(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 718 808 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.06.1996 Bulletin 1996/26

(51) Int Cl.[6]: **G07D 7/00**

(21) Application number: **95308909.1**

(22) Date of filing: **07.12.1995**

(84) Designated Contracting States:
DE ES FR GB IT

(30) Priority: **10.12.1994 GB 9424971**

(71) Applicant: **NCR International, Inc.**
Dayton, Ohio 45479 (US)

(72) Inventors:
- **Scott, Gregory**
Edinburgh EH12 6DJ, Scotland (GB)
- **Eccles, John**
Colston Bassett, Nottinghamsh. NG12 3FR (GB)

(74) Representative: **Robinson, Robert George et al**
International Intellectual Property Department,
NCR LIMITED,
915 High Road,
North Finchley
London N12 8QJ (GB)

(54) Document authentication system

(57) In a system for authenticating documents (12), such as banknotes, cheques or the like, a document (12) to be tested is driven past a sensing station (20) which provides a digital colour image of the document which is stored in a memory (38), in the form of plurality of digital images obtained by illuminating the document (12) with light of different colours. The stored colour image is processed using template matching, for example, to determine the type and orientation of the document (12). The type and orientation information is utilized to select a plurality of areas of the digital colour image for colour intensity analysis. For example, a statistical testing procedure using stored values derived from processing genuine documents may be utilised. Documents of different types are thus all processed in a uniform manner.

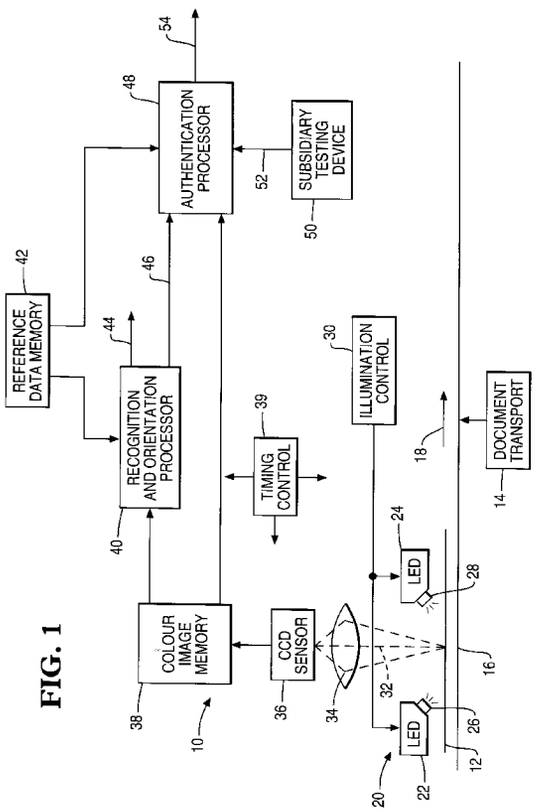

FIG. 1

EP 0 718 808 A2

Description

This invention relates to a method and apparatus for authenticating documents.

Automatic machines which accept banknotes and other documents such as cheques or giro documents are coming into increasing use. It is important for such machines to authenticate the documents, that is, to distinguish between genuine and counterfeit documents.

European Patent Application No. EP-A-O 101 115 discloses a device for recognising and examining banknotes or the like. In this known device, a monochrome (grey level) digital image of the transmittance of the banknote is formed by directing light onto the banknote, as it is being fed through the device, and sensing the transmitted light by using a row of photosensitive cells. Colour information may be derived by a separate photosensitive device or devices responsive to light of a particular colour or colours. The colour information may be integrated over the whole note. Depending on the country whose banknotes the device is adapted to accept, the denomination of an inserted banknote may be determined. For example, for Netherlands banknotes, the colour is characteristic of the denomination. For German banknotes the length or length/width ratio are characteristic of the denomination. Items which are not recognised can be rejected immediately. Using the determined denomination, a pattern recognition procedure takes place during which selected areas of the digital image are compared with data stored in memories to determine the authenticity of the banknote. If the device is adapted to accept items which are of uniform size and colour such as US banknotes, for example, the denomination of the banknote has to be determined solely by the pattern examination. Thus, the known device has the disadvantage that reconfiguration to operate in a different manner may be needed for some types of document to be authenticated.

It is an object of the present invention to provide a system for authenticating documents which is adapted to operate in a uniform matter, independent of the type of document to be authenticated.

Therefore, according to the present invention, there is provided a method of authenticating a document which may be of one of a plurality of types, characterized by the steps of: forming a digital colour image of said document; processing said digital colour image to identify the type to which said document belongs and the orientation of the document; and analysing said digital colour image in dependence on the identified document type to determine the authenticity of the document.

One embodiment of the present invention will now be described by way of example, with reference to the accompanying drawings, in which:-

Fig.1 is a simplified block diagram of apparatus according to the invention, for accepting and authenticating documents;

Fig.2 is a enlarged view of an LED array utilized in the apparatus of Fig 1;

Fig.3 is a diagram illustrating the storage of digital colour information derived from a document;

Fig.4 is a flowchart illustrating the general operation of the apparatus of Fig. 1;

Fig.5 is a flowchart illustrating the recognition procedure for recognising a document;

Fig.6 is a flowchart illustrating the authentication procedure for authenticating a document which has been recognised by the recognition procedure; and

Fig.7 is a graphical plot helpful in understanding the authentication procedure.

Referring first to Fig. 1, there is shown a simplified block diagram of a document authentication system 10. A document 12 is fed from an input slot (not shown) by document transport means 14, which may include conventional feed rollers and/or feed belts, along a feed path 16 in the direction of arrow 18. The document 12 is fed past an image capture station 20 which includes first and second LED (light emitting diode) arrays 22 and 24. In the preferred embodiment, the document 12 is driven in a vertical orientation and the LED arrays 22 and 24 are each formed by a vertical column of individual spaced LED's. In a modified arrangement the document 12 could be driven in a horizontal orientation, with the LED arrays being horizontally aligned. The LED array 22 includes a column of individual LED's, and the LED array 24 includes a column of individual LED's 28. The LED's of each array 22, 24 may be integrated on respective semiconductor substrates, enabling a very close spacing of the individual LED's.

Referring briefly to Fig. 2, there is shown a view of the LED array 22, which contains a column of LED's 26 referred individually as 26-1, 26-2, 26-3 etc. The LED's 26 each emit light at one of three different wavelengths, corresponding to green light, red light and infrared light. Thus the diodes 26-1, 26-4, etc. may emit green light, the diodes 26-2, 26-5 etc. may emit red light, and the diodes 26-3, 26-6 etc. may emit infrared light. However, other colours of LED's may be used, for example yellow or blue. Furthermore, the total number of colours may be different from three. For example, two or four colours may be used, although fewer colours reduces the amount of available information sensed from the document 10. The LED array 24 (Fig.1) is of identical construction to the LED array 22.

The LED arrays 22 and 24 operate under the control of an illumination control device 30, in a manner which will now be described, to direct light onto the document 12. Light is reflected from the document 12 along path 32 and focused by a lens system 34 on to a CCD (charge-coupled device) sensor device 36. In an alternative arrangement, the sensor could include an array of photodiodes. The CCD sensor device 36 provides, by sampling at periodic intervals, digital signals representing the reflected light of the respective colours, which

are stored in a colour image memory 38 as a colour image of the document 12. The colour image memory 38 will be described in more detail hereinbelow. A timing control circuit 39 synchronises the operation of the document transport 14, the illumination control circuit 30 and the colour image memory 38.

The illumination control 30 is effective to control the illumination of the LED's 26, 28 in the arrays 22, 24, such that the green LED's, the red LED's and the infrared LED's are operated sequentially and repeatedly, whereby the document 12 is illuminated sequentially and repeatedly by green light, red light and infrared light. This successive illumination is effected at a high speed relative to the movement of the document 12 along the feed path 16, such that successive green, red, and infrared images are captured of substantially the same regions of the document 12. In this connection, it should be understood that although the three images produced by the successive colour illuminations are slightly out of alignment, due to the movement of document 12, the resolution of the patterns on the document 12 being imaged is significantly greater than this, and the slight misalignment of the images can therefore be ignored in practice.

Although in the preferred embodiment a digital colour image of only one side of the document 12 is formed, it should be understood that, in a modified arrangement, the sensing station 20 could sense light reflected from both sides of the document 12, whereby digital colour images of both sides of the document could be generated and utilized in the subsequent recognition and authentication procedures. In another modified arrangement, instead of using light emitting diodes of different colours, a white light source could be utilized and a colour CCD imaging system using colour filters could be included in the CCD sensor.

The remaining portion of Fig. 1 will now be briefly described. The colour image data stored in the colour image memory 38 is first processed in a recognition and orientation processor 40, using reference data stored in a reference data memory 42, to determine the orientation of the document 12 and to recognize the type of the document 12. For example, if the document 12 is a banknote, the processor 40 will determine in addition to the orientation of the banknote, the country, or issuing bank, and the denomination of the banknote. If the document 12 is not recognised as being of a type for which reference data is stored in the memory 42, a reject signal is produced on an output line 44. The reject signal causes the rejected document to be returned to the input slot or diverted to a reject container (not shown).

Assuming that the document 12 is recognised, then a signal indicative of the type and orientation of the document is provided on an output line 46 to initiate a document authentication procedure, to be described hereinbelow, in an authentication processor 48, which, like the processor 40, uses data from the colour image memory 38 and reference data supplied from the reference data memory 42, to determine the authenticity of the document 12. Optionally, one or more subsidiary tests on the document 12 may be performed by the testing device 50. For example, the presence of magnetic ink, or a metallic strip may be tested. A signal representing the outcome of the subsidiary tests is applied by the testing device 50 over a line 52 to be utilized by the authentication processor 48 in determining the authenticity of the document 12. The authentication processor 48 provides an output signal on a line 54 representing the authenticity or non-authenticity of the document 12. Thus, if the document 12 is determined as authentic, the signal on the line 54 may enable further operations such as initiating further processing of the document 12, or, if the document is a banknote, effecting a financial transaction in accordance with the determined value of the banknote.

Referring now to Fig. 3, there is shown a representation helpful in understanding the manner in which the digital colour image data is stored in the colour image memory 38. The colour image data is arranged, notionally, in three "planes" 62, 64 and 66, wherein the plane 62 stores green colour data, the plane 64 stores red colour data and the plane 66 stores infrared colour data. The data for a single pixel area in the document 12 is represented along a line 68 linking shaded areas 72 in the green colour plane 62, shaded area 74 in the red colour plane 64, and shaded area 76 in the infrared colour plane 66. A similar representation to that shown in Fig. 3 will apply if the image capture station 20 utilises other colours than green, red and infrared, and/or a different number of colours.

Referring to Fig. 4, the general operation of the system 10 is illustrated in the form of a flowchart 80. Initially, as shown at block 82, a digital colour image of the document 12 is lifted in the manner described hereinabove, that is, the digital colour image is formed and stored in the colour image memory 38 (Fig.1).

Next, as shown at block 84, the type and orientation of the document are determined in the recognition and orientation processor 40 (Fig.1). If the document type is recognised, the flowchart proceeds to block 88, where the document is tested for authenticity. The result of the authenticity test is the output result (block 90). If, at block 86, the document type is not recognised, the flowchart proceeds directly to the output result block 90, as described hereinabove, wherein the authentication processor 48 (Fig.1) produces an output signal on the line 54 in accordance with the determined authenticity or non-authenticity of the document 12 which has been recognised. Thus all recognition and authentication information is presented on the lines 44 and 54.

Referring now to Fig. 5, the manner in which the document type and orientation are determined, in accordance with block 84 (Fig.4), will now be described in more detail, with reference to the flowchart 100 shown in Fig.5. Initially, the colour image of the document is stored in the colour image memory 38 (block 82). Next,

a size measurement of the document is effected (block 102). For example, the length and/or width of the document may be determined by scanning one of the three colour images stored in the colour planes 62, 64, and 66 (Fig.3). Alternatively, the length could be determined by a photosensor (not shown) located in the document feed path 16. On the basis of the determined document size, templates are selected in accordance with the determined size (block 104) and a template matching procedure, to be described hereinbelow, is performed (block 106). The template matching procedure results in the identification of the document 12 as being of a particular type and also determines its orientation. If no match is found, the document 12 is not recognised and may be rejected, as mentioned hereinabove. It should be understood that the size determining step (block 102) is optional, and may be omitted, although this may increase the processing time involved in the template matching procedure, since a larger number of templates may need to be utilized in the matching procedure.

The template matching procedure utilized in the preferred embodiment averages small square regions of the document image, typically regions of size 16 by 16 pixels, thereby reducing the amount of data to be matched and so speeding up the template matching procedure. Also, the template matching procedure is performed on a colour combination image, referred to herein as a grey image. For example the grey image may be formed by combining the green and red colour images stored in the respective planes 62 and 64 (Fig.3). However, other combinations are possible, e.g. the green and infrared images, as all three images could be combined, to form the grey image. The grey image may be stored in a memory portion of the processor 40.

The grey image is averaged by calculating the average pixel intensity value of regions of size 16 by 16 pixels, that is, 256 pixel size square regions. This corresponds to regions of size about 4mm by 4mm. However, regions of other sizes could be used. With a 16 by 16 pixel size region, a typical document image containing around 100,000 to 200,000 pixels is reduced to an image of less than 1,000 elements by the averaging procedure. As mentioned, this averaged image may be stored in a further memory portion of the processor 40, and utilized for matching with templates derived from the reference data memory 42 (Fig.1). The template matching procedure determines the template having the closest match to the averaged image, utilising a predetermined threshold value for rejecting unrecognisable images. It will be appreciated that the closest match template provides information as to the type and orientation of the document 12. The templates stored in the reference data memory 42 generated in a preliminary training procedure during which genuine documents of the types to be recognised are scanned in all four possible orientations.

Referring now to Fig. 6, the authentication procedure will now be described with reference to the flowchart 120 shown in Fig. 6. From the start block 122 the flowchart proceeds to block 124 where it is noted that the authentication regions for the determined document type and orientation are selected. Typically between eight and thirty-two regions are used, with a typical size of between 2.5mm and 7.5mm square, although the region size could be greater than these values. Preferably the regions are evenly spaced over document. However, regions which are not evenly space may be selected as appropriate for certain types of document. Since the image of the document is held in the colour image memory 38, regions may be selected dependent on the document type and orientation, under software control, without any hardware modifications for different document types.

Next, as shown at block 126, feature vectors are calculated for the selected regions. This is effected as follows. The pixel intensity values for the selected regions are averaged for each colour plane 62, 64, 66 (Fig. 3) to provide average colour intensities for the selected regions. For each selected region a feature vector z=(x, y) is calculated where x is the ratio of green to red average intensity for the region and y is the ratio of infrared to red average intensity for the selected region. It will be appreciated that by utilising intensity ratios, instead of absolute values, in calculating the feature vectors, the components from different samples are effectively normalised. Of course, instead of the ratios of green and infrared to red, other ratios such as red and infrared to green could be chosen.

Next, as shown at block 128, authentication parameters for the selected regions are retrieved from the reference data memory 42 (Fig.1), following which an authentication process for each selected region is performed (block 130). The retrieved reference data for each region is formed by a set of values, namely a mean vector and the elements of a 2x2 covariance matrix. The mean vector and elements of the covariance matrix are calculated from the feature vectors of sample genuine documents during an initial training phase which produces the reference data. Returning to the description of block 130, the Mahalanobis distance of the feature vector from the mean is then calculated using the retrieved reference data. The concept of Mahalanobis distance is well known to those skilled in the pattern recognition art. For example, see page 24 of the text book "Pattern Recognition and Scene Analysis" by R.O. Duda and P.E. Hart, published in 1973 by John Wiley & Sons. As is known from statistical theory, the contours of constant Mahalanobis distance from the mean are in the form of ellipses, centred on the mean value. For a threshold value of T, points having a Mahalanobis distance less than T lie within an ellipse, centred on the mean value and points having a Mahalanobis distance greater than T lie outside the ellipse.

Referring to Fig.7. the mean feature vector (M_x,M_y), shown as point 150, is the centre of an ellipse 160 which corresponds to threshold value T. The ellipse 160 has a

major axis 162 and a minor axis 164. If the calculated feature vector lies within the interior 166 of the ellipse 160, i.e. the Mahalanobis distance is less than T, then the corresponding region of the document 12 being authenticated is categorised as authentic. If the calculated feature vector lies outside the ellipse 160, i.e. the Mahalanobis distance is greater than T, then the corresponding region of the document 12 is categorised as non-authentic. If, in a modification, the feature vector has three or more components, then the ellipse would be replaced by an ellipsoid in multidimensional space.

Returning now to Fig. 6, there is shown an optional step of performing subsidiary tests on the document 12. As mentioned previously, the subsidiary testing device 50 (Fig.1) may perform tests such as a test for the presence of a metallic strip and/or the presence of magnetic ink. As shown in block 134 an authentication decision for the document 12 is now made, wherein the document 12 is categorised as authentic only if all, or at least a preselected number, of the selected regions tested for authenticity as described hereinabove have been found to be authentic, and the results of any optional subsidiary tests have also been found to be authentic. The flowchart 120 then ends (block 136) and the document 12 can then be utilized for a transaction operation, if authentic, or rejected, if non-authentic.

It should be understood that modifications of the described embodiment are possible. For example, instead of the statistical technique for determining document authenticity on the basis of Mahalanobis distance calculations, a neural network could be used to analyse the feature vectors. The neutral network would be trained by utilising genuine documents and would then be effective to authenticate a document by determining the authenticity of a plurality of document image regions. Also, the recognition and orientation procedure may use a pattern recognition procedure other than template matching.

Thus, there has been described a system for authenticating documents which is suitable for authenticating various types of documents including banknotes, cheques and giros, for example, in a uniform manner. The two-stage procedure of first determining document type and orientation and then determining authenticity enables an efficient document processing system having high security to be provided. Thus, unrecognised documents can be rejected immediately, without the need for authentication. Forming a digital colour image assists in providing a two-stage authentication procedure which is highly efficient since use of colour intensity values provides enhanced analysis capabilities and greater accuracy in determining authenticity as compared with monochrome analysis. Moreover, since digital colour information is derived from the whole document, the performance of the recognition and orientation procedure is not degraded by localised marks or damage. Also the authentication can be focused on selected regions by software control. Thus, the system can be easily reconfigured by software modification to handle additional document types.

Claims

1. A method of authenticating a document (12) which may be of one of a plurality of types, characterized by the steps of: forming a digital colour image of said document (12); processing said digital colour image to identify the type to which said document (12) belongs and the orientation of the document; and analysing said digital colour image in dependence on the identified document type to determine the authenticity of the document (12).

2. A method according to claim 1, characterized in that said step of forming a digital colour image includes the step of forming a plurality of digital images each representing the reflected light intensity from said document (12) for a respective colour.

3. A method according to claim 2, characterized in that said step of processing said digital colour image includes the step of identifying the document type by using a template matching procedure.

4. A method according to claim 3, characterized in that said processing step includes the steps of forming a grey level digital image by combining at least two of said digital images; averaging a plurality of areas of said grey level digital image; and utilising the averaged areas in said template matching procedure.

5. A method according to any one of the preceding claims, characterized in that said analysing step includes: selecting a plurality of regions of said digital colour image of said document (12); calculating a feature vector dependant on colour intensities for each of said regions; determining a distance measurement dependent on the difference between said feature vector and reference data derived from genuine documents; and determining said document (12) to be authentic if said distance measurement is less than a predetermined threshold value.

6. A method according to claim 5, characterized in that said calculating step includes the step of forming ratio values of average colour intensities for each of said plurality of regions.

7. A method according to claim 6, characterized in that said step of forming ratio values includes selecting from said digital colour image the colour intensity value of a predetermined colour and dividing the other colour intensity values from said digital colour image by the selected intensity value.

8. A method according to claim 7, characterized in that

said step of determining a distance measurement includes determining the Mahalanobis distance between said feature vector and a mean value vector representing a mean value for genuine documents, included in said reference data.

9. A method according to any one of claims 5 to 8, characterized by the steps of performing at least one additional authenticity test and determining said document (12) as authentic only if said additional authenticity test is also satisfied.

10. Apparatus for carrying out a method according to any one of the preceding claims, characterized by sensing means (20, 36) adapted to provide a digital colour image of a document (12) being authenticated, storage means (38) adapted to store said digital colour image, first processing means (40) adapted to determine the type of said document, in dependence on the stored digital colour image, and processing means (48) adapted to determine the authenticity of said document (12) in dependence on the determined document type and said stored digital colour image.

11. Apparatus according to claim 10, characterized by illuminating means (22,24) adapted to illuminate said document (12) successively with light of a plurality of different colours.

12. Apparatus according to claim 11, characterized in that light of three different colours is utilized.

13. Apparatus according to claim 11 or claim 12, characterized in that said illuminating means includes light emitting diodes (22,24).

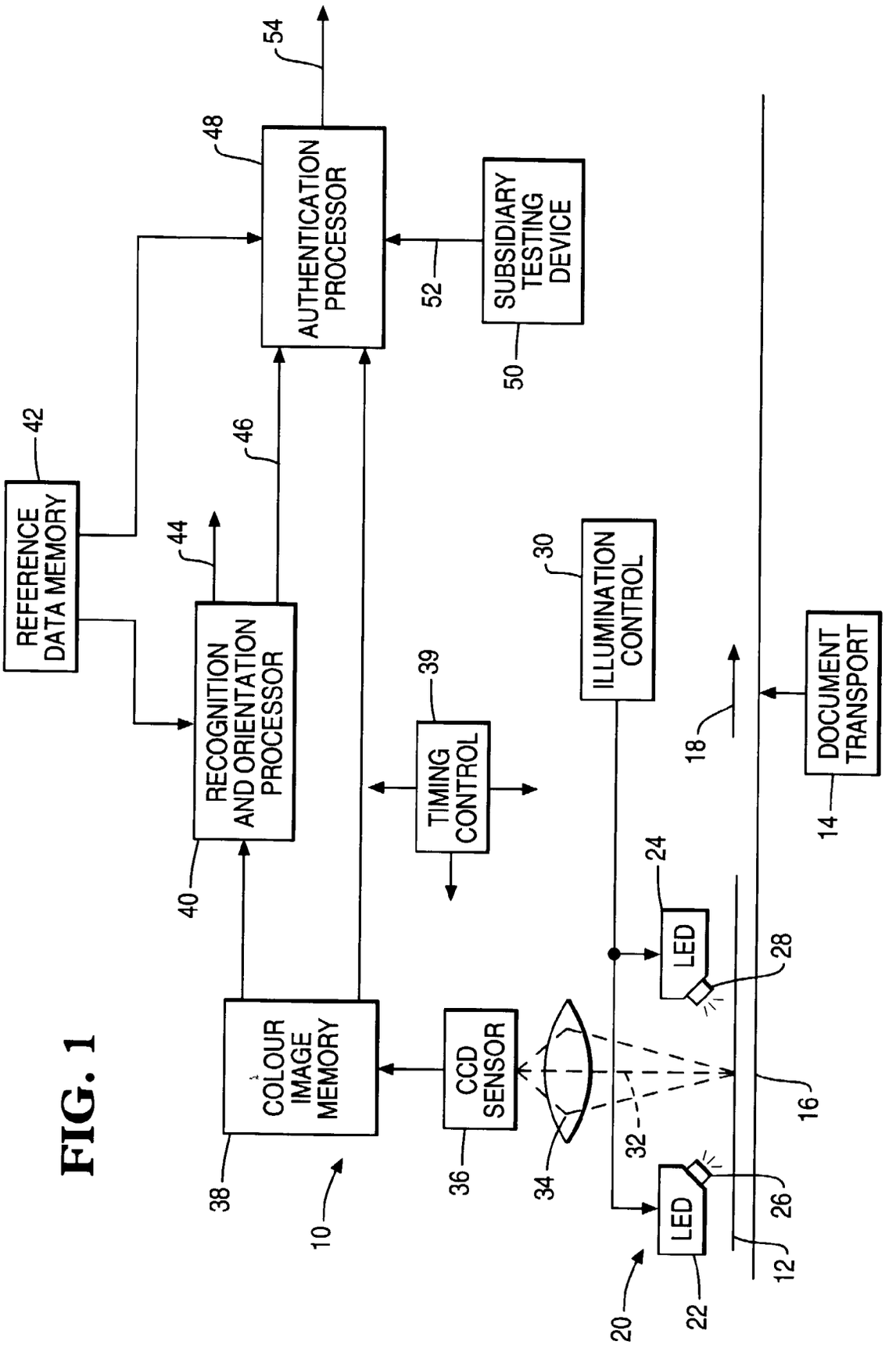
AUTHENTICATION PROCESSOR
SUBSIDIARY TESTING DEVICE
REFERENCE DATA MEMORY
RECOGNITION AND ORIENTATION PROCESSOR
TIMING CONTROL
ILLUMINATION CONTROL
DOCUMENT TRANSPORT
COLOUR IMAGE MEMORY
CCD SENSOR
LED
LED
10
12
14
16
18
20
22
24
26
28
30
32
34
36
38
39
40
42
44
46
48
50
52
54

FIG. 1

FIG. 2

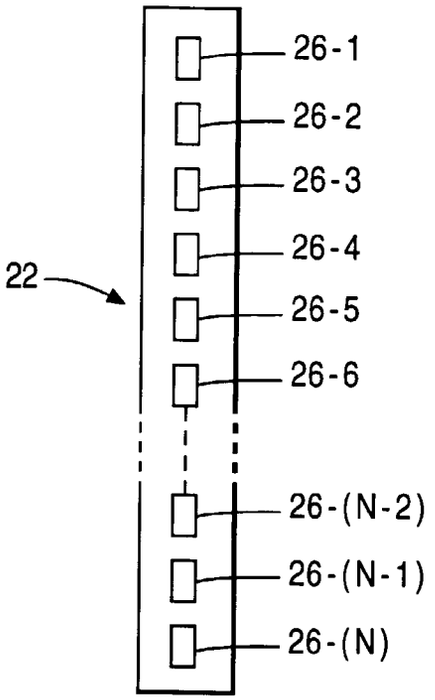

FIG. 3

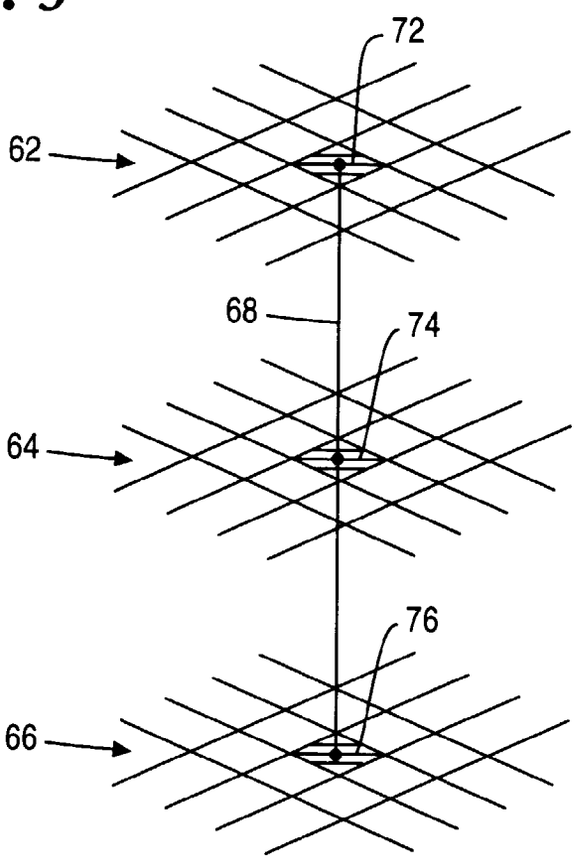

FIG. 4

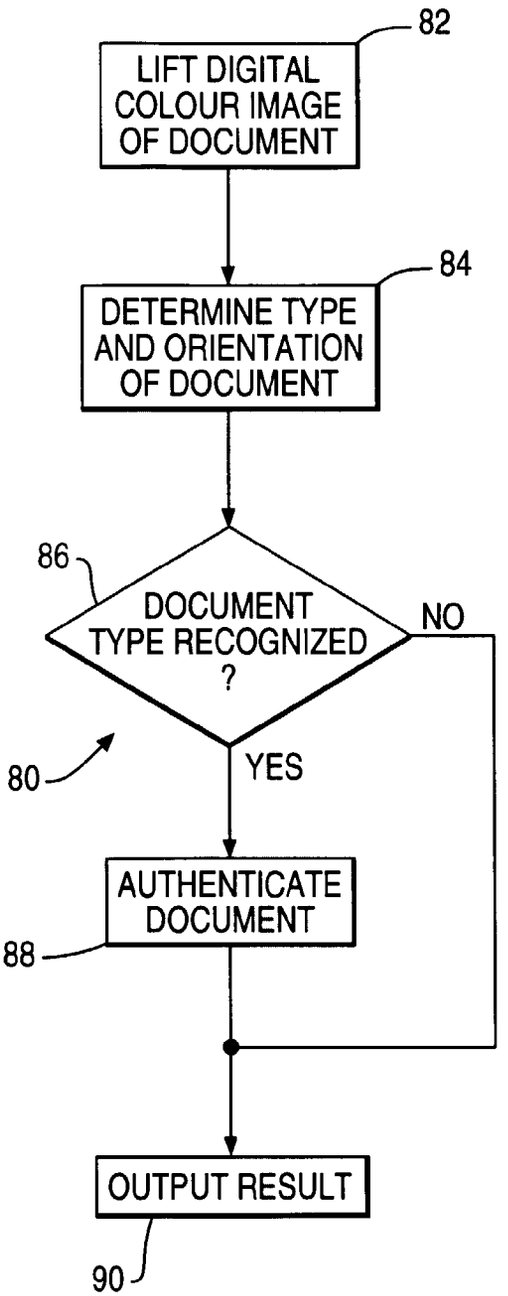
82
LIFT DIGITAL COLOUR IMAGE OF DOCUMENT
84
DETERMINE TYPE AND ORIENTATION OF DOCUMENT
86
DOCUMENT TYPE RECOGNIZED ?
NO
YES
80
AUTHENTICATE DOCUMENT
88
OUTPUT RESULT
90

FIG. 5

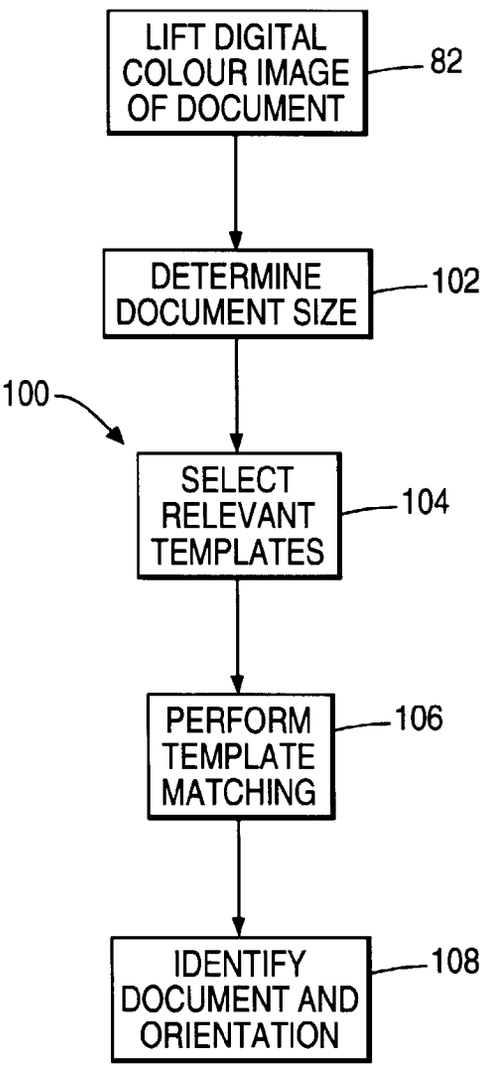
LIFT DIGITAL COLOUR IMAGE OF DOCUMENT
82
DETERMINE DOCUMENT SIZE
102
100
SELECT RELEVANT TEMPLATES
104
PERFORM TEMPLATE MATCHING
106
IDENTIFY DOCUMENT AND ORIENTATION
108

FIG. 6

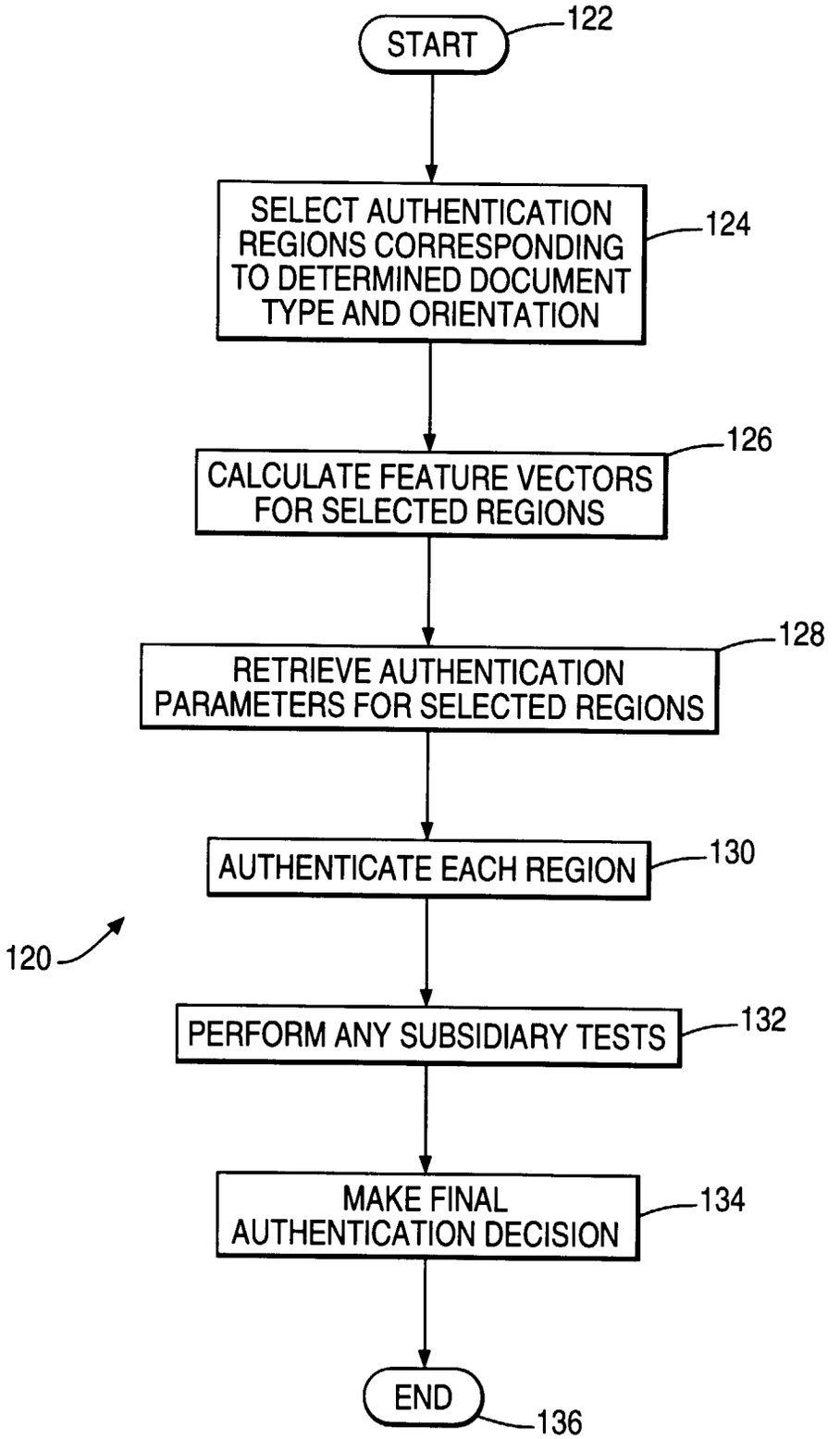
START
122
SELECT AUTHENTICATION REGIONS CORRESPONDING TO DETERMINED DOCUMENT TYPE AND ORIENTATION
124
CALCULATE FEATURE VECTORS FOR SELECTED REGIONS
126
RETRIEVE AUTHENTICATION PARAMETERS FOR SELECTED REGIONS
128
AUTHENTICATE EACH REGION
130
120
PERFORM ANY SUBSIDIARY TESTS
132
MAKE FINAL AUTHENTICATION DECISION
134
END
136

FIG. 7