

[DESCRIPTION]

[TITLE OF INVENTION]

**HOLOGRAPHIC ANTI-COUNTERFEITING CODE VERIFICATION
METHOD AND DEVICE**

[Technical field]

This disclosure pertains to the technical field of anti-counterfeiting codes, and in particular, to a holographic anti-counterfeiting code verification method and device.

[Background Art]

Holographic anti-counterfeiting technology is a novel anti-counterfeiting technology developed by applying laser anti-counterfeiting technology, and is also called laser holographic anti-counterfeiting. A label fabricated by using the holographic anti-counterfeiting technology contains more information, so it has a deeper anti-counterfeiting effect than an ordinary laser anti-counterfeiting label. Since a holographic image combines the latest achievements in subjects such as laser, precision machinery and physical chemistry, it has a higher technology content. For most small batch counterfeiters, the mastery of the full production technology and the acquisition of the production equipment are difficult to achieve.

"Holographic" means "all information", that is, as compared to a normal photograph that only records a change in the brightness of an object, a laser hologram can also record a spatial change of the object. Observing the holographic anti-counterfeiting code at different angles will present different images, e.g., a multi-channel holographic anti-counterfeiting technology: in the multi-channel holographic anti-counterfeiting, when rotating a logo, we will see different patterns appearing at the same position of the logo; a 360° computer dot matrix holographic technology: the 360° computer dot matrix holographic technology will display combinations and transformations of radial, annular, spiral etc. light spots in a 360° observation range of the image, and thus has a very strong dynamic effect; a dynamic coding anti-counterfeiting technology: the dynamic coding anti-counterfeiting

technology is to put the trademark in front of eyes and slowly rotate the logo to appear a pattern with continuous motions.

[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 of the disclosure in a simplified form as a prelude to the more detailed description that is presented later.

According to an aspect of this disclosure, a holographic anti-counterfeiting code verification method is provided, the method comprising:

- acquiring a video stream of a holographic anti-counterfeiting code under different projection angles;

- extracting a projection angle and an image feature of the holographic anti-counterfeiting code in each of one or more frames of the video stream;

- matching the projection angle and the image feature of the holographic anti-counterfeiting code in each frame in a pre-stored mapping table to obtain a matching ratio of the holographic anti-counterfeiting code in each frame, wherein the mapping table stores mapping relationships between different projection angles and image features of a sample holographic anti-counterfeiting code; and

- determining whether or not the holographic anti-counterfeiting code is successfully verified according to the matching ratio of the holographic anti-counterfeiting code in each frame.

According to another aspect of this disclosure, a holographic anti-counterfeiting code verification device is provided, the device comprising:

- a first acquiring module configured to acquire a video stream of a holographic anti-counterfeiting code under different projection angles;

- a first extracting module configured to extract a projection angle and an image

feature of the holographic anti-counterfeiting code in each of one or more frames of the video stream;

a matching module configured to match the projection angle and the image feature of the holographic anti-counterfeiting code in each frame in a pre-stored mapping table to obtain a matching ratio of the holographic anti-counterfeiting code in each frame, wherein the mapping table stores mapping relationships between different projection angles and image features of a sample holographic anti-counterfeiting code; and

a first determining module configured to determine whether or not the holographic anti-counterfeiting code is successfully verified according to the matching ratio of the holographic anti-counterfeiting code in each frame.

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

acquire a video stream of a holographic anti-counterfeiting code under different projection angles;

extract a projection angle and an image feature of a holographic anti-counterfeiting code in each of one or more frames of the video stream;

match the projection angle and the image feature of the holographic anti-counterfeiting code in each frame in a pre-stored mapping table to obtain a matching ratio of the holographic anti-counterfeiting code in each frame, wherein the mapping table stores mapping relationships between different projection angles and image features of a sample holographic anti-counterfeiting code; and

determine whether or not the holographic anti-counterfeiting code is successfully verified according to the matching ratio of the holographic anti-counterfeiting code in each frame.

According to one or more embodiments of this disclosure, it is able to realize low-cost, highly efficient automatic holographic anti-counterfeiting code verification.

[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 schematically shows a flowchart of a holographic anti-counterfeiting code verification method according to an embodiment of this disclosure;

FIG. 2 schematically shows a flowchart of a holographic anti-counterfeiting code verification method according to another embodiment of this disclosure;

FIG. 3 schematically shows a flowchart of a holographic anti-counterfeiting code verification method according to another embodiment of this disclosure;

FIG. 4 schematically shows a block diagram of a configuration of a holographic anti-counterfeit code verification device according to another embodiment of this disclosure;

FIG. 5 schematically shows a configuration of a computing device in which an embodiment according to this disclosure may be implemented.

[Detailed description of the drawings]

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.

Regarding the verification of the holographic anti-counterfeiting codes, the inventors know the way to perform the verification manually. Such manual verification requires the verification personnel to have professional anti-counterfeiting knowledge and a professional verification device is required for the verification. The

manual verification method has high verification cost and low efficiency. This disclosure provides a holographic anti-counterfeiting code verification method and device, which can realize low-cost, highly efficient automatic holographic anti-counterfeiting code verification.

Before explaining the technical solutions in the embodiments of this disclosure in further detail, a subject for carrying out the technical solution of this disclosure will be described first. The subject for carrying out the technical solution of this disclosure may be, for example, a mobile terminal such as a computer, an iPad, a mobile phone, or an electronic device such as a dedicated device for holographic anti-counterfeiting code verification.

The holographic anti-counterfeiting code verification method and device according to this disclosure will be described below with reference to FIGS.1-5.

FIG. 1 schematically shows a flowchart of a holographic anti-counterfeiting code verification method according to an embodiment of this disclosure.

As shown in Fig.1, in a step S101, a video stream of a holographic anti-counterfeiting code under different projection angles is acquired.

A holographic anti-counterfeiting code can be placed in a local area on the anti-counterfeiting label, which is a carrier of the holographic anti-counterfeiting code. In addition, the anti-counterfeiting label may also include information other than the holographic anti-counterfeiting code.

In some embodiments, the video stream data of the holographic anti-counterfeiting code may be acquired in advance using an image acquisition device. The image acquisition device may be, for example, a camera mounted on a mobile terminal such as a computer, an iPad, a mobile phone, or an electronic device such as a dedicated device for holographic anti-counterfeiting code verification. In addition, the image acquisition device may also be a device separate from the above-mentioned electronic device, and after the video stream is acquired, the video stream is input to the electronic device by the image acquisition device. A specific input process is not limited in the embodiments of this disclosure.

In some embodiments, shooting angles may be transformed during the

acquisition of the video stream to obtain a video stream of the holographic anti-counterfeiting code under different projection angles. In some embodiments, the shooting angles can be transformed according to preset angle transformation values. The preset angle transformation values may be an angle range value or a plurality of discrete angle values, and other angle transformation values may be set according to actual needs.

In some embodiments, the video stream of the holographic anti-counterfeiting code under different projection angles may be pre-recorded using an image acquisition device or acquired in real time by an image acquisition device, wherein the video stream data of the holographic anti-counterfeiting code may include multiple frames of continuous images.

The projection angle in this embodiment may be, for example, an angle formed between the holographic anti-counterfeiting code and a projection plane of the camera. Specifically, it may be an angle formed between a line connecting a center point of the holographic anti-counterfeiting code and a center point of the projection plane of the camera. An orthographic projection angle may correspond to an angle at which the holographic anti-counterfeiting code on the anti-counterfeiting label is shot from an upright direction.

In a step S102, a projection angle and an image feature of the holographic anti-counterfeiting code in each of one or more frames of the video stream is extracted.

In some embodiments, a computer vision method may be adopted for extracting the image feature of the holographic anti-counterfeiting code. For example, feature extraction algorithms such as orb, surf, or sift can be adopted. A specific extraction process is not limited in the embodiment of this disclosure.

In some embodiments, one or more frames extracted from the video stream may be consecutive frames or discrete frames arranged in a chronological order.

In some embodiments, extracting the projection angle of the holographic anti-counterfeiting code in each of one or more frames of the video stream may include: comparing the extracted image feature of the holographic anti-counterfeiting code in each frame with a pre-stored anti-counterfeiting code image feature,

generating a transformation matrix, and calculating the projection angle of the holographic anti-counterfeiting code in each frame. In some embodiments, the pre-stored anti-counterfeiting code image feature may be obtained by performing feature extraction in advance on the orthographic projection image of the sample holographic anti-counterfeiting code shot at an orthographic projection angle.

In some embodiments, the orthographic projection image feature and the orthographic projection angle may be stored in a pre-built mapping table in a correspondence relationship.

Alternatively, prior to the step S102, the method provided by the embodiment of this disclosure may further comprise:

pre-processing each of the one or more frames of the video stream, wherein the pre-processing may comprise operations such as truncation thresholding processing, contrast enhancement processing, and image denoising processing.

In this embodiment, by preprocessing each of the one or more frames of the video stream, noise that may exist in the video frame can be eliminated to restore useful real information, enhance detectability of relevant information, and simplify the desired image to the utmost, thereby increasing the reliability of image feature extraction performed in the step S102. Further, it is possible to increase matching reliability when matching the holographic anti-counterfeiting code as described in the following step S103.

In step S103, the projection angle and the image feature of the holographic anti-counterfeiting code in each frame is matched in a pre-stored mapping table to obtain a matching ratio of the holographic anti-counterfeiting code in each frame.

The mapping table stores mapping relationships between different projection angles of a sample holographic anti-counterfeiting code and image features of the sample holographic anti-counterfeiting code.

In some embodiments, for the holographic anti-counterfeiting code in each frame, query in the mapping table whether there is a projection angle the same as the projection angle of the holographic anti-counterfeiting code, and if so, calculate a similarity between the image feature of the holographic anti-counterfeiting code and

the image feature corresponding to the projection angle in the mapping table; and determine the matching ratio of the holographic anti-counterfeiting code in each frame according to the calculated similarity. Among them, means such as Euclidean distance, Mahalanobis distance or cosine function can be adopted to calculate the similarity.

A specific matching process is not limited in the embodiment of this disclosure.

In step S104, whether or not the holographic anti-counterfeiting code is successfully verified is determined according to the matching ratio of the holographic anti-counterfeiting code in each frame.

In some embodiments, the matching ratios of all holographic anti-counterfeiting codes in the one or more frames of the video stream can be statistically analyzed to determine if the holographic anti-counterfeiting code is successfully verified. The statistical matching ratio may be, for example, an average matching ratio of the holographic anti-counterfeiting codes in the one or more frames, or a sum of the matching ratio of the holographic anti-counterfeiting code in each frame. In addition, other methods can also be used to calculate the matching ratio.

In some embodiments, it may be determined whether the statistical matching ratio is greater than a preset threshold. If it is greater than the predetermined threshold, it is determined that the holographic anti-counterfeiting code is successfully verified; otherwise, it is determined that verification of the holographic anti-counterfeiting code fails.

The preset threshold can be set according to actual needs, for example, the preset threshold is set to 0.8, and when the statistical matching ratio is 0.6, it can be determined that verification of the holographic anti-counterfeiting code fails.

In some embodiments, a verification result indicating whether the verification of the holographic anti-counterfeiting code is successful may be generated and displayed to the user in the electronic device.

For example, the verification result may be output in a text form on the screen of the electronic device, e.g., outputting the text "verification successful" or "verification failed". In addition, it is also possible to indicate successful verification of the

holographic anti-counterfeiting code by outputting a symbol mark "√", and to indicate failed verification of the holographic anti-counterfeiting code by outputting a symbol mark "x", and the like.

In this embodiment, by matching the projection angle and the image feature of the holographic anti-counterfeiting code in the video stream in the pre-stored mapping table, and determining whether the holographic anti-counterfeiting code is successfully verified according to the matching ratio of the holographic anti-counterfeiting code, a purpose of accurate verification of the holographic anti-counterfeiting code is realized, thereby achieving the technical effect of low-cost, highly efficient automatic verification of the holographic anti-counterfeiting code.

FIG. 2 schematically shows a flowchart of a holographic anti-counterfeiting code verification method according to another embodiment of this disclosure. In this embodiment, the holographic anti-counterfeiting code verification method comprises steps S201 to S203 in addition to the steps described in FIG. 1. For the sake of description, the steps described in FIG. 1 are omitted.

The steps S201 to S203 are steps for constructing a mapping table, and may be performed, for example, before the step S103 described in FIG. 1.

As shown in FIG. 2, in step S201, a plurality of sample images of the sample holographic anti-counterfeiting code under different projection angles are acquired.

The different projection angles may include an orthographic projection angle, and the orthographic projection angle corresponds to the orthographic projection image.

In some embodiments, the sample holographic anti-counterfeiting code can be shot at different projection angles to obtain a plurality of sample images of the sample holographic anti-counterfeiting code under different projection angles. The sample holographic anti-counterfeiting code can be shot by a camera installed on the electronic device or the like. In addition, the sample holographic anti-counterfeiting code can be shot by using an image acquisition device separate from the electronic device, and then the plurality of sample images of the sample holographic

anti-counterfeiting code under different projection angles are input into the electronic device. A specific input process is not limited in the embodiments of this disclosure.

In the step S202, a plurality of sample image features corresponding to the different projection angles is extracted from the plurality of sample images.

In some embodiments, extraction of the image features may be accomplished using a method similar to the method described above in the step S102 for extracting the image feature of the holographic anti-counterfeiting code. For example, the feature extraction may be performed by using a computer vision method.

In the step S203, a mapping table is constructed according to correspondence relationships between the different projection angles and the plurality of sample image features. The mapping table may be stored in the electronic device for the matching process in the step S103 described above.

In the embodiment of this disclosure, the mapping table is constructed according to the correspondence relationships between the different projection angles and the plurality of sample image features, so that state changes indicating that the features of the anti-counterfeiting code change with the projection angles are stored in the mapping table, for the convenience of holographic anti-counterfeiting code verification with the mapping table.

FIG. 3 schematically shows a flowchart of a holographic anti-counterfeiting code verification method according to another embodiment of this disclosure. In this embodiment, the holographic anti-counterfeiting code verification method comprises steps S301 to S303 in addition to the steps described in FIG. 1. For the sake of description, the steps described in FIG. 1 are omitted.

The steps S301 to S303 shown in FIG. 3 are steps for determining authenticity of the video stream, and may be performed, for example, before the step S103 described in FIG. 1.

As shown in FIG. 3, in the step S301, the image features of the anti-counterfeiting label in the plurality of frames of the video stream are extracted, wherein the anti-counterfeiting label comprises a holographic anti-counterfeiting code.

In some embodiments, the step of extracting the image features of the

anti-counterfeiting label may be accomplished by a method similar to the method described above in the step S102 for extracting the image features of the holographic anti-counterfeiting code. For example, the feature extraction may be performed by using a computer vision method.

In the step S302, the image feature of the anti-counterfeiting label in each of the plurality of frames is compared with the image feature of the sample holographic anti-counterfeiting code stored in the mapping table to determine a position of the holographic anti-counterfeiting code in each of the plurality of frames on the anti-counterfeiting label.

In some embodiments, it may be determined that the holographic anti-counterfeiting code is located at a lower left position, a central position, or a lower right position, etc. of the anti-counterfeiting label.

In the step S303, authenticity of the video stream is determined according to a change in the position of the holographic anti-counterfeiting code in the plurality of frames on the anti-counterfeiting label.

In some embodiments, the position may include coordinate information. A position vector of the holographic anti-counterfeiting code can be calculated according to the coordinate information of the holographic anti-counterfeiting code; the change in the position of the holographic anti-counterfeiting code in the video stream is determined based on the position vector of the holographic anti-counterfeiting code in each frame of the plurality of frames and an order of the frame in the video stream.

In some embodiments, it may be determined whether there is a sudden change in the position of the holographic anti-counterfeiting code on the anti-counterfeiting label. If a sudden change exists, the video stream is determined to be counterfeit; and if no sudden change exists, the video stream is determined to be authentic.

In this embodiment, the authenticity of the video stream is determined according to the change in the position of the holographic anti-counterfeiting code in the video stream on the anti-counterfeiting label; if the change of the position in the video stream is smooth and fluent, the video stream can be determined to be authentic, and

if a sudden change occurs, for example, if the positions of two continuous frames change greatly, the video stream can be determined to be counterfeit. A specific determination process is not limited in the embodiment of this disclosure.

It should be noted that steps S301 to S303 may be performed before the step S102, may be performed after the step S102, or may be performed simultaneously with the step S102, which is not limited in the embodiment of this disclosure.

In the embodiment of this disclosure, the authenticity of the video stream is determined, and when the video stream is determined to be counterfeit, the matching process in the subsequent step S103 is not required, so that the efficiency of the holographic anti-counterfeiting code verification can be further improved.

Fig. 4 is schematically shows a block diagram of a configuration of a holographic anti-counterfeiting code verification device according to another embodiment of this disclosure.

In some embodiments, the device 4000 may include processing circuitry 4010. Processing circuitry 4010 of the device 4000 provides various functions of the device 4000. In some embodiments, processing circuitry 4010 of the device 4000 may be configured to perform the holographic anti-counterfeiting code verification method described above with reference to FIG. 1.

Processing circuitry 4010 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. The processing circuitry may include, for example, a circuit such as an Integrated Circuit (IC), an 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 a Field Programmable Gate Array (FPGA), and/or a system including multiple processors.

In some embodiments, the processing circuitry 4010 can include a first acquiring module 4020, a first extracting module 4030, a matching module 4040, and a first determining module 4050.

The first acquiring module 4020 is configured to acquire a video stream of a

holographic anti-counterfeiting code under different projection angles; the first extracting module 4030 is configured to extract a projection angle and an image feature of the holographic anti-counterfeiting code in each of one or more frames of the video stream; the matching module 4040 is configured to match the projection angle and the image feature of the holographic anti-counterfeiting code in each frame in a pre-stored mapping table to obtain a matching ratio of the holographic anti-counterfeiting code in each frame, wherein the mapping table stores mapping relationships between different projection angles and image features of a sample holographic anti-counterfeiting code; and the first determining module 4050 is configured to determine whether or not the holographic anti-counterfeiting code is successfully verified according to the matching ratio of the holographic anti-counterfeiting code in each frame. The above modules 4020 to 4050 may be respectively configured to execute the steps S101 to S104 in the holographic anti-counterfeiting code verification method shown in FIG. 1.

In some embodiments, the device 4000 may also include a memory (not shown). The memory of the device 4000 may store information generated by the processing circuitry 4010 as well as programs and data for operation of the device 4000. The memory may be a volatile memory and/or a non-volatile memory. For example, the memory may include, but is 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 device 4000 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 merely are logical modules that are divided according to the specific functions implemented by the modules, and are not intended to limit the specific implementations. In actual implementations, the above-described respective modules may be implemented as separate physical entities, or may also be implemented by a single entity (e.g., a processor (CPU, DSP, or the like), an integrated circuit, or the like).

In some embodiments, the device 4000 may further comprise: a second acquiring

module 4060 configured to acquire a plurality of sample images of the sample holographic anti-counterfeiting code under different projection angles; a second extracting module 4070 configured to extract the plurality of sample image features corresponding to the different projection angles from the plurality of sample images; and a constructing module 4080 configured to construct the mapping table according to the correspondence relationships between the different projection angles and the plurality of sample image features. The above modules 4060 to 4080 may be configured to execute the steps S201 to S203 in the holographic anti-counterfeiting code verification method shown in FIG. 2, respectively, for example.

In some embodiments, the device 4000 may further comprise: a third extracting module 4090 configured to extract the image features of the anti-counterfeiting label in the plurality of frames of the video stream; a comparing module 4100 configured to compare the image feature of the anti-counterfeiting label in each of the plurality of frames with the image feature of the sample holographic anti-counterfeiting code stored in the mapping table to determine a position of the holographic anti-counterfeiting code in each of the plurality of frames on the anti-counterfeiting label; and a second determining module 4110 configured to determine authenticity of the video stream according to a change in the position of the holographic anti-counterfeiting code in the plurality of frames on the anti-counterfeiting label. The above modules 4090 to 4110 may be configured to execute the steps S301 to S303 in the holographic anti-counterfeiting code verification method shown in FIG. 3, respectively, for example.

According to the holographic anti-counterfeiting code verification device of this disclosure, a low-cost, highly efficient automatic holographic anti-counterfeiting code verification can be achieved.

It is clear to those skilled in the art that, for the sake of convenience and brevity of description, the specific working processes of the above-described devices and modules may refer to the corresponding processes in the above-described method embodiments, and thus are not repeated here.

It should be noted that: when the holographic anti-counterfeiting code

verification device provided by the aforementioned embodiments performs the holographic anti-counterfeiting code verification method, the division of the aforementioned functional modules is taken only as an example, and in practical applications, the functions can be assigned to and be performed by different functional modules as needed, namely, the internal structure of the device is divided into different functional modules so as to complete all or part of the functions described above. In addition, the holographic anti-counterfeiting code verification device and the holographic anti-counterfeiting code verification method provided by the aforementioned embodiments belong to the same concept, and their specific implementations are detailed in the method embodiments and are not repeated here.

FIG. 5 shows an exemplary configuration of a computing device 500 in which an embodiment according to the invention may be implemented. Computing device 500 is an example of the hardware device to which the above-described aspects of the invention may be applied. Computing device 500 may be any machine configured to perform processing and/or computing. Computing device 500 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. 5, the computing device 500 may include one or more elements that may be connected to or communicate with a bus 502 via one or more interfaces. Bus 502 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. Computing device 500 may include, for example, one or more processors 504, one or more input devices 506, and one or more output devices 508. The one or more processors 504 may be any kind of processor and may include, but are not limited to, one or more general purpose processors or special purpose processors (such as a special purpose processing chip). Processor 504 may correspond, for example, to the processing circuitry 4010 in FIG. 4, configured to realize the functions of the various modules of the holographic

anti-counterfeiting code verification device of this disclosure. Input device 506 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 508 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.

Computing device 500 may also include or be connected to a non-transitory storage device 514, which may be any non-transitory storage device that can realize data storage, and may include, but is not limited to, a disk drive, an optical storage device, 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 buffer memory, and/or any other memory chip or module, and/or any other medium from which a computer can read data, instructions, and/or code. Computing device 500 may also include Random Access Memory (RAM) 510 and Read Only Memory (ROM) 512. The ROM 512 may store programs, utilities or processes to be executed in a nonvolatile manner. The RAM 510 may provide volatile data storage and store instructions related to the operation of the computing device 500. Computing device 500 may also include a network/bus interface 516 coupled to a data link 518. Network/bus interface 516 may be any type of device or system capable of enabling communication with external devices and/or networks 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.).

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

Solution 1: a holographic anti-counterfeiting code verification device comprises:
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 stream of a holographic anti-counterfeiting code under different

projection angles;

extract a projection angle and an image features of the holographic anti-counterfeiting code in each of one or more frames of the video stream;

match the projection angle and the image feature of the holographic anti-counterfeiting code in each frame in a pre-stored mapping table to obtain a matching ratio of the holographic anti-counterfeiting code in each frame, wherein the mapping table stores mapping relationships between different projection angles and image features of a sample holographic anti-counterfeiting code; and

determine whether or not the holographic anti-counterfeiting code is successfully verified according to the matching ratio of the holographic anti-counterfeiting code in each frame.

Solution 2: in the holographic anti-counterfeiting code verification device of Solution 1, the computer-executable instructions, when executed by the one or more processors, cause the one or more processors to:

acquire a plurality of sample images of the sample holographic anti-counterfeiting code under different projection angles;

extract a plurality of sample image features corresponding to the different projection angles from the plurality of sample images; and

construct the mapping table according to correspondence relationships between the different projection angles and the plurality of sample image features.

Solution 3: in the holographic anti-counterfeiting code verification device of Solution 1, the determining whether or not the holographic anti-counterfeiting code is successfully verified according to the matching ratio of the holographic anti-counterfeiting code in each frame comprises:

calculating an average matching ratio of the holographic anti-counterfeiting code in the one or more frames; and

comparing the average matching ratio with a preset threshold to determine whether the holographic anti-counterfeiting code is successfully verified.

Solution 4: in the holographic anti-counterfeiting code verification device of Solution 1, the video stream is obtained by shooting the holographic

anti-counterfeiting code by means of transforming shooting angles with preset angle transformation values.

Solution 5: in the holographic anti-counterfeiting code verification device of any of Solutions 1 to 4, the computer-executable instructions, when executed by the one or more processors, cause the one or more processors to:

extract image features of an anti-counterfeiting label in a plurality of frames of the video stream, wherein the anti-counterfeiting label comprises the holographic anti-counterfeiting code;

compare the image feature of the anti-counterfeiting label in each of the plurality of frames with the image feature of the sample holographic anti-counterfeiting code stored in the mapping table to determine a position of the holographic anti-counterfeiting code in each of the plurality of frames on the anti-counterfeiting label; and

determine authenticity of the video stream according to a change in the position of the holographic anti-counterfeiting code in the plurality of frames on the anti-counterfeiting label.

Solution 6: in the holographic anti-counterfeiting code verification device of Solution 5, authenticity of the video stream is determined according to whether a sudden change occurs in the position of the holographic anti-counterfeiting code in the plurality of frames on the anti-counterfeiting label.

All the above-mentioned alternative technical solutions may be combined arbitrarily to form the alternative embodiments of this disclosure, and no further description is provided herein. In the several embodiments provided in this disclosure, it should be understood that the disclosed method and device may be implemented in other ways. For example, the above-described device embodiments are merely illustrative, for example, the division of the modules is merely a kind of logical and functional division, and other divisions are possible in actual implementations, for example, multiple modules or components may be combined or integrated into another system, or some features may be omitted, or not performed.

It should be noted that in the description of this disclosure, the terms "first",

"second", and the like are used for descriptive purposes only and are not to be construed as indicating or implying a relative importance. Further, in the description of this disclosure, unless otherwise specified, "a plurality of" means two or more.

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 network-coupled computer systems 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 design circuitry, programmable logic arrays, etc..

The above only shows preferred embodiments of this disclosure, and is not intended to limit this disclosure, and any modification, equivalent substitution, improvement, etc. made within the spirit and principle of this disclosure are intended to fall within the scope of protection of this disclosure.

[CLAIMS]

1. A holographic anti-counterfeiting code verification method comprising:
acquiring a video stream of a holographic anti-counterfeiting code under different projection angles;

extracting a projection angle and an image feature of the holographic anti-counterfeiting code in each of one or more frames of the video stream;

matching the projection angle and the image feature of the holographic anti-counterfeiting code in each frame in a pre-stored mapping table to obtain a matching ratio of the holographic anti-counterfeiting code in each frame, wherein the mapping table stores mapping relationships between different projection angles and image features of a sample holographic anti-counterfeiting code; and

determining whether or not the holographic anti-counterfeiting code is successfully verified according to the matching ratio of the holographic anti-counterfeiting code in each frame,

the method further comprises:

extracting image features of an anti-counterfeiting label in a plurality of frames of the video stream, wherein the anti-counterfeiting label comprises the holographic anti-counterfeiting code;

comparing an image feature of the anti-counterfeiting label in each of the plurality of frames with an image feature of the sample holographic anti-counterfeiting code stored in the mapping table, to determine a position of the holographic anti-counterfeiting code in each of the plurality of frames on the anti-counterfeiting label; and

determining authenticity of the video stream according to a change in the position of the holographic anti-counterfeiting code in the plurality of frames on the anti-counterfeiting label.

2. The method according to claim 1, further comprising:

acquiring a plurality of sample images of the sample holographic anti-counterfeiting code under different projection angles;

extracting a plurality of sample image features corresponding to the different projection angles from the plurality of sample images; and

constructing the mapping table according to correspondence relationships between the different projection angles and the plurality of sample image features.

3. The method according to claim 1, wherein the determining whether or not the holographic anti-counterfeiting code is successfully verified according to the matching ratio of the holographic anti-counterfeiting code in each frame comprises:

calculating an average matching ratio of the holographic anti-counterfeiting code in the one or more frames; and

comparing the average matching ratio with a preset threshold to determine whether the holographic anti-counterfeiting code is successfully verified.

4. The method according to claim 1, wherein the video stream is obtained by shooting the holographic anti-counterfeiting code by means of transforming shooting angles with preset angle transformation values.

5. The method according to claim 1, wherein authenticity of the video stream is determined according to whether a sudden change occurs in the position of the holographic anti-counterfeiting code in the plurality of frames on the anti-counterfeiting label.

6. A holographic anti-counterfeiting code verification device, comprising:

a first acquiring module configured to acquire a video stream of a holographic anti-counterfeiting code under different projection angles;

a first extracting module configured to extract a projection angle and an image feature of the holographic anti-counterfeiting code in each of one or more frames of the video stream;

a matching module configured to match the projection angle and the image

feature of the holographic anti-counterfeiting code in each frame in a pre-stored mapping table to obtain a matching ratio of the holographic anti-counterfeiting code in each frame, wherein the mapping table stores mapping relationships between different projection angles and image features of a sample holographic anti-counterfeiting code; and

a first determining module configured to determine whether or not the holographic anti-counterfeiting code is successfully verified according to the matching ratio of the holographic anti-counterfeiting code in each frame,

the device further comprises:

a third extracting module configured to extract image features of an anti-counterfeiting label in a plurality of frames of the video stream, wherein the anti-counterfeiting label comprises the holographic anti-counterfeiting code;

a comparing module configured to compare an image feature of the anti-counterfeiting label in each of the plurality of frames with an image feature of the sample holographic anti-counterfeiting code stored in the mapping table, to determine a position of the holographic anti-counterfeiting code in each of the plurality of frames on the anti-counterfeiting label; and

a second determining module configured to determine authenticity of the video stream according to a change in the position of the holographic anti-counterfeiting code in the plurality of frames on the anti-counterfeiting label.

7. The device according to claim 6, further comprising:

a second acquiring module configured to acquire a plurality of sample images of the sample holographic anti-counterfeiting code under different projection angles;

a second extracting module configured to extract a plurality of sample image features corresponding to the different projection angles from the plurality of sample images; and

a constructing module configured to construct the mapping table according to correspondence relationships between the different projection angles and the plurality of sample image features.

8. The device according to claim 6, wherein the first determining module is configured to:

calculate an average matching ratio of the holographic anti-counterfeiting code in the one or more frames; and

compare the average matching ratio with a preset threshold to determine whether the holographic anti-counterfeiting code is successfully verified.

9. The device according to claim 6, wherein the video stream is obtained by shooting the holographic anti-counterfeiting code by means of transforming shooting angles with preset angle transformation values.

10. The device according to claim 6, wherein the second determining module is configured to determine authenticity of the video stream according to whether a sudden change occurs in the position of the holographic anti-counterfeiting code in the plurality of frames on the anti-counterfeiting label.

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

acquire a video stream of a holographic anti-counterfeiting code under different projection angles;

extract a projection angle and an image feature of the holographic anti-counterfeiting code in each of one or more frames of the video stream;

match the projection angle and the image feature of the holographic anti-counterfeiting code in each frame in a pre-stored mapping table to obtain a matching ratio of the holographic anti-counterfeiting code in each frame, wherein the mapping table stores mapping relationships between different projection angles and image features of a sample holographic anti-counterfeiting code;

determine whether or not the holographic anti-counterfeiting code is successfully

verified according to the matching ratio of the holographic anti-counterfeiting code in each frame,

extracting image features of an anti-counterfeiting label in a plurality of frames of the video stream, wherein the anti-counterfeiting label comprises the holographic anti-counterfeiting code;

comparing an image feature of the anti-counterfeiting label in each of the plurality of frames with an image feature of the sample holographic anti-counterfeiting code stored in the mapping table, to determine a position of the holographic anti-counterfeiting code in each of the plurality of frames on the anti-counterfeiting label; and

determining authenticity of the video stream according to a change in the position of the holographic anti-counterfeiting code in the plurality of frames on the anti-counterfeiting label.