



(11) (21) (C) **2,085,113**
(86) 1991/06/14
(87) 1991/12/16
(45) 2001/03/06

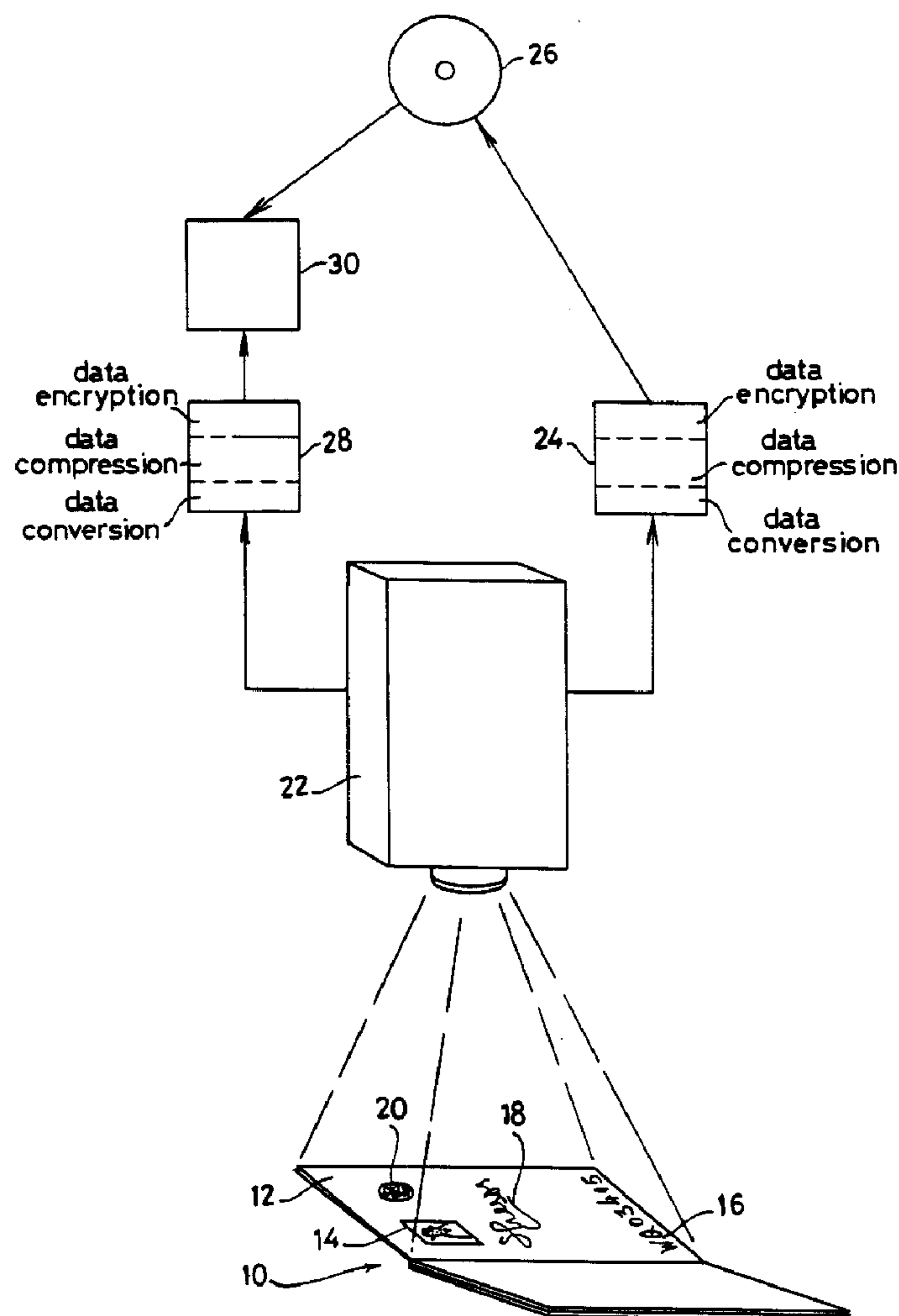
(72) Tel, Teunis, NL
(72) Tel, Teunis, NL
(73) Unicate B.V., NL

(51) Int.Cl.⁵ B42D 15/10

(30) 1990/06/15 (9001368) NL

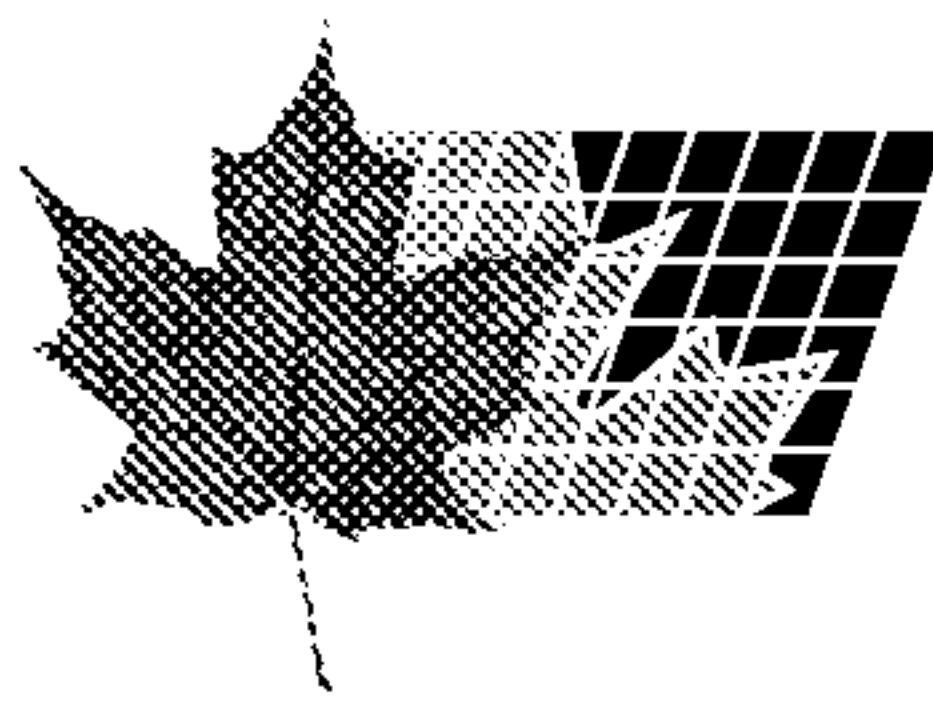
(54) **PROTECTION D'OBJETS OU DE DOCUMENTS**

(54) **SECURITY OF OBJECTS OR DOCUMENTS**



(57) Objet ou document (10) protégé contre toute utilisation frauduleuse, système de protection dudit objet ou document (10) contre l'utilisation frauduleuse et procédé visant à mettre en circulation publique et à vérifier ledit objet ou document (10), lequel comporte au moins une marque d'identification (14, 16, 18) et au moins une configuration enfermée (20) de fibres (2) qui

(57) An object or document (10) secured against fraud, a system for securing said object or document (10) against fraud, and a method of putting into public circulation and checking said object or document (10) which is provided with at least one identifying mark (14, 16, 18) and at least one confined pattern (20) of fibres (2) which is incorporated in a surface (12) of the object or document,



(11) (21) (C) **2,085,113**
(86) 1991/06/14
(87) 1991/12/16
(45) 2001/03/06

est incorporée dans une surface (12) de l'objet ou du document, les fibres étant fixées de manière arbitraire les unes par rapport aux autres et par rapport à la surface. La configuration se compose d'un morceau de matériau non-tissé encastré dans un matériau transparent en-deçà des bords de la surface. Le système comprend un élément de balayage (22) servant à balayer optiquement la configuration entière (20) à un certain angle par rapport à la surface dans laquelle elle est incorporée; un élément de balayage (22) servant à balayer optiquement une ou plusieurs marque(s) d'identification (14, 16, 18) sur l'objet ou le document (10); un élément de conversion (24, 28) destiné à convertir l'information optique obtenue à partir de l'élément de balayage (22) en données numériques, et vice versa; un élément de compression de données (24, 28) servant à convertir le nombre original de données numériques en un nombre réduit de données numériques équivalentes et vice versa; un élément de mémorisation (26) destiné à mémoriser le nombre réduit de données numériques dans une mémoire ROM; un élément de comparaison servant à comparer les données obtenues par l'élément de balayage (22), l'élément de conversion (24, 28) et l'élément de compression de données (24, 28) se rapportant à un objet ou un document (10), avec des données précédemment mémorisées par l'élément de mémorisation (26); le système peut aussi comprendre un élément de codage de données (24, 28) servant à convertir le nombre réduit de données numériques en données numériques codées et vice versa.

the fibres being fixed in an arbitrary manner relative to each other and the surface. The pattern is made up of a piece of nonwoven material embedded in a transparent material within the boundaries of the surface. The system comprises scanning means (22) for optically scanning the entire pattern (20) at an angle relative to the surface (12) in which it is incorporated; scanning means (22) for optically scanning one or more additional identifying marks (14, 16, 18) of the object or document (10); converting means (24, 28) for converting the optical information obtained by the scanning means (22) into digital data, vice versa; data compressing means (24, 28) for converting the original quantity of digital data into a reduced quantity of equivalent digital data, vice versa; storage means (26) for recording the reduced quantity of digital data in a read-only memory; comparing means for comparing the data obtained with the scanning means (22), the converting means (24, 28) and the data compressing means (24, 28) concerning an object or a document (10) with data previously recorded in the storage means (26) and can comprise data encryption means (24, 28) for converting the reduced quantity of digital data into coded digital data, vice versa.



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁵ :

B42D 15/10

2085113

A1

(11) International Publication Number:

WO 91/19614

(43) International Publication Date:

26 December 1991 (26.12.91)

(21) International Application Number: PCT/NL91/00098

(22) International Filing Date: 14 June 1991 (14.06.91)

(30) Priority data:

9001368

15 June 1990 (15.06.90)

NL

(71) Applicant (for all designated States except US): TEL-DEVELOPMENTS B.V. [NL/NL]; Verlengde Hereweg 192, NL-9722 AM Groningen (NL).

(72) Inventor; and

(75) Inventor/Applicant (for US only): TEL, Teunis [NL/NL]; Verlengde Hereweg 192, NL-9722 AM Groningen (NL).

(74) Agent: TIMMERS, C., H., J.; Exterpatent B.V., P.O. Box 90649, NL-2509 LP The Hague (NL).

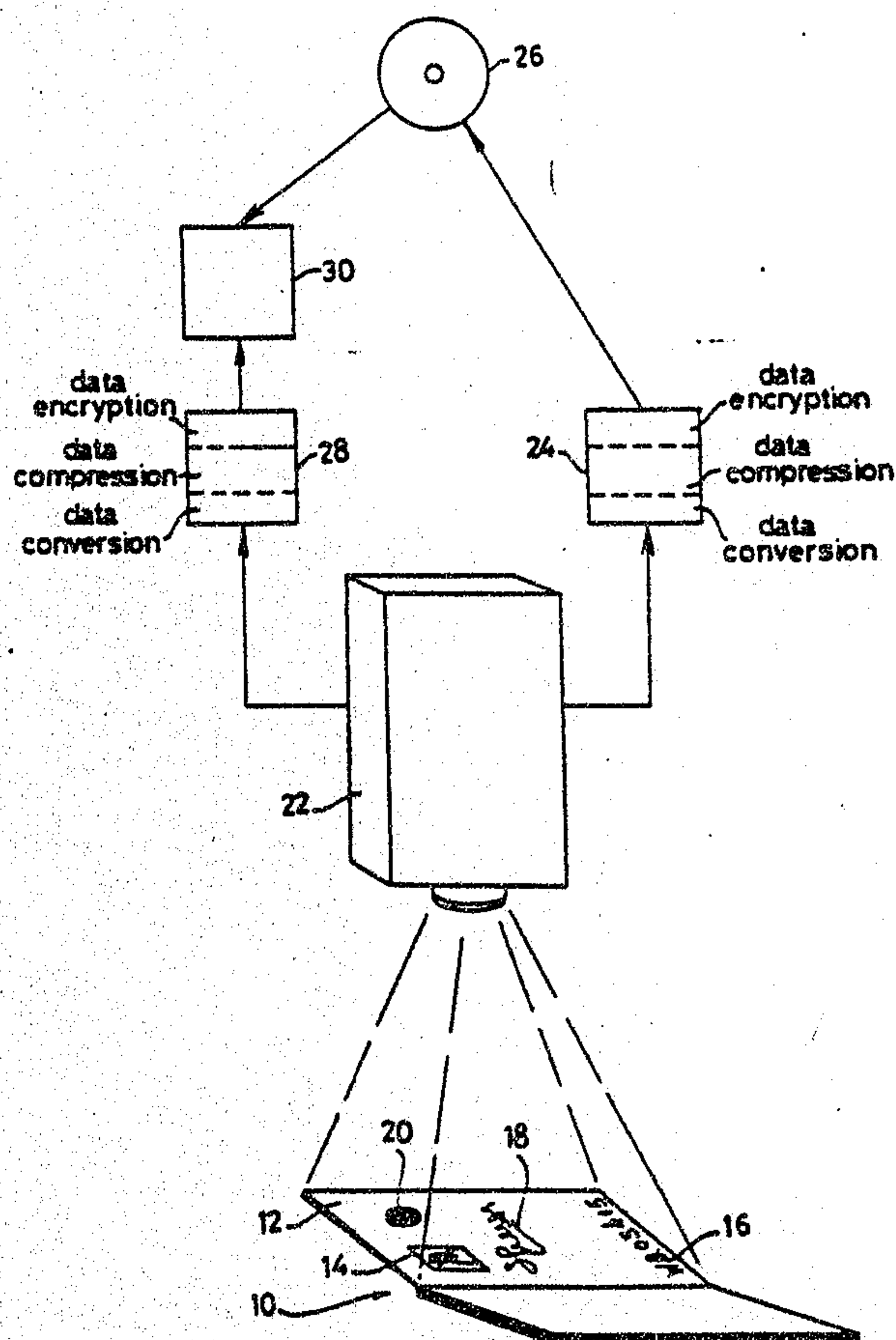
(81) Designated States: AT (European patent), BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent), US.

Published*With international search report.**Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

(54) Title: SECURITY OF OBJECTS OR DOCUMENTS

(57) Abstract

An object or document (10) secured against fraud, a system for securing said object or document (10) against fraud, and a method of putting into public circulation and checking said object or document (10) which is provided with at least one identifying mark (14, 16, 18) and at least one confined pattern (20) of fibres (2) which is incorporated in a surface (12) of the object or document, the fibres being fixed in an arbitrary manner relative to each other and the surface. The pattern is made up of a piece of nonwoven material embedded in a transparent material within the boundaries of the surface. The system comprises scanning means (22) for optically scanning the entire pattern (20) at an angle relative to the surface (12) in which it is incorporated; scanning means (22) for optically scanning one or more additional identifying marks (14, 16, 18) of the object or document (10); converting means (24, 28) for converting the optical information obtained by the scanning means (22) into digital data, vice versa; data compressing means (24, 28) for converting the original quantity of digital data into a reduced quantity of equivalent digital data, vice versa; storage means (26) for recording the reduced quantity of digital data in a read-only memory; comparing means for comparing the data obtained with the scanning means (22), the converting means (24, 28) and the data compressing means (24, 28) concerning an object or a document (10) with data previously recorded in the storage means (26); and can comprise data encryption means (24, 28) for converting the reduced quantity of digital data into coded digital data, vice versa.



2085113

1

Security of objects or documents.

The invention relates to an object or document secured against fraud. The invention also relates to a system for securing said object or document against fraud and to a method of putting into public circulation and
5 checking said object or document.

An object or document of the above-mentioned type can be, for example, a passport, a banker's card, a credit card, a security such as a banknote, a cheque or a share certificate, a product label, a travel card such as an
10 airline ticket, or an admission ticket, but it can also be a painting, a compact disc, a music-, photo-, film- or video cassette, or a car.

If, by way of example, a passport is considered, it is provided with identifying marks with the object of
15 safeguarding use of the document by making it unique and confined to one person. These identifying marks can comprise a specific layout of the document, a person's name, a passport photograph, an alphanumeric code, signatures, stamps and the like.

20 Another example of a document is a banknote, in the case of which efforts are made to counteract forgery by providing a watermark and other identifying marks which are difficult to copy, and also a unique serial number.

Some of the provided identifying marks are generally
25 applied by means of very advanced equipment and techniques - in particular in the case of banknotes - in order to minimise the chance of illegal duplication of the documents. The price which has to be paid for these security measures is consequently high.

30 However, none of the above-mentioned measures provides adequate protection against the forgery of individual objects or documents, since in the first place the identifying marks can be copied with little or great

2085113

2

effort. Further, when a passport is being checked the passport number or the person's name specified are used to check in a data file whether the passport number and the person's name exist and go together. This check does not, however, rule out the possibility that the person using the passport could be a different person from the one to whom the passport belongs, a fraud which can remain unnoticed through, for example, an indiscernible change of the passport photograph in the passport. It is also possible for the document itself to have been forged in such a way that this is not noticed by the authority checking it.

Secondly, a check on a specific combination of identifying marks is often impossible in practice. As already described above, it cannot be ruled out in the case of, for example, a passport that the document itself has been forged or that one of the identifying marks placed on it, such as a passport photograph, does not form a unit with the other identifying marks with which it is provided. The reason for this is that the data file forming the reference for the check contains purely alphanumeric information such as names and numbers and does not have any graphic information relating to, for example, the picture on a passport photograph or a signature.

Besides, it is generally not possible to check whether a specific object or document is genuine by means of a data file, but only by a human or mechanical assessment of a number of identifying marks of the object or document which are the same for all objects or documents, such as a line pattern, a colour, a watermark or the like.

From US-A-4 218 674 a system comprising an object, in particular a document, secured against fraud is known, which object is provided with random imperfections consisting of fibers of a magnetic or magnetizable material which can be detected when measuring along a predetermined measuring track on the object. The measured imperfections are converted into a row of electric pulses and synchronised with a timing pulse also derived from marks on the object.

Such a security system obviously does not function properly when the object has been subjected to external magnetic fields and therefore is of limited practical value. Besides, only a track is scanned, which provides only a limited
5 quantity of security data for securing the object.

In the known method, the obtained security data are not combined with any data related to possible identifying marks on the object, and although the authenticity of the object can be shown by proving by way of comparison with
10 previously recorded security data the authenticity of the security data obtained from the object, this provides no proof whatsoever of the identity of the user of the object without further precautions being taken.

Another disadvantage of the known system resides in
15 the fact that no measures are taken to reduce the obtained quantity of security data to a more compressed form. Consequently, a relatively large storage capacity of a computer is used and a relatively long processing time will be necessary to compare a read security code with a large
20 number of previously stored codes.

Last but not least, for an expert forger in the field of electronics and computers it does not present many problems to prepare a forged document which will produce a valid security codes and visually cannot be distinguished
25 from an authentic one. This could be accomplished, by example, by breaking into the computer where a list of security codes is stored, by tapping the electrical connection between a measuring station and said computer, or by analysis of the magnetic properties of an authentic
30 document.

The object of the invention is in the first place to provide an object or document which is provided with a unique mark which cannot be copied. The object or document, which is provided with at least one identifying mark and at
35 least one confined pattern of fibres which is incorporated in a surface of the object or document, the fibres being fixed in an arbitrary manner relative to each other and the

provide an object or document which is provided with a unique mark which cannot be copied.

Thus, according to a first aspect of the invention, there is provided a product having provision for verifying the legitimacy of the product against forgery and comprising a body member including a surface, a plurality of overlying individual fibers which are randomly disposed so as to define a number of differing geometrical configurations, and a transparent base material completely encasing and fixedly supporting said fibers so that said fibers are visible on said surface and such that said surface is optically scannable through the transparent base material so as to permit the geometrical configurations of the fibers to be scanned.

Thus, the object or document, is provided with at least one identifying mark and at least one confined pattern of fibers which is incorporated in a surface of the object or document, the fibers being fixed in an arbitrary manner relative to each other and the surface. The identifying mark is preferably characterized by a pattern (geometrical configurations) made up of a piece on nonwoven material embedded in a transparent material filling the space round said fibers, the geometrical properties of the individual fibers of the pattern being optically scannable from the side of said surface and being used for the security of said object or document against fraud.

If the pattern, in which many parts of fibers constituting the nonwoven material lie arbitrarily directed, is incorporated in a surface of an object or document, the latter is provided with a unique mark, which cannot be copied. The object or document is thus itself made unique and impossible to forge; the pattern forms, as it were, the fingerprint of the object or document. For a definition of nonwovens reference is

made here to international standard ISO 9092.

Great advantages of the use of nonwovens are their low thickness, the very low mass per unit volume, and the low cost.

The transparent material in which the nonwoven material is embedded can, in thin objects or parts thereof, take the form of a window where the pattern is visible both from the front and the back side.

The unique pattern must be constant in all circumstances of use, such as varying ambient temperature, humidity, mechanical stress, chemical, electric and magnetic influences and the like. It has been found that a particularly stable pattern is obtained if the core of the fibers is of polyester, and is surrounded by a polyamide covering.

The invention also provides a system for securing the object or document according to the invention. Thus, according to a second aspect of the invention, there is provided a system for verifying the legitimacy of a product against forgery and comprising a body member including a surface, a plurality of overlying individual fibers which are randomly disposed so as to define a number of differing geometrical configurations, and a transparent base material completely encasing and fixedly supporting said fibers so that said fibers are visible on said surface, scanning means for optically scanning said surface of said body member, converting means for converting the optical information obtained by said optical scanning means into digital data, and comparing means for comparing the digital data with previously stored information in storage means so as to permit verification of the legitimacy of said product, wherein said converting means includes means for converting the optical data into digital data representative of the geometrical configurations formed by the overlying fibers.

Optionally, the system may comprise, as is known from EP-B-0 054 071: scanning means for optically scanning the entire pattern at an angle relative to the surface in which it is incorporated; scanning means for optically scanning one or more additional identifying marks of the object or document; converting means for converting the optical information obtained by the scanning means into digital data, vice versa; data compressing means for converting the original quantity of digital data into a reduced quantity of equivalent digital data, vice versa; data encryption means for converting the reduced quantity of digital data into coded digital data, vice versa; storage means for recording the reduced quantity of digital data in a read-only memory; and comparing means for comparing the data obtained with the scanning means, the converting means, the data compressing means and the data encryption means concerning an object or a document with data previously recorded in the storage means. According to the invention the converting means are preferably arranged to determine one or more characteristics of a polygon defined by fiber parts of the nonwoven material on the basis of the optical information, and to convert these characteristics into digital data, vice versa.

According to another aspect of the invention, there is provided a method of verifying the legitimacy of a product against forgery, which product comprises a body member including a surface, a plurality of overlying individual fibers which are randomly disposed so as to define a number of differing geometrical configurations, and a transparent base material completely encasing and fixedly supporting said fibers so that said fibers are visible on said surface, the method comprising the steps of optically scanning said surface of said body member and including scanning said fibers, converting the

optical information obtained by said optical scanning step into digital data, and comparing the digital data with previously stored information in storage means so as to permit verification of the legitimacy of said product, wherein the converting step includes converting the optical information into digital data representative of the geometrical configurations formed by the overlying fibers.

According to yet another aspect of the invention, there is provided a method of verifying the legitimacy of a product against forgery, which product comprises a body member including a surface, at least one identifying mark provided on said surface, a plurality of overlying individual fibers which are randomly disposed so as to define a number of differing geometrical configurations, and a transparent base material completely encasing and fixedly supporting said fibers so that said fibers are visible on said surface the method comprising the steps of optically scanning said surface of said body member and including scanning the at least one identifying mark and said fibers at the time of issuance of the product, converting the optical information obtained by said optically scanning step into digital data representative of the geometrical configurations formed by the overlying fibers, and including converting the original quantity of data into a reduced quantity of equivalent data, and then converting the reduced quantity of data into coded digital data, storing the coded digital data in a permanent memory, and thereafter optically scanning said surface of said body member a second time, converting the optical information obtained by said second optically scanning step into digital data representative of the geometrical configuration formed by the overlying fibers, and including converting the original quantity of data into a reduced quantity of equivalent data, and then converting

the reduced quantity of data into coded digital data, and comparing the coded digital data obtained from said second scanning step with the previously stored data in said memory so as to permit verification of the legitimacy of said product.

Optically scanning the pattern enables a noncontact scan wherein only the positions of the fibers play a role and imposing wear on the pattern is avoided. When the entire pattern is scanned and not just a track across the pattern, depending on the resolution with which it takes place, much information is obtained which, as a whole, is quite unique.

The scanning means - e.g. a high resolution camera - scan the pattern at an angle which for practical reasons will be close to or equivalent to 90° , but may also be chosen much less, depending mainly on the angle of refraction of the transparent material.

Apart from the pattern at least one additional identifying mark is scanned. In most cases this mark will be the appearance of the object as a whole, while in the case of an object being an identity card said mark may be a

2085113

6

in a preferred embodiment the system comprises data encryption means for converting the reduced quantity of digital data into coded digital data, vice versa.

To enable a visual check performed by a security person, the system can reassemble the original optical information from the data stored in the memory of the storage means by reverse operation of the converting means, the data compressing means and possibly the data encryption means.

The pattern of nonwoven material comprises several layers and consequently has a three-dimensional structure. It is advantageous to scan this pattern from at least two different angles, because this produces different information which is correlated by the arrangement of the fibres, and which is more unique than the information derived from a single scanning of the pattern.

Advantageously, the converting means are arranged to determine one or more characteristics of a polygon defined by fibre parts of the nonwoven material on the basis of the optical information, and to convert these characteristics into digital data, vice versa.

In a preferred method for putting into public circulation and checking the object or document according to the invention with the system according to the invention, prior to the issue of the object or document, the related reduced quantity of possibly coded data is recorded in the memory of the storage means, which memory is retained at a data keeper, and when the object or document is being checked it is optically information thus obtained is processed by means of the converting means, the data compressing means and possibly the data encryption means, and the resulting data is compared with the data recorded in the memory of the storage means or a copy thereof. The data keeper, an independent person or institute, plays an important role in ensuring the integrity of the data obtained prior to the issue of the object or document, and can provide material evidence that an object being checked is forged or not.

7 2085113

The invention is explained with reference to the drawing, in which:

Fig. 1 shows a first pattern of fibres on a greatly enlarged scale according to the invention; and

5 Fig. 2 illustrates a method according to the invention for issuing and checking a passport.

Fig. 1 shows a part of a large, arbitrary pattern of intersecting fibres 2, which pattern continues in an arbitrary manner towards all sides outside the figure. The
10 fibres 2 are fixed relative to each other. A confined smaller pattern is obtained, for example, by cutting through the fibres 2 along the dashed and dotted line 4. The confined pattern thus formed can be fixed in a surface of an object or document.

15 It should be pointed out here that it is irrelevant for the invention whether or not the fibres are the same thickness as each other, whether or not the fibres are the same thickness over the entire length, whether the fibres are straight or bent, and whether or not they intersect one
20 another.

In Fig. 1 the fibres 2 define many different polygons, two of which are indicated with dashed lines. Thus, a triangle 3 and quadrangle 5 can be recognized, which are characteristic for the specific pattern of nonwoven
25 material. Attributes of such polygons, e.g. angles α , β and γ of triangle 3, may be evaluated and used for characterization of the pattern.

Figure 2 shows a passport 10 in which a page 12 is provided with a number of identifying marks. A passport
30 photograph 14, an alphanumeric code 16, a signature 18 and a pattern 20 are provided on the page 12. For the sake of clarity, the pattern 20 is shown relatively large, but in a practical application the largest dimension need not be greater than a few mm.

35 When the passport 10 is being issued not only the passport photograph 14, but also the signature 18 and the pattern 20 of fibres on the page 12 are optically scanned by

2085113

8

a camera 22, and after data conversion, data compression and data encryption, which operations are performed by means symbolised by block 24, the resulting coded data are stored in a permanent memory, symbolised in Fig. 2 by disk 26. Such
5 a permanent, read-only memory may comprise an optical WORM (Write Once Read Many) device.

Disk 26 or a copy thereof can be used at the place where the check is taking place for checking passports presented at that place. The information obtained there by a
10 check scan with camera 22, after data conversion, data compression and data encryption, jointly symbolised by block 28, is compared in comparison element 30 with the coded data stored on the disk 26, as a result of which fraud which may have occurred with the passport can be established.

15 It is also possible for the purpose of checking by means of data communication to consult a central memory which is accessible from several points.

If it is found during the check that one or more identifying marks of the combination of scanned identifying
20 marks differ from those of a combination of the recorded identifying marks, it is concluded that a forged passport is being presented. If, on the other hand, the combination of checked identifying marks corresponds fully to the combination of recorded identifying marks, it is then
25 concluded that the passport is not forged.

The coded data of at least as many identifying marks of an object or document as is necessary to establish fraud is stored in the memory.

By way of example, another application of the system
30 according to the invention is the issue of a registration certificate for a car, which is provided with a chassis number as usual, and a pattern of nonwoven material. The registration certificate is also provided with a pattern of nonwoven material. At issuing the registration certificate
35 together with the car both patterns and additional identifying marks are scanned and the coded scan data, together with the chassis number, are recorded in a

9 2085113

database. This information now is inseparably combined and can be found in the database. If at a check the information is not found, the originally scanned pictures can be found and it is easily discovered where and how forgery took place.

Still another application of the system and the method according to the invention is the production of trade mark labels for clothes, etc. As a first step in the process a data keeper, also referred to as a security printer, produces for a client a series of trade mark labels with a pattern of nonwoven material and a code number. The security printer fully automatically records the pattern and the code number by means of a digital camera, and stores the concerning coded data on a WORM optical disk. Next, the security printer delivers the trade mark labels and the optical disk or a copy thereof to the client and retains a copy of the optical disk or the original thereof, respectively. The client then processes the trade mark labels in the clothes and distributes the clothes. If there is a suspicion that certain batches of clothes are imitations, an inspector scans the label of a piece of clothing with a digital camera, which scan is sent by modem in coded form to a central place, where it is compared with the data recorded on the optical disk. If the scanned data are not found in the database, it can be proven that the piece of clothing is an imitation without any doubt, since the security printer possesses the original scanned data. This provides two witnesses.

If the clothes are stolen and the trade mark labels are still fixed to the clothes, a proof of the batch from which the clothes originate can be established at any time.

Claims:

1. A product having provision for verifying the legitimacy of the product against forgery and comprising
a body member including a surface, a plurality of
5 overlying individual fibers which are randomly disposed so as to define a number of differing geometrical configurations, and
a transparent base material completely encasing and
fixedly supporting said fibers so that said fibers are
10 visible on said surface and such that said surface is optically scannable through the transparent base material so as to permit the geometrical configurations of the fibers to be scanned.
2. The product as defined in claim 1 wherein at
15 least most of said fibers comprise a polyester core and a polyamide covering.
3. The product as defined in claim 1 wherein said fibers are non-magnetic.
4. The product as defined in claim 1 wherein said
20 body member is relatively thin and has opposite parallel surfaces, and said transparent base material extends through the thickness of said body member and such that said fibers are visible from both of said surfaces.
5. A product having provision for verifying the
25 legitimacy of the product against forgery and comprising
a body member including a surface, at least one identifying mark visible on said surface, a plurality of overlying individual fibers which are randomly disposed so as to define a number of differing geometrical configurations,
30 and

a transparent base material completely encasing and fixedly supporting said fibers so that said fibers are visible on said surface and such that said surface is optically scannable through the transparent base material so as to permit said at least one identifying mark and the geometrical configurations of the fibers to be scanned.

6. The product as defined in claim 1, wherein said fibers are in the form of a sheet of non-woven material which is supported by said transparent base material so that the sheet of non-woven material is generally parallel to said surface.

7. A system for verifying the legitimacy of a product against forgery and comprising a body member including

a surface, a plurality of overlying individual fibers which are randomly disposed so as to define a number of differing geometrical configurations, and

a transparent base material completely encasing and fixedly supporting said fibers so that said fibers are visible on said surface,

scanning means for optically scanning said surface of said body member,

converting means for converting the optical information obtained by said optical scanning means into digital data, and

comparing means for comparing the digital data with previously stored information in storage means so as to permit verification of the legitimacy of said product,

wherein said converting means includes means for converting the optical data into digital data representative of the geometrical configurations formed by the overlying fibers.

8. The system as defined in claim 7, wherein said converting means includes data compressing means for converting the original quantity of digital data into a reduced quantity of equivalent data, and data encryption means for converting the reduced quantity of data into coded digital data, and wherein said comparing means compares said coded digital data with previously stored information in a read only storage means.

9. The system as defined in claim 7, wherein said converting means includes means for converting the optical data into digital data representative of the geometrical configurations of one or more polygons formed by the overlying fibers.

10. A method of verifying the legitimacy of a product against forgery, which product comprises

a body member including a surface, a plurality of overlying individual fibers which are randomly disposed so as to define a number of differing geometrical configurations, and

a transparent base material completely encasing and fixedly supporting said fibers so that said fibers are visible on said surface, the method comprising the steps of optically scanning said surface of said body member and including scanning said fibers, converting the optical information obtained by said optical scanning step into digital data, and

comparing the digital data with previously stored information in storage means so as to permit verification of the legitimacy of said product, wherein the converting step includes converting the optical information into digital data representative of the geometrical configurations formed by the overlying fibers.

11. The method as defined in claim 10, wherein the optically scanning step includes scanning the fibers of said optically scannable portion from at least two different angles.

5 12. The method as defined in claim 10, wherein the converting step includes converting the optical information into digital data representative of the geometrical configurations of one or more polygons formed by the overlying fibers.

10 13. The method as defined in claim 10, wherein the converting step includes converting the original quantity of data into a reduced quantity of equivalent data, and then converting the reduced quantity of data into coded digital data.

15 14. A method of verifying the legitimacy of a product against forgery, which product comprises a body member including a surface, at least one identifying mark provided on said surface, a plurality of overlying individual fibers which are randomly disposed so as to define a number of
20 differing geometrical configurations, and a transparent base material completely encasing and fixedly supporting said fibers so that said fibers are visible on said surface the method comprising the steps of

25 optically scanning said surface of said body member and including scanning the at least one identifying mark and said fibers at the time of issuance of the product,

30 converting the optical information obtained by said optically scanning step into digital data representative of the geometrical configurations formed by the overlying fibers, and including converting the original quantity of data into a reduced quantity of equivalent data, and then converting the reduced quantity of data into coded digital data,

storing the coded digital data in a permanent memory,
and thereafter

5 optically scanning said surface of said body member a
second time, converting the optical information obtained by
said second optically scanning step into digital data
representative of the geometrical configuration formed by the
overlying fibers, and including converting the original
quantity of data into a reduced quantity of equivalent data,
and then converting the reduced quantity of data into coded
10 digital data, and

comparing the coded digital data obtained from said
second scanning step with the previously stored data in said
memory so as to permit verification of the legitimacy of said
product.

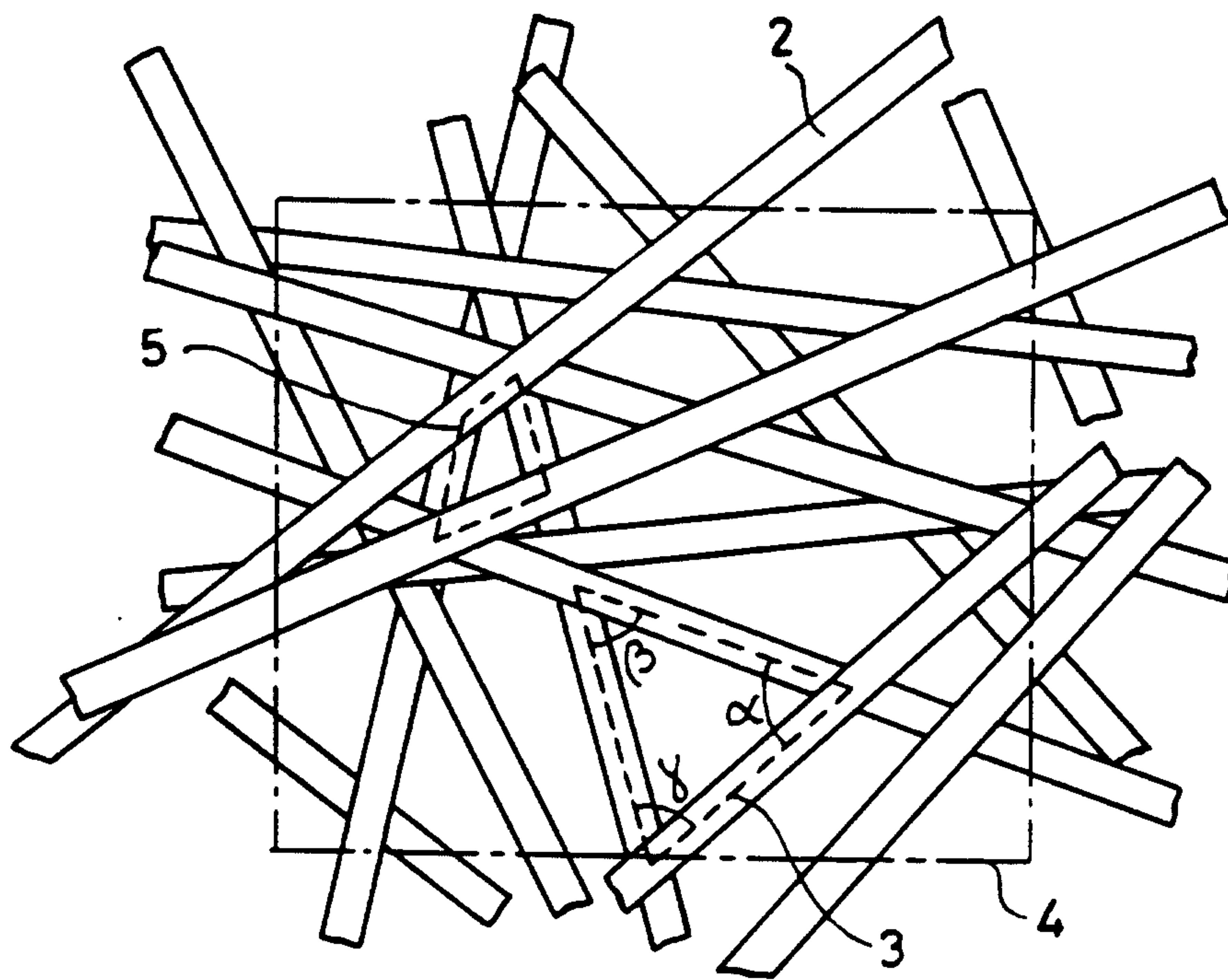


FIG. 1.

