

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 [0010]

The present invention has been made in view of the above-described problem and has the following features. In a first aspect, the present disclosure refers to a user authentication system designed to use, as a password of each of users who is to be authenticated, a one-time password  
10 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 each of the users as a presentation pattern, and authenticates said each of the users on the basis of a character string for authentication in which each of user IDs is embedded  
15 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

the authentication server includes:

a password storage unit 102 configured to store the user IDs 102a of  
20 the users, the one-time password deriving rules 102b of the users, and user ID embedding positions 102c which identify embedding positions at which each of the user IDs is to be embedded within the one-time password, in advance in association with one another for each of the said user IDs;

presentation pattern determination information generation means  
25 111 for generating presentation pattern determination information which determines the presentation pattern using a predetermined generation rule;

verification code generation means 106 for generating each of verification codes in which each of the user IDs is embedded on a basis of each of the user ID embedding

positions, in a result of applying each of the one-time password deriving rules associated with each of the user IDs to the pattern elements constituting the presentation pattern determined on a basis of the presentation pattern determination information, for each of the user IDs; 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  
15 presentation pattern determination information;

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  
20 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  
30 character string for authentication from the authentication request client;

and

user authentication means 108 for comparing the received character string for authentication with each of the verification codes generated for each of the user IDs 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 example, the presentation pattern determination information can be the pattern elements constituting the presentation pattern. Further, in the present example, 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 example, 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 example, 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 each of users 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 said each of the users as a presentation pattern, and authenticates said each of the users on a basis of a character string for authentication in which each of user IDs 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 IDs of the users, the one-time password deriving rules of the users, and user ID embedding positions which identify embedding positions at which each of the user IDs is to be embedded within the one-time password in association with one another in advance for each of the user IDs; generating, by the authentication server, presentation pattern determination information which determines the presentation pattern using a predetermined generation rule; generating, by the authentication server, each of verification codes in which each of the user IDs is embedded on a basis of each of the user ID embedding positions, in a result of applying each of the one-time password deriving rules 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 of the user IDs; 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 each of the verification codes generated for each of the user IDs 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 each of users 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 each of the users as a presentation pattern, and authenticates each of the users on a basis of a character string for authentication in which each of user IDs is embedded at a predetermined  
5 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 IDs of the users, the one-time password deriving rules of the users, and user ID embedding positions which identify embedding positions at which each of the user IDs is to be  
10 embedded within the one-time password in association with one another in advance for each of the user IDs; 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  
15 generating each of verification codes in which each of the user IDs is embedded on a basis of each of the user ID embedding positions, in a result of applying each of the one-time password deriving rules associated with each of the user IDs to the pattern elements constituting the presentation pattern determined on a basis of the presentation pattern determination information  
20 for each of the user IDs; 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  
25 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  
30 the received character string for authentication with each of the verification

codes generated for each of the user IDs 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.

5 [0011c]

In a fourth aspect, the present disclosure refers to a user authentication method designed to use, as a password of each of users 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  
10 where a plurality of pattern elements arranged in a predetermined pattern are presented to said each of the users as a presentation pattern, and authenticates said each of the users on a basis of a character string for authentication in which each of user IDs is embedded at a predetermined embedding position within the one-time password, and which is to be  
15 executed by an authentication server connected to an authentication request client, the user authentication method comprising steps of: storing the user IDs of the users, the one-time password deriving rules of the users, and user ID embedding positions which identify embedding positions at which each of the user IDs is to be embedded within the one-time password in association  
20 with one another in advance for each of the user IDs; generating presentation pattern determination information which determines the presentation pattern using a predetermined generation rule; generating each of verification codes in which each of the user IDs is embedded on a basis of each of the user ID embedding positions, in a result of applying each of the one-  
25 time password deriving rules associated with each of the user IDs to the pattern elements constituting the presentation pattern determined on a basis of the presentation pattern determination information, for each of the user IDs; transmitting the generated presentation pattern determination information to the authentication request client of the user who is to be  
30 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 each of the verification codes generated for each of the user IDs 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 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 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 example of the system can be grasped as the example of the method in which functions of the respective components are sequentially executed, and vice versa. In the 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 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.

[0014]

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

## Claims

### [Claim 1]

A user authentication system designed to use, as a password of each  
5 of users 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 said each of the users as a  
presentation pattern, and authenticates said each of the users on a basis of a  
10 character string for authentication in which each of user IDs is embedded at  
a predetermined embedding position within the one-time password, the user  
authentication system comprising:

an authentication server; and

an authentication request client,

15 wherein the authentication server comprises:

a password storage unit configured to store the user IDs of the users,  
the one-time password deriving rules of the users, and user ID embedding  
positions which identify embedding positions at which each of the user IDs is  
to be embedded within the one-time password, in advance in association with  
20 one another for each of the user IDs;

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

25 verification code generation means for generating each of verification  
codes in which each of the user IDs is embedded on a basis of each of the user  
ID embedding positions, in a result of applying each of the one-time password  
deriving rules associated with each of the user IDs to the pattern elements  
constituting the presentation pattern determined on a basis of the  
presentation pattern determination information for each of the user IDs; and

30 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,

the authentication request client comprises:

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

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

pattern display means 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 for accepting input of a  
15 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

20 authentication character string transmission means for transmitting the input character string for authentication to the authentication server, and the authentication server further comprises:

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

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

[Claim 2]

The user authentication system according to claim 1,  
wherein the presentation pattern determination information is the  
pattern elements constituting the presentation pattern.

5 [Claim 3]

The user authentication system according to claim 1,  
wherein the presentation pattern determination information is a  
pattern seed value which generates the pattern elements constituting the  
presentation pattern by being applied to a predetermined pattern element  
10 sequence generation rule.

[Claim 4]

The user authentication system according to any one of claims 1 to 3,  
wherein, in a case where the verification code which matches two or  
more user IDs exists, the verification code generation means repeats  
15 generation of the verification codes for each of the user IDs on a 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.

[Claim 5]

20 The user authentication system according to claim 4,  
wherein 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, and  
25 the user authentication means compares the received hashed  
character string for authentication with hashed verification codes obtained  
by hashing the verification codes generated for each of the user IDs with the  
hash function, and, in a case where the hashed verification code which  
matches the received hashed character string for authentication exists,  
30 transmits the user ID embedding position corresponding to the verification

code 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, makes authentication of the user ID successful.

5 [Claim 6]

A user authentication method designed to use, as a password of each of users 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  
10 a predetermined pattern are presented to said each of the users as a presentation pattern, and authenticates said each of the users on a basis of a character string for authentication in which each of user IDs 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  
15 request client, the user authentication method comprising steps of:

storing, by the authentication server, the user IDs of the users, the one-time password deriving rules of the users, and user ID embedding positions which identify embedding positions at which each of the user IDs is to be embedded within the one-time password in association with one another  
20 in advance for each of the user IDs;

generating, by the authentication server, presentation pattern determination information which determines the presentation pattern using a predetermined generation rule;

generating, by the authentication server, each of verification codes in  
25 which each of the user IDs is embedded on a basis of each of the user ID embedding positions, in a result of applying each of the one-time password deriving rules associated with each of the user IDs to the pattern elements constituting the presentation pattern determined on a basis of the presentation pattern determination information for each of the user IDs;

30 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 each of the verification codes generated for each of the user IDs 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.

[Claim 7]

The user authentication method according to claim 6,

wherein the presentation pattern determination information is the pattern elements constituting the presentation pattern.

[Claim 8]

The user authentication method according to claim 6,

wherein the presentation pattern determination information is a pattern seed value which generates the pattern elements constituting the presentation pattern by being applied to a predetermined pattern element sequence generation rule.

[Claim 9]

The user authentication method according to any one of claims 6 to 8,

wherein, in the step of generating the verification codes, in a case where the verification code which matches two or more user IDs exists, generation of the verification codes for each of the user IDs on a basis of the presentation pattern determination information newly generated in the step of generating the presentation pattern determination information is repeated until the verification code which matches two or more user IDs no longer exists.

[Claim 10]

The user authentication method according to claim 9,

wherein the step of transmitting the input character string for authentication to the authentication server includes storing the input character string for authentication, hashing the input character string for authentication with a hash function and transmitting the hashed character string for authentication to the authentication server, and

comparing the received character string for authentication with the verification code generated for each of the user IDs, and in a case where the verification code which matches the received character string for authentication exists, making authentication of the user ID corresponding to the verification code successful includes comparing the received hashed character string for authentication with each of hashed verification codes obtained by hashing the verification codes generated for each of the user IDs with the hash function, and in a case where the hashed verification code which matches the received hashed character string for authentication exists,

transmitting 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  
5 matches the user ID corresponding to the verification code, making authentication of the user ID successful.

[Claim 11]

An authentication server designed to use, as a password of each of users who is to be authenticated, a one-time password deriving rule for  
10 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 said each of the users as a presentation pattern, and authenticates said each of the users on a basis of a character string for authentication in which each of user IDs is embedded at  
15 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 IDs of the users, the one-time password deriving rules of the users, and user ID embedding  
20 positions which identify embedding positions at which each of the user IDs is to be embedded within the one-time password in association with one another in advance for each of the user ID;

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

verification code generation means for generating each of verification codes in which each of the user IDs is embedded on a basis of each of the user ID embedding positions, in a result of applying each of the one-time password deriving rules associated with each of the user IDs to the pattern elements  
30 constituting the presentation pattern determined on a basis of the

presentation pattern determination information for each of the user IDs;

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 each of the verification codes generated for each of the user IDs 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.

[Claim 12]

A user authentication method designed to use, as a password of each of users 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 said each of the users as a presentation pattern, and authenticates said each of the users on a basis of a character string for authentication in which each of user IDs 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 IDs of the users, the one-time password deriving rules

of the users, and user ID embedding positions which identify embedding positions at which each of the user IDs is to be embedded within the one-time password in association with one another in advance for each of the user IDs;

generating presentation pattern determination information which

5 determines the presentation pattern using a predetermined generation rule;

generating each of verification codes in which each of the user IDs is embedded on a basis of each of the user ID embedding positions, in a result of applying each of the one-time password deriving rules associated with each of the user IDs to the pattern elements constituting the presentation pattern

10 determined on a basis of the presentation pattern determination information, for each of the user IDs;

transmitting the generated presentation pattern determination information to the authentication request client of the user who is to be authenticated;

15 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

20 comparing the received character string for authentication with each of the verification codes generated for each of the user IDs 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.