Method and Apparatus for Video Authentication Of User

Field of the Invention

The present invention relates to network communication technologies, and more particularly, to a method and apparatus for performing video authentication on a user.

Background of the Invention

In an existing video authentication technology, it is required for a user to upload one photo in advance, and a photo of the user is taken by a video capture interface. Resolution of the video capture interface is 100×100. Then video authentication of the user is performed by a video real-time capture queue. In generally, as far as the photo uploaded by the user and the photo taken by the video capture interface are enough clear, the user may pass the video authentication.

During the process of achieving the present invention, the inventors find that above-mentioned existing video authentication technology has the following defects: the method does not compare the photo uploaded by the user with the photo taken by the video capture interface, thus can not overcome the problem of performing falsification on authentication photo by using a virtual camera. The size of the photo taken by the video capture interface is only 100×100, so the photo is not clear and is difficult to be identified.

In another existing video authentication technology, it is also required for a user to upload one photo in advance, and a photo of the user is taken by a camera. Then the system compares the photo taken by the camera with the photo uploaded by the user in a manual identification mode, and gives video authentication result in 72 hours according to a comparison result.

During the process of achieving the present invention, the inventors find that above-mentioned another existing video authentication technology has the following defects: the method causes the user to wait for too long a time. A single video photo is taken as the basis for video authentication can not overcome the problem of performing falsification on authentication photo by using a virtual camera, too.

Summary of the Invention

Embodiments of the present invention provide a method and apparatus for performing video authentication on users, so as to overcome the problem of performing falsification on authentication photo by using a virtual camera.

The method for performing video authentication on a user, including:

receiving an authentication photo submitted by a user;

capturing a continuous real-time video of the user within a period of time through a video pic-up device in a client of the user; decomposing the real-time video, and obtaining multiple video data frames; selecting a specific number of video data frames from the multiple video data frames, and generating at least one contrast picture for video authentication to the user based on the specific number of video data frames;

comparing the authentication photo with the contrast picture, and determining a video authentication result of the user according to a comparison result.

The apparatus for performing video authentication on a user, including:

an authentication photo obtaining module, configured to receive an authentication photo submitted by a user;

a contrast photo obtaining module, configured to capture a continuous real-time video of the user within a period of time through a video pic-up device in a client of the user, decompose the real-time video, and obtain multiple video data frames, select a specific number of video data frames from the multiple video data frames, and generate at least one contrast picture for video authentication to the user based on the specific number of video data frames;

a comparison determination module, configured to compare the authentication photo with the contrast picture, and determine a video authentication result of the user according to a comparison result.

As can be seen from the above technical solutions provided by embodiments of the present invention, in embodiments of the present invention, real-time video of the user is captured automatically and a contrast picture is generated according to data of the real-time video, the contrast picture is compared with an authentication photo submitted by the user and basic information of the user. Therefore, accurate and timely video authentication may be performed on the user, and the user may be prevented from

performing falsification on authentication photo by using a virtual camera.

Brief Description of Drawings

In order to make technical solutions of embodiments of the present invention clearer, accompanying drawings to be used in description of the embodiments will be simply introduced hereinafter. Obviously, the accompanying drawings to be described hereinafter

are only some embodiments of the present invention. Those skilled in the art may obtain other drawings according to these accompanying drawings without creative labor.

Figure 1 is a flowchart illustrating a method for performing video authentication on a user provided by a first embodiment of the present invention;

Figure 2 is a schematic diagram illustrating an apparatus for performing video authentication on a user provided by a second embodiment of the present invention.

Detailed Description of the Invention

In the present invention, an authentication photo submitted by a user is received, continuous real-time video of the user is captured by a video pic-up device in a client of the user, and a contrast picture is generated according to data of the real-time video. Then the authentication photo is compared with the contrast picture, and a video authentication result of the user is determined according to a comparison result.

Furthermore, the authentication photo of the user may be taken by a video pic-up device installed on a terminal, and the client may submit user information comprising the authentication photo, sex and age to a network server. The network server receives the user information.

In addition, the network server may perform detection on the authentication photo according to pixels of the authentication photo. When determining that the authentication photo is unqualified, the network server informs the user to submit an authentication photo again.

Moreover, the video pic-up device may include a Flash-based video capture camera, and a Flash controller in a terminal invokes the video capture camera to capture the real-time video of the user.

The video pic-up device automatically captures a continuous real-time video of the user within a period of time. The real-time video is decomposed and multiple video data frames are obtained. A specific number of video data frames are selected from the multiple video data frames, and at least one contrast picture for video authentication is generated based on the specific number of video data frames.

A specific number of video data frames are selected from the multiple video data frames according to a predetermined interval.

Furthermore, when the multiple video data frames include action information of the

user, the video data frames corresponding to the action information of the user are selected from the multiple video data frames.

In addition, besides authentication photo submitted by the user and the contrast picture generated are obtained, gender and age information of the user may be also obtained.

After it is determined that the authentication photo and the contrast picture belong to the same user, it may be further determined that whether the authentication photo and the contrast picture conform to the gender and age information of the user, if the authentication photo and the contrast picture conform to the gender and age information of the user, then the user is notified via the client that the user passes the video authentication, otherwise, the user is notified via the client that the user does not pass the video authentication.

For better understanding of technical solutions provided by embodiments of the present invention, the present invention will be described in detail hereinafter in some specific embodiments with reference to accompanying drawings. The embodiments are not used for limiting the protection scope of the present invention.

A first embodiment

Figure 1 is a flowchart illustrating a method for performing video authentication on a user provided by the first embodiment of the present invention, the method includes the following processes.

Step 11, a client submits an authentication photo of a user taken by a video pic-up device and basic information of the user to a network server in background.

When logging in a service system which needs video authentication, the user turns on the video pic-up device installed on a computer first, adjusts various parameters of the video pic-up device, and takes one authentication photo of the user through the video pic-up device. The user may take the authentication photo repeatedly so as to obtain the most satisfied photo. Then, the user stores the above-mentioned authentication photo in the computer. The authentication photo may also be taken via other camera device, and then be stored in the computer. For example, the authentication photo may be taken via a digital camera, and then be stored in the computer.

The user fills in his/her basic information, such as gender and age, via a login interface. The client obtains user information, such as above-mentioned authentication photo, gender and age, and submits the user information to the network server in

background.

In practical application, above-mentioned video pic-up device may be a Flash-based video pic-up camera, or other video capture tools, controllers or software. The size of

above-mentioned authentication photo may be set to 240×240, so as to obtain user information as much as possible in video environment.

In practical application, in order to guarantee the speed of video authentication of the user, a restriction may be imposed on the number of users requesting authentication. A threshold may be set for the total number of clients submitting above-mentioned user information. When the total number reaches the threshold, the client can't submit user information to the network server in background. At this time, the system will remind the client that it is busy currently, there are many users waiting for video authentication, and please submit user information later. Above-mentioned total number of clients corresponds to that of users.

Step 12, the video pic-up device automatically captures a continuous real-time video of the user, and a contrast picture for user video authentication is generated based on data of the real-time video.

After the authentication photo of the user is uploaded to the network server in background, a video authentication interface of the user is entered.

Firstly, the network server in background determines whether the quality of the authentication photo is qualified. The determining whether the quality of the authentication photo is qualified is implemented mainly by determining whether the photo is clear through analyzing the exposure of the initial photo. The photo which has been overexposed or has poor light is treated as unqualified one. After determining that the authentication photo is unqualified, the network server in background notifies, through the client, the user to resubmit a clear authentication photo.

After determining that the authentication photo is qualified, the network server in background notifies, through the client, the user that he should guarantee the front of the user being presented in a video frame of the video pic-up device, and keep in natural action, so to facilitate the system to perform video authentication on him; and notifies the user that the video authentication needs some time, and please be patient.

Whereafter, the above-mentioned video pic-up device automatically captures a continuous real-time video of the user within a specific period of time. Data of the continuous real-time video is decomposed and multiple video data frames are obtained. A specific number of video data frames are selected from the multiple video data frames, to generate one contrast picture for video authentication. In practical application, multiple contrast pictures may be generated based on different video data frames selected

separately as required. The specific period of time may be set to 30 seconds, 40 seconds, one minute, or the like.

The operation of selecting a specific number of video data frames may be performed according to a predetermined interval (such as 2 seconds). The specific number may be 1, 3, 5, 10, or the like.

If the user makes some actions in the process of video authentication, the continuous real-time video will include some action information of the user. The video data frames corresponding to the action information of the user may be selected to generate above-mentioned contrast picture(s). Thus real-time photo of the user may be obtained accurately.

Step 13, comparison between the authentication photo, the contrast picture and basic information of the user is performed to determine a video authentication result of the user.

The network server in background sends in time the authentication photo and basic information submitted by the user, and the contrast picture generated by the video pic-up device to manual client service or face recognition software.

The manual client service or the face recognition software needs to compare the authentication photo with the contrast picture, to determine whether they belong to the same user, and needs to determine whether the authentication photo and the contrast picture conform to the basic information of the user, such as gender and age.

After the manual client service or the face recognition software determines that the authentication photo and the contrast picture belong to the same user, and conform to the basic information of the user, the system notifies in time, through the client, the user that the user passes the video authentication, otherwise, the system notifies in time, through the client, the user that the user does not pass the video authentication.

A second embodiment

An apparatus for performing video authentication on a user is also provided by an embodiment of the present invention. The specific structure of the apparatus is shown in figure 2, and the apparatus includes the following modules.

An authentication photo obtaining module 21, configured to receive an authentication photo submitted by a user.

A contrast photo obtaining module 22, configured to capture a continuous real-time video of the user through a video pic-up device in a client of the user, and generate a contrast picture according to data of the real-time video.

A comparison determination module 23, configured to compare the authentication photo with the contrast picture, and determine a video authentication result of the user according to a comparison result.

The contrast photo obtaining module 22 may include:

A real-time video obtaining module 221, configured to automatically capture a continuous real-time video of the user within a period of time through the video pic-up device, decompose the real-time video, and obtain multiple video data frames.

A contrast picture generating module 222, configured to select a specific number of video data frames from the multiple video data frames, generate at least one contrast picture for video authentication to the user based on the specific number of video data frames.

The comparison determination module 23 may include:

An information obtaining module 231, configured to obtain the contrast picture generated, and authentication photo, gender and age information of the user submitted by the user.

A image identification module 232, configured to, after it is determined, through manual client service or face recognition software, that the authentication photo and the contrast picture belong to the same user, and the authentication photo and the contrast picture conform to the gender and age information of the user, determine that the user passes the video authentication; otherwise, determine that the user does not pass the video authentication.

Those skilled in the art may understand that all or part of the processes of above-mentioned method may be implemented by relevant computer hardware which is instructed by computer program. The program may be stored in a computer-readable storage media. When the program is executed, relevant hardware can perform the processes of the method in above-mentioned embodiment. The storage media may be a diskette, an optical disk, a Read-Only Memory (ROM), a Random Access Memory (RAM), or the like.

As stated previously, embodiments of the present invention automatically capture the real-time video of the user, generate the contrast picture, and perform comparison between the authentication photo, the contrast picture through, and basic information of the user through manual client service or program, therefore accurate video authentication on the user may be performed, and t the user may be prevented from performing

falsification on authentication photo by using a virtual camera.

The embodiments of the present invention can achieve an effect on either user experience or credibility of authentication close to that achieved by the scene that manual client service and the user have a one-to-one video chat. In general, the substance of the video is also a process of high-speed transmission and picture playing. The present invention combines video pictures, through Flash technology in browser side, for simulating video. Thus the procedure of network data transmission and operation between manual client service and the user is decreased.

Embodiments of the present invention may also make the user obtain the authentication result in time, thus improves the application effect for the user. In embodiments of the present invention, the size of the video picture is 240×240, thus picture information of the user in initial video environment may be restored as much as possible.

Embodiments of the present invention places a effective constraint on a real-time requesting queue, impose a rational restriction on the number of users requesting authentication. A threshold is set for the total number of users submitting above-mentioned user information. When the total number reaches the threshold, the user can't submit user information to the network server in background, thus guarantees the server load balance and high-quality, high-efficiency authentication service.

The foregoing description is only preferred embodiments of the present invention and is not used for limiting the protection scope thereof. Any modification, equivalent substitution, or improvement made without departing from the spirit and principle of the present invention should be covered by the protection scope of the present invention. Hence, the protection scope of the present invention should be determined by the protection scope of the claims.

Claims

1. A method for performing video authentication on a user, comprising:

receiving an authentication photo submitted by a user;

capturing a continuous real-time video of the user within a period of time through a video pic-up device in a client of the user; decomposing the real-time video, and obtaining multiple video data frames; selecting a specific number of video data frames from the multiple video data frames, and generating at least one contrast picture for video authentication to the user based on the specific number of video data frames;

comparing the authentication photo with the contrast picture, and determining a video authentication result of the user according to a comparison result.

2. The method according to claim 1, wherein the authentication photo is taken through a video pic-up device installed on a terminal;

before comparing the authentication photo with the contrast picture, the method further comprises: submitting, by the client, user information comprising the authentication photo to a network server; receiving, by the network server, the user information;

comparing, by the network server, the authentication photo with the contrast picture, and determining the video authentication result of the user according to a comparison result.

3. The method according to claim 2, further comprising:

detecting, by the network server, the authentication photo according to pixels of the authentication photo;

when determining the authentication photo is unqualified, notifying, by the network server, the client that an authentication photo is to be submitted again.

4. The method according to claim 1, wherein a Flash-based video capture camera in the video pic-up device is invoked by a Flash controller in a terminal to capture the real-time video of the user.

5. The method according to claim 1, wherein selecting a specific number of video data frames from the multiple video data frames comprises:

selecting a specific number of video data frames from the multiple video data frames according to a predetermined interval.

6. The method according to claim 1, wherein selecting a specific number of video

data frames from the multiple video data frames comprises:

when the multiple video data frames include action information of the user, selecting the video data frames corresponding to the action information of the user from the multiple video data frames.

7. The method according to claim 2, wherein the user information comprises gender and age information of the user;

wherein comparing the authentication photo with the contrast picture, and determining a video authentication result of the user according to a comparison result comprises:

determining whether the authentication photo and the contrast picture belong to the same user, and whether the authentication photo and the contrast picture conform to the gender and age information of the user;

if the authentication photo and the contrast picture belong to the same user, and the authentication photo and the contrast picture conform to the gender and age information of the user, determining that the user passes the video authentication; otherwise, determining that the user does not pass the video authentication.

8. A apparatus for performing video authentication on a user, comprising:

an authentication photo obtaining module, configured to receive an authentication photo submitted by a user;

a contrast photo obtaining module, configured to capture a continuous real-time video of the user within a period of time through a video pic-up device in a client of the user, decompose the real-time video, and obtain multiple video data frames, select a specific number of video data frames from the multiple video data frames, and generate at least one contrast picture for video authentication to the user based on the specific number of video data frames;

a comparison determination module, configured to compare the authentication photo with the contrast picture, and determine a video authentication result of the user according to a comparison result.

9. The apparatus according to claim 8, wherein the contrast photo obtaining module comprises:

a real-time video obtaining module, configured to automatically capture a continuous real-time video of the user within a period of time through the video pic-up device, decompose the real-time video, and obtain multiple video data frames;

a contrast picture generating module, configured to select a specific number of video data frames from the multiple video data frames, and generate at least one contrast picture for video authentication to the user based on the specific number of video data frames.

10. The apparatus according to claim 8 or 9, wherein the comparison determination module comprises:

an information obtaining module, configured to obtain the contrast picture generated, and authentication photo, gender and age information of the user submitted by the user;

a image identification module, configured to, after it is determined that the authentication photo and the contrast picture belong to the same user, and the authentication photo and the contrast picture conform to the gender and age information of the user, determine that the user passes the video authentication; otherwise, determine that the user does not pass the video authentication.