PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06K — A2

(11) International Publication Number: **WO 00/31675**

(43) International Publication Date: 2 June 2000 (02.06.00)

(21) International Application Number: PCT/US99/27012

(22) International Filing Date: 13 November 1999 (13.11.99)

(30) Priority Data:
60/109,259 19 November 1998 (19.11.98) US

(71) Applicant *(for all designated States except US)*: DIGIMARC CORPORATION [US/US]; Suite 500, One Centerpoint Drive, Lake Oswego, OR 97035 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: CARR, Jonathan, Scott [US/US]; 7814 S.W. 189th Avenue, Beaverton, OR 97007 (US). PERRY, Burt, W. [US/US]; 8145 S.W. Barnard Drive, Beaverton, OR 97007 (US).

(74) Agent: GALBI, Elmer; 13314 Vermeer Drive, Lake Oswego, OR 97035 (US).

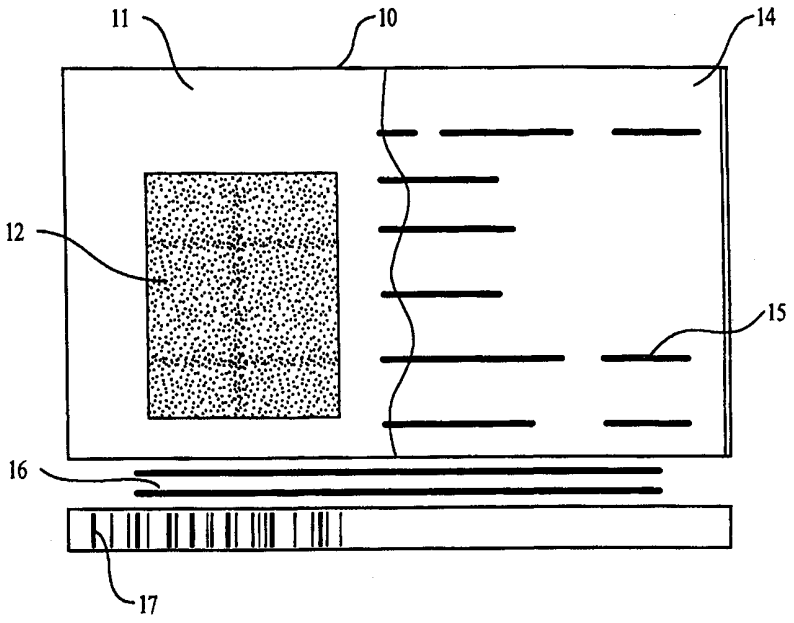
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, 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).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: PRINTING AND VALIDATION OF SELF VALIDATING SECURITY DOCUMENTS

(57) Abstract

Security documents which have multiple fields or areas each of which contains information that is perceptible in more than one way: One field can contain a visually perceptible image and a ditigal watermark that can be detected when the image is scanned and processed, another field can contain machine readable OCR text that can be read by both a human and by a programmed computer, and still another field can contain watermark data which can be correlated to the output of a fingerprint reader or apparatus which scans a user's iris. Documents are produced by beginning with a template which defines the placements of elements on the document and the interrelationships between hidden and visual information on the document. The template specifies the placement of elements such as images, photographs, and text and it also specifies the interrelationship between information that is visually perceptible to a user of the document and information that is hidden by means of ditigal watermarks. Different hidden digital watermark data is included in multiple elements of the document. The watermarks in the different graphic elements of the document are correlated to each other and correlated to the visual material on the document. Thus, the document cannot be forged by replacing one element (such as a picture) with a similar element from another document. In order to produce a document defined by a particular template, appropriate pictures, graphics and digital data are extracted from a data bank, and watermark data is embedded in the pictures and graphics as appropriate. The merged digital data is then sent to a printing engine and the final document is produced. An automatic validation system of the present invention reads multiple fields on the document, and it also automatically detects information about the user. The various information is correlated to validate the document.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

PRINTING AND VALIDATION OF SELF VALIDATING SECURITY DOCUMENTS

Field of the Invention:

The present invention relates to the security documents such as passports, driver's licenses, credit cards, etc. and to systems for producing and validating such documents.

Background of the Invention:

Many security documents contain a picture of the owner of the document. For example, a driver's license generally includes a picture of the driver and a passport generally includes a picture of the owner of the passport. Validation of such documents is performed by comparing the actual physical appearance of the person possessing the document to the picture on the document. A common counterfeiting techniques involves replacing the picture on a security document with a picture of someone who is not the owner of the document.

US Patent number 5,841,886 which will issue November 24, 1998 describes a technique whereby a digital watermark is included in the picture on a security document .

The security document contains human readable text that is related to the data contained in the watermark. The document can be inserted into a scanner which will read the watermark and the operator can compare the output of watermark reader to the text to insure that the person possessing the document is the legitimate owner.

Custom printing systems are available which accept data from multiple sources and which produce documents which are tailored to individual customer characteristics or to information concerning an individual customer. Such systems can for example produce personalized documents that include both fixed information that is on each document that is printed and variable information such as personal information about an individual's account at an institution such as a bank. One such system is commercially marketed under the trademark "PageFlex" by Bitstream Inc. or Cambridge Mass.

Likewise the technology for producing images which contain steganographic information in the form of digital watermarks is well developed. For example see U.S. patent 5,636,292, U.S. patent 5,748,783 or the "Communications of the ACM" published July 1998 Vol. 41. No. 7 pages 31 to 77. Commercial products which can store and read digital watermarks are also widely available. Examples of such products include "Adobe PhotoShop" Versions 4.0 and 5.0 and "Adobe ImageReady" Version 1.0 which are marketed by Adobe Corporation, "CorelDRAW" Versions 7 and 8, and "Corel PHOTO-PAINT" Versions 7 and 8 which are marketed by Corel Corporation, and Micrografx Webtricity" Versions 1 and 2, "Micrografx Graphics Suite 2", and "Micrografx Picture Publisher" Versions 7 and 8 which are marketed by Micrografx Corporation.

Security documents such as passports and drivers licenses have traditionally contained both images and printed text. However, the images and the text in such documents are generally prepared in separate processes and merely merged at a final step in the overall production.

The present invention is directed to an improved security document which has several correlated multi-level self validating features. The present invention is also directed to an improved overall method and system for producing security documents and to automatic authentication systems for such documents. With the present invention the document contains a number of different kinds of information that is hidden from normal view and which can be correlated to validate the document. The validation can be done entirely automatically decreasing the need for human intervention.

With the prior art systems, a human being such as an immigration officer must examine a passport to determine if the person presenting the document is the rightful owner of the document. With the present invention, the authentication can be done entirely automatically, leaving the human operator free to handle non-routine situations.

Summary of the Invention:

The present invention provides security documents which has multiple fields or areas each of which contains information that is perceptible in more than one way. For example, one field can contain a visually perceptible image and a digital watermark that can be detected when the image is scanned and processed, another field can contain machine readable OCR text that can be read by both a human and by a programmed computer, and still another field can contain watermark data which can be correlated to the output of a fingerprint reader or apparatus which scans a user's iris.

Documents in accordance with the present invention are produced by a system and method which begins with a template which defines the placements of elements on

the document and the interrelationships between hidden and visual information on the document. That is, the template specifies the placement of elements such as images, photographs, and text and it also specifies the interrelationship between information that is visually perceptible to a user of the document and information that is hidden (not perceptible to a user) by means of digital watermarks. Different hidden digital watermark data is included in multiple elements of the document. The watermarks in the different graphic elements of the document are correlated to each other and correlated to the visual material on the document. In this way the document can not be forged by replacing one element (such as a picture) with a similar element from another document. In order to produce a document defined by a particular template, appropriate pictures, graphics and digital data are extracted from a data bank, and watermark data is embedded in the pictures and graphics as appropriate. The merged digital data is then sent to a printing engine and the final document is produced.

An automatic validation system of the present invention reads multiple fields on the document, and it also automatically detects information about the user. The various information is correlated to validate the document.

Brief Description of the Drawings:

Figure 1 illustrates a security document in accordance with the present invention.

Figure 2 is an overall diagram of a preferred embodiment of a system to produce security documents in accordance with the present invention.

Figure 3 is a diagram of a document validation system that operates in accordance with the present invention.

Description of a preferred embodiment:

A diagram of a security document in accordance with the present invention is shown in Figure 1. The security features on the document are a pre-printed background 11 which has an image or pattern (not visible in Figure 1) which contains a digital watermark. The image in background 11 may contains lines the width of which are varied to carry a watermark in accordance with the technique described in co-pending application 09/074,034 filed May 6, 1998 (see also WO 99/53428) or which has a weave or tint patern in accordance with the teachings of co-pending application 09/127,502, filied July 31,998 (see also PCT/US99/14532). The disclosure and teaching contained in all of the above referenced applications is hereby incorporated herein in its entirety.

The document also contains a photograph 12 which shows the owner of the document. This photograph 12 contains a watermark such as that described in US. Patent number 5,841,886 which will issue November 24, 1998. The personalized background 14 can for example be a background image which corresponds to the image 12. While the personalized image 14 corresponds to the photograph 12, in area 14 the image is printed as a background image. Background images of various types are conventional, for example personal checks frequently have background images of animals, mountains, etc.. The background text makes it hard to change the human readable text 15 which is printed over the background text. The bottom of the document has machine readable OCR-B text 16 and a Bar code 17.

It should be clearly understood that the document shown in Figure 1 is merely illustrative of the various elements that can be combined to form a security document. The exact layout can vary depending upon the needs of the particular

application. If desired for a particular application, the document can be much more complex than the document shown in Figure 1. The document can have many more fields and elements than does the document shown in Figure 1. Furthermore the document could contain the various other known technology for preventing counterfeiting such as special paper and special ink.

Document shown in Figure 1 can for example be a document such as a driver's license in which case the picture 12 would be a picture of the owner of the license. Graphic image 11 could for example be a state seal. The text 15 could for example include the driver's license number, the owners age, and the owners address.

Document 10 can be a passport. In a passport , the hidden digital watermark data in picture 12 and in the other fields could be coordinated as follows:

	Watermark contains	**Correlates to**
Pre-printed background 11	unique document "batch" number	
Photo 12:	Batch number and passport number (cryptographically encoded)	OCR-B version of passport number, Human readable passport number, Master document
Personalized background 14	"hash" of fingerprint	fingerprint of the holder which is automatically read
Bar code 17	Passport number (in code not in watermark)	Watermark in photo 12

OCR-B text 16	Passport number Batch number (in text not in watermark)	Info in photo 12, background 11 And Bar code 17

An important point is that the various elements of hidden and visual information are coordinated in such a manner that the document is self authenticating. The hidden data in one field can be correlated with the hidden data in another field to insure that the document has not been altered.

If for example one tried to alter a document by replacing picture 12 with a different picture, the new picture would either contain no hidden data, or if it were a picture taken from a different document, the numbers stored in the picture would not match the printed information in text field 15.

If the picture from one document were substituted for the picture in a second document, the cryptographically encoded serial numbers could be used to determine the origin of the picture. It is noted that while in the example shown above, both the Batch number and passport number are cryptographically encoded, other numbers such as a serial number or an ID number could also be encoded in a special manner.

Figure 2 shows an overall diagram of a system for producing document 10. The system includes a number of units, the operation of which is controlled and coordinated by a control computer 20. The following explanation will illustrate how the embodiment shown in Figure 2 can be used to produce a document such as the document shown in Figure 1.

A template 21 is used to define the overall characteristics of a document. The characteristics specified by template 21, including the fields on the document, the data printed in any text fields and the watermarks included in each image included on the document.

The template 21 is used by document layout device 26 to layout a particular document for production. Data which is to be included in the watermarks in any image field are stored in Watermark data store 22. Any pictures, text data, and Graphics are stored in units 23, 24 and 25 respectively.

The document layout from unit 26, the digital watermark data from unit 22 and the pictures, text data and graphics from units 23, 24, and 25 are sent to Merging and watermarking unit 27. Unit 27 applies watermarks to pictures and graphics as specified by the layout information from unit 11. Application of the watermarks to the pictures and graphics can be done in a conventional manner; however, prior to sending the watermark payload (i.e. the data stored in the watermark) to the watermarking engine, the data can be passed through a conventional encryption program. Encrypting the payload data provides an added assurance that a counterfeiter could not make a counterfeit document. The level of encryption could be any level appropriate tot he value of the document.

The output from the Merging and watermarking unit 27 is then sent to a conventional printing engine 28 which produces a final document 10.

Watermark Data storage 22, picture storage 23, digital data storage 24 and graphics storage 25 can be conventional data storage servers. Physically they could all be

provided by one physical storage unit. Template input unit 21 is a conventional interactive terminal or personal computer with a graphic design program. Merging and watermarking unit 27 can be a conventional watermarking engine.

The system shown in Figure 2 produces various parts of the security document in a single step, thereby making it much harder to replace one element on a security document with a similar element from another document.

Figure 3 is a diagram of a document self authentication unit in accordance with the present invention. The system has three input units, each of which is conventional and commercially available. The input units are a magnetic stripe reader 301, a high resolution image scanner 302, and a fingerprint reader 303. The document 10, shown in Figure 1 does not include a magnetic stripe, but one of the alternatives for such a document is to include a magnetic stripe.

The output from scanner 305 goes to three units (that is, to three computer programs) 305, 307 and 311. Alternatively, the bar code reader 305 could be a separate unit which directly reads the bar code and provides information to comparison and authentication unit 312.

If the bar code reader 305 is a computer program which receives information from the output of scanner 302, The program 305 will read the bar code 17. OCR program 307 reads the text 15 and the text 16 and watermark detector 311 reads the watermarks in images 11, 12 and 14.

An authentication and comparison unit 312 which compares the data from units 305, 307 311 and 303 to determine if the data matches. If the data in some of the watermarks is encrypted, the comparison and authentication unit 312 would include an appropriate decryption program. The decryption program in unit 312 could obtain the decryption key from remote data base 314 in response to the number read by one of the devices. Alternatively, the encrypted data could be automatically sent to a central facility for decryption. The unit 312 can also access a remote data base 314 to determine if there is any special handling that is required for the document that has been presented. For example data base 314 could contain information about passports that have been cancelled for various reasons. The resulting information is displayed on a display unit 320.

I claim:

1. A self validating security document that has multiple elements with multiple hidden digital watermark data fields, such that comparison of the various fields with automatically read physical characteristics of the user can validate the document.

2. A system for producing a security document which contain both images, line art and text including means for digitally watermarking multiple images with selected digital data and means for reproducing said image including said digital watermark on a carrier, and means for reproducing human readable indicia on said carrier, said human readable indicia being related to said selected digital data.

3. A security document comprising an image which contains multiple digital watermark data fields, said data including machine readable characteristics of the owner of the document, and human readable indicia which is related to said digital watermark data.

4. A document validating system that includes means for automatically reading a physical characteristic of a person presenting the document and multiple watermarks from different elements of the document, and means for comparing the output of the physical reader with information stored in the hidden watermarks.

5. A method of producing a security document comprising: providing on the document, in OCR or bar code form, an identifier; encrypting the identifier to produce encrypted data; and encoding the encrypted data in hidden form on the document, wherein the provision of the identifier in unencrypted and

hidden/encrypted form on the document serves as an aid to document authentication and as deterrent to document counterfeiting.

6. An object comprising a substrate having thereon at least two regions, a first of said regions comprising a human-perceptible image with first plural-bit data steganographically encoded therein, a second of said regions comprising a background having unobtrusive markings arrayed thereacross and also comprising text amidst said background, the markings in the second region encoding second plural-bit data.

7. The object of claim 6 in which the second plural-bit data is different than the first.

8. An object comprising a substrate having thereon at least two regions, one of said regions having first plural-bit data steganographically encoded therein, another of said regions having second plural-bit data steganographically encoded therein, the first and second plural-bit data being different.

9. An object comprising a substrate having thereon a photographic image and a graphic that is not a photographic image, characterized in that both the photographic image and the graphic are encoded to steganographically convey plural-bit data.

10. The document of claim 9 in which the photographic image and the graphic are encoded to convey different data.

11. The object of claim 9 in which the photographic image and the graphic are encoded to convey the same data.

12. A method of printing a security document characterized by printing on a substrate (a) a photographic image, (b) a graphic distinct from the photographic image, and (c) a bar code or OCR text, all in a single printing operation, said photographic image and said graphic both having plural-bit data encoded therein.

13. A system for validating a security document comprising: a first computer system coupled to a second computer system, the second computer system being remote from the first, the first computer system including an optical scanner producing scan data corresponding to said document, the first computer system further including a watermark decoder receiving said scan data and outputting watermark data corresponding thereto, said watermark data being encrypted, the first and second computer systems cooperating to decrypt the watermark data.

14. The system of claim 13 in which the second computer has a memory storing decryption data, said data being transferred to the first computer for use at the first computer to decrypt the watermark data.

15. The system of claim 13 in which the second computer includes a decryption system having an input for receiving watermark data from the first computer, and an output for providing decrypted watermark data to the first computer.

16. The system of claim 13 in which the decryption proceeds in accordance with unencrypted data discerned by the first computer system from the scan data.

17. The system of claim 16 in which the unencrypted data comprises a document identifier printed on the document in OCR or bar code form.

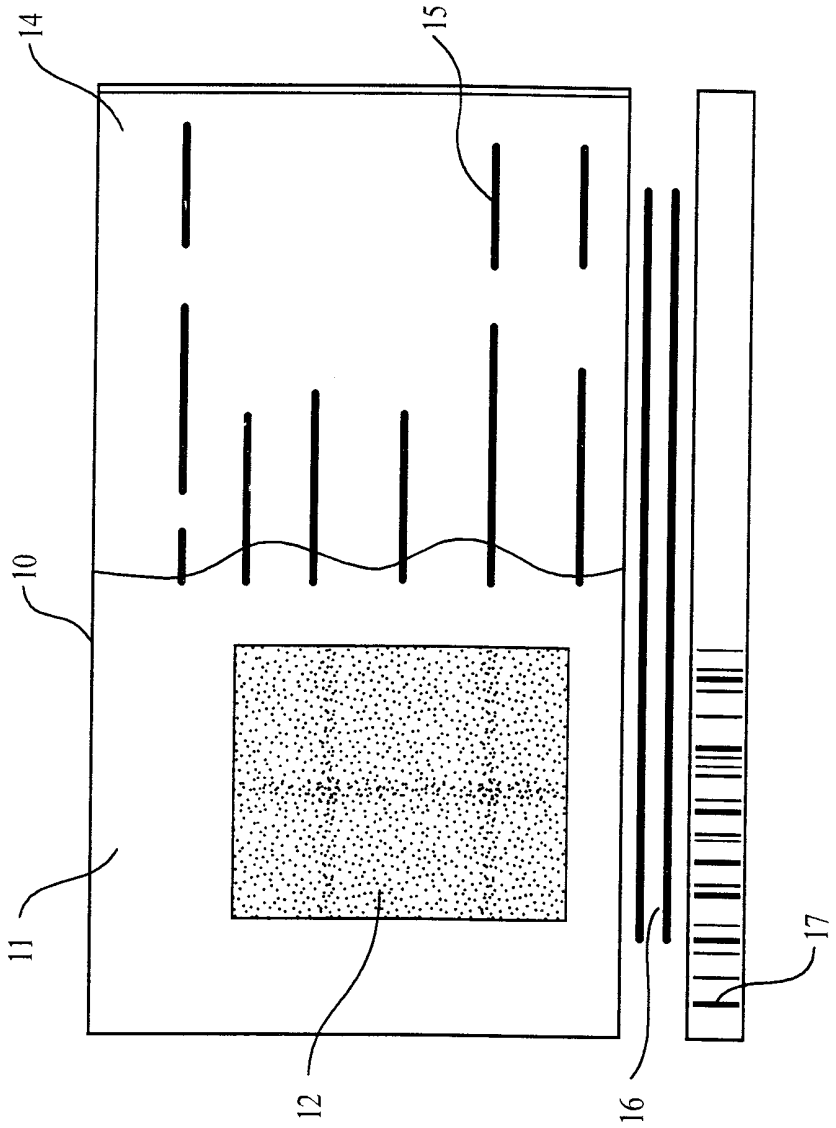


FIG. 1

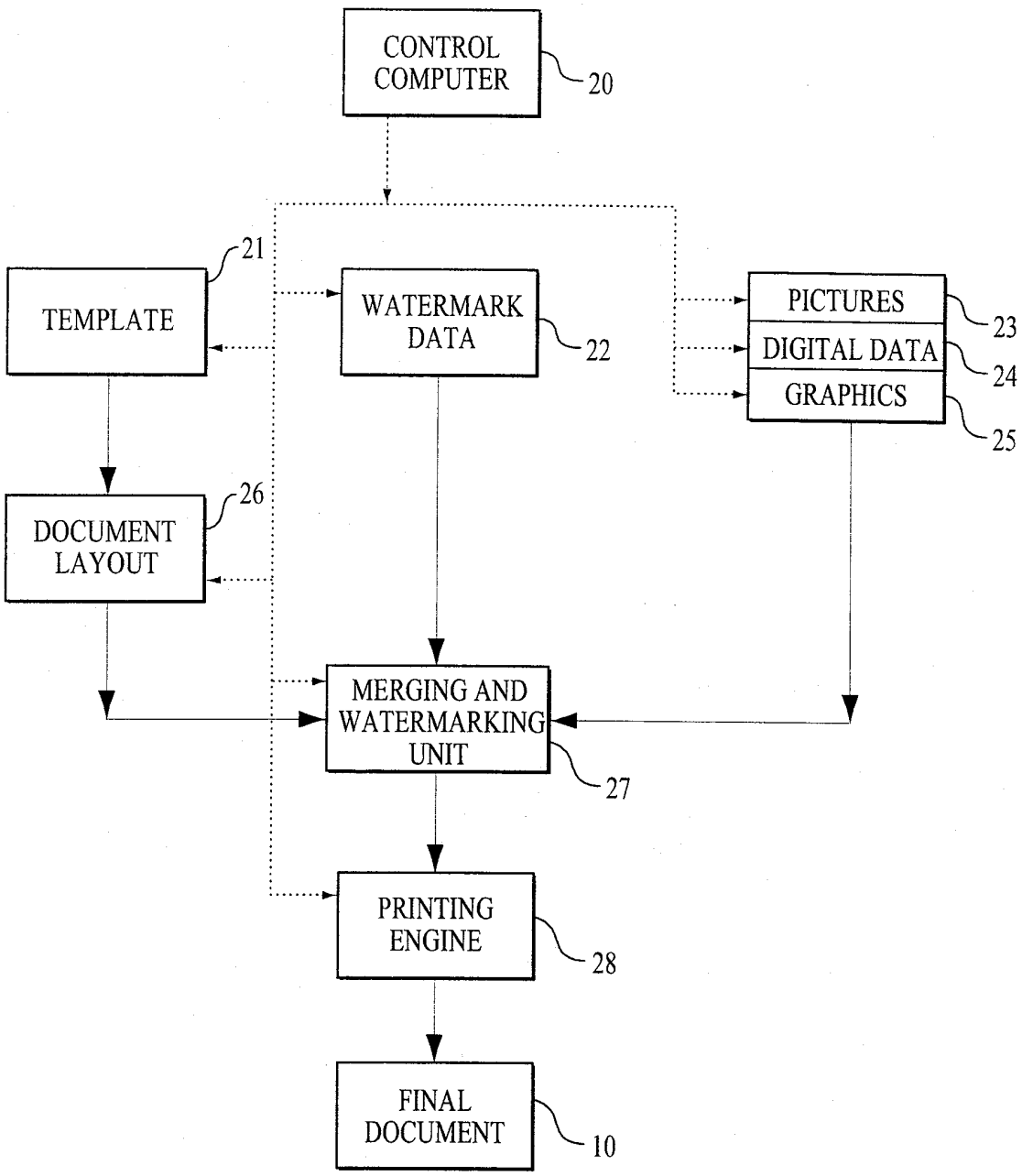

CONTROL COMPUTER
20
TEMPLATE
21
WATERMARK DATA
22
PICTURES
DIGITAL DATA
GRAPHICS
23
24
25
DOCUMENT LAYOUT
26
MERGING AND WATERMARKING UNIT
27
PRINTING ENGINE
28
FINAL DOCUMENT
10

FIG. 2

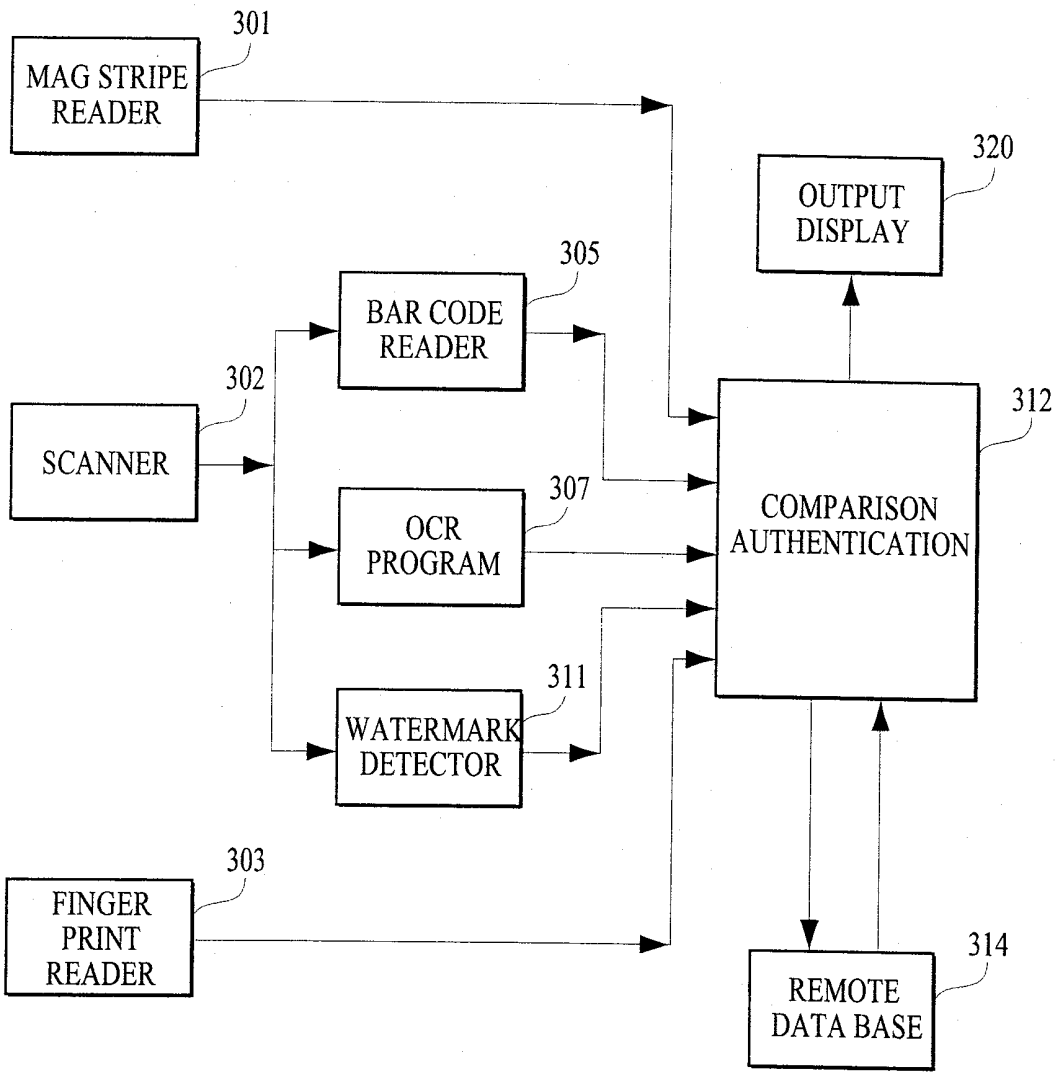

301
MAG STRIPE READER
320
OUTPUT DISPLAY
305
BAR CODE READER
302
SCANNER
312
COMPARISON AUTHENTICATION
307
OCR PROGRAM
311
WATERMARK DETECTOR
303
FINGER PRINT READER
314
REMOTE DATA BASE

FIG. 3