

based on the presentation pattern 291 are input from the keyboard 296. The one-time password transmission means 257 transmits the input one-time password 292 to the authentication server 201. The one-time password reception means 207 at the authentication server 201 receives the one-time password 292. The verification code generation means 206 generates a verification code 293 which is a result of applying the one-time password deriving rule 202b associated with the received user ID 281 to the transmitted pattern element sequence 290. The user authentication means 208 compares the received one-time password 292 with the verification code 293 and makes authentication of the user successful in a case where the one-time password 292 matches the verification code 293.

Citation List

Patent Literature

[0008]

Patent Literature 1: Japanese Patent Laid-Open No. 2007-264839

Summary of Invention

Technical Problem

[0009]

In a matrix authentication system in related art, first, a user ID is input on a user ID input screen at an authentication request client and transmitted to an authentication server, and then, pattern elements, or the like, constituting a presentation pattern in a matrix are transmitted from the authentication server to the authentication request client. The user then inputs a one-time password which is a response to the presentation pattern after the presentation pattern is displayed. In other words, it is necessary to input a user ID and then input a one-time password on another screen. Such an authentication method in related art which requires switching of display between two screens for authentication does not necessarily excel in

user-friendliness. It is therefore necessary to provide a system which eliminates the need for a user ID input step and which achieves both identification and authentication of a user ID with only one step of inputting a one-time password at the same time to improve the user-friendliness.

5

Solution to Problem

[0010]

The present invention has been made in view of the above-described problem and has the following features. ~~In other words, the present~~

10 ~~invention is~~ In a first aspect, the present disclosure refers to a user

authentication system designed to use, as a password of a user who is to be authenticated, a one-time password deriving rule for generating a one-time

password by being applied to pattern elements at specific positions in a case where a plurality of pattern elements arranged in a predetermined pattern

15 are presented to the user as a presentation pattern, and authenticates the user on the basis of a character string for authentication in which a user ID is embedded at a predetermined embedding position within the one-time password, the user authentication system including an authentication server and an authentication request client, in which

20 the authentication server includes:

a password storage unit 102 configured to store a user ID 102a of the user, the one-time password deriving rule 102b of the user, and a user ID embedding position 102c which identifies an embedding position at which the user ID is to be embedded within the one-time password, in advance in
25 association with one another for each said user ID;

presentation pattern determination information generation means
111 for generating presentation pattern determination information which determines the presentation pattern using a predetermined generation rule;

verification code generation means 106 for generating a verification
30 code in which the user ID is embedded on ~~the a~~ basis of the user ID embedding

position, in a result of applying the one-time password deriving rule associated with the user ID to the pattern elements constituting the presentation pattern determined on ~~the~~a basis of the presentation pattern determination information, for each said user ID; and

5 presentation pattern determination information transmission means 112 for transmitting the generated presentation pattern determination information to the authentication request client of the user who is to be authenticated,

the authentication request client includes:

10 presentation pattern determination information reception means 161 for receiving the presentation pattern determination information transmitted from the authentication server;

pattern element determination means 162 for determining pattern elements constituting the presentation pattern on the basis of the presentation pattern determination information;

15 pattern display means 155 for arranging the determined pattern elements in the predetermined pattern to generate a presentation pattern and displaying the presentation pattern on a screen;

authentication character string input means 156 for accepting input of a character string for authentication in which the user ID is embedded at the user ID embedding position in a one-time password which is a result of applying the one-time password deriving rule to the pattern elements included in the presentation pattern, from the user who is to be authenticated; and

25 authentication character string transmission means 157 for transmitting the input character string for authentication to the authentication server, and

the authentication server further includes:

authentication character string reception means 107 for receiving the character string for authentication from the authentication request client;

and

user authentication means 108 for comparing the received character string for authentication with the verification code generated for each said user ID and making authentication of the user ID corresponding to the verification code successful in a case where the verification code which matches the received character string for authentication exists.

[0011]

In the present [inventionexample](#), the presentation pattern determination information can be the pattern elements constituting the presentation pattern. Further, in the present [inventionexample](#), the presentation pattern determination information can be a pattern seed value which generates the pattern elements constituting the presentation pattern by being applied to a predetermined pattern element sequence generation rule. Still further, in the present [inventionexample](#), in a case where the verification code which matches two or more user IDs exists, the verification code generation means can repeat generation of the verification code for the user ID on the basis of the presentation pattern determination information newly generated by the presentation pattern determination information generation means until the verification code which matches two or more user IDs no longer exists. Further, in the present [inventionexample](#), the authentication character string transmission means stores the input character string for authentication, hashes the input character string for authentication with a hash function and transmits the hashed character string for authentication to the authentication server,

the user authentication means can compare the received hashed character string for authentication with a hashed verification code obtained by hashing the verification code generated for each said user ID with the hash function, and, in a case where the hashed verification code matches the received hashed character string for authentication, transmit the user ID embedding position corresponding to the verification code and a length of a

character string of the user ID to the authentication request client to inquire about the user ID within the character string for authentication, and in a case where the user ID obtained through the inquiry matches the user ID corresponding to the verification code, make authentication of the user ID successful.

[0011a]

In a second aspect, the present disclosure refers to a user authentication method designed to use, as a password of a user who is to be authenticated, a one-time password deriving rule for generating a one-time password by being applied to pattern elements at specific positions in a case where a plurality of pattern elements arranged in a predetermined pattern are presented to the user as a presentation pattern, and authenticates the user on a basis of a character string for authentication in which a user ID is embedded at a predetermined embedding position within the one-time password, and which is to be executed by an authentication server and an authentication request client, the user authentication method comprising steps of: storing, by the authentication server, the user ID of the user, the one-time password deriving rule of the user, and a user ID embedding position which identifies an embedding position at which the user ID is to be embedded within the one-time password in association with one another in advance for each said user ID; generating, by the authentication server, presentation pattern determination information which determines the presentation pattern using a predetermined generation rule; generating, by the authentication server, a verification code obtained in which the user ID is embedded on a basis of the user ID embedding position, in a result of applying the one-time password deriving rule associated with the user ID to the pattern elements constituting the presentation pattern determined on a basis of the presentation pattern determination information for each said user ID; transmitting, by the authentication server, the generated presentation pattern determination information to the authentication request client of the

user who is to be authenticated; receiving, by the authentication request client, the presentation pattern determination information transmitted from the authentication server; determining, by the authentication request client, pattern elements constituting the presentation pattern on a basis of the received presentation pattern determination information; arranging, by the authentication request client, the determined pattern elements in the predetermined pattern to generate a presentation pattern and displaying the presentation pattern on a screen; accepting, by the authentication request client, input of a character string for authentication in which the user ID is embedded at the user ID embedding position in a one-time password which is a result of applying the one-time password deriving rule to the pattern elements included in the presentation pattern, from the user who is to be authenticated; transmitting, by the authentication request client, the input character string for authentication to the authentication server; receiving, by the authentication server, the character string for authentication from the authentication request client; and comparing, by the authentication server, the received character string for authentication with the verification code generated for each said user ID and making authentication of the user ID corresponding to the verification code successful in a case where the verification code which matches the received character string for authentication exists.

[0011b]

In a third aspect, the present disclosure refers to an authentication server designed to use, as a password of a user who is to be authenticated, a one-time password deriving rule for generating a one-time password by being applied to pattern elements at specific positions in a case where a plurality of pattern elements arranged in a predetermined pattern are presented to the user as a presentation pattern, and authenticates the user on a basis of a character string for authentication in which a user ID is embedded at a predetermined embedding position within the one-time password, and which

is connected to an authentication request client, the authentication server comprising: a password storage unit configured to store the user ID of the user, the one-time password deriving rule of the user, and a user ID embedding position which identifies an embedding position at which the user ID is to be embedded within the one-time password in association with one another in advance for each said user ID; presentation pattern determination information generation means for generating presentation pattern determination information which determines the presentation pattern using a predetermined generation rule; verification code generation means for generating a verification code in which the user ID is embedded on a basis of the user ID embedding position, in a result of applying the one-time password deriving rule associated with the user ID to the pattern elements constituting the presentation pattern determined on a basis of the presentation pattern determination information for each said user ID; presentation pattern determination information transmission means for transmitting the generated presentation pattern determination information to the authentication request client of the user who is to be authenticated; authentication character string reception means for receiving a character string for authentication in which the user ID is embedded at the user ID embedding position in a one-time password which is a result of applying the one-time password deriving rule to pattern elements included in the presentation pattern determined on a basis of the presentation pattern determination information, transmitted from the authentication request client; and user authentication means for comparing the received character string for authentication with the verification code generated for each said user ID and making authentication of the user ID corresponding to the verification code successful in a case where the verification code which matches the received character string for authentication exists.

[0011c]

In a fourth aspect, the present disclosure refers to a user authentication

method designed to use, as a password of a user who is to be authenticated, a one-time password deriving rule for generating a one-time password by being applied to pattern elements at specific positions in a case where a plurality of pattern elements arranged in a predetermined pattern are presented to the user as a presentation pattern, and authenticates the user on a basis of a character string for authentication in which a user ID is embedded at a predetermined embedding position within the one-time password, and which is to be executed by an authentication server connected to an authentication request client, the user authentication method comprising steps of: storing the user ID of the user, the one-time password deriving rule of the user, and a user ID embedding position which identifies an embedding position at which the user ID is to be embedded within the one-time password in association with one another in advance for each said user ID; generating presentation pattern determination information which determines the presentation pattern using a predetermined generation rule; generating a verification code in which the user ID is embedded on a basis of the user ID embedding position in a result of applying the one-time password deriving rule associated with the user ID to the pattern elements constituting the presentation pattern determined on a basis of the presentation pattern determination information, for each said user ID; transmitting the generated presentation pattern determination information to the authentication request client of the user who is to be authenticated; receiving a character string for authentication in which the user ID is embedded at the user ID embedding position in a one-time password which is a result of applying the one-time password deriving rule to pattern elements included in the presentation pattern determined on a basis of the presentation pattern determination information, transmitted from the authentication request client; and comparing the received character string for authentication with the verification code generated for each said user ID and making authentication of the user ID corresponding to the verification code successful

in a case where the verification code which matches the received character string for authentication exists.

[0012]

The present invention-example is also embodied as a user authentication method using the above-described user authentication system, an authentication server for realizing such a user authentication system, and a user authentication method to be executed at such an authentication server.

[0013]

In the invention-example described above or recited in the claims, terms such as a server and a client do not limit specific forms or specific name of apparatuses and represent apparatuses including general functions of the apparatuses. Functions of one component may be implemented with two or more physical components or functions of two or more components may be implemented with one physical component. The invention-example of the system can be grasped as the invention-example of the method in which functions of the respective components are sequentially executed, and vice versa. In the invention-example of the method, execution order of respective steps is not limited to the described order, and the respective steps can be executed in free order as long as the functions can be executed without causing inconsistency as a whole. These inventions-examples are also embodied as a program for implementing predetermined functions in cooperation with predetermined hardware and also embodied as a recording medium in which the program is recorded.

Advantageous Effects of Invention

[0014]

The present invention-example provides that as a result of employing a configuration where a one-time password deriving rule for generating a one-

time password by being applied to pattern elements at specific positions in a case where a plurality of pattern elements arranged in a predetermined pattern are presented to a user who is to be authenticated as a presentation pattern, is used as a password of the user, the user is authenticated on the basis of a character string for authentication in which a user ID is embedded at a predetermined embedding position within the one-time password, and at that time, a correct character string for authentication for the presented presentation pattern is generated for all user IDs as a verification code, and in a case where the verification code which matches the character string for authentication input from the user exists, user authentication of the user ID corresponding to the verification code is made successful, it is not necessary to specify the user by inputting the user ID to an authentication system upon start of authentication, and it is possible to perform both specification of the user and confirmation of authenticity of the user by inputting a single character string for authentication upon authentication, so that it is possible to provide effects of eliminating the need for inputting the user ID before inputting the password upon authentication and eliminating the need for switching display between two screens for authentication. In other words, the present [invention-example](#) provides effects of eliminating the need for a user ID input step, and enabling both identification and authentication of the user ID to be performed at the same time through only one step of inputting a character string including a one-time password.

Brief Description of Drawings

[0015]

[Figure 1] Figure 1 is a hardware configuration diagram of a user authentication system 100 according to an embodiment of the present invention.

[Figure 2] Figure 2 is a functional block diagram of the user authentication system 100 according to an embodiment of the present invention.