Appeal Decision

Appeal No. 2021-5438

Appellant	LICENTIA GROUP LIMITED
Patent Attorney	KIKUCHI, Toru
Patent Attorney	KIKUCHI, Shinichi
Patent Attorney	MATSUMOTO, Hidetoshi
Appellant	MYPINPAD LIMITED
Patent Attorney	KIKUCHI, Toru
Patent Attorney	KIKUCHI, Shinichi
Patent Attorney	MATSUMOTO, Hidetoshi

The case of appeal against the examiner's decision of refusal of Japanese Patent Application No. 2017-561755, entitled "AUTHENTICATION METHOD AND SYSTEM" (International Publication No. WO 2016/189322 published on December 1, 2016, and National Publication of International Patent Application No. 2018-527639 published on September 20, 2018), has resulted in the following appeal decision.

Conclusion

The appeal of the case was groundless.

Reasons

Conclusion

The appeal of the case was groundless.

Reason

No. 1 History of the procedures

The application according to the request for appeal (hereinafter, referred to as "the present application") is a patent application whose international application date is May 27, 2016 (priority claim under the Paris Convention accepted by the foreign agency: May 27, 2015, UK, May 27, 2015, UK, November 24, 2015, UK, November 24, 2015, UK), and the details of the procedure are as follows.

January 26, 2018 : Submission of translation
April 27, 2020 : Notification of reasons for refusal
August 11, 2020 : Submission of written opinion and written amendment
December 21, 2020 : Decision of refusal
April 27, 2021 : Submission of written request for appeal and written amendment

No. 2 Invention

The inventions according to Claims 1 to 17 of the present application are specified by the matters recited in Claims 1 to 17 in the scope of claims amended in the written amendment made on April 27, 2021, and the invention according to Claim 1 (hereinafter referred to as "Invention") is an invention as follows. Note that the symbols "A" to "F" are added in the body, and each component is referred to as "component A" or the like.

"[Claim 1] F An authentication method comprising:

A presenting a keypad image on an operable keypad within a display zone of a screen associated with an electronic device;

B wherein the keypad image and/or the operable keypad are generated using at least one scrambled keypad layout locally generated on the electronic device;

C storing an encoded version of an identifier input to the electronic device by a user operating the operable keypad via the keypad image;

D sending the encoded version of the identifier to a remote computing resource; and

E sending at least one scrambled keypad layout to the remote computing resource to decode the encoded version of the identifier."

No. 3 Reason for refusal in the examiner's decision

The reason for refusal in the examiner's decision is that the inventions according to Claims 1 to 17 of the present application shall not be granted a patent under the provision of Article 29(2) of the Patent Act for the reason that the claimed invention(s) could have easily been made by persons who have common knowledge in the technical field to which the claimed invention(s) pertains prior to the filing of the patent application, on the basis of the invention described in the Cited Document 1 and the matters described in the Cited

Documents 2-5 listed below, which had been distributed in Japan or a foreign country or made available to the public through electric telecommunication lines before the priority claim date of the present application (hereinafter referred to as the "priority date").
Note
Cited Document 1: International Publication No. 2014/013252
Cited Document 2: United States Patent Application Publication No. 2014/0324708A1
Cited Document 3: JP 2008-506198A
Cited Document 4: JP 2006-309417A
Cited Document 5: JP 2000-165378A

Here, it is assumed that Invention could have easily been made by a person skilled in the art based on the invention described in Cited Document 1 and the matter described in Cited Document 2.

No. 4 Cited Documents
1 Description of Cited Document 1

International Publication No. WO 2014/013252 (hereinafter referred to as "Cited Document 1") cited in the reason for refusal in the examiner's decision describes the following matters together with the drawings (underlines are added by the body for emphasis, and "..." indicates an omitted part).

A "This invention relates generally to the field of user authentication, and more particularly to the field of PIN-based verification. The invention is suited for use in situations where a user is required to enter a code, such as a Personal Identification Number (PIN), which is validated prior to completing an operation. The operation might be any type of operation." (Page 1, lines 3-6)

B "According to a first aspect of the invention, there may be provided a computer-implemented verification method comprising the step of:

enabling a user to input an identifier into an electronic device having:

i) a screen; and

ii) a keypad operable within a keypad zone of the screen;

by operating at least one key of the keypad via an image of at least part of a scrambled keypad which is displayed at least partially within the keypad zone.

The image may be referred to as a 'scrambled keypad image' for ease of reference.

. . .

The scrambled keypad image is not a keypad per se because it is devoid of any functionality. It is merely a representation of a grid of keys. Touching, clicking on or otherwise selecting any 'key' depicted in the image does not, in and of itself, produce any effect or generate an input.

However, it should be noted that the scrambled keypad image may sometimes be referred to as a 'keypad' 'scrambled keypad' or an Overlying keypad' purely for ease of reference because in use it appears to function as a keypad. Areas of the image may be referred to as 'keys', again only for ease of reference because this is what the user appears to see and use. However, it should be remembered that this is not actually the case, and that the image is not a keypad in reality.

The invention may enable the user to enter his identifier via the same device component that is used to display the scrambled keypad image (the screen). Phrased another way, the screen may serve as both the output (display) device for the scrambled keypad image and the input device via which the user's identifier may be entered. This contrasts with any prior art disclosure wherein the keypad is displayed on one device component (e.g. screen) and the user's input is received via another device component (e.g. keyboard).

An advantage of this feature is that it may enable the user's input from the image to be mapped to the electronic keypad which may be at least partially hidden from the user's view such that the user's input is automatically encoded upon entry by the user. The input is automatically encoded in the sense that the electronic device may not need to convert, encode or in any way process the user's input. The keypad may be generated by a procedure call executed on the electronic device. The operable, electronic keypad may be referred to as a 'reference' or 'underlying' keypad for ease of reference.

Preferably, the user's operation of the keypad key via the image generates an encoded version of the user's intended input. Preferably, the image is displayed within the keypad zone such that as the user touches, clicks on or otherwise identifies a location within the image, an operable keypad key at that location is activated to provide an encoded version of the user's input.

. . .

Thus, in one sense the invention may be viewed as enabling a scrambled keypad image to be 'superimposed' over an 'underlying' keypad such that when the user enters his input

via the overlaid scrambled keypad image it is encoded in accordance with the layout of the underlying (preferably unseen) keypad.

The 'underlying' keypad may be viewed as an object generated and residing in the device's volatile memory at run-time to provide a model of a conventional mechanical keypad.

Thus, the invention provides the advantage that the user's 'real' identifier is never stored within the device and is not transmitted for verification. Therefore, the user's identifier cannot be derived by any potential interceptor without knowledge of the mapping between the overlaid image and underlying, functional keypad. Preferably, the mapping between the overlaid image and underlying keypad is not stored in the electronic device, or derivable by the electronic device. The mapping (or correlation) between the positions of the two sets of 'keys' may be stored on a server remote from the electronic device." (Page 8, line 26 - Page 11, line 28)

C "Preferably, the scrambled keypad image may be sent from a remotely located computer- based resource to the electronic device. The resource may be a server. Thus, the scrambled keypad image may not be generated on the electronic device. A version of the scrambled keypad image may be stored on the server. The version may be a record of the order of the symbols (keys) in the scrambled keypad image.

The keypad zone may be a defined area or portion of the screen. Thus, the keypad zone may occupy the entire screen area or a portion of the screen. The scrambled keypad image may be displayed such that it covers the keypad zone completely, exactly or partially. Preferably, the underlying keypad is at least partially hidden from view so that the user is not able to see at least some of the keys of the keypad.

The identifier may be a Personal Identification Code. It may be a PIN (Personal Identification Number). It may comprise any number, type or combination of symbols or indicia (as explained above). The identifier may have been pre-selected by the user prior to executing the presently claimed method. The identifier may be stored remotely from the electronic device e.g. on a server. The scrambled keypad image and/or keypad may comprise numeric digits, alphabetical characters, punctuation, symbols or any other indicia, or a combination thereof. One or more symbols may be associated with each key.

Preferably, the user may be able to select a plurality of keys in the scrambled keypad

image to input an identifier comprising more than one symbol.

The scrambled keypad image may be scrambled with respect to a reference keypad. The keypad image may depict a block or grid comprising a plurality of adjacent keys. It may be 'scrambled' in the sense that the symbols on the keys are not in sequential order and/or not in the order which one would expect, perhaps with reference to the reference keypad. The scrambling may be in accordance with a random generation process, or a process that approximates to a random process. The reference keypad may be the keypad operable within the keypad zone, or a default keypad associated as standard with a make, model, type of electronic device.

Thus, the same indicia may be present in both the underlying keypad and the scrambled keypad image but they are provided in different positions. Put yet another way, the order of the keys in the reference keypad is different from that of the scrambled image. The scrambled keypad image may provide the same 'look and feel' as the default keypad associated with the electronic device, but with the keys in different relative positions.

The respective positions of one, some or all key(s) in the scrambled keypad image may be different from the position of the same key(s) in the underlying keypad.

The user may operate the keys of the underlying keypad via the scrambled keypad image by interacting with the keys displayed on the screen. For example, the user's input may be entered by the user touching the screen (with a finger or other device) or by selecting the desired key(s) using a pointing device such as a mouse or tracker ball. Other selection methods may be used to similar effect, thus falling within the scope of the invention.

. . .

Preferably, the scrambled keypad image is received by the electronic device from a computer-based resource (e.g. a server) located remotely from the electronic device. It may be sent to the electronic device from the server in respect to a request for an image, the request being sent from the device to the server. The scrambled keypad image may be generated by the server.

Preferably, the scrambled keypad image is pre-generated. In one embodiment this may mean that it is generated prior to, not in response to, the request from the electronic device. The image may be generated prior to execution of the verification method.

The encoded version of the user's input (identifier) may be sent from the electronic device to a remote computer-based resource. This resource may be a server. Preferably, the server receives the encoded version of the user's input and processes it. The processing may provide a decoded version of the user's inputted identifier.

Thus, the user's 'real' identifier may not be transmitted. Only the encoded version may be transmitted, which may be meaningless to an unauthorised party who does not know the mapping between the the keys in the scrambled keypad image and the keys in the underlying keypad.

The decoding may be performed using a stored version or form of the scrambled keypad image. The stored version or form of the configuration of the keys may be a filename. The decoding step may provide a decoded version of the user's input. Thus, the user's 'real' identifier may be generated by translating each symbol in the encoded version into its corresponding counterpart in the scrambled keypad image.

The user's decoded input may be compared with a stored version of the identifier. The user's input may be deemed to be correct if the input matches the stored identifier." (Page 11, line 30 - Page 14, line 22)

D "Pin Pad Production

The 'PIN Pad Production Program' 6 is responsible for generating all of the scrambled keypad images 3 used throughout the system. An overview of this aspect of the invention is shown in Figure 5.

If simply randomly scrambled keypads are used, there is a risk that one or more keys may not be positionally scrambled. This could resort in one or more keys of the users input PIN corresponding positionally on the standard and scrambled PIN. This is not ideal.

Consequently, during PIN pad (image) generation, scrambled key pad images that would have one or more keys positionally corresponding to the standard keypad are discarded. The PIN pad production is therefore preferably not purely random, but is subjected to a selection process to select/discard according to a specific criteria.

The PIN pad (image) generation takes place in a secure environment, typically complaint with payment card industry data security standard. The output resolution and file type

must be initially set up before use on a particular target device 1 (in this case the type of mobile phone). This ensures that outputted images are generated to the optimum resolution for that device e.g. 256 x 184.

A master 'Background Image' 7 is then selected which matches the resolution as set above, and a 'Permutations File' 5 selected containing all the required permutations of digits (keys) for the final keypad images. In one implementation, this file 5 must be a comma separated text file with each permutation on a new line. However, a variety of implementations may be devised to the same effect. For example, each permutation could be separated by a # or *.

The 'Permutations File' 5 is then merged with the 'Background Image' 7 using the user's selection of Font Type, Size and Colour to produce the completed keypad image 3. The completed keypad image 3 is then optimized and reduced in size to be as small as possible for optimum transmission speed." (Page 24, line 25 - Page 25, line 24)

E "It should be noted that in certain alternative embodiments, 12 smaller key pictures (one for each number or hotspot) may be provided. The phone or other device may be arranged to to select a random number and rearrange the individual pictures into a 3x4 array (and thus making up a virtual keypad on demand). However, such embodiments present potential security loopholes and may provide several access points for malware to obtain the user' s PIN (as the handset/device would have to transmit the random number and thus the order of the PIN pad back to the server). Therefore, such an embodiment is suitable for applications where required security levels are somewhat relaxed." (Page 33, lines 6-13)

F "Additional PinPad Encryption

In order to further enhance the security of the system, the invention may employ one or more techniques for making it more difficult for an unauthorised party to figure out, discern or calculate the mapping between the displayed keypad image (i.e. the one that the user uses to enter his PIN) and the underlying keypad.

For example, if the user has selected a PIN which contains the same digit more than once (e.g. 1223) this may make it easier to compute the correlation between the input and the 'underlying' keypad.

One possible approach to overcoming this could be to create more than one underlying keypad. For example, a virtual keypad could be generated for each key press. An example is given below.

Figure 16a shows a scrambled keypad image, and Figure 16b shows an 'underlying' keypad. If the user's PIN is 1111 then the encoded PIN sent back to the server would be 9999. This provides a potential hacker with a starting point for an attempt at calculating or guessing the user's PIN.

However, if 4 different 'underlying' keypads are used instead of one, this problem is overcome. Thus, a sequence of digits can be sent to the target device (e.g. terminal, phone, PC) and the sequence is used by the target device to form the keypad. For the keypad in Figure 16b, the sequence would be. 3156790482. Using this approach, it is possible to generate a new keypad for each required key press.

Thus, the top pin pad as per Figure 16a is sent to the target device as an image, in accordance with the description set out above. Then, 4 numeric sequences are sent for the creation of the underlying keypad e.g. 3156790482, 0746189352, 0347156289, 2581673904. This produces the keypads shown in figures 16b to 16e.

Suppose now that the user's input is 1111. Instead of 9999 being produced, the code 9857 is produced and sent back to the server for decryption. As the server 'knows' which scrambled keypad image was sent, and which sequences of digits, the resulting encoded PIN appears to be much more random and is therefore much harder to decipher by an interceptor. The decryption process at the server end remains as set out above." (Page 35, line 27 - Page 35, line 27)

G "FIG.5

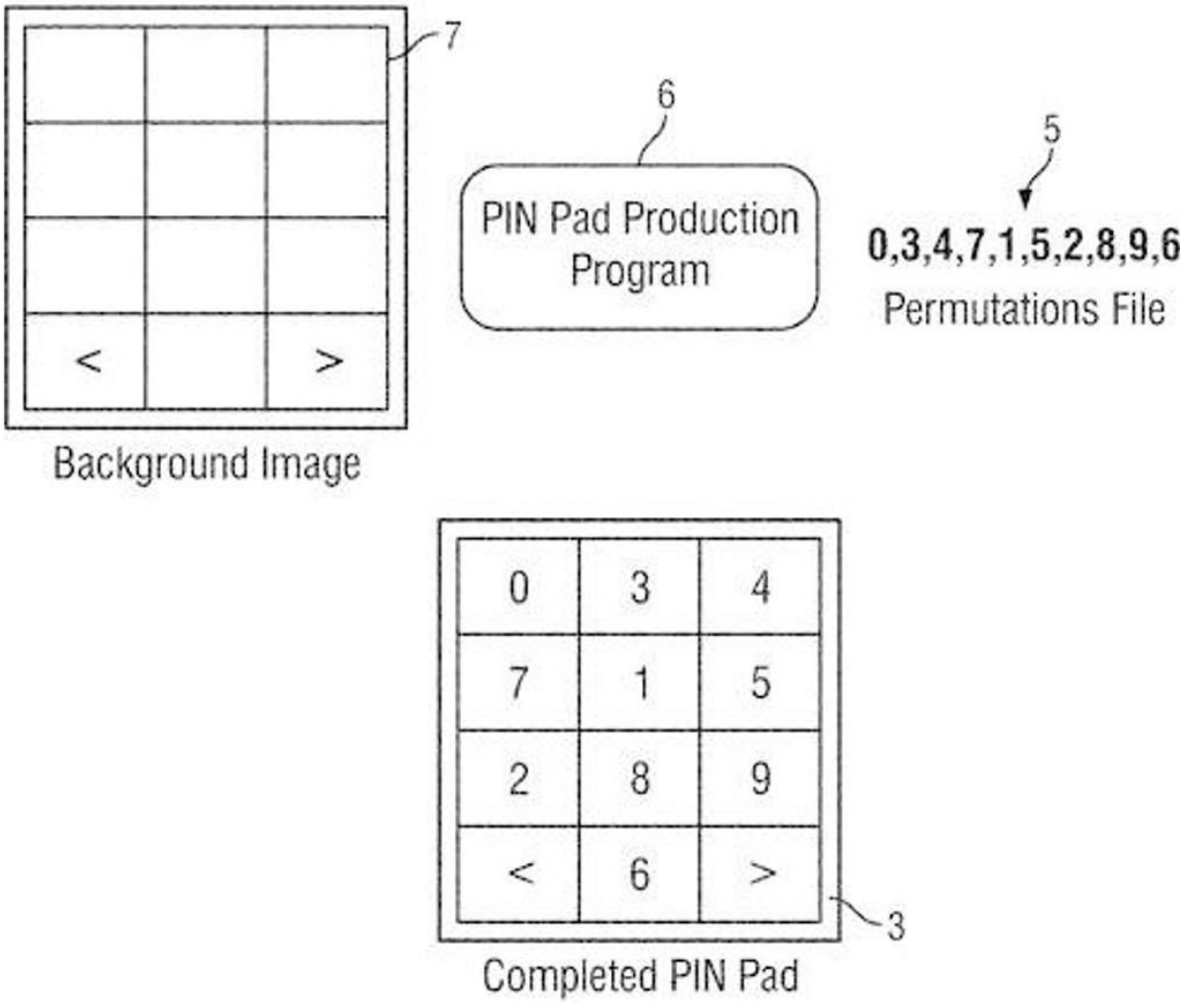
7
6
5
PIN Pad Production Program
0,3,4,7,1,5,2,8,9,6
Permutations File
<
>
Background Image
0
3
4
7
1
5
2
8
9
<
6
>
3
Completed PIN Pad

FIG. 5

"

H "FIG.16

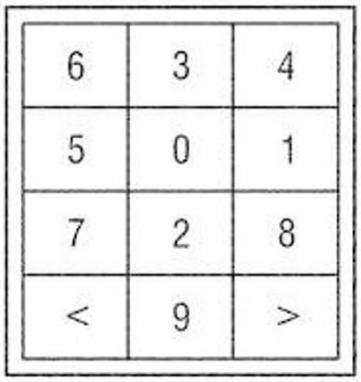

FIG. 16A

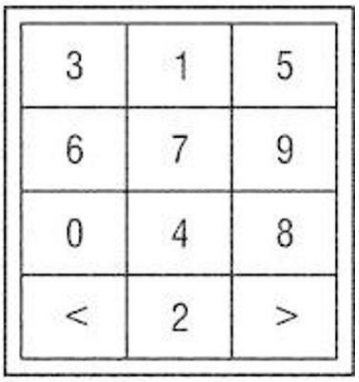

FIG. 16B

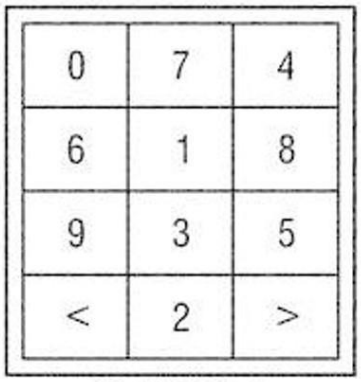

FIG. 16C

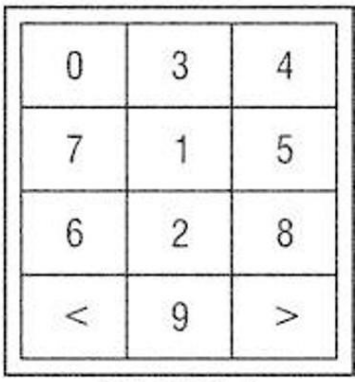

FIG. 16D

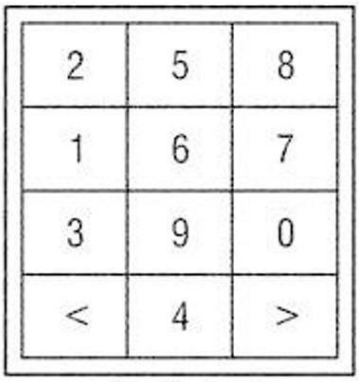

FIG. 16E

"

2 Cited Invention

A According to the above A of 1, Cited Document 1 describes "PIN-based verification" related to the field of user authentication.

B According to the above B of 1, Cited Document 1 describes the "verification method" including "the step of enabling a user to input an identifier into an electronic device" having "a keypad operable within a keypad zone of the screen", and the step is performed "by operating a key of the keypad" via "a scrambled keypad image" "which is displayed at least partially within the keypad zone".

Here, the "scrambled keypad image" enables the user's input from the image to be mapped to the keypad, the scrambled keypad image is "superimposed" over an "underlying" keypad such that the user's input via the "scrambled keypad image" is encoded in accordance with the layout of the underlying keypad, and "the user's operation of the keypad via the image generates an encoded version of the user's intended input."

Therefore, it can be said that Cited Document 1 describes an electronic device used for the "verification method of the identifier input by the user" includes "a keypad operable within a keypad zone of the screen of the electronic device" and "a scrambled keypad image displayed in the keypad zone", in which "the user's operation of the keypad via the scrambled keypad image generates an encoded version of the user's intended input."

C According to the above C of 1, Cited Document 1 describes that the "scrambled keypad image" is generated by "a server that is a computer-based resource located remotely" and is sent to the electronic device and the position of a key in "the scrambled keypad image" is different from the position of the same key in the operable keypad.

Further, Cited Document 1 describes that the user selects a plurality of keys in the "scrambled keypad image" and inputs a PIN used as an identifier, the encoded version of the input PIN is sent from the electronic device to the server, and the server processes the PIN to obtain the decoded version of the PIN as the identifier.

Therefore, Cited Document 1 describes that the "PIN" is used as an identifier of a user, that "the scrambled keypad image is sent to an electronic device from a server that is a computer-based resource located remotely", and that "an encoded version of the PIN is sent from the electronic device to the server, and the encoded version of the PIN is decoded in the server."

D According to the above D and G, Cited Document 1 describes that the "scrambled keypad image" is generated using the "permutation file including all permutations of keys necessary for the final keypad images."

E From the above, it is recognized that Cited Document describes the following invention (hereinafter, referred to as "Cited Invention"). Note that the reference numerals "a" to "f" of the respective components are given by the body for explanation (hereinafter, the components to which the reference numerals are given are referred to as the "component a" to "component f").

(Cited Invention)

f A method for verifying a PIN input by a user, wherein

a a keypad operable within a keypad zone of a screen of an electronic device and a scrambled keypad image displayed in the keypad zone,

b the scrambled keypad image is generated using a permutation file including all permutations of keys necessary for final keypad images, and is sent to the electronic device from a server that is a computer-based resource located remotely,

c the user's operation of the keypad via the scrambled keypad image generates an encoded version of the PIN of the user's intended input,

d the encoded version of the PIN is sent from the electronic device to the server, and

e the server obtains a decoded version of the PIN.

3 Description of Cited Document 2

United States Patent Application Publication No. 2014/0324708 A1 (hereinafter referred to as "Cited Document 2") cited in the reason for refusal in the examiner's decision describes the following matters together with the drawings (underlines are added by the body for emphasis).

A "[0014] A technique to secure passcode entry on an electronic device is disclosed herein. The technique involves encrypting raw input events from an input device of an electronic device. A complete passcode entry may produce multiple raw input events, such as multiple touch events on a touch screen. In such instances, each raw input may represent the location of a touch event on a touch screen, and each event representing a touch location is encrypted. Thus, encryption of individual input events serves as a measure to prevent unauthorized discovery (e.g., by malware) of the passcode."

B "[0017] The raw input events can be touch events as recorded by a touch screen of the electronic device. A passcode interface, such as a PIN or key pad, may be displayed on the touch screen. The user may enter the passcode entry for authentication on the touch screen. The electronic device may encrypt the touch events resulting from the interaction with the touchscreen. The electronic device may then transmit the encrypted touch events represented by touch screen coordinates to a trusted computing system to cause the trusted computing system to decipher the passcode, as entered by the user, based on the encrypted touch events. To cause in this context is intended to include sending a command, a request, or any other type of message or signal that results in the stated action, such as deciphering the passcode based on the encrypted touch events.

[0018] In various embodiments, only the trusted computing system performs the transformation from the encrypted raw input events into the passcode entry. Instead of deciphering the passcode entry on the electronic device, the input events are sent to the trusted computing system for interpretation. The trusted computing system, which may be external to the electronic device, can then decrypt each input event to decipher the passcode entered by the user.

[0019] Deciphering of the passcode may include comparing the decrypted touch event to a passcode interface configuration. For example, the passcode interface configuration may be or include a key pad layout, which can be represented as a data structure or object. As a more specific example, the key pad layout can be generated by the trusted computing system and sent to the electronic device for presentation. As another specific example, the key pad layout can be generated by the electronic device, and sent to the trusted computing system for deciphering. Either way, the trusted computing system may use the passcode interface configuration, e.g., key pad layout, to map sensor input events to a sequence of characters used to compose the passcode entry.

[0020] The key pad layout may include geometry, position, relative position, animation sequence, or other variations of the presentation of the key pad. The key pad may include multiple buttons taking up regions of the touch screen of the electronic device. Each touch event may be represented by an (X,Y) location coordinate, where each coordinate or set of coordinates is encrypted in accordance with various embodiments of the disclosed technique. The passcode can then be deciphered by mapping each (X,Y) coordinate to a two dimensional space corresponding to a specific soft-button representing a character used to compose a passcode entry."

C "[0023] FIG. 1 is a data flow diagram illustrating a technique 100 of sensor entry

encryption. As shown, the technique 100 involves an electronic device 102 and an authentication system 104. The electronic device 102 may be a general purpose device with data processing capabilities. For example, the electronic device 102 may be a mobile phone, a tablet, an e-reader, other mobile or portable computing devices, or other stationary computing devices. The authentication system 104 may be a trusted computing system in data communications with the electronic device 102, such as over a network. The authentication system 104 may be one or more computing devices. For example, the authentication system 104 may be a server computer, a network of computing systems, a cloud computing environment, a virtualized computing environment, or any combination thereof. Communication between the authentication system 104 and the electronic device 102 may be any form of data communication, including mobile telecommunication (e.g., cellular), WiFi, wireless Ethernet, wired Ethernet, or any other form of Internet connection.

[0024] The electronic device 102 may be a mobile device, such as a smartphone or a tablet computer, that presents a passcode interface 106 on an output device. In the illustrated embodiment, the output device is a touch screen 108. A user seeking authentication may input through a sensor (i.e. an input device) of the electronic device 102, a series of inputs composing a passcode, such as a PIN, a passphrase, a digital key, or any combination thereof. In the illustrated embodiment, the sensor is the touch screen 108. Note, however, that the sensor (e.g., a touch panel or a cursor device) for detecting an input may be different from the output device (e.g., a display, a projection device, a speaker, or other devices capable of presenting the passcode interface 106)."

D "[0027] In various embodiments, a portion of the sensor input stream 114 is sent to the authentication system 104 for deciphering. In various embodiments, when the authentication system 104 receives the portion of the sensor input stream 114, the authentication system 104 may decrypt the sensor entries 110 prior to deciphering the passcode entry 116 by the user. A passcode interface configuration 118, which defines the mechanism of interaction with the passcode interface, may be generated by the electronic device 102 and then sent over to the authentication system 104 as well. The passcode interface configuration may specify a mapping between sensor values of the sensor entries and a set of characters used to compose a passcode entry As an example, where the passcode interface is displayed on the touch screen 108, the passcode interface configuration may include geometric definition of the passcode interface on the touch screen 108. In other embodiments, the passcode interface configuration is generated by the authentication system 104. The passcode interface configuration may be generated

specifically for a session with a user interacting with the passcode entry interface."

E "[0034] FIG. 2 is a block diagram illustrating an electronic device 200, which may represent device 102 in FIG. 1, for passcode entry. The electronic device 200 may be a general-purpose computing device. The electronic device 200 includes various modules and storage as described below. The electronic device 200 includes a passcode interface module 202, which is configured to present and maintain a passcode interface.

[0035] In various embodiments, the passcode interface module 202 is configured to generate the passcode interface. The passcode interface module 202 may generate the passcode interface randomly or pseudo-randomly. As an example, the passcode interface may be configured as a PIN pad layout. The size, arrangement, position, orientation, shape, and other absolute or relative geometric characteristics of the passcode interface and elements within the passcode interface are all examples of the passcode interface configuration. The passcode interface configuration may be selected to promote concealment of a user's entry of a passcode on the passcode interface. For example, the elements on the passcode interface may be characters from which the passcode combination (e.g., the passcode entry 116) may be chosen. The arrangement of the characters and the geometric shapes and sizes of the characters may be randomized. Other attributes of the passcode interface configuration may be wholly or partially randomly generated. The passcode interface configuration, such as the absolute and relative (e.g., relative to a display of the electronic device 200) geometric characteristics of the passcode interface, may be stored in an interface configuration store 204.

[0036] In other embodiments, the passcode interface configuration is provided by a remote system through a network, such as the authentication system 104 of FIG. 1. For example, the passcode interface configuration may be received through an authentication communication module 206. In those embodiments, once received, the passcode interface configuration may be stored in the interface configuration store 204. The passcode interface configuration may then be used by the passcode interface module 202 to present the passcode interface to the user.

[0037] When the passcode interface configuration is generated on the electronic device 200, the authentication communication module 206 may transmit the passcode interface configuration to the remote system such that the remote system may use a portion of the sensor input stream and the passcode interface configuration to decipher the passcode entry."

F "FIG.1

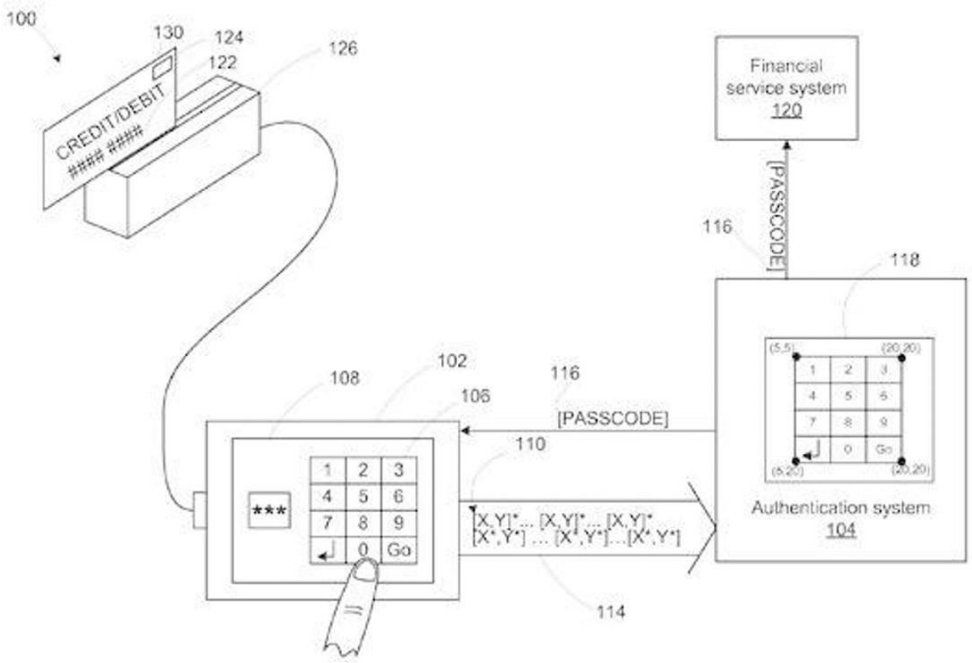
100
130
124
122
126
CREDIT/DEBIT
####
Financial service system
120
[PASSCODE]
116
118
108
102
106
116
[PASSCODE]
110
1 2 3
4 5 6
7 8 9
0 Go
***
[X,Y]*... [X,Y]*... [X,Y]*
[X*,Y*] ... [X*,Y*]...[X*,Y*]
Authentication system
104
114

FIG. 1

"

G "FIG.2

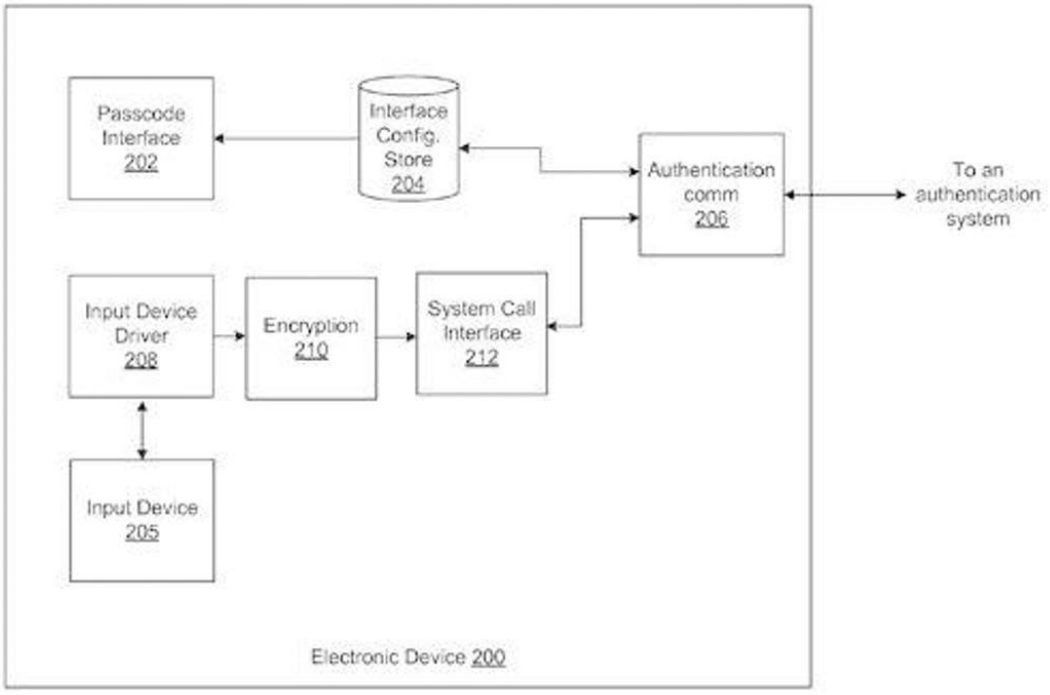

FIG. 2

"

H As described above, Cited Document 2 describes that as "a technique to secure passcode input," "a passcode interface configuration used for inputting and deciphering a passcode is generated by an electronic device and sent to a trusted computing system for decoding."

I Since Cited Document 2 also describes a specific example in which the "passcode interface configuration" is "generated by a trusted computing system provided outside the electronic device and sent to the electronic device," it is recognized that "generating a passcode interface configuration by a trusted computing system and sending it to an electronic device" and generating a passcode interface configuration by an electronic device and sending it to a trusted computing system" are suggested to be interchangeable.

Further, it is recognized that Cited Document 2 also mentions "randomizing arrangement of characters" as the "passcode interface configuration."

No. 5 Comparison

1 Comparison of Invention and Cited Invention

A Regarding component A of Invention and component a of Cited Invention

The "keypad zone of the screen of the electronic device" of Cited Invention corresponds to the "display zone of a screen associated with an electronic device" of Invention, and the "scrambled keypad image" displayed in the "keypad zone" of Cited Invention corresponds to the "keypad image" presented on the "operable keypad" of Invention.

Therefore, there is no difference between the component a of Cited Invention and the component A of Invention.

B Regarding component B of Invention and component b of Cited Invention

The "permutation file including all permutations of keys necessary for the final keypad images" of Cited Invention is common to the "at least one scrambled keypad layout" used for generating the "keypad image and/or operable keypad" in Invention in that both are a layout of the keypad used for the "scrambled keypad image."

On the other hand, Invention is different from Cited Invention in that "at least one scrambled keypad layout" of Invention is "locally generated on an electronic device," whereas in Cited Invention, the "scrambled keypad image" is sent to an electronic device from a server that is a computer-based resource located remotely and the "permutation file" used for the generation is not locally generated in the electronic device.

C Regarding component C and D of Invention and component c and d of Cited Invention

The "PIN" intentionally input by the user in Cited Invention corresponds to the "identifier" of Invention, and thus the "encoded version of the PIN of the user's intended input" generated by "the user's operation of the keypad via the scrambled keypad image" of Cited Invention corresponds to the "encoded version of an identifier input to the electronic device by a user operating the operable keypad via the keypad image" of Invention.

Here, Invention is configured to "store" the "encoded version of the identifier," but it is obvious that "generating" is performed prior to "storing," and there is no difference from Cite Invention in this regard.

The "server" that sends the encoded version of the PIN in Cited Invention corresponds to the "remote computing resource" that sends the encoded version of the identifier in Invention.

Therefore, it can be said that the component C and D of Invention and the

component c and d of Cited Invention are different from each other in that Invention has a configuration in which the encoded version of the identifier is stored, whereas it is unclear whether the encoded version of the PIN is stored in Cited Invention, but are the same in other respects.

D Regarding component E of Invention and component e of Cited Invention

"Obtaining the decoded version of the PIN" in Cited Invention corresponds to "decoding" the "encoded version of the identifier" sent from the electronic device in Invention.

Here, Invention is different from Cited Invention in that Invention is configured to "send at least one scrambled keypad layout to the remote computing resource" in order to enable decryption, whereas Cited Invention does not have a configuration corresponding thereto.

E Regarding component F of Invention and component f of Cited Invention

According to the above A of 1 in No. 4, it can be said that since the "method for verifying a PIN input by a user" of Cited Invention is a procedure for user authentication, the "method for verifying a PIN input by a user" of Cited Invention corresponds to the "authentication method" of Invention.

2 Corresponding Features and Different Features

Therefore, Invention and Cited Invention correspond and differ in the following features.

(Corresponding Features)

An authentication method comprising: presenting a keypad image on an operable keypad within a display zone of a screen associated with an electronic device, wherein the keypad image is generated using a scrambled keypad layout;

generating an encoded version of an identifier input to the electronic device by a user operating the operable keypad via the keypad image;

sending the encoded version of the identifier to a remote computing resource; and

decoding the encoded version of the identifier in the remote computing resource.

(Different Feature 1)

The "scrambled keypad layout" of Invention is "locally generated on an electronic device," whereas the "permutation file" of Cited Invention is not locally generated in the electronic device.

(Different Feature 2)

The encoded version of the generated identifier is stored in Invention, whereas it is unclear whether the encoded version of the generated PIN is stored in Cited Invention.

(Different Feature 3)

In Invention, the "scrambled keypad layout" is "sent to a remote computing device," whereas Cited Invention does not have such a configuration.

No. 6 Judgment

1 Judgment for Different Features

A Different Features 1 and 3

As described in the above 3 of No. 4, Cited Document 2 discloses that relating to "a technique to secure passcode input," "a passcode interface configuration used for inputting and deciphering a passcode is generated by an electronic device and sent to a trusted computing system for decoding."

Here, it is obvious to a person skilled in the art that the "passcode interface configuration" described in Cited Document 2 corresponds to the "permutation file including all permutations of keys necessary for the final keypad images" of Cited Invention because the "passcode interface configuration" includes "geometric definition of the passcode interface on the touch screen 108" and "specifies a mapping between sensor values of the sensor entries and a set of characters used to compose a passcode entry" (D of 3 in No. 4).

In addition, in view of the fact that Cited Document 2 discloses "randomizing arrangement of characters" relating to the "passcode interface configuration" (E of 3 in No. 4), and suggests that "generating a passcode interface configuration by a trusted computing system and sending it to an electronic device" and generating a passcode interface configuration by an electronic device and sending it to a trusted computing system" are interchangeable (I of 3 in No. 4), it is not recognized that a person skilled in the art requires a special creativity to obtain the constitution of Invention according to the different features 1 and 3 by adopting a configuration in which the "permutation file" necessary for decryption is sent to the server as a configuration in which the "permutation file including all permutations of keys necessary for the final keypad images" and the "scrambled keypad image" are generated using the electronic device.

In case of adopting such a configuration, though a "permutation file" or the like have to be made in the electronic device, which makes the processing load of the

electronic device get increased, the server does not have to make a "permutation file" or a "scrambled keypad image". Thus, such a configuration has an effect of reducing the processing load on the server, which is merely a matter that could have easily been conceived by a person skilled in the art.

B Regarding Difference 2

In Cited Invention, when the encoded version of the generated PIN is sent from the electronic device to the server, the step of storing the encoded version of the PIN in the electronic device is intervened, which is merely a matter easily adopted by a person skilled in the art.

C Summary

As described above, the configurations according to the differences 1 to 3 could have been easily conceived by a person skilled in the art, and the functions and effects of Invention are also within a range that can be predicted by a person skilled in the art based on the descriptions of Cited Documents 1 and 2.

Therefore, Invention could have been easily made by a person skilled in the art based on the invention described in Cited Document 1 and the technical matters described in Cited Document 2, and thus cannot be granted a patent under the provision of Article 29(2) of the Patent Act.

2 The Appellant's allegation

The appellant believes that Invention has an inventive step, and alleges that (1) "Since Cited Document 1 does not disclose the layout generated locally, a person skilled in the art cannot arrive at Invention starting from Cited Document 1," (2) "Cited Document 1 not only silences the feature recited in Claim 1 of the present application, but also clearly teaches the use of scrambled layouts that are generated remotely from the user's local device and sent to the user's device, and thus Cited Document 1 is actually far from the features of Invention. This is completely the opposite of the feature recited in Claim 1 of the present application, and in order to devise a device that actually operates in the opposite manner, a person skilled in the art needs to change 180 degrees based on the teaching of Cited Document 1, which cannot be done by a person skilled in the art," and (3) "The method of Invention provides technical advantages over Cited Document 1. ... This means that the server is freed from the processing requirements for layout generation, and that less time is required compared to the case where a layout is sent from the server to the device. Accordingly, an authentication solution that is more efficient and

operates faster than Cited Document 1 is realized." (The numbers(1)to (3) above are added by the body. The same shall apply hereinafter.)

However, in Cited Invention, since it is easy for a person skilled in the art to obtain the configuration of Invention according to Different Features 1 and 3 based on the disclosure of Cited Document 2, it is impossible to adopt the appellant's allegations (1) to (3).

The appellant also alleges that (4) "Generating a scrambled layout locally means that the scrambled layout is not be intercepted while sending from a remote server to the user's device. When the scrambled layout is intercepted, an unauthorized person can know and calculate the mapping between the user's input and the keypad/image layout, and can decipher the user's secret input. This is a potential vulnerability in Cited Document 1, but the vulnerability is overcome by Invention."

However, Invention includes the configuration E in which " at least one scrambled keypad layout can be sent to the remote computing resource to decode the encoded version of the identifier," and thus "the scrambled layout is not be intercepted while sending from a remote server to the user's device" by "generating the scrambled layout locally," but a person skilled in the art normally conceives that "the scrambled layout generated locally being intercepted while sending from the user's device to a remote server " may occur anew. It can be said that Invention potentially creates a new vulnerability in exchange for overcoming the "potential vulnerability of Cited Document 1" mentioned by the appellant. It is also clear from the description, relating to configuring a PIN pad randomly arranged on the user's device,in Cited Document 1(E of 1 in No. 4) that "Security loopholes are potentially provided and several access points may be provided for malware to obtain the user's PIN (as the handset/device would have to transmit the random number and thus the order of the PIN pad back to the server). Therefore, such an embodiment is suitable for applications where required security levels are somewhat relaxed,". Then, since it cannot be said that the matter according to the appellant's allegation (4) supports effect beyond the expectation of a person skilled in the art, which can affirm the inventive step of Invention, the appellant's allegation (4) cannot be adopted either.

Further, the appellant alleges that Cited Document 2 does not teach (5) "generating a mapping between the keys depicted in the keypad image and the keys of the underlying operable keypad," (6) "enabling an encoded version of a user's identifier to be input to an electronic device with the underlying operable keypad," and (7) "generating the keypad image and/or the operable keypad using at least one scrambled keypad layout locally generated on the user's local electronic device," and that functions lacking in Cited

Document 1 cannot be added.

However, as described in A of 1, regardless of the presence or absence of the teachings of (5) to (7) above, it is recognized that Cited Document 2 discloses the technical matters as described in the above H and I of 3 in No. 4, and based on the disclosure, a person skilled in the art could have easily conceived of obtaining the configuration of Invention according to the Different Features 1 and 3 in Cited Invention. It cannot be said that the fact that there is no teaching about (5) to (7) according to the appellant's allegation in Cited Document 2 and the fact of obtaining the configuration according to the Different Features 1 and 3 constitute an inhibition factor. Therefore, the above appellant's allegation regarding Cited Document 2 cannot be adopted.

3 Note

The component B of Invention is that "the keypad image and/or the operable keypad are generated using at least one scrambled keypad layout locally generated on the electronic device," and includes not only the case examined above where the "keypad image" is "generated using a scrambled keypad layout," but also a configuration in which the "operable keypad" is "generated using a scrambled keypad layout" instead of the "keypad image" or in addition to the "keypad image." Therefore, the configuration in which the "operable keypad" is "generated using a scrambled keypad layout" will also be examined tentatively.

According to the above F and H of 1 in No. 4, Cited Document 1 describes that the "operable keypad" is generated and used in the electronic device by using the "permutation file" received from the server in addition to the "scrambled keypad image." Here, as described in the above A of 1, a person skilled in the art could have easily conceive of locally creating a "permutation file" used for generation of a "scrambled keypad image" in an electronic device and sending the permutation file to a server for decoding in the invention described in Cited Document 1, and as described in the above E of 1 in No. 4, Cited Document 1 describes that a random number is selected in the device, and thus it is not recognized that it is difficult for a person skilled in the art to make a configuration in which a "permutation file" for generating an "operable keypad" in an electronic device is locally created in the electronic device and sent to a server for decoding.

No. 7 Closing

As described above, since Invention shall not be granted a patent under the provision of Article 29(2) of the Patent Act, the present application should be rejected

without examining the inventions according to the remaining Claims.

Therefore, the appeal decision shall be made as described in the conclusion.

November 19, 2021

Chief administrative judge: ISHII, Shigekazu
Administrative judge: SHINOHARA, Koichi
Administrative judge: KANEKO, Hidehiko