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

(11) Publication number: **0 590 224 A2**

(12) # EUROPEAN PATENT APPLICATION

(21) Application number: **92830598.6**

(51) Int. Cl.5: **G07C 9/00**

(22) Date of filing: **30.10.92**

(30) Priority: **29.09.92 IT MI922255**

(43) Date of publication of application:
06.04.94 Bulletin 94/14

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR LI NL PT SE

(71) Applicant: **Russi, Franco**
Via Settembrini, 41
I-20124 Milano(IT)

(72) Inventor: **Russi, Franco**
Via Settembrini, 41
I-20124 Milano(IT)

(74) Representative: **Cicogna, Franco**
Ufficio Internazionale Brevetti
Dott.Prof. Franco Cicogna
Via Visconti di Modrone, 14/A
I-20122 Milano (IT)

(54) **Improved method for making credit documents in general and device for detecting property marks thereon.**

(57) There is disclosed an improved method for making credit document in general and for suitably detecting property marks or signs thereon,so as to prevent non authorized persons from using the documents.To this end,the method comprises the step of providing the document with a code for detecting and biometrically identifying the authorized user or owner,which step is performed based on the provision of a biometric sensor and a comparator for comparing the identification code with the code sensed by the biometric sensor.

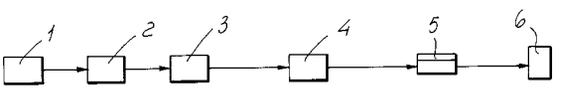

FIG. 1

EP 0 590 224 A2

BACKGROUND OF THE INVENTION

The present invention relates to a method for making credit documents in general and to a device for properly detecting property marks or signs thereon.

As is known,there are at present broadly used payment system based on microprocessor controlled magnetic and/or electronic cards.

Also known is that a main drawback associated with the above mentioned cards consists of a substantial impossibility of detecting in an absolutely safe manner if the person submitting for payments the card is the legitimate owner thereof,or if the card has been stolen.

In order to overcome the above mentioned drawback, several methods have been devised,such as the application to the card of secret codes,signature on receipt bills for the credit cards,phone checking thereof and the like.

The above mentioned methods,however,in addition to limiting the servicing,are moreover not fully safe since nobody can establish for a certainty if the person submitting the card is the legitimate owner thereof.

Moreover,in the case of a magnetic read out card,such as a Bancomat or P.O.S card,the user must form on a keyboard the secret code born among the data recorded on the card,which involves that the user remembers his/her code which is very difficult especially if said user has a lot of secret codes associated with different cards.

Thus,in order to quickly recover his code,the user frequently writes it on paper bills,which can be easily lost and used by other persons.

SUMMARY OF THE INVENTION

Accordingly,the aim of the present invention is to overcome the above mentioned drawbacks,by providing a credit document(microprocessor controlled magnetic cards and/or electronic credit cards) which allows to establish with an absolute certainty if the person submitting the card or document is the legitimate owner thereof.

Within the scope of the above mentioned aim, a main object of the present invention is to provide a method for making,by means of known making apparatus, a credit document having the above indicated main feature.

Another object of the present invention is to provide credit documents which can be exclusively used by the regular holders.

According to one aspect of the present invention, the above mentioned aim and objects,as well as yet other objects,which will become more apparent hereinafter,are achieved by a method for making credit documents and for properly detecting the regular ownership thereof,characterized in that said method comprises the steps of providing a credit document body,forming on said credit document body a biometric code for biometrically identifying a regular holder of said credit document by means of a biometric sensor and comparing means for comparing the code sensed by said biometric sensor and said biometric code formed on said credit document body.

BRIEF DESCRIPTION OF THE DRAWINGS

Further characteristics and advantages of the improved credit document according to the present invention will become more apparent hereinafter from the following detailed description of a preferred,though not exclusive embodiment thereof,which is illustrated, by way of an indicative but not limitative example, in the figures of the accompanying drawings,where:

FIGURE 1 is a schematic diagram of an apparatus for forming on a credit document body biometric code data univocally corresponding to a regular holder of said document;

FIGURE 2 is a schematic view of an apparatus for detecting the regular ownership of the document;

FIGURE 3 illustrates an apparatus operatively equivalent to those of the preceding figures and which can be used as a common data base is available for all of the credit organizations interested in such a service;

FIGURE 4 illustrates a further embodiment of an apparatus for providing a credit card with coded biometric data relating to a regular holder; and

FIGURE 5 is a schematic view illustrating a further apparatus for detecting the regular ownership of the credit card coded by the apparatus illustrated in figure 4.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

With reference to the number references of the figures of the accompanying drawings,the method for making credit documents in general according to the present invention provides for the use of a biometric sensor 1 and a store 2 for storing therein the data supplied by the sensor.

More specifically,as is shown in figure 1,in the case of an user requesting a Bancomat or P.O.S type of service,the user must allow the credit organization to record,as the agreement is made,his/her biometric personal data to be detected or sensed by the above mentioned sensor.

This data,stored in the store 2,are sent to a coder circuit 3,comprising a cryptographic coder,of any suitable type,which will sent to the central

office the coded data.

At the end of the process for forming the subject novel electronic card,the data will be recalled by a so-called badge magnetizer 4,which will record,on a set track of the badge itself,all of the biometric data obtained by masking and stored in the central store.

Thus,a badge 5 will be obtained,holding both service and recognition data,which will be delivered to the owner or user 6.

The user,in particular,as desires to use the card services,will introduce his/her card into a badge read-out device 7,associated with the Cash or P.O.S apparatus 8.

The read-out device,as it should be apparent, will be provided with a read-out head,adapted to also read out the service track bearing thereon the user's coded biometric data.

Then,the data read out by the read out device will be sent to a decoder 9 which,by an operation which is the reverse of that performed by the coder, will decode the data.

The decoded data will then be sent to a comparing circuit 10,which will wait for,for comparing purposes,those which will be sent by a local biometric sensor 11.

More specifically,the decoder 9,after having performed a first raw verification of the congruency of the data received from the read out device 7,will sent to a suitable display or TV device 12 included in the Cash or P.O.S system a call to subject to a biometric recognition the member -a hand,finger or the like of the user-to be examined by the system by means of the mentioned biometric sensor 11.

This sensor,in operation,will detect or sense all of the parameters related to the user's member being examined and will send the detected parameters to the comparator,without performing any handling operation on this data.

The comparator 10,in turn,will verify that the two data strings (derived respectively from the badge and the sensor) are mutually identical and,if yes,then it will allow the apparatus operation to proceed.

If the response is No,then the comparator will ask the user,through the display,to repeat all of the disclosed operations,starting from the read-out of the badge.

However, if, after a second and/or third attempt, there is no congruency between the data supplied by the read-out device and the data of the biometric sensor, then it can be provided that the card is not retained by the system, as at present occurs in the case of an erroneous input of the conventional secret code.

According to the present method, there are substantially stored the parameters identifying the person by means of specifically designed sensors, which are adapted to detect these parameters, and, as the system is used, the stored data string is compared with that of the data detected by the control sensor.

If the two data strings correspond, then the identity of the person can be established in an absolutely sure way, with the same approximation as that of the method used for the biometrical detection.

Each of these biometric devices is based on the fact that it is actually impossible that in the world exist two persons with the same fingerprints, or having the same volumetric pattern of the hand, of the same retina extension of the eye bottom, and so on.

In particular, as the service is supplied by banks which are already interconnected at a national level, and accordingly having a common data bank or base, then the biometric data of the clients using the service can be advantageously stored in said data base.

In this case, the data detected by the biometric sensor 1 is sent to a store 2, which, through a modem 13, is interconnected with a central unit or electronic central unit 14.

The latter will store said data and will transmit this data, by means of other modems 13, to a central file 15 of the common data base, which can be accessed by all of the banks which are recorded in the circuit of the specific proposed service.

In this connection it should be pointed out that the biometric data can also be not stored in the badge, since this data will be already residing in the electronic central unit of the emitting Institute 14, and in the common collection central unit 15.

In such a case, in fact, it is provided that as a client introduces the badge in the read-out device 7 of a Cash or P.O.S. of another Institute, then his regular identifying data will be transferred, through a store 16 and other modems 13,to a local electronic central unit 17.

The latter, after having verified that the user or client pertains to another institute, will send this data to the common data base which, after having detected the client and related bank, will feed back to the requesting Cash or P.O.S. the data string identifying said user.

Simultaneously with the read-out step in which the badge data is read-out, the client or user is requested, through the display 12, to subject to the read-out of the local biometric sensor 11, the body member analyzed during the recording step.

The data detected by this sensor will be sent to the comparing circuit 10, which will compare this data with the data sent to it from the above mentioned common data base 15.

If the result of the comparing is positive or yes, then the Cash or P.O.S. will be enabled to perform the operation; if the response is No, then the same comparator will request the client, through the above mentioned display, a novel or new read-out of the biometrically analyzed member, and then it will perform a further comparing of the detected data.

Also in this case, anyhow, it is provided, after a given number of non regular biometrical detections, to retain the badge.

In the case of making a credit card (Figure 4), the biometric identifying data, as detected by the sensor 1 and stored in the memory 2, will be sent to the coder 3 which will mask and compress this data.

The code, in the form of a number, or of an alpha-numeric word, will be sent to a punching machine 18, which will print on the credit card or badge 5', the code of the client.

In this connection it should be apparent that on the magnetic band or strip provided on this badge, in particular, it will be possible to record, by means of a suitable magnetic recorder 19, the conventional data for identifying the owner of the card.

At the payment moment (Figure 5), the client or user 6, after having submitted his/hor credit card, will be requested to subject the provided member (hand, finger or other) to a biometric test, which will be performed by means of a local sensor 11.

The data detected by this sensor will be sent to a coder 3, which, by the same method as that thereinabove disclosed, will compress and mask this data.

The data string obtained by the coder will be sent to a small printer 20, which will print it on the payment bill 21, which must be signed by the client.

The comparing between the number printed on the payment bill and the number punched on the credit card will provide the seller the certitude of the regular property of the card.

On the payment bill, as it should be apparent, will be recorded, by means of a punching or printing apparatus 22, the total of the expenses 21 made by the client.

Moreover, for a better perfomance of the service, the seller can be advantageously provided with a local electronic store 23, which, by means of a modem 23, can be periodically updated by the service institute about all of the specific data related to the lost or stolen credit cards.

From the above disclosure and the observations of the several figures of the accompanying drawings, the great functionality and facility of use characterizing the improved method for making credit documents according to the present invention will be self evident.

While the invention has been disclosed and illustrated with reference to some preferred embodiments thereof, it should be apparent that the disclosed embodiments are susceptible to several modifications and variations all of which will come within the spirit and scope of the appended claims.

Claims

1. A method for making credit documents and for properly detecting the regular ownership thereof, characterized in that said method comprises the step of providing a credit document body, forming on said credit document body a biometric code for biometrically identifying a regular holder of said credit document by means of a biometric sensor and comparing means for comparing the code sensed by said biometric sensor and said biometric code formed on said credit document body.

2. A method, according to Claim 1, characterized in that, in the case in which an user requires a service of the "Bancomat" or "P.O.S." type, said method comprises the step of detecting the biometric data of said user (fingerprint, pattern of the hand or the like) by a suitable sensor; said data, stored in a store, being sent to a coder circuit comprising a cryptographic coder, of a known and reliable type, adapted to code said data.

3. A method, according to the preceding Claims, characterized in that said method comprises the step, after having completed all of the conventional procedures for making the new electronic card, of recalling said data from a badge magnetizer, which will record, on a set track of said badge, all of the biometric data obtained by a masking step and preserved in the central store.

4. A method, according to one or more of the preceding claims, characterized in that said method comprises the step of, as the user desires a service enabled by his/her personal card, introducing said card in a badge read-out device, said badge read-out device being associated with Cash or P.O.S. apparatus, said read-out device being further provided with a read-out head also for the track provided by the service and bearing the coded biometric data.

5. A method, according to one or more of the preceding claims, characterized in that said method comprises the step of transmitting the

data read-out by said read-out device to a decoder which, by a procedure which is the reverse of that performed by said recording coder, will decodify said data, the decodified data being then sent to a comparing circuit which will compare said decoded data with the data sent to it by a local biometric sensor.

6. A method, according to one or more of the preceding claims, characterized in that said method comprises the step of causing said decoder, after a first raw verification of congruency of the data sent by said read-out device, to send to a suitable TV or display included in said Cash or P.O.S. system, an invitation to subject to a biometric detection the member (hand, or finger, or the like of the user) tested by the system by means of said local biometric sensor, said sensor detecting all of the parameters characteristic of the member being tested and sending said parameters to said comparator without further handling said parameters.

7. A method, according to one or more of the preceding claims, characterized in that said method comprises the step of causing said comparator to verify that the two data strings (respectively derived from the badge and the sensor) are mutually identical and, if they are actually identical, said comparator enabling the apparatus to operate, and, in a contrary case, that same comparator requesting the client, through the display, to repeat all of the operations.

8. A method, according to one or more of the preceding claims, characterized in that said method comprises the further step of using, as the service is offered by banks interconnected on a national level, a common data base, the biometric data of the client which use the service being advantageously stored in said data base; in this case the data detected by the biometric sensor being sent to a store interconnected, through a modem, with a central unit or electronic central unit; in this case the biometric data can also be not stored in the badge since they are already stored in the electronic center of the emitting institute and in the common data base.

9. A method, according to one or more of the preceding claims, characterized in that said method comprises the step of, in the case of making a credit card, sending the identifying biometric data detected by the sensor and stored in the store to the coder, which will mask and compress this data; the code, in a number form, or having the form of an alphanumeric expression, being sent to a punching machine adapted to punch on the credit card or badge said code.

10. A method, according to one or more of the preceding claims, characterized in that, in the case of a credit card, said method comprises the step of sending the data detected by the local sensor to a coder which, by the same method, will compress and mask said data; the thus obtained data string being sent to a small printer, which will print this data string on a payment bill to be signed by the user.

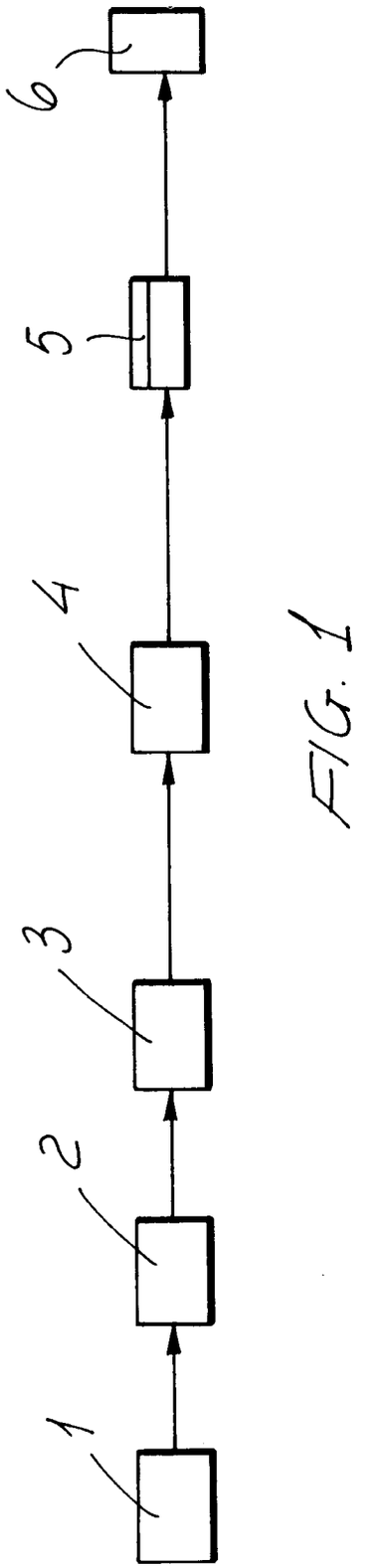

FIG. 1

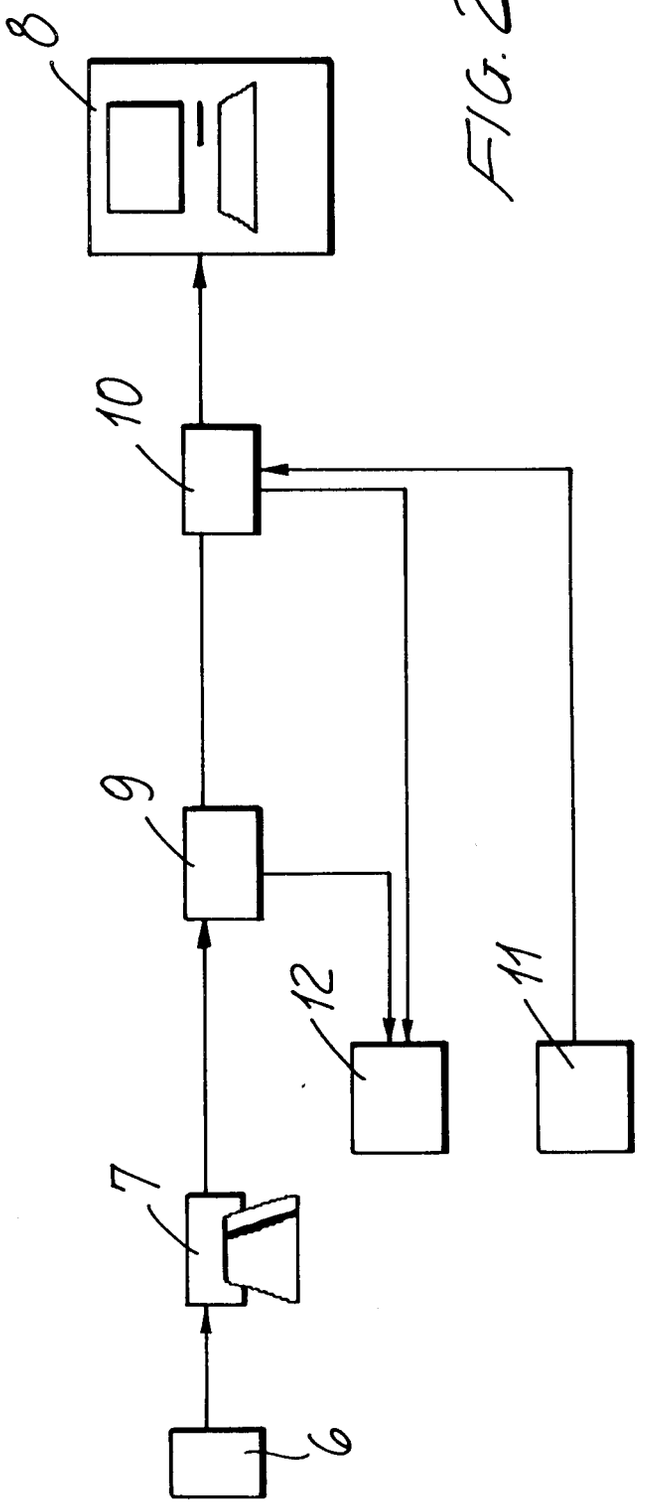

FIG. 2

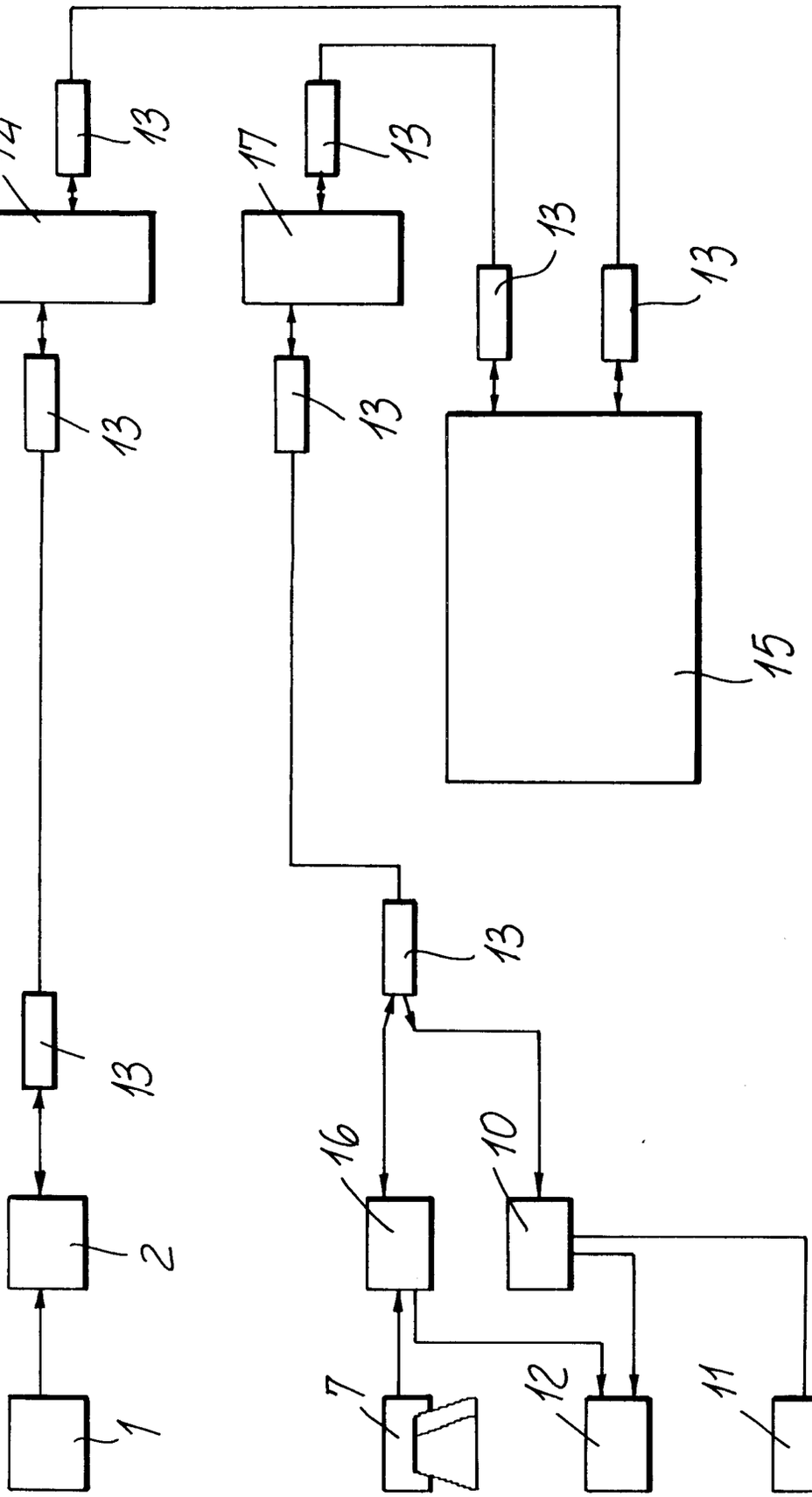

FIG. 3

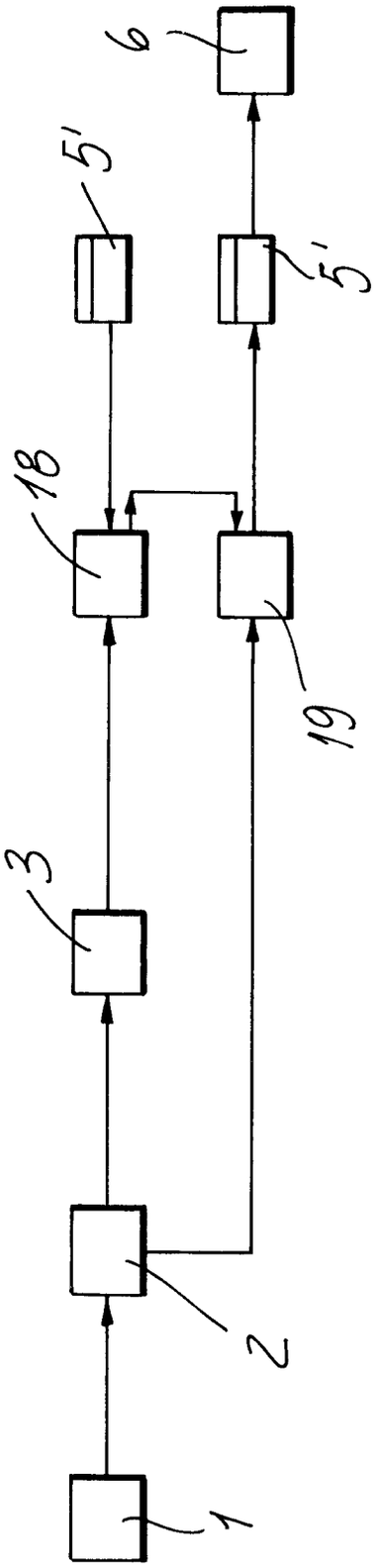

FIG. 4

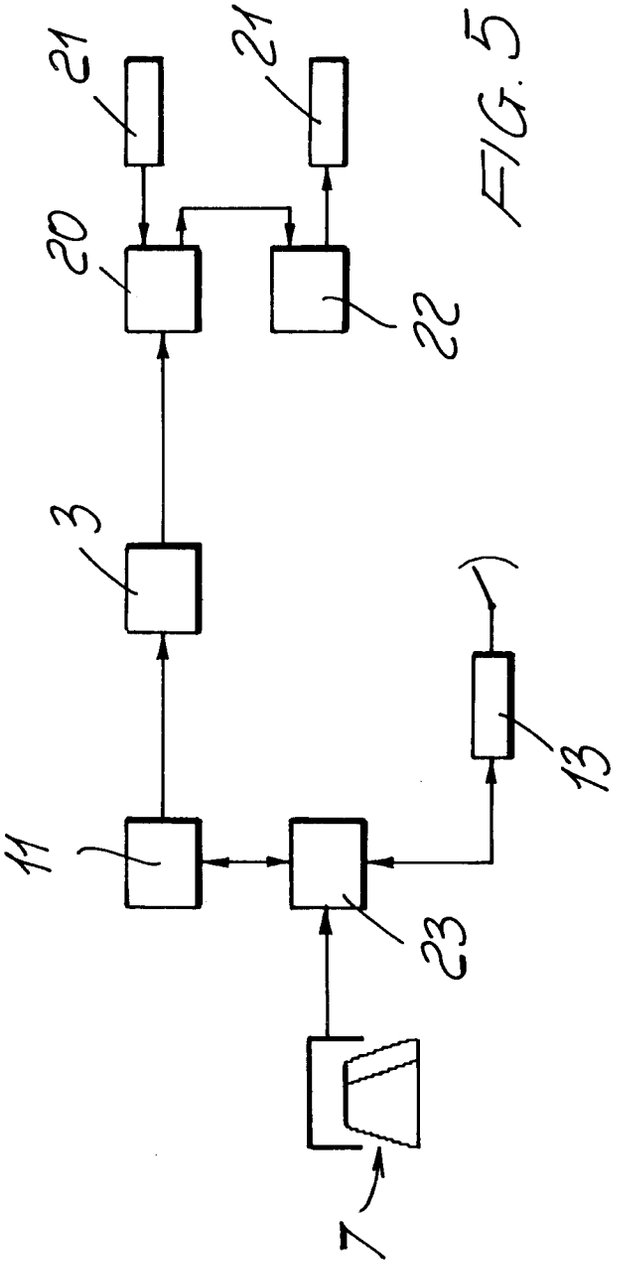

FIG. 5