

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
30 August 2007 (30.08.2007)

PCT

(10) International Publication Number
WO 2007/096648 A1

(51) International Patent Classification:
G06F 21/20 (2006.01)

(21) International Application Number:
PCT/GB2007/000656

(22) International Filing Date:
23 February 2007 (23.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0603581.0 23 February 2006 (23.02.2006) GB

(71) Applicant (for all designated States except US): **THE QUEEN'S UNIVERSITY OF BELFAST** [GB/GB];
University Road, Belfast BT7 1NN (GB).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **KUBER, Ravi Anil** [GB/GB]; 11 Greenfield Road, Devizes, Wiltshire SN10 5BP (GB). **YU, Wai** [GB/GB]; 43 Lansdowne Avenue, Newtownards, Co Down, BT23 4GJ (GB).

(74) Agent: **MURGITROYD & COMPANY**; 165-169 Scotland Street, Glasgow G5 8PL (GB).

(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, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, 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.

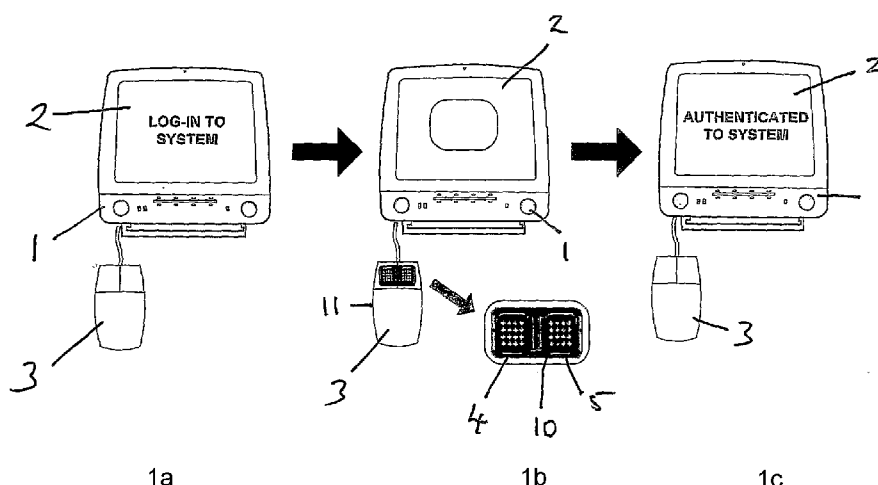
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, 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

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.

(54) Title: SYSTEM AND METHOD FOR USER AUTHENTICATION



(57) Abstract: A method for user authentication are provided, the method comprising the steps of obtaining an identification element of a user, presenting the user with a plurality of user perceptible variables which are perceptible by the user using their sense of touch, detecting selection of at least one of the user perceptible variables by the user, comparing the at least one selected user perceptible variable with one or more user perceptible variables previously associated with the identification element of the user, and authenticating the user if the at least one selected user perceptible variable corresponds to at least one of the user perceptible variables previously associated with the identification element of the user. The user perceptible variables may be perceptible by the user using tactile sensory information. The user perceptible variables may comprise patterns of tactile sensory information, for example any of patterns of pressure, patterns of vibration, patterns of temperature. In one embodiment of the invention, each user perceptible variable may comprise a pattern of pressure provided by a plurality of pins, perceptible by the user by placing at least one fingertip in contact with the pins.

WO 2007/096648 A1

System and Method for User Authentication

5 The present invention relates to a system and method for user authentication.

10 In order to allow individuals to access personal data or services within a computer-based system, it is commonplace to present trusted individuals with a username and alphanumeric password as a method of authorized entry. Password ownership is recommended to increase individual accountability, reduce illicit usage, allow for establishment of system usage audit trails and reduce frequent password changes due to group membership fluctuations.

15 User authentication is the process required to provide an individual with secure access to data. The three main techniques for user authentication include knowledge-based systems, token-based systems, and the use of biometrics. Modern technology predominantly favours knowledge-based schemes, compared with biometrics, due to its relative infancy and expense of additional hardware. Entry to a knowledge-based system is done through a process of user identification and authentication. The identification step, establishes that user's right to access the system. Upon identification, the authentication mechanism verifies that the user is the legitimate owner of the ID. Many token-based authentication systems
20 also make use of knowledge-based schemes, to prevent impersonation through theft or loss of the token. For example, an ATM system makes use of a token (card) and secret knowledge (a PIN) to authenticate entry. Where knowledge-based systems are implemented, problems with security, and memorability of user authentication sequences are inherent.

30

Whereas in the past, security mechanisms have focused almost entirely on technical issues, it is now widely recognized that most security mechanisms cannot succeed without taking into account the user. Authentication information needs to be both recalled and kept secure.

5 Humans are now generally considered to be the weakest link in the security chain. The human memory for sequences of items is temporally limited, so remembering a longer alphanumeric password may prove to be difficult. Due to the vast array of passwords that need to be committed to memory, individuals find it difficult to precisely recall secret information.

10 Precise recall is not a strong point of human cognition, so if the user makes a small error in entering the secret information, the authentication fails. Individuals forget passwords due to information fading over time in our cognitive system (natural decay) and interference from other chunks of information. Lack of appropriate retrieval cues adds to the problem. As a
15 result, individuals often externalize information, by writing down, sharing or even reusing existing passwords. These factors pose a potential threat to system security.

As users lack key security knowledge, they tend to select shorter 'weaker'
20 passwords, which can easily be 'cracked' due to their poor design. Research has indicated that once a password has been chosen, it is not likely to be changed, until it has been shown to be compromised. A trade-off between memorability and 'user issue' security seems apparent. Some passwords are very easy to remember (e.g. single words in the user's
25 native language) but also very easy to guess with dictionary searches. In contrast, some are tougher to remember. System generated passwords have been recommended for optimal security in knowledge-based schemes, as these prove more difficult to recall and thus, crack. However, user generated passwords are potentially more memorable and thus less
30 likely to be disclosed, but may be easier to crack. It seems apparent a

system embracing both issues of memorability and security, focusing on the problems discussed in the earlier section, could provide benefit to the user, when accessing a system, in a secure manner. A new system would be beneficial for human-computer interaction.

5

Traditional alphanumeric passwords utilise recall memory, which involves a search of memory and then the comparison process once something is found. This is a more resource intensive process than recognition which solely performs the comparison process. It has been found that cued
10 recall leads to better remembering than recall alone, and recognition has better accuracy than cued recall. Systems such as associative passwords based on remembering a set of words and associated responses, and authentication based on personal history have offered methods of promoting memorable authentication strings, which are not easily
15 guessable by outsiders.

According to a first aspect of the present invention there is provided a method for user authentication, the method comprising the steps of:-

- obtaining an identification element of a user,
- 20 presenting the user with a plurality of user perceptible variables which are perceptible by the user using their sense of touch,
- detecting selection of at least one of the user perceptible variables by the user,
- comparing the at least one selected user perceptible variable with
25 one or more user perceptible variables previously associated with the identification element of the user, and
- authenticating the user if the at least one selected user perceptible variable corresponds to at least one of the user perceptible variables previously associated with the identification element of the user.

30

Touch is a complex sense, divided into two major categories of sensory information: tactile and kinesthetic. Tactile sensory information comprises cutaneous stimulation, and includes the sensation of wetness, temperature, skin curvature and stretch, velocity, vibration, slip, pressure and local force. This conveys information about the initial contact with objects, surface textures and geometry. Kinesthetic sensory information relates to the physical forces applied to and by the body. This includes proprioception or sensing and awareness of body position.

10 The user perceptible variables may be perceptible by the user using tactile sensory information. The user perceptible variables may comprise patterns of tactile sensory information, for example any of patterns of pressure, patterns of vibration, patterns of temperature. The patterns may be static or cyclic or animated or a combination thereof. In one
15 embodiment of the invention, each user perceptible variable may comprise a pattern of pressure provided by a plurality of pins. Each pattern of pressure may be perceptible by the user by placing at least one fingertip in contact with the pins.

20 User perceptible variables perceived using the sense of touch cannot be easily externalised (i.e. passed onto others, aurally or in writing) and cannot be immediately observed and recreated by an onlooker.

The user perceptible variables may be presented to the user on request by
25 the user. The, or at least some of the, user perceptible variables may be presented to the user concurrently. The user perceptible variables may be presented to the user sequentially. The user perceptible variables may be presented to the user until selection of a predetermined number of user perceptible variables has been detected. The user perceptible variables
30 may be presented to the user in a first series of user perceptible variables

until selection of a user perceptible variable is detected, and then a second series of user perceptible variables until selection of a user perceptible variable is detected, said process being repeated a plurality of times until selection of a predetermined number of user perceptible variables has been detected. Authentication of the user may take place if each of a plurality of selected user perceptible variables corresponds to a user perceptible variable previously associated with the identification element of the user. Authentication of the user may take place if each of a plurality of selected user perceptible variables corresponds to a user perceptible variable previously associated with the identification element of the user, and the order in which the user perceptible variables is selected by the user corresponds to a predetermined order of the user perceptible variables previously associated with the identification element of the user.

The user perceptible variables may be perceptible by the user without requiring movement of the user.

The one or more user perceptible variables previously associated with the identification element of the user may comprise user perceptible variables previously chosen to the user and associated with the identification element of the user. The one or more user perceptible variables previously associated with the identification element of the user may be perceptible by a user using their sense of touch.

The method may further comprise enrolling a user. Enrolling the user may comprise obtaining an identification element of the user, presenting the user with a plurality of user perceptible variables which are perceptible by the user using their sense of touch, detecting choice of at least one of the user perceptible variables by the user, and associating the identification element of the user with the at least one chosen user perceptible variable.

Thus in the user authentication method and system of the invention, a user may be presented with one or more user perceptible variables to which the user has previously been exposed, and selects one or more of the variables corresponding to previously-chosen variables. Selection of
5 the one or more user perceptible variables takes place by recognition of the variables. In using recognition rather than recall in an authentication method and system, all of the advantages discussed above are realised.

Obtaining the identification element of the user may comprise one or more
10 of, receiving an alphanumeric identification element from the user, interrogating a token, card, RFID tag or similar unique identifier provided by the user to read the identification element, sensing a biometric parameter presented by the user.

15 According to a second aspect of the present invention there is provided a user authentication system comprising:-

an identifier device which obtains an identification element of a user,

20 a user perceptible variable generator device which generates a plurality of user perceptible variables which are perceptible by the user using their sense of touch,

a presentation device which presents the plurality of user perceptible variables to the user,

25 a detector device which detects selection of at least one of the user perceptible variables by the user,

a comparator device which compares the at least one selected user perceptible variable with one or more user perceptible variables previously associated with the identification element of the user, and

30 an authentication device which authenticates the user if the at least one selected user perceptible variable corresponds to at least one of the

user perceptible variables previously associated with the identification element of the user.

5 The presentation device may comprise a tactile device which presents user perceptible variables comprising tactile sensory information to the user. The tactile device may comprise a pressure device which presents user perceptible variables comprising pressure patterns to the user. The pressure device may comprise a plurality of pins which presents user perceptible variables comprising pin patterns to the user. Each of the
10 plurality of pins may be placed in a retracted position or an extended position to present the pin patterns to the user. The presentation device may comprise a haptic mouse. The haptic mouse may comprise a plurality of pins.

15 The tactile device may comprise a temperature device which presents user perceptible variables comprising temperature patterns to the user. The temperature device may comprise a plurality of pins which presents user perceptible variables comprising pin temperature patterns to the user. Each of the plurality of pins may have a temperature which is controlled to
20 present the pin temperature patterns to the user.

The presentation device may present the, or at least some of the, user perceptible variables to the user concurrently. The presentation device may present the user perceptible variables to the user sequentially. The
25 presentation device may present the user perceptible variables to the user until selection of a predetermined number of user perceptible variables has been detected. The presentation device may present a first series of user perceptible variables to the user until selection of a user perceptible variable is detected by the detector device, and then present a second
30 series of user perceptible variables to the user until selection of a user

perceptible variable is detected, said process being repeated a plurality of times until selection of a predetermined number of user perceptible variables has been detected.

5 The user perceptible variable may be incorporated, at least partially, within the presentation device. The detector device may be incorporated, at least partially, within the presentation device. The comparator device and/or the authentication device may comprise a processor, running comparison/authentication software.

10

The identifier device may comprise a receiver, for example a keypad or keyboard, which receives an alphanumeric identification element from the user. The identifier device may comprise an interrogation device, for example a reader, which interrogates a token, card, RFID tag or similar
15 unique identifier provided by the user to read the identification element. The identifier device may comprise a biometric sensor, which senses a biometric parameter presented by the user.

15

Embodiments of the present invention will now be described by way of
20 example only, and with reference to the accompanying drawings in which:

Fig 1 is a schematic diagram of a user authentication system according to a first embodiment of the present invention;

25

Fig 2 is a detailed view of the input device of the system of Fig 1;

Fig 3 is a representation of the user authentication system of Fig 1 when operated in a first operative embodiment;

Fig 4 is a representation of the screen display of Fig 3 during operation of the user authentication system;

5 Fig 5 is a representation of the user authentication system of Fig 1 when operated in a second operative embodiment, and

Fig 6 is a representation of the screen display of Fig 5 during operation of the user authentication system.

10 Individuals are often required to remember a number of passwords for authentication by and subsequent entry into various systems, due to the growth and ubiquity of such systems. As a result of the workload needed to memorise authentication strings, individuals tend to choose insecure, or previously used passwords and PINs to foster authentication, which
15 possess a potential threat to system security. To address these issues, an approach has been developed examining the use of recognition-based authentication, through the use of the sense of touch.

The user authentication method and system of the present invention
20 enables authentication of a user, through ability of the user to recognize previously perceived user perceptible variables. The idea behind the user authentication method and system of the invention is to make use tactile sensory information (for example pin patterns) as an alternative means to conventional visual information (for example textual characters on a PIN
25 pad/keyboard).

Referring to Figure 1, and particularly Figure 1a, the user authentication system according to an embodiment of the present invention comprises a microprocessor 1, a visual display unit (VDU) 2 and a haptic mouse 3.

As shown in more detail in Figure 1b and Figure 2, the haptic mouse 3 comprises two adjacent arrays 4,5 of pins 10 mounted in a housing 11, each array having sixteen pins 10 arranged in a 4x4 grid. Each pin 10 in the grid is selectively axially moveable between a retracted position wherein an uppermost portion of the pin 10 is substantially level with the surrounding housing 11, and an extended position wherein the pin 10 extends above the level of the surrounding housing 11. Each array 4,5 of pins 10 is dimensioned such that it can be substantially covered by a fingertip of a user of the user authentication system. Each array 4,5 of pins 10 presents various pin patterns generated by the pins to the user via one or more fingertips.

The user authentication system is used as follows. A user first enrolls with the system. The user enters an identification element into the system, using an identifier device thereof. This may comprise, for example, entering a unique alphanumeric identification element via a keyboard or keypad of the system, or presenting an identification token or card which is interrogated by a card reader of the system to obtain the identification element of the user, or presenting a biometric parameter of the user which is read by a biometric sensor of the system to obtain the identification element of the user. The identification element of the user is stored by the microprocessor 1.

A user perceptible variable generator device of the system then generates a plurality of user perceptible variables which are perceptible by the user using their sense of touch. Each user perceptible variable comprises a pattern of tactile sensory information, comprising a pattern of pressure. The user perceptible variable generator device may comprise a processor, for example as part of the microprocessor 1, and may generate 36 distinct pressure patterns.

The pressure patterns are then presented to the user using a presentation device of the system, comprising the haptic mouse 3. Each distinct pressure pattern is presented to the user using a distinct pattern of the pins 10 in each of the arrays 4, 5 of the haptic mouse 3. Each pin pattern of each array is generated by placing a number of the pins in their retracted position and placing the remainder of the pins in their extended position. The pin patterns can be formed from static arrangement of the pins in each array in either their retracted or extended positions, and/or dynamic or cyclic moving patterns of the pins in each array. The pin patterns may be sequentially presented to the user, once or more preferably repeatedly. Pin patterns may be presented to the user on request by the user. For example, the VDU 2 may display an image corresponding to each pin pattern, and the user may request presentation of a pin pattern by selecting, for example by using the haptic mouse 3, the image corresponding to the pin pattern. Each pin pattern presented to the user is distinct and is perceived to be so by the user. Thus the user may differentiate between patterns. The system may encourage the user to place a fingertip over each array 4, 5 of pins 10 of the haptic mouse 3, by for example displaying visual information on the VDU 2, or using a sound generator of the system. The user perceives each pin pattern via the fingertips using his sense of touch.

The authentication system then encourages the user to choose four user perceptible variables each comprising a pin pattern of the two arrays 4, 5 of pins 10 of the haptic mouse 3 presented to the user. This may again be achieved by displaying visual information on the VDU 2, or using a sound generator of the system. A button 6 is provided on the side of the housing 11 of the haptic mouse 3. When the user has chosen a pin pattern, he clicks the button 6, which causes a detector device of the system to detect choice of the pin pattern. Each chosen pin pattern is stored by the

microprocessor 1, and is associated with the identification element of the user.

5 The authentication system may then be used to authenticate a user. The user first enters an identification element into the system, as described above. The identification element is stored by the microprocessor 1, and is compared to previously-stored identification elements of users which have enrolled with the system. If the identification element of the user does not correspond to any of the previously-stored identification
10 elements, the system may ask the user to enrol (as described above) or may deny the user access to the system. Assuming that the identification element of the user corresponds to a previously stored identification element, the identification element is used to retrieve the four user perceptible variables (pin patterns) chosen by the user in his enrolment
15 with the system, and previously associated with the identification element of the user.

The authentication system then generates a plurality of user perceptible variables comprising a plurality of pin patterns, as described above. The
20 plurality of pin pattern user perceptible variables will include the four pin pattern user perceptible variables chosen by the user in his enrolment with the system, and previously associated with the identification element of the user. The authentication system uses the VDU 2 to display an image corresponding to each of the pin pattern user perceptible variables in the
25 plurality of pin patterns. The images comprise minimal visual information, i.e. do not comprise an actual representation of any of the pin patterns of the user perceptible variables.

30 In a first operative embodiment of the invention, the images are presented on the VDU 2 in a grid-style format (see Figures 3 and 4). A first grid-style

format of nine images corresponding to nine pin pattern user perceptible variables is displayed by the VDU 2. These nine pin patterns include a first pin pattern chosen by the user during enrolment. The user uses the haptic mouse 3 to hover a cursor over a first image in the first grid. This causes the haptic mouse to present the pin pattern corresponding to the first image to the user by placing appropriate pins 10 of the arrays 4, 5 of pins in their retracted or extended positions. The system then encourages the user to place a fingertip over each array of pins. When the user places a fingertip over each of arrays of pins, he perceives the presented pin pattern using his sense of touch. By placing a fingertip over each array, the user will be occluded from the visual layout of the pins, and will be required to rely on the sense of touch alone to recognise a pin pattern. If the user perceives that the presented pin pattern corresponds to the first pin pattern chosen during enrolment, the user selects the presented pin pattern by clicking the button 6 of the haptic mouse 3. The user will perceive correspondence between the presented pin pattern and the first pin pattern chosen during enrolment using just recognition of the presented pin pattern. The microprocessor 1 stores the selected pin pattern. If the user perceives that the presented pin pattern does not correspond to the first pin pattern chosen during enrolment, the user does not select the presented pin pattern. The user then uses the haptic mouse 3 to hover a cursor over a second image in the first grid, which causes the haptic mouse to present the pin pattern corresponding to the second image to the user as before. If the user perceives that this presented pin pattern corresponds to the first pin pattern chosen during enrolment, the user selects the presented pin pattern as before, and the microprocessor 1 stores the selected pin pattern. If the user perceives that the presented pin pattern does not correspond to the first pin pattern chosen during enrolment, the user does not select the presented pin pattern, and moves to a third, fourth etc. image in the first grid, until correspondence between

a presented pin pattern and the first pin pattern chosen during enrolment is found, and this pin pattern is selected. A second grid-style format of nine images corresponding to nine pin pattern user perceptible variables is then displayed by the VDU 2. These nine pin patterns include a second
5 pin pattern chosen by the user during enrolment. The user uses the haptic mouse 3 to hover a cursor over a first, second, etc. image in the second grid, as before, and selects a pin pattern corresponding to the second pin pattern chosen by the user during enrolment, and the microprocessor 1 stores the selected pin pattern. A third grid-style format of nine images
10 corresponding to nine pin pattern user perceptible variables is then displayed by the VDU 2. These nine pin patterns include a third pin pattern chosen by the user during enrolment. The user uses the haptic mouse 3 to hover a cursor over a first, second, etc. image in the third grid, as before, and selects a pin pattern corresponding to the third pin pattern
15 chosen by the user during enrolment, and the microprocessor 1 stores the selected pin pattern. A fourth grid-style format of nine images corresponding to nine pin pattern user perceptible variables is then displayed by the VDU 2. These nine pin patterns include a fourth pin pattern chosen by the user during enrolment. The user uses the haptic
20 mouse 3 to hover a cursor over a first, second, etc. image in the fourth grid, as before, and selects a pin pattern corresponding to the fourth pin pattern chosen by the user during enrolment, and the microprocessor 1 stores the selected pin pattern. The position of each image in each of the grids is randomly chosen.

25 The microprocessor 1 comprises stored values of each of the four selected pin patterns. The microprocessor 1 then retrieves the pin patterns associated with the identification means of the user during enrolment, and a comparator device of the system then compares each of
30 the selected patterns with the pin patterns previously associated with the

identification element of the user during enrolment. An authentication device of the system then authenticates the user if the first selected pin pattern corresponds to the first pin pattern previously associated with the identification element of the user, the second selected pin pattern corresponds to the second pin pattern previously associated with the identification element of the user, the third selected pin pattern corresponds to the third pin pattern previously associated with the identification element of the user, and the fourth selected pin pattern corresponds to the fourth pin pattern previously associated with the identification element of the user.

To be authenticated, the user must therefore not only correctly select the pin patterns corresponding to those chosen during enrolment, but must also select the pin patterns in the order in which they were chosen during enrolment. If any errors are made, the user will gain the chance to reauthenticate with the system, however authentication attempts will be limited to a pertinent level.

In a second operative embodiment of the invention, the images are presented on the VDU 2 sequentially in a slide-show format (see Figures 5 and 6). A first slide-show format of nine images corresponding to nine pin pattern user perceptible variables is displayed one after the other by the VDU 2. These nine pin patterns include a first pin pattern chosen by the user during enrolment. The user uses the haptic mouse 3 to hover a cursor over the first displayed image in the first slide-show. This causes the haptic mouse to present the pin pattern corresponding to the first image to the user by placing appropriate pins 10 of the arrays 4, 5 of pins in their retracted or extended positions. The user is again encouraged to place a fingertip over each of arrays of pins, and perceives the presented pin pattern using his sense of touch. By placing the fingertips over the

arrays, the user will be occluded from the visual layout of the pins, and will be required to rely on the sense of touch alone to recognise a pin pattern. If the user perceives that the presented pin pattern corresponds to the first pin pattern chosen during enrolment, the user selects the presented pin pattern by clicking the button 6 of the haptic mouse 3. The user will perceive correspondence between the presented pin pattern and the first pin pattern chosen during enrolment using just recognition of the presented pin pattern. The microprocessor 1 stores the selected pin pattern. If the user perceives that the presented pin pattern does not correspond to the first pin pattern chosen during enrolment, the user does not select the presented pin pattern. The VDU 2 then displays the second image in the first slide show, and the user selects or does select the presented pin pattern as appropriate. This process is repeated until correspondence between a presented pin pattern and the first pin pattern chosen during enrolment is found, and this pin pattern is selected. A second slide-show format of nine images corresponding to nine pin pattern user perceptible variables is then sequentially displayed by the VDU 2. These nine pin patterns include a second pin pattern chosen by the user during enrolment. The user uses the haptic mouse 3 to hover a cursor over the first, second, etc. image displayed in the second slide show, as before, and selects a pin pattern corresponding to the second pin pattern chosen by the user during enrolment, and the microprocessor 1 stores the selected pin pattern. A third slide-show format of nine images corresponding to nine pin pattern user perceptible variables is then sequentially displayed by the VDU 2. These nine pin patterns include a third pin pattern chosen by the user during enrolment. The user uses the haptic mouse 3 to hover a cursor over the first, second, etc. image displayed in the third slide show, as before, and selects a pin pattern corresponding to the third pin pattern chosen by the user during enrolment, and the microprocessor 1 stores the selected pin pattern. A

fourth slide-show format of nine images corresponding to nine pin pattern user perceptible variables is then sequentially displayed by the VDU 2. These nine pin patterns include a fourth pin pattern chosen by the user during enrolment. The user uses the haptic mouse 3 to hover a cursor over the first, second, etc. image displayed in the fourth slide show, as before, and selects a pin pattern corresponding to the fourth pin pattern chosen by the user during enrolment, and the microprocessor 1 stores the selected pin pattern. The position of each image in each of the slide shows is randomly chosen.

As before, the microprocessor 1 comprises stored values of each of the four selected pin pattern user perceptible variables. The microprocessor 1 then retrieves the pin patterns associated with the identification means of the user during enrolment, and a comparator device of the system then compares each of the selected patterns with the pin patterns previously associated with the identification element of the user during enrolment. An authentication device of the system then authenticates the user if the first selected pin pattern corresponds to the first pin pattern previously associated with the identification element of the user, the second selected pin pattern corresponds to the second pin pattern previously associated with the identification element of the user, the third selected pin pattern corresponds to the third pin pattern previously associated with the identification element of the user, and the fourth selected pin pattern corresponds to the fourth pin pattern previously associated with the identification element of the user.

Again, to be authenticated, the user must therefore not only correctly select the pin patterns corresponding to those chosen during enrolment, but must also select the pin patterns in the order in which they were chosen during enrolment. If any errors are made, the user will gain the

chance to reauthenticate with the system, however authentication attempts will be limited to a pertinent level.

- 5 In a third operative embodiment of the invention, after generation of the plurality of pin pattern user perceptible variables, these are presented to the user using the pin arrays as before, but without the use of images corresponding to the pin patterns. The system may use a sound generator to communicate presentation of the pin patterns to the user. The user may use a sound receiver of the system to communicate that he
- 10 is ready to receive presentation of one or more of the pin patterns. For example, the pain patterns may be presented to the user sequentially, in one or more series of patterns. The user may communicate readiness to receive the first pin pattern in the first series of patterns to the system via the sound receiver, and when he has decided to select or not select the
- 15 presented pin pattern, may communicate readiness to receive the second pin pattern in the first series of patterns to the system via the sound receiver, etc., until four pin patterns have been selected which correspond to the pin patterns previously chosen by the user.
- 20 In the embodiments described above, user perceptible variables comprising tactile sensory information are presented to the user, via pin patterns perceived through the user's fingertips. It is envisaged that the tactile sensory information may be presented in a manner to be detectable by other parts of the user's body. Further, embodiments are described
- 25 where four pin pattern user perceptible variables are selected by the user, it will be appreciated that selection of more or less pin patterns may be used.

Benefits of tactile authentication include:

1) Increased security

• The pin patterns are not visible to the eye, and authentication information is perceived directly through the sense of touch alone. The position of image corresponding to pin patterns in the grid and slide show formats are randomly chosen, so the order of selected pin patterns cannot be memorised by third parties.

• As the sense of touch is personal to each individual, user perceptible variables comprising tactile sensory information are difficult to describe in concrete terms, so the information necessary for authentication cannot be easily shared with others.

2) Memorability

• Traditional alphanumeric passwords utilise recall memory, which involves a search of memory and then the comparison process once something is found. This is a more resource intensive process than recognition, which solely performs the comparison process. The tactile authentication system of the invention makes use of recognition, reducing the workload for users.

• As individuals often have to remember a large amount of passwords/PINs, the tactile authentication system offers them an alternative method of remembering information.

3) Accessibility

• The system could potentially be used by the visually-impaired community, who commonly experience problems authenticating entry in conventional computer-based systems.

Various modifications and variations to the described embodiments of the inventions will be apparent to those skilled in the art without departing from the scope of the invention as defined in the appended claims. Although

the invention has been described in connection with specific preferred embodiments, it should be understood that the invention as claimed should not be unduly limited to such specific embodiments.

5 While in the preferred embodiment the array of pins provides a sensory stimulus to the fingertips of the user by axial movement of individual pins between retracted and extended positions, it is envisaged that distinctive sensory information might be created by varying the temperature of each pin or adjacent groups of pins instead of or in addition to axial movement
10 of the pins.

Any haptic or tactile sensory information may be used for the user perceptible variables, including vibrotactile stimuli and force feedback stimuli. Furthermore, it is envisaged that auditory and/or visual stimuli
15 and/or stimulation of the senses of taste and smell may be utilised in addition to tactile sensory information.

Other input devices are also envisaged, such as haptic gloves or other devices fitting close to the user's skin, or any other haptic devices.
20 Furthermore, tactile stimulation may be applied to other regions of the user's body, other than the fingertips. As such, other distinguishable modes of tactile stimulation are envisaged within the scope of the present invention.

25 The user authentication method and system according to the present invention may have a wide variety of applications, including controlling access to computer systems, either stand alone or networked systems, access to shared data repositories, Internet access, access to automated teller machines (ATM) for banking, credit and/or debit card authentication
30 and for controlling access to buildings or secure storage devices such as a

safe (e.g. controlling operation of a locking device). The system and method of the invention may also be applicable to portable security devices which are often used in Internet banking to provide additional security. Such portable security devices generate random security codes for one-time use, dependent on the ID. The user normally enters a user name, password and random code to gain access to a banking web site. Instead of a customer using the generated numerical code, he/she could use a tactile authentication string.

Claims

1. A method for user authentication, the method comprising the steps of:-
 - 5 obtaining an identification element of a user,
presenting the user with a plurality of user perceptible variables which are perceptible by the user using their sense of touch,
detecting selection of at least one of the user perceptible variables by the user,
 - 10 comparing the at least one selected user perceptible variable with one or more user perceptible variables previously associated with the identification element of the user, and
authenticating the user if the at least one selected user perceptible variable corresponds to at least one of the user perceptible variables
 - 15 previously associated with the identification element of the user.
2. A method according to claim 1 in which the user perceptible variables are perceptible by the user using tactile sensory information.
- 20 3. A method according to claim 2 in which the user perceptible variables comprise patterns of tactile sensory information.
4. A method according to claim 3 in which the patterns of tactile sensory information comprise any of patterns of pressure, patterns of vibration, patterns of temperature.
- 25 5. A method according to claim 3 or claim 4 in which the patterns are any of static or cyclic or animated or a combination thereof.

6. A method according to any of claims 3 to 5 in which each user perceptible variable comprises a pattern of pressure provided by a plurality of pins.

5 7. A method according to claim 6 in which each pattern of pressure is perceptible by the user by placing at least one fingertip in contact with the pins.

8. A method according to any preceding claim in which the user
10 perceptible variables are presented to the user on request of the user.

9. A method according to any preceding claim in which the, or at least some of the, user perceptible variables are presented to the user concurrently.
15

10. A method according to any of claims 1 to 8 in which the user perceptible variables are presented to the user sequentially.

11. A method according to any preceding claim in which the user
20 perceptible variables are presented to the user until selection of a predetermined number of user perceptible variables has been detected.

12. A method according to claim 11 in which the user perceptible
25 variables are presented to the user in a first series of user perceptible variables until selection of a user perceptible variable is detected, and then a second series of user perceptible variables until selection of a user perceptible variable is detected, said process being repeated a plurality of times until selection of a predetermined number of user perceptible variables has been detected.

13. A method according to any preceding claim in which authentication of the user takes place if each of a plurality of selected user perceptible variables corresponds to a user perceptible variable previously associated with the identification element of the user.

5

14. A method according to any preceding claim in which authentication of the user takes place if each of a plurality of selected user perceptible variables corresponds to a user perceptible variable previously associated with the identification element of the user, and the order in which the user perceptible variables is selected by the user corresponds to a predetermined order of the user perceptible variables previously associated with the identification element of the user.

10

15. A user authentication system, comprising:-

15

an identifier device which obtains an identification element of a user,

a user perceptible variable generator device which generates a plurality of user perceptible variables which are perceptible by the user using their sense of touch,

20

a presentation device which presents the plurality of user perceptible variables to the user,

a detector device which detects selection of at least one of the user perceptible variables by the user,

a comparator device which compares the at least one selected user perceptible variable with one or more user perceptible variables previously associated with the identification element of the user, and

25

an authentication device which authenticates the user if the at least one selected user perceptible variable corresponds to at least one of the user perceptible variables previously associated with the identification element of the user.

30

16. A system according to claim 15 in which the presentation device comprises a tactile device which presents user perceptible variables comprising tactile sensory information to the user.

5 17. A system according to claim 16 in which the tactile device comprises a pressure device which presents user perceptible variables comprising pressure patterns to the user.

10 18. A system according to claim 17 in which the pressure device comprises a plurality of pins which presents user perceptible variables comprising pin patterns to the user.

15 19. A system according to claim 18 in which each of the plurality of pins may be placed in a retracted position or an extended position to present the pin patterns to the user.

20. A system according to any of claims 16 to 19 in which the presentation device comprises a haptic mouse.

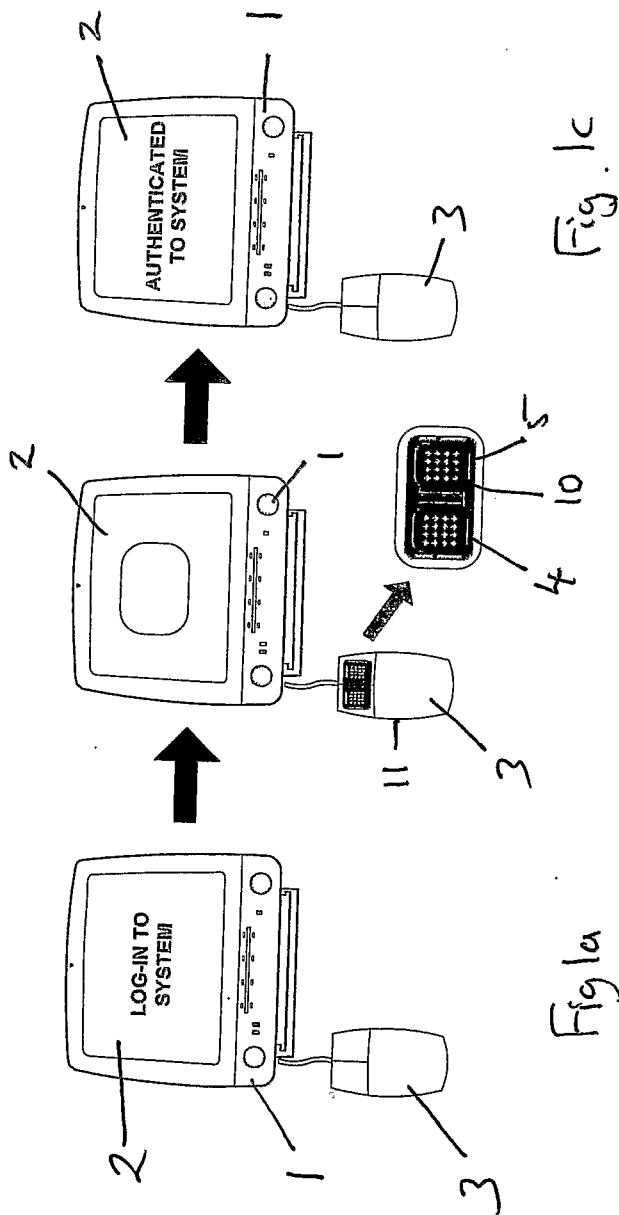


Fig. 1

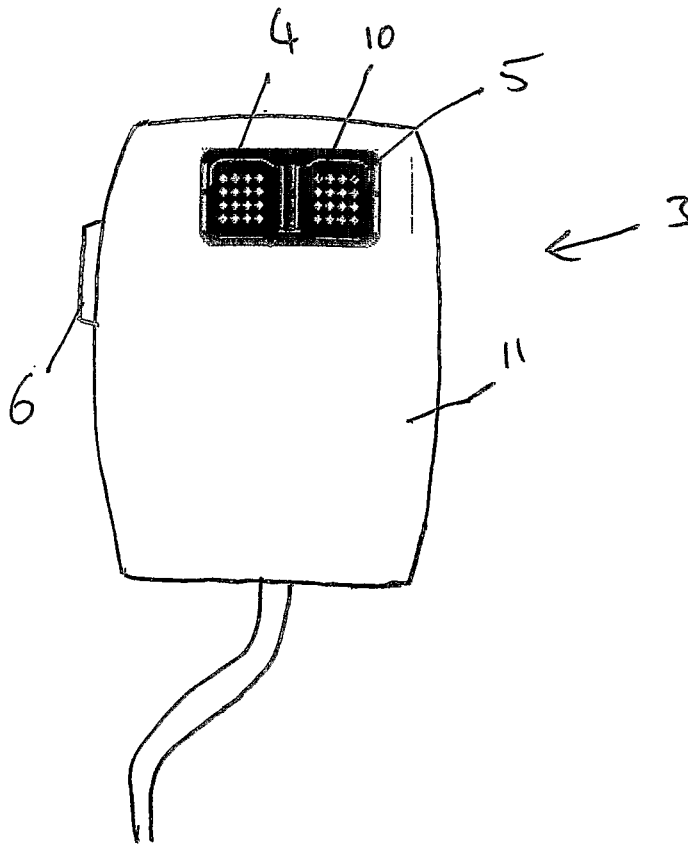


Fig. 2

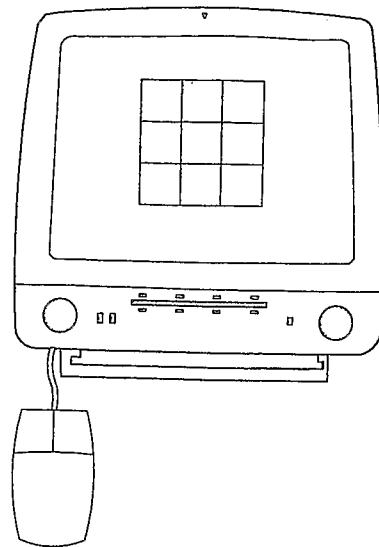


Fig. 3

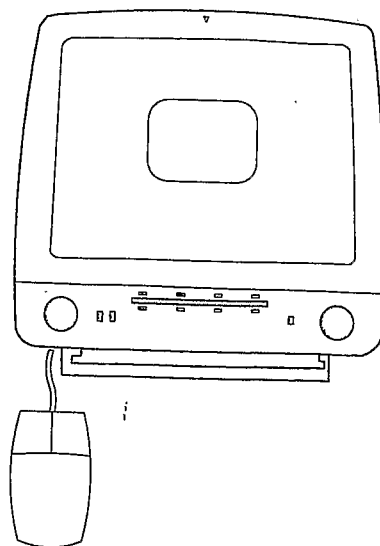


Fig. 5

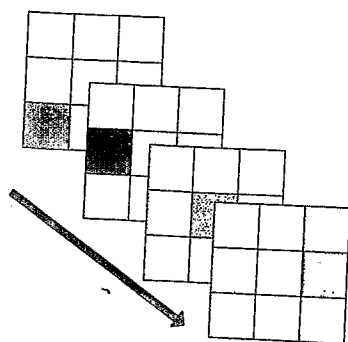


Fig. 4

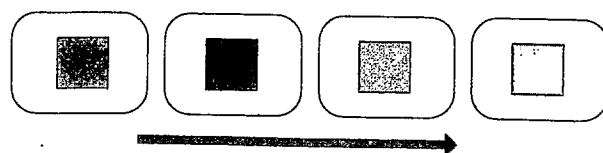


Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2007/000656

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/20

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

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

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

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	ROTH ET AL: "How to fend off shoulder surfing" JOURNAL OF BANKING & FINANCE, NORTH-HOLLAND, vol. 30, no. 6, 2 November 2005 (2005-11-02), pages 1727-1751, XP005431324 ISSN: 0378-4266 paragraph [03.5]; figure 7	1-20
X	US 2005/005119 A1 (KIRKPATRICK SCOTT [IL] ET AL) 6 January 2005 (2005-01-06) claim 1 claim 15 paragraph [0027]	1-20
X	US 2005/171851 A1 (APPLEBAUM TED H [US] ET AL) 4 August 2005 (2005-08-04) paragraph [0034]; claim 1	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 document 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

3 July 2007

Date of mailing of the international search report

20/07/2007

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Mäenpää, Jari

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2007/000656

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
US 2005005119	A1	06-01-2005	WO	2005004366 A2	13-01-2005
US 2005171851	A1	04-08-2005	EP	1728244 A2	06-12-2006
			WO	2005074503 A2	18-08-2005