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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 December 2010 (23.12.2010)

PCT

(10) International Publication Number
WO 2010/146352 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/GB2010/001172

(22) International Filing Date:
15 June 2010 (15.06.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0910545.3 18 June 2009 (18.06.2009) GB
0912008.0 10 July 2009 (10.07.2009) GB

(71) Applicant *(for all designated States except US)*: **RESEARCH IN MOTION LIMITED** [CA/CA]; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **RIDDIFORD, Martin** [GB/GB]; 93 Calton Avenue, London SE21 7DF (GB).

(74) Agent: **KILBURN & STRODE LLP**; 20 Red Lion Street, London WC1 R 4PJ (GB).

(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, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

(54) **Title**: COMPUTING DEVICE WITH GRAPHICAL AUTHENTICATION INTERFACE

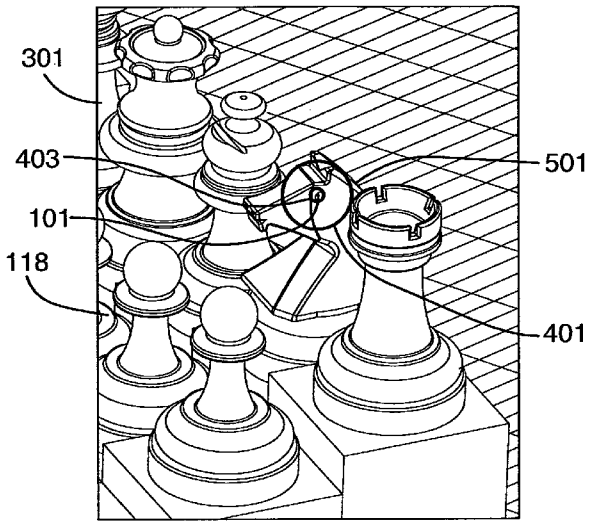

FIG. 5

(57) **Abstract**: A computing device with a graphical authentication interface in which the device displays a base image and authenticates a user when a pre-selected element in a secondary image overlying the base image is aligned with a pre-selected element in the base image.

WO 2010/146352 A1

COMPUTING DEVICE WITH GRAPHICAL AUTHENTICATION INTERFACE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0000] This application claims the benefit of priority of prior Patent Application No. GB0910545.3, filed June 18, 2009 in the United Kingdom Intellectual Property Office, and Patent Application No. GB0912008.0, filed July 10, 2009 in the United Kingdom Intellectual Property Office, the entire contents of both applications are incorporated herein by reference.

FIELD

[0001] This disclosure relates to a computing device with a graphical authentication interface.

BACKGROUND

[0002] Although most computing devices (particularly personal computing devices) have built in password security, many people choose not to have the hassle of initiating it. Those that do are often frustrated by it, and often there is a corporate insistence on changing the password every month. Every log-in ideally needs a different password. Remembering all those passwords and selecting the appropriate one is very onerous.

[0003] In practice password systems for computing devices can be breached in several ways, for example: random trial and error, e.g., hitting random keys, where eventually the correct password will be found, but may take a long time; systematic trial and error, e.g., trying 0000, 0001, 0002, and so forth for a PIN number; inspired guesswork, e.g., trying general favorite numbers, for example, 1066, 1234, and so forth, or personal numbers, for example, birthday, telephone number, and so forth; learning the password by surveillance, shoulder surfing, finding the password written down somewhere, and so forth; hacking, e.g., key click measurement, on-line interception, and so forth; forced disclosure to a mugger.

[0004] A 4 number PIN has a theoretical security of 1 in 10x10x10x10 = 1 in 10,000 or 0.0001. Hackers would probably give up if they had the typical three chances at these odds. However in practice the problem is that people find it hard to remember multiple passwords / numbers, so either they choose a

memorable personal number which is likely to be used widely elsewhere, or a non-memorable one which they need to write down somewhere - usually next to the computing device requiring the security. Finally there have been many reported instances of surveillance scams to learn passwords, or just looking over someone's shoulder when they are entering their PIN or password. So the practical security offered by a PIN number, say (from a hacker's or thieves point of view) is in fact quite modest.

SUMMARY

[0005] A computing device with a graphical authentication interface in which the device displays a base image and authenticates a user when a pre-selected element in a secondary image overlying the base image is aligned with a pre-selected element in the base image.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIG. 1 shows an unsuccessful graphical authentication in accordance with the disclosure.

[0007] FIG. 2 shows a successful graphical authentication in accordance with the disclosure.

[0008] FIG. 3 shows a base image for graphical authentication in accordance with the disclosure.

[0009] FIG. 4 shows a point of interest in the base image and associated circular authentication area during graphical authentication set-up in accordance with the disclosure.

[0010] FIG. 5 shows selection of the point of interest during graphical authentication set-up in accordance with the disclosure.

[0011] FIG. 6 shows selection of an element for a secondary image in the form of a number in accordance with the disclosure.

[0012] FIG. 7 shows a confirmation screen illustrating successful authentication set-up in accordance with the disclosure.

[0013] FIG. 8 shows the base image overlaid by the secondary image in accordance with the disclosure.

[0014] FIG. 9 shows authentication by aligning an element of the secondary image with the point of interest of the base image in accordance with the disclosure.

[0015] FIG. 10 shows a screen confirming successful authentication in accordance with the disclosure.

[0016] FIG. 11 shows a block diagram of a computing device in accordance with the disclosure.

DETAILED DESCRIPTION

[0017] A computing device with a graphical authentication interface in which the device displays a base image and a user, in order to authenticate, aligns a pre-selected element present in a secondary image layer overlying the base image, with a pre-selected element in the base image.

[0018] The method exploits our high degree of visual acuity and memory. We can all remember thousands of faces, many hundreds of images and countless views. It is this natural capacity for easily memorising even minute visual details that is utilised in this method; it requires, in one implementation, a user to memorise an exact spot on a familiar image and to be able to memorise another visual element and align that element over the spot. The user experience is far better than conventional PIN or password based systems. It is also more secure, especially against someone watching you authenticate using this system. Also, users also cannot write down an image or part of an image for others to see or steal, unlike PIN codes or passwords.

[0019] The method will be described with reference to an implementation called Clixel. Clixel is based on a simple analogue alignment task performed on a portable, personal computing device with a colour screen and a 2 dimensional cursor control or other way of (a) selecting a location on an image and (b) moving an image. (In the future this may take place in a 3D virtual environment, and hence require a 3 dimensional controller, but the current Clixel implementation uses a 2D cursor control.)

[0020] The computing device screen displays a base layer image, usually fixed in a static position. Although Clixel uses a static base image layer, the ability to move this could increase security. For example, the computing device could automatically re-size / re-position the base image layer slightly each new time it is displayed to further prevent copying.

[0021] This base image layer is the equivalent to the desktop background picture, probably imported from the user's photos library. A personal picture will be more memorable to the user than a generic sample. A busy, detailed picture works best; software running on the computing device could analyse a picture for busy-ness and score for suitability.

[0022] When setting up the authentication process, the user identifies a memorable point of interest in this base image (we will refer to this as a 'Safe Point') and positions a pointer over it using a mouse or similar and clicks to confirm and set up the target on this layer. Other navigation devices that can be used include a trackpad, ISO point, trackball, touchscreen, tilt /gesture / shake control, cursor keys etc. In some simple touch screen computing devices, such as navigation systems, there is no cursor as such; instead a user simply selects the point of interest by touching it.

[0023] The size of the adjustable target is inversely proportional to the level of security. Once confirmed, the pointer disappears, and the invisible target is activated. A secondary layer now appears and overlays the base layer. Clixel uses 2 layers with x and y cursors controlling the position of each layer, or a simple touch-to-drag the secondary layer approach. Multiple layers (e.g., 3 or more) are also possible for even greater number of permutations and hence security.

[0024] This secondary (it may be the top layer) may be transparent or translucent except for an array of user identifiable elements arranged in a regular pattern or grid. The elements could be numbers, letters words, colours, shapes, lines, icons etc., or any combination of these. (Note that the minimum that is needed for Clixel to work is a cursor for the top layer. This would have a theoretically high level of security if no one was watching, but in practice this is a poor solution as it is so easy to copy.)

[0025] When the cursor/mouse is moved, the whole grid array in the secondary image layer moves over the static base picture. In a touch screen device without a cursor, then the user can simply draw or flick his finger across the touch screen to cause the grid to move over the static base picture. Physics-based modelling can be used so that the speed of touch flick varies the distance the grid moves. Shake or tip control can be used in a computing device with accelerometer(s); a small tip could cause the grid to appear to start sliding over the base image. The grid is repeated or looped in all directions so that there is no edge to it. This means that the selected element is repeated too.

[0026] The task in the set-up phase is to align a preselected identifiable element present in the top layer with the selected point of interest (or Safe Point) in the base layer, and typically to then click to confirm.

[0027] The smaller the grid size, the higher is the number of elements in the second or top layer; the more elements there are, the greater the security, but the harder it is for a user to quickly and easily locate a specific element. Where clicking is inconvenient, say with a touchscreen, a timed dwell could be used as a confirmation. There would however need to be software to prevent 'mine-sweeping' - scanning back and forth slowly enough to trip the timed dwell.

[0028] This set-up procedure can be performed directly on the computing device that requires an authentication mechanism - once the set-up is complete, then the user will need to authenticate himself when accessing the computing device (or specific functions/levels of access offered by the computing device). So, for example, a user of a PC or mobile telephone could complete the above set-up procedure on that PC or mobile telephone. In addition, the user could complete the above set-up procedure on one computing device, and that could be applied to multiple other devices, so the user has merely to go through the set-up once, and then all computing devices to which he may need access share the same authentication process. This is particularly appropriate for authentication required by organisations with multiple computing devices, or for cloud computing applications, for point of sale authentication (e.g., at cash machines and when making purchases using credit or debit cards to replace conventional Chip and PIN systems).

[0029] When a user needs to authenticate himself to a computing device (e.g., whenever the device has been unused for more than a pre-selected time; the same circumstances in which a conventional PIN or password entry would be required), then the device displays the base image. The secondary image layer can then be called up. This can be done in a variety of ways. For a PC, the secondary image layer may appear automatically once the user touches any key on the keyboard or moves the mouse. For a touch screen device, a single touch to the screen could call up the secondary image layer. For a handheld device like a mobile telephone, a short shake (or any of the preceding actions) could call up the secondary image layer. Once the secondary image layer is displayed, the user has to move the elements in that secondary image layer so that the pre-selected element in that secondary image layer sufficiently aligns over the pre-selected point of interest. Because the elements in the secondary image layer are formed into a linked grid of elements, moving one element causes all the rest to move in a predictable manner. So the user does not have to select the pre-selected element and move that – instead, any element can be selected (e.g., the user can place his cursor or simply touch anywhere in the secondary image layer) and then moved until there is a sufficient alignment between the pre-selected element in the secondary image layer and the point of interest in the base layer. But an observer looking over the shoulder of the user will have no idea as to which element the user is aligning, and which region of the base image is the target.

[0030] A display 118 of width X and height Y for a computing device 100 is shown in FIG. 1. The pre-selected point of interest 101 of the base image and the position of the pre-selected element 103 of the secondary image are shown. A successful authentication, e.g., log-in attempt, occurs when the pre-selected element in the secondary image sufficiently aligns over the pre-selected point of interest. In the example of FIG. 1, a circle, having radius D, centered on the point of interest 101 is the authentication area 105 in which a successful authentication results for a position of the pre-selected element. In this example, D is the maximum distance from point of interest to element location for a successful authentication, such as a log-in. E is the distance from the point of interest 101 to the position of the pre-selected element 103 of the secondary

image. Because distance E is greater than the distance D, authentication is not successful in this example.

[0031] In FIG. 1, the authentication is not successful because the alignment between the selected element in the top layer and the point of interest or Safe Point in the base layer is insufficiently accurate. Note that the authentication area 105 can be changed by modifying the value of D. This alters the percentage of the overall screen area (X * Y) that would result in a successful log in attempt. If D is smaller, the position of the element of the secondary image 103 is more accurately aligned to the point of interest 101 to successfully log in. If D is larger, the position of the element of the secondary image 103 can be less accurately aligned to the point of interest 101 to successfully log in. In practice, a vendor of a computing device will through careful testing establish optimal parameter values for a given screen resolution and size, and a given cursor mechanism. The user may also be given the ability to select the effective size of the region associated with a point of interest (i.e., distance D).

[0032] FIG. 2 shows a successful alignment, leading to authentication and hence access to the computing device (or confirmation of a sale if the device is a point of sale terminal, etc.).

[0033] The following reviews the method as described above against the 6 ways of breaching a standard password or PIN.

[0034] Random trial and error, systematic trial and error - The security level is the target area divided by the screen area. A 2mm target on a laptop screen gives about the same level of security as a 4 digit PIN number. If greater security is required, then two or more targets can be used with clicks in sequence. With two targets, security for each stage halves due to the area of the two targets, but the 2 stage operation multiplies the odds, hence this increases theoretically to about 1 in 25 million for the laptop example. Over the shoulder security will be different depending whether the two targets are on the base layer or top layer. However two targets on the base layer and one target on the top layer is likely to be the quickest to use. Further security can be added by tracking the move between both clicks - the vector / gesture / timing can be analysed as a signature.

[0035] Inspired guesswork - Analysis of the base picture might determine that there are say 100 possible points of interest, and areas of no detail hence locally no points of interest. If there are 100 elements in the grid array, then the security is 1 in 1000. However as this is an analogue system, in reality there is likely to be many more than 100 target positions, as the user might target the edge of something, or the boundary between things etc.

[0036] Learning the password by surveillance - If it is desired to protect against someone looking over your shoulder, then Clixel can be adapted to excel in this area. As described above, the grid array always appears the same, so anyone can look at the relationship between a fixed point on the base layer, say the bottom left hand corner, and the nearest element to it on the top layer, and repeat that action. But if the layout of the grid array is changed every time it appears, then this will not work. The changes could be to the pitch of the grid, the orientation or skew of the grid, the order of the elements in the grid, the shape of the grid etc, or any combination of these, giving potentially hundreds of randomly selected variations on the array. These changes would be designed to be subtle and appear similar to the user so as not to confuse.

[0037] As there are two simple, personal entities to remember - the point of interest on the base layer and the identifiable element on the top layer - it should be easier to remember, and therefore there will be less reason to write it down. Because both layers act as prompts there is no chance of choosing the wrong password for the wrong log-in. Even a written down reminder is likely to carry a level of ambiguity - (i.e., "55 and the corner of Anne's mouth"). Knowledge of only one of these entities reduces the level of security in the above example to about 1 in 100 - still a worthwhile hindrance.

[0038] Hacking - the use of the analogue mouse / trackball / touchscreen to enter the password prevents the use of hacking programs such as key stroke grabbers and other such technology being capable of intercepting the user's login details. While the mouse could indeed be tracked, due to the random generation of numbers in the grid tracking the trajectory of the mouse would not elicit the user's password.

[0039] On-line security is further enhanced through use of the combination of hexadecimal information available from both layers for use as the authentication key. Rather than using a simple set of numbers, i.e., the pixel point on the screen and x, y co-ordinate of the picture (although this is indeed an option), the system can merge the binary information from the top grid layer with the base picture layer which is used to render the picture, resulting in a byte code sequence many hundreds of times longer than an average user password. This byte code sequence, rather than a set of letters or numbers, can then be used to authenticate the user against the server system. Due to the length of the sequence this would therefore be far harder to interpret or hack than an average user entered password.

[0040] The information for rendering the separate layers, e.g., the top level grid and the bottom level picture, can also potentially reside in different areas, e.g., the user's picture can be secured and rendered from information within their credit card or mobile phone, while the specific elements required to generate the particular grid for that user can be held on a server system, or generated by the ATM. This segregation of the key elements required to generate the authentication key adds a further level of security by preventing third party access to both elements simultaneously, at least without the item containing the user's original image.

[0041] Forced disclosure to a mugger. Clixel offers a bold victim the chance to mislead a mugger by describing a false alignment while logging-in. Later, when this is tried again, it will not work because of the random grid change.

[0042] A factor for the security and usability of the system is the appearance of the top layer array. There is a trade off between the ease of locating your chosen identifiable element and the number of elements. This is compounded by the requirement to randomly modify the array. Finding your chosen element (say the number 55 in a grid of 10 x 10 grid of 100 numbers) is made easier by arranging the numbers in sequence. This works well for elements with well known sequences, like numbers and letters.

[0043] Another benefit of Clixel is that it can be graphically tailored to suit different users or their preferences. For example the top layer of a child's Clixel

might consist of a selection of coloured shapes. In order to make it easy to find the selected element, the two variables (colour and shape) can be arranged horizontally and vertically, say, so the green triangle is always at the intersection of the green line and the triangle line. Three variables would give a hexagon like grid. To prevent copying the order of the colours and shapes can change every time it appears, as can the pitch / orientation / skew, etc., as before.

[0044] Having a range of base layer images / targets enable the user to have a number of easy to remember logins for different areas of their life - work / home, mobile phone, laptop, on line banking, on line transactions etc. These could all have the same top layer element, or could have different arrays of elements where required. Seeing a picture of the family overlaid with an array of coloured shapes is a visual prompt that you should be lining up the green triangle with Anne's mouth.

[0045] In most scenarios it is envisioned that if the first attempt to log-in is denied, then at least one more is allowed. It may be more convenient to use exactly the same grid array in the last position it was set to start the next attempt, rather than randomly set a new array. This will make it much faster for a user who has been careless with the target alignment. If access is denied again then you are locked out. There are many different known ways to override the lock out, depending on the equipment or service that is protected. It is envisaged that the first lock out will be 'soft', so that some functionality remains, giving the user / thief / hacker / finder appropriate options to rectify the situation.

[0046] A way of increasing the security is to simply have more login screens, i.e., a multiplication of the login process described. After successfully passing the first login screen (a base image / identifier pair) the user is presented with a second screen (base image / identifier pair) and so on until the required number of login stages has been achieved. This is especially important when dealing with smaller screens where the smaller screen size has a negative effect on the maximum security level that can be achieved for a single log in screen (base image / identifier pair).

[0047] This multiplication of log in screens allows for a quick initial access with a lesser level of security (e.g., a single login base image / identifier pair for unlocking a device) and a greater level of security for accessing certain areas of a device that require greater security (banking, email access etc.) or be enforced in an enterprise environment to ensure an adequate level of security. An example would be where only a single login screen is required to unlock a device and access certain functions, like making a call or browsing the web, but to make a payment or access company emails would require a user to pass three login screens before being granted access. Multiplying the screens provides a convenient mechanism for maintaining the flow of the login process but extending the security level by enforcing more login screens as required. The order in which subsequent screens appear could be randomised. An implementation will be described with reference to the accompanying FIG. 3 through FIG. 10. To set up Clixel, a user first chooses any personal image (generally a photograph) as their base image 301 in FIG. 3. This becomes the user's desktop or home screen that appears by default each time the user wishes to start a work session or gain access to the system by entering their name or simply switching the device on.

[0048] Choosing a point of interest 101 (we will refer to this as a 'Safe Point'): By pressing a pre-determined key on a keyboard, clicking on a screen button with the cursor of a mouse or other pointing device, or by using a touchscreen the user activates the Safe Point curser301, shown in FIG. 4 in its default central position.

[0049] The user is now prompted to select a position 401 for their personal Safe Point 101 anywhere on the Base Image 301, in this case the eye the white knight chess piece 501, as shown in FIG. 5.

[0050] The Safe Point cursor 401 can be adjusted in size to suit different screen resolutions, sizes and desired security level – the smaller the size of the Safe Point the more secure the method becomes.

[0051] Setting a Password: The user is now prompted to select a Password, in this case a single number between 1 and 64, equally it could be any form of alphanumerical sequence in this implementation. A typical window is shown in

FIG. 6. In this case the user has chosen the number 11. This prompts a confirmation screen, shown in FIG. 7.

[0052] What the user does to log-in: when the user wishes to log-in or otherwise authenticate, they may, e.g., click on the Clixel logo and Safe Point selector appears overlaid on the Base Image 301, as shown in FIG. 8. In the example illustrated here the Safe Point selector is a repeating series of grids 801, each grid containing randomly generated alphanumeric characters – here nine grids each displaying numerals between 1 and 64 in a variation of sequences. The grids can be moved by the user to any part of the base image to line up the memorised Safe Point 803 with the chosen password, as shown in FIG. 9. When the user has lined up their chosen password 803 on the Safe Point 101, they press enter and if the positioning is correct Clixel permits them to log-in, as shown in FIG. 10.

[0053] A block diagram of an example of a computing device 100, which is shown as a portable electronic device in this example, is shown in FIG. 1. The computing device 100 includes multiple components, such as a processor 102 that controls the overall operation of the computing device 100. Communication functions, including data and voice communications, are performed through a communication subsystem 104 that communicates with a wireless network 150. The wireless network 150 may be any type of wireless network, including, but not limited to, data wireless networks, voice wireless networks, and networks that support both voice and data communications. A power source 142, such as one or more rechargeable batteries or a port to an external power supply, powers the computing device 100.

[0054] The processor 102 interacts with other components, such as Random Access Memory (RAM) 108, memory 110, a display 118, which may optionally be a touch-sensitive display comprising a touch-sensitive overlay operably coupled to an electronic controller, one or more auxiliary input/output (I/O) subsystems 124 including, e.g., navigation devices, a data port 126, a speaker 128, a microphone 130, and other device subsystems 134 known in the art. Information, such as text, characters, symbols, images, icons, and other items that may be displayed or rendered on the computing device 100, is displayed on the display 118 via the processor 102. The processor 102 may interact with an

accelerometer 136 that may be utilized to detect direction of gravitational forces or gravity-induced reaction forces. User identification information may be stored in memory 110. The computing device 100 includes an operating system 146 and software programs or components 148 that are executed by the processor 102 and are typically stored in a persistent, updatable store such as the memory 110. Additional applications or programs may be loaded onto the computing device 100 through the wireless network 150, the auxiliary I/O subsystem 124, the data port 126, or any other suitable subsystem 134.

[0055] Clixel is designed as a personal log-in or authentication method for any electronic device or system that has a digital display such as personal computers, personal information managers, cellular telephones, automated teller machines, security access systems, and so forth.

[0056] Extensions to the basic system. The above implementation involves the user defining, in set-up mode, a specific point of interest (or SafePoint) in a base image and then aligning a specific element from a secondary image layer with that specific point. When access or authentication is subsequently required, the user has to align that element with the specific point of interest. This approach can be generalised to defining, in the set-up phase, a specific type of element in a base image which does not have a fixed location in the base image. A specific type of element from the secondary image layer is aligned with that type of element in the base image layer. For example, the base image could be random arrangement of small images of cars. The user selects a particular car in the set up phase. The secondary image layer could contain a random arrangement of small images of say motor bikes. The user aligns a specific motor bike image over his selected car image. When authentication is subsequently required, the base image of cars appears as before and the secondary image can then be called up. The user alters the grid of motor bike images until there is alignment between his pre-selected car and motor bike. Naturally, any choice of suitable images can be used for the base and secondary image layer, appropriate to the target user base.

[0057] As with the primary Clixel example, more than two layers of images can be used for enhanced security. So for example, the user may in the set-up phase have selected a specific image of a car, a motor-bike, a lady's face; then

when authentication is required, an image layer with for example multiple faces is shown, overlaid with images of multiple cars; the user has to perform the correct alignment and when this occurs, a further image layer with motor bikes appears over the multiple faces; when the correct alignment is carried out, authentication is complete. The type of images do not have to appear in a set-order and the location of the different faces etc within a layer does not have to be the same each time. However, the area associated with each image in a layer has to be a sufficiently small percentage of the overall screen size to make a brute-force attack at least as challenging as in a conventional PIN or password based system. But the authentication process is far more enjoyable to the user.

[0058] The method provides a user with a fast and easy to use way to authenticate himself to the computing device. It is more secure than many conventional password and PIN based authentication systems. It can be used anywhere passwords, PINs and other simple authentication systems are used as log-ins for computers, mobile phones etc, on-line banking and transactions, ATM and Chip and PIN credit and debit card security etc. It can be used in any kind of computing device with a display, including Personal Computers, Personal Information Managers, Cellular Telephones, Automated Teller Machines, Point of Sale terminals and Security Access Systems.

[0059] Improved security is provided by making surveillance by an observer difficult to learn the key. Ease and acceptance of use is facilitated. Easy to remember graphical passwords may be utilized for access to multiple different devices, such as work/home portable phones, laptops, on-line banking, on-line transactions, and so forth.

[0060] A computing device comprises a graphical authentication interface in which the device displays a base image and a user has, in order to authenticate itself, to align a pre-selected element present in a secondary image layer overlying the base image, with a pre-selected element in the base image. The selected element in the base image may be a point of interest in a fixed location in the base image. The user may identify the point of interest in the base image by touching it or selecting it with a cursor. The point of interest may have an associated, surrounding region and the size of the surrounding region may be user-selected. Software running on the computing device may analyse a picture

for suitability as a base image. The secondary image layer may include user-identifiable elements that are numbers, letters words, colours, shapes, lines, icons or any combination of these. The secondary image layer may be transparent except for an array of user-identifiable elements arranged in a pattern or grid. The pattern or grid may be regular. The whole pattern or grid may be made to move over the static base picture to enable the user to align correctly. Physics-based modelling may be used so that the speed of a touch flick varies the distance the pattern or grid moves. Shake or tip control may be used to control the way in which the pattern or grid moves. The pattern or grid may be repeated or looped in all directions so that there is no edge to it. The layout of the pattern or grid may be changed every time it appears. The change may be to the pitch of the pattern or grid, the orientation or skew of the pattern or grid, the order of the elements in the pattern or grid, the shape of the pattern or grid, or any combination of these. Two or more points of interest in the base image may be successively aligned to. The same element in the secondary image layer may be aligned to each of the multiple points of interest in the base image. The combination of hexadecimal information associated with the pre-selected elements in the base image and the secondary image layer may be used as an authentication key. An authentication key may be generated using information associated with the pre-selected element in the base image and information associated with the pre-selected element in the secondary image layer; and each item of information is held in physically remote devices. The choice of elements in the base image and the secondary image layer may be tailored to suit different users or their preferences. After one secondary image layer appears and the user successfully aligns, a further secondary image layer may appear and the user aligns a pre-selected element present in this further secondary image layer with a pre-selected element in the base image. Three or more secondary image layers may be used. The number of secondary image layers may vary depending on the level of security required. The pre-selected element in the base image may be a type of element that does not have a fixed position in the base image but that can appear anywhere in the base image. The computing device may be any of the following group: personal computers, personal information managers, cellular telephones, automated teller machines, security access systems, point of sale terminals.

[0061] The present disclosure may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the disclosure is, therefore, indicated by the appended claims rather than by the foregoing description. All changes that come within the meaning and range of equivalency of the claims are to be embraced within their scope.

CLAIMS

1. A computing device with a graphical authentication interface in which the device displays a base image and authenticates a user when a pre-selected element in a secondary image overlying the base image is aligned with a pre-selected element in the base image.

2. The computing device of claim 1 wherein the selected element in the base image is a point of interest in a fixed location in the base image.

3. The computing device of claim 1 or 2, wherein the point of interest in the base image is identified by touch or selection with a cursor.

4. The computing device of claim 2 or 3, wherein the point of interest has an associated, surrounding region and the size of the surrounding region is user-selected.

5. The computing device of any preceding claim, wherein software running on the computing device analyses a picture for suitability as a base image.

6. The computing device of any preceding claim, wherein the secondary image includes elements that are numbers, letters words, colours, shapes, lines, icons, or any combination thereof.

7. The computing device of any preceding claim, wherein the secondary image is transparent except for an array of elements arranged in a pattern or grid.

8. The computing device of claim 7, wherein the pattern or grid is regular.

9. The computing device of claim 7 or 8, wherein the pattern or grid moves over the static base image to enable alignment.

10. The computing device of claim 9, wherein physics-based modelling is used such that the speed of a touch flick varies the distance the pattern or grid moves.

11. The computing device of claim 9 or 10, wherein shake or tip control controls the way in which the pattern or grid moves.

12. The computing device of any of claim 7 through claim 11, wherein the pattern or grid is repeated or looped.

13. The computing device of any of claim 7 through claim 12, wherein the layout of the pattern or grid is changed every time the pattern or grid is displayed.

14. The computing device of claim 13, wherein the change is to the pitch of the pattern or grid, the orientation or skew of the pattern or grid, the order of the elements in the pattern or grid, the shape of the pattern or grid, or any combination thereof.

15. The computing device of any preceding claim, wherein two or more points of interest in the base image are successively aligned to.

16. The computing device of claim 15, wherein the same element in the secondary image is aligned to each of the two or more points of interest in the base image.

17. The computing device of any preceding claim, wherein a combination of information associated with the pre-selected elements in the base image and the secondary image is at least part of an authentication key.

18. The computing device of any preceding claim, wherein an authentication key is generated using information associated with the pre-selected element in the base image and information associated with the pre-selected element in the secondary image layer, and each item of information is held in physically remote devices.

19. The computing device of any preceding claim, wherein the of elements in the base image and the secondary image are tailored to suit different users or their preferences.

20. The computing device of any preceding claim, wherein after one secondary image appears and successfully alignment is detected, a further secondary image is displayed and authentication results from alignment of a pre-selected element in the further secondary image with a pre-selected element in the base image.

21. The computing device of claim of any preceding claim, wherein three or more secondary image layers are used.

22. The computing device of claim 20, wherein the number of secondary image layers varies depending on the level of security required.

23. The computing device of any preceding claim, wherein the pre-selected element in the base image is a type of element that does not have a fixed position in the base image but that appears anywhere in the base image.

24. The computing device of any preceding claim, comprising any of a personal computers, a personal information manager, cellular telephones, an automated teller machine, a security access system, a point of sale terminal.

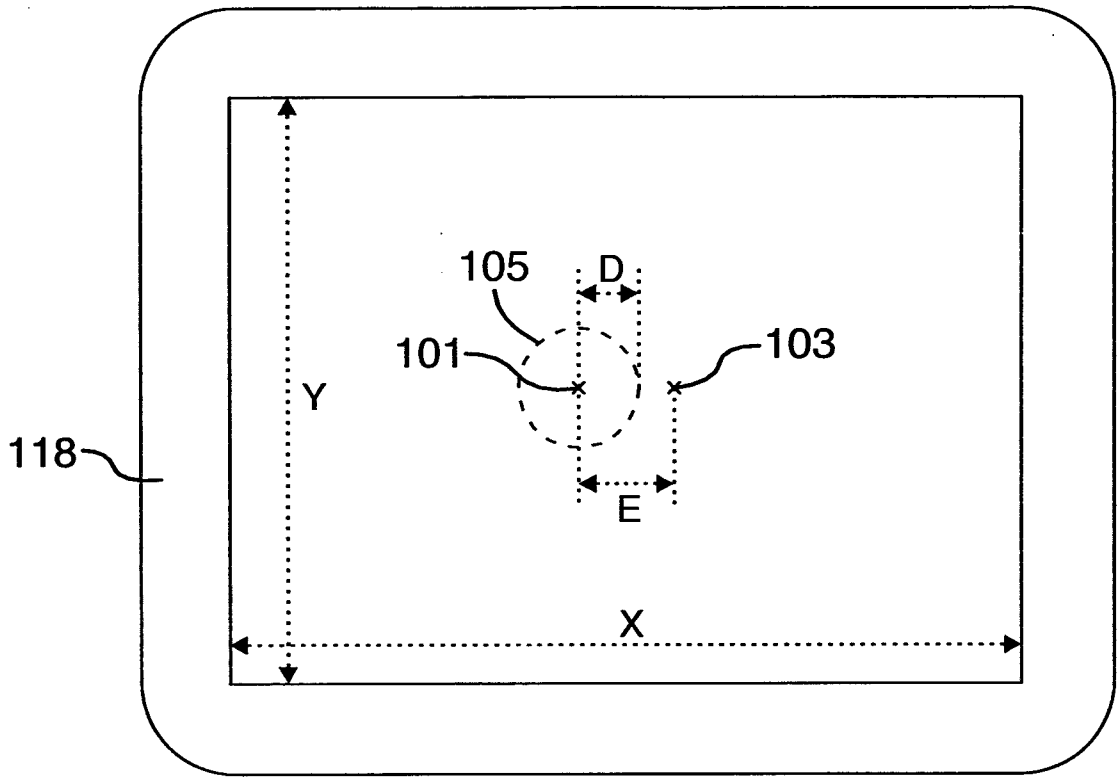

FIG. 1

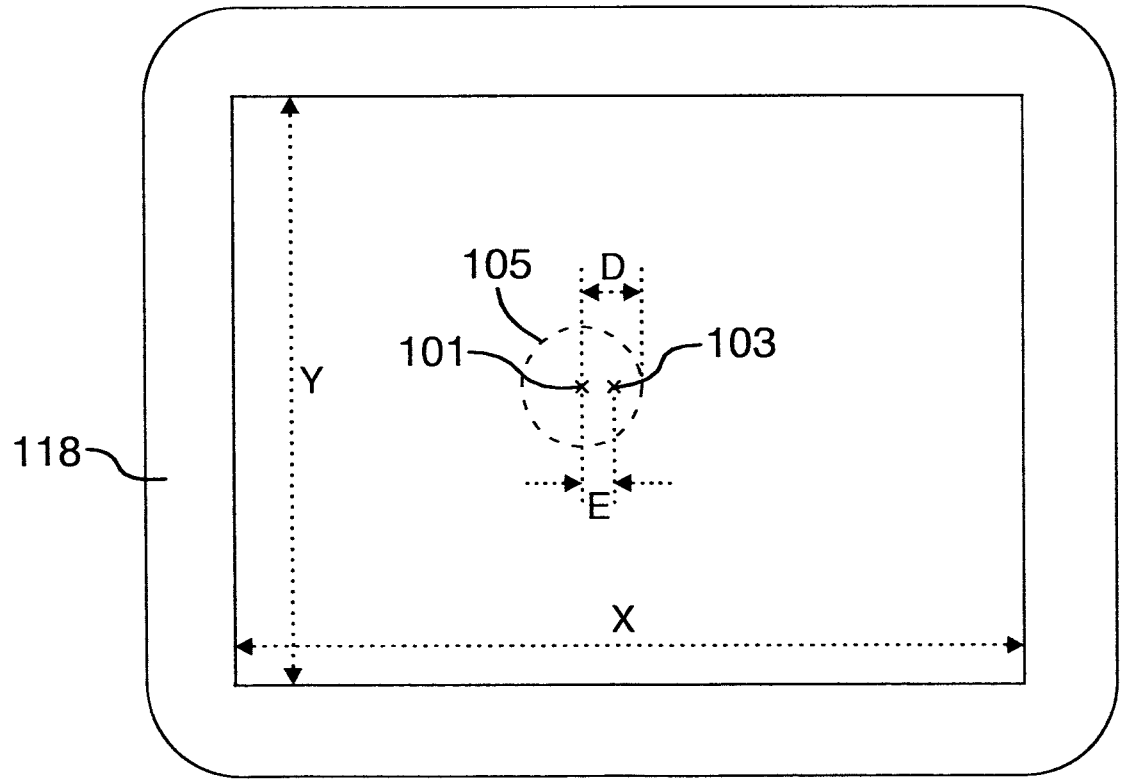

FIG. 2

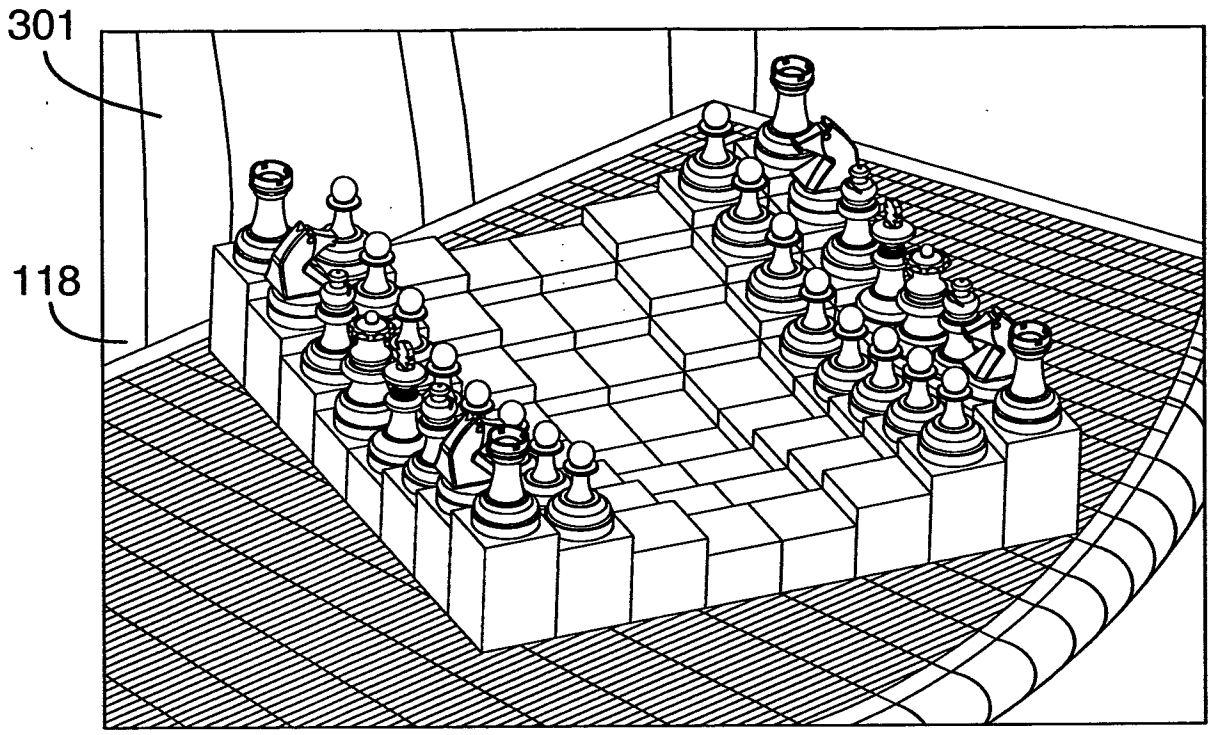

FIG. 3

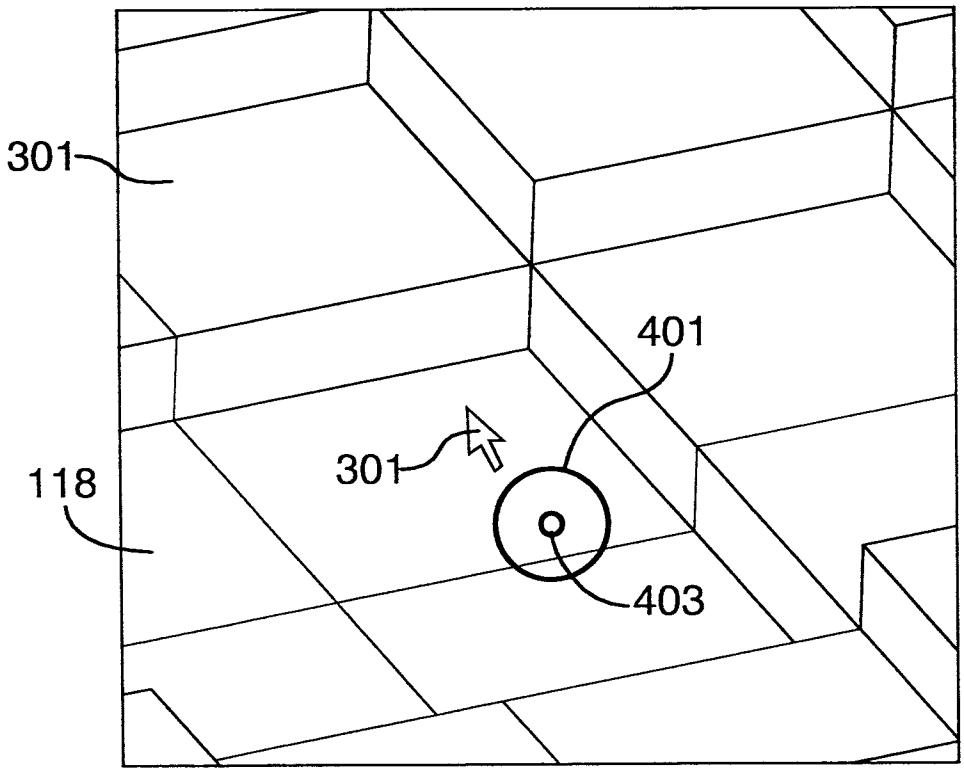

FIG. 4

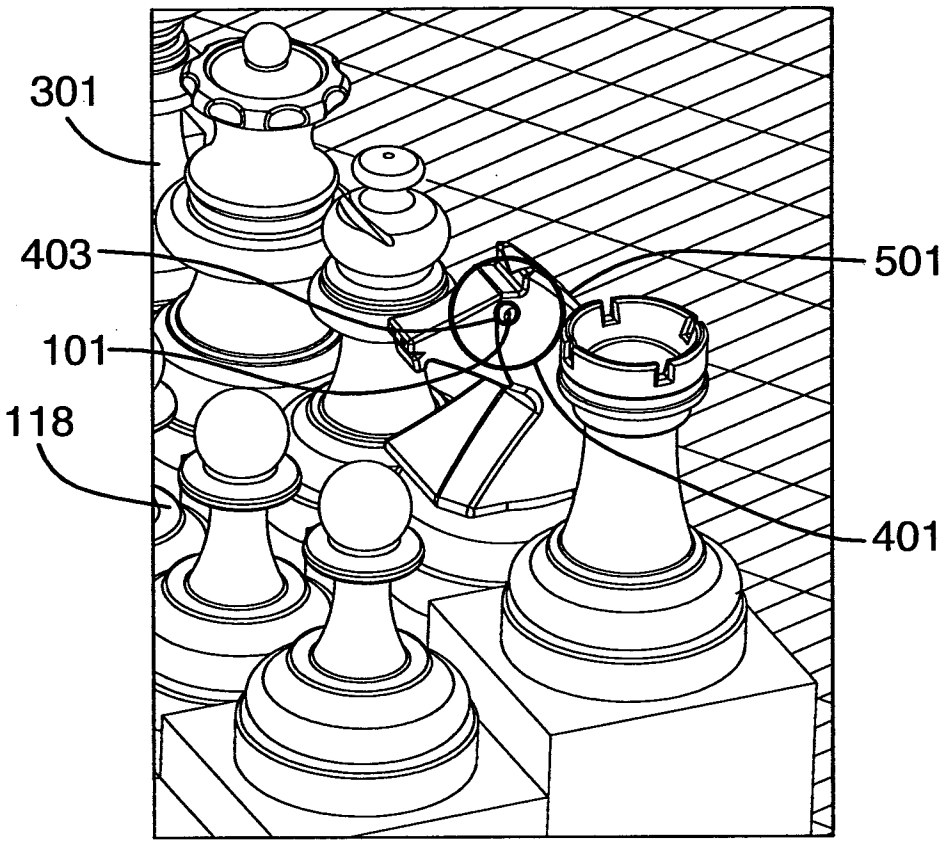

FIG. 5

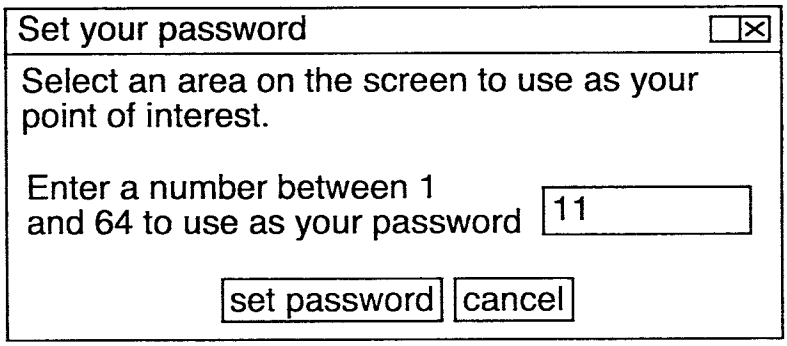

FIG. 6

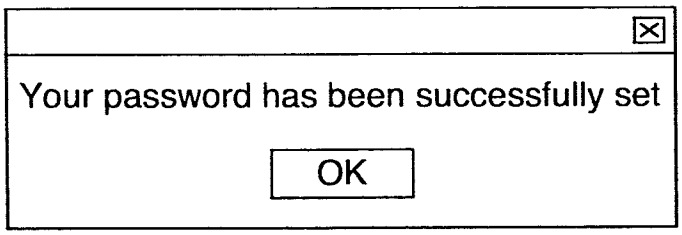

FIG. 7

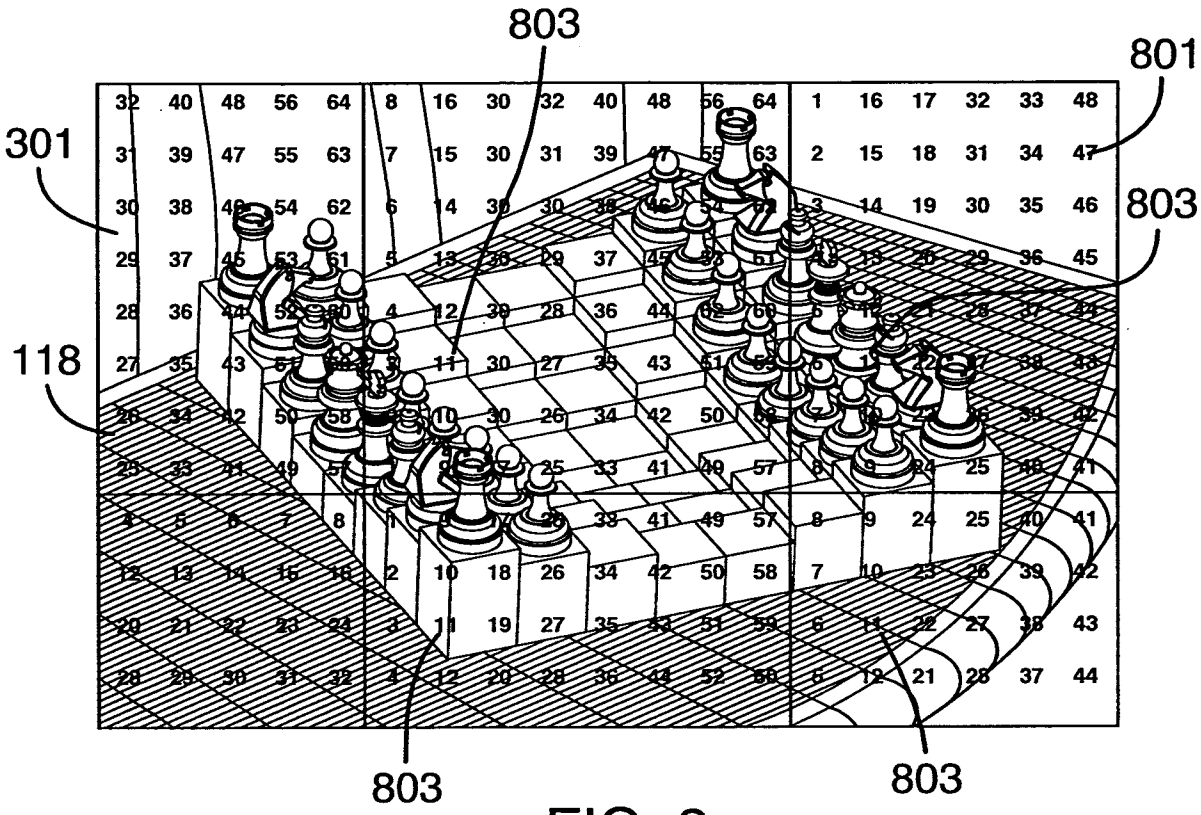

FIG. 8

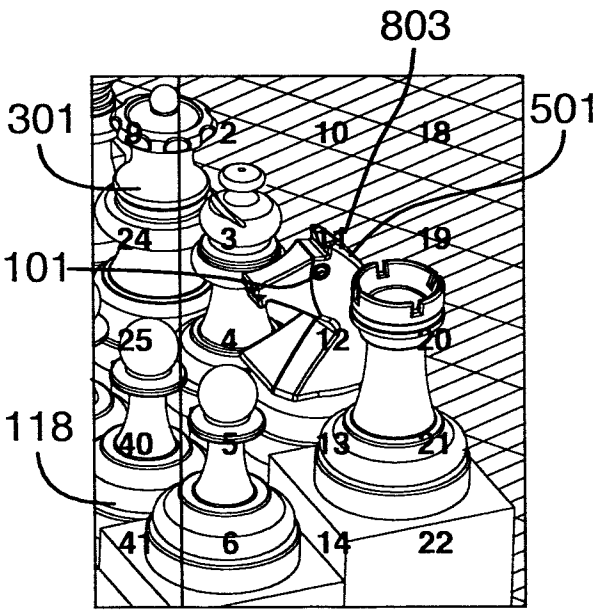

FIG. 9

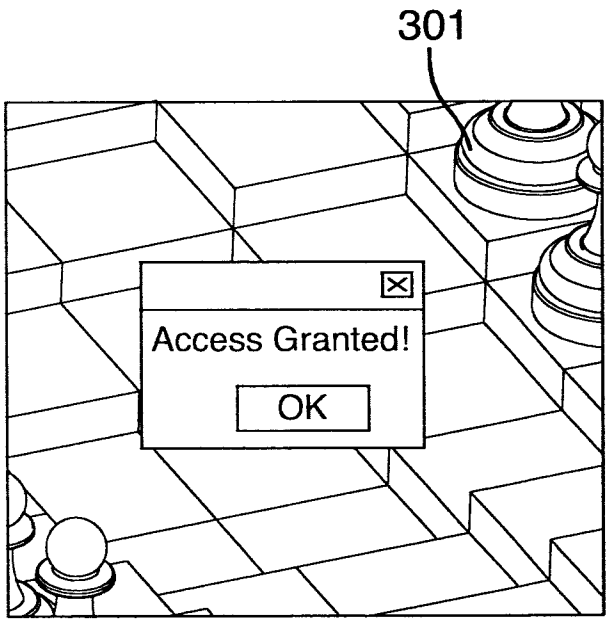

FIG. 10

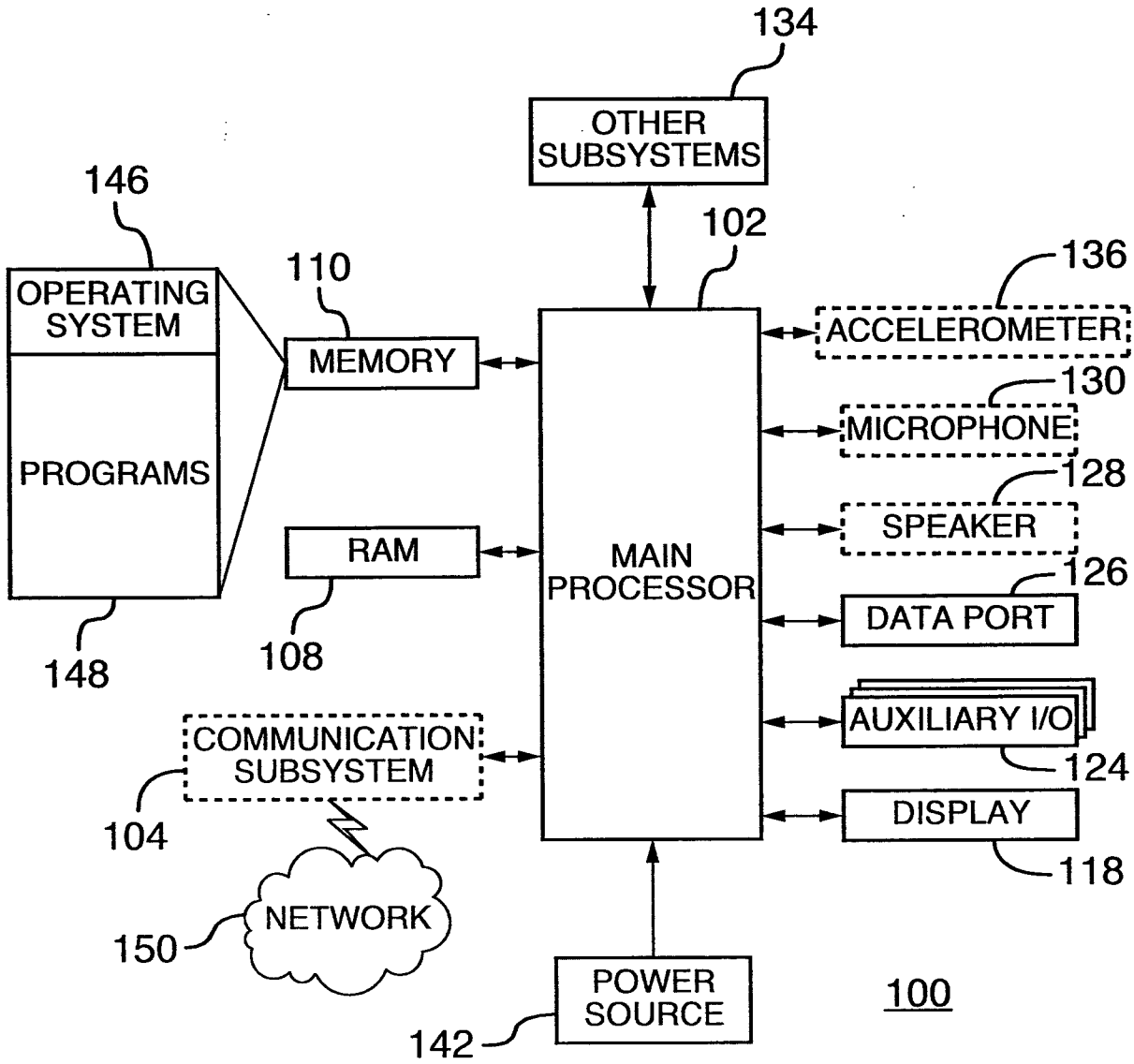
134
OTHER SUBSYSTEMS
146
OPERATING SYSTEM
PROGRAMS
110
MEMORY
102
136
ACCELEROMETER
130
MICROPHONE
128
SPEAKER
126
DATA PORT
AUXILIARY I/O
124
DISPLAY
118
RAM
MAIN PROCESSOR
148
108
COMMUNICATION SUBSYSTEM
104
NETWORK
150
POWER SOURCE
142
100

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2010/001172

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
ADD.

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	WO 2008/124708 A2 (TOMENY THOMAS JOSEPH [US]) 16 October 2008 (2008-10-16) page 5, line 1 - page 20, line 9; figures 5B-5F	1-24
X	EP 0 901 060 A2 (FUJITSU LTD [JP]) 10 March 1999 (1999-03-10) paragraph [0011] - paragraph [0022] paragraph [0024] - paragraph [0162] figures 14-16	1-24
X	EP 1 422 589 A1 (AVIMIR LLC [US]) 26 May 2004 (2004-05-26) paragraph [0005] - paragraph [0035]	1-24

-/--

[X] 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 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	Date of mailing of the international search report
8 September 2010	15/09/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Pinto, Raúl

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2010/001172

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2009/022242 A1 (SONY ERICSSON MOBILE COMM AB [SE]; MARCISZKO TOBIAS [SE]; DE LEON DAVI) 19 February 2009 (2009-02-19) page 1, line 10 - page 4, line 2 page 4, line 25 - page 19, line 17 -----	1-24

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2010/001172

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2008124708 A2	16-10-2008	US 2010037313 A1	11-02-2010
EP 0901060 A2	10-03-1999	DE 69817109 D1	18-09-2003
		DE 69817109 T2	29-04-2004
		JP 3781874 B2	31-05-2006
		JP 11088324 A	30-03-1999
		US 6118872 A	12-09-2000
EP 1422589 A1	26-05-2004	CN 1547688 A	17-11-2004
		JP 2004537116 T	09-12-2004
		WO 03010641 A1	06-02-2003
		US 2009178136 A1	09-07-2009
		US 2004172564 A1	02-09-2004
WO 2009022242 A1	19-02-2009	CN 101772772 A	07-07-2010
		EP 2179380 A1	28-04-2010
		US 2009046929 A1	19-02-2009