Appeal decision

Appeal No. 2015-20015

USA
Appellant QUALCOMM INCORPORATED

Tokyo, Japan
Patent Attorney MURAYAMA, Yasuhiko

Tokyo, Japan
Patent Attorney KURODA, Shimpei

The case of appeal against the examiner's decision of refusal of Japanese Patent Application No. 2014-524051, entitled "Method and apparatus for using a multi-factor password or a dynamic password for enhanced security on a device" (International Publication dated February 7, 2013, WO 2013/019880, national publication dated October 2, 2014, National Publication of International Patent Application No. 2014-526105) has resulted in the following appeal decision:

Conclusion

The appeal of the case was groundless.

Reason

No. 1 History of the procedures

The present application was originally filed on August 1, 2012 as an International Patent Application (priority claim under the Paris Convention: received by the foreign receiving office on August 2, 2011, United States).

A translation written into Japanese of the specification, claims, and drawings (only description in drawings) in accordance with the provisions of Article 184(4)(i) of the Patent Act was submitted on February 21, 2014 together with the request for examination. A notice of reasons for refusal was issued by the examiner on January 13, 2015, and a written opinion and written amendment were submitted on April 22, 2015. However, a decision of refusal was issued by the examiner on June 25, 2015

(certified copy was transmitted on July 6, 2015), and a request for appeal and a written amendment were submitted on November 6, 2015. A report based on the provisions of Article 164(3) of the Patent Act was issued by the examiner on December 17, 2015, and a written statement was submitted on April 4, 2016. Then, a notice of reasons for refusal was issued by the body on March 21, 2017, and a written opinion and written amendment were submitted on June 27, 2017.

No. 2. Regarding the Invention

The invention according to Claim 1 of the present application (referred to as "the Invention" below) described in Claim 1 amended based on the written amendment dated on June 27, 2017 is as follows.

"A method of performing authentication, comprising the steps of:

receiving entered information for a plurality of factors of a multi-factor password including the plurality of different factors selected by a user;

determining the multi-factor password based on the received entered information, and determining the multi-factor password of which the plurality of factors corresponds to different types of information used to authenticate the user; and

authenticating the user based on the determination by a device, wherein

the multi-factor password is authenticated based on the authentication results of the plurality of factors and an order of the selected factors, and

the order of the plurality of factors included in the multi-factor password is previously selected by the user."

No. 3 Matters described in cited publications

1. Japanese Unexamined Patent Application Publication No. 2011-022953 (published on February 3, 2011) which had already been known before the filing of the present application in the first country and was cited in the notice of reasons for refusal dated March 21, 2017 (referred to as "the notice of reasons for refusal by the body" below) as cited publication 1 discloses the following matters together with the related drawings.

A "[0028]

With reference to a displayed image, a user operates an input unit 120 to input a numeric character string corresponding to an authentication character string to an authentication information registration unit 170b. The user previously determines a password character string to be used as authentication information. Here, as an example, it is assumed that the password character string is "cgi2".

[0029]

The user associates a numeric character string "2579" corresponding to the authentication information "cgi2" with a user ID and inputs the associated information to the authentication information registration unit 170b. The authentication information registration unit 170b associates the user ID with the numeric character string and registers the associated information to a user management table 160a."

B. "[0048]

Subsequently, authentication processing of authenticating the user by an authentication apparatus 100 is described. FIG. 9 is a flowchart of a processing procedure of the authentication processing. As illustrated in FIG. 9, the authentication apparatus 100 obtains the user ID (step S201), and an authentication processing unit 170c retrieves a numeric character string corresponding to the user ID from the user management table 160a (step S202).

[0049]

The authentication apparatus 100 obtains biological information from a biological sensor 110 (step S203), and a hash value generation unit 170a generates a hash value character string based on the biological information (step S204).

[0050]

The authentication processing unit 170c specifies a password character string corresponding to the numeric character string based on the numeric character string and first correspondence table data (step S205). The authentication processing unit 170c randomly rearranges the hash value character string (step S206) and outputs a displayed image in which each numerical value corresponds to block identification information (step S207).

[0051]

The authentication processing unit 170c receives the numeric character string (step S208), and specifies a character string corresponding to the numeric character string by comparing the numeric character string with second correspondence table

data (step S209). The authentication processing unit 170c determines whether the specified character string is identical to the password character string (step S210).
[0052]

When the specified character string is identical to the password character string (step S211, Yes), the authentication processing unit 170c determines that the authentication has succeeded (step S212). On the other hand, when the specified character string is different from the password character string (step S211, No), the authentication processing unit 170c determines that the authentication failed (step S213).
[0053]

As described above, after rearranging the hash value character string of the biological information, the authentication apparatus 100 according to the second embodiment makes each piece of block information having the rearranged character string and a dummy character string mixed with each other correspond to each numerical value and outputs the display screen. The authentication apparatus 100 determines whether the character string corresponding to the numeric character string input by the user is identical to the password character string and authenticates the user based on the determination result. Since the order of the characters in the string displayed in the display screen changes every time, the numeric character string input by the user is different every time. Therefore, even when an input operation is glanced with a data logger having a screen shot or the like, the authentication information is not leaked."

C. "[0058]
The authentication apparatus 100 can be realized by installing respective functions of the hash value generation unit 170a, the authentication information registration unit 170b, and the authentication processing unit 170c to a known information processing apparatus. The known information processing apparatus corresponds to, for example, a personal computer, a work station, a mobile phone, a PHS terminal, a mobile communication terminal, or a PDA."

D. In FIG. 2, at least, it is described that the "authentication apparatus" includes the "biological sensor," an "input unit," an "output unit," an "input/output controller," and a "controller" including the "hash value generation unit," an "authentication information registration unit," and an " authentication processing unit," and in addition, the

"authentication apparatus" includes a "storage unit" including a "user management table."

2. Japanese Unexamined Patent Application Publication No. 2011-145906 (published on July 28, 2011) which had already been known before the filing of the present application in the first country and was cited in the original examination's notice of reasons for refusal dated January 13, 2015 (referred to as "the original examination's notice of reasons for refusal " below) and in the notice of reasons for refusal by the body as cited publication 2 discloses the following matters together with the related drawings.

E. "[0057]

The authentication method here is, for example, code number, a password, finger vein authentication, palm authentication, fingerprint authentication, handwriting authentication, or voiceprint authentication, e.g. An authentication method other than those described above can be introduced as an authentication method presented as an option. As long as the method serves to perform authentication, the method can be introduced.

[0058]

The user previously registers a place and an authentication method used at that place from among a plurality of displayed frames, and the combination of the place and the method is used as the authentication. For example, the password is selected for an authentication method selection frame 1, the code number is selected for an authentication method selection frame 3, and the finger vein authentication is selected for an authentication method selection frame 7. The combination of the authentication method selection frame and the kind of the authentication method is used as one kind of authentication."

3. Japanese Unexamined Patent Application Publication No. 2007-334707 (published on December 27, 2007) which had already been known before the filing of the present application in the first country and was cited in the original examination's notice of reasons for refusal and the notice of reasons for refusal by the body as cited publication 3 discloses the following matters together with the related drawings.

F. "[0007]

In the authentication system according to the present invention, since the user is authenticated by a previously set authentication procedure based on at least one kind of biological information for authentication selected by the user from among a plurality of kinds of registered biological information which has been previously registered, the number and the kind of biological information which is used by the user for authentication can be freely set. With this system, the user can freely set complicated authentication with high accuracy and simple authentication according to a transaction state. Here, the "biological information" means information indicating biological features such as a fingerprint, voiceprint, iris, voice, or a vein pattern of a part of a body."

G. "[0010]

In the biological authentication apparatus,

when the plurality of kinds of biological information for authentication are selected, the user confirmation unit may confirm the user with an authentication method based on the plurality of kinds of biological information for authentication and an authentication order which is an order of the authentication performed by using the plurality of kinds of biological information for authentication."

No. 4 Invention described in cited publications

1. Based on the description such that "the authentication apparatus 100 obtains biological information from a biological sensor 110" in B described above, the description such that "the authentication processing unit 170c receives the numeric character string" in B also described above, the description such that "the numeric character string input by the user" in B also described above, the matters disclosed in FIG. 2 indicated in D described above, the description such that "the authentication apparatus 100 can be realized by installing respective functions of the hash value generation unit 170a, the authentication information registration unit 170b, and the authentication processing unit 170c to a known information processing apparatus" in C described above, and the description such that "the known information processing apparatus corresponds to, for example, a personal computer, a work station, a mobile phone, a PHS terminal, a mobile communication terminal, or a PDA, e.g." in C also described above, it can be read that "the authentication apparatus is realized by a known information processing apparatus such as a mobile phone, a PHS terminal, a mobile communication terminal, or a PDA" from the cited publication 1, and these "known

information processing apparatuses" are referred to as a "communication device" or "mobile device"; that is, a kind of a "device." Therefore,

from the cited publication 1,

it can be read that "the device obtains the biological information of the user from the biological sensor, and the authentication processing unit included in the device receives the numeric character string input by the user via the input unit of the device."

2. Based on the description such that "specifies a character string corresponding to the numeric character string by comparing the numeric character string with second correspondence table data" in B described above, the description such that "the authentication processing unit 170c determines whether the specified character string is identical to the password character string" in B also described above, and the matters examined in 1. described above, from the cited publication 1,

it can be read that "the authentication processing unit specifies a character string corresponding to the received numeric character string by using correspondence table data and determines whether the specified character string is identical to the password character string."

3. Based on the description such that "when the specified character string is identical to the password character string (step S211, Yes), the authentication processing unit 170c determines that the authentication was succeeded" in B described above, the description such that "determines whether to be identical to the password character string and authenticates the user based on the determination result" in B also described above, and the matters examined in 1. described above, from the cited publication 1

it can be read that "the device authenticates the user based on the determination result."

4. Based on the description such that "operates an input unit 120 to input a numeric character string corresponding to a password character string to an authentication information registration unit 170b. The user previously determines the password character string to be used as authentication information" in A described above, the description such that "the user associates a numeric character string '2579' corresponding to the authentication information 'cgi2' with a user ID and inputs the associated information to the authentication information registration unit 170b. The authentication information registration unit 170b associates the user ID with the

numeric character string and registers the associated information to a user management table 160a" in A described above, and the matters examined in 2. and 3. described above, from the cited publication 1,

it can be read that "the character string used for authentication is previously determined by the user."

5. As described above, it is obvious that the matters examined in 1. to 4. are methods of "authenticating" the "user" by the "device." Therefore, according to the matters examined in 1. to 4., it is acknowledged that the following invention (referred to as "Cited Invention" below) is described in the cited publication 1.

A method of authenticating a user by a device, wherein

the device obtains biological information of the user from a biological sensor, and an authentication processing unit included in the device receives a numeric character string input by the user via an input unit of the device,

the authentication processing unit specifies a character string corresponding to the received numeric character string by using correspondence table data and determines whether the specified character string is identical to a password character string,

the device authenticates the user based on the determination result, and

the character string used for authentication is previously determined by the user.

No. 5. Comparison between the Invention and Cited Invention

1. "A method of authenticating a user by a device" in Cited Invention

corresponds to "a method of performing authentication" in the Invention.

2. In Cited Invention, a plurality of kinds of information including the "biological information" required for authentication and the "numeric character string" input by the "user" are received, and the "numeric character string" in the plurality of kinds of information relates to the "character string used for authentication" determined by the "user." Therefore, the numeric character string can be assumed as "a factor selected by the user," and used for the determination regarding the authentication.

In Cited Invention, the authentication is performed by using the "biological information" of the "user" obtained from the "biological sensor" and the "numeric character string" input by the "user." Therefore, it is obvious that the "biological information" and the "numeric character string" are the "entered information" and the "password" in Cited Invention includes the "biological information" and the "numeric character string."

In addition, the "biological information" and the "numeric character string" are the "different factors."

Therefore, the "biological information" and the "numeric character string" in Cited Invention

correspond to the "factors of the password" in the Invention.

Therefore, "to obtain biological information of the user from a biological sensor, an authentication processing unit included in the device receives a numeric character string input by the user via an input unit of the device" in Cited Invention and

"receiving entered information for a plurality of factors of a multi-factor password including the plurality of different factors selected by a user" in the Invention are common in that

both are "steps of receiving entered information for a plurality of factors of a password including a factor selected by a user."

3. As examined in 2. described above, the "password" in Cited Invention includes the "biological information" and the "numeric character string." However, to determine whether the "specified character string" obtained from the input "numeric character string" "is identical to a password character string" is synonymous with to determine validity of the "password." It is obvious that the "biological information" and the "numeric character string" in Cited Invention are the "different types of information" to "authenticate" the "password" including the "biological information" and the "numeric character string."

Accordingly, "to specify a character string corresponding to the received numeric character string by using correspondence table data and determine whether the specified character string is identical to a password character string" in Cited Invention and

"determining the multi-factor password based on the received entered information, and determining the multi-factor password of which the plurality of factors corresponds to different types of information used to authenticate the user" in the Invention are common in that

both are "steps of determining the password based on the received entered information and determining the password of which the plurality of factors correspond to different types of information used to authenticate the user."

4. "The device authenticates the user based on the determination result" in Cited Invention
corresponds to "authenticating the user based on the determination by a device" in the Invention.

5. In Cited Invention, the "character string used for authentication" is "previously determined by the user," and the "character string used for authentication" is "information required for authentication."

Therefore, "the character string used for the authentication is previously determined by the user" in Cited Invention and

"the order of the plurality of factors included in the multi-factor password is previously selected by the user" in the Invention

are common in that "the information required for the authentication is previously selected by the user."

6. As described above, based on the matters examined in 1. to 5. described above, corresponding features and different features of the Invention and Cited Invention are as follows.
[Corresponding feature]]

A method of performing authentication, comprising the steps of:

receiving entered information for a plurality of factors of a password including a factor selected by a user;

determining the password based on the received entered information and determining the password of which the plurality of factors corresponds to different types of information used to authenticate the user; and

authenticating the user based on the determination by a device, wherein

information required for the authentication is previously selected by the user.

[The different feature 1]

The "password including a factor selected by a user" is

"the multi-factor password including a plurality of different factors selected by a user" in the Invention.

Whereas, in Cited Invention, it is mentioned that the "password character string" is previously determined by the "user." However, the selection of the "biological information" is not especially mentioned.

[The different feature 2]

"Determining the password based on the received entered information" is "determining the multi-factor password" in the Invention.

Whereas, in Cited Invention, only the "specified character string" is determined.

[The different feature 3]

In the Invention, "the multi-factor password is authenticated based on the authentication results of the plurality of factors and an order of the selected factors."

Whereas, in Cited Invention, the authentication of the "biological information" is not especially mentioned.

[The different feature 4]

Regarding the point that "the information required for the authentication is previously selected by the user," in the Invention, the "order of the plurality of factors" is "selected by the user."

Whereas, in Cited Invention, the order of the acquisition of the "biological information" and the input of the "numeric character string" cannot be changed.

No. 6 Judgment by the body regarding the different features

1. Regarding [the different feature 1]

Based on the description such that "the authentication method here is, for example, a code number, a password, finger vein authentication, palm authentication, fingerprint authentication, handwriting authentication, and voiceprint authentication. An authentication method other than those described above can be introduced as an

authentication method presented as an option" of the cited publication 2 cited in E described above, the description such that "the user previously registers a place and an authentication method used at that place from among a plurality of displayed selection frames, and the combination of the place and the method is used as the authentication. For example, the password is selected for an authentication method selection frame 1, the code number is selected for an authentication method selection frame 3, and the finger vein authentication is selected for an authentication method selection frame 7. The combination of the authentication method selection frame and the kind of the authentication method is used as one kind of authentication" cited in E described above, and the description such that "since the user is authenticated by a previously set authentication procedure based on at least one kind of biological information for authentication selected by the user from among a plurality of kinds of registered biological information which has been previously registered, the number and the kind of biological information which is used by the user for authentication can be freely set. With this system, the user can freely set complicated authentication with high accuracy and simple authentication according to a transaction state. Here, the "biological information" means information indicating biological features such as a fingerprint, a voiceprint, iris, voice, or a vein pattern of a part of a body" of the cited publication 3 cited in F described above, the method in which the "user" selects some kinds from among the plurality of kinds of "biological information" is a technical matter which had been widely known by a person skilled in the art before the filing of the present application in the first country.

Therefore, to select the plurality of kinds of "biological information" used for the "authentication" by the "user" would have been easily made by a person skilled in the art in Cited Invention based on the inventions described in Cited Invention and the cited publications 2 and 3.

Accordingly, [the different feature 1] is not exceptional.

2. Regarding [the different feature 2]

Based on the description such that "the user may be confirmed with an authentication method based on the plurality of kinds of biological information for authentication and an authentication order which is an order of the authentication performed by using the plurality of kinds of biological information for authentication" of the cited publication 3 cited in G described above, "to authenticate the plurality of kinds of input biological information based on the order"; that is, "to

perform authentication based on the plurality of kinds of input biological information" is a technical matter which had been widely known by a person skilled in the art before the filing of the present application in the first country.

Therefore, in Cited Invention, "to determine based on the plurality of kinds of input biological information" is a matter which can be appropriately achieved by a person skilled in the art.

Accordingly, [the different feature 2] is not exceptional.

3. Regarding [the different feature 3]

As described in G described above and in the cited publication 3 cited in 2. described above, the point that "the user is authenticated with an authentication method based on an authentication order of the plurality of kinds of biological information" is a technical matter which had been widely known by a person skilled in the art before the filing of the present application in the first country. "When a plurality of kinds of information to be authenticated are subsequently authenticated, it is determined whether to perform next authentication according to the previous authentication result; that is, the authentication is continued based on the authentication result" is a matter which can be appropriately selected by a person skilled in the art.

Therefore, "to entirely perform authentication based on the previous authentication result and the order of the authentication when the authentication is performed by using the plurality of kinds of biological information" in Cited Invention can be appropriately achieved by a person skilled in the art.

Accordingly, [the different feature 3] is not exceptional.

4. Regarding [the different feature 4]

As described in the description of the cited publication 2 in E described above cited in 1. described above or as described in the description of the cited publication 3 in F described above, "to previously select the information used for authentication by the user" is a technical matter which had been widely known by a person skilled in the art before the filing of the present application in the first country.

As examined in 2. and 3. described above, to authenticate the user by using the authentication method based on the order of the authentication is a technical matter which has been widely known by a person skilled in the art. Therefore, "to include an order of the plurality of kinds of authentication and an order of a plurality of

factors" as the "information used for authentication" is a matter which can be appropriately achieved by a person skilled in the art.

Accordingly, in Cited Invention, "to include the order of the plurality of factors in the information used for authentication and to previously select the order of the plurality of factors by the user" is a matter which can be appropriately achieved by a person skilled in the art.

Accordingly, [the different feature 4] is not exceptional.

5. As examined in 1. to 4. described above, [the different feature 1] to [the different feature 4] are not exceptional. The effect obtained by the structure of the Invention can be easily predicted by a person skilled in the art and cannot be assumed as an exceptional effect.

No. 7 Closing

Therefore, the Invention could be easily made by a person skilled in the art according to an invention described in a publication distributed in Japan and abroad prior to the filing of the present application or an invention available to the public through electric telecommunication lines. Accordingly, the appellant should not be granted a patent for the Invention in accordance with the provisions of Article 29(2) of the Patent Act.

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

September 22, 2017

Chief administrative judge: TAKAGI, Susumu

Administrative judge: ISHII, Shigekazu

Administrative judge: SUDA, Katsumi