DESCRIPTION

TITLE OF THE INVENTION

IMAGE INFORMATION VERIFICATION APPARATUS

TECHNICAL FIELD

[0001]

The present invention relates to verification of image information and an authentication technology based thereon.

BACKGROUND ART

[0002]

An identification certificate is made, as a general case, by printing attribute information such as a face photograph and a name on a face side of an IC card, a plastic card, or the like and is then issued; however, in recent years when mobile equipment such as smartphones has been widespread, there is a demand for presentation of identification using the mobile equipment which is carried all the times, instead of the card-type identification certificate.

[0003]

When the identification certificate is to be implemented by the mobile equipment, upon digitization of the attribute information such as the face photograph and the name to prove the ID, there are, for example, a possible method of displaying the digitized data on a display of the mobile equipment and verifying the validity of the identification certificate by visually checking it and a possible method of sending the data to verification equipment via communication and having the equipment which performs the verification mechanically verify the validity of the identification certificate data. However, in the latter case, the mobile equipment stores various data other than the identification certificate data in many cases and may possibly mistakenly send unnecessary data to the equipment which performs the verification. Therefore, what is desirable is a mechanism capable of proving the ID simply by displaying and presenting an image of the identification certificate on the display as in the former case.

[0004]

However, in the case of the digitized identification certificate data unlike the conventional card-form identification certificate printed on the face side of the card, it is easy to switch the face photograph to another face photograph and it is difficult to detect the trace of switching the face photograph even if the switched image data is displayed.

[0005]

So, there has been proposed a technology that uses a face photograph and an image of a two-dimensional code, in which data of the face photograph is embedded, as an identification certificate and judges authenticity, when proving the ID, by restoring the face photograph from the two-dimensional code and comparing it with the original face photograph (PTL 1).

CITATION LIST

PATENT LITERATURE

[0006]

PTL 1: Japanese Patent Application Laid-Open (Kokai) Publication No. 2005-141626

SUMMARY OF THE INVENTION

PROBLEMS TO BE SOLVED BY THE INVENTION

[0007]

However, since the face photograph data itself is embedded in the two-dimensional code in the conventional technology, there has been a problem of an increase in the size of the two-dimensional code. Normally, even the face photograph data of the size used for the identification certificate has a data volume of several kilobytes to several tens of kilobytes. Even when the data is compressed, if the face photograph data is embedded in the two-dimensional code and its resolution is set so that the face photograph data can be recognized by a two-dimensional code reader, the size of the two-dimensional code would increase to, for example, about a half of a A4 size depending on the data volume of the face photograph data, which results in a problem of incapability to display that two-dimensional code on the display of a smartphone.

[0008]

Contrarily, if an attempt is made to embed the face photograph data in the two-dimensional code of the size which is small enough to be displayed on the

smartphone, it becomes necessary to reduce the data volume of the face photograph data. So, this causes the face photograph to become a rough image and results in a problem with the difficulty to check the validity of the face photograph by using that rough image.

MEANS TO SOLVE THE PROBLEMS

[0009]

In order to solve the above-described problem, technology used for biometrics authentication is applied to extract feature values capable of uniquely identifying a face photograph (such as the “positions of feature points, such as eyes, a nose, and mouth corners, in a face” and a “cut-out image of only an eye portion which characterizes the face”), from the face photograph data and embed the feature values in a two-dimensional code.

[0010]

Then, when the face photograph and the two-dimensional code are displayed as the same screen on a display of a smartphone to verify the relevant image (which can be used as an identification certificate), image capture equipment such as a digital camera, a WEB camera, or a scanner is used to read the image which is displayed on the display, an electronic signature from the two-dimensional code in the displayed image is verified, and whether the two-dimensional code is authentic or not is judged.

[0011]

Furthermore, another invention authenticates a camera object based on a face image captured by an external camera or the like and the face photograph which has been verified as authentic.

ADVANTAGEOUS EFFECTS OF THE INVENTION

[0012]

The feature of the present invention is that the validity of an image (which can be used as the identification certificate) can be verified using a smaller data volume than that of a case where the face photograph data is embedded in the two-dimensional code.

BRIEF DESCRIPTION OF DRAWINGS

[0013]

Fig. 1 is a diagram illustrating a system configuration example of Embodiment 1 of this invention;
Fig. 2 is a diagram illustrating a hardware configuration example of an issuing apparatus, a verification apparatus, and a smartphone according to Embodiments 1 and 2 of this invention;
Fig. 3 is a sequence diagram illustrating a processing sequence for issuing a digital identification certificate according to Embodiments 1 and 2 of this invention;
Fig. 4 is a sequence diagram illustrating a processing sequence for verifying the digital identification certificate according to Embodiment 1 of this invention;
Fig. 5 is a diagram displaying the verification results of the verification apparatus according to Embodiment 1 of this invention;
Fig. 6 is a diagram illustrating a system configuration example of Embodiment 2 of this invention (the difference from Fig. 1);
Fig. 7 is a sequence diagram illustrating a processing sequence for verifying a digital identification certificate according to Embodiment 2 of this invention and a processing sequence for authenticating a holder of the digital identification certificate; and
Fig. 8 is a diagram illustrating the authentication results of the verification apparatus according to Embodiment 2 (the difference from Fig. 5).

DESCRIPTION OF EMBODIMENTS
[Embodiment 1]
[0014]
--- System Configuration ---
Embodiment 1 of the present invention will be explained below in detail with reference to the drawings.
[0015]
Fig. 1 is a diagram illustrating an overall configuration example of a digital identification certificate system 1 according to this Embodiment 1. This drawing also illustrates a functional configuration example of each computer which configures the digital identification certificate system 1 together with the overall configuration. The digital identification certificate system 1 illustrated in Fig. 1 is a system designed so that an issuing apparatus 10 issues a digital identification certificate (image data) 301 to a smartphone 30 and a verification apparatus 20 reads the image of the digital identification certificate 301 displayed on a display of the smartphone 30 and judges

the authenticity of the presented digital identification certificate 301, based on that image.

[0016]

As illustrated in Fig. 1, the issuing apparatus 10 manages a signature key SK104 for generating an electronic signature and a common key K105 used in common with the verification apparatus 20 and can be configured of: a feature value extracting function 106 which extracts feature values from data of a face photograph, an encryption processing function 103 which executes data encryption and electronic signature generation processing; a two-dimensional code generating function 102 which generates the two-dimensional code; and an identification certificate forming function 101 which forms the digital identification certificate (image data) 301 from face photograph data 302, attribute information 303 such as a name, and a two-dimensional code 304. Furthermore, the verification apparatus 20 is linked to an image capturing equipment 21 and the verification apparatus 20 manages a verification key PK204 for verifying the electronic signature and a common key K205 used in common with the issuing apparatus 10 and can be configured of: a data reading function 201 which reads an image of the digital identification certificate 301 displayed on the display of the smartphone 30; a two-dimensional code reading function 202 which takes out a two-dimensional code portion 304 from the read image and decodes the two-dimensional code; an encryption processing function 203 which executes processing for decoding the data and verifying the electronic signature; a character recognition function 206 which recognizes characters of the attribute information 303 such as a name from the image of the read digital identification certificate 301; a matching function 207 which compares the feature values embedded in the two-dimensional code with the face photograph image 302 included in the image of the read digital identification certificate 301 and performs verification; and a verification result processing function 208 which displays screens according to the verification result and issues an instruction to open or close a gate for entrance and exit management. Furthermore, the smartphone 30 installs and stores the digital identification certificate (image data) 301 acquired by, for example, distribution via a network or a medium and displays the digital identification certificate 301 on the display as necessary.

[0017]

The issuing apparatus 10, the verification apparatus 20, and the smartphone 30 which have the above-described functions can be implemented by general information processing equipment 40 as illustrated in Fig. 2. For example, the feature value extracting function 106, the encryption processing function 103, the two-dimensional code generating function 102, and the identification certificate forming function 101 of the issuing apparatus 10 and the data reading function 201, the two-dimensional code reading function 202, the encryption processing function 203, the character recognition function 206, the matching function 207, and the verification result processing function 208 of the verification apparatus 20 can be implemented as computer programs executed by a CPU 405 such as a CPU (Central Processing Unit). These computer programs can be used by, for example, storing it in advance in a storage device 404 such as a hard disk and retaining it there or receiving its distribution from a network and expanding it in a memory 403.

[0018]

Furthermore, instructions from a user who uses this digital identification certificate system 1 are input via an input device 401 such as a keyboard, a mouse, and a touch panel which accept inputs; and processing results obtained as a result of the instructions are output from an output device 402 such as a liquid crystal display device and an organic EL (Electro Luminescence) display.

[0019]

These devices for the issuing apparatus 10, the verification apparatus 20, and the smartphone 30 can be configured in the information processing equipment 40 connected via an internal communication line such as a bus (hereinafter referred to as the bus) 406.

[0020]

Furthermore, the image capturing equipment 21 linked to the verification apparatus 20 is implemented by equipment such as a digital camera, a WEB camera, or a scanner.

[0021]

--- Processing Sequence Examples ---

The processing sequences according to this Embodiment 1 will be explained below with reference to the drawings. Various types of operations explained below are implemented by programs that are read to a memory or the like and executed respectively by the respective apparatuses/devices which configure the digital identification certificate system 1.

[0022]
Fig. 3 is a sequence diagram illustrating a processing sequence for issuing the digital identification certificate 301 according to this embodiment.
[0023]
The face photograph data 302 of a person who should become a holder of the digital identification certificate 301 is input to the issuing apparatus 10; and the issuing apparatus 10 employs the feature value extracting function 106 and thereby extracts the feature values (such as the “positions of feature points, such as eyes, a nose, and mouth corners, in a face” and a “cut-out image of only an eye portion which characterizes the face”) which are of a relatively small data volume and are capable of uniquely identifying the face photograph, from the face photograph data 302 (step S101). Then, the issuing apparatus 10 employs the encryption processing function 103 and thereby encrypts the feature values with the common key K105 to be used in common with the verification apparatus 20 (step S102). Furthermore, the attribute information 303 such as the name of the person who should become the holder of the digital identification certificate 301 is input to the issuing apparatus 10 and the issuing apparatus 10 connects the attribute information 303 to the encrypted feature values (step S103). Next, the issuing apparatus 10 calculates an electronic signature value with respect to data of the encrypted feature values and the attribute information 303, which are connected together, by using the signature key SK104 of the issuing apparatus 10 and assigns the electronic signature value to the data of the encrypted feature values and the attribute information 303 which are connected together (step S104). Then, the two-dimensional code generating function 102 is employed and the two-dimensional code 304 is thereby generated by using the encrypted feature values, the attribute information 303, and the electronic signature data which are connected together, as inputs. Specifically speaking, the above-described connected data are encoded into the two-dimensional code (step S105). Then, the issuing apparatus 10: employs the identification certificate forming function 101 and thereby locates and forms the face photograph data 302, the attribute information 303, and the two-dimensional code 304 so that they can be displayed at the same time on the display of the smartphone (step S106); and outputs them externally as the digital identification certificate (image data) 301 (step S107).
[0024]

The smartphone 30 acquires the digital identification certificate (image data) 301 by, for example, distribution via a network or a medium (step S108) and stores the digital identification certificate (image data) 301 in the storage device 404 for the smartphone 30 (step S109).

[0025]

Fig. 4 is a sequence diagram illustrating a processing sequence for verifying the digital identification certificate according to this Embodiment 1.

[0026]

The smartphone 30 displays the digital identification certificate (image data) 301, which was stored in step S109, on the display of the smartphone 30 and presents it to the image capturing equipment 21 (step S200).

[0027]

The image capturing equipment 21 captures the image displayed on the display of the smartphone 30 (step S201); and the verification apparatus 20 acquires a screen image captured by the image capturing equipment 21 from the image capturing equipment 21 (step S202). Then, the verification apparatus 20 reads the two-dimensional code from the screen image acquired by the two-dimensional code reading function 202 in step S202 and decodes the two-dimensional code (step S203). The decoded data is composed of the encrypted feature values , the attribute information, and the electronic signature value and the electronic signature is verified based on these pieces of data by using the encryption processing function 203 (step S204). If the signature verification fails, it is displayed, as error processing, on the display of the verification apparatus 20 as illustrated in a drawing at the upper left part of Fig. 5 that the two-dimensional code 304 portion in the digital identification certificate 301 is false and the signature verification has thereby failed (step S205).

[0028]

If the signature verification is successful, characters relating to the attribute information 303 from the screen image acquired in step S202 are recognized by using the character recognition function 206 and are compared with the attribute information decoded in step S203 to perform verification (step S206). If these pieces of information do not match each other, it is displayed, as the error processing, on the display of the verification apparatus 20 as illustrated in a drawing at the upper right part of Fig. 5 that the attribute information 303 portion in the digital identification

certificate 301 is false and the attribute information has been forged, and then correct attribute information is displayed (step S207).

[0029]

If the above-described pieces of the attribute information match each other, the encryption processing function 203 is employed and the encrypted feature values decoded in step S203 are thereby decoded with the common key K205 (step S208); and the decoded feature values are compared with a face photograph portion of the screen image acquired in step S202 to perform the verification by using the matching function 207 and whether the feature values are the data extracted from that face photograph or not is verified (step S209). The matching function 207 expresses the correlation between the face photograph and the feature values as a numerical value; and if a matching rate between the face photograph and the feature values is equal to or less than a threshold value, it is displayed, as the error processing, on the display of the verification apparatus 20 as illustrated in a drawing at the lower left part of Fig. 5 that the face photograph 302 portion in the digital identification certificate 301 is false and the face photograph has been forged (step S210).

[0030]

If the matching rate between the face photograph and the feature values is equal to or more than the threshold value, it is displayed, as authenticity result processing, on the display of the verification apparatus 20 as illustrated in a drawing at the lower right part of Fig. 5 that the digital identification certificate 301 is authentic (step S210).

[Embodiment 2]

[0031]

Embodiment 2 of the present invention will be explained in detail with reference to the drawings. Embodiment 2 is implemented in addition to Embodiment 1.

[0032]

Fig. 6 is a diagram illustrating an overall configuration example of a digital identification certificate system 2 according to this Embodiment 2 (the difference from Fig. 1). In Embodiment 2, the verification apparatus 20 is a system that is also linked to a portrait image capturing equipment 22 and also verifies whether a person who presented the digital identification certificate 301 is a right holder or not, via a face authentication function 209 used for biometrics authentication based on the face photograph 302 and videos and images captured by the portrait image capturing equipment 22. The portrait image capturing equipment 22 which is linked to the

verification apparatus is implemented by equipment such as a digital camera or a WEB camera.

[0033]

It should be noted that in Embodiment 2, the digital identification certificate 301 is issued in the same manner as in Embodiment 1.

[0034]

Fig. 7 is a sequence diagram illustrating a processing sequence for verifying the digital identification certificate according to this Embodiment 2 and a processing sequence for authenticating the holder of the digital identification certificate. Steps from S200 to step S210 are the same processing as that of Embodiment 1.

[0035]

The portrait image capturing equipment 22 captures an image of a person who presented the digital identification certificate 301 (step S301); and the verification apparatus 20 acquires a portrait image captured in step S301 from the portrait image capturing equipment 22 (step S302). Then, the verification apparatus 20 performs comparison and verification by using the face photograph data, which was determined as authentic in step S209, and the portrait image data acquired in step S301, and thereby verifies whether the person who presented the digital identification certificate 301 is the right holder or not (step S303). The face authentication function 209 expresses the correlation between the face photograph and the portrait image as a numerical value; and if a matching rate between the face photograph and the portrait image is equal to or less than a threshold value, it is displayed, as error processing, on the display of the verification apparatus 20 as illustrated in a drawing at the upper part of Fig. 8 that the face photograph 302 of the digital identification certificate 301 does not match the face of the person who presented the digital identification certificate 301 (step S304).

[0036]

If the matching rate between the face photograph and the portrait image is equal to or more than the threshold value, it is displayed, as authenticity result processing, on the display of the verification apparatus 20 as illustrated in a drawing at the lower part of Fig. 8 that the digital identification certificate 301 is authentic and matches the face of the person who presented the digital identification certificate 301 (step S305).

REFERENCE SIGNS LIST

[0037]

1: digital identification certificate system

2: digital identification certificate system

10: issuing apparatus

20: verification apparatus

21: image capturing equipment

22: portrait image capturing equipment

30: smartphone

40: information processing equipment

101: identification certificate forming function

102: two-dimensional code generating function

103: encryption processing function

104: signature key SK

105: common key K

106: feature value extracting function

201: data reading function

202: two-dimensional code reading function

203: encryption processing function

204: verification key PK

205: common key K

206: character recognition function

207: matching function

208: verification result processing function

209: face authentication function

301: digital identification certificate

302: face photograph

303: attribute information

304: two-dimensional code

401: input device

402: output device

403: memory

404: storage device

405: CPU (Central Processing Unit)

406: bus

CLAIMS

[Claim 1]
An image information verification apparatus comprising:
an extraction unit that reads an image and extracts an identifier image and a face image from the image;
an identifier image verification unit that verifies the identifier image based on an electronic signature included in the identifier image; and
an image verification unit that compares first feature value information extracted from the face image with second feature value information included in the identifier image and verifies authenticity of the image information.
[Claim 2]
The image information verification apparatus according to claim 1,
wherein the extraction unit further extracts an attribute information image regarding the face image from the image; and
wherein the image verification unit further compares attribute information included in the identifier image with the extracted attribute information image and verifies authenticity of the image information.
[Claim 3]
The image information verification apparatus according to claim 2,
wherein the first feature value and the second feature value are information regarding a feature point position in a face.
[Claim 4]
The image information verification apparatus according to claim 3,
further comprising a display unit that displays a result of the verification.
[Claim 5]
An authentication system comprising the image information verification apparatus stated in claim 4 and an image capturing apparatus,
wherein the image information verification apparatus further includes an authentication unit that compares an image captured by the image capturing apparatus with the face image and authenticates an object whose image has been captured by the image capturing apparatus.
[Claim 6]
The authentication system according to claim 5,

wherein the authentication unit compares the captured image with the face image by using the feature values.

[Claim 7]

The authentication system according to claim 6,

further comprising a gate that executes processing according to a result of the authentication of the object.

[Claim 8]

The authentication system according to claim 7,

wherein the identifier image is created by encrypting the second feature value with a public key.

[Claim 9]

An image information verification method comprising:

an image reading step of reading an image;

an extraction step of extracting an identifier image and a face image from the image;

an identifier image verification step of verifying the identifier image based on an electronic signature included in the identifier image; and

an image verification step of comparing first feature value information extracted from the face image with second feature value information included in the identifier image and verifying authenticity of the image information.

[Claim 10]

An authentication method comprising:

an image reading step of reading an image;

an extraction step of extracting an identifier image and a face image from the image;

an identifier image verification step of verifying the identifier image based on an electronic signature included in the identifier image;

an image verification step of comparing first feature value information extracted from the face image with second feature value information included in the identifier image and verifying authenticity of the image information; and

an authentication step of comparing an image captured by an image capturing apparatus with the face image and authenticating an object whose image has been captured by the image capturing apparatus.