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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/080228 A1

(51) International Patent Classification:
G07F 7/10 (2006.01) *G07F 19/00* (2006.01)

(21) International Application Number:
PCT/CA2007/002378

(22) International Filing Date:
31 December 2007 (31.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2/574,983 5 January 2007 (05.01.2007) CA

(71) Applicant and
(72) Inventor: **SIMMONS, Paul** [CA/CA]; 327 Durie Street, Toronto, Ontario, M6S 3G2 (CA).

(74) Agent: **SIMMONS, Paul**; 327 Durie Street, Toronto, Ontario, M6S 3G2 (CA).

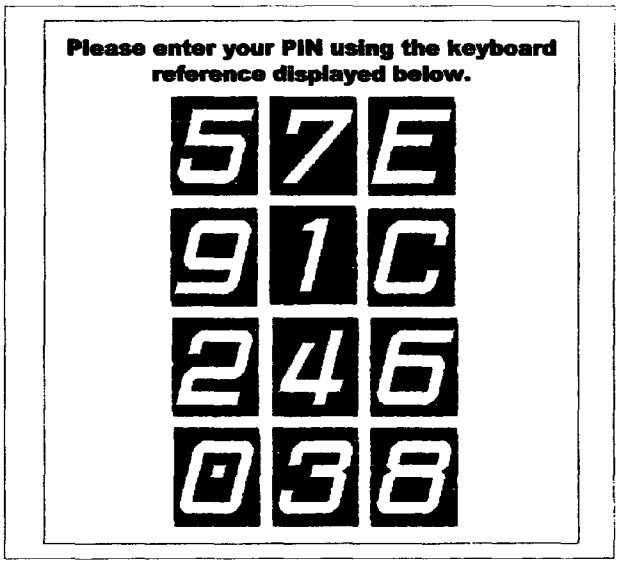
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, 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, IS, IT, LT, LU, LV, MC, MT, 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).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report*

(54) **Title:** A METHOD AND DEVICE FOR PASSWORD PATTERN RANDOMIZATION



(57) **Abstract:** An embodiment of the present invention is a method of password pattern randomization comprised of providing a predetermined number of input keys and a data array of a predetermined number of values, the number of data array values equalling the number of input keys. Each data array value is assigned to each input key, correspondingly mapped and then correspondingly displayed in operative connection with each of said key. On operation of any key, its corresponding value is transmitted to a processor. The assignment of each value to each key is random. Another embodiment of the present invention is a keyboard device employing this method of password pattern randomization.

WO 2008/080228 A1

Title

[0001] A Method And Device For Password Pattern Randomization

Field of Invention

[0002] This invention relates to a method and device for identity validation and more specifically identity validation using passwords or pass codes such as personal identification numbers (PINs), whereby the password or pass codes are entered using input keys having a randomized configuration.

Background

[0003] PINs are often used in conjunction with data media such as credit or company identity cards that are swiped or inserted into a transaction processing device as an initiation of a request for a desired service. Examples include the use of automated teller machines ("ATM") for monetary withdrawal; point of sale (POS) integrated chip card transactions ("Smart Card technology" or "Chip and Pin") for commercial purchases; and username and password entry on computers or terminals for secure data access.

[0004] Validating an identity using a PIN reduces the risk that a lost, stolen or cloned medium (card or device) can be used fraudulently by an unauthorized user.

[0005] Many transaction locations (or entry points) where PINs are used are located in publicly accessible and are permanently situated where there is an opportunity for eavesdropping or "shoulder surfing". Most entry points or

transaction locations provide a processor device having a fixed input keyboard configuration, for password or PIN entry.

[0006] For any particular medium, the secret password or PIN is also often fixed. Even where the PIN is not fixed, movement of fingers across a fixed configuration keyboard (to enter a PIN into an entry point processing device) or observation of the general movement pattern (of fingers) of an individual while entering a PIN may cause inadvertent disclosure of the PIN to a second party, increasing the risk of fraudulent use.

[00007] US patent 5,239,583 discloses an improvement in structure and credit account access security employing method and means for ensuring that repeating an exact access code which was successful in accessing the account will be unsuccessful at the next or subsequent tries. This method is flawed because it requires the user to memorize multiple passwords, which is difficult. There is a high probability a user will forget some of those passwords.

[0008] US patent 5,428,349 discloses a password access method/algorithm by generating a pseudorandom array of each letter of the alphabet and the numerals 0 through 9 such that the password entry can be monitored without disclosing the letters or numerals contained in the password. This method is flawed because relatively short passwords can still be easily cracked without knowledge of the actual password.

Summary

[0009] A preferred embodiment of the present invention provides a method of password pattern randomization for an individual transaction comprised of providing a predetermined number of input keys and a data array

of a predetermined number of values, the number of data array values equalling the number of input keys. Each of said data array values are assigned to each of said input keys, correspondingly mapped and then correspondingly displayed in operative connection with each of said keys. On operation of any key, its corresponding value is transmitted to a processor. The assignment of each of said values to each of said keys is random.

[0010] Another preferred embodiment of the present invention provides a device for password pattern randomization in an individual transaction comprised of a processor, a pre-determined number of input keys operatively connected to said processor, a display operatively connected to said input keys, and a data array of a predetermined number of values. The number of data array values equals the number of input keys. The data array is resident in (or operatively connected to) said processor, and the data array values are randomly assigned and correspondingly mapped and displayed in operative connection with said pre-determined number of input keys. On operation of any key, its corresponding value is transmitted to the processor.

Description of the drawings

[0011] Figure 1 is a perspective drawing of a processor device providing an input keyboard.

[0012] Figure 2 is a representative mapping of a conventional device processor input keyboard.

[0013] Figure 3 is a representative conventional device processor input keyboard.

[0014] Figure 4 is a sample populated data array with ten randomized data array values.

[0015] Figure 5 is a sample populated data array with twelve randomized data array values.

[0016] Figure 6 is an example input keyboard mapped with ten randomized data array values.

[0017] Figure 7 is a second example input keyboard mapped with twelve randomized data array values.

[0018] Figure 8 is an example input keyboard having a remote display.

[0019] Figure 9 is an example traditional 104-key input keyboard configuration having a remote display and blank keys.

[0020] Figure 10 is an example traditional 104-key input keyboard configuration having a remote display displaying randomized keys by light emission.

Detailed description of the drawings

[0021] In a preferred embodiment of the present invention, the transaction method herein can be practised on any processor device (10) including the type shown in figure 1. The processor device (10) is typically housed in a casing (34), has an input keyboard (14) comprised of a pre-determined number of input keys (26) operatively connected to the processor (10), an optional transmitter (22) (to transmit data to a selected source outside the processor (10)) and an optional data

reader (18) (for reading, for example, magnetic data strips found on credit cards) operatively connected (meaning able to transmit and possibly receive data) to the processor (10). A separate data reader (18) is not mandatory since transactions using the method herein can allow for key (26) based input as an alternate method of receiving magnetic strip data or the like.

[0022] The input keys (26) are pre-determined in number, have an assigned value selected from a populated data array of values (for example figures 4 and 5) in accordance with the method herein, and each value is displayed on its corresponding key face (38) (digitally in figure 1 as an example). The value of each key (26) can be shown locally on its face (38) or on a remote display (30) operatively connected (meaning able to receive and possibly send data) to the keyboard (figure 8), according to preference. The keys (26) are operatively connected to the processor (10) meaning that on operation (typically, pressing) of any key (26) during a transaction, the processor (10) is able to determine which key (26) is being operated, and the corresponding value transmitted.

[0023] A transaction can be defined as a single event like operating an individual key (26) (i.e. one keystroke), or as a series of events like the pressing or operating of a number of keys (26) in series to establish a password like "1X3Q". Especially where a transaction is defined as a single event, the method herein improves security further when it is repeated after each individual transaction (i.e. after each single key press, a new random assignment is formed (figure 4), and correspondingly mapped (figure 2) and displayed (figures 6 and 7)).

[0024] Resident in (or operatively connected to (generally in a software sense)) the processor (10) is a populated data array (figures 4 and 5) of a pre-

determined number of values (for example iconic, alphanumeric, cryptographic, or Braille values). The number of data array values matches the number of input keys (26). The data array values are randomly assigned (figure 4 showing an algorithm for random assignment of ten values to ten keys, and assignment of two values to two keys where the probability of those assignments being made is certain; figure 5 showing an algorithm for random assignment of twelve values to twelve keys), and correspondingly mapped (figure 2 showing a basic keyboard (14) map) and displayed (figures 3, 6 and 7) in operative connection (meaning each key (26) is connected to a specific data array value which the processor (10) can determine on operation of said key (26)) with the input keys (26). Each of the data array values is transmittable to the processor (10) on operation of each of the corresponding keys (26). In one embodiment of this invention, it may be preferable to not randomly assign certain keys (26). Figures 4 and 6 show an example of where it may be desirable to keep the values "Cancel" (figure 6 "Can") and "Enter" (figure 6 "Ent") in a pre- specified location, for convention and convenience. Where that is not required, all values can be randomized (figure 5) to generate a different result (figure 7 "C" and "E" respectively).

[0025] In any embodiment of this invention, it is possible to populate the data array either with unique or repeating values, depending on preference and need.

[0026] In operation, this method of password pattern randomization for an individual transaction provides to a user (not shown) a pre-determined number of input keys (26) available on any keyboard (14). A populated data array (figures 3, 4, and 5) comprised of a number of values equal in number to the number of input keys is provided, and the values within the array are randomly assigned to the available keys (26). Each value assignment is then

mapped (figures 2 through 7 inclusive) to its corresponding key (26). A user-friendly keyboard (14) map (figures 6 and 7) is then displayed for a user either locally (figure 1) or remotely (figure 8), depending on preference.

[0027] Every time a key (26) is operated it will transmit its corresponding assigned value to the processor (10). Depending on password requirements and the definition of the transaction, the steps of random assignment and correspondingly mapping, displaying and transmitting on key operation, may be repeated. For a higher level of security, after every key operation, a reassignment (and subsequent necessary operations) can occur. For a lower level of security, it may be suitable to run this method once, and accept a multi-value (multi-character) password based on a single keyboard (14) configuration. Once the user has entered his password, the processor (10) either validates the password, or if it is not so equipped, the processor (10) transmits the password to a selected destination for validation via the optional transmitter (22).

[0028] The present invention can be practised on any type of keyboard (14) including in a traditional 104-key input keyboard configuration (Figures 9 and 10).

[0029] Where a reassignment, etc. occurs after every key (26) operation, the probability of correctly breaking a three character (value) password using a three by three matrix keypad populated with nine unique values and absolutely no knowledge of the existing password (i.e. a pure guess), is 1 in 729. In contrast, the preexisting art (for example US patent 5,428,349) in the same situation would yield a probability of 1 in 27.

[0030] In a matrix of thirty-six keys (26) arranged six rows by six columns, the probability of a four or six character password being (purely) guessed

correctly is 1 in 1,296 and 1 in 46,656 respectively using the U.S. patent no. 5,428,349 solution. In the present invention the same arrangement would yield probabilities of 1 in 1,679,616 and 1 in 2,176,782,336 respectively. The invention herein is 1,296 times and 46,656 times respectively more secure.

Claims

What is claimed is:

1. A method of password pattern randomization for an individual transaction comprising:

a) providing a predetermined number of input keys;

b) providing a data array of a predetermined number of values, the number of data array values equalling the number of input keys;

c) assigning each of said data array values to each of said input keys;

d) correspondingly mapping each of said data array values to each of said input keys;

e) correspondingly displaying each of said values in operative connection with each of said keys;

f) correspondingly transmitting each of said values on operation of each of said keys to a processor; and

g) the assignment of each of said values to each of said keys being random.

2. The method as defined in claim 1 wherein each data array value is unique within the data array.

3. The method as defined in claim 1 wherein the random assignment and corresponding mapping, displaying and transmitting is repeated for each new individual transaction.

4. A device for password pattern randomization in an individual transaction comprising:

a) a processor;

b) a pre-determined number of input keys operatively connected to said

processor;

c) a display operatively connected to said input keys; and

d) a data array of a predetermined number of values, the number of data array values equalling the number of input keys, the data array being resident in said processor, the data array values being randomly assigned and correspondingly mapped and displayed in operative connection with said input keys, each of said data array values being transmittable to the processor on operation of each of said corresponding keys.

5. The device as defined in claim 4 further comprising a data reader operatively connected to said processor.

6. The device as defined in claim 4 wherein each data array value is unique within the data array.

7. The device as defined in claim 4 wherein the random assignment and corresponding mapping and displaying is repeated for each new individual transaction.

Figure 1

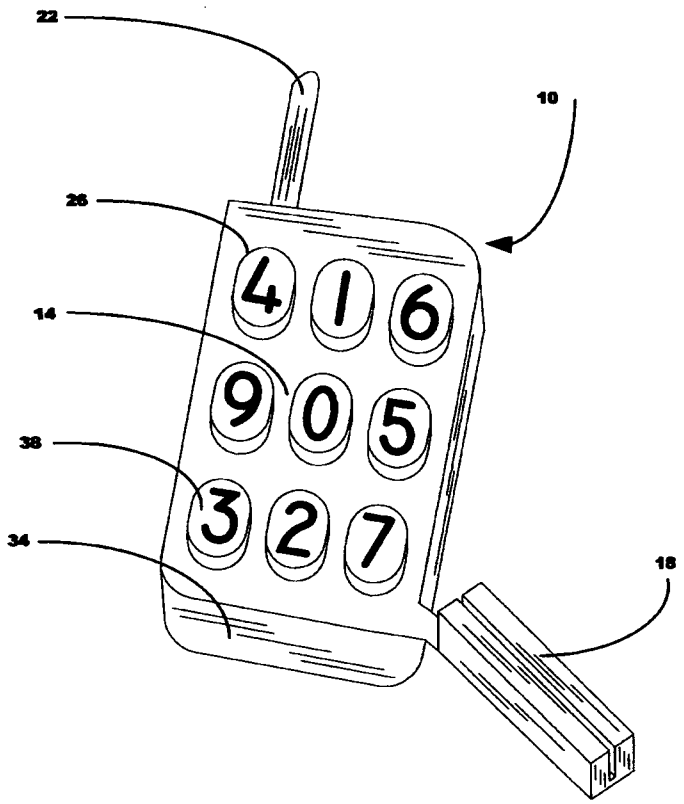
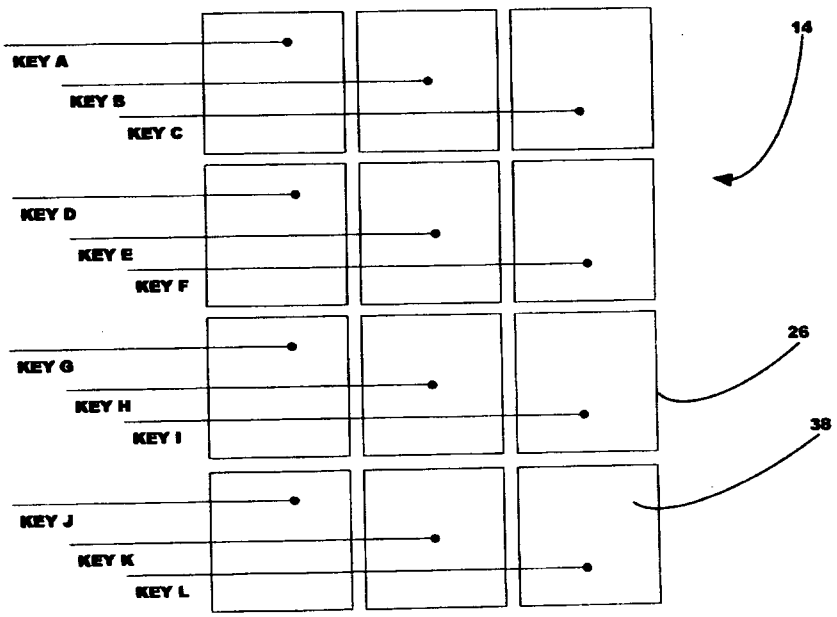
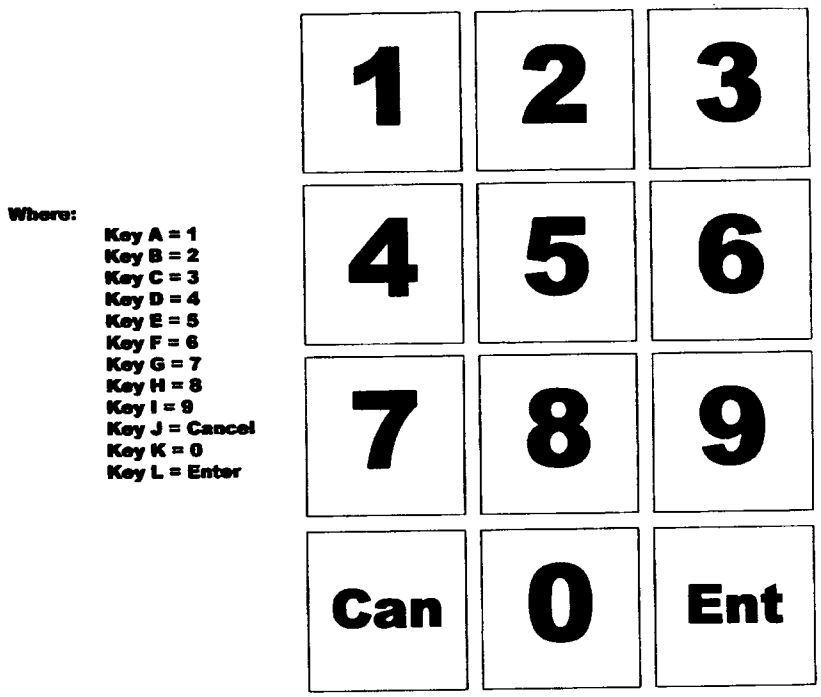


Figure 2



RECTIFIED SHEET (RULE 91.1)

Figure 3



Where:

Key A = 1
Key B = 2
Key C = 3
Key D = 4
Key E = 5
Key F = 6
Key G = 7
Key H = 8
Key I = 9
Key J = Cancel
Key K = 0
Key L = Enter

Figure 4

{1,2,3,4,5,6,7,8,9,0} are randomly populated into the Array Random(10)

Therefore:

Key A = Random(1)
Key B = Random(2)
Key C = Random(3)
Key D = Random(4)
Key E = Random(5)
Key F = Random(6)
Key G = Random(7)
Key H = Random(8)
Key I = Random(9)
Key J = Cancel
Key K = Random(10)
Key L = Enter

RECTIFIED SHEET (RULE 91.1)

Figure 5

(1,2,3,4,5,6,7,8,9,0,Can,Ent) are randomly populated into the Array Random(12)

Therefore:

Key A = Random(1)
Key B = Random(2)
Key C = Random(3)
Key D = Random(4)
Key E = Random(5)
Key F = Random(6)
Key G = Random(7)
Key H = Random(8)
Key I = Random(9)
Key J = Random(10)
Key K = Random(11)
Key L = Random(12)

Figure 6

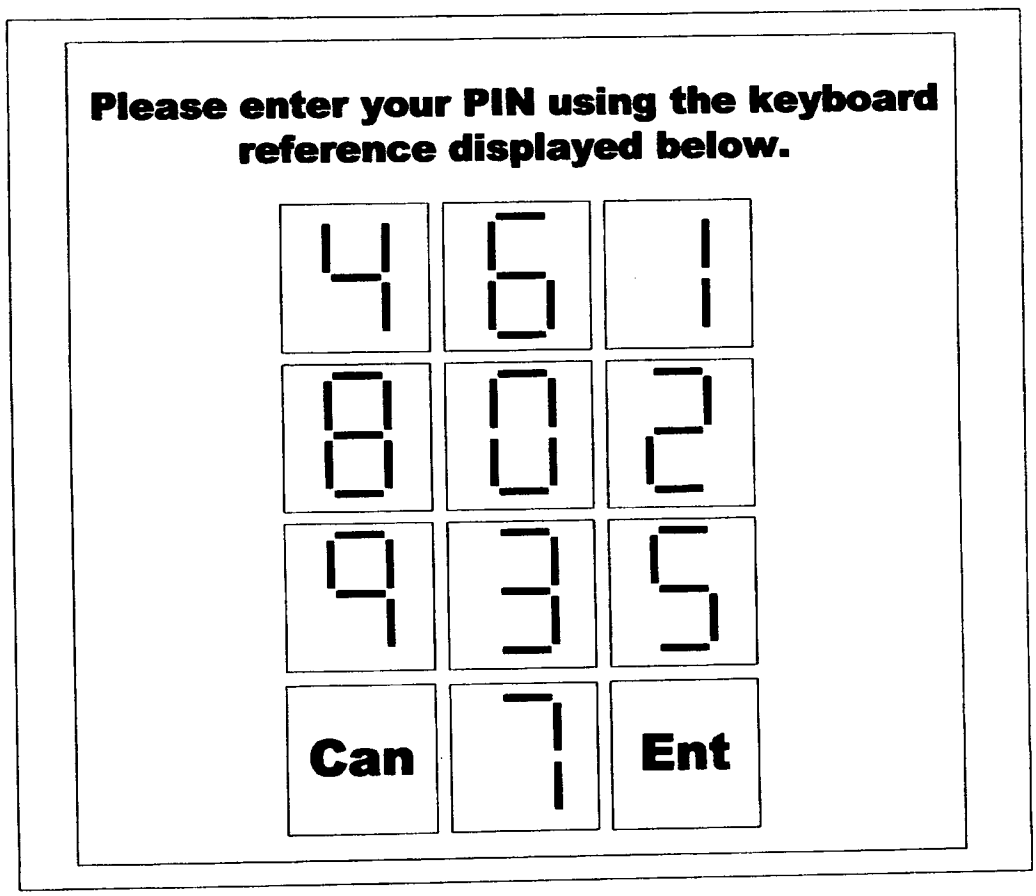


Figure 7

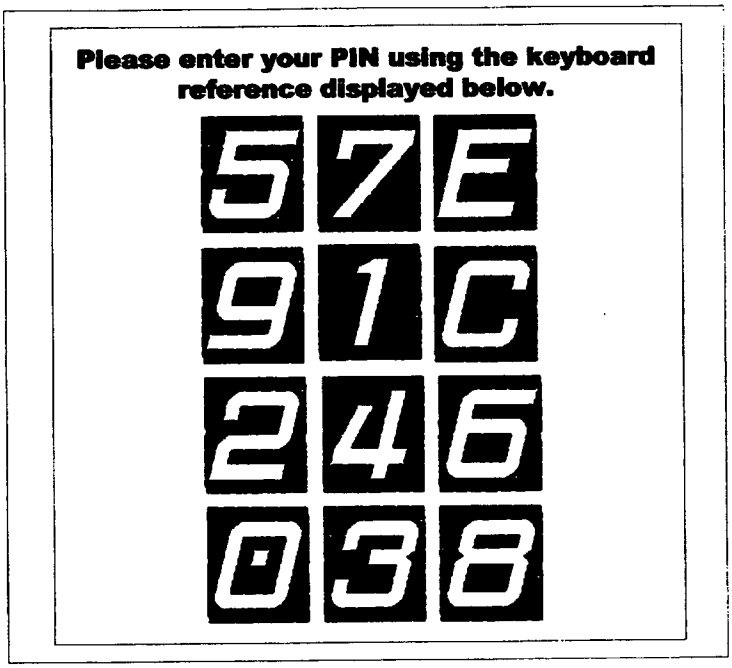


Figure 8

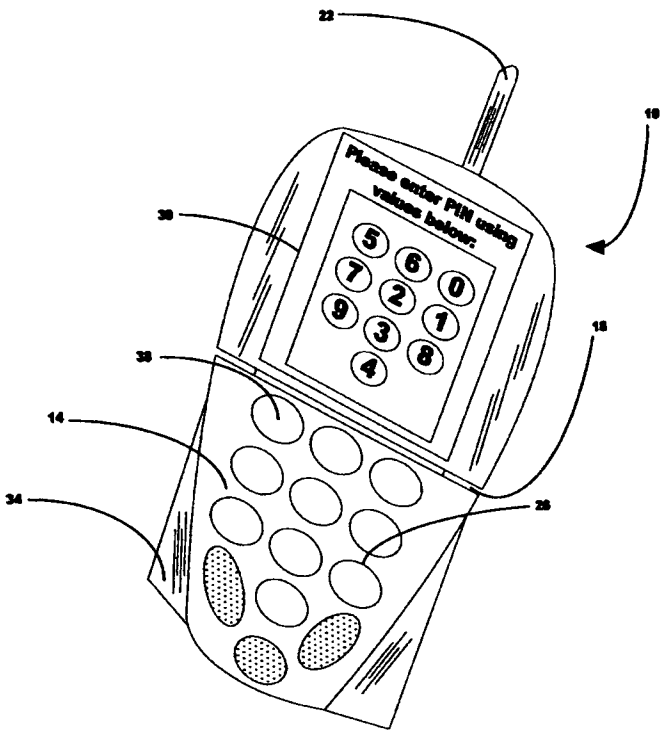


Figure 9

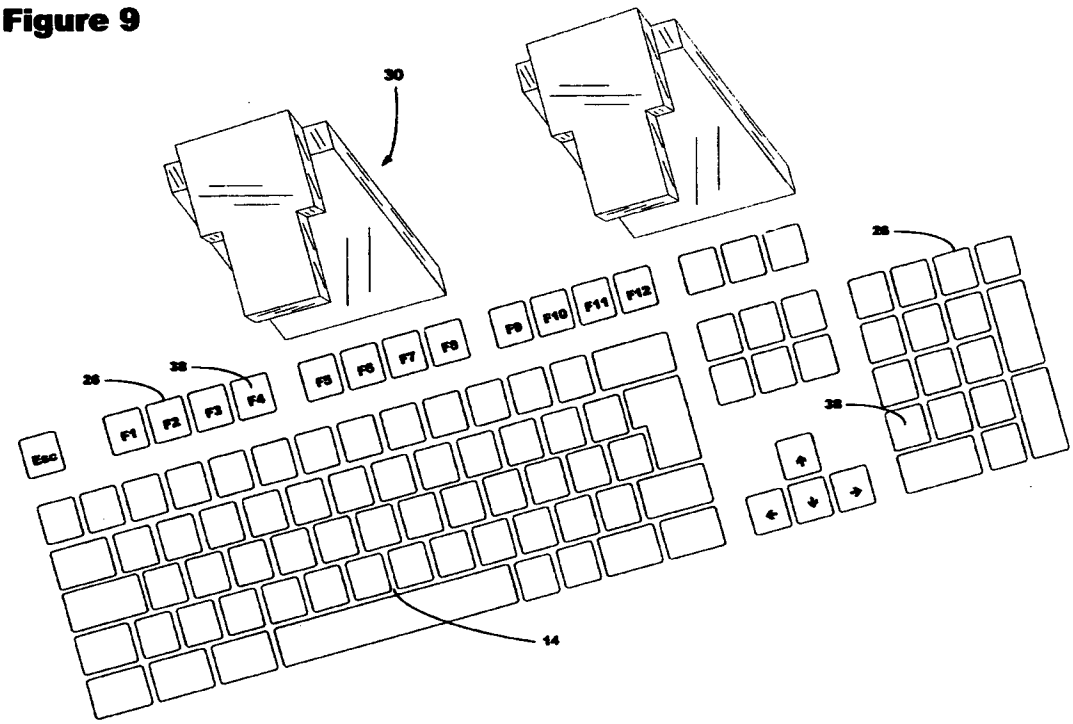
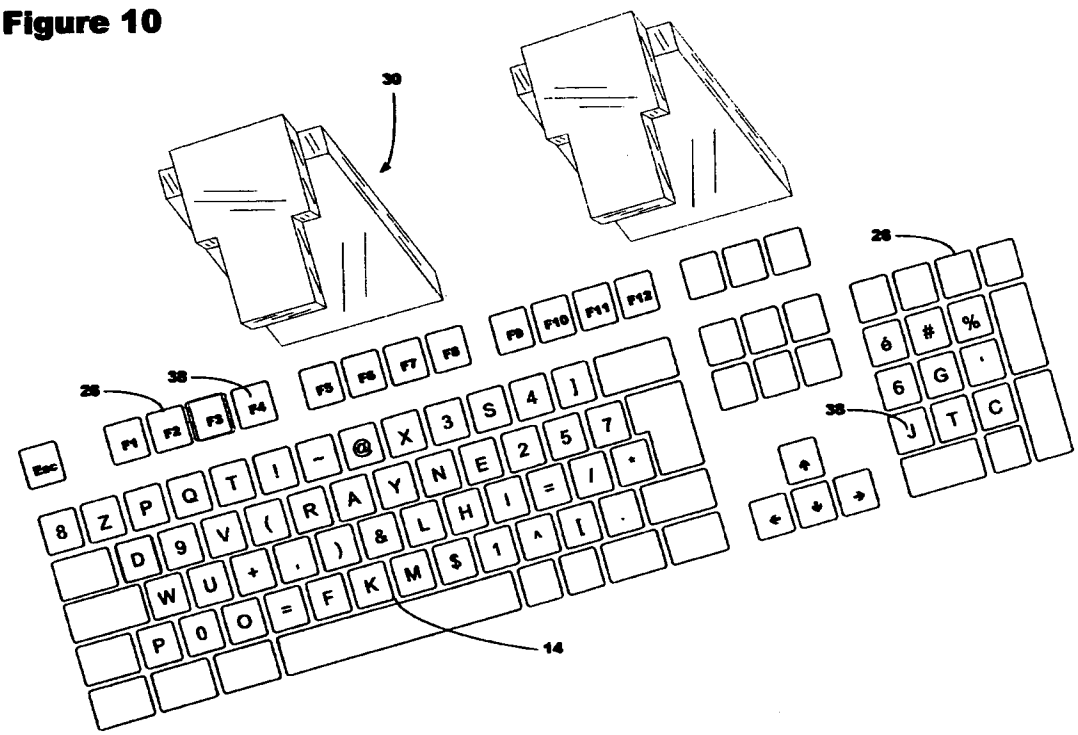


Figure 10



INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2007/002378

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***G07F 7/10*** (2006.01) , ***G07F 19/00*** (2006.01)
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)
IPC: G07F

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Databases Searched: Delphion and US West Patent Database
Keywords Searched: password, random, transaction, key, display, data array

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,428,349 (BAKER) 27 June 1995 (27-06-1995) abstract column 1, lines 32-46 column 2, line 57 - column 3, line 8 figs 1, 2	1-7
X	US 2004/0044739 (ZIEGLER) 4 March 2004 (04-03-2004) figs. 2a-2c and 5 page 3, paragraphs 0043-0045	1-7
A	WO 85/03787 (WHITE) 29 August 1985 (29-08-1985) see entire document	1-7
A	US 2003/0004827 A1 (WANG) 2 January 2003 (02-01-2003) see entire document	1-7

[ ] Further documents are listed in the continuation of Box C.

[X] 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 another 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
30 March 2008 (30-03-2008)	18 April 2008 (18-04-2008)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476	Dennis Atkinson 819- 953-0816

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2007/002378

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US 5428349A	27-06-1995	None	
US 2004044739A1	04-03-2004	AU 2003304191A1	04-01-2005
		AU 2003304191A8	04-01-2005
		US 2005055318A1	10-03-2005
		WO 2004109426A2	16-12-2004
		WO 2004109426A3	05-01-2006
WO 8503787A1	29-08-1985	CA 1232684A1	09-02-1988
		EP 0172877A1	05-03-1986
		EP 0172877A4	27-04-1988
		JP 5014298B	24-02-1993
		JP 61501477T	17-07-1986
		US 4630201A	16-12-1986
US 2003004827A1	02-01-2003	AU 2059701A	24-09-2001
		AU 4004300A	21-09-2000
		AU 5383198A	29-06-1998
		AU 2002247213A1	12-09-2002
		AU 2002357047A1	02-09-2003
		AU 2002367640A1	08-10-2003
		AU 2002367640A8	08-10-2003
		CA 2365644A1	08-09-2000
		CA 2403332A1	20-09-2001
		CN 1265292C	19-07-2006
		CN 1307594C	28-03-2007
		CN 1344396A	10-04-2002
		CN 1452739A	29-10-2003
		CN 1623173A	01-06-2005
		EP 1159700A2	05-12-2001
		EP 1272933A1	08-01-2003
		HK 1077386A1	12-10-2007
		JP 2003517658T	27-05-2003
		JP 2003527714T	16-09-2003
		TW 487864B	21-05-2002
		TW 560159B	01-11-2003
		TW 565786B	11-12-2003
		US 5917913A	29-06-1999
		US 6175922B1	16-01-2001
		US 6282656B1	28-08-2001
		US 6594759B1	15-07-2003
		US 6850916B1	01-02-2005
		US 7089214B2	08-08-2006
		US 7107246B2	12-09-2006
		US 2002023215A1	21-02-2002
		US 2002123967A1	05-09-2002
		US 2007089168A1	19-04-2007
		WO 0052866A2	08-09-2000
		WO 0052866A3	21-12-2000
		WO 0052866A9	30-08-2001
		WO 0169388A1	20-09-2001
		WO 9825371A1	11-06-1998
		WO 02069291A2	06-09-2002
		WO 02069291A3	16-10-2003
		WO 03065318A2	07-08-2003
		WO 03065318A3	26-02-2004
		WO 03081377A2	02-10-2003
		WO 03081377A3	04-03-2004