel de seguridad no disminuirá al nivel de seguridad de una clave numérica proveída como una llave de ayuda.

REIVINDICACIONES

1.- Un método de servicio de acceso de seguridad para procesar el registro de un miembro en un servicio en linea, caracterizado porque comprende:

Un paso de autenticación por la introducción de texto;
Un paso de de rastreo de localización de acceso;
Un paso de autenticación a través de la introducción de coordenadas, y
Un paso de reporte de acceso al historial.

2.- El método de servicio de acceso de seguridad de acuerdo con la reivindicación 1, caracterizado además porque el paso de rastreo de localización de acceso es efectuado entre los dos pasos de autenticación.

3.- El método de servicio de acceso de seguridad de acuerdo con la reivindicación 1, caracterizado además porque el paso de reporte de acceso al historial incluye los pasos de:

Si se intenta otro acceso con un usuario que ya ha accedido, compara la ubicación de la persona que intenta acceder, lo cual se obtiene en el paso de rastreo de localización de acceso, con la localización de acceso de un estatus de registro actual y si la localización del usuario y de la ubicación de acceso del estatus actual de registro son diferentes, inmediatamente reporta la ubicación de acceso de la persona que trata de acceder al usuario del estatus actual registrado a través de una pantalla y.

Si la ubicación del usuario y la ubicación de acceso del estatus actual de registro son las mismas, la información posicional obtenida de la persona que intenta acceder es reportada siempre al usuario en el siguiente inicio de sesión.

4.- El método de servicio de acceso de seguridad de acuerdo con la reivindicación 1, caracterizado además porque el paso de reporte de acceso al historial incluye el paso de, si el paso de autenticación para el acceso de las coordenadas falla, inmediatamente envía un mensaje de alarma a través los medios de mensaje diseñados por el usuario.

5.- Un método de servicio de acceso de seguridad para procesar el registro del miembro en un servicio en linea, caracterizado porque comprende:

Un paso de autenticación a través de la introducción de texto; y
Un paso de autenticación a través de la introducción de coord nadas.

6.- Un método de servicio de acceso de seguridad de acuerdo con cualquiera de las reivindicaciones 1 a 5, caracterizado además porque el paso de autenticación a través de la introducción de las coordenadas comprende los pasos de:

Transmitir una tabla de imágenes en la cual una imagen clave es aleatoriamente mezclada con una pluralidad de otras imágenes en la pantalla del usuario;

Manipular todas las imágenes para tener el mismo valor al mismo tiempo de acuerdo a un valor de manipulación del teclado o del ratón del ordenador del usuario;

Confirmar una posición manipulada por la imagen clave, y si las coordenadas cuya manipulación de una posición es confirmada y las coordenadas clave previamente diseñadas por el usuario coinciden entre sí, determina que esa autenticación es exitosa pero si dichas coordenadas no coinciden entre sí, determina que la autenticación no fue exitosa.

7.- El método de servicio de acceso de seguridad de acuerdo con la reivindicación 6, caracterizada además porque las coordenadas clave son posiciones diseñadas usando una segunda imagen clave.

8.- El método de servicio de acceso de seguridad de acuerdo con la reivindicación número 7, caracterizado además porque comprende el paso de, si la primera imagen clave pasa a través de una posición diseñada por una imagen clave de trampa a través de la manipulación del usuario, determinando que la autenticación no es exitosa, y transmitiendo un mensaje de alarma a un ordenador del usuario o a un propietario original de un código de identificación (ID).

9.- El método de servicio de acceso de seguridad de acuerdo a la reivindicación 7 caracterizado además porque comprende los pasos de, si el usuario coloca una primera imagen clave en una posición diseñada por una imagen clave de reporte y posteriormente confirma la manipulación, determina que a autenticación es exitosa permitiendo este hecho ser automáticamente reportada a través de un sistema de guardia.

10.- Un método para autenticar con seguridad a un usuario, caracterizado porque comprende los pasos de:

Transmitir una tabla de imágenes en la cual una imagen clave es aleatoriamente mezclada con una pluralidad de otras imágenes a una pantalla del usuario;

Manipular la totalidad de las imágenes para tener el mismo valor al mismo tiempo de acuerdo a un valor de manipulación de un teclado o de un ratón de ordenador del usuario;

Confirmar una posición manipulada por la imagen clave; y si las coordenadas cuya manipulación de una posición es confirmada y las coordenadas clave previamente diseñadas por el usuario coinciden entre sí, determina que la autenticación es exitosa y si dichas coordenadas no coinciden entre sí, determina que la autenticación no es exitosa.

11. El método para autenticar con seguridad de acuerdo con la reivindicación 10, caracterizado además porque las coordenadas clave son posiciones diseñadas usando una segunda imagen clave.

12.- El método para autenticar con seguridad de acuerdo con la reivindicación 11 caracterizado además porque comprende el paso de, si una primera imagen clave pasa a través de una posición diseñada por una imagen clave de trampa a través de la manipulación del usuario, determina que la autenticación no es exitosa, y transmite un mensaje de alarma a un ordenador del usuario o a un propietario original de un código de identificación (ID).

13.- El método para autenticar con seguridad de acuerdo con la reivindicación 11, caracterizado además porque comprende el paso de, si el usuario coloca una primera imagen clave en una posición diseñada por una imagen clave de reporte y luego confirma la manipulación, determina que la autenticación es exitosa, permitiendo este hecho ser automáticamente reportado a través de un sistema de guardia.

14.- El método para autenticar con seguridad de acuerdo con cualquiera de las reivindicaciones 1 a 9, caracterizado además porque comprende el paso de registrar una tabla de imágenes de personalización en la cual un historial de construcción de

imágenes de tablas de imágenes proveídas es registrada de manera distinga en una base de usuario.

15.- El método para autenticar con seguridad de acuerdo con la reivindicación 14, caracterizado además porque el paso de registro de la personalización de la tabla de imágenes comprende los pasos de:

Permitir al usuario seleccionar una imagen clave a través de una imagen de coordenadas o una imagen de coordenadas de terminal de un grupo de imágenes, cuyo número es mucho mayor que las imágenes que son requeridas en la tabla de personalización de imagen y posteriormente introducir las imágenes seleccionadas;

Permitir a un servidor extraer aleatoriamente tantas imágenes como el número de las que son necesarias para completar la tabla de imágenes, de las imágenes restantes excepto por las seleccionadas, y mezclando las imágenes que son seleccionadas e introducidas por el usuario y las imágenes que son seleccionadas por el servidor, y registrando la personalización de la tabla de imágenes.

16.- El método para autenticar con seguridad de acuerdo con cualquiera de las reivindicaciones 10 a 13, caracterizado además porque comprende el paso de introducir un texto de contraseña, y

Porque el paso del proceso de autenticación incluye determinar que la autenticación es exitosa solamente cuando tanto el texto de contraseña como las coordenadas clave son válidas luego que la introducción del texto de contraseña y las coordenadas ha sido completada, y se determina que la autenticación no es exitosa si el texto de la contraseña o las coordenadas clave no son válidos.

17.- El método para autenticar con seguridad de acuerdo con lo reivindicado en cualquiera de las reivindicaciones 1 a 9, 14 y 15 caracterizado además porque comprende:

Un paso de registro de coordenadas para proveer a la interfase para que permita el usuario definir diferentemente las coordenadas clave para un ordenador principal y unas coordenadas clave para una computadora extraña y registrar la información introducida;

Un paso de adquisición de información terminal de adquisición de información reconocida de un ordenador del usuario;

Un paso de reconocimiento de terminal para determinar al ordenador como el ordenador principal o el ordenador extraño basado en la información reconocida en el ordenador del usuario, la cual se obtiene en el paso de la adquisición de la información de la terminal.;

Un paso de registro de un ordenador principal, si está determinado que el ordenador es el extraño en el paso de reconocimiento de la terminal, registrado la información del ordenador para proveer una interfase de registro de ordenador principal, y registrar la información introducida; y

Un paso de alarma de ordenador extraño, si en el paso de reconocimiento de terminal se determina que el ordenador no es el principal, notificando al usuario del mensaje de alarma sin importar el resultado de la autenticación,

En donde el paso de autenticación a través de la introducción de las coordenadas incluye determinar si las coordenadas, la manipulación de la posición de la que es confirmada y las coordenadas clave previamente diseñadas por el usuario coinciden entre si, si se determina que el ordenador es el principal en el paso de reconocimiento de la terminal, confirma las coordenadas clave para el ordenador principal, y si se determina que el ordenador es el extraño en el paso de reconocimiento de terminal, confirma las coordenadas clave para el ordenador extraño.

18.- El método para autenticar con seguridad de acuerdo con la reivindicación 17, caracterizado además, porque las coordenadas clave son dos o mas, y todas las coordenadas clave se confirman en el ordenador extraño y solamente algunas de las coordenadas clave son confirmadas en el ordenador principal.

19.- Un método para autenticar con seguridad a un usuario, caracterizado porque comprende los pasos de:

Un paso de registro de contraseña que provee la internase para permitir a un usuario definir diferentemente contraseñas para un ordenador principal y contraseñas para un ordenador extraño, y almacenar la información introducida;

Un paso d reconocimiento de terminar para determinar el ordenador como el principal o como el ordenador extraño basados en información reconocida del ordenador del usuario, la cual es adquirida en el paso de adquisición de información de la terminal;

Un paso de registro de ordenador principal, si se determina que el ordenador es el extraño en el paso de reconocimiento de terminal, registrando la información del ordenador para proveer una interfase de registro de ordenador principal que puede ser registrada como el ordenador principal; y

Un paso de procesamiento de autenticación, si se determina que el ordenador es el principal en el paso de reconocimiento de terminal, confirmando una contrasefia para el ordenador principal, y si se determina que el ordenador es el extraño en el paso de reconocimiento de terminal, confirma una contrasefia para el ordenador extraño.

20.- El método para autenticar con seguridad de acuerdo con la reivindicación 19, caracterizado además porque comprende los pasos de:

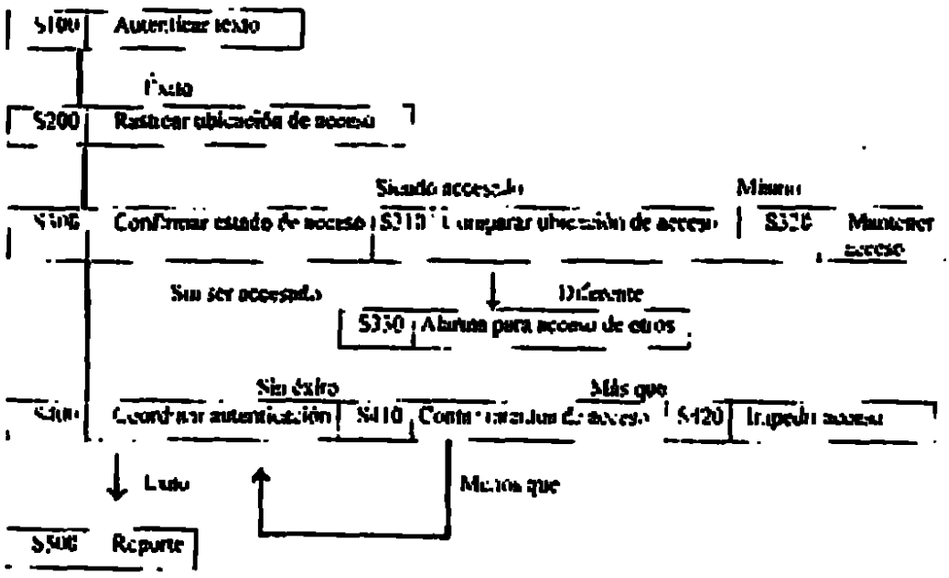
Proveer la interfase para permitir al usuario registrar un punto de contacto donde el mensaje de alarma sea recibido, y guardar la información ingresada; y

Un paso de alarma de ordenador extraño, si se determina que el ordenador es el extraño en el paso de reconocimiento de terminal, notificando el mensaje de alarma al punto de contacto sin importar el resultado de la autenticación.

RESUMEN

La presente invención se refiere a hacer segura la autenticación. De acuerdo a la presente invención, un método de servicio de acceso de seguridad incluye un paso de autenticación a través de la introducción de un texto, un paso de rastreo de ubicación de acceso, un paso de autenticación a través de la introducción de coordenadas y un paso de reporte de acceso al historial.

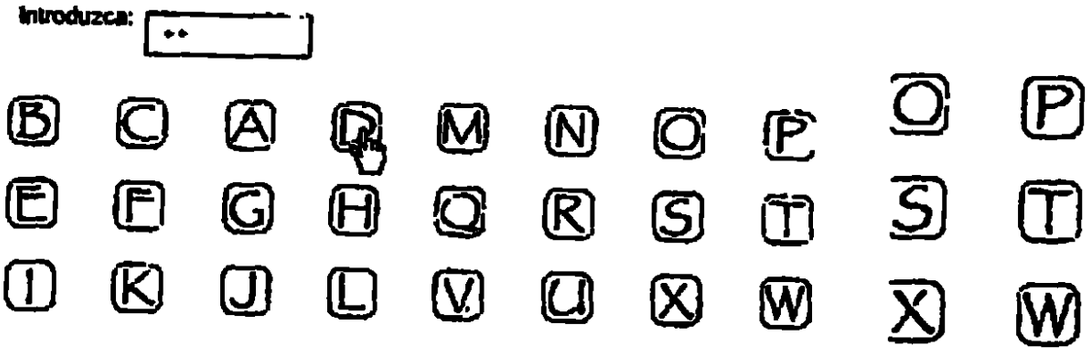
[Fig.1]



[Fig.2

Imagen de contraseña reducida en secuencia

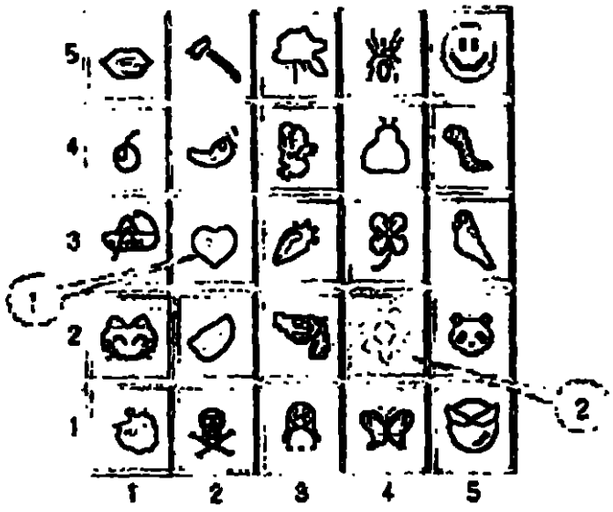
Imagen de contraseña reducida en secuencia



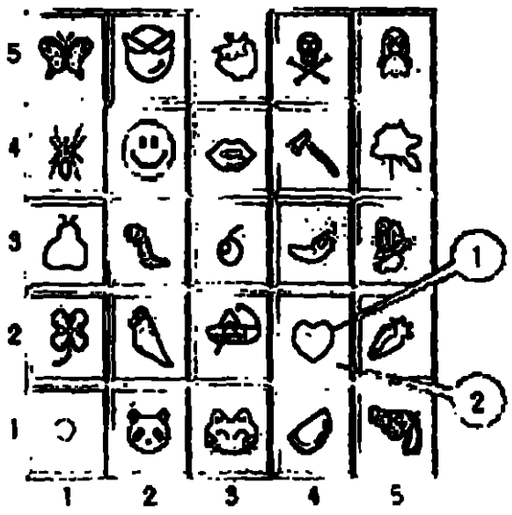
【Fig.3】

Fecha de acceso	Ubicación de acceso	Resultado de autenticación	Hora de acceso
9/14 22:02	203.66.101.2	segunda autenticación fallida	-
9/14 10:37	168.253.66.15	segunda autenticación fallida	12.14
9/13 19:05	168 253.66.15	segunda autenticación fallida	45 06
9/13 09:57	168 253 66.15	segunda autenticación fallida	28:11

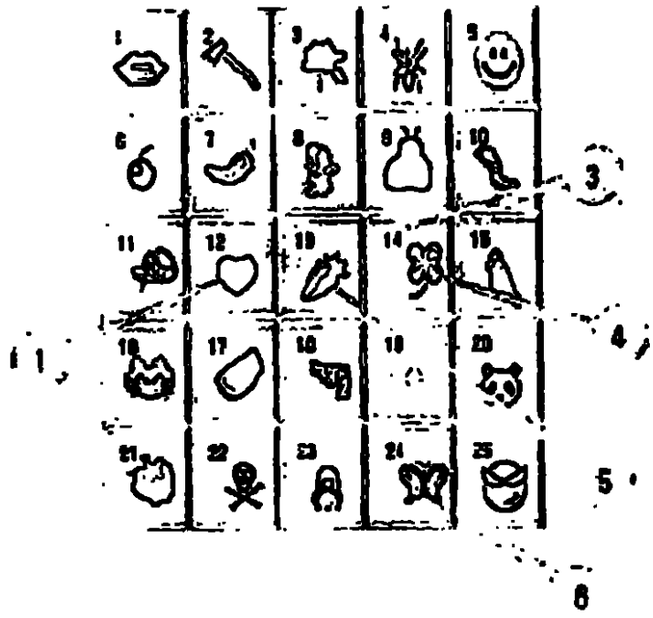
【Fig.4】



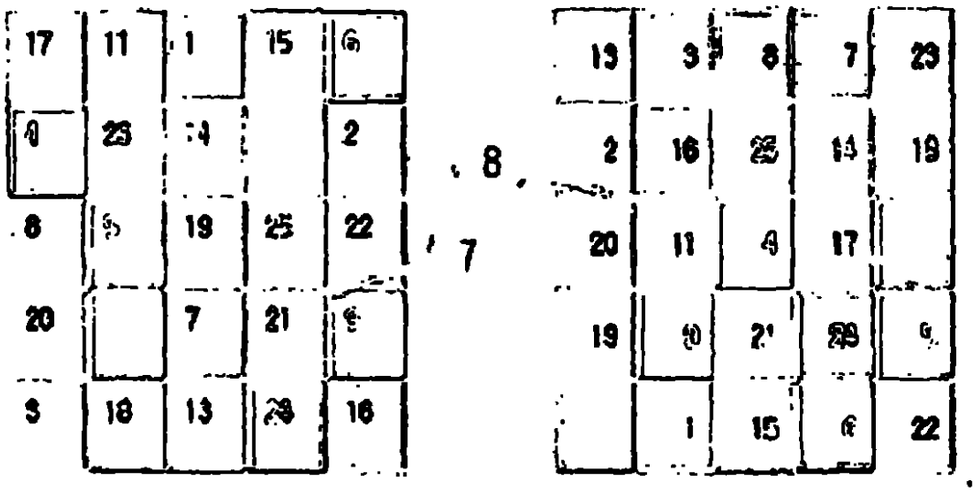
【Fig.5】



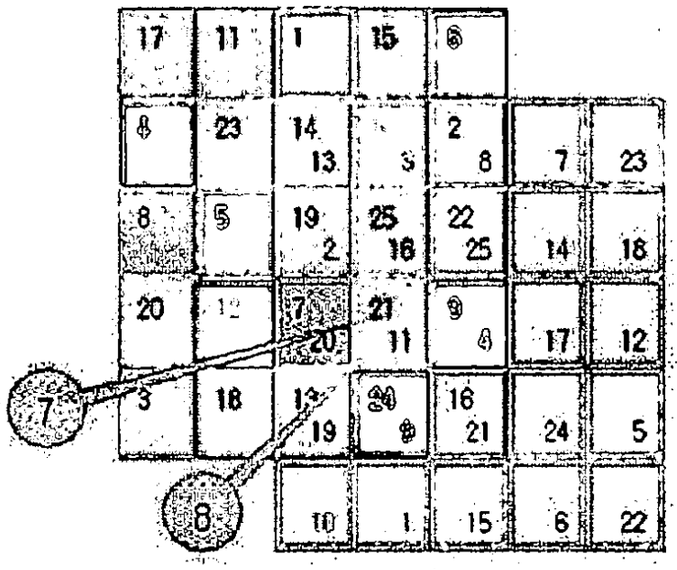
[Fig 6]



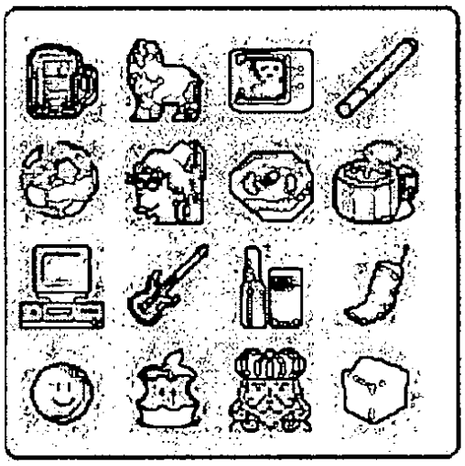
[Fig.7]


17 11 1 15 6
4 25 14 2
8 5 19 25 22
20 7 21 9
3 18 13 23 16
8
7
13 3 8 7 23
2 16 25 14 19
20 11 4 17
19 10 21 23 9
1 15 6 22

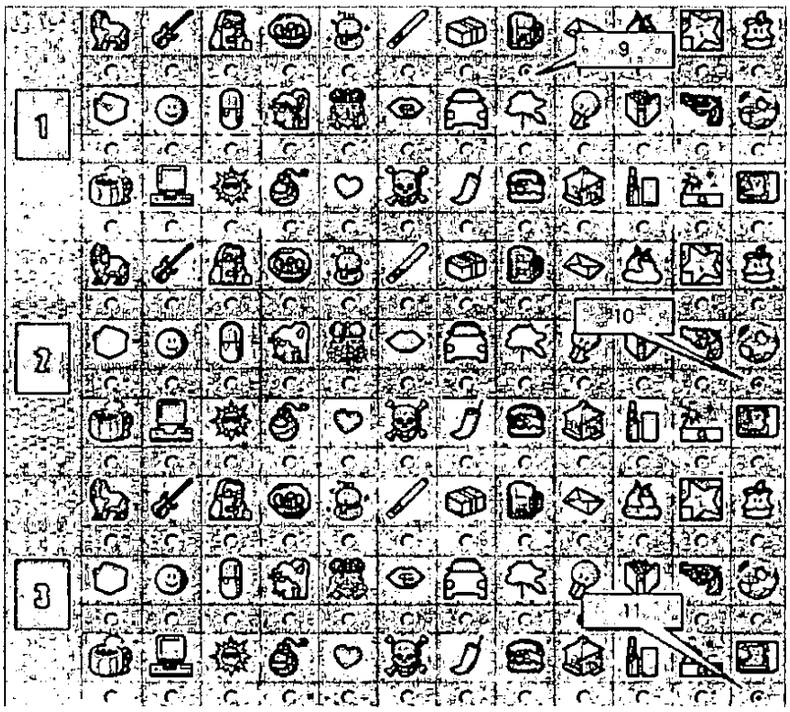
【Fig.8】



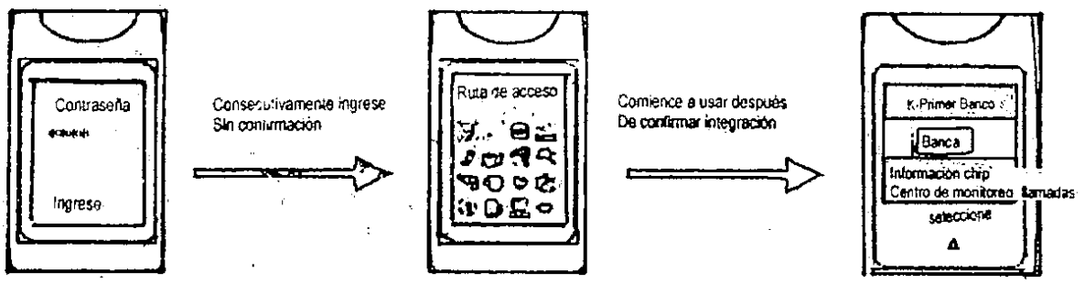
【Fig.9】



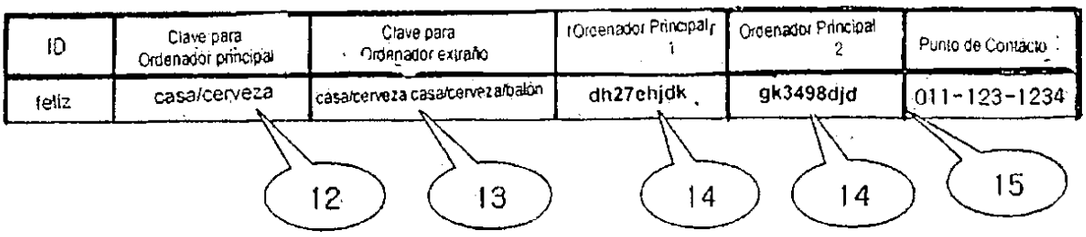
【Fig.10】


1
2
3
9
10
11

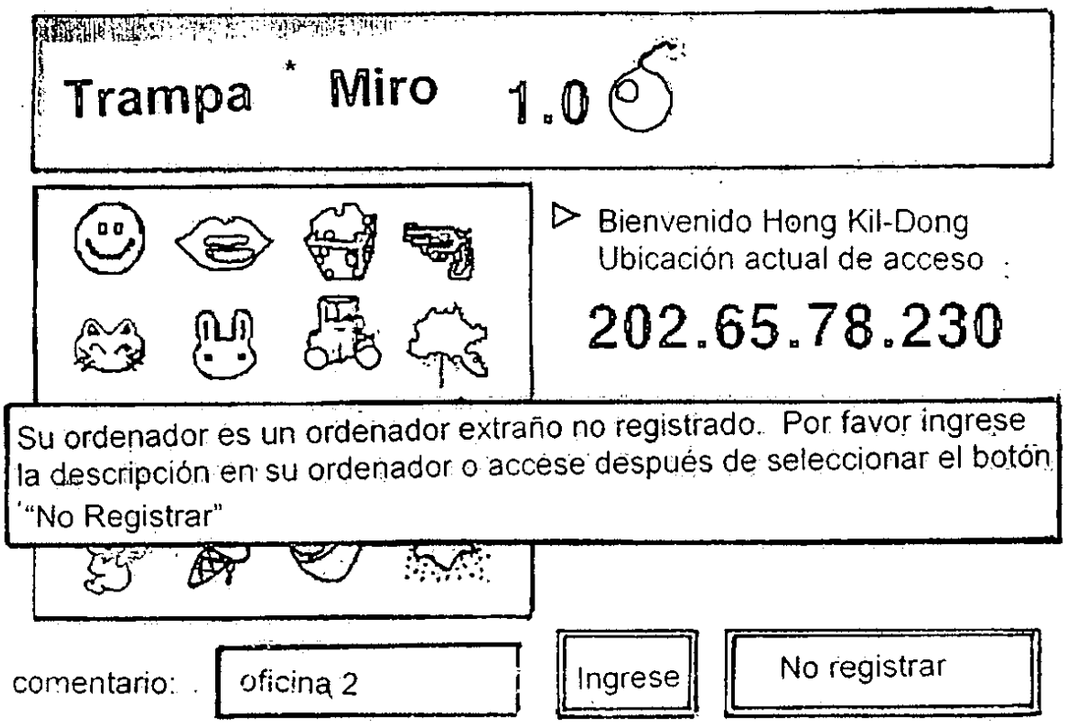
【Fig.11】


Contraseña
Ingrese
Consecutivamente ingrese
Sin confirmación
Ruta de acceso
Comience a usar después
De confirmar integración
K-Primer Banco
Banca
Información chip
Centro de monitoreo
llamadas
seleccione

【Fig.12】


ID
Clave para Ordenador principal
Clave para Ordenador extraño
Ordenador Principal 1
Ordenador Principal 2
Punto de Contacto
feliz
casa/cerveza
casa/cerveza casa/cerveza/balón
dh27ehjdk
gk3498djd
011-123-1234
12
13
14
14
15

【Fig.13】


Trampa Miro 1.0
Bienvenido Hong Kil-Dong
Ubicación actual de acceso
202.65.78.230
Su ordenador es un ordenador extraño no registrado. Por favor ingrese la descripción en su ordenador o accese después de seleccionar el botón "No Registrar"
comentario:
oficina 2
Ingrese
No registrar

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 March 2005 (31.03.2005)

PCT

(10) International Publication Number
WO 2005/029216 A2

(51) International Patent Classification⁷: G06F

(21) International Application Number:
PCT/KR2004/003495

(22) International Filing Date:
25 September 2004 (25.09.2004)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2003-0066452
25 September 2003 (25.09.2003) KR
10-2004-0053149 8 July 2004 (08.07.2004) KR
10-2004-0068356 30 August 2004 (30.08.2004) KR

(71) Applicant and
(72) Inventor: HWANG, Jay-Yeob [KR/KR]; 1555 Bunji Joongsan village, doosan apartment 108-708, Baan2-Dong Ilsan-Gu, Goyang 411 728 (KR).

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

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 2005/029216 A2

(54) Title: THE METHOD OF SAFE CERTIFICATION SERVICE

(57) Abstract: The present invention relates to safe authentication. According to the present invention, a security access service method includes an authentication step by the input of card, an access location tracking step, an authentication step by the input of confirmation, and an access history report step.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 March 2005 (31.03.2005)

PCT

(10) International Publication Number
WO 2005/029216 A3

(51) International Patent Classification⁷: G06F 17/00

(21) International Application Number:
PCT/KR2004/003495

(22) International Filing Date:
25 September 2004 (25.09.2004)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2003-0066452 25 September 2003 (25.09.2003) KR
10-2004-0053149 8 July 2004 (08.07.2004) KR
10-2004-0066356 30 August 2004 (30.08.2004) KR

(71) Applicant and
(72) Inventor: HWANG, Jay-Yeob [KR/KR]; 1555 Bunji joongsan village, dosan eyomyun 108-705, Nam2-Dong Ilsan-Gu, Goyang 411-728 (KR).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
2 June 2005

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 2005/029216 A3

(54) Title: THE METHOD OF SAFE CERTIFICATION SERVICE

(57) Abstract: The present invention relates to safe authentication. According to the present invention, a security access service method includes an authentication step by the input of user, an access location tracking step, an authentication step by the input of coordinates, and an access history report step.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2004/003495

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 G06F 17/00

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)

IPC7 G06F 17/00, H04L 12/22

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

Korean patents and applications for inventions since 1975

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 2001-109864 A (3WINDOTCOM INC.) 12 DEC. 2001 SEE THE WHOLE DOCUMENTS	1-20
A	KR 2002-71293 A (JUN JONG-CHAN) 12 SEP. 2002 SEE THE WHOLE DOCUMENTS	1-20
A	KR 2002-54459 A (LG ELECTRONICS) 9 JUL. 2002 SEE THE WHOLE DOCUMENTS	1-20
A	KR 2001-42902 A (SUNMICRO SYSTEMS INC.) 25 MAY 2001 SEE THE WHOLE DOCUMENTS	1-20

☐ 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
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 MARCH 2005 (18.03.2005)	29 MARCH 2005 (29.03.2005)
Name and mailing address of the ISA/KR Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer JEONG, Jae Hoon Telephone No. 82-42-481-5787

Form PCT/ISA/210 (second sheet) (January 2004)

(12) SOLICITUD INTERNACIONAL PUBLICADA EN VIRTUD DEL TRATADO DE COOPERACION EN MATERIA DE PATENTES (PCT)

(19) Organización Mundial de la Propiedad Intelectual
Oficina Internacional

(43) Fecha de la Publicación Internacional
Marzo 31 de 2005 (31.03.2005)

(10) Numero de Publicación Internacional WO 2005/029216 A2

---

(51) Clasificación Internacional de Patentes[7]: G06F

(21) Número de la solicitud internacional: PCT/KR2004/002495

(22) Fecha de depósito internacional: 25 de Septiembre de 2004 (25.09.2004)

(25) Idioma del depósito: Koreano

(26) Idioma de la publicación: Inglés

(30) Datos referentes a la prioridad:

10-2003-0066452	25 de Septiembre de 2003 (25.09.2003)	KR
10-2004-0053149	08 de Julio de 2004 (08.07.2004)	KR
10-2004-0068356	30 de Agosto de 2004 (30.08.2004)	KR

(71) Depositante e

(72) Inventor: HWANG, Jay-Yeob (KR/KR); 1555 Bunji-juongsan village, doosan apartment 108-708, Ilsan2-Dong Ilsan-Gu, Goyang 411-728 (KR).

(81) Estados Designados (*Salvo indicación en contrario, para todo título de Protección Nacional disponible):* AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Estados designados (*salvo indicación en contrario para todo título de protección regional disponible):* ARIPO, (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW,), Eurasia (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), Europeas, (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publicado:

- Sin informe de búsqueda internacional y para ser publicado al recibo de ese informe.

En lo que respecta a los códigos de dos letras y otras abreviaturas, consultar las "Notas Explicativas referentes a los códigos y abreviaturas" que figuran al final de cada número ordinario de la Gazeta del PCT.

(54) Título: METODO DE SERVICIO DE CERTIFICACION SEGURA

(57) Resumen: La presente invención se refiere a hacer segura la autenticación. De acuerdo a la presente invención, un método de servicio de acceso de seguridad incluye un paso de autenticación a través de la introducción de un texto, un paso de rastreo de ubicación de acceso, un paso de autenticación a través de la introducción de coordenadas y un paso de reporte de acceso al historial.

(12) SOLICITUD INTERNACIONAL PUBLICADA EN VIRTUD DEL TRATADO DE COOPERACION EN MATERIA DE PATENTES (PCT)

(19) Organización Mundial de la Propiedad Intelectual
Oficina Internacional

(43) Fecha de la Publicación Internacional
Marzo 31 de 2005 (31.03.2005)

(10) Numero de Publicación Internacional WO 2005/029216 A3

---

(51) Clasificación Internacional de Patentes[7]: G06F 17/00

(21) Número de la solicitud internacional: PCT/KR2004/002495

(22) Fecha de depósito internacional: 25 de Septiembre de 2004 (25.09.2004)

(25) Idioma del depósito: Koreano

(26) Idioma de la publicación: Inglés

(30) Datos referentes a la prioridad:

10-2003-0066452	25 de Septiembre de 2003 (25.09.2003)	KR
10-2004-0053149	08 de Julio de 2004 (08.07.2004)	KR
10-2004-0068356	30 de Agosto de 2004 (30.08.2004)	KR

(71) Depositante:

(72) Inventor: HWANG, Jay-Yeob (KR/KR); 1555 Bunji-joongsm village, doosan apartment 108-708, Ilsan2-Dong Ilsan-Gu, Goyang 411-728 (KR).

(81) Estados Designados (*Salvo indicación en contrario, para todo tipo de Protección Nacional disponible*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Estados designados (*salvo indicación en contrario para todo título de protección regional disponible*): ARIPO, (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW,), Eurasia (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), Europeas, (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publicado:

- En relación con investigación internacional.

- Antes de la expiración del período previsto para la modificación de las reivindicaciones, será publicado si se reciben las modificaciones.

(88) Fecha de publicación del informe de búsqueda internacional:

2 de Junio de 2005

En lo que respecta a los códigos de dos letras y otras abreviaturas, consultar las "Notas Explicativas" referentes a los códigos y abreviaturas" que figuran al final de cada número ordinario de la Gazeta del PCT.

(54) Título: METODO DE SERVICIO DE CERTIFICACION SEGURA

(57) Resumen: La presente invención se refiere a hacer segura la autenticación. De acuerdo a la presente invención, un método de servicio de acceso de seguridad incluye un paso de autenticación a través de la introducción de un texto, un paso de rastreo de ubicación de acceso, un paso de autenticación a través de la introducción de coordenadas y un paso de reporte de acceso al historial.

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

SOLMAZE CO., LTD
1212 Kolong Digital Tower
222-7 Guro3-dong
Guro-gu
Seoul 152-777
Republic of Korea

Date of mailing (day/month/year)	
06 June 2005 (06.06.2005)	
Applicant's or agent's file reference	**IMPORTANT NOTIFICATION**
auth_maze	
International application No.	**International filing date (day/month/year)**
PCT/KR2004/002496	25 September 2004 (25.09.2004)

1. The following indications appeared on record concerning:

[X] the applicant [ ] the inventor [ ] the agent [ ] the common representative

Name and Address	State of Nationality	State of Residence
HWANG, Jay-Yeob 106-dong 703-ho, 1555 Bunji-Joongsan village Jisan2-Dong Ilsan-Gu Goyang-Si, Gyunggi-do 411-728 The Republic of Korea	KR	KR
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[X] the person [ ] the name [ ] the address [ ] the nationality [ ] the residence

Name and Address	State of Nationality	State of Residence
SOLMAZE CO., LTD 1212 Kolong Digital Tower 222-7 Guro3-dong Guro-gu Seoul 152 777 Republic of Korea	KR	KR
	Telephone No. 82-2-2103-2410	
	Facsimile No.	
	Teleprinter No.	

3. Further observations, if necessary:
The person in Box No.1 remains as applicant for US only and inventor for all designated States. The one in Box No.2 is now recorded as applicant for all designated States except US.

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[X] the designated Offices concerned
[ ] the elected Offices concerned
[ ] other:

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Kinam HA (fax 338-7090)
Facsimile No. (41-22) 338 70 90	Telephone No. (41-22) 338 8031

Form PCT/IB/308 (March 1994) 006710827

PATENT COOPERATION TREATY

79

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To

LEE, In, Sik
1114 Geumsan Bldg.
17-1, Yeouido-dong
Yeongdeungpo-gu
Seoul 150-727
Republic of Korea

RECEIVED
2006 06. 12.
ACORE

Date of mailing (day/month/year)	IMPORTANT NOTIFICATION
31 March 2006 (31.03.2006)	
Applicant's or agent's file reference: auth_maze	
International application No.: PCT/KR2004/002495	International filing date (day/month/year): 25 September 2004 (25.09.2004)

1. The following indications appeared on record concerning:

[X] the applicant [X] the inventor [ ] the agent [ ] the common representative

Name and Address	State of Nationality	State of Residence
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[X] the person [ ] the name [ ] the address [ ] the nationality [ ] the residence

Name and Address	State of Nationality	State of Residence
YANG, Ki, Ho 126-26, Daesin-dong Seodaemun-gu Seoul 120-160 Republic of Korea	KR	KR
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	

3. Further observations, if necessary:
The person identified in Box 2 should be added to the record as applicant for the United States of America only and inventor for all designated States.

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[X] the designated Offices concerned
[ ] the elected Offices concerned
[ ] other:

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Rodolfo CLEMENTE
Facsimile No. +41 22 338 7090	Telephone No. (41-22) 338 8456

Form PCT/IB/308 (March 1994) 009828820

80

Industria y Comercio
SUPERINTENDENCIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIVISION DE NUEVAS CREACIONES
EXTRACTO PARA PUBLICACIÓN
SOLICITUD DE PATENTE DE INVENCIÓN PCT

(21) No. de solicitud: (22) Fecha de solicitud: 25-04-2006 0:SI (31) 10-2003-0066482 (32) 25-09-2003 (33) KR 10-2004-0053140 08-07-2004 KR 10-2004-0068356 30-08-2004 KR	(51) Int Cl: (71) Solicitante(s): SOLMAZE CO., LTD. (Korea Corp.) (72) Inventor(es): HWANG JAY-YEUB YANG KI-HO (74) Agente: JESUS ARMANDO CARDENAS ALFARO
(85) Fecha inicio fase nacional: (86) Datos relativos a la presentación de la solicitud PCT Fecha de presentación de la solicitud: 25-09-2004 No. de solicitud PCT/KR2004/002495	(87) Publicación internacional Fecha: 31-03-2005 No. publicación: WO 2005/029821 OOR 6
(54) Título. METODO DE SERVICIO DE CERTIFICACIÓN SEGURA	

Reivindicación(es):

1. Un método de servicio de acceso de seguridad para procesar el registro de un miembro en un servicio en línea, caracterizado porque comprende:
   Un paso de autenticación por la introducción de texto;
   Un paso de de rastreo de localización de acceso;
   Un paso de autenticación a través de la introducción de coordenadas, y
   Un paso de reporte de acceso al historial.
2. El método de servicio de acceso de seguridad de acuerdo con la reivindicación 1, caracterizado además porque el paso de rastreo de localización de acceso es efectuado entre los dos pasos de autenticación.
3. El método de servicio de acceso de seguridad de acuerdo con la reivindicación 1, caracterizado además porque el paso de reporte de acceso al historial incluye los pasos de:
   Si se intenta otro acceso con un usuario que ya ha accedido, compara la ubicación de la persona que intenta acceder, lo cual se obtiene en el paso de rastreo de localización de acceso, con la localización de acceso de un estatus de registro actual y si la localización del usuario y de la ubicación de acceso del estatus actual de registro son diferentes, inmediatamente reporta la ubicación de acceso de la persona que trata de acceder al usuario del estatus actual registrado a través de una pantalla y,
   Si la ubicación del usuario y la ubicación de acceso del estatus actual de registro son las mismas, la información posicional obtenida de la persona que intenta acceder es reportada siempre al usuario en el siguiente inicio de sesión.
4. El método de servicio de acceso de seguridad de acuerdo con la reivindicación 1, caracterizado además porque el paso de reporte de acceso al historial incluye el paso de, si el paso de autenticación para el acceso de las coordenadas falla, inmediatamente envía un mensaje de alarma a través los medios de mensaje diseñados por el usuario.
5. Un método de servicio de acceso de seguridad para procesar el registro del miembro en un servicio en línea, caracterizado porque comprende:
   Un paso de autenticación a través de la introducción de texto: y

Un paso de autenticación a través de la introducción de coordenadas.

6. Un método de servicio de acceso de seguridad de acuerdo con cualquiera de las reivindicaciones 1 a 5, caracterizado además porque el paso de autenticación a través de la introducción de las coordenadas comprende los pasos de:
Transmitir una tabla de imágenes en la cual una imagen clave es aleatoriamente mezclada con una pluralidad de otras imágenes en la pantalla del usuario;
Manipular todas las imágenes para tener el mismo valor al mismo tiempo de acuerdo a un valor de manipulación del teclado o del ratón del ordenador del usuario;
Confirmar una posición manipulada por la imagen clave, y si las coordenadas cuya manipulación de una posición es confirmada y las coordenadas clave previamente diseñadas por el usuario coinciden entre sí, determina que esa autenticación es exitosa pero si dichas coordenadas no coinciden entre sí, determina que la autenticación no fue exitosa.
7. El método de servicio de acceso de seguridad de acuerdo con la reivindicación 6, caracterizada además porque las coordenadas clave son posiciones diseñadas usando una segunda imagen clave.
8. El método de servicio de acceso de seguridad de acuerdo con la reivindicación número 7, caracterizado además porque comprende el paso de, si la primera imagen clave pasa a través de una posición diseñada por una imagen clave de trampa a través de la manipulación del usuario, determinando que la autenticación no es exitosa, y transmitiendo un mensaje de alarma a un ordenador del usuario o a un propietario original de un código de identificación (ID).
9. El método de servicio de acceso de seguridad de acuerdo a la reivindicación 7 caracterizado además porque comprende los pasos de, si el usuario coloca una primera imagen clave en una posición diseñada por una imagen clave de reporte y posteriormente confirma la manipulación, determina que a autenticación es exitosa permitiendo este hecho ser automáticamente reportada a través de un sistema de guardia.
10. Un método para autenticar con seguridad a un usuario, caracterizado porque comprende los pasos de:
Transmitir una tabla de imágenes en la cual una imagen clave es aleatoriamente mezclada con una pluralidad de otras imágenes a una pantalla del usuario;
Manipular la totalidad de las imágenes para tener el mismo valor al mismo tiempo de acuerdo a un valor de manipulación de un teclado o de un ratón de ordenador del usuario;
Confirmar una posición manipulada por la imagen clave; y si las coordenadas cuya manipulación de una posición es confirmada y las coordenadas clave previamente diseñadas por el usuario coinciden entre si, determina que la autenticación es exitosa y si dichas coordenadas no coinciden entre si, determina que la autenticación no es exitosa.
11. El método para autenticar con seguridad de acuerdo con la reivindicación 10, caracterizado además porque las coordenadas clave son posiciones diseñadas usando una segunda imagen clave.
12. El método para autenticar con seguridad de acuerdo con la reivindicación 11 caracterizado además porque comprende el paso de, si una primera imagen clave pasa a través de una posición diseñada por una imagen clave de trampa a través de la manipulación del usuario, determina que la autenticación no es exitosa, y transmite un mensaje de alarma a un ordenador del usuario o a un propietario original de un código de identificación (ID).
13. El método para autenticar con seguridad de acuerdo con la reivindicación 11, caracterizado además porque comprende el paso de, si el usuario coloca una primera imagen clave en una posición diseñada por una imagen clave de reporte y luego confirma la manipulación, determina que la autenticación es exitosa, permitiendo este hecho ser automáticamente reportado a través de un sistema de guardia.
14. El método para autenticar con seguridad de acuerdo con cualquiera de las reivindicaciones 1 a 9, caracterizado además porque comprende el paso de registrar una tabla de imágenes de personalización en la cual un historial de construcción de imágenes de tablas de imágenes proveídas es registrada de manera distinga en una base de usuario.
15. El método para autenticar con seguridad de acuerdo con la reivindicación 14, caracterizado además porque el paso de registro de la personalización de la tabla de imágenes comprende los pasos de:
Permitir al usuario seleccionar una imagen clave a través de una imagen de coordenadas o una imagen de coordenadas de terminal de un grupo de imágenes, cuyo número es mucho mayor que las imágenes que son requeridas en la tabla de personalización de imagen y posteriormente introducir las imágenes seleccionadas;

Permitir a un servidor extraer aleatoriamente tantas imágenes como el número de las que son necesarias para completar la tabla de imágenes, de las imágenes restantes excepto por las seleccionadas, y mezclando las imágenes que son seleccionadas e introducidas por el usuario y las imágenes que son seleccionadas por el servidor, y registrando la personalización de la tabla de imágenes.

16. El método para autenticar con seguridad de acuerdo con cualquiera de las reivindicaciones 10 a 13, caracterizado además porque comprende el paso de introducir un texto de contraseña, y
Porque el paso del proceso de autenticación incluye determinar que la autenticación es exitosa solamente cuando tanto el texto de contraseña como las coordenadas clave son válidas luego que la introducción del texto de contraseña y las coordenadas ha sido completada, y se determina que la autenticación no es exitosa si el texto de la contraseña o las coordenadas clave no son válidos.
17. El método para autenticar con seguridad de acuerdo con lo reivindicado en cualquiera de las reivindicaciones 1 a 9, 14 y 15 caracterizado además porque comprende:
Un paso de registro de coordenadas para proveer a la interfase para que permita el usuario definir diferentemente las coordenadas clave para un ordenador principal y unas coordenadas clave para una computadora extraña y registrar la información introducida;
Un paso de adquisición de información terminal de adquisición de información reconocida de un ordenador del usuario;
Un paso de reconocimiento de terminal para determinar al ordenador como el ordenador principal o el ordenador extraño basado en la información reconocida en el ordenador del usuario, la cual se obtiene en el paso de la adquisición de la información de la terminal.;
Un paso de registro de un ordenador principal, si está determinado que el ordenador es el extraño en el paso de reconocimiento de la terminal, registrado la información del ordenador para proveer una interfase de registro de ordenador principal, y registrar la información introducida; y
Un paso de alarma de ordenador extraño, si en el paso de reconocimiento de terminal se determina que el ordenador no es el principal, notificando al usuario del mensaje de alarma sin importar el resultado de la autenticación.
En donde el paso de autenticación a través de la introducción de las coordenadas incluye determinar si las coordenadas, la manipulación de la posición de la que es confirmada y las coordenadas clave previamente diseñadas por el usuario coinciden entre si, si se determina que el ordenador es el principal en el paso de reconocimiento de la terminal, confirma las coordenadas clave para el ordenador principal, y si se determina que el ordenador es el extraño en el paso de reconocimiento de terminal, confirma las coordenadas clave para el ordenador extraño.
18. El método para autenticar con seguridad de acuerdo con la reivindicación 17, caracterizado además, porque las coordenadas clave son dos o mas, y todas las coordenadas clave se confirman en el ordenador extraño y solamente algunas de las coordenadas clave son confirmadas en el ordenador principal.
19. Un método para autenticar con seguridad a un usuario, caracterizado porque comprende los pasos de:
Un paso de registro de contraseña que provee la interfase para permitir a un usuario definir diferentemente contraseñas para un ordenador principal y contraseñas para un ordenador extraño, y almacenar la información introducida;
Un paso de reconocimiento de terminar para determinar el ordenador como el principal o como el ordenador extraño basados en información reconocida del ordenador del usuario, la cual es adquirida en el paso de adquisición de información de la terminal;
Un paso de registro de ordenador principal, si se determina que el ordenador es el extraño en el paso de reconocimiento de terminal, registrando la información del ordenador para proveer una interfase de registro de ordenador principal que puede ser registrada como el ordenador principal; y
Un paso de procesamiento de autenticación, si se determina que el ordenador es el principal en el paso de reconocimiento de terminal, confirmando una contraseña para el ordenador principal, y si se determina que el ordenador es el extraño en el paso de reconocimiento de terminal, confirma una contraseña para el ordenador extraño.
20. El método para autenticar con seguridad de acuerdo con la reivindicación 19, caracterizado además porque comprende los pasos de:
Proveer la interfase para permitir al usuario registrar un punto de contacto donde el mensaje de alarma sea recibido, y guardar la información ingresada; y

Un paso de alarma de ordenador extraño, si se determina que el ordenador es el extraño en el paso de reconocimiento de terminal, notificando el mensaje de alarma al punto de contacto sin importar el resultado de la autenticación.

Industria y Comercio
SUPERINTENDENCIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIVISION DE NUEVAS CREACIONES
TARJETA ARCHIVO TEMATICO

PATENTE DE INVENCION ___ PCT ___ MODELO DE UTILIDAD ___ DISEÑO INDUSTRIAL ___

(21) No. de solicitud:
(51) Clasificación Internacional:
(72) Fecha de solicitud: 25-04-2006

(71) Solicitante(s) SOLMAZE CO., LTD. (Korean Corp.)

(72) Inventor(es) HWANG JAY-YEON y YANG KI-HO

(74) Agente: JESUS ABELARDO CARDENAS ALVARO

(30) Prioridad	(31) No. *Prioridad*	(32) *Fecha*	(33) *País*
SI	10-2003-0066452	25-09-2003	KR
SI	10-2004-0053149	08-07-2004	KR
SI	10-2004-0068356	30-08-2004	KR

(85) Fecha inicio fase nacional:
(80) Datos relativos a la presentación de la solic. PCT
Fecha de presentación de la solicitud: 25-09-2004
No. de solicitud PCT/KR2004/002408

(87) Publicación Internacional
Fecha: 31-03-2005
No. publicación: WO 2005/029316

FIGURA CARACTERISTICA
8 X 6 cm

(54) Título: METODO DE SERVICIO DE CERTIFICACION SEGURA

(57) Resumen: La presente invención se refiere a hacer segura la autenticación. De acuerdo a la presente invención, un método de servicio de acceso de seguridad incluye un paso de autenticación a través de la introducción de un texto, un paso de rastreo de ubicación de acceso, un paso de autenticación a través de la introducción de coordenadas y un paso de reporte de acceso al historial

85

FORMATO DE DIGITALIZACION
RELACION DE ANEXOS

Royal Technologies S.A.

Item	Expediente No	0603894 No de unidades	No de Folio
1	CD		
2	DVD		
3	REVISTA		
4	LIBRO		
5	PERIODICO		
6	DISQUETES		
7	SOBRE DE MANILA	1	
8	SOBRE BLANCO TAMAÑO CARTA		
9	SOBRE BLANCO TAMAÑO OFICIO		
10	OTROS:		

Observaciones: Acta Final

86

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Rad: 08-000004 -00000-0000 Fec: 2008-04-25 16:28:01
Dep: 2020 NUEVAS CREACIONES
Tra: 11 PATENTES Sec: 278 FASE NACIONAL
Act: 411 PRESENTACION Fol: 85

Industria y Comercio

SUPERINTENDENCIA

Delegatura de Propiedad Industrial
División de Nuevas Creaciones

REQUISITOS NECESARIOS PARA PRESENTACIÓN Y AGILIZACIÓN DEL TRAMITE

PCT

	USUARIO	RADICADOR
PATENTE DE INVENCIÓN ( ) MODELO DE UTILIDAD ( )	( )	( )
-Indicación de que se solicita la concesión de una patente.	( )	(X)
-Datos de identificación del solicitante o de la persona que se presenta la solicitud.	( )	(X)
-Descripción de la invención.	( )	(X)
-Dibujos de ser estos pertinentes.	( )	(X)
-Comprobante de Pago de las tasas establecidas.	( )	(X)
COMPLETA (X) INCOMPLETA ( )	( )	( )
DISEÑO INDUSTRIAL ( )		
-Indicación de que se solicita el registro de Diseño Industrial.	( )	( )
-Datos de identificación del solicitante o de la persona que se presenta la solicitud.	( )	( )
-Representación gráfica y fotográfica del Diseño Industrial o muestra del Material que incorpora el diseño.	( )	( )
-Comprobante de Pago de las tasas establecidas.	( )	( )
COMPLETA ( ) INCOMPLETA ( )	( )	( )
ESQUEMA DE TRAZADO ( )		
-Indicación de que se solicita el registro de Diseño Industrial.	( )	( )
-Datos de identificación del solicitante o de la persona que se presenta la solicitud.	( )	( )
-Representación gráfica del Esquema Trazado.	( )	( )
-Comprobante de Pago de las tasas establecidas.	( )	( )
COMPLETA ( ) INCOMPLETA ( )	( )	( )

Firma y nombre Ltda: _____

Fecha: _____

REPUBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Bogotá,
2020

Doctor(a)
CARDENAS A JESUS ABELARDO

REFERENCIA	Radicación No.	06 38994
	Solicitud internacional	KR2004/002495
	Fecha inicio fase nacional	25/04/2006
	Trámite	11
	Evento	378
	Actuación	430
	Oficio No.	6329

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, artículo 27 del Tratado de Cooperación en Materia de Patentes (PCT), regla 51 bis del Reglamento y Circular Única de la Superintendencia de Industria y Comercio, se le comunica que:

1. La solicitud no contiene la copia del documento en que consta la cesión del derecho a la patente del inventor al solicitante o a su causante. (Art. 26-k) Decisión 486.

2. La solicitud no contiene el poder debidamente otorgado, con el lleno de los requisitos exigidos por los artículos 63 y subsiguientes del Código de Procedimiento Civil. Adicionalmente, deberá presentar el documento que acredita la existencia y representación legal de la sociedad solicitante, cuando ésta fuere persona jurídica.

3. Debe aclarar el nombre de los inventores por cuanto difieren en la publicación internacional y en el documento de cesión aportado con la solicitud. De acuerdo con lo anterior presentar la copia del documento en que consta la cesión del derecho a la patente del inventor al solicitante o a su causante. (Art. 26-k) Decisión 486/00.

En cumplimiento de lo dispuesto por el artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos meses siguientes a la fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Unica No.10 de 2001.

Continua en la página siguiento...

REPUBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCI

Radicación No.:6 38994

ALIX CARMENZA CESPEDES DE VERGEL
Jefe de la división de Nuevas Creaciones

El anterior requerimiento fue notificado por fijación en lista de fecha 09 JUL 2013
adpall