

SPECIFICATION

CARD WHICH CAN BE AUTHENTICATED BY HOLOGRAM CHIP

Field of The Invention

[0001]

The present invention relates to a structure of an object such as a card, a bank note, securities, etc., which is often forged or counterfeited and which requires authentication to check whether it is authentic or not. The invention also relates to a method for identifying authenticity of such the object.

Background Art

[0002]

In the present-day society, which is often called a card-oriented society, a great number of different types of cards are widely propagated. Specifically, a cash card and a credit card issued by a credit company which are relating to the assets of property owners and a prepaid card as securities, and identification cards such as a driver's license, a health insurance card and a passport are widely used.

[0003]

In many of the cards relating to property or securities and bonds, necessary information is written on a magnetic stripe disposed on the surface or on the rear surface of the card. By using automatic machines such as an ATM (automated teller machine) or a manual reading device, the magnetic information is read from the magnetic stripe, and various types of processing are executed.

[0004]

Fig. 1 shows an example of a flow of processing the cash card currently in use.

(1) When an owner of a card inserts the cash card into a card slot of a terminal

device such as an ATM, a sensor at the card slot senses the inserted card, and the card is taken into the device.

[0005]

(2) When the card is taken into the device, the terminal device reads card information from a magnetic recording portion of the card. In case of a cash card, the card information such as a bank code, a bank branch code, a type of account, an account number, etc. is read. A card identification number, the expiration date, a type of account and an account number are recorded as the card information on the magnetic recording portion of a credit card. If a personal identification number is recorded on a cash card or a credit card, the personal identification number is also read.

[0006]

(3) The terminal device judges whether or not the inserted card is a valid card, which can be handled by the terminal device.

[0007]

(4) If it is not confirmed that the card can be handled by the device from the card information thus read, or if the information on the card cannot be read because the card is broken or stained even though the card is a valid card, the terminal device judges that it is an invalid card which cannot be handled and discharges the card.

[0008]

(5) When the card is a valid card and when the information on the magnetic recording portion of the card has been read correctly, communication with a host computer starts.

[0009]

(6) The host computer requests the inputting of the personal identification number.

[0010]

(7) In response to the request from the host computer, the card user inputs the personal identification number.

[0011]

(8) When the card user inputs the personal identification number in response to the request of the host computer, the host computer compares the inputted personal identification number with the personal identification number which is stored in the host computer and which corresponds to the card information thus read.

[0012]

(9) If the numbers differ, this fact is recorded on the magnetic recording portion of the card, and the inputting of the personal identification number is requested again. In a case where the personal identification number inputted again is proper and valid, subsequent procedure is carried out. In a case where the inputted number differs from the stored number, the inputting of the personal identification number is requested further again. If erroneous inputting of the personal identification number is repeated three times, the card is invalidated and is, for example, taken into the terminal device as the result of invalidation procedure.

[0013]

(10) In a case where the personal identification numbers are equal, the host computer judges that the card user is a legitimate card owner and requests the user to input the amount to be paid.

[0014]

(11) The user inputs the amount which he (she) wishes to draw.

[0015]

(12) When the amount to be paid is proper, the amount is paid and the cash card is discharged from the terminal device. Then, the payment is recorded on a bankbook, or a slip indicating the dealing is issued, and the processing finishes. If the personal identification number is recorded on the cash card, the dealing is carried out under the assumption that the personal identification number is valid. Then, the personal identification number is erased from the magnetic recording portion.

[0016]

Fig. 2 (a) illustrates an example of the cash card used in the processing flow of the currently used cash card as shown in Fig. 1. The reference number 1 shows a cash card body made of a material such as plastics. On the surface of the card, a magnetic stripe 2 where information is recorded and an arrow mark 3 to indicate the direction to insert the cash card are disposed. Although not shown in the drawing, other necessary matters are entered thereon by embossed characters.

[0017]

As information written in the magnetic stripe can be easily read by using a device called a skimmer, the card may be forged, and often causes damage by using the card thus forged.

[0018]

To cope with this problem, an IC card incorporating a semiconductor memory has been used. Banks and other organizations have been making efforts to propagate this type of card to replace the magnetic card.

[0019]

However, the information stored in the memory of the IC card is still possible to be read. If more elaborate forgery is attempted, we may not be able to say that the IC card is absolutely safe. In addition, the IC card is very expensive compared to the magnetic card, and it would be hard to expect the rapid propagation of IC cards.

[0020]

In case of the cash card used in banks, it would suffice if the card can be used within the boundary of one country. However, in case of the credit card, the card is necessary to be used also in foreign countries. It is practically impossible to replace all of the credit cards, i.e. magnetic cards, used in the whole world with IC cards under unified standards.

[0021]

Further, in cash cards and credit cards, the information such as the name of the card owner is marked by embossing, and these types of information are also used for the magnetic information. In this respect, the embossed information may be used as a clue or a key in the preparation for forging a card.

[0022]

If the magnetic card or the IC card is lost or stolen, and if the card returned into the hand of the card owner, in particular, when the card owner does not aware of the fact of stealing, it is liable to cause damage by the use of the forged card.

[0023]

A personal identification number, consisting of 4-digit numbers, has been used not for preventing cards from being illegitimately used by the prevention of the forgery but as the means to determine whether or not the card user is proper. Since

assumable numbers have been often used for these personal identification numbers, there have been many cases of the loss and damage. In recent years, the personal identification number is stolen not only by assumption of it but also by peeping such as the means of stealthily taking a photograph of the personal identification number. It is now very difficult to prevent the illegitimate use of cards by using the personal identification number.

[0024]

For the purpose of preventing the damage caused by the forged card, some adopts the biometric technique using the pattern recognition technology. The typical examples of the biometric technique are iris recognition, fingerprints recognition, palm-prints recognition, finger vein recognition, palm vein recognition, and hand-back vein recognition. For these recognition, it is necessary to register the pattern in advance. Time and procedures are required for the registration of the pattern, and also time is needed for the recognition of the pattern itself and for determining, and that results higher costs.

[0025]

In case of the contact-type recognition, the user must come into direct contact with the detection device, and there arises a problem that the user may feel physiological repugnance or disgust. Also, in a case where the user has injury on the physical part necessary for the biometrical recognition, or in the worst case, where the user has lost the physical part to be needed for the recognition, it is impossible to use the biometrical recognition. Also, the recognition is partially made during the process of identifying, and accordingly, it is not a perfect method.

[0026]

In the system using the biometrical recognition, the card user himself or herself can only use his or her own card. When the card user has not enough time to use

the card personally or does not find a card processing device nearby, even if the user wants to entrust a representative or an agent to use the card, it is not allowed. This is very inconvenient for the user.

[0027]

As one of the means for preventing the forgery, an embossed hologram is mounted to form surface irregularities on the plastic surface in case of credit cards, prepaid cards, securities, etc. This embossed hologram is very difficult to duplicate. In this respect, it is actually impossible to forge the card provided with the embossed hologram. In the current condition of the use, however, it is a person, who read the embossed hologram at a glance. Thus, it is possible that the card is forged by using the embossed hologram of similar type.

[0028]

Fig. 2 (b) illustrates an example of a credit card with the embossed hologram, on which the card authentication is verified according to the human sense. The reference numeral 1 shows a credit card body made of a material such as plastics. On the surface of the card, a magnetic stripe 2 where information is recorded and an arrow mark 3 to indicate the direction to insert the cash card are disposed. Although not shown in the drawing, other necessary matters are entered thereon by embossed characters.

[0029]

This cash card 1 is inserted into a terminal device with a portion with the arrow mark placed at the foremost position. Near the foremost portion on the card, an authentication verifying chip 4 consisted of, for example, an embossed hologram is mounted.

[0030]

The magnetic stripe is disposed, unlike the cash card, on the rear surface of the credit card, but the direction to insert the card into the terminal device is the same. As a result, the direction to read the magnetic information on the credit card is reverse to that of the cash card.

[0031]

In the authentication verifying chip 4, a pattern "A", as an example, is confirmed by a person, who inserts the card into the terminal device, visually, i.e. by sensuous means, but is not read by the card terminal device.

[0032]

The authentication verifying by sensuous means provides high effects in primary screening but its reliability is low because there are variations in the ability of each individual person who confirms and identifies or there are also variations in the identifying environment and psychological and/or physical conditions of the person.

[0033]

The method for reading the embossed hologram pattern by machine can be roughly divided as a method for reading an image in a planar shape by means such as a camera; and a method for reading data in a linear shape by the combination of light emitting elements and light detecting elements. The method for reading the image in the planar shape is effective for verifying the authenticity, while the amount of information to be processed is large and the device for this method is more complicated.

[0034]

The arrangements for reading data in the linear shape are disclosed in Japanese Patent Laid-Open Publication Nos. H06-124866, H06-318282, H07-220077, H09-319849, H11-180079, H10-143621, 2000-47557, 2000-48146 and 2002-74283.

[0035]

According to each of the methods described in these references, the embossed hologram is read along a straight line in longitudinal direction of a rectangular shape card where the embossed hologram or a diffraction grating is formed. As a result, the device used is relatively simple in structure and it is easy to use, however, is less resistant to forgery.

[0036]

In addition to the above references, Japanese Patent Laid-Open Publication No. H11-272836 discloses an identification technique using a diffraction grating, Japanese Patent Laid-Open Publication No. 2002-279480 discloses an identification technique using embossed hologram and moire, and Japanese Patent Laid-Open Publication No. 2002-341733 discloses an identification technique using embossed hologram and latent image.

[0037]

The arrangements for reading data in the linear shape are disclosed in Japanese Patent Laid-Open Publication Nos. H06-124866, H06-318282, H07-220077, H09-319849, H11-180079, H10-143621, 2000-47557, 2000-48146 and 2002-74283.

[0038]

According to each of the methods described in these references, the embossed hologram is read along a straight line in longitudinal direction of a rectangular shape card where the embossed hologram or a diffraction grating is formed. As a result, the device used is relatively simple in structure and it is easy to use, however, is less resistant to forgery.

[0039]

In addition to the above references, Japanese Patent Laid-Open Publication No. H11-272836 discloses an identification technique using a diffraction grating, Japanese Patent Laid-Open Publication No. 2002-279480 discloses an identification technique using embossed hologram and moire, and Japanese Patent Laid-Open Publication No. 2002-341733 discloses an identification technique using embossed hologram and latent image.

[0040]

When verifying the authentication by using an auxiliary tool, it is carried out by ultra-fine lines, special lines and micro-characters by using a screen with special shape, a magnifying device such as a magnifying glass or a special type filter generating optical interferences.

[0041]

Practically, a light-emitting base material or a material having a special optical property such as a light-emitting laminated film, light-emitting ink, thermo-chromic ink, photo-chromic ink, etc., is mixed into the base material, laminated film or ink and the auxiliary tool of a special filter, a ultra-violet ray lamp, etc. is used. However, these are also low in reliability because recognition and identification are consequently relying on the human sense.

[0042]

The authentication verifying by mechanical processing is to verify authenticity by mechanically detecting the property of the object material. The magnetic property and the optical property may be used for the detection.

[0043]

Practically, a light-emitting material or a magnetic material is mixed into a base material, laminated film or ink and a detection device is used. Or, specific coded

information is magnetically or optically added by using OCR characters or magnetic barcodes, and a magnetic or optical detection device is used.

[0044]

In the authentication verifying by the mechanical processing, an artifact-metrics system using an artifact without having reproducibility, randomly arranged in a medium, is used instead of the information specific to the living body. This is described in "Financial Business and Artifact-Metrics" published by the Institute for Monetary and Economic Studies, the Bank of Japan (<http://www.imes.boj.or.jp/japanese/jdps/2004/04-J-12.pdf>) and "The Patterns of Artifact-Metrics in Financial Field"; 6th Information Security Symposium (<http://www.imes.boj.or.jp/japanese/kinyu/2004/kk23-2-6.pdf>) .

[0045]

In the artifact-metrics system, a light reflecting pattern of granular substances, a transmission light pattern of optical fibers, a parallax image pattern of polymer fibers, a fiber image pattern, a magnetic pattern of magnetic fibers, a random-recorded magnetic pattern, a random magnetic pattern of a magnetic stripe, a random electric charge pattern of a memory cell, a resonance pattern of electrically conductive fibers, a resonance pattern of a vibrating seal, etc., which are formed by chance, are used.

[0046]

As the matters subject to the illegitimate use or the forgery of the card, "the information of the descriptions of the card" added when the card is issued to a user and "the information of the card" given to the card in the manufacturing process are included. ("Handbook on the Technique to Prevent Forgery on the Surface of Affiliated IC Cards", published by the National Printing Bureau, the Ministry of Finance (see: <http://www.npb.go.jp/ja/info/ichb.pdf>) .

[0047]

The information of the descriptions of the card is the information which is accorded and printed on the card body when issued to the user, and which is relating to the card issuance such as the card owner information, the period of validity, etc.

[0048]

Falsification, which is a typical act of the illegitimate use of the card, is an act to alter all or a part of the information of the descriptions of the card, done by erasing the genuine information and adding illegitimate information.

[0049]

The information of the card is the information of the card itself, other than the information of the descriptions of the card in the issued card. It is the information relating to the card body such as the physical shape of the card, background patterns applied to the card in pre-printing factory, printing layer on underlying layer and protected laminated layer, etc.

[0050]

Forgery is an illegal act carried out for the card body. It is carried out by duplicating or imitating the design, patterns, etc., relating to the card body to forge a card, which is similar to the authentic card in the external appearance. Actually, the design, patterns, etc. on the surface of the authentic card are read by the means such as a scanner, which are then, edited or amended by using the means such as a printer.

[0051]

Many types of techniques to prevent the forgery of the card body are known through combining the printing mode, types of ink, printing patterns, etc., only in

the printing art, but no decisive technique is known yet at present.

[0052]

The methods for authentication verifying to recognize and identify the forgery can be roughly classified as a method based on human sensuous ability; a method using auxiliary tools; and a method by mechanical processing.

[0053]

In the authentication verifying by the human sensuous ability, the authenticity of a card is identified by the sensuous ability such as the visual sense, the tactile sense, etc. The means to identify by the visual sense includes colors of the card itself, a watermark and an embossed hologram, which changes the color and patterns provided on the card by changing the viewing angle. The means to identify by the tactile sense includes detecting the surface irregularities added on the card and detecting the texture of the card body itself. Actually, a logo mark, a special font, printing lines for preventing duplication, special color ink, embossed hologram, an optically changing material, a latent image pattern, etc., which are difficult to duplicate or copy and in which the authenticity of the card can be easily identified by the visual sense are used. And embossing, surface irregularities, perforation, etc. are also used, on which the authenticity can be identified by finger feeling or by the visual sense.

[0054]

Fig. 3 shows a conventional example of a card, to which an artifact-metrics chip using metal granules is mounted as disclosed in Japanese Patent Laid-Open Publication No. H10-44650. Fig. 3 (a) is a general view, Fig. 3 (b) is a cross-sectional view and Fig. 3 (c) is an enlarged view of the card.

[0055]

In the card 1, the artifact-metrics chip 4 in thin-plate shape made of a transparent resin mixed with metal granules 5 is layered on a card base member 7, having a non-transparent property, which has an opening 8 for the authentication verifying chip on it. And a non-transparent card surface plate 6 is further layered, in which a magnetic stripe 2 and an arrow mark 3 are formed thereon and another opening is arranged at the same position as the opening on the card base member 7.

[0056]

The metal granules 5 are mixed three-dimensionally in the transparent resin without regularity. As a result, the arrangement pattern of the metal granules 5 observed through the opening is inherent in each of the artifact-metrics chip 4. By utilizing these characteristics, a light to pass through the artifact-metrics chip 4 is photographed via the opening, and the arrangement pattern of the metal granules 5 can be observed. Therefore, it is possible to identify each individual artifact-metrics chip 4 and then, the card.

[0057]

Fig. 4 shows another conventional example of a card, to which an artifact-metrics chip using fibers as disclosed in Japanese Patent Laid-Open Publication No. 2003-29636. Fig. 4 (a) is a general view, Fig. 4 (b) is a cross-sectional view and Fig. 4 (c) is an enlarged view of the artifact-metrics chip.

[0058]

In the card, the artifact-metrics chip 8 containing a mesh member 9 and short fibers 10 three-dimensionally mixed in a transparent resin is placed into an opening of the card base member 1, which has a non-transparent property and a magnetic stripe 2 and an arrow mark 3 are disposed on the surface thereof. On the artifact-metrics chip 8, an interference pattern is generated by the pattern of the mesh member 9 and the short fibers 10.

[0059]

This interference pattern is inherent in each of the artifact-metrics chip 8, i.e., in each card. By utilizing this characteristic, the pattern of the artifact-metrics chip 8 of the authentication verifying chip is photographed by a transmitted light or a reflected light for the card to be identified.

[0060]

Mechanical reading of such the pattern of biometrics or artifact-metrics is generally performed by an image-pickup device and the result is identified by a pattern recognition technique. In this respect, there is a possibility that forgery can be made according to a duplicating technique.

[0061]

The arrangements for reading data in the linear shape are disclosed in Japanese Patent Laid-Open Publication Nos. H06-124866, H06-318282, H07-220077, H09-319849, H11-180079, H10-143621, 2000-47557, 2000-48146 and 2002-74283.

[0062]

According to each of the methods described in these references, the embossed hologram is read along a straight line in longitudinal direction of a rectangular shape card where the embossed hologram or a diffraction grating is formed. As a result, the device used is relatively simple in structure and it is easy to use, however, is less resistant to forgery.

[0063]

In addition to the above references, Japanese Patent Laid-Open Publication No. H11-272836 discloses an identification technique using a diffraction grating, Japanese Patent Laid-Open Publication No. 2002-279480 discloses an identification

technique using embossed hologram and moire, and Japanese Patent Laid-Open Publication No. 2002-341733 discloses an identification technique using embossed. As described above, the technique to determine the authenticity of the card itself is not yet firmly established, and a card, which cannot be forged, is not realized.

Also, the technique to eliminate the use of a forged card is not yet realized.

[Patent Document 1] Japanese Patent Laid-Open Publication No. H10-44650

[Patent Document 2] Japanese Patent Laid-Open Publication No. 2003-29636

[Patent Document 3] Japanese Patent Laid-Open Publication No. H06-124866

[Patent Document 4] Japanese Patent Laid-Open Publication No. H06-318282

[Patent Document 5] Japanese Patent Laid-Open Publication No. H07-220077

[Patent Document 6] Japanese Patent Laid-Open Publication No. H09-319849

[Patent Document 7] Japanese Patent Laid-Open Publication No. H11-180079

[Patent Document 8] Japanese Patent Laid-Open Publication No. H11-272836

[Patent Document 9] Japanese Patent Laid-Open Publication No. H10-143621

[Patent Document 10] Japanese Patent Laid-Open Publication No. 2000-47557

[Patent Document 11] Japanese Patent Laid-Open Publication No. 2000-48146

[Patent Document 12] Japanese Patent Laid-Open Publication No. 2000-66567

[Patent Document 13] Japanese Patent Laid-Open Publication No. 2000-298880

[Patent Document 14] Japanese Patent Laid-Open Publication No. 2002-74283

[Patent Document 15] Japanese Patent Laid-Open Publication No. 2002-279480

[Patent Document 16] Japanese Patent Laid-Open Publication No. 2002-341733

[Patent Document 17] Japanese Patent Laid-Open Publication No. 2005-205897

[Non-Patent Document 1] "Financial Business and Artifact-Metrics" published by the Institute for Monetary and Economic Studies, the Bank of Japan

(<http://www.imes.boj.or.jp/japanese/jdps/2004/04-J-12.pdf>)

[Non-Patent Document 2] "The Patterns of Artifact-Metrics in Financial Field"; 6th Information Security Symposium

(<http://www.imes.boj.or.jp/japanese/kinyu/2004/kk23-2-6.pdf>)

[Non-Patent Document 3] "Handbook on the Technique to Prevent Forgery on

the Surface of Affiliated IC Cards", published by the National Printing Bureau, the Ministry of Finance (<http://www.npb.go.jp/ja/info/ichb.pdf>)

[Non-Patent Document 4] Nikkei Electronics; No. 883

Disclosure of The Invention

Object of The Invention

[0064]

It is an object of the present invention to provide a structure of a card for increasing security without adding basic changes to a cash card or a credit card as practically used, and to provide a method for processing the card and a card processing device.

Means

[0065]

To attain the above object, an authentication verifying chip formed with an embossed hologram or with a diffraction grating is non-separably fixed on the card.

[0066]

A card authentication verifying device is provided in an apparatus for processing the card. For detecting information of the verifying chip, in addition to making the card in a fixed condition, scanning it by utilizing the movement of the verifying chip when the card is taken into the apparatus is carried out.

Effects of The Invention

[0067]

Because the embossed hologram or the diffraction grating utilizing the optical interference has a three-dimensional structure, it is impossible to duplicate it unless produce a replica directly from the prototype. For this reason, even when the magnetic recording data or the data in the IC chip may be copied as practiced

in the past, it is practically impossible to use a forged card.

[0068]

Further, when it is attempted to illegally use the card, such the use can be rejected and damage or loss can be prevented before it actually occurs. Or, an illegitimate card may be allowed for the use to some extent, but it is easily possible to specify the user of the illegitimate card by finally ensuring to hold the illegitimate card. The use of illegitimate card can be prevented before it is actually used or the use of the illegitimate card can be easily detected and accordingly, illegal use of the card can be prevented.

Brief description of the drawings

[0069]

Fig. 1 is a flow chart to show a flow of the processing of a currently used cash card;

Fig. 2 shows a cash card and a credit card of conventional type;

Fig. 3 shows an example of a conventional type card using artifact-metrics by using metal granules;

Fig. 4 shows an example of a conventional type card using artifact-metrics by using fibers;

Fig. 5 shows a card using an embossed hologram according to the present invention;

Fig. 6 shows an example of writing authentication verifying data using an embossed hologram;

Fig. 7 shows examples of the mounting position of the authentication verifying chip;

Fig. 8 shows an example of authentication verifying data of the present invention as prepared by a computer;

Fig. 9 is an example of random numbers to be used in the verifying chip according to the present invention;

Fig. 10 shows an arrangement example of random numbers to be used in the verifying chip according to the present invention;

Fig. 11 shows an example where the random numbers used in the verifying chip are arranged in binary numbers according to the present invention;

Fig. 12 shows an arrangement example where the random numbers used in the verifying chip are in binary numbers according to the present invention;

Fig. 13 shows an example of the additional random numbers used in the verifying chip according to the present invention;

Fig. 14 shows an example where additional random numbers used in the verifying chip are arranged in binary numbers according to the present invention;

Fig. 15 shows an example where additional random numbers used in the verifying chip are arranged in quaternary numbers according to the present invention;

Fig. 16 shows an arrangement example where the random numbers used in the verifying chip are in quaternary numbers according to the present invention;

Fig. 17 shows an example where a plurality of verifying chips are obtained from one random numbers group;

Fig. 18 shows a verifying chip reading device using an image pickup device;

Fig. 19 shows a verifying chip reading device using reading elements in a matrix form;

Fig. 20 shows a verifying chip reading device using a mono-color reading device in array;

Fig. 21 shows arrangements of a device detecting the mono-color in array;

Fig. 22 shows a verifying chip reading device using multi-color reading elements in array;

Fig. 23 shows an arrangement of a device detecting the multi-color in array;

Fig. 24 shows a verifying chip reading device designed with a paraboloid mirror and a polygonal mirror combined;

Fig. 25 shows a verifying chip reading device using a single reading element according to the present invention;

Fig. 26 shows a verifying chip reading device using two reading elements according to the present invention;

Fig. 27 shows an example of a reading route;

Fig. 28 shows examples of a different reading route;

Fig. 29 shows a reading route of a verifying chip using binary random numbers;

Fig. 30 shows an example of the feature extraction on a verifying chip using binary random numbers;

Fig. 31 shows an example of the feature extraction on a verifying chip using quaternary random numbers;

Fig. 32 shows an example of analog processing of the verifying chip using binary random numbers;

Fig. 33 shows an example of a mark for position alignment, a reading start line, a reading finish line, and a mark for synchronization signal;

Fig. 34 shows an example of a flow of card authentication verifying processing;

Fig. 35 shows another example of a flow of card authentication verifying processing;

and

Fig. 36 shows still another example of a flow of card authentication verifying processing.

Brief Description of The Reference Numerals

[0070]

1, 11 card

2 a magnetic stripe

3 an arrow

4, 8, 11, 12, 15, 18, 21, 22, 32, 42, 46, 78, 124, 126, 128

an authentication verifying chip

5 metal granules

6, 14 a surface plate

7, 13 a base plate

9 a mesh member

10 fibers

16, 19, 22, 23, 25, 101, 104, 106, 107, 108 a pit
17, 20, 24, 103 a portion where the pit is not formed
48 a position alignment mark
49 a line to start the reading in moving direction
50 a line to finish the reading in moving direction
51, 52 a line to indicate the end portion
111 a reading elements matrix
112, 123, 131, 133 a reading element
113, 114 a container contains a reading elements array
115R an array of red light reading elements
115G an array of green light reading elements
115B an array of blue light reading elements
119 an image pickup device
120 a reflecting mirror having a parabolic cylinder
121 a light transmission hole
122 a polygonal mirror
125, 127 a reflecting mirror having a parabolic cylinder
130, 132 a container
132, 120 a straight line route
133 plural lines route

Best Mode for Carrying Out The Invention

[0071]

Detailed description will be given below on the best aspect for carrying out the invention by referring to the accompanied drawings.

Fig. 5 shows a basic arrangement of a card, on which an embossed hologram chip is mounted. Fig. 5 (a) shows a general view, Fig. 5 (b) is a cross-sectional view, and each of Figs. 5 (c) to (e) shows an enlarged view of the embossed hologram chip.

[0072]

A card 11 comprises a surface plate 14 with an opening being mounted on a card base member 13 having non-transparent property, and an embossed hologram chip 12 being placed into the opening. On the surface plate 14, a magnetic stripe 2 and an arrow mark 3 are disposed.

[0073]

The embossed hologram chip is composed of a pit portion with depth equal to $1/4$ wavelength of a laser beam used and a portion where the pit is not formed. On the pit portion, a reflected laser beam is eliminated by an incident laser beam, and the reflected laser beam is not detected. On the portion without the pit, the reflected laser beam is detected as not eliminated by the incident laser beam.

[0074]

The laser beam used is an infrared laser beam with λ (lambda) = 780 nm ($\lambda/4$ = 195 nm) in case of a CD. In case of a DVD, red laser with λ = 650 nm ($\lambda/4$ = 151.25 nm) is used. In case of the next generation DVD, using blue-violet laser with λ = 405 nm, ultraviolet laser with λ = 351 nm or far ultraviolet laser with λ = 266 nm is under study. $\lambda/4$ is 101.25 nm, 87.75 nm or 66.5 nm respectively.

[0075]

Fig. 5 (c) shows the most basic structure. Pit portions 16 with the depth of $1/4$ wavelength of the laser beam used and portions 17 without a pit are arranged with an adequate distance between them one another on an embossed hologram chip 15. In the example shown in this figure, each solid line shown by bidirectional arrows indicates that both incident light and reflected light are present. Each broken line shown by a uni-directional arrow indicates that there is incident light

but no reflected light is present.

[0076]

Fig. 5 (d) shows an example where the direction of the laser beam is inclined. Unless information on the tilt angle is available, it is difficult to read the data written therein. In this example, a inclined pit portion 19 with the depth of $1/4$ wavelength of the laser beam used and a inclined portion 20 without a pit are arranged with an adequate distance between them one another on an embossed hologram chip 18.

[0077]

In the example shown in this figure also, each solid line shown by bidirectional arrows indicates that both incident light and reflected light are present, and each broken line shown by a uni-directional arrow indicates that there is incident light but reflected light is not present. It is almost impossible to duplicate the embossed hologram chip of this structure. It is possible that the structure shown in Fig. 5 (c) and the structure shown in Fig. 5 (d) coexist.

[0078]

Fig. 5 (e) shows an example where laser beams with a plurality of wavelengths are used. Unless information on all of the laser beams used is available, it is difficult to read the written data. In this example, a pit portion 22 with the depth of $1/4$ wavelength of the red (R) laser beam; a pit portion 23 with the depth of $1/4$ wavelength of the green (G) laser beam; a pit portion 25 with the depth of $1/4$ wavelength of the blue (B) laser beam; and a portion 24 without a pit are arranged with an adequate distance between them one another on an embossed hologram chip 21.

[0079]

In the example shown in this figure also, each solid line shown by bidirectional arrows indicates that both incident light and reflected light are present. Each broken line shown by a uni-directional arrow indicates that there is incident light but no reflected light is present. It is almost impossible further to duplicate the embossed hologram chip of this structure. It is also possible that the structure shown in Fig. 5 (d) and the structure shown in Fig. 5 (e) coexist.

[0080]

[Embodiment 1 of the authentication verifying chip]

Referring to Fig. 6, descriptions below are on authentication verifying data written on pits. The pits where data is to be displayed are arranged regularly to ensure the reading. In Fig. 6, one dot chain line indicates the stationing of pits. Fig. 6 (a) and Fig. 6 (b) show examples where a laser beam with a single wavelength is used and where the same data is recorded. Fig. 6 (c) shows an example where laser beams with multiple wavelengths (three wavelengths in this case) are used.

[0081]

In Figs. 6 (a), (b) and (c), the pits where data is recorded are arranged at regular intervals. Fig. 6 (a) corresponds to Fig. 5 (c). A pit 101 is formed at a position where data of "101010110" of an embossed hologram chip base member 15 is recorded, and a protective layer 100 is disposed on it.

[0082]

[Embodiment 2 of the authentication verifying chip]

Fig. 6 (b) corresponds to Fig. 5 (d). In order to record data of "101010110" of an embossed hologram chip base member 18, a pit 104 having a inclined surface at a position of the data 1 is formed and a inclined surface 103 is formed at a position of the data 0, and a protective layer 102 is formed on it. In order that the data can be detected from a direction different from the inclined surface 103 and the pit 104, a

inclined surface and a pit with a different inclination angle from those inclination angles may be formed.

[0083]

[Embodiment 3 of the authentication verifying chip]

Fig. 6 (c) corresponds to Fig. 5 (e). A pit 108 for data "00101010" for a 780 nm infrared laser beam, a pit 107 for data "01000100" for a 650 nm red laser beam and a pit 105 for data "10010001" for a 405 nm blue laser beam are formed on an embossed hologram chip base member 21, and a protective layer 105 is disposed on it.

[0084]

[Embodiment 4 of the authentication verifying chip]

In a verifying chip, which is to be read by a machine, there is no need that a pattern such as characters, design, etc. recognizable by a person is written. Fig. 8 shows a pit arrangement example of the verifying chip, prepared by using binary data by a compute, suitable for mechanical reading.

[0085]

In this verifying embossed hologram chip, 1024 binary data are arranged in a matrix form of 32×32 , consisting of an embossed hologram. In this figure, the position where binary data "0" is written is shown in blank, and the position where the binary data "1" is written is shown with a mark "*".

[0086]

Now, a method to obtain the binary data is described. Fig. 9 shows an example of true random numbers with hexadecimal numbers of 256 digits, which are obtained by detecting a radiation ray irradiated as the result of nuclear fission of radioactive substance. Random numbers used for a crypt key or the like are generally

supplied as hexadecimal numbers as such.

[0087]

Fig. 10 shows hexadecimal random numbers shown in Fig. 9 arranged in the matrix form of 8 columns $\times$ 32 rows. The hexadecimal numbers can be expressed by replacing with binary 4-digit numbers.

That is, "0" of the hexadecimal number corresponds to "0000" of binary numbers. Similarly, "1" corresponds to "0001", "2" corresponds to "0010", "3" corresponds to "0011", "4" corresponds to "0100", "5" corresponds to "0101", "6" corresponds to "0110", "7" corresponds to "0111", "8" corresponds to "1000" and "9" corresponds to "1001". "A" corresponds to "1010", "B" corresponds to "1011", "C" corresponds to "1100", "D" corresponds to "1101", "E" corresponds to "1110" and "F" corresponds to "1111".

[0088]

Based on the expressions as given above, 256-digit hexadecimal random numbers shown in Fig. 9 are substituted by binary random numbers as shown in Fig. 11. One digit of the hexadecimal number can be replaced by 4-digit binary numbers. Thus, 256-digit hexadecimal numbers correspond to $256 \text{ digits} \times 4 \text{ digits} = 1024$ digits in binary numbers. These binary numbers can be obtained directly in a random number generator, and in such a case, it is not necessary to perform substitution operation.

[0089]

These numbers are arranged in the matrix of 8 columns $\times$ 32 rows as shown in Fig. 10. Further, for each digit of binary numbers, matrix of 32 columns $\times$ 32 rows are arranged as shown in Fig. 12.

[0090]

Finally, the position corresponding to "0" of the binary number in the matrix of Fig. 12 is left without writing the data. Data is written to the position with the mark "*" to correspond to "1". The arrangement of the verifying chip as shown in Fig. 8 is thus, obtained.

The authentication verifying chip prepared in this way has $32 \text{ column} \times 32 \text{ rows} \times 1 \text{ bit} = 1024 \text{ bits}$ for authentication verifying, that is, it has an authentication verifying key of 1024 bits.

[0091]

For the embossed hologram chip shown in Fig. 6 (c), the lights with a plurality of wavelengths can be used. Next, an example of the pit arrangement of a verifying chip of a card, which is prepared by computer suitable for mechanical reading of binary data, and which uses the lights of generally called red (R), green (G) and blue (B) is described.

[0092]

These "R", "G" and "B" can express a total of four conditions including "0" where no data is written. In other words, these can be handled as quaternary numbers.

The quaternary numbers can be expressed by four 2-bit numbers, i.e., "00", "01", "10", and "11".

[0093]

Fig. 13 shows hexadecimal random numbers of 256 digits shown in Fig. 9 and further hexadecimal random numbers of 256 digits which antecede those. Here, what is shown as "hexadecimal random numbers group a" is the same random numbers as shown in Fig. 9, and "hexadecimal random numbers group b" is the random numbers, which antecedes "hexadecimal random numbers group a".

[0094]

These hexadecimal random numbers group is converted to a binary random numbers group. Fig. 14 shows the random numbers divided for every 2 bits in order to convert to the quaternary numbers expressed as "0", "R", "G" and "B".

[0095]

Further, binary number "00" is converted to quaternary number "0", binary number "01" to quaternary number "R", binary number "10" to quaternary number "G" and binary number "11" to quaternary number "B" as shown in Fig. 15.

[0096]

The quaternary numbers thus obtained are arranged in the matrix of 32 columns $\times$ 32 rows, similarly to the binary numbers shown in Fig. 8 or Fig. 12, and these are shown in Fig. 16. The verifying chip thus prepared has the data of 32 columns $\times$ 32 rows $\times$ 2 bits = 2048 bits for authentication verifying, in other words, it has an authentication verifying key of 2048 bits.

[0097]

[Embodiment 5 of the authentication verifying chip]

Now, referring to Fig. 17, a method to obtain a plurality of verifying chips from one random numbers group is described. Fig. 17 (a), Fig. 17 (b), Fig. 17 (c) and Fig. 17 (d) each shows a matrix pattern of 16 $\times$ 16 based on the matrix pattern of 32 $\times$ 32 in Fig. 8. Fig. 17 (a) has the origin at the coordinates (0,0), Fig. 17 (b) has the origin at the coordinates (1,0), Fig. 17 (c) has the origin at the coordinates (0,1) and Fig. 17 (d) has the origin at the coordinates (1,1). In this way, it is possible to have a plurality of matrix patterns from one matrix pattern obtained from the random numbers group shown in Fig. 6.

[0098]

For the purpose of obtaining a plurality of matrix patterns from one random

numbers group, it is also possible to use various methods such as a method to change the use position to start the random numbers group shown in Fig. 6 or a method to change the preparation position to start the matrix pattern shown in Fig. 7.

[0099]

In so doing, a card issuer can maintain secrecy by arranging one random numbers group as a master random numbers group and can obtain a plurality of matrix patterns based on the master random numbers group. It is also possible to automatically control the plurality of matrix patterns based on the information of the origin.

[0100]

In the examples shown in Fig. 8, Fig. 12 and Fig. 17, the authentication verifying data is recorded by binary numbers expressed in 1 bit, and in the example shown in Fig. 16, the authentication verifying data is recorded by quaternary numbers expressed in 2 bits. In addition to these, it is also possible to use octal numbers expressed in 3 bits and hexadecimal numbers expressed in 4 bits.

[0101]

[Mounting position of the authentication verifying chip]

Fig. 7 shows examples of the mounting positions of the verifying chip according to the structural features as described above. The verifying chip 46 can be mounted, other than the position at about the central portion of the card body as shown in Fig. 5, at the following positions: at the foremost position in the middle portion as shown in Fig. 7 (a); at the central position in the middle portion as shown in Fig. 7 (b); at the posterior position in the middle portion as shown in Fig. 7 (c); at the foremost position in the lower portion as shown in Fig. 7 (d); at the central position in the lower portion as shown in Fig. 7 (e); and at the posterior position

in the lower portion as shown in Fig. 7 (f). While it can also be mounted at a position in the upper portion, it is desirable for the mounting position to avoid the position in the upper portion, when there may be influence on the reading of the information from the magnetic stripe.

[0102]

[Embodiment 1 of the reading device]

Descriptions below are on the reading of a verifying chip, which is an embossed hologram chip. A method to read the embossed hologram chip simply as a plane, a method to read a plane as an assembly of lines and a method to read a plane as an assembly of dots are known.

[0103]

Fig. 18 shows an example using an image pickup device of the most basic arrangement in the method to read the embossed hologram chip simply as a plane. From a card body 11, which consists of a card base plate 13, a card surface plate 14 and an embossed hologram chip 15, the embossed hologram chip 15 is read by an image pickup device 110, and the result is verified by the pattern recognition technique.

[0104]

When the card 11 is taken into a reading apparatus and is stopped, the image pickup device 110 photographs the embossed hologram chip 15, which is irradiated by a laser beam source (not shown). By the image thus photographed, the embossed hologram chip 15 is authenticated, and accordingly, the authenticity of the card 11 is verified.

[0105]

[Embodiment 2 of the reading device]

Referring to Fig. 19, description will be given below on an arrangement example of a reading device, which comprises detection elements in the form of matrix and which performs reading in the planar shape. Fig. 19 (a) shows a general arrangement of a reading device and Fig. 19 (b) shows the corresponding relation between the card and the reading device. In Fig. 19, the reference numeral 11 shows a card body; 13 a base plate; 14 a surface plate; and 15 a verifying chip, which is an embossed hologram chip. The reference numeral 111 shows a reading elements matrix where small size reading elements 112 are arranged in the planar shape so as to cover up the verifying chip 15. Each of the reading elements has a light source comprising a semiconductor laser or the like and a light detecting element comprising a photodiode or the like.

[0106]

When the card 11 is taken into a reading apparatus and is stopped, the verifying chip 15 is positioned under the reading elements matrix 111 in planar shape. Then, the reading elements matrix 111 reads authentication verifying data of the verifying chip 15.

[0107]

[Embodiment 3 of the reading device]

Description will be given below on a device for reading the plane of the verifying chip as an assembly of lines.

Fig. 20 shows an example where the reading elements are arranged in array. Fig. 20 (a) shows a general arrangement of a detecting unit of a reading device and Fig. 20 (b) shows the corresponding relation between the card and the reading elements in array. The card 11 is the same as the card shown in Fig. 19, and the detailed description on the card is not given here.

[0108]

In Fig. 20, the reference numeral 113 shows a container with a length, which is slightly longer than the width in moving direction of the verifying chip 15. A plurality of reading elements array 112 are placed in a linear arrangement within the container and make up together a reading elements array. Each of the reading elements has a light source comprising a semiconductor laser and the like and a light detecting element comprising a photodiode or the like.

[0109]

When the card 11 is taken into a card reading apparatus, it passes under the reading elements array. At this moment, the reading elements array 112 reads authentication verifying data of the verifying chip 15.

[0110]

Fig. 21 shows examples of arrays of the reading elements in the reading device as shown in Fig. 20. As shown in Fig. 21 (a), 32 reading elements are placed from "D00" to "D31" in a single column on a base. These may be placed from "D00" to "D31" in a zigzag arrangement as shown in Fig. 21 (b).

[0111]

[Embodiment 4 of the reading device]

Fig. 22 shows an arrangement example of a device for the card authentication verifying when a plurality of different colors are used, which are quaternary numbers as shown in Fig. 16. In this example, according to the reading elements array shown in Fig. 20, a container 114 contains an array of red light reading elements 115R, an array of green light reading elements 115G, and an array of blue light reading elements 115B.

[0112]

The red light reading elements array 115R, the green light reading elements array

115G and the blue light reading elements array 115B are given here simply as examples, and it is needless to say that any combination of color lights may be used.

[0113]

Fig. 23 shows an arrangement example of arrays of reading elements when a laser beam R, a laser beam G and a laser beam B as shown in Fig. 22 are used. In this example, an array of the laser beam R reading elements "R00" to "R31", an array of the laser beam G reading elements "G00" to "G31", and an array of the laser beam B reading elements "B00" to "B31", having 32 reading elements each are arranged in three columns.

[0114]

[Embodiment 5 of the reading device]

In the efforts to develop the next generation DVD, it has been under study that laser beams of a laser for CD, a laser for DVD and a laser for the next generation DVD can be detected by an optical detector applicable to three wavelengths by using an optical head using the optical system to be integrated or by using a 3-wavelength laser which can emit three laser beams by a single element. (See Nikkei Electronics, No. 883, p.119, September 27, 2004). When the optical detectors are aligned in one row and are used, it is possible to have an arrangement of the reading elements array for the laser beam R, the laser beam G and the laser beam B, similar to the arrangement shown in Fig. 20.

[0115]

[Embodiment 6 of the reading device]

Fig. 24 shows a reading device with the new arrangement. Optical scanning means to use the reflection of the laser beam by a rotating polygonal pillar mirror is adopted in the device such as a laser beam printer. In this scanning means, optical scanning can be performed only by the rotating movement of the polygonal

pillar mirror. Because the reflection light beam obtained is reflected in radial direction, the light beam does not enter perpendicularly to an object. In this sense, the optical scanning by the polygonal pillar mirror is not the optimal means to be used as the detecting means for an embossed hologram chip by reading the information according to the depth of pits and to the wavelength of the incident light.

[0116]

Paraboloid is used in a reflecting telescope or a parabola antenna as the means to obtain parallel beams. Fig. 24 (a) shows the relation between a paraboloid and parallel beams. In this figure, reference symbol X represents X-axis and the symbol Y represents Y-axis which is orthogonal to X-axis and the symbol O represents the origin. The symbol P represents a parabola, which is expressed as $Y = -X^2$. This parabola has a focal point F at the position of $X = 0$ and $Y = -1/4$. All straight lines running in parallel to Y-axis are concentrated to the focal point F when reflected by the parabola P. In other words, any straight line starting from the focal point F runs in parallel to Y-axis when reflected by the parabola 100.

[0117]

A basic arrangement of a device for reading an embossed hologram by applying this principle is shown in Fig. 24 (b). In this figure, the reference numeral 120 represents a reflecting mirror having a parabolic cylindrical surface. It is designed in semi-cylindrical shape with its length running in a direction perpendicularly crossing the drawing surface. Also, a light transmission hole 121 where light can pass through is formed at a position which corresponds to the origin in Fig. 24 (a). Further, at the focal point of the reflecting parabolic cylinder mirror 120, a polygonal mirror 122 is disposed, which has a rotation axis in parallel to extending axis of the reflecting parabolic cylinder mirror 120 and has a polygonal reflecting surface. The reference numeral 124 represents an embossed hologram chip.

[0118]

A laser beam emitted from a light emitting/detecting element 123 in direction of Y-axis as shown in Fig. 24 (a) passes through the light transmission hole 121 and incidents on the polygonal mirror 122. The laser beam, thus incidented on the polygonal mirror, is reflected and incidents on the reflecting parabolic cylinder mirror 120. Then, it is reflected and incidents on the embossed hologram chip 124.

[0119]

As the polygonal mirror 122 is disposed at the focal point of the reflecting parabolic cylinder mirror 120, the laser beam, which is reflected by the polygonal mirror 122 and incidents on the reflecting parabolic cylinder mirror 120, is reflected again. It is reflected in a direction in parallel to the advancing direction of the laser beam emitted from the light emitting/detecting element 123 and it then, incidents on the embossed hologram chip 124. When the laser beam, which has incidented on the pit of the embossed hologram chip 124, is reflected without being eliminated, the laser beam runs along the same route as the incident laser beam in reverse direction and the reflected laser beam incident on the light emitting/detecting element 123. As it can be understood from the above explanation, all of the laser beams emitted from the light emitting/detecting element 123 incidents on the embossed hologram chip 124 in a direction perpendicular to it.

[0120]

[Embodiment 7 of the reading device]

In the embossed hologram reading device as shown in Fig. 24 (b), it is not possible to read the information on the embossed hologram chip 124 on a portion, which is on rear side of the polygonal mirror 122 as seen from the direction of the light emitting/detecting element 123. It can be so designed that necessary information is not written on this portion or that only unnecessary information is

written on this portion. However, if an arrangement shown in Fig. 24 (c) is adopted, there is no portion, which corresponds to the rear side of the polygonal mirror 122, and all of the information written in the embossed hologram chip 124 can be read out.

[0121]

Fig. 24 (c) shows the most basic arrangement for this purpose, which uses a half of the reflecting parabolic cylinder mirror. In Fig. 24 (c), the reference numeral 125 represents a reflecting mirror with a paraboloid surface, and it is designed in semi-cylindrical shape having its length in a direction running perpendicularly crossing the drawing surface only on the portion where the value of X is negative in Fig. 24 (a). The light transmission hole 121 as shown in Fig. 24 (b) is not formed because it is not needed. Further, at the focal point of the reflecting half-parabolic cylinder mirror 125, a polygonal mirror 122 is disposed, which has a rotation axis in parallel to the axis in extending direction of the reflecting half-parabolic cylinder mirror 125 and has a polygonal reflecting surface. The reference numeral 126 represents an embossed hologram chip.

[0122]

After being emitted from the light emitting/detecting element 122 in direction of the polygonal mirror 122, the laser beam is reflected by the polygonal mirror 122 and incidents on the reflecting half-parabolic cylinder mirror 125. Then, it is reflected and incidents on the embossed hologram chip 126 in a direction perpendicular to it. In this embossed hologram reading device, it is only an end portion of the embossed hologram chip 124, which is on rear side of the polygonal mirror 122 when seen from the direction of the light emitting/detecting element 123. Accordingly, the portion which cannot be read has little influence.

[0123]

[Embodiment 8 of the reading device]

Further, when the central portion of a reflecting partial paraboloid cylindrical mirror 127 is reduced as shown in Fig. 24 (d) and it is configured that a portion where the polygonal mirror 122 faces to the reflecting semi-parabolic cylinder mirror 127 is offsetted. There is no more portion, which cannot be read, and it is possible to read the information written in all parts of the embossed hologram chip 128.

[0124]

[Embodiment 9 of the reading device]

When a plurality of reading devices as shown in Figs. 24 (b), (c) and (d) are provided corresponding to a plurality of wavelengths, it is possible to read a plurality of wavelengths.

[0125]

[Embodiment 10 of the reading device]

Description will be given as below on a reading device, which reads the plane of the authentication verifying chip as an assembly of dots. Fig. 25 shows a reading device using a single reading element. Fig. 25 (a) shows a general arrangement of the relation between the card and the reading device and Fig. 25 (b) is a drawing to explain a data detecting method. The reference numeral 11 represents a card body; 13 a card base plate; 14 an upper surface plate of the card; 15 a verifying chip; 131 a reading element; and 130 a container to accommodate the reading element 131. The reading element 131 moves in a direction which perpendicularly crosses the direction that the card is taken into the reading apparatus.

[0126]

For the movement which perpendicularly crosses the direction that the card is taken into the apparatus, either of appropriate methods such as a pseudo-linear

movement based on the rotation on one point as a fulcrum, a linear movement based on the conversion from rotary movement to linear movement and a linear movement based on a linear motor can be adopted. Fig. 25 (b) shows a typical example of a movement route. In this example, the reading element moves at the uniform speed in a direction indicated as shown by an arrow mark in Fig. 25 (b) and moves along a linear route 132 which is resulted from the movement synthesized with the moving direction of the card itself. The reading element 131 does not necessarily move, and it can be used by moving to an arbitrary position in a direction which perpendicularly crosses the direction of the card 11 being taken, and by fixing it there.

[0127]

[Embodiment 11 of the reading device]

While a single reading element is used in the reading device shown in Fig. 25, a plurality of reading elements as shown in Fig. 26 allow the reading by a plurality of routes. As a result, the reliability of the reading can be increased. Because the information to be processed is linear information, this does not increase the load of processing.

[0128]

Fig. 26 (a) shows a general arrangement of the relation between the card and the reading device and Fig. 26 (b) is a drawing to explain a detecting method. The card 11 is the same as the card 11 shown in Fig. 25, and detailed description on the card is not given here.

[0129]

In this Example, in addition to a first reading device which comprises the reading element 131 and the container 130 as shown in Fig. 25, a second reading device is provided which comprises a reading element 132 and a container 133.

[0130]

The second reading device composed of the reading element 132 and the container 133 moves in a direction reverse to the moving direction of the first reading device composed of the reading element 131 and the container 130. However, it can be so designed that the moving directions of the reading devices are the same.

[0131]

Fig. 26 (b) shows a typical example of the moving route. In this example, the first reading device and the second reading device move at the uniform speed in a direction indicated respectively as shown by arrow marks in Fig. 26 (b) and move along linear routes 132 and 120 which are resulted from the movements synthesized with the moving direction of the card itself.

[0132]

[The reading route]

A reading error may be caused from an error in the route or from the operation failure of the reading device. In such the case, reading is performed by a plurality of reading elements at the same time as shown by the reference numeral 134 in Fig. 27. By finding an average value or by a value determined according to the majority value, the final reading information is determined.

[0133]

[Embodiment 12 of the reading device]

Description will be given below on the cases where the reading devices shown in Fig. 25 to Fig. 28 are applied to the verifying chips shown in Fig. 12 and Fig. 16. To facilitate the explanation, an example using binary numbers as shown in Fig. 12 is described referring to Fig. 29. This can also be applied in similar manner to the example using quaternary numbers as shown in Fig. 16.

[0134]

In Fig. 29, authentication verifying data on a linear detecting route from the coordinate (0,0) to the coordinate (31,31) is shown as "11000101001001101010101101110111". Also, authentication verifying data on a linear detecting route from the coordinate (0,31) to the coordinate (31,0) is shown as "11100101001010000000110000010011".

[0135]

The detecting route is not limited to the routes shown in Fig. 29. For instance, an arbitrary route shown in Fig. 28 may be adopted, or the route can be changed each time when the reading is performed.

Also, converting the coordinate can be made within the apparatus after the reading has been performed.

[0136]

The combination of the data detecting routes as described above may result in a substantially large number as $32 \times 32 = 1048$, even under the condition that the data detecting route does not turn back. However, the data of the pattern to be stored in the reading apparatus for comparison is as small as 1024 bits.

[0137]

Compared with the example of the quaternary numbers, the example of quaternary numbers shown in Fig. 16 is merely different in that the amount of information of the pattern for comparison is increased to 2048 bits, and then, detailed description is not given here.

[0138]

[The reading route]

Fig. 28 shows several examples of the reading routes. Figs. 28 (a) - (d) each shows an example of using a single data reading route. Figs. 28 (e) - (f) each shows an example of using two data reading routes. Also, it may be possible to use three or more reading routes.

[0139]

These reading routes can also be realized by selecting and changing the reading elements of arrays for detection as shown in Fig. 21 and Fig. 23. For instance, in the arrays shown in Fig. 21, when the detecting elements are read in the order of D00, D01, D02, D03, D28, D29, D30 and D31, the route 132 as shown in Fig. 25 is obtained. The reading routes are not limited to these examples, and any arbitrary route can be adopted. Further, it is also possible to electrically read in irregular order.

[0140]

Description will be given below on a method for verifying the authenticity on the verifying chip as shown in Fig. 12 and Fig. 16 by applying the feature extraction method used in biometrics. Referring to Fig. 30, a method for verifying the authenticity on the verifying chip based on the binary number data of 0 and 1 shown in Fig. 12 is described. In Fig. 30, when the number "0" continuously appears in four or more times, the figures of "0" are shown as white-black inverted figures. Similarly, when the number "1" continuously appears in four or more times, the figures are shown as enclosed figures.

For instance, there are 13 occurrences of the figures "0000", starting from the coordinates (16,1).

There are 7 occurrences of "00000", starting from the coordinates (15,5).

There is one occurrence of "0000000" at the coordinates (13,31).

There are 3 occurrences of "00000000", starting from the coordinates (24,2).

There is one occurrence of "00000000000000" at the coordinates (6,12).

There is one occurrence of "00000000000000" at the coordinates (7,15).

[0141]

There are 12 occurrences of the figures "1111", starting from the coordinates (14,4).

There are 8 occurrences of "11111", starting from the coordinates (0,7).

There is one occurrence of "111111" at the coordinates (19,1).

There is one occurrence of "1111111" at the coordinates (12,19).

There are 2 occurrences of "11111111", starting from the coordinates (17,6).

There is one occurrence of "1111111111" at the coordinates (14,3).

By detecting each of these features and by detecting coordinates of the starting positions of these features, the authenticity can be verified on the verifying chip.

[0142]

[Embodiment 13 of the reading device]

Referring to Fig. 31, a method for verifying the authenticity on the verifying chip based on quaternary numbers shown in Fig. 16 is described. As shown in Fig. 16, as the features in the matrix, there are 5 occurrences of the figures "000", 3 occurrences of "0000", 0 occurrence of "00000" and 2 occurrences of "000000", aligned in the transverse direction.

Also, there are 9 occurrences of "RRR", four occurrences of "RRRR" and 0 occurrence of "RRRRR" aligned in the transverse direction.

Further, there are 5 occurrences of "GGG", 4 occurrences of "GGGG" and 1 occurrence of "GGGGG" aligned in the transverse direction.

Also, there are 8 occurrences of "BBB", 0 occurrence of "BBBB" and 3 occurrences of "BBBBB" aligned in the transverse direction.

[0143]

By detecting each of these features and by detecting the coordinates of the starting

positions of these, the authenticity can be verified on the verifying chip. As the feature to be extracted, in addition to the same verifying data aligned in the transverse direction, the same verifying data aligned in the longitudinal direction or the same verifying data aligned in a hooked form may be used. Further, specific arrangement such as "0RGB" of different information may be also used.

[0144]

Also, in case of using the binary data, when adopting intermediate data, e.g., intermediate two gray colors in the white-black binary data, it is possible to be of quaternary numbers. These arrangements, as described above, make carrying out forgery more difficult. Also, when using some of "0" in the binary data for the intermediate color tone as dummies, this will further embarrass those who attempt to forge.

[0145]

The intermediate color tone can be similarly used in the case where the quaternary data such as 0, R, G and B is used, and this makes it possible to be of 3-bit octal numbers, 4-bit hexadecimal numbers, etc.

[0146]

The authentication verifying methods as described above are to digitally process the authentication verifying data recorded digitally. Fig. 32 shows an arrangement of analog processing of authentication verifying data which has been digitally recorded.

[0147]

In Fig. 32, the pattern of the verifying chip as shown in Fig. 32 (a) is scanned, for instance, along the routes shown by the reference numerals 132 and 120 by using the verifying chip reading device as shown in Fig. 25 or Fig. 26 and electric signals

shown in Fig. 32 (b) and Fig. 32 (c) are obtained. By comparing these electric signals patterns with the valid patterns as stored, a unit for identifying the card authenticity is verified and the card itself can be authenticated.

[0148]

[Embodiment 14 of the reading device]

Physical standards for a cash card and a credit card are strictly stipulated from the viewpoint of the practical use. Accordingly, physical standards of the components to be mounted on it are also strictly provided. Notwithstanding, it is not entirely deniable that deformation may occur due to the excessive use.

[0149]

To cope with such the problem, it is desirable to arrange a position alignment mark 48 as shown in Fig. 33 on the verifying chip. In the simplest case, only one position alignment mark may be used. Preferably, two or more marks are provided to ensure the more reliable position alignment.

The position alignment mark is useful not only for the reading in the linear shape but also for the reading in the planar shape using the image pickup device.

[0150]

In order to perform the reading more reliably, at the same time with the use of the position alignment mark, it would be desirable to arrange some other marks at the position to start the reading and the position to finish the reading of the unit for identifying the card. For instance, a line 49 to start the reading in moving direction and a line 50 to finish the reading in moving direction and further, lines 51 and 52 to indicate the end portions may be arranged.

[0151]

The reading of information on the card identifying unit is performed by the relative

movement of the card identifying unit and the reading device. To ensure the reliable reading, it is necessary to synchronize the movements of the card identifying unit and the reading device. If a mark 53 for synchronization signal is disposed on the card identifying unit, the movement of the reading device can be synchronized according to the reading of the mark.

[0152]

Also, the reading start line and the reading finish line and/or the mark for synchronization signal can be used for the normalization of the signal in the signal processing.

The position alignment mark, the reading start/finish lines and/or the mark for synchronization signal are made of fluorescent substance particles, and these particles can be prepared by an adequate printing means such as an ink jet printer.

[0153]

[Embodiment 1 of the processing flow]

Fig. 34 to Fig. 36 each shows an example of a flow of card authentication verifying processing. Fig. 34 shows Embodiment 1 of a basic arrangement.

[0154]

(1) A card user inserts a cash card into a card slot of a terminal device such as an ATM by setting the portion of the card marked with an arrow at the foremost position, the sensor at the card slot senses it, and the card is taken into the device.

[0155]

(2) When the card is taken into the device, the terminal device reads the card information from the magnetic recording portion of the card.

[0156]

(3) The terminal device judges whether the inserted card is a valid card which can be processed by the terminal device or not.

[0157]

(4) If it is not confirmed that the card can be processed by the device from the card information thus read, or if the information of the card cannot be read because the card is broken or stained even though it is a valid card, the terminal device judges that it is an illegitimate card which cannot be processed and discharges the card.

[0158]

(5) The terminal device reads the authentication verifying data from the verifying chip by mechanical scanning using the movement of the card when the card is taken into the device or under the stopped condition after the card is taken in.

[0159]

(6) The terminal device judges whether the card authentication verifying data thus read is valid or not.

[0160]

(7) In a case where the terminal device judges that the card authentication verifying data is not valid, it is judged that the inserted card is not a valid card. Then, the card is discharged from the terminal device, and the processing is terminated.

The judgment on the validity of the authentication verifying data and subsequent processing of the card may be carried out in parallel with the other processing.

[0161]

(8) In a case where the terminal device judges that the card authentication

verifying data is valid, it instructs the user to perform further input operations, for example, input on the amount to draw.

[0162]

(9) The user follows the instruction and performs the input operation such as the inputting of the amount to be paid.

[0163]

(10) The host computer judges whether the content of the input operation such as the amount to be paid is adequate or not.

[0164]

(11) If the host computer judges that the content of the input operation is inadequate, for example, the balance short in the deposit, the card is discharged from the device, and the processing is terminated.

[0165]

(12) When the host computer judges that the content of the input operation such as the amount to be paid is adequate, the output operation such as paying of the amount is performed. Then, the card is discharged from the terminal device and the processing is terminated.

[0166]

[Embodiment 2 of the processing flow]

Referring to Fig. 35, Embodiment 2 of the flow of the card authentication verifying process is described.

In the flow of the card authentication verifying process, if the card authentication verifying data is not valid, the card is discharged from the terminal device in the example as shown in Fig. 34. In the Embodiment 2, if the authentication verifying

data is not valid, the card is taken into the terminal device, and an alarm is given. In so doing, it can be easy to dig up the illegitimate card.

[0167]

(1) When a card user inserts a cash card into a card slot of a terminal device such as an ATM by setting the portion of the card marked with an arrow at the foremost position, the sensor at the card slot senses it, and the card is taken into the device.

[0168]

(2) When the card is taken into the device, the terminal device reads the card information from the magnetic recording portion of the card.

[0169]

(3) The terminal device judges whether the inserted card is a valid card which can be processed by the terminal device or not.

[0170]

(4) If it is not confirmed that the card can be processed by the device from the card information thus read, or if the information of the card cannot be read because the card is broken or stained even though it is a valid card, the terminal device judges that it is an illegitimate card which cannot be processed and discharges the card.

[0171]

(5) The terminal device reads the authentication verifying data from the verifying chip by mechanical scanning using the movement of the card when the card is taken into the device or under the stopped condition after the card is taken in.

[0172]

(6) The terminal device judges whether the card authentication verifying data thus read is valid or not.

[0173]

(7) In a case where the terminal device judges that the card authentication verifying data is not valid, it is judged that the inserted card is not a valid card. Then, the card is taken into the device, and the alarm is given.

It may be possible that the alarm is issued only at a place remote from the terminal device, and a message of operation failure is displayed on the terminal device.

This makes it easy to have the user of the illegitimate card under control.

The judgment on the validity of the authentication verifying data and subsequent processing of the card may be carried out in parallel with the other processing.

[0174]

(8) In a case where the terminal device judges that the card authentication verifying data is valid, it instructs the user to perform further input operations, for example, input on the amount to draw.

[0175]

(9) The user follows the instruction and performs the input operation such as the inputting of the amount to be paid.

[0176]

(10) The host computer judges whether the content of the input operation such as the amount to be paid is adequate or not.

[0177]

(11) If the host computer judges that the content of the input operation is

inadequate, for example, the balance short in the deposit, the card is discharged from the device, and the processing is terminated.

[0178]

(12) When the host computer judges that the content of the input operation such as the amount to be paid is adequate, output operation such as paying of the amount is performed. Then, the card is discharged from the terminal device and the processing is terminated.

[0179]

[Embodiment 3 of the processing flow]

Referring to Fig. 36, Embodiment 3 of the flow of the card authentication verifying process is described. In the flow of the card authentication verifying process, while if the card authentication verifying data is not valid, the card is quickly taken into the terminal device and an alarm is given in the Embodiment 2 as shown in Fig. 35, if the authentication verifying data is not valid, the process to use the card continues in the Embodiment 3. In so doing, it can be easy to dig up the use of the illegitimate card.

[0180]

(1) A card user inserts a cash card into a card slot of a terminal device such as an ATM by setting the portion of the card marked with an arrow at the foremost position. Then, the sensor at the card slot senses it, and the card is taken into the device.

[0181]

(2) When the card is taken into the device, the terminal device reads the card information from the magnetic recording portion of the card.

[0182]

(3) The terminal device judges whether the inserted card is a valid card which can be processed by the terminal device or not.

[0183]

(4) If it is not confirmed that the card can be processed by the device from the card information thus read, or if the information of the card cannot be read because the card is broken or stained even though it is a valid card, the terminal device judges that it is an illegitimate card which cannot be processed and discharges the card.

[0184]

(5) The terminal device reads the authentication verifying data from the verifying chip by mechanical scanning using the movement of the card when the card is taken into the device or under the stopped condition after the card is taken in.

[0185]

(6) The terminal device judges whether the card authentication verifying data thus read is valid or not.

[0186]

(7) In a case where the terminal device judges that the card authentication verifying data is not valid, it instructs the user to perform further input operations, for example, input on the amount to draw.

The judgment on the validity of the authentication verifying data and subsequent processing of the card may be carried out in parallel with the other processing.

[0187]

(8) The user follows the instruction and performs the input operation such as the

inputting of the amount to be paid.

[0188]

(9) Then, the card is taken into the terminal device, and an alarm is given.

[0189]

It may be arranged that the alarm is issued only at a place remote from the terminal device, and a message of operation failure is displayed on the terminal device. This makes it easy to have the user of the illegitimate card under control.

[0190]

(10) In a case where the terminal device judges that card authentication verifying data is valid, it instructs the user to perform further input operations such as the input of the amount to draw.

[0191]

(11) The user follows the instruction and performs the input operation such as the input of the amount to be paid.

[0192]

(12) The host computer judges whether the content of the input operation such as the amount to be paid is adequate or not.

[0193]

(14) If the host computer judges that the content of the input operation is inadequate, for example, the balance short in the deposit, the card is discharged from the device, and the processing is terminated.

[0194]

With the arrangement as described above, the time, during which the user who uses the illegitimate card uses the terminal device, can be extended. This means not only that gives longer time for capturing the card user, but also that makes it possible to obtain further evidence such as the user's fingerprints by the input operation. If a contact-type touch switch is adopted, this makes the taking of fingerprints much easier.

[0195]

Physical standards for a cash card and a credit card are strictly stipulated from the viewpoint of the practical use. Accordingly, physical standards of the components to be mounted on it are also strictly provided. However, it is not entirely deniable that deformation may occur due to the excessive use.

Industrial applicability

[0196]

The card authentication verifying chip and the card with the card authentication verifying chip as described above can be adopted in the applications such as bank cash cards, credit cards, prepaid cards, membership cards, securities, ID cards, admission allowance and other types of certificate.

CLAIMS

1. A card comprising a base plate and an authentication verifying chip, wherein said verifying chip is layered on said base plate, and an embossed hologram is disposed on said verifying chip.
2. A card according to claim 1, wherein a surface plate is further layered on said verifying chip, and said surface plate is comprised of a synthetic resin with highly transparent property.
3. A card according to claim 1 or 2, wherein said embossed hologram is composed of pits with the same depth disposed perpendicularly to said chip.
4. A card according to claim 1 or 2, wherein said embossed hologram is composed of pits with different depths disposed perpendicularly to said chip.
5. A card according to claim 1 or 2, wherein said embossed hologram is composed of pits with the same depth disposed inclined on said chip.
6. A card according to claim 1 or 2, wherein said embossed hologram is composed of pits with different depths disposed inclined on said chip.
7. A card according to claim 1, 2, 3, 4, 5 or 6, wherein said pits are disposed in a matrix form.
8. A card according to claim 7, wherein said pits are arranged by binary random numbers.
9. A card according to claim 8, wherein said pits are a part of the pits arranged

by binary random numbers.

10. A card according to claim 7, wherein said pits are arranged by quaternary random numbers.

11. A card according to claim 10, wherein said pits are a part of the pits arranged by quaternary random numbers.

12. An embossed hologram chip reading device for reading the embossed hologram of an authentication verifying chip mounted on a card, wherein said reading device has a light emitting/detecting elements matrix with the same area as said authentication verifying chip.

13. An embossed hologram chip reading device for reading the embossed hologram of an authentication verifying chip mounted on a card, wherein said reading device has a light emitting/detecting elements array with the same width as said authentication verifying chip.

14. An embossed hologram chip reading device for reading the embossed hologram of an authentication verifying chip mounted on a card, wherein said reading device has a reflecting paraboloid mirror in a cylindrical shape, a polygonal mirror and a light emitting/detecting element, a rotation axis of said polygonal mirror is arranged at the focal point of said reflecting mirror, and the light emitting/detecting element is disposed behind said reflecting mirror.

15. An embossed hologram chip reading device according to claim 13, wherein said paraboloid is a full-paraboloid, a light transmission hole is disposed at the center of the reflecting mirror, and said light detecting element is arranged behind said reflecting mirror and behind said light transmission hole.

16. An embossed hologram chip reading device according to claim 13, wherein said paraboloid is a half-paraboloid.

17. An embossed hologram chip reading device according to claim 13, wherein said paraboloid is a paraboloid smaller than a half-paraboloid, and said polygonal mirror is disposed in an offset arrangement.

18. An embossed hologram chip reading device for reading the embossed hologram of an authentication verifying chip mounted on a card, wherein said embossed hologram chip reading device has a light emitting/detecting element movable in direction of the width of said verifying chip, and said light emitting/detecting element reads the embossed hologram of the verifying chip in moving.

19. An embossed hologram chip reading device according to claim 17, wherein said reading device has one more light emitting/detecting element.