



ACTION

1

9900624-9
18 JUL 2002
IPBS copy



166166

METHOD OF REGISTERING ORIGINAL INFORMATION FOR
PERSONAL IDENTITY AUTHENTICATION AND
PERSONAL IDENTITY AUTHENTICATION DEVICE

Background of the Invention:

This invention relates to a method of registering an original information about a subject used for personal identity authentication such as a fingerprint.

On authenticating a personal identity, external means is used such as a seal impression, a sign, or a public certificate. Furthermore, a fingerprint may be used on authentication.

On the personal identity, a computer is employed to authenticating an intrinsic feature such as a fingerprint, a palm print, a voice print, an iris, a retina, or a face.

In order to authenticate the personal identity, a conventional fingerprint authentication device compares a fingerprint image with each of registered fingerprint data.

However, it is difficult to authenticate the personal identity at a high accuracy in the conventional fingerprint authentication device, as will be described later.

Summary of the Invention:

It is an object of this invention to provide a method of registering original information about a subject for personal identity authentication in order to authenticate a personal identity at a high accuracy.

It is another object of this invention to provide a personal authentication device capable of authenticating a personal identity at a high accuracy.

Other objects of this invention will become clear as the description proceeds.

According to a first aspect of this invention, there is provided a method of registering original information for personal identity authentication. The original information being used as a reference for verification of an authentication subject. The method comprises (A) a first step of extracting a feature point in number of N from the authentication subject to produce first through N -th feature point data, where N represents a positive integer which is not less than three, (B) a second step of comparing an n -th feature data with each of remaining feature data to produce levels of similarities as coincidence degrees in each of the first through the N -th feature point data, where n is variable between 1 and N , both of inclusive, (C) a third step of calculating a sum degree of the coincidence degrees in each of the first through the N -th feature point data to produce first through N -th sum data, and (D) a fourth step of selecting a maximum one of the first through the N -th sum data to register, as the original information, one of the first through the N -th feature data that has the maximum sum data.

According to a second aspect of this invention, there is provided a personal identity authentication device authenticates an authentication subject. The personal identity authentication device comprises (A) first means

for extracting a feature point from the authentication subject to produce extracted feature point data on authentication, the first means extracting a feature point in number of N from the authentication subject to produce first through N -th feature point data on registration, where N represents a positive integer which is not less than three, (B) second means for registering a reference feature point data therein, (C) third means for comparing the extracted feature point data with the reference feature point data to judge whether or not the authentication subject is true on authentication, the third means comparing an n -th feature data with each of remaining feature data to produce levels of similarities as coincidence degrees in each of the first through the N -th feature point data on registration, where n is variable between 1 and N , both of inclusive, and (D) fourth means for selecting a maximum one of the first through the N -th sum data to register, as the reference feature point data in the second means, one of the first through the N -th feature data that has the maximum sum data.

According to a third aspect of this invention, there is provided a recording medium memorizing a control program which is for registering original information for personal identity authentication. The original information being used as a reference for verification of an authentication subject. The control program comprises (A) a first procedure of extracting a feature point in number of N from the authentication subject to produce first through N -th feature point data, where N represents a positive integer

which is not less than three, (B) a second procedure of comparing an n-th feature data with each of remaining feature data to produce levels of similarities as coincidence degrees in each of the first through the N-th feature point data, where n is variable between 1 and N, both of inclusive, (C) a third procedure of calculating a sum degree of the coincidence degrees in each of the first through the N-th feature point data to produce first through N-th sum data, and (D) a fourth procedure of selecting a maximum one of the first through the N-th sum data to register, as the original information, one of the first through the N-th feature data that has the maximum sum data.

Brief Description of the Drawings:

Fig. 1 is a block diagram of a conventional fingerprint authentication device;

Fig. 2 is a schematic diagram of a fingerprint camera portion of the fingerprint authentication device shown in Fig. 1;

Fig. 3 is a schematic perspective view of a fingerprint identity authentication device for executing a method of registering fingerprints in accordance with a first embodiment of the invention;

Fig. 4 is a block diagram of a fingerprint identity authentication device for executing the method of registering fingerprints in accordance with the first embodiment of the invention;

Fig. 5 is a flowchart illustrating the method of registering fingerprints in accordance with the first

embodiment of the invention;

Fig. 6 is a schematic perspective view of a personal identity authentication device using fingerprints for managing entry into a room, the authentication device utilizing the first embodiment of the invention;

Fig. 7 is a schematic perspective view of a terminal incorporating the personal identity authentication device using fingerprints, the authentication device being built in accordance with the first embodiment;

Fig. 8 is a schematic perspective view of a palm print identity authentication device for executing a method of registering palm prints in accordance with a second embodiment of the invention;

Fig. 9 is a schematic perspective view of a personal identity authentication device for executing a method of registering retinas or irises in accordance with a third embodiment of the invention;

Fig. 10 is a schematic perspective view of a personal identity authentication device for executing a method of registering facial shapes in accordance with a fourth embodiment of the invention; and

Fig. 11 is a schematic perspective view of a personal identity authentication device for executing a method of registering voice prints in accordance with a fifth embodiment of the invention.

Description of the Preferred Embodiments:

Referring to Fig. 1, a conventional fingerprint authentication device will be described at first in order to facilitate an understanding of this invention. The

illustrated fingerprint authentication device comprises a fingerprint image input section 810, an operation input section 841 such as a keyboard, a display section 851, a recording section 852 such as a printer, and a central processing unit (CPU) 820. The fingerprint image input section 810 comprises a light projecting section 811, a prism 812, and an image sensor 813.

Referring to Fig. 2 in addition to Fig. 1, the light projection section 811 has a light source which irradiates a white light. The prism 812 has a finger surface on which a finger 814 is located. The prism 812 reflects the white light as a reflected light so as to satisfy a total reflection condition at the finger surface. The image sensor 813 receives the reflected light to obtain a fingerprint image. In case where the finger 814 is not in contact with the finger surface of the prism 812, the white light is totally reflected as the reflected light by the finger surface of the prism 812. As a result, the image sensor 813 produces the image which is totally bright.

The finger 814 is pressed on the finger surface of the prism 812 on obtaining a fingerprint image of a two-dimensional. When the finger 814 is pressed on the finger surface of the prism 812, the convex portions of the finger 814 are in contact with the finger surface of the prism 812. The total reflection condition is not satisfied on the convex portions of the finger 814. The white light is mostly absorbed into the convex portions of the finger 814 and is partially reflected on the finger surface.

On the other hand, the concave portions of the finger 814 are not in contact with the finger surface of the prism 812. Therefore, the total reflection condition is satisfied on the concave portions of the finger 814. The white light is totally reflected on the finger surface of the prism 812 and is given to the image sensor 813.

As readily understood from the above description, the image sensor 813 produces the fingerprint image which has bright portions in correspondence to the concave portions of the finger 814. The fingerprint image has dark portions in correspondence to the convex portions of the finger 814.

Again referring to Fig. 1, the fingerprint image is supplied from the image sensor 812 to the CPU 820. The CPU 820 comprises a control section 821. The CPU 820 further comprises a storage section 822, an image processing section 831, a feature point extraction section 832, a numerical value deriving section 833, fingerprint register section 834, a fingerprint comparison section 835, and a decision section 836, all of which controls by the control section 821.

On registering the fingerprint image, the control section 821 is supplied with a register command from the operation input section 841. Responsive to the register command, the control section 821 puts each of the light projection section 811 and image sensor 813 into operation. The above-mentioned fingerprint image is supplied from the image sensor 813 to the image processing section 831. The image processing section 831 processes the fingerprint

image into a processed fingerprint image as a gray scale image. The feature point extraction section 832 extracts feature points from the processed fingerprint image. The feature points may be end points and branching points of the fingerprint. The numerical value deriving section 833 searches coordinates of the feature points. The numerical value deriving section 833 extracts certain phenomena of the feature points to derive numerical values from the certain phenomena. The numerical values may be called feature point data. The fingerprint register section 834 registers the feature point data as registered feature point data therein.

On carrying out authentication, a finger is located on the finger surface of the prism 812. The control section 821 is supplied with an authentication command from the operation input section 841. Responsive to the authentication command, the control section 821 puts each of the light projection section 811 and the image sensor 813 into operation. The fingerprint image is supplied from the image sensor 813 to the image processing section 831. In a similar manner described in registration, the feature point data is produced as an authentication feature point data by the numerical value deriving section 833.

The fingerprint comparison section 835 compares the authentication feature point data with the registered feature point data to produce similarity between the authentication feature point data and the registered feature point data. The decision section 836 judges the authenticity of the person in accordance with the

similarity.

On the other hand, palm prints are verified by a similar manner as used in the case of fingerprints. In case where judgments are made based on pattern structures of capillary vessels of retinas, patterns of irises, facial shapes, or the like, images are directly entered by a camera adapted for the purpose. After image processing, verification is made by a processing procedure similar to that used for fingerprints. In the case of voice prints, voice information entered from a microphone is converted into a frequency band distribution, compared against voice parameters of the registered person himself or herself, and a decision is made based on given standards from the similarity.

At any rate, the entered information is processed, irrespective of the entry manner. The feature points are extracted from the entered information. Phenomena are extracted about each feature point. The numerical values are derived from the feature points. In the case of the subject of authentication that becomes a reference in comparisons, it is registered in the register section. In the case of a subject to be authenticated, it is compared with the registered numerical values in order to produce its similarity. The person is judged to be true in accordance with the similarity.

By the way, a subject to be authenticated such as a fingerprint of a different person has different features and so it is selected as a subject to be authenticated, since it is considered that the features hardly vary with

the passage of time. For example, the contents of the image information are slightly varied depending on the tilt of the finger or on the force with which the finger is pressed, in the case of a fingerprint. When the person is not judged to be genuine, the subjects may be reentered and verification may be reattempted. When the registered feature point data are not typical data about the person, it is difficult to authenticate a person with a high accuracy.

Referring to Figs. 3 and 4, description will proceed to a fingerprint authentication device according to a first embodiment of this invention. The illustrated fingerprint authentication device carries out registration of a fingerprint image. The fingerprint authentication device comprises a fingerprint image input section 110, a central processing unit (CPU) 121, an operation input section 141 such as a keyboard, an IC card information input section 142 for reading data as read data out of an IC card 143 to supply the read data to the CPU 121, a display section 151 for displaying the results of processing and so on, and a recording section 152 such as a printer.

The fingerprint image input section 110 has a light projection section 111, a prism 112, and an image sensor 113. The fingerprint image input section 110 is operable in a similar manner described in conjunction with Fig. 2.

The CPU 120 comprises a control section 121. The CPU 120 further comprises a storage section 122, an image processing section 131, a feature point extraction section 132, a numerical value deriving section 133, fingerprint

register section 134, a fingerprint comparison section 135, a decision section 136, a coincidence calculating section 137, and fingerprint selection section 138, all of which are controlled by the control section 121. The storage section 122 is for storing necessary information. The CPU 120 is connected to a recording medium 129 which records processing procedures for fingerprint authentication.

Referring to Fig. 5 in addition to Figs. 3 and 4, the fingerprint of the finger of the same person is picked up by the fingerprint image input section 110 N -th times on carrying out registration of fingerprint image, where N represents a positive integer which is not less than three. In the example being illustrated, the positive number N may be equal to three.

On registration of a reference fingerprint image, a registration command is supplied from the operation input section 141 to the control section 121 at a first step S102. The registration command is representative of registration of the reference fingerprint image. The registration command may have the positive integer N . Otherwise, the positive integer N may be preset in the control section 121. Responsive to the registration command, the control section 121 controls the display section 151 to make the display section 151 display the positive integer N at a second step S103. Furthermore, the number fingerprint acquisition is displayed as a number X on the display section 151 at a third step S104, where X is positive number between 1 and N , both of inclusive. The examinee puts a finger on the fingerprint image input section 110 at a fourth step S105.

At a first time, the fingerprint image is supplied as a first fingerprint image from fingerprint image input section 110 to the CPU 120. The control section 121 controls the display section 151 to make the display section 151 display an end of a first acquisition at fifth step S106. When the end of the first acquisition is displayed on the display section 151, the examinee releases the finger. At a sixth step S107, the third through the fifth steps S104 to S106 are repeated until the number X is equal to the positive integer N. When the number X is equal to the positive integer N, an end of fingerprint acquisition is displayed on the display section 151 at a seventh step S108.

It will be assumed that first through N-th fingerprint images are supplied to the CPU 120. Supplied with the first fingerprint image, the CPU 120 processes the first fingerprint image into a first processed fingerprint image at a eighth step S109. The CPU 120 extracts feature points as first feature points from the first processed fingerprint image at a ninth step S110. The CPU 120 derives numerical values representing the first feature points to create first feature point data at a tenth step S111. The first feature point data are temporarily registered in the fingerprint register section 134 at a eleventh step S112.

More particularly, the image processing section 131 is supplied with the first fingerprint image from the fingerprint image input section 110. The image processing section 131 processes the first fingerprint image into the

first processed fingerprint image. The feature point extraction section 132 extracts feature points such as end points and branching points of the first processed fingerprint image. The numerical value deriving section 133 searches coordinates of the feature points to extract certain phenomena of each feature point. Furthermore, the numerical value deriving section 133 derives numerical values from the phenomena to produce the first feature point data. The fingerprint register section 134 registers the first feature point data therein.

In a similar manner described above, n -th fingerprint images are processed into n -th feature point data which are temporarily registered in the fingerprint register section 134, where n is a positive number between 2 and N , both of inclusive.

After the first through the N -th feature point data are temporarily registered in the fingerprint register section 134, twelfth step S113 is carried out. In the twelfth step S113, the first through the N -th feature point data are supplied from the fingerprint register section 134 to the coincidence calculating section 137. The coincidence calculating section 137 compares every combination of the first through the N -th feature point data to produce levels of similarities as coincidence degrees. The coincidence calculating section 137 calculates first through N -th total sums of coincidence degrees at first through the N -th feature point data, respectively, at a thirteenth step S114. The fingerprint selection section 138 selects a selected one of the first

through the N-th total sums that has a highest total sum. Namely, the fingerprint selection section 138 selects a selected feature point data most typical of the features of the fingerprint of the person according to the accumulated degrees of coincidence at a fourteenth step S115. The selected feature point data are formally registered as a reference or typical feature point data in the register section 134 at a fifteenth step S116. The reference feature point data are recorded on the IC card 143 of the person at a sixteenth step S117. At a seventeenth step S118, the procedure of registration ends.

On authenticating the fingerprint, an authentication command is supplied from the operation input section 141 to the control section 121. Responsive to the authentication command, the control section 121 controls the image processing section 131, the feature point extraction section 132, the numerical value deriving section 133, the fingerprint register section 134, the fingerprint comparison section 135, and the decision section 136.

As described in conjunction with registration of fingerprint image, the person puts a finger on the fingerprint image input section 110 in order to obtain a fingerprint image as an authentication fingerprint image which is supplied to the image processing section 131. The image processing section 131 processes the authentication fingerprint image into an authentication processed fingerprint image. The feature point extraction section 132 extracts feature points such as end points and branching points of the authentication processed

fingerprint image. The numerical value deriving section 133 searches coordinates of the feature points to extract certain phenomena of each feature point. Furthermore, the numerical value deriving section 133 derives numerical values from the phenomena to produce an authentication feature point data.

The fingerprint comparison section 135 compares the authentication feature point data with the reference feature point data which is registered in the fingerprint register section 134. The reference feature point data may be read out of the IC card 143 to be supplied to the fingerprint register section 134. The fingerprint comparison section 135 produces a similarity between the authentication feature point data and the reference feature point data. On the basis of the similarity, the decision section 136 judges whether or not the person is true to produce a judgement signal. The judgement signal is supplied to the display section 151 through the control section 121. In response to the judgement signal, the display section 151 displays whether or not the person is true.

By the way, data about the attributes of the person are recorded on the IC card 143. The data may be entered from the operation input section 141.

In the personal identity authentication device, the operation input section 141 and the IC card information input section 142 are collectively used as an input section. Alternatively, the IC card information input section 142 may be omitted. Necessary information may be supplied from

the operation input section 141. With respect to the reference feature point data about the person, the data reference feature point data is read out of the fingerprint register section 134. Furthermore, the fingerprint image input section 110 and the IC card input section 142 may be incorporated into the operation input section 141 or into the CPU 120.

A control program is recorded in the recording medium 129. The control program is read out of recording medium 129 to be supplied to the CPU 120. The CPU 120 operates in accordance with the control program. More particularly, the CPU 120 carries out the registration of the fingerprint image and the authentication of the fingerprint image in accordance with the control program as described in conjunction with Figs. 4 and 5.

Referring to Fig. 6, the personal identity authentication device may be for use in managing entry into a room. In the example being illustrated, the personal identity authentication device is installed as a small-sized and wall-mounted personal identity authentication device 200 near a door 260. On managing open and close of the door 260, the IC card is inserted into the IC card insertion slot 242a in order to read IC card information out of the IC card. Furthermore, input information is entered from the operation input section 241. A fingerprint image is entered from the fingerprint image input section 210. As described in conjunction with Figs. 4 and 5, the personal identity authentication device 200 checks the IC card information, the input information, and

the fingerprint image in order to manage the open and the close of the door 260. When the person is judged to be true, the person is allowed to enter.

Referring to Fig. 7, the personal identity authentication device may be used in a terminal. In the example being illustrated, the fingerprint personal identity authentication device is incorporated in a terminal 300 such as an ATM of a financial institution. Requisite items are entered from the operation input section 341. Instead of entry of a code number, the IC card 343 is inserted into the IC card insertion slot 342a. A finger is placed on the fingerprint image input section 310 according to instructions from the display section 351. The identity is verified as described above.

Referring to Fig. 8, description will proceed to a palm print authentication device according to a second embodiment of this invention. The illustrated palm print authentication device executes a palm print registration and palm print authentication. In the palm print authentication device, palm print image is used instead of a fingerprint image on authenticating an individual. The palm print authentication device comprises a palm print image input section 410 which carries a palm 415 thereon. The palm print image input section 410 produces a palm print image. An IC card information input section (not shown) is for entering requisite information from an IC card 443 inserted in an IC card insertion slot 442a. The palm print authentication device further comprises a display section 451, an operation input section 441 such as

a keyboard, and a CPU 420. The palm image input section 410 has an input surface which increases with the size of the palm. The palm print authentication device operates in a similar manner described in conjunction with Figs. 4 and 5.

Referring to Fig. 9, description will proceed to a personal identify authentication device for retinas or irises according to a third embodiment of this invention. Instead of a fingerprint image, the illustrated personal identify authentication device authenticates structural patterns of capillary vessels of retinas or patterns of irises. An Individual is authenticated from the structural patterns of capillary vessels of retinas or features of patterns of irises.

The personal identity authentication device comprises a CPU 520, a camera 510, an IC card information input section (not shown), a display section 551, and an operation input section 541 such as a keyboard. The camera 510 takes a picture of a retina or an iris to produce a pattern image. More particularly, the camera 510 directly takes an image of the retina of an eyeball or the iris around a pupil and enters the structural pattern of the capillary vessel of the retina or an image of the pattern of the iris. The IC card information input section reads requisite information out of an IC card 543 inserted into an IC card insertion slot 542a.

The image input camera 510 is used instead of the fingerprint image input section 110 described in conjunction with Figs. 4 and 5. The image input camera 510

supplies the pattern image to the CPU 520. Except that the pattern image is used instead of the fingerprint image, the personal identity authentication device carries of the registration and authentication in a similar manner described in conjunction with Figs. 4 and 5.

Referring to Fig. 10, description will proceed to a personal identity authentication device for a facial shape according to a fourth embodiment of this invention. In Fig. 10, the facial shape is used for authentication instead of a fingerprint. An Individual is authenticated from features of structural elements extracted from an image of the facial shape. The personal identity authentication device comprises a CPU 620, a camera 610, an IC card information input section (not shown), a display section 651, and an operation input section 641 such as a keyboard.

The camera 610 takes a picture of a face to produce a facial shape image. More specifically, the camera 610 is disposed in front of a face 617 to directly take an image of the shape of the face 617 and to produce the facial shape image. The IC card information input section reads requisite information out of an IC card 643 inserted into an IC card insertion slot 642a.

The shape image input camera 610 is used instead of the fingerprint image input section 110 described in conjunction with Figs. 4 and 5. The shape image input camera 610 supplies the facial shape image to the CPU 620. Except that the facial shape image is used instead of the fingerprint image, the personal identity authentication device carries of the registration and authentication in a

similar manner described in conjunction with Figs. 4 and 5.

Referring to Fig. 11, description will proceed to a personal identity authentication device for a voice print according to a fifth embodiment of this invention. In Fig. 11, the voice print is used for authentication instead of a fingerprint. Parameters of a frequency distribution are extracted as an extracted voice print from a voice of person. On carrying out the authentication, the extracted voice print is compared with a reference voice print.

The personal identity authentication device comprises a CPU 720, a microphone 710, an IC card information input section(not shown), a display section 751, and an operation input section 741 such as a keyboard. The microphone 710 is disposed in front of a face. The microphone 710 receives a to produce voice information. The IC card information input section reads requisite information out of an IC card 743 inserted into an IC card insertion slot 742a. The CPU 720 produces the parameters form the voice information.

The microphone 710 is used instead of the fingerprint image input section 110 described in conjunction with Figs. 4 and 5. The microphone 710 supplies the voice information to the CPU 720. Except that the voice information is used instead of the fingerprint image, the personal identity authentication device carries of the registration and authentication in a similar manner described in conjunction with Figs. 4 and 5.

While this invention has thus far been described in conjunction with the preferred embodiments thereof, it will

readily be possible for those skilled in the art to put
this invention into practice in various other manners.

WHAT IS CLAIMED IS:

1. A method of registering original information for personal identity authentication, said original information being used as a reference for verification of an authentication subject, comprising:

a first step of extracting a feature point in number of N from said authentication subject to produce first through N-th feature point data, where N represents a positive integer which is not less than three;

a second step of comparing an n-th feature data with each of remaining feature data to produce levels of similarities as coincidence degrees in each of said first through said N-th feature point data, where n is variable between 1 and N, both of inclusive;

a third step of calculating a sum degree of said coincidence degrees in each of said first through said N-th feature point data to produce first through N-th sum data; and

a fourth step of selecting a maximum one of said first through said N-th sum data to register, as said original information, one of said first through said N-th feature data that has said maximum sum data.

2. A method as claimed in Claim 1, wherein said first step comprises:

a fifth step of extracting a feature point in number of N from said authentication subject to produce first through N-th feature points; and

a sixth step of converting said first through said N-th feature points into first through N-th numerical values to produce said first through N-th numerical values as said first through said N-th feature point data.

3. A method as claimed in Claim 2, wherein said second step comprises:

a seventh step of comparing said n-th feature data with each of said remaining feature data to produce levels of similarities in each of said first through said N-th feature point data; and

an eighth step of converting said levels into numerical levels in each of said first through said N-th feature point data to produce said numerical levels as said coincidence degrees.

4. A method as claimed any one of Claims 1 to 3, wherein said authentication subject is a fingerprint.

5. A method as claimed any one of Claims 1 to 3, wherein said authentication subject is a palm print.

6. A method as claimed any one of Claims 1 to 3, wherein said authentication subject is a voice print.

7. A method as claimed any one of Claims 1 to 3, wherein said authentication subject is a structural pattern of capillary vessels of retinas.

8. A method as claimed any one of Claims 1 to 3, wherein said authentication subject is a pattern of irises.

9. A method as claimed any one of Claims 1 to 3, wherein said authentication subject is a facial shape.

10. A personal identity authentication device for authenticating an authentication subject, comprising:

first means for extracting a feature point from said authentication subject to produce extracted feature point data on authentication, said first means extracting a feature point in number of N from said authentication subject to produce first through N-th feature point data on registration, where N represents a positive integer which is not less than three;

second means for registering a reference feature point data therein;

third means for comparing said extracted feature point data with said reference feature point data to judge whether or not said authentication subject is true on authentication, said third means comparing an n-th feature data with each of remaining feature data to produce levels of similarities as coincidence degrees in each of said first through said N-th feature point data on registration, where n is variable between 1 and N, both of inclusive; and

fourth means for selecting a maximum one of said first through said N-th sum data to register, as said reference feature point data in said second means, one of said first through said N-th feature data that has said maximum sum data.

11. A personal identity authentication device as claimed in Claim 10, wherein said second means is an IC card.

12. A recording medium memorizing a control program which is for registering original information for personal identity authentication, said original information being used as a reference for verification of an authentication

subject, wherein said control program comprises:

a first procedure of extracting a feature point in number of N from said authentication subject to produce first through N-th feature point data, where N represents a positive integer which is not less than three;

a second procedure of comparing an n-th feature data with each of remaining feature data to produce levels of similarities as coincidence degrees in each of said first through said N-th feature point data, where n is variable between 1 and N, both of inclusive;

a third procedure of calculating a sum degree of said coincidence degrees in each of said first through said N-th feature point data to produce first through N-th sum data; and

a fourth procedure of selecting a maximum one of said first through said N-th sum data to register, as said original information, one of said first through said N-th feature data that has said maximum sum data.