Title: SECURING INPUTTING OF SENSITIVE INFORMATION

Abstract: A method of obtaining an input from a user using a user input device, the method comprising: obtaining location data for identifying one or more alternate locations for displaying a symbol; displaying a plurality of symbols on a display of the user input device, each symbol being displayed at a respective initial location on the display; receiving a sequence of selections from the user, each selection corresponding to a location at which one of the plurality of symbols is currently displayed; and in response to one or more of the selections, modifying the location at which one of the plurality of symbols is displayed so that the symbol is instead displayed at one of the alternate locations.

Figure 4
Published:

— with international search report (Art. 21(3))
Securing inputting of sensitive information

Field of the invention

This invention relates to methods, apparatus and computer programs for obtaining and receiving input from a user.

Background of the invention

It is known that certain information and data usually needs to be kept secret, such as bank account numbers, passwords (such as a personal identification numbers (PINs)), private telephone numbers, credit and debit card numbers, etc. It will be appreciated that many other types (or classes) of information also generally need to be kept secret. In this specification, such information shall be referred to as sensitive information (although terms such as restricted information, secret information and secure information may also be used).

To actually use the sensitive information, the information often has to be input (or entered or provided) by a user. For example, for a user to be able to access certain data records stored on a computer, the user may have to input a password or a PIN (i.e. sensitive information). If the user correctly enters a valid password or PIN, then that user will be provided access to those data records. Conversely, if the user does not correctly enter a valid password or PIN, then that user will not be provided access to those data records. As another example, for a user to access details about his bank account, he must correctly enter his bank account number (i.e. sensitive information). Furthermore, for a user to perform a credit card purchase over the Internet, the user will have to enter his credit card number (i.e. sensitive information).

Once the sensitive information has been provided by the user, then the storage, transmission and processing of that sensitive information should be performed in a secure manner. There are various known mechanisms, often
based on encryption, decryption and cryptographic authentication mechanisms, for performing such operations in a secure manner.

Figure 1 of the accompanying drawings schematically illustrates an exemplary networked system 100. A first computing apparatus, in the form of a conventional computer 102 (such as a desktop computer, a personal computer, a laptop, a mainframe computer, etc.) is provided. This computer 102 comprises a processor 104a, a keyboard 106a and a screen (or monitor or display) 108a. As is known in this field of technology, the processor 104a performs various processing operations, and may process data received as an input from the user via the keyboard 106a. The results of the processing performed by the processor 104a may be displayed to the user on the screen 108a.

Other known means of providing input from the user to the processor 104a, such as a mouse and a track-ball, may be used. The screen 108a may be touch-sensitive, so that the user may provide an input to the processor 104a by touching or pressing the screen 108a (e.g. with a finger or a pointer), with the input by the user being dependent on the position at which the user touches or presses the screen 108a.

The computer 102 is connected, via a network 112, to a computer system 114. The network 112 may comprise one or more of: the Internet, a local area network, a wide area network, a metropolitan area network, cable networks, satellite networks, wireless networks, etc. The computer system 114 and the computer 102 communicate with each other, and exchange data with each other, over the network 112. The computer system 114 may comprise one or more computers, servers, etc. for providing various functionality to the computer 102, as discussed in more detail later.

In addition to, or as an alternative to, the computer 102, the networked system 100 comprises a mobile device 116 (such as a mobile telephone, a personal digital assistant, a pager, a laptop, etc.), i.e. a portable device that a user may carry around with him. Similar to the computer 102, the mobile device 116 comprises a processor 104b, a keyboard 106b and a screen (or monitor or
As is known in this field of technology, the processor 104b performs various processing operations, and may process data received as an input from the user via the keyboard 106b. The results of the processing performed by the processor 104b may be displayed to the user on the screen 108b. Again, the screen 108b may be touch-sensitive, so that the user may provide an input to the processor 104b by touching or pressing the screen 108b.

The mobile device 116 is connected, via the network 112, to the computer system 114. The mobile device 116 may be arranged to communicate wirelessly with the computer system 114 over the network 112 via voice channels and/or data channels, as is well known in this field of technology. As such, the network 112 may comprise well known telecommunications apparatus for performing telephonic communications and for converting between telephonic/wireless communications and IP-based or network-based communications.

As mentioned, the system 100 is merely exemplary, and other apparatus forming part of the system 100 may be used by a user. These other devices may have a keyboard 106 (with one or more keys or buttons) with which the user can provide his input, and a display 108 capable of displaying data and information to the user. Alternatively, these other devices may simply have a touch-sensitive display 108 for both receiving the user input and displaying information to the user. Such a device could be, for example, an ATM machine (also known as a cash-machine or a cash dispenser), which usually uses a keyboard 106 to allow a user to enter a PIN associated with a debit card or a credit card in order to perform transactions with that debit card or credit card. Additionally, payment by a credit card or a debit card is increasingly requiring a user to enter a PIN associated with that credit card or debit card at a device that is provided by a retailer, restaurant, etc. All of these additional types of devices and machines (which are referred to as user input devices in the remainder of the description) may form part of the system 100 in a similar manner to the computer 102 and the mobile device 116, and may communicate over the network 112 with a computer system 114. The system 100 may thus comprise zero or more such additional
types of devices, zero or more computers 102 and zero or more mobile devices 116, with these numbers potentially varying over time.

The remainder of this description will therefore be described with reference to various types of user input device and in particular the mobile device 116. However, it will be appreciated that the following description applies equally to the computer 102 and to any of the above-mentioned additional user input devices.

A user may need to enter sensitive information at the mobile device 116. This sensitive information may be data that is used solely at the mobile device 116. For example, it may be a password or PIN that the user uses to log-in to the mobile device 116. In this case, the mobile device 116 may not currently form part of the system 100 and may be added to the system 100 once the user has logged-in to the mobile device 116. After the user has logged-in to the mobile device 116, the sensitive information that the user input is no longer stored by the mobile device 116.

The sensitive information may, instead, be data that the user enters at the mobile device 116 for storage at the mobile device 116 so that the user can access and use it later.

Alternatively, the sensitive information may be data that is to be transmitted to the computer system 114. For example, the computer system 114 may be operated by a bank to allow a bank account holder to access his bank account via the network 112. In this case, the user may have to enter the bank account number, and possibly a password, at the mobile device 116, with the mobile device 116 subsequently transmitting this data to the computer system 114 so that the bank account information can be accessed by the mobile device 116. As another example, the computer system 114 may be operated by a sales outlet (such as a florist selling flowers or a retailer of train tickets) and the user may wish to buy something from the sales outlet. In this case, the user may have to enter a credit card number at the mobile device 116, with the mobile device
116 subsequently transmitting this data to the computer system 114 so that the credit card information can be used to complete the user's desired purchase.

Although the storage and transmission of sensitive information can often be performed in a secure manner (using encryption, cryptographic authentication, etc. as is known in this field of technology), the actual input and entry of the sensitive information by the user is often not performed in as secure a manner. For example, it is known for so-called key-logger applications to be surreptitiously installed on the mobile device 116 and which, unbeknownst to the user, are executed by the processor 104b to create a record, or log, of the various keystrokes entered by the user at the keyboard 106b. In this way, an attacker may use the key-logger application to determine the sensitive information entered by the user by inspecting the log of keystrokes generated by the key-logger application. For example, when a user types in a password using the keyboard 106b, the sequence of keystrokes corresponding to that password will be recorded by the key-logger application, thereby revealing the password to the attacker. This breach of security would occur regardless of any subsequent cryptographic techniques that are used to secure the storage and transmission of the password.

Additionally, an application that logs which parts of a touch-sensitive display 108b have been pressed may be surreptitiously installed on the mobile device 116 and may, unbeknownst to the user, be executed by the processor 104b to create a record, or log, of the various display-touches entered by the user. Thus, in a similar manner to the above-described key-logger application, such an application may be used to determine what information a user has input via the touch-sensitive display 108b, and, when this information is sensitive information, a security breach will then have occurred.

Furthermore, when a user needs to enter data (such as a PIN at an ATM), it is sometimes possible for somebody to visually observe the keystrokes used by that user. That observer may then be able to make use of the observed keystrokes. This is known as "shoulder-surfing". For example, that observer
may have observed the keystrokes used by a user for entering a PIN for a credit card. If that observer then steals that credit card, he can make use of the credit card as he knows how to enter the PIN.

Further security concerns involve so-called "phishing", in which an attacker pretends to be a different entity to fool a user into interacting with the attacker in the mistaken belief that he is interacting with that different entity. In this way, the user may be fooled into divulging sensitive information to the attacker that they would not normally have revealed to the attacker.

Additionally, it may be possible for an attacker to intercept a transmission between a transmitter and a receiver and interpret the intercepted data, which may include sensitive information. This might require the attacker knowing how to decrypt the intercepted data.

It would therefore be desirable to improve the methods of receiving input data from the user to overcome these security problems.

Furthermore, a common characteristic of the communication for mobile devices in a mobile communication network is that the signal strength varies with time and/or movement, which can sometimes result in intermittent connectivity between the mobile device and the mobile communication network. It may therefore be further desirable to minimise the number of data transmissions (or communication round-trips) required to address the above-mentioned security problems.

Summary of the invention

According to a first aspect of the invention, there is provided a method of obtaining an input from a user using a user input device, the method comprising:

- obtaining location data for identifying one or more alternate locations for displaying a symbol;
- displaying a plurality of symbols on a display of the user input device, each symbol being displayed at a respective initial location on the display;
- receiving a sequence of selections from the user, each selection corresponding to a location at which one of the plurality of symbols is currently
displayed; and in response to one or more of the selections, modifying the location at which one of the plurality of symbols is displayed so that the symbol is instead displayed at one of the alternate locations.

In some embodiments of the invention, said modifying modifies the location at which two or more of the plurality of symbols are displayed so that said two or more symbols are instead displayed at respective ones of the alternate locations.

In some embodiments of the invention, the location data provide an ordering for the alternate locations, and wherein said modifying selects a next alternate location according to said ordering for use in modifying the location at which said one of the plurality of symbols is displayed.

In some embodiments of the invention, modifying the location at which one of the plurality of symbols is displayed in response to a selection of the one or more selections comprises modifying the location at which the symbol that is currently displayed at the location selected by that selection is displayed.

In some embodiments of the invention, the alternate locations correspond to locations on the display of the user input device at which no symbol is initially displayed.

In some embodiments of the invention, modifying the location at which one of the plurality of symbols is displayed so that the symbol is instead displayed at one of the alternate locations comprises determining whether a second symbol is currently displayed at said one of the alternate locations, and, if so, modifying the location at which the second symbol is displayed so that the second symbol is instead displayed at the location at which said one of the plurality of symbols is displayed.

In some embodiments of the invention, modifying the location at which one of the plurality of symbols is displayed so that the symbol is instead displayed at one of the alternate locations comprises determining whether a second symbol is currently displayed at said one of the alternate locations, and, if so, modifying the
location at which the second symbol is displayed so that the second symbol is instead displayed at a further one of the alternate locations.

In some embodiments of the invention, modifying the location at which one of the plurality of symbols is displayed so that the symbol is instead displayed at one of the alternate locations comprises setting the location at which said one of the plurality of symbols is currently displayed to be an additional alternate location.

The method may further comprise displaying a visual cue illustrating the modification.

The method may comprise receiving, at the user input device, the location data together with position data for identifying the initial locations.

In a second aspect of the invention, there is provided a method of receiving input from a user of a user input device, the method comprising: obtaining position data for identifying, for each symbol of a plurality of symbols, a respective initial location for displaying that symbol on a display of the user input device; obtaining location data for identifying one or more alternate locations for displaying a symbol on the display; and receiving, from the user input device, a sequence of selections representing the input from the user of the user input device, each selection corresponding to a location at which one of a plurality of symbols was displayed on the display of the user input device when the selection was made; wherein the user input device is configured to obtain said sequence of selections by carrying out any one of the above-mentioned methods based on said initial locations and said alternate locations.

The method of the first and/or second aspects may further comprise generating a sequence of symbols by determining, for each selection in the sequence of selections, which symbol was displayed at the corresponding location when the selection was made.

In some embodiments of the first and/or second aspects, the location data comprises a seed value and the method comprises randomly determining the one or more alternate locations based on the seed value.
The method of the first and/or second aspects may comprise randomly determining the initial locations based on a seed value.

In a third aspect of the invention, there is provided an apparatus arranged to carry out any one of the above-mentioned methods.

In a fourth aspect of the invention, there is provided a computer program which, when executed by a processor, causes the processor to carry out any one of the above-mentioned methods.

In a fifth aspect of the invention, there is provided a computer readable medium storing a computer program according to the fourth aspect.

**Brief description of the drawings**

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

Figure 1 schematically illustrates an exemplary networked system;

Figures 2A, 2B, 2C, 2D, 3A and 3B schematically illustrate symbols displayed on a display according to embodiments of the invention; and

Figure 4 is a flow diagram schematically illustrating a method for receiving input from a user according to an embodiment of the invention.

**Detailed description of embodiments of the invention**

In the description that follows and in the figures, certain embodiments of the invention are described. However, it will be appreciated that the invention is not limited to the embodiments that are described and that some embodiments may not include all of the features that are described below. It will be evident, however, that various modifications and changes may be made herein without departing from the broader spirit and scope of the invention as set forth in the appended claims.

Embodiments of the invention will be described with reference to the system 100 described above with reference to figure 1. In particular,

embodiments of the invention will be described using various types of user input
device, such as the mobile device 116, as examples of devices at which a user provides an input and which receives the input from the user. However it will be appreciated that the embodiments described below apply equally to the computer 102 and to any of the other above-mentioned additional devices (such as ATM machines, and credit card and debit card payment devices). It will also be appreciated that, unless stated otherwise, embodiments of the invention do not need to make use of the networked system 100, and may be used by the above-mentioned devices in isolation from the networked system 100 (for example when data is to be entered at a device and used solely by that device).

The user input device, such as the mobile device 116, executes a computer program for carrying out a method for receiving input from a user, as described in more detail below. This may also involve the computer system 114 executing a computer program for use in coordination with the mobile device 116. These computer programs may be stored on a storage medium (such as a ROM, a RAM, a CD-ROM, a DVD-ROM, a BluRay disk, a memory card/device, etc.). These computer programs may be stored on a transmission medium (such as the data communication channels established in the networked system 100).

In embodiments of the invention, information is to be input by a user at a device (such as the mobile device 116) and received from the user at that device. The information may relate to and comprise sensitive information. However, embodiments of the invention apply equally to information that does not comprise sensitive information.

The information to be input by the user may be considered to comprise one or more symbols. Each of the symbols of this input data may be selected by the user from a plurality, or a set or alphabet, of available symbols. For example, if the symbols are to be numbers and the input data is to be numerical, then the set of symbols may be \{0, 1, 2, ..., 9\}, whereas if the symbols are to be letters and the input data is to be purely textual, then the set of symbols may be \{a, b, ..., z\}. 
A symbol may be a number, a letter, a punctuation mark, or, indeed, any character or token, so that the information entered by the user is then a sequence of one or more symbols, such as a numerical string, a series of letters, an alphanumeric sequence, etc.

The set of symbols may have a natural, or customary or standard, ordering (or arrangement). For example, when the symbols are numbers, the ordering $0, 1, 2, \ldots, 9$ and $1, 2, \ldots, 9, 0$ are normal, and when the symbols are letters, the alphabetic ordering is normal. The ordering may be a 1-dimensional ordering, as in the examples given above. However, the ordering may be multi-dimensional.

For example, the natural ordering may be 2-dimensional, such as (a) the standard QWERTY layout for letters on a keyboard or (b) the standard arrangement of number buttons on a telephone or credit card payment device.

In an embodiment of the invention, the set of symbols to be used for the information to be entered by the user is displayed on the display 108. These symbols are displayed in a particular order or arrangement (as will be described below in more detail). The ordering may be a 1-dimensional ordering (in which the symbols are displayed in a row or a line) or may be 2-dimensional ordering (in which the symbols may be ordered by a first coordinate and then a second coordinate of the 2-dimensional display).

Figures 2A, 2B, 2C and 2D schematically illustrate a set (or plurality) of symbols $\{0, 1, 2, \ldots, 9\}$ being displayed in an initial arrangement 200A and in subsequent arrangements 200B, 200C and 200D on a display 108 of a user input device according to an embodiment of the invention.

The set of symbols displayed in the exemplary arrangements 200A, 200B, 200C and 200D is the set of numbers $\{0, 1, 2, \ldots, 9\}$, such as may be used for allowing a user to securely enter a PIN number. It will be appreciated, however, that the set of symbols can be any set of symbols comprising any types of symbols in any combination as discussed above.

The arrangements 200A, 200B, 200C and 200D identify locations 210 at which symbols can be displayed - i.e. they associate a respective location 210
with each symbol to be displayed. A location 210 may be considered to be a point, or a coordinate, on the display 108, or it may be a region or an area of the display 108. The locations 210 (or symbols at the locations 210) are selectable by the user to allow the user to select and input the symbol displayed at that location 210. A user may select a particular symbol in a variety of ways. For example, the display 108 may be touch sensitive, in which case the user may simply touch the display 108 at the location 210 at which the desired symbol is displayed, thereby selecting and inputting that symbol. Consequently, the locations 210 may be implemented as areas of the display 108, as opposed to distinct points on the display 108. Alternatively, when the user uses the keyboard 106, the user may use certain keys (such as cursor-keys or a scroll key or forwards and backwards keys) as is well-known) to move a displayed cursor 202 to highlight one of the locations 210. The cursor 202 may be, for example, an enhanced border or edge displayed around a currently highlighted or chosen location 210 or symbol. Alternatively, the cursor 202 may be achieved by inverting the colours within the currently chosen location 210 (such as swapping around black and white). Once the user has highlighted a chosen location 210 at which the symbol he wishes to enter is displayed, then the user may use an enter-key on the keyboard 106 to select that location 210, and hence input the symbol displayed at that location 210. It will be appreciated that other methods of using the keyboard 106 may be used to select a location 210 and thereby input a correspondingly displayed symbol.

The symbols are displayed at the locations 210 on the display. All of the available locations 210 may be occupied by symbols, meaning a symbol is displayed at each location 210. Alternatively, only some of the available locations 210 may be occupied by symbols, with the remaining locations, at which no symbol is currently displayed, being unoccupied or empty locations. The arrangement 200 may also contain unoccupied or empty locations 210, at which no symbol is currently displayed. As an example, in the arrangement 200A, locations 210(2), 210(4), 210(5), 210(7), 210(10), 210(11), 210(13), 210(14),
210(15) and 210(16) are occupied by the symbols '6', '7', '5', '2', '1', '0', '3', '9', '4' and '8' respectively, whilst locations 210(1), 210(3), 210(6), 210(8), 210(9) and 210(12) are unoccupied, with no symbols being displayed at these locations.

All of the symbols in the set of symbols may be displayed at the same time (as shown), or alternatively, a sub-set of the set of symbols may be displayed, and a mechanism for changing the particular sub-set that is displayed is provided, such as displaying arrows (not shown) for the user to select to allow him to move forwards and backwards through various sub-sets of the set of symbols. This display of sub-sets of the set of symbols may be particularly useful if there are more symbols in the set of symbols than there are locations 210, or alternatively if a particular number of unoccupied locations are desired and there are not enough remaining locations to display the entire set of symbols.

The initial arrangement 200A of the set of symbols is created according to a mapping which associates each symbol with a respective initial location 210 at which that symbol is to be displayed. The process of generating the mapping and displaying the symbols in an initial arrangement 200A is discussed in further detail below with reference to figure 4.

The subsequent arrangements 200B, 200C and 200D are displayed in response to selections received from the user. The subsequent arrangements are formed (or created) from the currently displayed (or current) arrangement by modifying the locations at which a number of symbols in the set of symbols are displayed so that those particular symbols are instead displayed at alternate locations 210 from the set of locations 210 instead of at their current locations 210. In preferred embodiments, this number is kept small (relative to the number of symbols displayed) so that the subsequent arrangement is not too different from the current arrangement, thereby preventing the user from becoming overly confused. In particular, this number may be just a single symbol, although it could also be, for example, 2 or 3 symbols. The process of forming and displaying the subsequent arrangements in response to selections received from the user is discussed in further detail below with reference to figure 4.
Whilst figures 2A, 2B, 2C and 2D illustrate the locations 210 at which the symbols may be displayed being arranged in a regular grid (or a set) of predetermined locations 210, the locations 210 used for the arrangement need not be in such a regular grid - the available locations 210 for an arrangement could, instead, be in some other predetermined configuration.

Figures 3A and 3B schematically illustrate the symbols of figure 2A, 2B, 2C and 2D displayed on the display 108 using two further different generated arrangements 300A and 300B. In figure 3A, the locations 210 are arranged in a circle and no empty or unoccupied locations 210 are present. In the embodiments shown in figures 2A, 2B, 2C, 2D and 3A, the arrangements make use of a predetermined set of available locations 210 (or at least a subset of a predetermined set of available locations 210), i.e. the locations 210 may be distributed across the display 108 in a predetermined manner. However, alternative embodiments of the invention may generate the set of available locations 210 to be used in a non-predicted or random manner. For example, the set of locations 210 to use for the arrangement may be randomly chosen coordinates on the display 108, or randomly chosen non-overlapping areas on the display 108. Thus, as shown in figure 3B, the locations 210 may be scattered and distributed randomly on the display 108. The determination of the positioning of the available locations 210 may be made independently to the generation of the mapping/assignment/association of symbols to locations 210.

In summary, figures 2A, 2B, 2C and 2D schematically illustrate a set of symbols {0, 1, 2, ..., 9} being displayed in an initial arrangement 200A and in subsequent arrangements 200B, 200C and 200D on a display 108 of a user input device. These exemplary arrangements 200 illustrated in figures 2A, 2B, 2C and 2D will now be discussed further in relation to figure 4. However, it will be appreciated that other arrangements could be used in relation to the method figure 4, that other sets of symbols could be used in relation to the method of figure 4, and that more or fewer arrangements than the four illustrated in figures
2A, 2B, 2C and 2D could be used in the method of figure 4 when inputting an amount of data.

Figure 4 is a flow diagram schematically illustrating a method for receiving an input from a user according to an embodiment of the invention. Figure 4 will be discussed in conjunction with figures 2A, 2B, 2C and 2D to illustrate an example of providing input of a PIN by a user (hereafter referred to as the PIN entry example). However it will be appreciated that the method can be used to provide data entry for any purpose on any type of user input device.

At a step S402, an initial arrangement 200A of the plurality of symbols is determined (or created or generated or identified). In particular, each of the plurality of symbols is associated with a respective initial location 210 on the display 108. The set of initial locations 210 may be predetermined; alternatively, at the step S402, the set of initial locations 210 may be generated or established, e.g. the initial locations 210 (or their coordinates or regions or positions) may be randomly or pseudo-randomly generated at least in part (e.g. based on a seed value) or initial locations 210 may be selected (potentially randomly) from a set of predetermined locations 210 (e.g. from a set of locations making up a predetermined configuration of locations, such as a grid). Similarly, the assignment or association of a symbol of the plurality of symbols to a corresponding initial location 210 may be predetermined (e.g. to form a natural or standard ordering in which to display the plurality of symbols as mentioned above); alternatively, the assignment or association of a symbol of the plurality of symbols to a corresponding initial location 210 may be determined randomly or pseudo-randomly. Thus, the initial arrangement 200A may be predetermined or the initial arrangement 200A may be generated, at least in part, randomly or pseudo-randomly.

As an example, for the initial arrangement 200A as shown in figure 2A, the possible locations 210 are predetermined locations forming a grid, the set of initial locations chosen 210(11), 210(10), 210(7), 210(13), 210(15), 210(5), 210(2), 210(4), 210(16) and 210(14) is a random selection, and the association of
the symbols 'O', '1', '2', '3', '4', '5', '6', '7', '8', '9' with the locations 210(1),
210(10), 210(7), 210(13), 210(15), 210(5), 210(2), 210(4), 210(16) and 210(14)
respectively is a random assignment. For the initial arrangement 300B as shown
in figure 3B, the whole set of possible locations 210 is randomly determined, as is
the association of the symbols 'O', '1', '2', '3', '4', '5', '6', '7', '8', '9' with their
respective initial locations 210.

The initial arrangement 200A may be determined by the computer system
114, with data identifying (or specifying or defining) the initial arrangement 200A
being provided to, or retrieved by, the user input device from the other computer
system 114. This data may specify the whole of the initial arrangement 200A -
e.g. (a) the data may identify a respective location 210 (e.g. a coordinate or a
region) associated with, or assigned to, each of the symbols or (b) the data may
be in the form of an image depicting the symbols positioned at their respective
locations 210. Alternatively, this data may merely specify sufficient information to
enable the user input device to generate the initial arrangement 200A, e.g. a
seed value for the user input device to use in a random number generator.
Alternatively, the initial arrangement 200A may be determined by the user input
device independently of the computer system 114 - if the user input device is to
communicate with the computer system 114, then the user input device may
inform the computer system 114 of the initial arrangement 200A (e.g. by
providing data identifying the respective location 210 associated with, or assigned
to, each of the symbols).

At a step S404, the user input device obtains location data. The location
data identifies one or more alternate (or alternative) locations 210 at which a
symbol may be displayed. As will be described in more detail shortly, the location
data is used to modify the display (or arrangement) of the set of symbols in
response to the selection of one or more symbols by a user of the user input
device. The alternate locations 210 that are identified are to be used as new
locations 210 at which symbols are to be displayed, instead of displaying those
symbols at their current locations 210, when modifying the display of the set of symbols.

The alternate locations 210 may be predetermined; alternatively, the alternate locations 210 may be randomly or pseudo-randomly generated at least in part (e.g. based on a seed value) or they may be selected (potentially randomly) from a set of predetermined locations 210 (e.g. from a set of locations making up a predetermined configuration of locations, such as a grid). For the example shown in figure 2A, there is a grid or arrangement of predetermined possible locations 210, some of which are selected (randomly) as initial locations 210 for the symbols, and some of which are selected as alternate locations 210.

Preferably, the alternate locations 210 that are identified by the location data may correspond only to unoccupied locations 210, i.e. locations 210 to which no symbol is assigned in the initial configuration 200A. For example, in the initial configuration shown in figure 2A, the alternate locations 210 may be chosen (potentially at random) from the unoccupied locations 210(1), 210(3), 210(6), 210(8), 210(9) and 210(12). However, it will be appreciated that the alternate locations 210 that are identified by the location data may, additionally or alternatively, correspond to occupied locations 210, i.e. locations 210 to which a symbol has been assigned in the initial configuration 200A.

The location data may be obtained by retrieving the location data from a computer system on the network 112, such as computer system 114.

The location data may be obtained from the same source as the initial configuration 200A or a different source. As an example, the initial configuration 200A may be obtained from a computer system 114 on the network 112 and the location data may be obtained from either the same computer system 114 or a different computer system (not shown).

The location data may be generated by the user input device itself.

The location data may be generated based on a random or pseudo-random sequence. The location data may be generated based on a seed value,
such as a value that is retrieved from another computer system or a value that is
associated with the user that is performing the data entry, etc.

The location data to be used with a particular current data entry session
(or process) may be obtained in a single step, as illustrated in figure 4, that is to
say for any given data entry session the location data may be obtained only once
and identifies a sufficient number of alternate locations for the entire data entry
session. However, whilst figure 4 illustrates the location data being obtained in a
single step, it will be appreciated that the location data may be obtained in
multiple steps (or portions or batches). The location data may therefore identify a
number of alternate locations and additional location data identifying further
alternate locations may be obtained by further iterations of the step S404 (not
shown) in the data entry session. Where the location data is obtained in multiple
steps, additional location data might only be obtained as it is needed. As an
example, the location data may identify a single alternative location and
additional location data may be obtained every time the display (or arrangement)
of the plurality of symbols is required to be modified - thus, the step S404 may be
incorporated as part of a step S412 (to be described below).

The location data, or at least a first portion of the location data, may be
obtained at the same time as the initial configuration 200A is determined at the
step S402 (and the step S404 may, therefore, be viewed as forming a part of the
step S402). As an example, at the step S402, data may be received from
another computer system, such as computer system 114, on the network 112,
which specifies both the initial configuration 200A and the location data, or at
least a first portion of the location data.

Continuing the PIN entry example illustrated by figures 2A, 2B, 2C and 2D,
the location data that is obtained may identify locations 210(12), 210(8) and
210(3) as being alternate locations for displaying a symbol.

At a step S406, the user input device displays the symbols in the initial
arrangement 200A, each symbol being displayed at its respective initial location
At a step S408, a selection is received from the user. The selection corresponds to a location 210 at which one of the set of symbols is currently (i.e. at the point in time at which the selection is made) displayed.

Methods of selecting a location 210 have been described above (for example, using the keyboard 106 and cursor 202, or using a touch-sensitive display 108). In this way, the user has selected the symbol that is displayed at the selected location 210.

The selection may form part of a sequence of selections, with the processing of the method returning (or re-iterating) to this step S408 from a later step S412, discussed in further detail below, in order to receive subsequent selections in the sequence of selections from the user.

Continuing the PIN entry example illustrated by figures 2A, 2B, 2C and 2D, in order to enter the PIN '3463', the user selects the locations 210 at which the symbols '3', '4', '6' and '3' are displayed at the point in time at which the user makes those individual selections. Therefore, at a first iteration of the step S408 at which the set of symbols are displayed in an initial arrangement 200A, the user makes a first selection (illustrated via the cursor 202(1)), corresponding to location 210(13), where the symbol '3' is displayed. Then in subsequent iterations of the step S408, the user makes subsequent selections (illustrated via the cursors 202(2), 202(3) and 202(4)), based upon the subsequent displays (or arrangements) 200B, 200C and 200D of the set of symbols. The subsequent selections correspond to locations 210(15), 210(2) and 210(12), at which the symbols '4', '6' and '3' are displayed in the respective subsequent arrangements 200B, 200C and 200D. The selected locations 210(13), 210(15), 210(2) and 210(12) therefore correspond to the locations at which the symbols '3', '4', '6' and '3' were displayed at the time the selections were made.

In summary, at step S408, a selection, forming part of a sequence (or series or ordered list) of selections, is received from the user.

At a step S410, it is determined whether the sequence of selections (or data entry) to be received from the user is complete. If it is determined that the
sequence of selections to be received from the user is complete, then the processing will proceed to a step S414, which is discussed further below. If it is determined that the sequence of selections to be received from the user is not complete, then the processing will proceed to a step S412, which is discussed in further detail below, before returning back to the step S408 to receive a further selection from the user.

The user input device may provide a means (not shown in figures 2A, 2B, 2C, 2D, 3A or 3B) by which the user can indicate that the sequence of selections is complete. The determination that the sequence of selections to be received from the user is complete may therefore be made by identifying whether such an indication has been received from the user. As an example, the user input device might have a button labelled "enter" or "ok" and in response to the user pushing such a button will determine that the sequence of selections to be received from the user is complete.

The sequence of selections that is to be received may be of a pre-determined length (or size or number). The determination as to whether the sequence of selections to be received from the user is complete may therefore be achieved by determining whether the length of the sequence of selections made by the user so far is the same as the pre-determined length: if not, the sequence of selections is not complete; if so, then the sequence of selections is complete. As an example, in a PIN entry to access an application the PIN might have a pre-determined length (e.g. of four symbols), that is to say that any PIN must contain exactly that number (e.g. four) of symbols - therefore the step S410 may determine that the sequence of selections to be received from the user is complete once the user has made that number of selections. The pre-determined length may be contextual based on the type of data that is expected by a target for the data entry. As an example, a field into which the data is to be entered may specify a maximum input length, in which case the data input method may determine that the sequence of selections is complete if the current number of selections in the sequence of selections matches the maximum input
length. The pre-determined length may be specified by another computer system on the network 112, such as the computer system 114. As an example, whilst the mobile device 116 is interacting with the computer system 114, the computer system 114 may determine that the user should enter their PIN to authenticate their identity and may specify that the PIN has a pre-determined length of symbols (e.g. four symbols).

The determination that the sequence of selections to be received from the user is complete may be made by another computer system on the network 112, such as computer system 114. The user input device may provide an indication to the other computer system 114 every time a selection is received (or possibly, as discussed further below, may transmit each selection to the other computer system 114 without waiting for the entire sequence of selections to be received). The other computer system may then indicate to the user input device that the sequence of selections is complete.

A user input device which allows data entry of many different types of data (such as PINs, passwords, credit card numbers, etc) may make use of different means for determining whether the sequence of selections to be received from the user is complete, depending upon the context of the current data being entered. As an example, when the context of the data entry is the entry of a PIN, the data entry method might determine whether the sequence of selections is complete based on a pre-determined length method, whereas when entering a password, the user input device might display an "enter" button to allow the user to indicate when the sequence of selections is complete.

There are many ways in which it might be determined whether the sequence of selections to be received from the user is complete. It will be appreciated that other mechanisms for determining whether the sequence of selections by the user is now complete may be used at the step S410.

Returning to the PIN entry example illustrated in figures 2A, 2B, 2C and 2D, it may be predetermined that the PIN will be 4 digits long. Therefore, after the user makes their first selection, the step S410 will determine that the
sequence of selections is not complete and the processing will return or reiterate (after processing the step S412) to the step S408 in order to receive the second selection from the user. Similarly, the processing will return to the step S408 after receiving the second selection and after receiving the third selection to allow the user to make further selections. However, after the user makes their fourth selection, the step S410 will determine that the sequence of selections is complete, since the number of selections in the sequence of selections is the same as the pre-determined length (of 4 digits), and the processing will continue to the step S414, discussed below.

At the step S412, the display (or arrangement) of the plurality (or set) of symbols is modified according to the location data. Modifying the arrangement (or display) 200 of the set of symbols results in a subsequent (or new) arrangement 200B, 200C or 200D of the set of symbols being displayed to the user, upon which the user’s next selection, at the step S408, will be based. After the display is modified at the step S412, processing returns to the step S408, as discussed above, to receive another selection from the user using the new arrangement.

The new arrangement 200 is formed from the current arrangement 200 by modifying the location at which one of the set of symbols is displayed (also referred to in this specification as moving the symbol) so that that symbol is displayed in the new arrangement 200 at one of the alternate locations 210 identified by the location data instead of the location at which it was displayed in the current arrangement 200.

The display (or arrangement) of the set of symbols may be modified after each selection 202 is received from the user, as illustrated in figure 4. However, the arrangement of the set of symbols may be modified less frequently, in which case the step S412 may include a determination (not shown) as to whether the display of the set of symbols should be modified after the current selection has been received at the step S408.
The determination as to whether the display of the set of symbols should be modified may be made randomly. As an example, the display of the set of symbols may be modified after a random number of selections have been received.

The determination as to whether the display of the set of symbols should be modified may be based on a fixed number of selections being received. As an example, the display of the set of symbols may be modified after every second selection is received.

The determination as to whether the display of the set of symbols should be modified may be made with reference to the location data. The location data may indicate that the display of the set of symbols should be modified every time a certain number of selections have been received. As an example, the location data may indicate that the display of the set of symbols should be modified after every second selection. The location data may indicate points (or indexes) in the sequence of selections at which the display of the set of symbols should be modified. As an example, the location data may indicate that the display of the set of symbols should be modified after the second, fifth and tenth selections are received.

The determination of the alternate location to which one of the set of symbols is to be moved to (i.e. the alternate location at which the symbol is to be displayed at instead of its current location) is conducted with reference to the location data.

The alternate location 210 to which one of the symbols in the set of symbols is to be moved may be determined at random from the alternate locations identified by the location data.

The location data may identify an order in which the alternate locations are to be used. The alternate location 210 to which one of the symbols in the set of symbols is to be moved may then be determined by selecting the next alternate location 210 identified by the ordering.
The location data may associate each alternate location 210 with a particular point in the sequence of selections at which that alternate location 210 should be used to modify the display. In this case, the alternate location 210 to which one of the symbols in the set of symbols is to be moved is determined to be the alternate location 210 that is associated with the current point in the sequence of selections. As an example, the location data may specify that after the third selection, the display should be modified using alternate location 210(3), therefore after the user's third selection has been received, the display will be modified by moving one of the symbols of the set of symbols to be displayed at the alternate location 210(3).

The symbol that is to be moved to the alternate location may be identified in a number of ways.

The symbol that is to be moved may be identified randomly from the set of symbols.

The symbol that is to be moved may be the same symbol that is displayed at the location selected by the user in the previous step S408 - this is the embodiment illustrated in the sequence of arrangements shown in figures 2A, 2B, 2C and 2D. As an example, if the user's most recent selection corresponds to the location 210(13) at which the symbol '3' is displayed, the symbol '3' is the symbol that will be moved.

The symbol that is to be moved may be specified by the location data. As an example, the location data may specify that the first symbol to be moved is the symbol '5' and the second symbol to be moved is the symbol '9'. The location data may indicate a symbol that is to be used with each alternate location. As an example, the location data may specify that if the determined alternate location to which a symbol is to be moved is the alternate location 210(9), then the display is to be modified by moving symbol '1' to the alternate location 210(9).

Modifying the arrangement (or display) 200 of the set of symbols by moving the identified symbol to the determined alternate location 210 may be achieved in a number of ways.
The alternate location 210 may be unoccupied, with no symbol currently displayed at that location, in which case, the arrangement may be modified by changing the location at which the identified symbol is displayed (or moving the identified symbol) to the determined alternate location.

The alternate location may be occupied, with another symbol ('the other symbol') already displayed at that location, in which case, the arrangement may be modified by also moving the other symbol (in addition to moving the identified symbol to the determined location). The other symbol may be moved so that it is instead displayed at the location at which the identified/selected symbol was displayed prior to the modification, resulting in the locations 210 at which the symbols are displayed being swapped. The other symbol may be moved by making further reference to the location data to determine another alternate location 210 to which the other symbol may be moved. If this other alternate location 210 is also occupied, the process may be repeated for the symbol that is occupying the other alternate location 210. In this manner, multiple symbols may be moved, with symbols being swapped until an unoccupied alternate location has been determined.

Other methods of modifying the arrangement of the set of symbols may result in multiple symbols being moved in a single modification. Such methods may involve the identification and determination of multiple symbols and alternate locations using any combination of the methods discussed above. As an example, the location data may associate multiple alternate locations and symbols with a particular point in the sequence of selections to be received from the user. As a result, the display may be modified by moving each of those identified symbols to their respective alternate locations, possibly in combination with any of the methods of moving the symbols outlined above, such as by swapping the symbols with any symbols that are displayed at the alternate location.

The location 210 associated with the selection 202 that was received from the user in the step S408 may be added (e.g. appended) to the location data as
an additional alternate location. In this way, even if a limited number of alternate locations are originally provided, alternate locations can be provided for an indefinite length of input. As an example, if the location data originally identified a single unoccupied alternate location, with each selection made by the user, the symbol at the selected location could be moved to the alternate location, leaving the moved symbol's original location unoccupied and available to be used as the next alternate location for the symbol at the next selected location. Whilst this example specifies that the selected symbol is the symbol that is to be moved and the alternate location is empty, it will be appreciated that this is not necessary, and any of the other possibilities described above may be used instead.

There are many ways in which the arrangement (or display) 200 of the set of symbols may be modified using different ways of identifying symbols to move, the locations to which they are to be moved using the location data, and the manner in which they are to be moved. It will be appreciated that any such method may be used.

Continuing the PIN entry example illustrated by figures 2A, 2B, 2C and 2D, after receiving the first selection from the user, the initial arrangement 200A of the set of symbols is modified by changing the location of the symbol '3' which is at the selected location 210(13) so that it is instead displayed at the first of the alternate locations 210(12) identified by the location data retrieved at the step S404. In this manner, the subsequent arrangement 200B of the set of symbols is displayed to the user. Similarly, in response to the second symbol selection, the arrangement 200B is modified by moving the symbol '4' at the selected location 210(15) so that it is instead displayed at the second alternate location 210(8) identified by the location data. The subsequent arrangement 200C is therefore displayed to the user in response to the user's second selection. Finally, in response to the third symbol selection, the arrangement 200C is modified by moving the symbol '6' at the selected location 210(2) so that it is instead displayed at the third alternate location 210(3) identified by the location data. The subsequent arrangement 200D is therefore displayed to the user in response to
the user's third selection. In this manner, the user is displayed all four arrangements 200 of the set of symbols as he enters his PIN, with a different arrangement being used for each selection that the user makes.

This method of modifying the arrangement of the set of symbols provides many advantages.

The security of the data entry is greatly improved. The locations at which the symbols are displayed are disassociated from the meaning or natural ordering of the symbols. This means that an observer able to detect the locations selected by the user during the data entry process is not able to deduce any information about the actual data that was entered based on the pattern of the selected locations.

As an example, the first selection made by the user in the PIN entry example corresponded to the top left hand side of the data entry display, where one might expect to find a relatively high number such as a '7' on a normal PIN entry pad. An observer of such a selection on a normal PIN entry pad might deduce that the first digit of a user's PIN is '7'; however, clearly such a deduction would be invalid on a PIN entry pad utilizing an embodiment of the present invention.

Additionally, the modification to the current arrangement of the set of symbols to display a subsequent arrangement of the set of symbols in response to a selection received from the user provides a temporal disassociation between the locations at which the symbols are displayed and the meaning of the symbol. This means that even if the data contains multiple occurrences of the same symbol, such as the digit '3' in the PIN number '3463' entered in the PIN entry example, the user might never select the same location more than once. In the PIN entry example, the meaning of the selection of the location 210(13) at which the symbol '3' is displayed at the point in time that the first digit is entered is different from the meaning of that location at a later point in time, when the second digit '3' is selected by selecting the different location 210(12). Equally,
even if the data did not contain any repeat occurrences of any symbol, the data entry method might result in the user selecting the same location multiple times.

Whilst the data entry method provides an increase in security, the increase in security is provided in a manner which minimises confusion and inconvenience to the user and therefore allows the user to enter the data efficiently. The subsequent arrangements of the set of symbols that are displayed to the user after selections made by the user are formed based on the current arrangement of the set of symbols by modifying the location at which one or more of the symbols is displayed as discussed above. The location of the majority of the symbols is therefore unchanged between the current arrangement and the subsequent arrangement with only a subset of the symbols changing location. This reduces the cognitive burden placed on the user in assessing the subsequent layout and learning the new locations at which the symbols are displayed, thereby allowing him to proceed with his next selection quicker. As an example, when the first symbol selection, corresponding to the symbol '3', is made from the initial arrangement 202A of the set of symbols in the PIN entry example, the location of the user's next selection, corresponding to the symbol '4', is unchanged between the initial arrangement 202A that the user has learnt and the subsequent arrangement 202B from which the user has to select it. The user therefore can select the next symbol quickly, as it is where he expects it to be. This effect may be particularly prevalent in embodiments where small numbers of symbols are moved, particularly where the symbol that is moved is the one that was selected by the user, since this symbol has the user's current focus and its movement will be most noticeable, as illustrated in figures 2A, 2B, 2C and 2D. This effect may be further enhanced by providing visual cues to the user of the changes that are made between the current arrangement and a subsequent arrangement, such as temporarily flashing or highlighting the symbols that have been moved between the two arrangements, or displaying arrows or other cues to highlight the movement (or modification) to the user.
Furthermore, the security and reduction in user confusion and inconvenience that is provided by these data entry methods is achieved whilst minimizing the memory and/or bandwidth required by the system. The amount of data required to represent the mapping of an entire arrangement of the set of symbols, is comparatively large compared to the amount of data required to represent an alternative location at which one of the symbols may be displayed when modifying the arrangement. The data required to specify each of the arrangements 200A, 200B, 200C and 200D as separate individual mappings of the set of symbols is therefore a lot larger than those required to specify each of the arrangements 200A, 200B, 200C and 200D using a mapping for the initial arrangement and location data identifying alternative locations 210(12), 210(8) and 210(6) to which a symbol may be moved. 

At a step S414, the sequence of selections that were received from the user is converted to a sequence of symbols.

As discussed above, each selection of the sequence of selections that is received from the user corresponds to a location 210 (hereafter referred to as the selected location) at which one of the symbols was displayed when the selection was made. Converting the sequence of selections to symbols involves identifying, for each selection in the sequence, which symbol was displayed at the selected location at the time the selection was made. The identification of the symbol that was displayed at the selected location at the time the selection was made may be achieved using the initial arrangement 200A (which specifies the initial locations 210 associated with the set of symbols), the location data and the sequence of selections itself. The initial arrangement 200A is used to determine the initial association of the set of symbols with locations 210, whilst the subsequent arrangements of the set of symbols are formed from the current arrangement using the location data and, in some embodiments, the selections themselves, as discussed above in relation to the step S412.

The conversion of the sequence of selections to the sequence of symbols may be done by the user input device. The sequence of symbols may then be
used by the user input device itself. As an example, the user input device may use a data entry method according to an embodiment of the invention to allow the user to enter a PIN to unlock the device, in which case the conversion and use of the entered data may be entirely local to the user input device. The sequence of symbols may be transmitted to another computer system on the network 112, such as computer system 114, for use by that computer system. As an example, a user may be interacting with an application on the other computer system 114 using the user input device and may have to enter a password in order to authenticate with the application on the other computer system 114. The user input device may therefore allow the user to enter the password using a data entry method according to an embodiment of the invention and convert the sequence of selections to a sequence of symbols before transmitting the sequence of symbols to the other computer system to allow the other computer system to authenticate the user.

The conversion of the sequence of selections may take place at another computer system on the network 112, such as computer system 114. The sequence of selections is therefore transmitted to the other computer system 114 (or retrieved by the other computer system 114) to be converted using the initial arrangement 200A and the location data.

The other computer system 114 may already have access to the initial arrangement 200A and/or the location data. As an example, the initial arrangement 200A and/or location data may have been sent to the user input device at the steps S402 and/or S404 by the other computer 114, in which case the other computer 114 may retain a copy of the initial arrangement 200A and/or location data for use in converting the sequence of selections to a sequence of symbols.

The other computer system 114 may generate the initial arrangement 200A and/or the location data in order to convert the sequence of selections to the sequence of symbols. As an example, the other computer system 114 may have indicated to the user input device a seed value for the generation of the
initial arrangement 200A and/or location data at the steps S402 and/or S404 by the user input device, in which case the other computer system 114 may also generate the initial arrangement 200A and/or location data using the same seed value.

The other computer system may not initially have access to the initial arrangement 200A and/or the location data. The initial arrangement 200A and/or location data (or data which enables their generation, such as a seed value) may by transmitted to the other computer system 114 by the user input device (or may be retrieved from the user input device by the other computer system 114). As an example, the initial arrangement 200A and/or the location data may have been generated randomly or pseudo-randomly by the user input device, in which case the initial arrangement 200A and the location data may be transmitted to the other computer system 114 to enable the other computer system 114 to convert the sequence of selections into a sequence of symbols. Similarly, some embodiments involve the random generation of other components used to modify the arrangements, such as the random selection of which symbol of the set of symbols is to be moved to generate a subsequent arrangement or the random selection of an alternate location. These other components (or data which enables their generation, such as a seed value) may also be transmitted to the other computer system 114 by the user input device (or may be retrieved from the user input device by the other computer system 114), to allow the other computer system to convert the sequence of selections into a sequence of symbols.

Whilst the step S414 is illustrated as a single step, with the entire sequence of selections being converted at once, it will be appreciated that the step S414 could occur more than once, with a sub-set of the sequence of selections being converted each time the step S414 occurs. As an example, each individual selection might be converted to its associated symbol as soon as the selection is made, before any further selections are made.
Returning to the example of the user entering a PIN, illustrated in figures 2A, 2B, 2C and 2D, the sequence of selections received from the user consists of 4 selections indicated via cursors 202(1), 202(2), 202(3) and 202(4) in figures 2A, 2B, 2C and 2D. The first selection corresponds to the location 210(13) and was made based on the initial arrangement 200A of the plurality of symbols.

Therefore, the first selection can be converted into the symbol '3', since this is the symbol that was displayed at the location 210(13) in the initial arrangement 200A of the plurality of symbols. Similarly, the subsequent selections correspond to the locations 210(15), 210(2) and 210(12) respectively and were made based on the arrangements 200B, 200C and 200D. These selections can therefore be converted into the symbols '4', '6' and '3' respectively. By following this process the sequence of selections made by the user can be converted into the sequence of symbols '3463', which is the PIN entered by the user.

In summary, at step S414, the sequence of selections that were received from the user is converted to a sequence of symbols. The conversion makes use of the initial arrangement 200A and the location data to identify the symbols that were displayed at each of the selected locations at the time the selection was made. There are therefore three elements of data that are needed to obtain the actual sequence of symbols input by the user: the sequence of selections, the initial arrangement 200A and the location data (although one or both of the initial arrangement 200A and the location data may be generated from one or more seed values, e.g. for a random number generator). The security of the user's input data is therefore also improved since in order to obtain the data input by the user, one would need to obtain all three elements of the data input session, namely, the sequence of selections, the initial arrangement 200A and the location data. Clearly each element of the data input session may be retrieved or communicated via a different channel, making it harder for someone with visibility of any one of the channels to obtain the user's input data.

As an example, a user input device using the secure data entry method may receive a sequence of selections from a user and transmit this sequence of
selections to another computer system on the network 112, such as computer system 114, to be converted to a sequence of symbols to be used as input for an application on that computer system. The user input device may display an initial arrangement of the plurality of symbols based on mapping data which is retrieved from a local memory based on the identity of the user. The user input device may then display subsequent arrangements of the plurality of symbols based on location data which is generated locally from a seed value retrieved from the other computer system 114. The other computer system 114, may then receive the sequence of selections from the user input device. The other computer system 114 may then also retrieve the mapping data from its own local memory based on the identity of the user and may also generate the location data based on the seed value that the other computer system sent to the user input device. The other computer system 114 is therefore able to convert the sequence of selections into a sequence of values based on this mapping and location data.

However, someone able to monitor the network 112 and observe the sequence of selections that were sent to the other computer system 114 would not be enabled to convert the sequence of selections into a sequence of values (even in the absence of any other form of protection, such as encryption) as they would not have access to the mapping data or the location data. The other person is therefore unable to retrieve the user's securely inputted data.

It will be appreciated that the methods described have been shown as individual steps carried out in a specific order. However, the skilled person will appreciate that these steps may be combined or carried out in a different order whilst still achieving the desired result.

It will be appreciated that embodiments of the invention may be implemented using a variety of different information processing systems. In particular, although the figures and the discussion thereof provide an exemplary computing system and methods, these are presented merely to provide a useful reference in discussing various aspects of the invention. Embodiments of the invention may be carried out on any suitable data processing device, such as a
personal computer, laptop, personal digital assistant, mobile telephone, set top box, television, server computer, etc. Of course, the description of the systems and methods has been simplified for purposes of discussion, and they are just one of many different types of system and method that may be used for embodiments of the invention. It will be appreciated that the boundaries between logic blocks are merely illustrative and that alternative embodiments may merge logic blocks or elements, or may impose an alternate decomposition of functionality upon various logic blocks or elements.

It will be appreciated that the above-mentioned functionality and modules may be implemented as hardware and/or software. For example, the above-mentioned modules may be implemented as one or more software components for execution by a processor of the system. Alternatively, the above-mentioned modules may be implemented as hardware, such as on one or more field-programmable-gate-arrays (FPGAs), and/or one or more application-specific-integrated-circuits (ASICs), and/or one or more digital-signal-processors (DSPs), and/or other hardware arrangements.

It will be appreciated that, insofar as embodiments of the invention are implemented by a computer program, then a storage medium and a transmission medium carrying the computer program form aspects of the invention. The computer program may have one or more program instructions, or program code, which, when executed by a computer carries out an embodiment of the invention. The term "program," as used herein, may be a sequence of instructions designed for execution on a computer system, and may include a subroutine, a function, a procedure, an object method, an object implementation, an executable application, an applet, a servlet, source code, object code, a shared library, a dynamic linked library, and/or other sequences of instructions designed for execution on a computer system. The storage medium may be a magnetic disc (such as a hard drive or a floppy disc), an optical disc (such as a CD-ROM, a DVD-ROM or a BluRay disc), or a memory (such as a ROM, a RAM, EEPROM, EPROM, Flash memory or a portable/removable memory device), etc. The
transmission medium may be a communications signal, a data broadcast, a communications link between two or more computers, etc.
CLAIMS

1. A method of obtaining an input from a user using a user input device, the method comprising:
   obtaining location data for identifying one or more alternate locations for displaying a symbol;
   displaying a plurality of symbols on a display of the user input device, each symbol being displayed at a respective initial location on the display;
   receiving a sequence of selections from the user, each selection corresponding to a location at which one of the plurality of symbols is currently displayed; and
   in response to one or more of the selections, modifying the location at which one of the plurality of symbols is displayed so that the symbol is instead displayed at one of the alternate locations.

2. The method of claim 1, wherein said modifying modifies the location at which two or more of the plurality of symbols are displayed so that said two or more symbols are instead displayed at respective ones of the alternate locations.

3. The method of any one of the preceding claims, wherein the location data provide an ordering for the alternate locations, and wherein said modifying selects a next alternate location according to said ordering for use in modifying the location at which said one of the plurality of symbols is displayed.

4. The method of any one of the preceding claims, wherein modifying the location at which one of the plurality of symbols is displayed in response to a selection of the one or more selections comprises modifying the location at which the symbol that is currently displayed at the location selected by that selection is displayed.
5. The method of any one of the preceding claims, wherein the alternate locations correspond to locations on the display of the user input device at which no symbol is initially displayed.

6. The method of any one of claims 1-4, wherein modifying the location at which one of the plurality of symbols is displayed so that the symbol is instead displayed at one of the alternate locations comprises determining whether a second symbol is currently displayed at said one of the alternate locations, and, if so, modifying the location at which the second symbol is displayed so that the second symbol is instead displayed at the location at which said one of the plurality of symbols is displayed.

7. The method of any one of claims 1-4, wherein modifying the location at which one of the plurality of symbols is displayed so that the symbol is instead displayed at one of the alternate locations comprises determining whether a second symbol is currently displayed at said one of the alternate locations, and, if so, modifying the location at which the second symbol is displayed so that the second symbol is instead displayed at a further one of the alternate locations.

8. The method of any one of the preceding claims, wherein modifying the location at which one of the plurality of symbols is displayed so that the symbol is instead displayed at one of the alternate locations comprises setting the location at which said one of the plurality of symbols is currently displayed to be an additional alternate location.

9. The method of any one of the preceding claims, further comprising displaying a visual cue illustrating the modification.
10. The method of any one of the preceding claims, comprising receiving, at the user input device, the location data together with position data for identifying the initial locations.

11. A method of receiving input from a user of a user input device, the method comprising:
   obtaining position data for identifying, for each symbol of a plurality of symbols, a respective initial location for displaying that symbol on a display of the user input device;
   obtaining location data for identifying one or more alternate locations for displaying a symbol on the display; and
   receiving, from the user input device, a sequence of selections representing the input from the user of the user input device, each selection corresponding to a location at which one of a plurality of symbols was displayed on the display of the user input device when the selection was made;
   wherein the user input device is configured to obtain said sequence of selections by carrying out the method of any one of claims 1-10 based on said initial locations and said alternate locations.

12. The method of any one of the preceding claims, further comprising generating a sequence of symbols by determining, for each selection in the sequence of selections, which symbol was displayed at the corresponding location when the selection was made.

13. The method of any one of the preceding claims, wherein the location data comprises a seed value and the method comprises randomly determining the one or more alternate locations based on the seed value.

14. The method of any one of the preceding claims, comprising randomly determining the initial locations based on a seed value.
15. An apparatus arranged to carry out a method according to any one of the preceding claims.

16. A computer program which, when executed by a processor, causes the processor to carry out a method according to any one of claims 1 to 14.

17. A computer readable medium storing a computer program according to claim 16.
FIGURE 1
S402
Determine initial arrangement to be used to initially display the plurality of symbols

S404
Obtain location data identifying one or more alternate locations for displaying a symbol

S406
Display the symbols at their respective initial locations according to the arrangement

S408
Receive from the user, a selection corresponding to a location at which a symbol is currently displayed

S412
Modify the display of the plurality of symbols according to the location data

S410
Is the sequence of selections to be received from the user complete?

S414
Convert the sequence of selections into a sequence of symbols

FIGURE 4
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**

**INV. G06F21/83**

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 practicable, search terms used)

EPO-Internal, WPI Data

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>GB 2 457 733 A (MOBANK LTD [GB]) 26 August 2009 (2009-08-26) figure 5 page 21, line 13 - line 16 page 22, line 13 - line 20 page 25, line 7 - line 11 page 29, line 1 - line 13 page 25, line 13 - line 14</td>
<td>1-17</td>
</tr>
</tbody>
</table>

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

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "Z" document member of the same patent family

**Date of the actual completion of the international search**

23 September 2013

**Date of mailing of the international search report**

27/09/2013

**Name and mailing address of the ISA**

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

**Authorized officer**

Vinck, Bart
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>GB 2457733 A</td>
<td>26-08-2009</td>
<td>EP 2260432 Al</td>
</tr>
<tr>
<td>GB 2457733 A</td>
<td></td>
<td>GB 2457733 A</td>
</tr>
<tr>
<td>US 2011191856 A</td>
<td></td>
<td>US 2011191856 Al</td>
</tr>
<tr>
<td>WO 2009106800 Al</td>
<td></td>
<td>WO 2009106800 Al</td>
</tr>
<tr>
<td>US 2010109920 Al</td>
<td>06-05-2010</td>
<td>US 2010109920 Al</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2010053594 Al</td>
</tr>
<tr>
<td>US 2002188872 Al</td>
<td>12-12-2002</td>
<td>US 2002188872 Al</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 02100016 Al</td>
</tr>
</tbody>
</table>