

[DESCRIPTION]

[TITLE OF INVENTION]

METHOD AND APPARATUS FOR VERIFYING CERTIFICATE AND CERTIFICATE HOLDER

[Technical Field]

The invention relates to the field of computer technology, and in particular to a method and apparatus for verifying a certificate and a certificate holder.

[Background]

The anti-counterfeiting technology refers to some means capable of inhibiting counterfeit behaviors, which can greatly increase difficulties and costs of counterfeiting, or reduce a simulation degree of counterfeiting. The form anti-counterfeiting refers to anti-counterfeiting technologies outside of products, and generally has very strong adaptability and a longer anti-counterfeiting life cycle. Since it depends on anti-counterfeiting means outside of products, its anti-counterfeiting identification must be tightly combined with the product or the package thereof to form an inseparable whole. For example, technologies such as anti-tearing adhesive labels, hot stamping labels, direct printing or molding. At present, most anti-counterfeiting technologies and methods belong to form anti-counterfeiting, such as package anti-counterfeiting, password anti-counterfeiting, various anti-counterfeiting identifications or trademarks.

Image processing refers to a technique of analyzing, processing, and treating an image such that it meets visual, psychological, or other requirements. Image processing is an application of signal processing in the field of image. At present, most images are stored in a digital form, so image processing refers to as digital image processing in many cases. In addition, processing methods based on the optical theory still play an important role. Image processing is a subclass of signal processing, and has a close relationship with fields such as computer science and artificial intelligence.

With the popularization of the Internet, more and more online transactions are required. Online transactions require users to upload their personal certificate images, such as identification cards, passports, driver's licenses and the like, and in some cases it is needed to verify authenticity of the certificates.

[Summary of the Invention]

A brief summary of this disclosure is given below in order to provide a basic understanding of some aspects of this disclosure. However, it should be understood that this summary is not an exhaustive summary of this disclosure. It is not intended to identify critical or important elements of the disclosure, nor is it intended to be used to limit the scope of the disclosure. Its sole purpose is to present some concepts related to the disclosure in a simplified form as a prelude to the more detailed description that is presented later.

According to one aspect of this disclosure, a method of verifying a certificate and a certificate holder is provided, comprising the steps of:

- acquiring a video of the certificate with a specified series of projection angles in real time;

- extracting image features of the certificate under different projection angles in the video;

- verifying authenticity of the certificate according to the image features of the certificate;

- acquiring a human face video in real time;

- verifying whether it is a real person in the human face video;

- extracting image features of the human face in the human face video; and

- when the certificate is verified to be authentic and it is a real person in the human face video, comparing the image features of the certificate with the image features of the human face in the human face video, to determine whether the certificate holder is the owner of the certificate.

According to another aspect of this disclosure, an apparatus for verifying a certificate and a certificate holder is provided, comprising:

- a first video acquiring module for acquiring a video of the certificate with a specified series of projection angles in real time;

- a first extracting module for extracting image features of the certificate under different projection angles in the video;

- a first verifying module for verifying authenticity of the certificate according to the image features of the certificate;

- a second video acquiring module for acquiring a human face video in real time;

a second verifying module for verifying whether it is a real person in the human face video;

a second extracting module for extracting image features of the human face in the human face video; and

a comparing module for, when the certificate is verified to be authentic and it is a real person in the human face video, comparing the image features of the certificate with the image features of the human face in the human face video, to determine whether the certificate holder is the owner of the certificate.

According to still another aspect of this disclosure, an apparatus for verifying a certificate and a certificate holder is provided, comprising:

one or more processors;

a memory having stored thereon computer-executable instructions that, when executed by the one or more processors, cause the one or more processors to:

acquire a video of the certificate with a specified series of projection angles in real time;

extract image features of the certificate under different projection angles in the video;

verify authenticity of the certificate according to the image features of the certificate;

acquire a human face video in real time;

verify whether it is a real person in the human face video;

extract image features of the human face in the human face video; and

when the certificate is verified to be authentic and it is a real person in the human face video, compare the image features of the certificate with the image features of the human face in the human face video, to determine whether the certificate holder is the owner of the certificate.

According to yet another aspect of this disclosure, there is provided a computer-readable storage medium on which a computer program is stored, wherein when the program is executed by a processor, causes the processor to:

acquire a video of the certificate with a specified series of projection angles in real time;

extract image features of the certificate under different projection angles in the video;

verify authenticity of the certificate according to the image features of the

certificate;

acquire a human face video in real time;

verify whether it is a real person in the human face video;

extract image features of the human face in the human face video; and

when the certificate is verified to be authentic and it is a real person in the human face video, compare the image features of the certificate with the image features of the human face in the human face video, to determine whether the certificate holder is the owner of the certificate.

According to one or more embodiments of this disclosure, whether the certificate is currently held by the owner of the certificate can be further authenticated while authenticity of the certificate is effectively verified.

[Brief description of the drawings]

In order to more clearly illustrate the technical solutions in the embodiments of the invention, the drawings that are needed in the description of the embodiments are briefly discussed below, and obviously, the drawings described in the following are merely some embodiments of the invention, and other drawings can be obtained by those skilled in the art according to these drawings without creative work.

FIG. 1 is an exemplary flowchart of a method of verifying a certificate and a certificate holder in accordance with an embodiment of this disclosure;

FIG. 2 is an exemplary configuration block diagram of an apparatus for verifying a certificate and a certificate holder in accordance with an embodiment of this disclosure;

FIG. 3 is an exemplary configuration of a computing device capable of implementing the embodiments according to this disclosure.

[Detailed Description]

In order to make the objectives, technical solutions and advantages of the present invention clearer, the technical solutions in the embodiments of the invention will be described clearly and completely below with reference to the drawings in the embodiments of the invention, and it is apparent that the described embodiments are only some embodiments of the invention, but not all embodiments thereof. All other embodiments obtained by a person of ordinary skill in the art without making any creative work based on the embodiments of the invention fall within the scope of

protection of the invention.

In online transactions, sometimes it is required to upload a personal certificate image to verify authenticity of the certificate. One way the inventors of this disclosure know is to upload the certificate image. However, it cannot make sure that the certificate is authentic in this way, for example, it is possible to upload a counterfeit certificate image. In addition, it cannot make sure that the user who uploaded the certificate image is the certificate holder himself. Therefore, such a way possibly will pose a certain risk to the transaction.

The invention provides a method and apparatus for verifying a certificate and a certificate holder, which verify whether the certificate is authentic or false through different projection angles, verify whether the certificate is held by a real person, and verify whether the certificate is held by its owner by comparing image features of a human face of a real person with image features of the human face on the certificate. According to one or more embodiments of this disclosure, whether the certificate is currently held by the owner can be further authenticated while authenticity of the certificate is effectively verified.

The method and apparatus for verifying a certificate and a certificate holder according to this disclosure will be described below with reference to FIGs. 1 to 3.

FIG. 1 illustrates an exemplary flowchart of the method of verifying a certificate and a certificate holder in accordance with an embodiment of this disclosure.

As shown in FIG. 1, in step S1, a video of the certificate with a specified series of projection angles is acquired in real time.

In some embodiments, the video may be captured in real time, for example, by a camera mounted on a terminal device such as a dedicated device for verifying certificates and holders, a mobile terminal such as a smart computer, a tablet computer, or the like.

In the step S1, in order to acquire a video with a specified series of projection angles, in some embodiments, it is able to acquire a video of which the holder holds the certificate to perform a specified series of actions that cause the certificate to have the specified series of projection angles. In such an embodiment, the certificate holder himself performs the specified series of actions, and additional manpower and hardware devices are not required, so that manpower and physical costs can be reduced.

In some embodiments, the video with the specified series of actions may be

completed by an acquisition assist device taking the certificate, the specified series of actions causing the certificate to have the specified series of projection angles. The acquisition assist device can be, for example, a program-controlled manipulator. In such embodiments, the video with the specified series of actions is completed by the acquisition assist device, thus the specified series of projection angles in the acquired video are more standard, enabling a more accurate subsequent certificate validation process.

In addition, in some embodiments, the video with the specified series of projection angles may be acquired also by configuring staff who perform with the certificate.

For the sake of description, an example in which the holder himself holds the certificate to perform the video with the specified series of actions will be described.

In some embodiments, before the step S1, the following steps may be further included: randomly calling a plurality of standard certificate action pictures, generating a video with a series of actions and performing front-end display, and prompting the certificate holder to perform the specified series of actions as illustrated. When the certificate holder performs the series of actions, the certificate can be sequentially positioned at different positions and have different projection angles.

The projection angle in this embodiment may be, for example, an angle formed between the certificate and a projection surface of the camera. Specifically, the angle may be an angle formed between a line connecting a central point of the certificate to a central point of a camera projection plane, and the camera projection plane.

The number of the specified series of projection angles may be one or more. In some embodiments, by setting multiple projection angles in different directions and/or different angular ranges, image features of the certificate in different directions and/or under different projection angles can be acquired, thereby improving reliability of the verification.

Illustratively, a set of the series of projection angles of the certificate can include: upper 45 °, left 45 °, lower 45 °, right 45 °, and middle 90 °. The certificate is held such that the certificate is positioned upper 45 °, left 45 °, lower 45 °, right 45 °, and right ahead of the central point of the camera projection plane in sequence. The respective projection angles mentioned above can be presented to the certificate holder through the front-end display, so that the certificate holder is prompted to

perform the specified series of actions as illustrated.

In the step S2, image features of the certificate under different projection angles in the video are extracted.

In some embodiments, the step S2 may include the following substeps:

S21, splitting the video into a plurality of pictures by frames;

S22, extracting image features of the certificate in each picture;

S23, calculating a projection angle of each picture according to the position of the certificate in each picture;

S24, recording the image features of the certificate in each picture and the projection angles of the corresponding pictures.

The image features of the certificate in the step S22 may include a visual anti-counterfeiting feature of the certificate and image features of a human face in the certificate. Computer vision related techniques can be used to extract image features of the certificate. In some embodiments, algorithms such as SIFT, SURF, BRIEF, ORB may be employed for the extraction.

In some embodiments, the step S22 may include step S221: extracting the visual anti-counterfeiting feature of the certificate in the picture.

The visual anti-counterfeiting feature of the certificate may comprise a static visual anti-counterfeiting feature. The static visual anti-counterfeiting feature includes for example texture, color, text, etc., and does not change with the projection angle of the certificate onto the camera projection plane. The static visual anti-counterfeiting feature can be verified by a computer vision algorithm. In addition, the visual anti-counterfeiting feature of the certificate can include dynamic visual anti-counterfeiting features. The dynamic visual anti-counterfeiting feature may include color, shape, etc., and will change with the projection angle. The dynamic visual anti-counterfeiting feature can be for example a laser anti-counterfeiting code, and the changes in the laser anti-counterfeiting code at different angles can be recorded by a computer vision method to verify the dynamic visual anti-counterfeiting feature.

In some embodiments, the step S22 may include step S222: extracting image features of the human face of the certificate in the picture.

In some embodiments, the step S222 may specifically include the following substeps:

S2221, defining and positioning feature points of the human face, wherein the feature points of the human face in the picture can be defined and positioned by using

a direction of image gradient;

S2222, extracting feature vectors of the feature points of the human face in the step S2221;

S2223, marking the feature points of the human face by means of a statistical model considering features and relative relationship of the feature points of the human face, by using a statistical reference method, thereby determining the positions of the required feature points of the human face .

Generally, the feature points of the human face may include features of eye, nose, etc.

In some embodiments, the step S23 may include the following substeps:

S231, acquiring a position of the certificate in each picture through a feature matching algorithm, specifically, searching and calculating a homograph matrix, and then calculating a specific position of the certificate through a radial transformation.

S232, calculating the projection angle of the certificate according to the angle formed between the certificate position in each picture calculated and obtained in the step S231, and the camera projection plane.

In the step S3, authenticity of the certificate is verified according to the image features of the certificate.

In some embodiments, the step S3 may include the following substeps:

S31, calling a standard projection angle range of the certificate in each action in the pictures of the certificate with the specified series of actions, and standard data ranges of the static anti-counterfeiting feature and the dynamic anti-counterfeiting feature in the standard projection angle range;

S32, comparing the visual anti-counterfeiting feature of the certificate extracted from the corresponding picture with the standard data range of the visual anti-counterfeiting feature. When the visual anti-counterfeiting feature in the picture falls within the standard data range of the visual anti-counterfeiting feature, determine that the certificate is authentic, and enter the next step; otherwise, the certificate is false, terminate the verification and prompt the certificate holder to further check the certificate. In some embodiments, when the visual anti-counterfeiting feature comprises a static visual anti-counterfeiting feature and a dynamic visual anti-counterfeiting feature, the static visual anti-counterfeiting feature and the dynamic visual anti-counterfeiting feature are respectively compared with the standard data

range of the static visual anti-counterfeiting feature and the standard data range of the dynamic visual anti-counterfeiting feature to confirm the authenticity of the certificate.

By setting a standard projection angle range in each action, a small deviation is allowed when the verifier performs the specified series of actions of the certificate. Therefore, even if there are differences in height and/or differences in sensory judgment between the verifiers, the verification can be performed smoothly, and a false alarm rate of the verification can be reduced.

In some embodiments, before the step S3, step S8 may be further included: verifying whether video acquisition of the certificate under the specified series of projection angles is finished or not according to the image features of the certificate under different projection angles. If yes, execute the step S3; and if not, acquire the video for the certificate again.

In some embodiments, whether the acquisition of the certificate under the specified series of projection angles is performed, i.e., whether the certificate holder has finished the series of actions, can be verified by verifying whether the projection angles of the pictures in the image split by frames conform to the projection angles that the certificate should have under the specified series of projections.

In the step S4, the human face video is acquired in real time.

In some embodiments, the video of the certificate is acquired first, and on the premise that the certificate is successfully verified, the human face video is further acquired to verify the certificate holder. In this way, if the certificate verification fails, the verification of the certificate holder is not required, which can accelerate the verification process and save system overhead.

In some embodiments, the human face video and the certificate video may be acquired in the same video. For example, from the video of which the certificate holder holds the certificate and performs the specified series of actions, the video of the certificate with the specified series of projection angles and the human face video can be acquired. In such embodiments, both the human face video and the certificate video can be acquired using the same video acquisition module.

By acquiring the video having both the certificate and the certificate holder and verifying the certificate and the certificate holder respectively, not only the flow can be simplified and user satisfaction can be improved, but also the real person holds the authentic certificate and the owner holds his certificate can be further ensured, which

further improve the verification reliability.

In the step S5, whether it is a real person in the human face video is verified.

In some embodiments, the verification process in the step S5 may be performed by a living body detection. The living body detection is a method for determining real physiological features of an object in some identity authentication scenes, and can be used in scenes such as face-brushing payment, remote identity authentication and the like. In face recognition applications, the living body detection can verify whether the user is a real living human body or not through combined actions of blinking, opening mouth, shaking head, nodding and the like, by using technologies such as human face key point positioning, human face tracking and the like. The method can effectively resist common attack means such as photo, face changing, mask, shielding, screen copying and the like, thereby assisting in discriminating fraudulent behaviors and ensuring the user's benefits. The detection mode of the living body detection may be stereoscopic living body detection, sub-plane detection, or infrared FMP detection, and in the present embodiment, the stereoscopic living body detection mode is preferable.

In some embodiments, living body detection may be performed on the human face video by frames.

In some embodiments, when it is verified that it is not a real person in the human face video, the verification process may be directly stopped without the need of proceeding with the subsequent extraction of the human face image features from the human face video and the comparison of the image features.

In the step S6, image features of the human face in the human face video is extracted.

In some embodiments, human face image features may be extracted from the human face video by frames. The human face image feature extraction method adopted in this step may refer to the specific extraction mode in the step S222.

In the step S7, when the certificate is verified to be authentic and it is a real person in the human face video, the image features of the certificate are compared with the image features of the human face in the human face video, to determine whether the certificate holder is the owner of the certificate.

In some embodiments, the human face image features of the certificate extracted in the step S222 may be compared with the image features of the human face in the human face video.

In the comparison, the comparison can be made by comparing feature vectors of the same feature point of the human face and comparing shapes and sizes of the feature points of the human face. In some embodiments, the comparison may be made by means of depth learning of the image processing, and a determination may be made by calculating a similarity using image similarity algorithm. In some embodiments, a certain similarity threshold may be set, and when the similarity is within the threshold, the comparison may be considered to pass. By setting the similarity threshold, the influences of objective conditions such as light rays, definition and the like to the comparison can be eliminated.

When the comparison is passed, the certificate holder is proved to be the certificate owner, and when the comparison is not passed, the certificate holder is proved not to be the certificate owner. In some embodiments, if the comparison is passed, the display terminal prompts pass of the comparison, and if the comparison is not passed, non-pass of the comparison is displayed and the certificate holder is prompted to make the comparison again or quit.

According to the method of verifying the certificate and the certificate holder, whether the certificate is currently held by the certificate owner or not can be further authenticated while authenticity of the certificate is effectively verified.

FIG. 2 illustrates an exemplary configuration block diagram of an apparatus 2000 for verifying a certificate and a certificate holder in accordance with an embodiment of this disclosure.

In some embodiments, the apparatus 2000 may include processing circuitry 2010. Processing circuitry 2010 of the apparatus 2000 provides various functions of the apparatus 2000. In some embodiments, the processing circuitry 2010 of the apparatus 2000 may be configured to perform the method of verifying a certificate and a certificate holder described above with reference to FIG. 1.

Processing circuitry 2010 may refer to various implementations of digital circuitry, analog circuitry, or mixed-signal (a combination of analog and digital) circuitry that performs functions in a computing system. Processing circuitry may include, for example, circuit such as Integrated Circuit (IC), Application Specific Integrated Circuit (ASIC), a portion or circuit of a separate processor core, an entire processor core, a separate processor, a programmable hardware device such as Field Programmable Gate Array (FPGA), and/or a system including multiple processors.

In some embodiments, the processing circuitry 2010 may include a first video

acquiring module 2020, a first extracting module 2030, a first verifying module 2040, a second video acquiring module 2050, a second verifying module 2060, a second extracting module 2070, and a comparing module 2080.

The first video acquiring module 2020 is used for acquiring a video of the certificate with a specified series of projection angles in real time the first extracting module 2030 is used for extracting image features of the certificate under different projection angles in the video; the first verifying module 2040 is used for verifying authenticity of the certificate according to the image features of the certificate; the second video acquiring module 2050 is used for acquiring a human face video in real time; the second verifying module 2060 is used for verifying whether it is a real person in the human face video; the second extracting module 2070 is used for extracting image features of the human face in the human face video; and the comparing module 2080 is used for, when the certificate is verified to be authentic and it is a real person in the human face video, comparing the image features of the certificate with the image features of the human face in the human face video, to determine whether the certificate holder is the owner of the certificate. The modules 2020 to 2080 may be configured to perform the steps S1 to S7 of the method for verifying a certificate and a certificate holder shown in FIG. 1, respectively.

In some embodiments, the apparatus 2000 may also include a memory (not shown). The memory of the apparatus 2000 may store information generated by the processing circuitry 2010 as well as programs and data for the operation of the apparatus 2000. The memory may be a volatile memory and/or a non-volatile memory. For example, the memory may include, but not limited to, Random Access Memory (RAM), Dynamic Random Access Memory (DRAM), Static Random Access Memory (SRAM), Read Only Memory (ROM), and flash memory. In addition, the apparatus 2000 may be implemented at a chip level, or may also be implemented at a device level by including other external components.

It should be understood that the various modules described above are merely logical modules that are divided according to the specific functions implemented by the modules, but are not intended to limit the specific implementations. In actual implementations, the above-described modules may be implemented as separate physical entities, or may also be implemented by a single entity (e.g., a processor (CPU, DSP, etc.), an integrated circuit, or the like).

In some embodiments, the apparatus 2000 can include a third verifying module

2090 for verifying whether video acquisition of the certificate at the specified series of projection angles is finished based on the image features of the certificate at different projection angles. The third verifying module 2090 may be configured to perform the aforementioned step S8, for example.

In some embodiments, the first extracting module 2030 may include the following modules: a splitting sub-module 2031 for splitting the video into a plurality of pictures by frames; a first extracting sub-module 2032 for extracting image features of the certificate in each of the plurality of pictures; a first processing sub-module 2033 for calculating a projection angle of each picture according to a position of the certificate in each of the plurality of pictures; and a recording submodule 2034 for recording the image features of the certificate in each of the plurality of pictures and the projection angle of the corresponding picture. The modules 2031 to 2034 may be configured to perform the steps S21 to S24, respectively, for example.

According to the apparatus for verifying the certificate and the certificate holder, whether the certificate is currently held by the certificate owner or not can be further authenticated while authenticity of the certificate is effectively verified.

FIG. 3 illustrates an exemplary configuration of a computing device 300 capable of implementing the embodiments according to the invention. Computing device 300 is an example of a hardware device to which the above-described aspect of the invention may be applied. Computing device 300 may be any machine configured to perform processing and/or computing. Computing device 300 may be, but is not limited to, a workstation, a server, a desktop computer, a laptop computer, a tablet computer, a Personal Data Assistant (PDA), a smart phone, an on-board computer, or a combination thereof.

As shown in FIG. 3, the computing device 300 may include one or more elements that may be connected to or communicate with a bus 302 via one or more interfaces. Bus 302 may include, but is not limited to, an Industry Standard Architecture (ISA) bus, a Micro Channel Architecture (MCA) bus, an Enhanced ISA (EISA) bus, a Video Electronics Standards Association (VESA) local bus, and a Peripheral Component Interconnect (PCI) bus, among others. The computing device 300 may include, for example, one or more processors 304, one or more input devices 306, and one or more output devices 308. The one or more processors 304 may be any kind of processor and may include, but is not limited to, one or more general purpose processors or special purpose processors (such as a special purpose processing chip).

The processor 304 may correspond, for example, to the processing circuitry 2010 in FIG. 2, and is configured to implement the functions of the modules of the apparatus for verifying the certificate and the certificate holder of this disclosure. Input device 306 may be any type of input device capable of inputting information to the computing device and may include, but is not limited to, a mouse, a keyboard, a touch screen, a microphone, and/or a remote controller. Output device 308 may be any type of device capable of presenting information and may include, but is not limited to, a display, a speaker, a video/audio output terminal, a vibrator, and/or a printer.

The computing device 300 may also include or be connected to a non-transitory storage device 314, which may be any non-transitory storage device that can implement data storage, and may include, but is not limited to, a disk drive, an optical storage device, a solid-state memory, a floppy disk, a flexible disk, a hard disk, a magnetic tape, or any other magnetic medium, a compact disk, or any other optical medium, a cache memory, and/or any other memory chip or module, and/or any other medium from which the computer can read data, instructions, and/or code. The computing device 300 may also include a Random Access Memory (RAM) 310 and a read-only memory (ROM) 312. The ROM 312 may store programs, application programs, or processes to be executed in a nonvolatile manner. The RAM 310 may provide volatile data storage and store instructions related to the operation of the computing device 300. The computing device 300 may also include a network/bus interface 316 coupled to a data link 318. The network/bus interface 316 may be any type of device or system capable of enabling communication with an external device and/or network and may include, but is not limited to, a modem, a network card, an infrared communication device, a wireless communication device, and/or a chipset (such as a BluetoothTM device, a 802.11 device, a WiFi device, a WiMax device, a cellular communication facility, etc.).

Besides, one or more embodiments of this disclosure may be implemented as follows.

Solution 1:

an apparatus for verifying a certificate and a certificate holder, comprising:

one or more processors;

a memory having stored thereon computer-executable instructions that, when executed by the one or more processors, cause the one or more processors to:

acquire a video of the certificate with a specified series of projection angles in

real time;

extract image features of the certificate under different projection angles in the video;

verify authenticity of the certificate according to the image features of the certificate;

acquire a human face video in real time;

verify whether it is a real person in the human face video;

extract image features of the human face in the human face video; and

when the certificate is verified to be authentic and it is a real person in the human face video, compare the image features of the certificate with the image features of the human face in the human face video, to determine whether the certificate holder is the owner of the certificate.

Solution 2: in the apparatus for verifying a certificate and a certificate holder of Solution 1,

the video of the certificate with the specified series of projection angles and the human face video is acquired from a video of which the certificate holder holds the certificate and performs a specified series of actions, wherein the specified series of actions enables the certificate to have the specified series of projection angles.

Solution 3: in the apparatus for verifying a certificate and a certificate holder of Solution 1, the computer-executable instructions, when executed by the one or more processors, cause the one or more processors to:

verify whether the video acquisition of the certificate under the specified series of projection angles is finished or not according to the image features of the certificate under different projection angles.

Solution 4: in the apparatus for verifying a certificate and a certificate holder of Solution 1, the computer-executable instructions, when executed by the one or more processors, cause the one or more processors to:

split the video into a plurality of pictures by frames;

extract image features of the certificate in each of the plurality of pictures;

calculate a projection angle of each picture according to a position of the certificate in each of the plurality of pictures; and

record the image features of the certificate in each of the plurality of pictures and the projection angle of the corresponding picture.

Solution 5: in the apparatus for verifying a certificate and a certificate holder of

Solution 1,

the image features of the certificate comprise a visual anti-counterfeiting feature of the certificate and image features of a human face in the certificate,

the authenticity of the certificate is verified according to the visual anti-counterfeiting feature of the certificate, and

the image features of the human face in the certificate is compared with the image features of the human face in the human face video, to determine whether the certificate holder is the certificate owner.

Solution 6: in the apparatus for verifying a certificate and a certificate holder of Solution 5,

the visual anti-counterfeiting feature includes a dynamic visual anti-counterfeiting feature that changes with the projection angles.

It should be understood that the reference to "embodiment" or similar expressions throughout this specification means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of this disclosure. Thus, the appearance of the phrase "in an embodiment of this disclosure" and similar expressions throughout this specification not necessarily refer to the same embodiment.

The various aspects, solutions, implementations, or features of the foregoing embodiments, may be used alone or in any combination. Various aspects of the foregoing embodiments may be implemented by software, hardware, or a combination of hardware and software.

For example, the foregoing embodiments may be embodied as computer readable code on a computer readable medium. The computer readable medium is any data storage device that can store data which can thereafter be read by a computer system. Examples of the computer-readable medium include read-only memory, random-access memory, CD-ROM, DVD, magnetic tape, hard drive, solid-state drive, and optical data storage device. The computer readable medium can also be distributed over the network-coupled computer system so that the computer readable code is stored and executed in a distributed fashion.

For example, the foregoing embodiments may take the form of hardware circuitry. The hardware circuitry may include any combination of combined logic circuits, clock storage devices (such as floppy disks, flip-flops, latches, etc.), finite state machines, memories such as static random access memories or embedded

dynamic random access memories, custom designed circuitry, programmable logic arrays, etc.

It is to be noted that the above only shows preferable embodiments of the invention and the technical principles applied. It will be understood by those skilled in the art that the invention is not limited to the particular embodiments described herein, and those skilled in the art could make numerous evident changes, rearrangements and substitutions without departing from the scope of protection of the invention. Therefore, although the present invention has been described in detail with reference to the above embodiments, the invention is not limited to the above embodiments, and more other equivalent embodiments may be further included without departing from the spirit of the invention, and the scope of the invention is defined by the appended claims.

[CLAIMS]

1. A method of verifying a certificate and a certificate holder, characterized by comprising the steps of:

acquiring a video of the certificate with a specified series of projection angles in real time;

extracting image features of the certificate under different projection angles in the video;

verifying authenticity of the certificate according to the image features of the certificate;

acquiring a human face video in real time;

verifying whether it is a real person in the human face video;

extracting image features of the human face in the human face video; and

when the certificate is verified to be authentic and it is a real person in the human face video, comparing the image features of the certificate with the image features of the human face in the human face video, to determine whether the certificate holder is the owner of the certificate.

2. The method of verifying a certificate and a certificate holder according to claim 1, characterized in that

the video of the certificate with the specified series of projection angles and the human face video is acquired from a video of which the certificate holder holds the certificate and performs a specified series of actions, wherein the specified series of actions enables the certificate to have the specified series of projection angles.

3. The method of verifying a certificate and a certificate holder according to claim 1, characterized by further comprising:

verifying whether the video acquisition of the certificate under the specified series of projection angles is finished or not according to the image features of the certificate under different projection angles.

4. The method of verifying a certificate and a certificate holder according to claim 1, characterized in that the step of extracting image features of the certificate under different projection angles in the video comprises the following substeps:

splitting the video into a plurality of pictures by frames;

extracting image features of the certificate in each of the plurality of pictures;
calculating a projection angle of each picture according to a position of the certificate in each of the plurality of pictures; and
recording the image features of the certificate in each of the plurality of pictures and the projection angle of the corresponding picture.

5. The method of verifying a certificate and a certificate holder according to claim 1, characterized in that

the image features of the certificate comprise a visual anti-counterfeiting feature of the certificate and image features of the human face in the certificate,

the authenticity of the certificate is verified according to the visual anti-counterfeiting feature of the certificate, and

the image features of the human face in the certificate is compared with the image features of the human face in the human face video, to determine whether the certificate holder is the owner of certificate.

6. The method of verifying a certificate and a certificate holder according to claim 5, characterized in that

the visual anti-counterfeiting feature includes a dynamic visual anti-counterfeiting feature that changes with the projection angles.

7. An apparatus for verifying a certificate and a certificate holder, comprising:
a first video acquiring module for acquiring a video of the certificate with a specified series of projection angles in real time;

a first extracting module for extracting image features of the certificate under different projection angles in the video;

a first verifying module for verifying authenticity of the certificate according to the image features of the certificate;

a second video acquiring module for acquiring a human face video in real time;

a second verifying module for verifying whether it is a real person in the human face video;

a second extracting module for extracting image features of the human face in the human face video; and

a comparing module for, when the certificate is verified to be authentic and it is a real person in the human face video, comparing the image features of the certificate with the image features of the human face in the human face video, to determine whether the certificate holder is the owner of the certificate.

8. The apparatus for verifying a certificate and a certificate holder according to claim 7, characterized in that

the first video acquiring module and the second video acquiring module acquire the video of the certificate with the specified series of projection angles and the human face video respectively, from a video of which the certificate holder holds the certificate and performs a specified series of actions, wherein the specified series of actions enables the certificate to have the specified series of projection angles.

9. The apparatus for verifying a certificate and a certificate holder according to claim 7, characterized by further comprising:

a third verifying module for verifying whether the video acquisition of the certificate under the specified series of projection angles is finished or not according to the image features of the certificate under different projection angles.

10. The apparatus for verifying a certificate and a certificate holder according to claim 7, characterized in that the first extracting module comprises:

a splitting submodule for splitting the video into a plurality of pictures by frames;
a first extracting submodule for extracting image features of the certificate in each of the plurality of pictures;

a first processing submodule for calculating a projection angle of each picture according to a position of the certificate in each of the plurality of pictures; and

a recording submodule for recording the image features of the certificate in each of the plurality of pictures and the projection angle of the corresponding picture.

11. The apparatus for verifying a certificate and a certificate holder according to claim 7, characterized in that

the image features of the certificate comprise a visual anti-counterfeiting feature of the certificate and image features of the human face in the certificate,

the first verifying module verifies the authenticity of the certificate according to

the visual anti-counterfeiting feature of the certificate, and

the comparing module compares the image features of the human face in the certificate with the image features of the human face in the human face video, to determine whether the certificate holder is the owner of certificate.

12. The apparatus for verifying a certificate and a certificate holder according to claim 11, characterized in that

the visual anti-counterfeiting feature includes a dynamic visual anti-counterfeiting feature that changes with the projection angles.

13. A computer-readable storage medium on which a computer program is stored, wherein when the program is executed by a processor, causes the processor to:

acquire a video of the certificate with a specified series of projection angles in real time;

extract image features of the certificate under different projection angles in the video;

verify authenticity of the certificate according to the image features of the certificate;

acquire a human face video in real time;

verify whether it is a real person in the human face video;

extract image features of the human face in the human face video; and

when the certificate is verified to be authentic and it is a real person in the human face video, compare the image features of the certificate with the image features of the human face in the human face video, to determine whether the certificate holder is the owner of the certificate.