

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
19 April 2001 (19.04.2001)

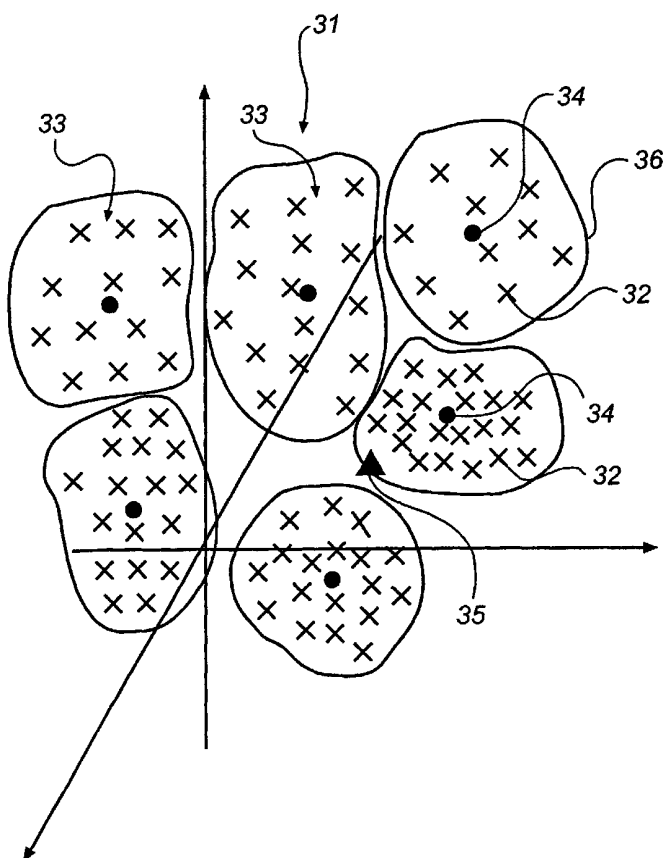
PCT

(10) International Publication Number
WO 01/26549 A1

- (51) International Patent Classification⁷: **A61B 5/117**,
G06K 9/50, 9/00
- (21) International Application Number: PCT/SE00/01997
- (22) International Filing Date: 13 October 2000 (13.10.2000)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
9903684-0 13 October 1999 (13.10.1999) SE
60/160,471 21 October 1999 (21.10.1999) US
- (71) Applicant (for all designated States except US): **PRE-CISE BIOMETRICS AB** [SE/SE]; Dag Hammarskjölds väg 2, S-224 64 Lund (SE).
- (72) Inventors; and
(75) Inventors/Applicants (for US only): **WIEBE, Linus** [SE/SE]; Bokhållaregatan 33, S-211 56 Malmö (SE). **ÖBRINK, Mårten** [SE/SE]; Exercisgatan 3, S-211 49 Malmö (SE). **BERGENEK, Jerker** [SE/SE]; Lagerbrings väg 4B, S-224 60 Lund (SE). **KAHL, Fredrik** [SE/SE]; Karl XI gatan 6, S-222 20 Lund (SE).
- (74) Agent: **AWAPATENT AB**; Box 5117, S-200 71 Malmö (SE).
- (81) Designated States (national): AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD,

[Continued on next page]

(54) Title: METHOD AND DEVICE FOR PROCESSING BIOMETRIC DATA, BY DETERMINING FEATURES AND CLASSIFYING THE DATA



(57) Abstract: A method of generating reference data from current biometric data of an individual comprises the steps of generating feature values; letting the feature values form coordinates, which are combined in such manner that they define a current dot (35) in a space (31). The space (31) is divided into subspaces (33) which are represented by an associated class with a class denomination; selecting to which subspace (33) the current dot (35) belongs; and equating said reference data to the class denomination. The space (31) comprises a number of data dots (32) which correspond to a quantity of biometric data, collected in advance, of a number of individuals. The method allows great probability for the same reference data to be generated for repeated collections of the same biometric parameter or characteristic of one and the same person. The disclosure also includes a device operating according to the methods, and a method, system and processing unit for checking the right to access to sensitive information, as well as a method for checking if current biometric data is represented in a database.

WO 01/26549 A1



SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

Published:

— *With international search report.*

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method and device for processing biometric data, by determining features and classifying the data.

Field of the Invention

The present invention relates generally to a method
5 of generating reference data from biometric data of an individual. The invention also relates to a device for generating such reference data. Moreover, the invention relates to a method of checking, based on biometric data of an individual, the right to access to sensitive information, and a method of checking whether biometric data
10 is represented in a database. The invention also concerns a system for checking the right to access of the type mentioned above, and a processing unit included in the system.

15 Background Art

Biometry means measuring, analogously or digitally, one or some individual- and body-specific parameters or characteristics, such as the appearance of or the pattern of an individual's fingerprint, palm, fundus of the eye,
20 iris, or face, or some other information that is not related to appearance, such as the individual's voice. This information can be used, for instance, in verification, authenticity control, or identification of an individual.

25 In many cases, the access to information of various kinds must be reserved to certain individuals only. This also applies to, for instance, the access to particular rooms or buildings. When one wants to verify an individual's right to access to, for instance, an information
30 quantity, i.e. his right to access this information, it is common to employ systems using, for example, a multi-digit code, such as a PIN code (PIN = personal identification number) or a password. A drawback of such systems is that individuals having the right to access must

remember the code or password. Thus, an individual can, if he forgets the code/password, be refused access even if he is actually authorized. Since most people must remember a large number of codes/passwords, there is a risk that the codes or passwords are written down on a sheet of paper or that an individual uses the same code for several purposes. This makes it easier for unauthorized people to get hold of the code/password. It goes without saying that this reduces the security in a system of the type described above. Moreover, it is not checked whether the person indicating the correct code/password is one of the individuals who have originally received the code or password, i.e. the right to access. Thus, the group of people who is in fact given access to sensitive information or buildings/rooms can quickly be increased by unauthorized people to which the code or password has been "lent".

To avoid the above problems, an individual's right to access can be verified by means of biometry. Then the individual does not have to remember a code or password but instead some kind of body-specific and individual-specific or individual-unique characteristic or parameter of the individual at issue is verified. For example, a system based on this technique may use biometric information of any of the kinds stated above. The method is based on reading, in a first step using a collecting method of some type, biometric data in the form of, for example, image or sound data of a number of people. Data is preprocessed and then an algorithm of some kind is applied to preprocessed biometric data, so that for each individual a first reference data or a first template is generated from collected biometric data. Such reference data usually consists of a reduced quantity of original data. In the verification of an individual's right to access, current biometric data is collected by means of the same or some other collecting method. Subsequently, such collected current biometric data is preprocessed,

and an algorithm (the same as before or some other algorithm) is applied to such preprocessed current biometric data to form a second reference data from said current biometric data. For comparing said first and second reference data or template, which can have the same or different formats, a second algorithm is applied in such manner that a measure of how well these two reference data or templates correlate is obtained. This measure is finally compared with a predetermined threshold value. In this way, it is determined whether it may be considered that said first and second reference data, which represent previously collected biometric data and current biometric data, respectively, come from the same individual or not.

A problem of prior-art biometric systems is that they do not generate the same reference data or templates from two sets of biometric information, i.e. biometric data from different collectings/readings from the same individual (such as two images of the same finger which have been taken using the same collecting method). Thus, a comparison or matching of two different reference data is carried out in, for example, verification. The outcome of the comparison is determined by means of a threshold value. If a threshold value is set at, for example, 90%, the two reference data are considered to come from the same individual if they agree to at least 90%. Consequently, this is a complicated process which cannot be performed in, for example, environments which are extremely limited as regards memory, processor capacity etc. A further drawback of prior-art biometric systems is that original biometric data could be recovered from reference data, thus reducing the security.

Today, use is often made of smart cards (intelligent cards) as data carriers of sensitive information. Part of the information that is stored on a smart card consists of a template or reference data, which can be described as prestored reference information regarding the card

user. It is with this template that a comparison is made each time the card user wishes to verify his right to use the card. If the card is intended for use as an entry card or key card, for example for physical access to a room or building, no information other than the template need be stored on the card. The right to access to standard-type smart cards is presently checked by somehow presenting a PIN code, which usually consists of four digits between 0 and 9. If one wants to avoid the above problems with codes and instead use biometry to access a common smart card, this is usually carried out by storing the necessary PIN code somewhere outside the card in software or hardware. If the comparison or matching of reference data from biometric data produces a positive result, the PIN code is then presented to the card. The storing of the PIN code outside the card reduces the security in such a system.

One related example is found in US-A-5 509 083 which discloses a method for confirming the identity of an individual presenting an identification card. The card has stored thereon a code containing code-addresses to a number of templates which are stored in a template library in a central processing unit, and code-coordinates for each template being addressed by the code. The templates are target images, typically with a size of 16*16 pixels. To confirm the identity of an individual, a fingerprint image is registered, and correlation values are calculated in each position in the image as identified by the code-coordinates, by correlating the target image addressed by the code with the fingerprint image at the associated position. The resulting correlation values are compared to a threshold value, whereupon it is decided whether to accept the identity of the cardholder.

When one wants to check whether current biometric data of a person is included in a database, which comprises biometric data, recorded in advance, of a plura-

lity of people, reference data corresponding to current biometric data is compared with a respective one of a number of reference data included in the database. The structure of the database determines with which biometric data comparisons are to be performed. One way is to search the database hierarchically. A difficulty in hierarchic search, however, is that a large number of comparisons are necessary, which makes the process time-consuming. Moreover, a method as described above may result in possibly relevant parts of the database being missed in the search.

Summary of the Invention

A general object of the present invention is to wholly or at least essentially obviate the above problems of prior art. More specifically, it is a general object to provide a method, improved over prior art, of generating reference data from current biometric data of an individual. A further general object of the invention is to provide a device for generating such reference data. More specifically, the inventive method and the inventive device should afford great probability that the same reference data is generated from two sets of biometric information regarding the same individual-specific characteristic of one and the same person. Moreover, the generated reference data should consist of information which makes it difficult or impossible to recover original biometric data. Moreover, the inventive method and the inventive device should place low demands in respect of memory space and processor capacity.

A further object of the present invention is to provide a method of checking, based on current biometric data of an individual, the right to access to sensitive information. This method should be quick, safe and simple, and the probability that an individual with a right to access is refused access and that an individual with no right to access is granted access should be small.

One more object of the invention is to provide a system for checking such right to access. The system should be safe and simple in its design.

Moreover, an object of the invention is to provide a
5 processing unit for checking the right to access to sensitive information stored on a portable data carrier, said check being based on current biometric data of an individual.

It is also an object of the present invention to
10 provide a method of checking whether current biometric data of an individual is represented in a database. More specifically, an object of the invention is to provide a method of permitting in a simple manner that only parts of a database need be searched with no risk that relevant
15 parts of the database are missed.

These objects are achieved wholly or partly by a method and a device for generating reference data according to appended claims 1 and 18, respectively, a method, a system and a processing unit for checking the right to
20 access according to appended claims 30, 37 and 44, respectively, and a method of checking whether current biometric data of an individual is represented in a database according to appended claim 48. Preferred embodiments are stated in the dependent claims.

25 By selecting, according to the inventive method of generating reference data, starting from a number of feature values, a class for current biometric data and equating the reference data thereof with the class denomination of the selected class, there is allowed very
30 great probability that the same reference data is to be generated for repeated collections of the same biometric parameter or characteristic of one and the same individual. This follows from the fact that the feature values could differ to some extent for repeated collections of
35 biometric data and still generate the same reference data since they may be considered to belong to the same class.

Preferably, current biometric data is divided into one or more data subsets before the feature values are generated, thereby permitting that a number of variables or features which are independent of each other are defined. Moreover, an optimal utilization of the information in said current biometric data is allowed since it thus is possible to, for example, attach greater importance to the data subsets which are most relevant or contains most information.

An advantage of defining a starting point is, if the starting point is consistently locatable, that exactly the same division of biometric data can be made and, thus, the same feature values can be generated from different collections of the same biometric parameter of one and the same individual.

By letting the feature values of both current biometric data and each biometric data collected in advance preferably constitute coordinates for a respective point in a space which is divided into subspaces corresponding to the classes, an easily comprehensible representation of data is obtained. This allows the use of simple algorithms to decide, for example, class association for the current biometric data.

An advantage of letting the subspaces mutually correspond to essentially the same quantity of biometric data collected in advance is that a better resolution and, thus, security are allowed, for instance, when one wants to use reference data generated from current biometric data for verification purposes.

Each class denomination consists of a data string, preferably comprising a combination of characters, such as figures only, letters only, or figures and letters. Since reference data is equated to a class denomination of this kind, reference data without any redundant information is obtained, and an exact matching can be made when comparing two reference data. The comparison can be carried out quickly and easily since it does not require

a complicated algorithm. It is only necessary to match figures and/or letters with each other. They are either equal or not. The result of such a comparison can thus be only "yes, equal" or "no, not equal" and therefore a threshold value for this decision is not necessary either. Moreover, both reference data and a comparison algorithm requires a small storage space. A further advantage is that data cannot easily be recovered from reference data/template.

10 The fact that reference data preferably consists of, for example, a combination of figures allows generation, directly from current biometric data, of reference data which serves as a code, such as a PIN code, for e.g. a smart card.

15 The inventive device for generating reference data from biometric data presents advantages corresponding to those of the inventive method of generating reference data.

 The portable data carrier, which is included in the inventive system for checking the right to access, may have a simple signal processing device since the comparison of reference data is simple. Further the simple comparison algorithm for the signal processing device of the data carrier takes little place in the memory of the data carrier. Thus, simple portable data carriers, such as standard type smart cards, can be used, which allows an inexpensive system. An advantage of the sensitive information regarding the data carrier user/owner, i.e. reference data or template, being stored in the data carrier and not in, for example, the processing unit of the system is that the system will be more secure since said information then accompanies the portable data carrier and its owner. The inventive system can also be made simple thanks to the fact that only small information quantities for checking the right to access need be transferred between the parts of the system. Such a system also allows that a data carrier can give the right to

access to a plurality of users by a plurality of templates being stored on the data carrier.

By selecting, in the inventive method for checking whether current biometric data of an individual is represented in a database, for said current biometric data a class from a plurality of classes having respective class denominations, and by letting the items of the database have item denominations corresponding to a respective one of the class denominations, the class denomination of the class selected for said current biometric data can, in checking, be used to choose a suitable part of the database. In this way, a comparison with the most relevant biometric data can be quickly made with little risk that relevant parts of the database are missed such as in, for instance, a hierarchic search of a database.

Brief Description of the Drawings

The invention and its advantages will be described in more detail below with reference to the accompanying schematic drawings, which for the purpose of exemplification illustrate presently preferred embodiments.

Fig. 1 is a schematic view of an inventive system for checking the right to access.

Fig. 2 is a block diagram which illustrates an inventive method of checking the right to access.

Fig. 3 is a schematic view of a space, which is used to represent biometric data of a plurality of people. The space is divided into subspaces to each of which an attraction point has been assigned.

Fig. 4 is a schematic view of a space, which is represented by attraction points only.

Fig. 5 shows a presently preferred method of dividing a two-dimensional representation of a fingerprint for generating feature values.

Figs 6-7 show alternative methods of generating feature values.

Description of Preferred Embodiments

Fig. 1 is a schematic view of a preferred embodiment of an inventive system for checking the right to access to sensitive information, said checking being based on biometric data of an individual whose right to access to the sensitive information is to be checked. The system comprises a portable data carrier 1 and a processing unit 2. As a rule, the system comprises a plurality of portable data carriers 1, since each individual with a right to access usually has a data carrier 1 of his own. The data carrier 1 comprises a memory 3, a signal processing device 4 and a communication device 5. The processing unit 2, which can be a PC (Personal Computer), comprises a signal processing device 6, a communication device 7 and a sensor 8 for collecting/reading of biometric data in the form of a digital representation, such as a digital image. The signal processing device 6 in turn comprises a memory 9 and a processing means 10.

The data carrier 1 consists of an intelligent card, smart card, of a standard type, for instance a Java or MULTOS card. The communication device 5 of the card 1 is adapted to communicate with the communication device 7 in the PC 2. The communication devices 5, 7 can be designed either for contact-type communication or contactless communication. An example of the latter type is communication by means of infrared light (IR) and by means of radio signals. In the memory 3 of the card 1 there are stored on the one hand the sensitive information to which the current user wants to be granted the right to access and, on the other hand, a template, i.e. reference data from biometric data of the individual having the right to access. Such current biometric data may consist of a digital image of an individual- and body-specific characteristic or parameter, such as a fingerprint. A plurality of templates can be stored in the memory 3, for instance when several people want to share a card. A system in

which the sensitive information to which access is desired, is stored in a unit outside the card 1 is also possible.

The PC 2 is arranged to receive, via the sensor 8,
5 current biometric data of the individual whose right to access is to be checked. In this embodiment, the sensor 8 is a capacitive sensor. However, also other types of sensors which can record fingerprints can be used, such as heat sensors and optical sensors. The sensor 8 can be
10 arranged separate from the processing unit 2. Moreover, the PC 2 is arranged to carry out, by means of the signal processing device 6, a preprocessing of the digital image, and starting from the preprocessed image generate with the aid of the processing means 10 a current tem-
15 plate, i.e. reference data from said current biometric data, and to transfer the current template to the signal processing device 4 of the card 1 via the communication devices 5, 7. Preprocessing may comprise binarization and vectorization. The signal processing device 4 is designed
20 to compare this received current template with the template stored in advance in the memory 3 of the card 1 to determine whether the right to access to the sensitive information exists. This template stored in advance consists of reference data for, for example, a fingerprint.
25 The signal processing device 4 is further designed to determine, in cases of correspondence between the received current template and the template stored in advance, which operations the PC 2 is allowed to perform on the sensitive information. The signal processing device 6 of
30 the PC 2 is designed to perform operations on the sensitive information, based on the rights which are assigned to the PC 2 by the card 1. The comparison of the current template and the template stored in advance could be carried out outside the card 1, for instance in the PC 2.
35 The memory means 9 included in the signal processing device 6 of the PC 2 contains a set of data which corresponds to biometric data of a number of people which has

been collected in advance. This set of data is used in the generating of the current template from current biometric data by means of the signal processing device 6, as will be described in more detail below with reference to Figs 3 and 4.

Fig. 2 illustrates an embodiment of an inventive method of checking, based on current biometric data in the form of a fingerprint of a person, the right to access to sensitive information. In step 20, an image of a fingerprint of the person whose right to access is to be checked is collected by means of the sensor 8 in the PC 2. Then follows step 21 of generating, starting from the image of the finger, the current template. This occurs in the signal processing device 6 of the PC 2. In step 22, the current template is compared with the template that has been stored on the card 1 in its memory 3. If the comparison in step 22 generates the result that the current template and the template stored on the card 1 are equal, the right to access to the sensitive information stored in the memory 3 of the data carrier 1 is granted.

Step 21, in which the current template from the image collected with the sensor 8 is generated, comprises a number of partial steps. First, a starting point or reference point in the image is defined. Below follows a description of how this definition can be performed. Starting from the starting point, the image is then divided into sub-areas or data subsets. Based on these data subsets, feature values are generated. A preferred method of making the division of the image into data subsets and generating the feature values will be described in more detail below.

Starting from the feature values, one of a plurality of classes is then selected, each class corresponding to a quantity of biometric data, collected in advance, of a number of people. Each class has a class denomination. The classes are defined starting from feature values,

which represent the quantity, belonging to the respective classes, of biometric data collected in advance. To select a class, one lets the feature values from said current biometric data represent coordinates which are combined so as to define a current point in an n-dimensional space. The number of dimensions, n , is determined by the number of feature values generated from each biometric data. Figs 3 and 4 show a three-dimensional space, i.e. the number of feature values is in this case three. Figs 3 and 4 will be explained in detail below. The n-dimensional space is divided into subspaces, which correspond to said classes and the associated class denominations. Subsequently a class can be selected by determining to which subspace the current point belongs. Finally, the current template is equated to the class denomination for the selected class. A preferred method of dividing the n-dimensional space into subspaces will also be described below.

Definition of Starting Point in an Image of a Fingerprint:

It has traditionally been an extremely complex operation to define a consistently locatable starting point in an image of a fingerprint owing to the many existing types of fingerprints. Also in traditional, manual fingerprint classification, starting from a large set of rules for identification of the starting points for many types of fingerprints, starting points cannot be defined for certain types of fingerprints.

However, in one embodiment of the present invention, only two procedures are required. The first procedure is based on a vectorization of the gray scale image and locates a starting point from the vector representation of the gray scale image. The second procedure, which is used only if the first procedure does not manage to locate a starting point, locates the geographic center of the image. Alternatively, the second procedure can be based on counting the number of ridges in a binarized

image, or by calculating fast Fourier transforms (FFT) for the fingerprint image and selecting the point corresponding to the dominant frequencies.

A more exhaustive description of how a starting point or reference point can be defined is to be found in Applicant's International Patent Publication WO 99/51138, which is incorporated herein by reference.

A preferred method of locating or defining a starting point in an image of a fingerprint has been described above. It will be appreciated that there are many different methods of carrying out this location or definition and that the essential thing is not where in the fingerprint the starting point is located or the appearance of the structures in its surroundings, but that it is located in the same position in each collection of the same fingerprint. The term starting point should thus be interpreted as a position in a sense which in each collection is the same relative to other positions in the image. In other types of biometric data, the starting point of course represents something else than it does in an image of a fingerprint. For example, the starting point in face recognition may be the nose and in voice recognition a frequency.

A Preferred Method of Generating Feature Values:

According to a preferred embodiment, the image is divided into smaller areas, which gives a number of data subsets, by arranging, with the starting point S in the zero point, eight concentric circles with an increasing radius around the starting point S (see Fig. 5). Then the image is divided further by arranging ten radii starting from the starting point S, uniformly distributed over 360°. This gives $8 \times 10 = 80$ smaller areas or data subsets. When the division is completed, a number of, for instance eight, filters, such as Gabor filters, are applied to each area. For each filter and area, a feature value is obtained in the form of a number. It will be appreciated that there are a large number of dif-

ferent ways of carrying out the division of the image or the data quantity. The Gabor filter is a common filter in image processing and is generally described in e.g.

Granlund, Knutsson "Signal Processing for Computer

5 Vision", Kluwer, 1995 and in connection with fingerprint identification in Jain et al, "A FingerCode: A Filterbank for Fingerprint Representation and Matching", IEEE Conference on CVPR, Colorado, USA, 1999. The filter can be applied to two-dimensional images to identify edge and
10 line structures. When applied to images of fingerprints, a characterization of the extension of ridges and valleys in the fingerprint is obtained. When it is approximately known how wide (in pixels) the ridges and the valleys are in the image, the Gabor filters can be set in such manner
15 that they react particularly on these structures while other structures do not affect the result to the same high degree. The Gabor filter is direction-dependent, which means that a filter merely indicates structures in one direction (for instance vertical) in the image. In
20 practice, Gabor filters are therefore used with 4-8 different directions to cover all directions.

Alternative Methods of Generating Feature Values:

According to an alternative embodiment of the invention and as illustrated in Fig. 6, feature values can be
25 generated from a two-dimensional image of a fingerprint by a polygon 51, such as a square, being superimposed on the image in a position which is determined in relation to the starting point S. The area typically comprises 100*100 pixels. Four feature values are obtained by
30 counting the number of ridges, alternatively the number of transitions from black to white and white to black, along the respective edge lines 52-55 of the square 51. In the example in Fig. 6, there are 11, 13, 9 and 6 ridges for the respective edge lines 52-55.

35 According to a further alternative embodiment of the invention, the step of generating feature values from said current biometric data can be carried out with the

aid of Principal Component Analysis (PCA), which is also referred to as Karhunen-Loève and Hotelling transform and which is described in Gonzales-Woods, 'Digital Image Processing', Addison Wesley, 1993. This is a known method of
5 identifying the most significant features in two-dimensional images. Using a number of two-dimensional example images of fingerprints (with the zero point suitably in the starting point), it is possible to calculate how these vary by estimating their covariance matrix. The
10 eigenvectors, belonging to the maximum eigenvalues, of the covariance matrix describe the most significant variations in the original example series of images. These eigenvectors can be referred to as $v_1, v_2, \dots, v_m$, where m is the number of eigenvectors. A new image of a
15 fingerprint (with the zero point in the starting point), called f , can then be approximated with linear combinations of the eigenvectors, i.e. $f \approx a_1*v_1 + a_2*v_2 + \dots + a_m*v_m$, wherein $a_1, a_2, \dots, a_m$, is m scalars (numbers). The m scalars ($a_1, a_2, \dots, a_m$) form feature values.

20 A related method of generating feature values is to apply a number of statistically generated target images, principal components, to the current fingerprint and then investigate how well these correlate therewith. An example of how this is done is illustrated in Fig. 7. The
25 image is divided into, for example, four target areas 61-64. Each target image 65-68 is compared with each target area 61-65 to investigate with which part of the target area 61-65 the target image 65-68 correlates best. These "best correlation values" form feature values, and
30 in the present example, 16 feature values (= number of target images * number of target areas) are thus obtained.

According to a further alternative embodiment, feature values can be generated starting from measures in
35 the image, such as average width of the lines (ridges) in the fingerprint, the curvature of the line just above the

starting point and the average distance between the lines.

Definition and Division of the Space:

According to a preferred embodiment of the invention, the n-dimensional space is defined by the steps of defining starting point or reference point and generating feature values being carried out on biometric data, collected in advance, of a large number of people. For each individual's biometric data, the feature values form coordinates. These coordinates are combined so that they represent a data point or data dot for the associated individual in the n-dimensional space. Each individual can also be represented by more than one data. Fig. 3 illustrates such a representation for n=3. In the three-dimensional space 31, there is a large number of data dots 32. Based on the amount of data dots 32, the n-dimensional space 31 is divided into subspaces 33, in such a manner that each subspace 33 preferably contains the same amount of data dots 32. If, for instance, biometric data of 100,000 people has been collected, which gives 100,000 data dots 32, and 100 subspaces 33 are requested, each subspace 33 should thus comprise about 1,000 data dots 32. Subsequently, a "typical point" or attraction point 34 is assigned to each subspace 33 in such manner that each data dot 32 in the subspace 33 is closer to this attraction point 34 than the attraction points 34 belonging to the other subspaces 33. A method of dividing the n-dimensional space 31 is to use a clustering technique, such as 'Self-organizing Maps' which are described in, for instance, Kohonen, "Self-organizing Maps", Springer, 1995. A division of this type proceeds in such manner that, like before, it is assumed that there are 100,000 data dots 32 in the n-dimensional space 31. Then 100 attraction points 34 are placed in the space 31 so that the sum of the distances between each attraction point 34 and the respective about 1,000 closest data dots 32 will be as small as possible. A distance can be

determined as, for instance, a Euclidean distance. Each of the 100 attraction points 34 thus is in some sense the "typical point" for the associated subspace 33 or class and is usually referred to as prototype. Each attraction point 34 or subspace/class 33 can be represented by a class denomination, which consists of a numeric digit (alternatively alphanumeric, or of a bit sequence), in the example above 0-99.

A person skilled in the art realizes that after completion of the division of the n-dimensional space 31, only the coordinates for the attraction points 34 are necessary to define the subspaces 33 and thus the classes (see Fig. 4). Thus, feature values need not be stored, which saves a lot of memory space. A class/subspace 33 for said current biometric data is thus selected by determining the distance between the corresponding current data dot 35 and the attraction points 34, and the class/subspace 33 is selected, whose attraction point 34 is positioned at the shortest distance D from the current dot 35.

The division of the n-dimensional space 31 could be adaptive so that the division is adjusted each time one studies new biometric data of a person which one wants to be included in known data.

Alternative Method of Representing Subspaces in the n-dimensional Space:

According to an alternative embodiment of the invention, the subspaces 33 in the n-dimensional space 31 can be described by means of the coordinates of their boundary 36. In the schematic space 31 in Figs 3 and 4, the attraction points 34 would thus not be necessary and it would be possible to find out to which subspace 33 the current dot 35 belongs by investigating in which subspace 33 it is positioned. Each subspace 33 would in this case be represented by a class denomination. According to this embodiment, either the subspaces 33 together should fill the entire space 31, or special measures must be taken if

the current dot 35 is located between the defined sub-spaces 33.

Method of Searching a Database:

The inventive method, as described above, of
5 generating reference data from current biometric data of an individual can also be used when searching a database to check if current biometric data of an individual is represented in the database. The database to be searched according to the invention generally contains a large
10 number of items, each item corresponding to biometric data of an individual and being assigned an item denomination.

In its most general aspect, the inventive method of searching the database comprises the steps of generating,
15 based on the current biometric data, a number of current feature values; selecting, based on the current feature values, one of a plurality of classes, each class corresponding to a quantity of biometric data, collected in advance, of a number of individuals, and having a
20 class denomination; and comparing the current biometric data with biometric data associated with at least one item which is assigned an item denomination that corresponds to the class denomination of the selected class. Thus, the inventive method of generating reference
25 data is used in providing a classification of the current biometric data, the classification being used in searching the database, to select a suitable part of the database to be searched. In this way, a comparison with the most relevant biometric data can be quickly made with
30 little risk that relevant parts of the database are missed such as in, for instance, a hierarchic search of a database. For reasons of search speed, it is preferred that the step of comparing is effected by comparing the current feature values with a combination of feature
35 values associated with the one or more database items that have a suitable item denomination.

The feature values can be generated according to any of the alternative methods described above. Likewise, the selection of class can be made according to any one of the alternative methods described above, for example by letting the current feature values represent a data dot in an n-dimensional space divided into subspaces that correspond to the classes and are assigned the class denominations, and by determining to which subspace (class) the data dot belongs.

10 The invention has been described above with reference to embodiments selected by way of examples, and variations and modifications are feasible within the scope of the invention. For example, the portable data carrier, which has been exemplified above as a smart card, can also be, for instance, a Java ring, a Palm pilot (PDA) or a SIM card. The processing unit can, as mentioned above, be a computer of some type, such as a PC, but there is a large number of other applications. For example, the processing unit could be a cash dispenser, a mobile phone, a door lock, a TV box which grants access to certain cable television channels etc.

The memory means in the portable data carrier and in the signal processing device of the processing unit have not been rendered more precise, but may consist of e.g. RAM, ROM, Flash or EPROM. Furthermore, the signal processing devices in the data carrier and in the processing unit may comprise, for example, a processor, an FPGA, or an ASIC.

The processing means of the processing unit may comprise, for example, an algorithm, hardware, such as a processor, an FPGA or an ASIC, or e.g. an optical lens. The communication between the units of the system described above can be carried out, as mentioned above, either in a contactless manner or with the aid of some type of physical lines, such as Ethernet, Bluetooth, or Firewire, and some type of protocol such as USB, IP or RF232 serially.

It will also be appreciated that a distance between dots in the n-dimensional space can be determined in several ways. The geometric distance can be determined, for example, by using Pythagoras's theorem or n-dimensional octagons, which gives the above-mentioned Euclidean distance. In the description, only an orthogonal system has been described, but the term "distance" is intended to be interpreted in a wide sense and to apply also to spaces in non-orthogonal systems.

In the above described, presently preferred embodiments of the invention, biometric data has represented a fingerprint. However, the invention also functions for other types of biometric data, i.e. for representations of other types of body- and individual-specific characteristics or parameters. The biometric information may consist of, for example, the pattern of an individual's palm, fundus of the eye, iris, or face, or some other information which is not related to appearance, such as the individual's voice. It will be appreciated that the sensor for collecting biometric data must be selected for and adapted to the type of biometric parameter. The division of the images and the generation of feature values can be carried out in a similar manner for the biometric data that is represented by images. For a voice specimen, division and identification of features can instead be performed with respect to, for example, frequencies.

The class denominations are data strings, i.e. they comprise "a combination of characters such as figures and/or letters" or "a numeric or alternatively an alphanumeric digit". These expressions are intended to be interpreted in a very wide sense, such as a combination of characters of some kind. By digits are meant digits with any base or radix whatever.

Summing up, the invention thus comprises all such alternatives, modifications and variations as fall within the scope of the appended claims.

CLAIMS

5 1. A method of generating reference data from current biometric data of an individual, comprising the steps of:

 generating, based on said current biometric data, a number of feature values,

10 selecting, based on said feature values, one of a plurality of classes, each class corresponding to a quantity of biometric data collected in advance from a number of individuals and having a respective class denomination in the form of a data string, and

15 equating said reference data to the class denomination for the selected class.

 2. A method as claimed in claim 1, wherein the step of generating feature values further comprises the steps of:

20 defining a starting point in said current biometric data,

 dividing, starting from the starting point, said current biometric data into at least one data subset, and processing said current biometric data for generating at
25 least one feature value for each data subset.

 3. A method as claimed in claim 2, wherein the step of processing said current biometric data comprises the steps of applying an algorithm to said current biometric data.

30 4. A method as claimed in claim 2 or 3, wherein said current biometric data is a two-dimensional representation of an individual-specific characteristic.

 5. A method as claimed in any one of claims 2-4, wherein the step of processing said current biometric
35 data further comprises the steps of:

 investigating, in said data subset, the frequency of at least one feature, and

assigning, based on said frequency of each feature, a corresponding feature value.

6. A method as claimed in claim 5, wherein said current biometric data is a two-dimensional representation of a fingerprint and wherein the step of generating feature values further comprises the steps of:

superimposing, starting from said starting point (S), a polygon (51) on the two-dimensional representation,

counting the number of fingerprint ridges cutting the respective sides (52-55) of the polygon, and

generating, for each of the sides (52-55) of the polygon (51), a feature value corresponding to the associated number of fingerprint ridges.

7. A method as claimed in claim 4, wherein the step of dividing said current biometric data further comprises the steps of:

arranging, in said two-dimensional representation, concentric circles (41) around said starting point (S) and lines (42) which extend from said starting point (S) and which each cut every circle (41) once, thereby dividing said current biometric data into said data subsets.

8. A method as claimed in claim 7, wherein one or more filters are applied to said data subsets for generating at least one feature value for each data subset.

9. A method as claimed in any one of claims 1-3, wherein said current biometric data is a two-dimensional representation of an individual-specific characteristic and wherein said step of generating feature values further comprises the steps of:

comparing a number of target images (65-68) with said two-dimensional representation and generating a respective correlation value, and

generating for each target image (65-68) a feature value, which corresponds to said respective correlation value.

10. A method as claimed in any one of the preceding claims, wherein said classes are defined on the basis of feature values which represent the quantity, belonging to the associated class, of biometric data collected in advance.

11. A method as claimed in any one of the preceding claims, wherein the selection of class comprises the steps of:

letting the feature values for said current biometric data constitute coordinates,
combining the coordinates,
letting the combined coordinates define a current dot (35) in a space (31), which is divided into subspaces (33), which correspond to said classes and the associated class denominations, and
determining to which subspace (33) the current dot (35) belongs and, thus, to which class said current biometric data belongs.

12. A method as claimed in claim 11, wherein said subspaces (33) mutually correspond essentially to the same amount of biometric data collected in advance.

13. A method as claimed in claim 11 or 12, wherein each subspace (33) is at least represented by an attraction point (34) in said space (31).

14. A method as claimed in any one of claims 11-13, wherein the division of said space (31) occurs by a respective attraction point (34) being assigned to each subspace (33) in such manner that the sum of the distances between said attraction point (34) and data dots (32), which represent said quantity of biometric data collected in advance and which are adapted to be comprised by the subspace (33), is minimized.

15. A method as claimed in any one of claims 11-14 wherein the selection of class further comprises the steps of:

determining, for each of said subspaces (33), a distance (D) between the current dot (35) and the associated attraction point (34), and

5 selecting the class which corresponds to the subspace (33) to the attraction point (34) of which said distance (D) is smallest.

16. A method as claimed in claim 11 or 12, wherein the selection of class further comprises the steps of:

10 comparing the coordinates for the current dot (35) with coordinates for a boundary surface (36) of each subspace (33), and

selecting the class corresponding to the subspace (33) within which the current dot (35) is located.

15 17. A method as claimed in any one of the preceding claims, wherein each of said class denominations comprise a combination of characters, preferably figures and/or letters.

20 18. A device which is adapted to generate reference data from current biometric data of an individual, comprising:

a memory means (9), which comprises a set of data dividable into a plurality of classes, which each correspond to a quantity of biometric data of a number of individuals that has been collected in advance, and to
25 each of which a class denomination in the form of a data string is assigned, and

a processing means (10) which is adapted to generate, based on said current biometric data, a number of feature values, to select, on the basis of said
30 feature values, one of said classes, and to equate said reference data to the class denomination of the selected class.

19. A device as claimed in claim 18, wherein the processing means (10) is designed to define a starting
35 point (S) in said current biometric data, to divide, starting from the starting point (S), said current biometric data into at least one data subset, and to process

said current biometric data for generating at least one feature value for each data subset.

20. A device as claimed in claim 19, wherein the processing means (10) is designed to apply an algorithm
5 to said current biometric data.

21. A device as claimed in claim 19 or 20, wherein said current biometric data is a two-dimensional representation of an individual-specific characteristic.

22. A device as claimed in any one of claims 18-21,
10 wherein the set of data in the memory means (9) is dividable into said classes starting from feature values representing the quantity, belonging to the associated class, of biometric data collected in advance.

23. A device as claimed in any one of claims 18-22,
15 wherein the processing means (10) is designed to let the feature values of said current biometric data constitute coordinates, to combine the coordinates, to let the combined coordinates define a current dot (35) in a space (31), which is dividable into subspaces (33), which
20 correspond to said classes and the associated class denominations, and to decide to which subspace (33) the current dot (35) belongs and, thus, to which class said current biometric data belongs.

24. A device as claimed in claim 23, wherein the set
25 of data in the memory means (9) is dividable into said subspaces (33) in such manner that said subspaces mutually correspond to essentially the same amount of biometric data collected in advance.

25. A device as claimed in claim 23 or 24, wherein
30 the set of data in the memory means (9) is dividable into said subspaces (33), each of the subspaces (33) at least being represented by an attraction point (34) in said space (31).

26. A device as claimed in any one of claims 23-25,
35 wherein said attraction point (34) is assigned to the associated subspace (33) in such manner that the sum of the distances between said attraction point (34) and data

dots (32), which represent said quantity of biometric data collected in advance and which are adapted to be comprised by the subspace (33), is minimized.

27. A device as claimed in any one of claims 23-26,
5 wherein the processing means (10) is designed to determine for each of said subspaces (33) a distance (D) between the current dot (35) and the associated attraction point (34), and to select the class corresponding to the subspace (33) to whose attraction point (34) said
10 distance (D) is smallest.

28. A device as claimed in claim 23 or 24, wherein the processing means (10) is designed to compare the coordinates for the current dot (35) with coordinates for a boundary surface (36) of each subspace (33), and to
15 select the class corresponding to the subspace (33) within which the current dot (35) is located.

29. A device as claimed in any one of claims 18-28, wherein the processing means (10) is designed to form each class denomination as a combination of characters,
20 preferably figures and/or letters.

30. A method of checking, based on current biometric data of an individual, the right to access to sensitive information, comprising the steps of:

collecting said current biometric data,
25 generating, starting from said current biometric data, first reference data by a method as claimed in any one of claims 1-17,

comparing said first reference data with second reference data which is stored on a data carrier (1), and
30 giving, in case of correspondence between said first and second reference data, the individual the right to access to the sensitive information.

31. A method as claimed in claim 30, further comprising the step of determining which operations which
35 the individual having the right to access is allowed to perform on the sensitive information in case of correspondence between said first and second reference data.

32. A method as claimed in claim 30 or 31, wherein the step of comparing said first reference data with said second reference data comprises the step of comparing two combinations of characters, preferably figures and/or letters.

33. A method as claimed in any one of claims 30-32, wherein said current biometric data is a fingerprint.

34. A method as claimed in any one of claims 30-33, wherein the sensitive information is stored on the portable data carrier (1).

35. A method as claimed in any one of claims 30-34, wherein said comparison occurs on said data carrier (1).

36. A method as claimed in any one of claims 30-35, wherein said generation of reference data occurs in a processing means (10) separated from the data carrier (1), and that said first reference data is transferred from the processing means (10) to the data carrier (1) before said comparison.

37. A system for checking the right to access to sensitive information, said check being based on current biometric data of an individual whose right to access to the sensitive information is to be checked, wherein the system comprises:

a portable data carrier (1) comprising a memory means (3) which contains the sensitive information, a signal processing device (4) and a communication device (5), and

a processing unit (2), which is adapted to receive said current biometric data of the individual and which comprises a communication device (7) and a signal processing device (6) according to any one of claims 18-29,

wherein the processing unit (2) is adapted to generate by means of the signal processing device (6) current reference data from said current biometric data, to transfer said current reference data to the signal

processing device (4) of the data carrier (1) via the communication devices (5,7), and

wherein the signal processing device (4) of the data carrier (1) is adapted to compare said current reference data with reference data stored in advance in the memory means (3) of the data carrier (1) to determine whether the right to access to the sensitive information exists.

38. A system as claimed in claim 37, wherein said current biometric data is a two-dimensional representation of an individual-specific characteristic.

39. A system as claimed in claim 38, wherein said two-dimensional representation is a digital image.

40. A system as claimed in any one of claims 37-39, wherein the signal processing device (4) of the data carrier (1) is further designed to determine, in case of correspondence between said current reference data and said reference data stored in advance, which operations the processing unit (2) is allowed to perform on the sensitive information.

41. A system as claimed in any one of claims 37-40, wherein said current biometric data is a fingerprint.

42. A system as claimed in claim 41, wherein the memory means (3) of the data carrier (1) further contains reference data, stored in advance, of a fingerprint.

43. A system as claimed in any one of claims 37-42, wherein the data carrier (1) is a smart card.

44. A processing unit for checking the right to access to sensitive information stored on a portable data carrier (1), said checking being based on current biometric data of an individual, wherein the processing unit (2) comprises a communication device (7) and a signal processing device (6) according to any one of claims 18-29, the processing unit (2) being adapted to generate, by means of the signal processing device (6), current reference data from said current biometric data, and to transfer said current reference data to the signal pro-

cessing device (4) of the data carrier (1) via the communication devices (5, 7).

45. A processing unit as claimed in claim 44, wherein the signal processing device (6) is further designed
5 to perform operations on the sensitive information, based on rights which are assigned to the processing unit (2) by the data carrier (1).

46. A processing unit as claimed in claim 44 or 45, wherein the processing unit (2) is further provided with
10 a sensor (8) for collecting said current biometric data of the individual.

47. A processing unit as claimed in claim 46, wherein said current biometric data is a digital image.

48. A method for checking whether current biometric
15 data of an individual is represented in a database containing items, each item corresponding to biometric data of an individual and being assigned an item denomination, said method comprising the steps of:

generating, based on said current biometric data, a
20 number of current feature values,

selecting, based on said current feature values, one of a plurality of classes, each class corresponding to a quantity of biometric data, collected in advance, of a number of individuals, and having a class denomination,
25 and

comparing said current biometric data with biometric data associated with at least one item being assigned an item denomination that corresponds to the class denomination of the selected class.

49. A method as claimed in claim 48, wherein the step of comparing comprises comparing the current feature values with a combination of feature values associated with said at least one item.

50. A method as claimed in claim 48 or 49, wherein
35 the step of generating current feature values further comprises the steps of:

defining a starting point (S) in said current biometric data,

dividing, starting from the starting point (S), said current biometric data into at least one data subset, and
5 processing said current biometric data for generating at least one feature value for each data subset.

51. A method as claimed in claim 50, wherein the step of processing said current biometric data comprises the step of applying an algorithm to said current biometric data.
10

52. A method as claimed in claim 50 or 51, wherein the step of processing said current biometric data further comprises the steps of:

investigating in said data subset the frequency of
15 at least one feature, and

assigning, based on said frequency of each feature, a corresponding feature value.

53. A method as claimed in claim 52, wherein said current biometric data is a two-dimensional representation of a fingerprint and wherein the step of generating feature values further comprises the steps of:

superimposing, starting from said starting point (S), a polygon (51) on the two-dimensional representation,
25 counting the number of fingerprint ridges intersecting the respective sides (52-55) of the polygon (51), and
generating, for each of the sides (52-55) of the polygon (51), a feature value which corresponds to the associated number of fingerprint ridges.

54. A method as claimed in any one of claims 48-53, wherein said current biometric data is a two-dimensional representation of an individual-specific characteristic.

55. A method as claimed in claim 54, wherein the step of dividing said current biometric data further
35 comprises the step of arranging in said two-dimensional representation concentric circles (41) around said starting point (S) and lines (42), which extend from said

starting point (S) and which each cut every circle (41) once, thereby dividing said current biometric data into said data subsets (43).

56. A method as claimed in claim 55, wherein one or
5 more filters are applied to said data subsets (43) for generating at least one feature value for each data subset (43).

57. A method as claimed in any one of claims 48-51,
wherein said current biometric data is a two-dimensional
10 representation of an individual-specific characteristic, and wherein the step of generating current feature values further comprises the steps of:

comparing a number of target images (65-68) with
said two-dimensional representation and generating an
15 associated correlation value, and

generating, for each target image (65-68), a feature
value which corresponds to said associated correlation
value.

58. A method as claimed in any one of claims 48-57,
20 wherein said classes are defined on the basis of feature values which represent the quantity, belonging to each class, of biometric data collected in advance.

59. A method as claimed in any one of claims 48-58,
wherein the selection of class comprises the steps of:
25 letting the current feature values form coordinates,
combining the coordinates,
letting the combined coordinates define a current
dot (35) in a space (31), which is divided into subspaces
(33) which correspond to said classes and the associated
30 class denominations, and
determining to which subspace (33) the current dot
(35) belongs and, thus, to which class said current bio-
metric data belongs.

60. A method as claimed in claim 59, wherein said
35 subspaces (33) mutually correspond to essentially the same quantity of biometric data collected in advance.

61. A method as claimed in claim 59 or 60, wherein each subspace (33) is at least represented by an attraction point (34) in said space (31).

62. A method as claimed in any one of claims 59-61,
5 wherein the division of said space (31) occurs by an attraction point (34) being assigned to each subspace (33) in such manner that the sum of the distances between said attraction point (34) and data dots (32) which represent said quantity of biometric data collected in
10 advance and which are adapted to be comprised by the subspace (33), is minimized.

63. A method as claimed in any one of claims 59-62, wherein the selection of class further comprises the steps of:

15 determining for each of said subspaces (33) a distance (D) between the current dot (35) and the associated attraction point (34), and

selecting the class corresponding the subspace (33) to whose attraction point (34) said distance (D) is
20 smallest.

64. A method as claimed in claim 59 or 60, wherein the selection of class further comprises the steps of:

comparing the coordinates for the current dot (35) with coordinates for a boundary surface (36) of each
25 subspace (33), and

selecting the class which corresponds to the subspace (33) within which the current dot (35) is located.

65. A method as claimed in any one of claims 48-64, wherein each of said class denominations is a combination
30 of characters, preferably figures and/or letters.

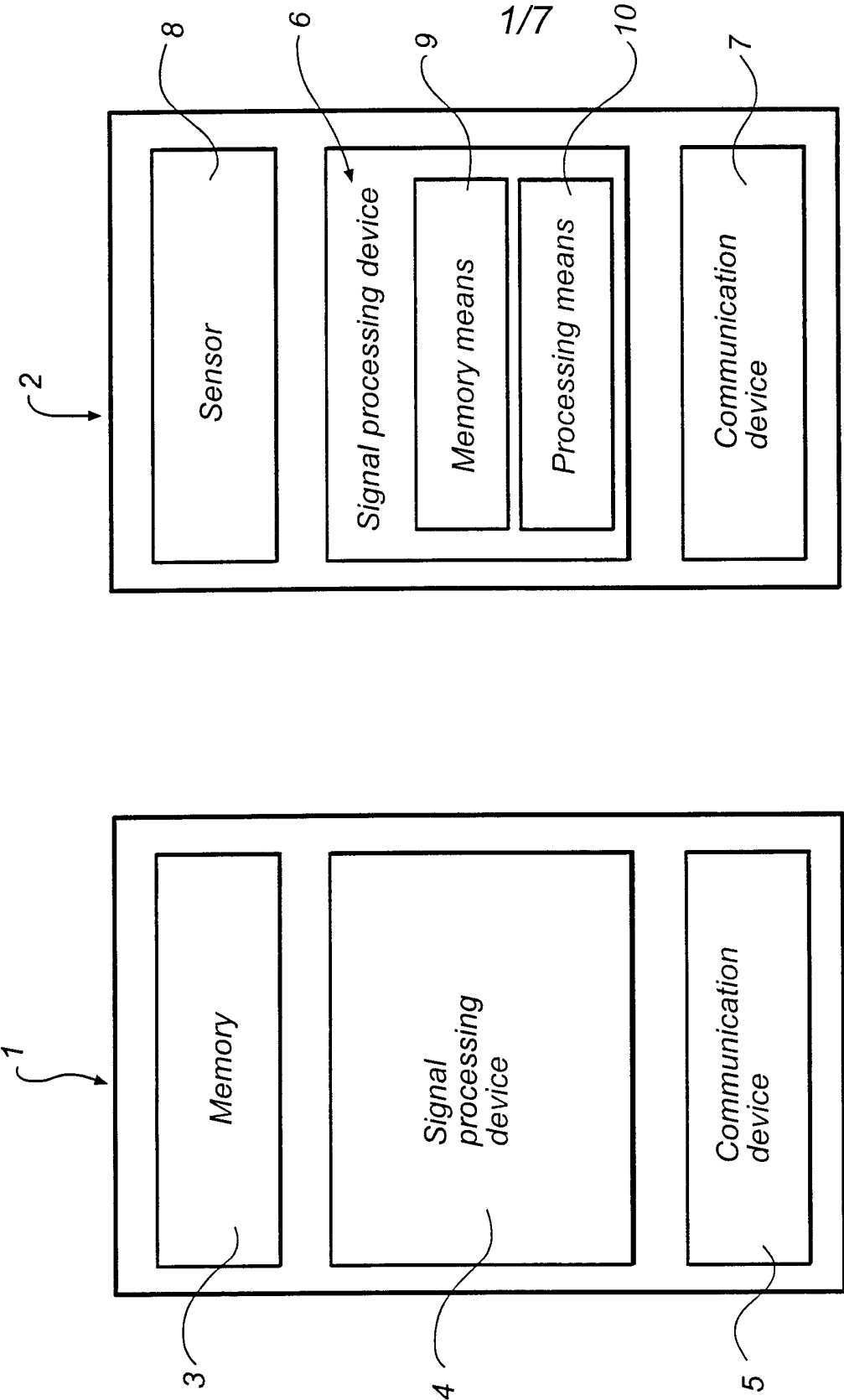
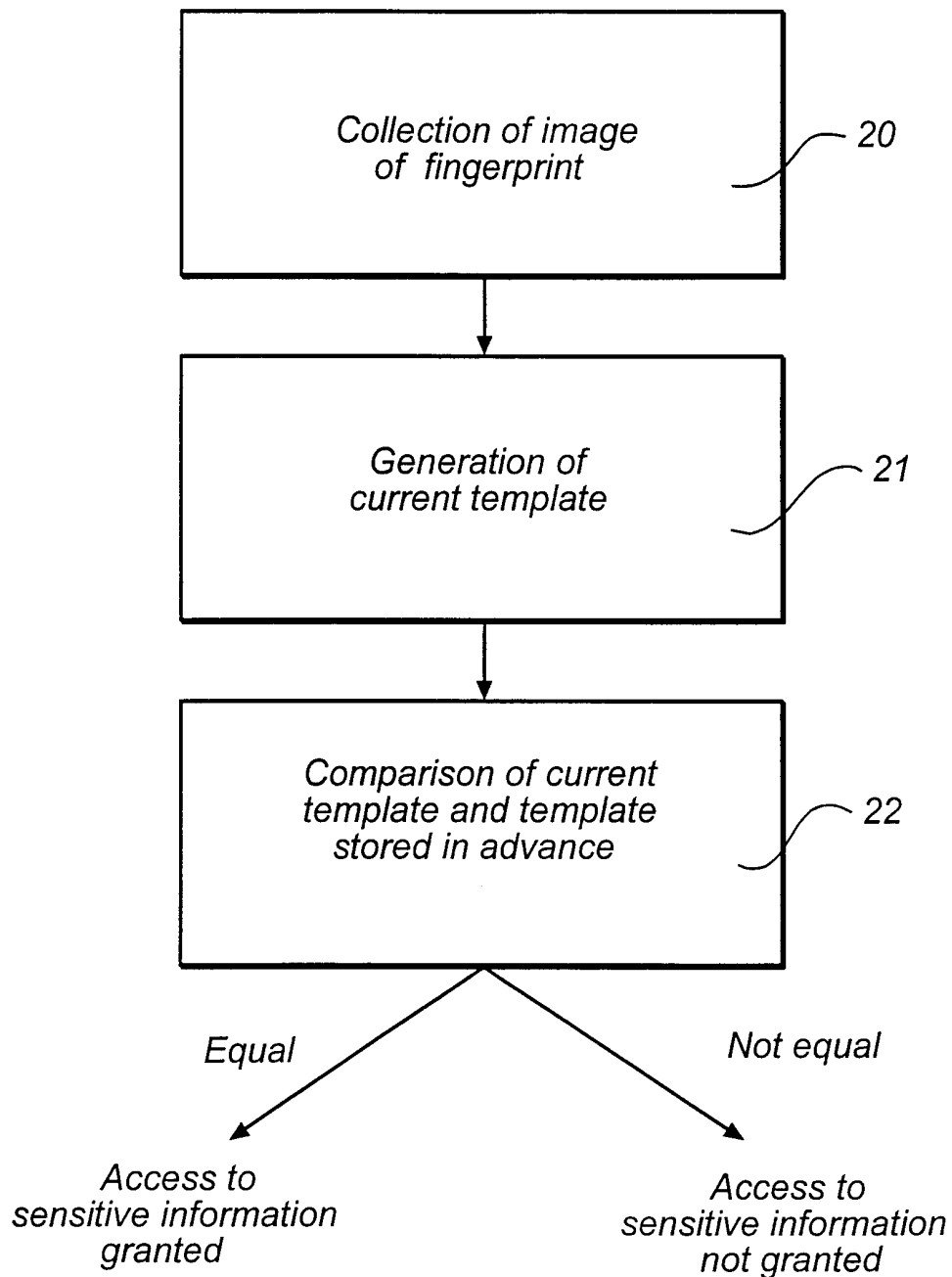


Fig. 1

2/7

*Fig. 2*

3/7

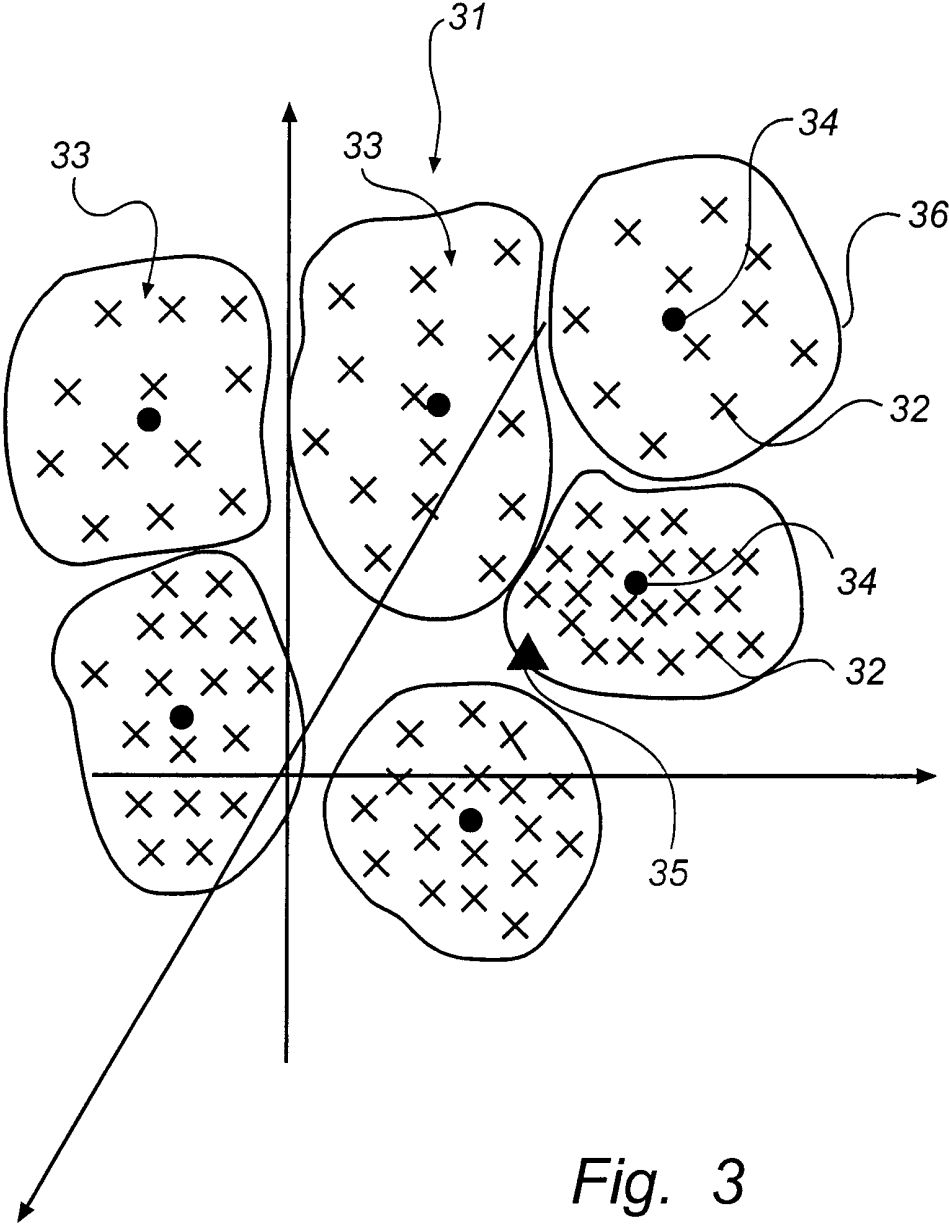


Fig. 3

4/7

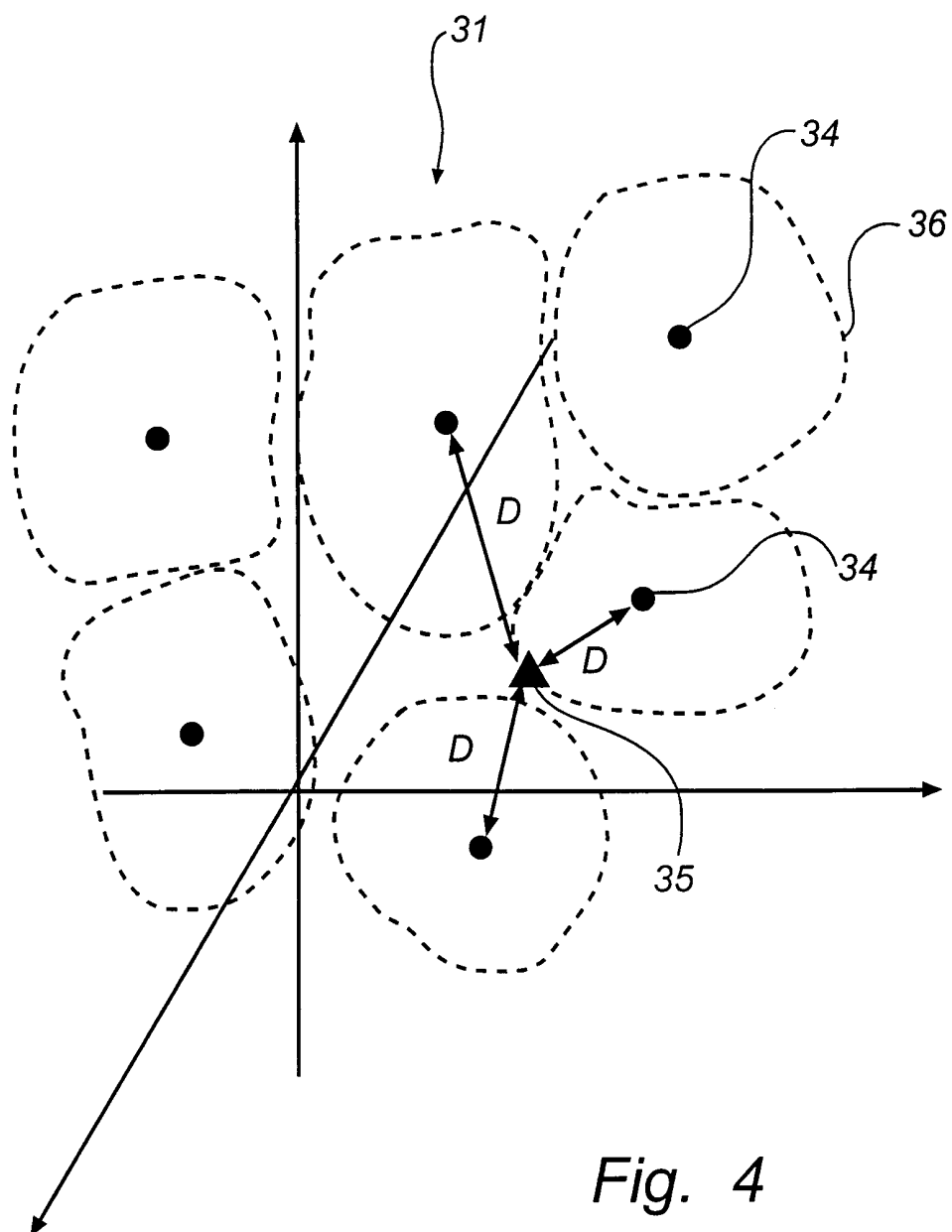


Fig. 4

5/7

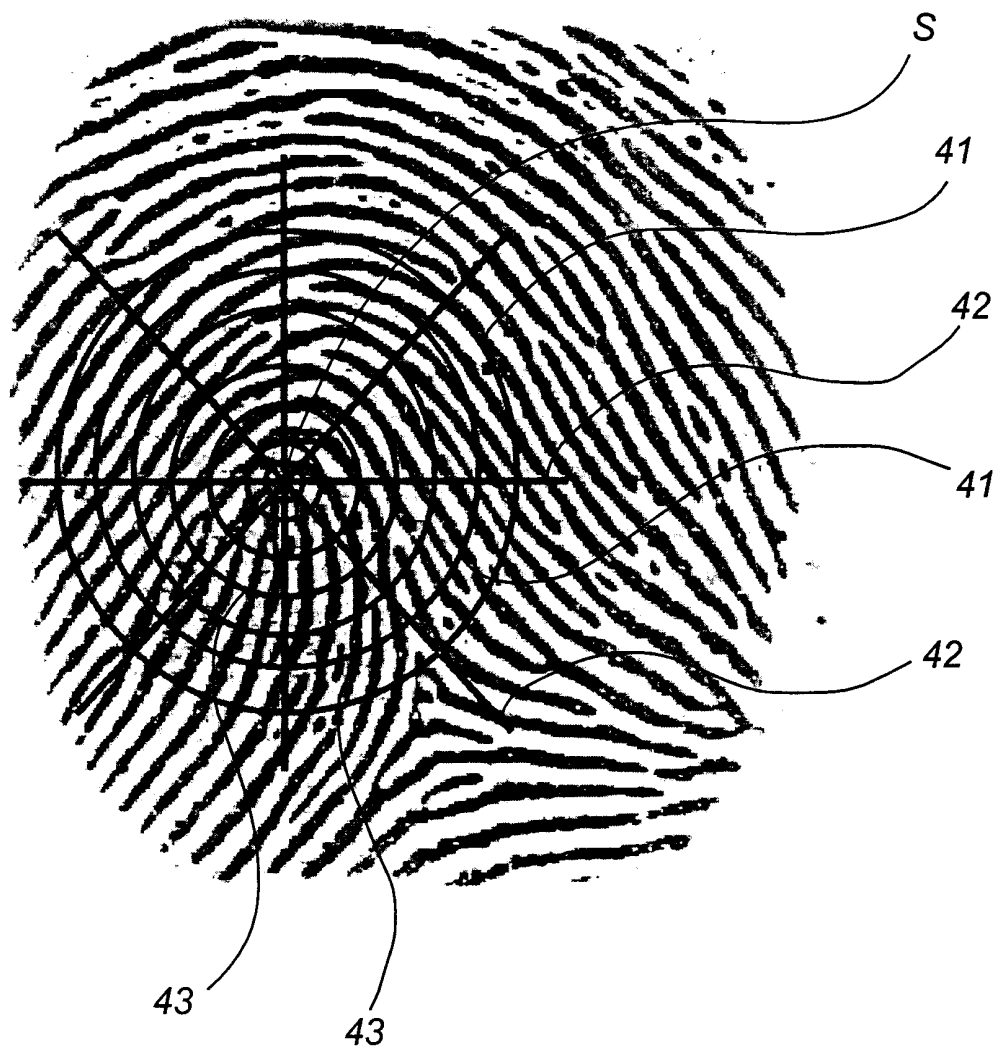


Fig. 5

6/7

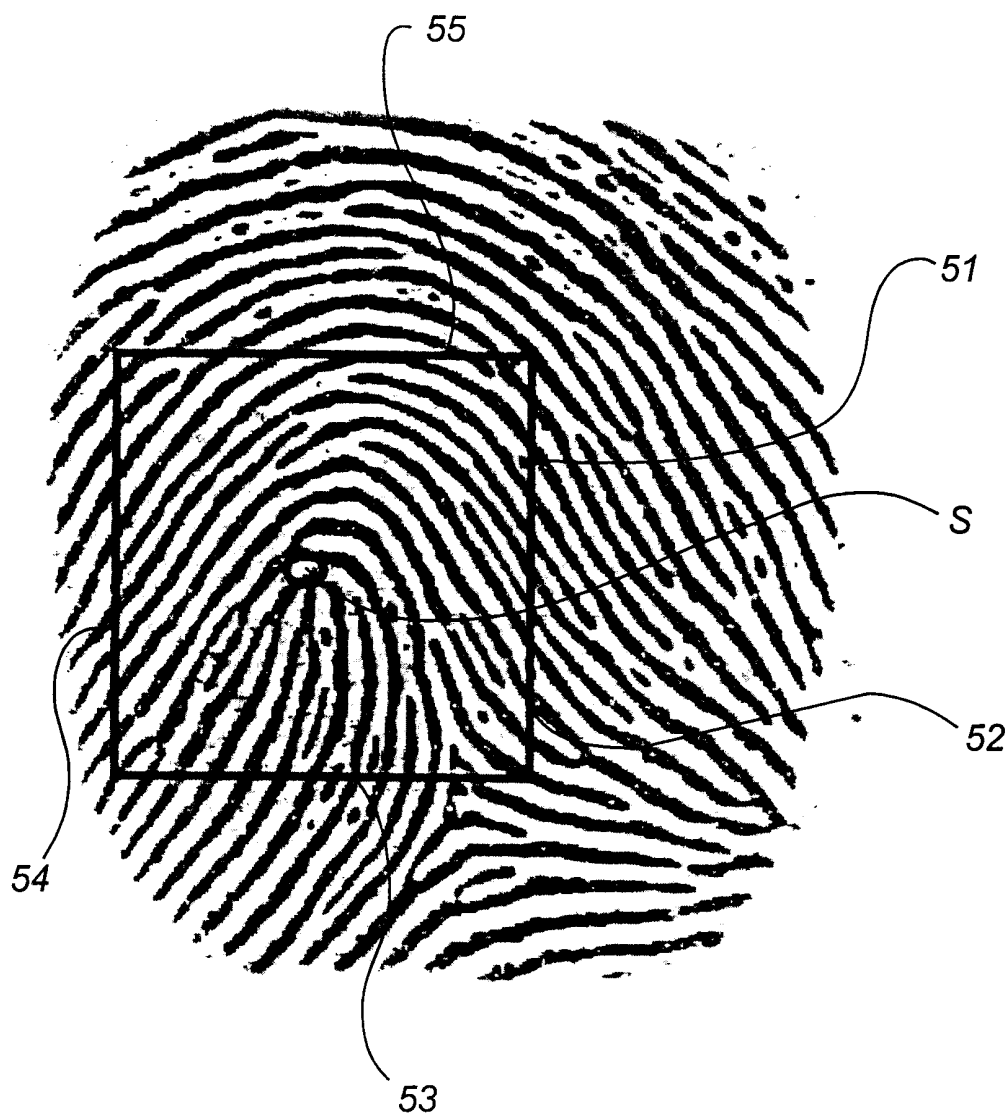
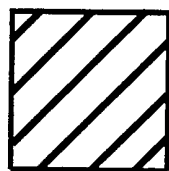


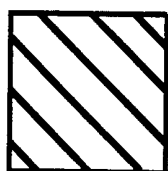
Fig. 6



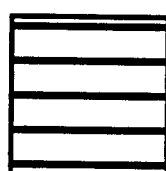
Fig. 7



65



66



67



68

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 00/01997

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: A61B 5/117, G06K 9/50, G06K 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: A61B, G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5509083 A (N.S. ABTHAI ET AL), 16 April 1996 (16.04.96), column 5, line 55 - column 11, line 58, figure 3, claims 1,16 --	1-5,9-10, 17-22,29-53, 57-58,65
A	WO 9513592 A1 (AEROFLEX SYSTEMS CORPORATION), 18 May 1995 (18.05.95), figures 1,7, abstract --	1-65
A	EP 0779595 A2 (NEC CORPORATION), 18 June 1997 (18.06.97), figure 1, abstract -- -----	1-65

☐ Further documents are listed in the continuation of Box C.
 ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

29 January 2001

Date of mailing of the international search report

31 -01- 2001

Name and mailing address of the ISA/

Swedish Patent Office
Box 5055, S-102 42 STOCKHOLM
Facsimile No. +46 8 666 02 86

Authorized officer

Patrik Blidefalk/mj
Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

27/12/00

International application No.

PCT/SE 00/01997

Patent document cited in search report			Publication date	Patent family member(s)	Publication date
US	5509083	A	16/04/96	NONE	
WO	9513592	A1	18/05/95	US	5465303 A 07/11/95
EP	0779595	A2	18/06/97	DE	69610689 D 00/00/00
				JP	2737734 B 08/04/98
				JP	9161054 A 20/06/97
				US	5974163 A 26/10/99