SPRUSON & FERGUSON

Australia

Patents Act 1990

NOTICE OF ENTITLEMENT

I, John Gordon Hinde, of Spruson & Ferguson, St Martins Tower, 31 Market Street, Sydney, New South Wales 2000, Australia, being the patent attorney for the Applicant(s)/Nominated Person(s) in respect of Application No 66301/94 state the following:-

The Applicant(s)/Nominated Person(s) has/have entitlement from the actual inventor(s) as follows:-

The Applicant(s)/Nominated Person(s) is/are the assignee(s) of the actual inventor(s).

The Applicant(s)/Nominated Person(s) is/are entitled to rely on the application(s) listed in the Declaration under Article 8 of the PCT as follows:

The Applicant(s)/Nominated Person(s) is/are the assignee(s) of the basic applicant(s).

The basic application(s) listed on the Declaration under Article 8 of the PCT is/are the first application(s) made in a Convention country in respect of the invention.

DATED this FIFTH day of OCTOBER 1995

.....

John Gordon Hinde

IRN: 315623 INSTR CODE: 60933

13

1054P

AU9466301

(12) PATENT ABRIDGMENT (11) Document No. AU-B-66301/94
(19) AUSTRALIAN PATENT OFFICE (10) Acceptance No. 680901

(54) Title
METHOD AND APPARATUS FOR FINGERPRINTING AND AUTHENTICATING MAGNETIC MEDIA

International Patent Classification(s)
(51)[5] G06K 009/00

(21) Application No. : 66301/94 (22) Application Date : 08.04.94

(87) PCT Publication Number : WO94/24638

(30) Priority Data

(31) Number	(32) Date	(33) Country
046040	09.04.93	US UNITED STATES OF AMERICA
Not Given	04.04.94	US UNITED STATES OF AMERICA

(43) Publication Date : 08.11.94

(44) Publication Date of Accepted Application : 14.08.97

(71) Applicant(s)
WASHINGTON UNIVERSITY

(72) Inventor(s)
RONALD SCOTT INDECK; MARCEL WETTSTEIN MULLER; GEORGE LAWRENCE ENGEL; ALAN LEE HEGE

(74) Attorney or Agent
SPRUSON & FERGUSON , GPO Box 3898, SYDNEY NSW 2001

(56) Prior Art Documents
US 4985614
US 4806740
AU 17267/76 G06K 9/00

(57)

As explained throughout the specification of the subject application, "remanent noise" refers to *microstructural* noise originating from the microstructure of the magnetic medium. In contrast, a · · · · each of the citations rely on *macroscopic* noise for authenticating a magnetic medium. Because macroscopic noise does not fall within the meaning of "remanent noise" as used throughout the specification and claims, the present invention as claimed is fully patentable over the citations.

Claim

1. A device for fingerprinting an object for the later determination of its identity, said object including at least in part, a magnetic medium portion, said device having means for determining a remanent noise for said medium portion, said remanent noise comprising a fingerprint for said object, and means for recording said remanent noise for later comparison with the later determination of said remanent noise to thereby identify said object.

31. A device for authenticating an object having a fingerprint recorded, said object having a magnetic medium portion, said fingerprint comprising a remanent noise for said medium portion, said device including means for reading said recorded fingerprint, means for translating said

.../2

remanent noise from said fingerprint, means for determining a remanent noise directly from said magnetic medium portion, and means for comparing said translated remanent noise with said determined remanent noise to determine whether they match, thereby authenticating said object.

63. An object having its fingerprint recorded for the later verification of its identity, said object having a magnetic medium portion, said fingerprint comprising a remanent noise for said magnetic medium portion determined by a first read of said magnetic medium portion, and data related to said read being recorded in association with said fingerprint for later use in compensating for differences between a speed of a subsequent read and the speed of said first read.

OPI DATE 08/11/94 APPLN. ID 66301/94
AOJP DATE 22/12/94 PCT NUMBER PCT/US94/03917

AU9466301

INT

(51) International Patent Classification 5 : G06K 7/00

A1

(11) International Publication Number: WO 94/24638

(43) International Publication Date: 27 October 1994 (27.10.94)

(21) International Application Number: PCT/US94/03917

(22) International Filing Date: 8 April 1994 (08.04.94)

(30) Priority Data:
08/046,040 9 April 1993 (09.04.93) US
Not furnished 4 April 1994 (04.04.94) US

(71) Applicant: WASHINGTON UNIVERSITY [US/US]; One Brookings Drive, St. Louis, MO 63130 (US).

(72) Inventors: INDECK, Ronald, Scott; 729 Gralee Lane, Olivette, MO 63132 (US). MULLER, Marcel, Wettstein; 4954 Lindell Boulevard, St. Louis, MO 63108 (US). ENGEL, George, Lawrence; 9325 Garber Road, St. Louis, MO 63126 (US). HEGE, Alan, Lee; Apartment B, 1049 Allen Avenue, St. Louis, MO 63104 (US).

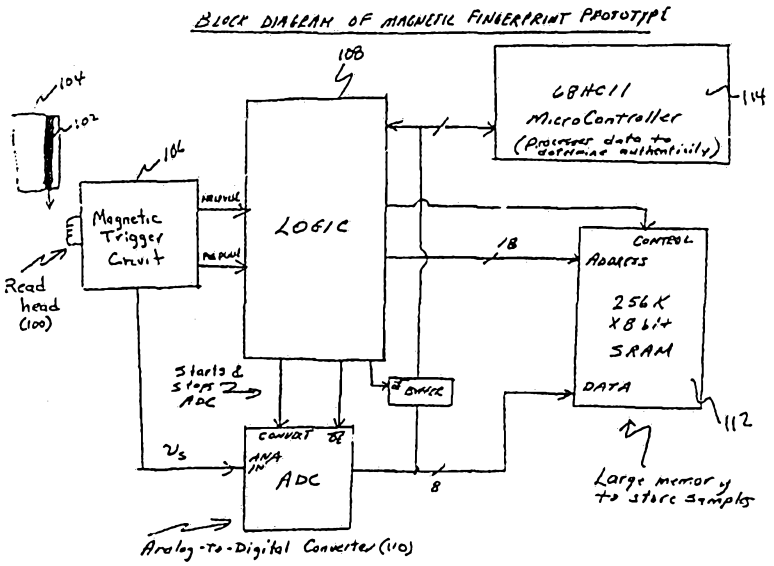
(74) Agent: HAFERKAMP, R.; Rogers, Howell & Haferkamp, Suite 1400, 7733 Forsyth Boulevard, St. Louis, MO 63105-1817 (US).

(81) Designated States: AU, BB, BG, BR, BY, CA, CZ, FI, HU, JP, KP, KR, KZ, LK, MG, MN, MW, NO, NZ, PL, PT, RO, RU, SD, SK, UA, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
With amended claims and statement.

680901

(54) Title: METHOD AND APPARATUS FOR FINGERPRINTING AND AUTHENTICATING MAGNETIC MEDIA



(57) Abstract

A method and apparatus is disclosed for determining the remanent noise in a magnetic medium (102) by DC saturation of a region thereof and measurement of the remaining DC magnetization. A conventional magnetic recording transducer may be used to determine the remanent noise. Upon determination, the remanent noise may then be digitized and recorded on the same magnetic medium to thereby "fingerprint" the magnetic medium. This "fingerprint" may then be later used to verify and authenticate (114) the magnetic medium as being an original. In such manner, any magnetic medium, or any object having an associated magnetic medium, may be "fingerprinted" including credit cards, computer programs, compact discs, videotapes, cassette tapes, etc.

METHOD AND APPARATUS FOR FINGERPRINTING AND AUTHENTICATING MAGNETIC MEDIA

Background and Summary of the Invention

The sources of noise in a readback signal from a magnetic recording medium have been investigated and identified. One of those sources includes the irregularities and defects in the microstructure of the magnetic medium itself. For many years, the noise generated from this source has been thought, as with the noise generated from other identified sources, to be random and subject only to statistical analysis for its determination. The inventors herein have recently demonstrated that this noise component is instead deterministic, i.e. is permanent and repeatable, depending entirely on the head-medium position and on the magnetic history of the medium. As confirmed by experiments conducted by the inventors herein, when the medium has had no signal writ-

AUSTRALIA PATENT OFFICE

ten on it and has been exposed only to DC fields, the observed readback signals are almost identical. The magnetic contribution to the readback signal under these conditions results from spatial variations in the medium's magnetization: magnetic domains, ripple, local fluctuations of the anisotropy field and saturation magnetization. These local properties, in turn, are affected by the morphology and magnetic properties of the individual grains which make up the domain and which do not change after deposition. Hence, the noise from a nominally uniformly magnetized region measured at a fixed position on a magnetic medium is reproducible. As shown by the inventors herein, a magnetic medium may be DC saturated and its output then measured to determine its remanent state or remanent noise. The inventors have confirmed that this remanent noise is a function of the magnetic microstructure by comparing the remanent noise after a positive DC saturation with the remanent noise after a negative DC saturation. It has been found that these wave forms are virtual "mirror images" of each other thereby demonstrating a close correlation. Similarly, other methodologies were used to confirm that the remanent noise was deterministic, repeatable, and related to the physical microstructure of the magnetic medium itself. Remanent noise arising from the permanent microstructure exhibits identifiable features characteristic of that permanent microstructure after practically any magnetic history. See *Spatial Noise Phenomena of Longitudinal Magnetic Recording Media* by Hoinville, Indeck and Muller, IEEE Transactions on Magnetics, Volume 28, No. 6, November 1992, the disclosure of which is incorporated herein by reference.

There is a long felt need in the art for a method and apparatus to identify or fingerprint various kinds of documents as well as the wide variety of prerecorded magnetic media presently being marketed and/or distribut-

ed in the United States and throughout the world. Examples of these magnetic media include those produced and sold in the entertainment industry including magneto-optic discs and tapes, cassette tapes, reel to reel tapes, videotapes, etc. Still another major market in magnetic media is the tremendous volume of computer programs routinely sold and/or distributed on floppy diskettes. Magnetic media are also used for other purposes for which it is important to be able to identify and authenticate originals including videotapes, cassette tapes, and other prerecordings on magnetic media of telephone conversations, video recordings of criminal activities, and other such investigative and documentary uses. Still another example of a need in the art for authentication and verification of magnetic media lies in the magnetic data card field. Examples of magnetic data cards include the well known credit card as well as ATM cards, debit cards, security or ID cards, mass transit cards, and even airline tickets or other vouchers which have magnetic stripes thereon for the magnetic recording of data. As well known in the art, virtually every magnetic data card has a magnetic stripe of prerecorded magnetic data which is used to record the customer's account number or some other such identifying data. Tremendous sums of money are lost annually through forgery and other fraudulent copying and use schemes which could be virtually eliminated if an apparatus and methodology could be implemented for reliably authenticating and verifying the identity of a magnetic data card prior to its being approved for its associated transaction. Still other examples extend to paper documents and the like for which there has been some specific efforts of which the inventors herein are aware.

As related in an article entitled *Novel Applications of Cryptography in Digital Communications* by Omura, IEEE Communications Magazine, May 1990, a technique is

disclosed for creating counterfeit-proof objects. As related therein, the basic idea is to measure some unique "fingerprint" of the paper and to sign (encrypt) it using the secret key of the manufacturer of, for example, a stock certificate. The fingerprint is obtained by moving a narrow intense light beam along a line on the paper and measuring the light intensity that passes through the paper. The light intensity function determined by the unique random pattern of paper fibers along the line then forms the fingerprint of the particular piece of paper. This fingerprint is then digitized and encrypted by the secret encryption function. The encrypted fingerprint is then separately printed onto the paper in digital form such as a bar code. At a later date, the authenticity of the stock certificate may be verified by using a non-secret public decryption function to decrypt the encrypted data on the paper and reconstruct the intensity function, or fingerprint, that was recorded thereon. Next, the actual intensity function of the stock certificate is measured. If this newly measured intensity function agrees with the intensity function reconstructed from the decrypted data, the document may be declared authentic. This scheme takes advantage of a well know secrecy system referred to as a public key cryptosystem. This system employs a trap door one way function. A user chooses a secret key (the trap door) and after applying the trap door one way function to the data, the procedure determines an algorithm used for decoding which is made publicly known. The trap door one way function is also used to produce the encrypted message. Then every other user can understand the original message by applying the algorithm to the cryptogram. In this system no one else can produce a publicly readable message attributable to the original user's trap door as only the user has knowledge of that algorithm. This prevents the simplistic forgery

attempt of changing the pre-recorded fingerprint to agree with a forged document's fingerprint.

Still another example of an attempt in the prior art to fingerprint or counterfeit-proof objects is shown in U.S. Patent 4,806,740. As shown therein, an object, such as a stock certificate, has deposited thereon a stripe of magnetic medium having a variable density resulting from the non-uniformity of the paper, the process of depositing the magnetic medium on the document, and the dispersion of magnetic particles within the medium. The density variations are randomly created as the magnetic medium is applied, which affords a unique document as these density variations are fixed and repeatable to identify the document. A second magnetic stripe is also applied to the document, but this magnetic stripe is comprised of a medium that is tightly specified and highly controlled in accordance with well known standards in the recording art to be part of a magnetic read/write system. In operation, the non-uniform magnetic stripe is erased, recorded by a standard recording comprised of a linear DC signal or a linear AC signal or a linear bias signal. After recording, another head senses the magnetic characteristic of the recorded magnetic stripe which is translated into a digital, machine readable format, and then separately recorded on the second magnetic stripe in a simple write function. For authentication, the stock certificate is passed under another set of heads which first reads the digitally recorded machine readable representation of the sensed noise signal and then a second set of heads reads the variable density magnetic stripe by first erasing it, recording the same standard noise function, and then sensing the output of the prerecorded noise function as it is "distorted" by the variable density magnetic stripe. If it matches the recorded representation thereof, then the document is declared to be authentic and original. Thus, with the

method of the '740 patent, a pair of magnetic stripes must be applied to the document and a specified signal (denominated as noise) must be recorded, measured, and then its output digitally recorded. Furthermore, one of the magnetic stripes must be applied in other than recording industry standard and in a random manner to ensure the randomness of the output thereof. These steps make the '740 patent method difficult and inconvenient to implement.

Yet another example of a prior art attempt to utilize a magnetic fingerprint of a magnetic medium for authenticating credit cards, documents, and the like is found in Pease et al U.S. Patent 4,985,614 issued on June 15, 1991. This '614 patent is actually quite similar in concept to the '740 patent discussed above in that it focuses on the macroscopic, hereinafter denoted "macro" variations in a magnetic medium, and their effect on an "enhancing" signal recorded thereon in one embodiment or standing alone in a second embodiment. With either embodiment, these "macro" variations are determined by reading a chosen length of approximately 2.6 inches of a magnetic stripe between 3 and 9 times (5 in the preferred embodiment) and then correlating the collected data points to "average out" the effects of head noise, electrical noise, and any other non-medium noise. This correlation results in a "representative profile" which represents the variances which would be induced by these macro effects to a signal if it were recorded on this 2.6 inch portion of magnetic stripe. If these variations are not significant enough to produce a reliable correlation, indicating a lack of significant macroscopic nonuniformities in the medium, the medium is discarded. This is an indication that the medium has been manufactured too closely to tolerance, or otherwise does not have enough macro level variation which might be present due to a manufacturer's watermark or the like, to induce reliably

detectable and repeatable variations to a recorded signal. The '614 patent also suggests that macro level noise may be enhanced by locally altering the apparent magnetic characteristics of the stripe such as by placing magnetic symbols on the substrate underlying the magnetic region, or by embossing selected regions of the magnetic material so as to physically move some amount of the material. As the noise levels measured have significant effects on the peaks of a recorded enhancing signal, a simple peak detect and hold circuit is taught as sufficient to collect the data, and a simple "comparison" of the pre-recorded "representative profile" with the presently sensed data points is taught as sufficient to determine if the medium is authentic. Therefore, not only does the '614 patent focus on the use of macro level noise, its device and methodology disclosed for implementing a macro level noise detector is believed to be incapable of reliably creating a microstructure noise level fingerprint and validating its existence at a later time in order to authenticate an original.

In accordance with one aspect of the present invention, there is provided a device for fingerprinting an object for the later determination of its identity, said object including at least in part, a magnetic medium portion, said device having means for determining a remanent noise for said medium portion, said remanent noise comprising a fingerprint for said object, and means for recording said remanent noise for later comparison with the later determination of said remanent noise to thereby identify said object.

In accordance with another aspect of the present invention, there is provided the device of claim 3 further comprising means for encrypting said remanent noise prior to recording said remanent noise by said recording means.

In accordance with another aspect of the present invention, there is provided a device for authenticating an object having a fingerprint recorded, said object having a

AUSTRALIA PATENT OFFICE

magnetic medium portion, said fingerprint comprising a remanent noise for said medium portion, said device including means for reading said recorded fingerprint, means for translating said remanent noise from said fingerprint, means for determining a remanent noise directly from said magnetic medium portion, and means for comparing said translated remanent noise with said determined remanent noise to determine whether they match, thereby authenticating said object.

In accordance with another aspect of the present invention, there is provided a method for authenticating an object, said object including at least in part a magnetic medium portion, said object having a fingerprint recorded, said fingerprint comprising a previously determined remanent noise for said medium portion, said method comprising the steps of:

determining a remanent noise directly from said medium portion,

reading said fingerprint, and

comparing said determined remanent noise with said fingerprint.

In accordance with another aspect of the present invention, there is provided a method for fingerprinting an object for the later determination of its identity, said object including at least in part a magnetic medium portion, said method comprising the steps of determining a remanent noise for said medium portion, said remanent noise comprising said fingerprint, and recording said fingerprint on said object for the later comparison thereof with the later determination of said remanent noise.

In accordance with another aspect of the present invention, there is provided a device for authenticating an object having a fingerprint recorded, said object having a magnetic medium portion, said recorded fingerprint comprising a signal corresponding to a first read of a remanent noise in said magnetic medium portion, means for determining said fingerprint by a second read of said remanent noise in said magnetic medium portion, and means

AUSTRALIA PATENT OFFICE

for comparing said recorded fingerprint with said determined fingerprint including means for compensating for differences in data obtained by said first read and said second read to determine whether said fingerprints match, thereby authenticating said object.

In accordance with another aspect of the present invention, there is provided a method for authenticating an object, said object including at least in part a magnetic medium portion having a fingerprint, said fingerprint comprising a remanent noise for said magnetic medium portion previously determined by a first read thereof, said method comprising the steps of:

determining a remanent noise directly from said magnetic medium portion by a second read thereof,

comparing said determined remanent noise with said previously determined remanent noise, and

compensating for differences in data obtained by

said first read and said second read to determine whether said fingerprints match, thereby authenticating said object.

In accordance with another aspect of the present invention, there is provided an object having its fingerprint recorded for the later verification of its identity, said object having a magnetic medium portion, said fingerprint comprising a remanent noise for said magnetic medium portion determined by a first read of said magnetic medium portion, and data related to said read being recorded in association with said fingerprint for later use in compensating for differences between a speed of a subsequent read and the speed of said first read.

In accordance with another aspect of the present invention, there is provided a security card with a fingerprint for limiting access to a controlled access environment, said security card having a magnetic medium portion, said fingerprint comprising a remanent noise for said magnetic medium portion, said security card being validated to permit access only upon a match of a subsequent

AUSTRALIAN PATENT OFFICE

determination of said fingerprint with a previously determined fingerprint.

In accordance with another aspect of the present invention, there is provided an object having its fingerprint recorded for the later verification of its identity, said object having a magnetic medium portion, said fingerprint comprising a remanent noise for said magnetic medium portion, and at least one data bit recorded on said magnetic medium portion, a value of said data bit corresponding to a location of said fingerprint.

The inventors herein have developed a method and apparatus for utilizing the unique, deterministic, remanent noise characteristic of the magnetic medium itself due to its magnetic microstructure to fingerprint not only documents, but other objects and more importantly, the magnetic medium itself so that it can be identified and authenticated. This inventive technique relies upon the discovery that the microscopic structure of the magnetic medium itself is a permanent random arrangement of microfeatures and therefore deterministic. In other words, once fabricated, the recording medium's physical microstructure remains fixed for all conventional recording processes. In particulate media, the position and orientation of each particle does not change within the binder for any application of magnetic field; in thin

film media, the microcrystalline orientations and grain boundaries of the film remain stationary during the record and reproduce processes. It is the magnetization within each of these fixed microfeatures that can be rotated or modified which forms the basis of the magnetic recording process. If a region of a magnetic medium is saturated in one direction by a large applied field, the remanent magnetization depends strongly on the microstructure of the medium. This remanent state is deterministic for any point on the recording surface. Each particle or grain in the medium is hundreds to thousands of Angstroms in dimension. Due to their small size, a small region of the magnetic surface will contain a very large number of these physical entities. While the fabrication process normally includes efforts to align these particles, there is always some dispersion of individual orientations and positions. The actual deviations will be unique to a region of the medium's surface making this orientation a signature or a "fingerprint" of that medium. To reproduce this distribution, intentionally or not, is practically impossible since this would entail a precise manipulation of the orientation of numerous particles at the submicrometer level. Thus, the orientation of a large set of particles on a specific portion of a recording surface can uniquely identify that medium. In experiments, the inventors have found that the remanent noise from a length of between about 30 micrometers and 4300 micrometers provides enough data to "fingerprint" a magnetic medium. This may be contrasted with the 66,040 micrometers (2.6 inches) of length required in the '614 patent in order to fingerprint a magnetic medium with macro noise.

In essence, the present invention is elegantly simple and adapted for implementation by conventional recording heads as are commonly found and used in virtually every read or read/write device presently utilized

by the public at large. Such examples include credit card readers, magneto-optic disc players, cassette players, VCRs and personal computers. Furthermore, a card reader may be coupled with virtually any device or process, and the card reader used as a "gatekeeper" to permit input or access only by those who can present a valid passcard for authentication. In its simplest implementation, a conventional recording head need merely DC saturate a specified portion of a magnetic medium, and then "read" or "play back" the remanent noise which remains. For convenience, the fingerprint may be obtained from the region between two recorded magnetic transitions already in place on the medium. This remanent noise, which is an analog signal, may then be digitized and recorded, in the medium itself or elsewhere, in machine readable format perhaps using a trap door function. Thusly, the magnetic medium has become "labeled" with its fingerprint. Verification or authentication of that magnetic medium is simply achieved by reversing this process except that in the more security sensitive applications the digitally recorded fingerprint must be decrypted using the publicly known key. Should the measured remanent noise match the remanent noise as recorded, the magnetic medium is authenticated.

There are many variations in utilization of the inventors' method and apparatus which expand its universe of applications. For example, some applications need not require the use of a trap door function such as, for example, when the encoded objects are not publicly distributed and instead are being identified solely for the user's purposes. One such example would be for use with inventory items.

Still another application involves the "copy protection" of mass distributed application software. Over the years, many schemes have been tried and almost uniformly abandoned for copy protecting publicly distrib-

uted diskettes of prerecorded software. This has happened for many reasons including the problem that almost all of the copy protection schemes previously implemented interfere with the running of the software on the user's computer. With the present invention, a copy protection scheme may be implemented which does not interfere with the running of the software and instead merely provides a precondition to running of what is otherwise normally written code. In its implementation, a software diskette may first instruct the computer in which it is inserted to read a fingerprint of a specified portion of the diskette and compare it with a prerecorded version of the same fingerprint. If the fingerprints match, then the software may permit the computer to further read and implement the application software stored thereon. However, if the fingerprint detected by the computer does not match that which is stored in the software, then the software itself may inhibit further reading of the program and prevent its implementation. This would absolutely prevent a user from making a copy of a program for use by someone else. This scheme may also be slightly modified as discussed in the detailed description of the preferred embodiment to permit a user to make a single archive or backup copy such that the fingerprint comparison permits the first non-matching fingerprint copy to be run but then prevents any other non-matching fingerprinted copies to run. This implementation is easily achieved and "copy protects" application software reliably, inexpensively, and requires only minor hardware changes to the massive number of computers already in consumers' hands.

Still another significant application of the present invention involves authenticating credit cards using the single magnetic stripe already implemented on most major credit cards. Again, this may be contrasted with the '614 patent which suggests that a second stripe

be added because of the required 2.6 inches of stripe length which must be dedicated to the macro fingerprint techniques. The same method would be used as explained above to measure and record the "fingerprint" of the particular magnetic stripe contained on a particular credit card and then a credit card reader would require that same fingerprint to be matched every time it is used to verify its authenticity. While there are already a large number of credit cards in circulation, these cards are routinely subject to expiration such that there is a continual replacement of these cards in the public's hands. Thus, over time the installed base of credit cards could be readily transformed to those which have been "fingerprinted".

In a variation to this application, the present invention may be coupled with a data base or processor, such as in so-called Smart Cards. These credit card-like devices actually contain, in addition to perhaps the standard credit card magnetic stripe, an on-board electronic memory and/or microprocessor. This memory or microprocessor may contain all sorts of information including money substitute data. For example, at present a large number of these smart cards are in use in Europe as pre-paid telephone cards which are pre-loaded with a monetary amount which is charged against by a pay phone. The cards are used until their pre-loaded monetary equivalent has been depleted and then they are discarded. While various security methodologies have been developed to protect against fraud, these are subject to breach. The present invention is uniquely suited as a security scheme for smart cards as it depends solely on the magnetic microstructure of the particular magnetic medium. In use, the magnetic fingerprint could be stored on the magnetic stripe, in the smart card memory (on board the card), or in a central computer. When coupled with a trap door function, no fraudulent card could be created

without access to the trap door function and every transaction could be quickly pre-authorized at a local card reader, without phoning a central clearing authority. In an extension to all credit card applications, the fingerprint data may be stored along with each transaction so that a complete record or trail is created which traces a particular card's history. Thus, the present commonly used scheme where a number of fraudulent cards are created with a correct but stolen account number could either be thwarted or effectively prosecuted.

Another level of security incorporates random placement of the fingerprint position. This might be a function of the card's number. For example, the card number modulo "P" might point the read electronics to a particular data bit around which the fingerprint will be found.

Still another significant category of applications involves utilizing the present invention in its gatekeeper function. Any system, process, machine, location, or other function to which access is desired to be restricted to only those who are authorized, the present invention provides a unique and reliable solution. In its simplest implementation, a passcard may be created with a magnetic stripe which is fingerprinted in accordance with the present invention. Although examples will be discussed in terms of utilizing a passcard, it should be understood that any magnetic medium can be similarly used in accordance with the teachings herein. As such, all other such examples and implementations are intended to be included within the present invention and shall be understood to be included within the term "passcard". This passcard may then become a personal ID card which may be used not only to control access, but also identify the particular person accessing the service, function, etc. by storing the particular magnetic fingerprint of the card being used. Numerous examples may be readily

considered. For example, access to a computer network through a remote terminal may be controlled utilizing a passcard of the present invention. This would be implemented through the use of a diskette which may be readily inserted in any floppy disk drive which could authenticate the fingerprint on the diskette. Alternatively, an inexpensive card reader, adapted to read a passcard, could be utilized as well. Many other applications would utilize the modified card reader. For example, a bank teller may be assigned a passcard which could then be used to track all of the transactions entered by the teller and thereby more reliably guard against teller fraud. The myriad of identification cards utilized by businesses, health plans, universities, hospitals, and other organizations or facilities could readily adopt and use a passcard to more securely identify and preauthorize the users of its services, facilities, etc. Not only would existing uses be readily amenable to replacement with the passcard of the present invention, but other new services and systems could be implemented because of the high degree of security provided by the present invention. This may include home shopping and pay-per-view video. This may well lead to the creation of national data bases, national ID cards, and other more universal implementations of credit cards or passcards. This is especially true if a system utilizes not only the magnetic fingerprint of a particular passcard, but also utilizes a secondary security check such as a picture ID, human fingerprint, hologram (presently imprinted on credit cards), or other such methodology which would thereby render the passcard system virtually impregnable. With such security, individuals may be more willing to turn over such detailed personal financial and health information as would make these systems feasible.

While the principal advantages and features of the invention have been described above, and a number of

examples given, a greater understanding of the invention may be attained by referring to the drawings and the description of the preferred embodiment which follow.

Brief Description of the Drawings

Figure 1 is a magnified representative depiction of the microscopic structure of a region of magnetic medium;

Figure 2 is a magnified depiction of several tracks of a magnetic medium having microscopic structure representatively shown thereon;

Figure 3 is a partial view of a track of magnetic media having its fingerprint recorded thereon in machine readable code;

Figure 4 depicts three conventional recording heads and a magnetic medium traveling thereunder;

Figure 5 is a view of a credit card having fingerprint data encoded thereon for reading by a credit card reader;

Figure 6 depicts a personal computer with a computer diskette for insertion in a floppy disk drive thereof;

Figure 7 is a perspective view of a magneto-optic disc player with a magneto-optic disc in its tray;

Figure 8 is a cassette player depicting a cassette tape for play therein;

Figure 9 is a perspective view of a VCR with a tape ready for insertion;

Figure 10 is a block diagram of a magnetic fingerprint verification circuit;

Figure 11 is a block diagram of the magnetic trigger circuit shown in Figure 10;

Figure 12 is a schematic diagram of an implementation of the present invention utilizing a PC;

Figure 13 is a schematic diagram of the memory utilized in the implementation of Figure 12;

Figure 14 is a schematic diagram of the trigger circuits utilized in the implementation of Figure 12;

Figure 15 is a schematic diagram of the preamp circuits utilized in the implementation of Figure 12;

Figure 16 is a block diagram of a magnetic fingerprint verification circuit set up for implementation in an IC;

Figure 17 is a schematic diagram of a correlation circuit utilizing single bit data streams;

No Figure 18;

Figure 19 is a schematic diagram of an active differentiator;

Figure 20 is a schematic diagram of the threshold generator;

No Figure 21;

Figure 22 is a schematic diagram of the ADC reference generator;

Figure 23 is a schematic diagram of a gain circuit;

Figure 24 is a plot from a read of a magnetic credit card stripe;

Figure 25 is an enlarged view of the encircled portion of the waveform in Figure 24; and

Figure 26 is a waveform giving the correlation of two fingerprints.

Detailed Description of the Preferred Embodiment

As shown in Figure 1, a region of magnetic medium 20 is built up with a plurality of microcrystalline structures 22 in a random pattern. This microcrystalline structure 22 is comprised of particles or grains varying from hundreds to thousands of Angstroms in diameter. The view of Figure 1 is greatly enlarged and magnified in order to depict this physical microstructure. As shown in Figure 2, this microcrystalline structure extends throughout the magnetic medium even though the magnetic

medium 24 shown in Figure 2 may be itself comprised of tracks 26, 28, 30 as well known in the art. Although shown schematically as separate regions, the fingerprint can be obtained from any portion of the medium 24.

Referring now to Figures 3 and 4, a plurality of conventional recording heads 32, 34, 36 are shown mounted in a head transport 37 with a traveling magnetic medium 38 controllably driven past recording heads 32, 34, 36 all as is well known in the art. These recording heads 32-36 may be any magnetic transducer or magneto-optic transducer head, as known in the art. Recording heads 32-36 are all connected to electronic circuitry 39, as well known in the art, to control and read their input and output and to further process signals for playback or other use. Although only three heads 32, 34, 36 are being shown in Figure 4, it will be well understood to those of ordinary skill in the art that a plurality of recording heads of any number may just as easily be provided and, as taught herein, may be required in order to effect the purposes of the present invention. As shown in Figure 3, the magnetic "fingerprint" at a specified region 40 of a thin film magnetic medium or tape 42, shown representationally in Figure 3 as a thin film tape, may be recorded at a second position 44 on said thin film magnetic medium or tape 42 in a digitized, machine readable code 46 or the like.

As their preferred embodiment, the inventors have utilized a methodology for reading or determining the remanent microstructural noise characteristic of the region 40 of the magnetic medium which is being "fingerprinted". Preferably, this region 40 is on the order of several tens to hundreds of micrometers. This region is then DC saturated and then subjected to a "read" step for determining the remanent noise produced thereby.

While this is the preferred embodiment, it should be understood that the fingerprint is always there,

whether the medium has been recorded over or not. Therefore, it is not strictly necessary that the specified portion of medium containing the fingerprint be DC saturated, or DC saturated in the same polarity in order to obtain the fingerprint. Instead, it is only important that the remanent noise be determined in a manner which facilitates its being correlated successfully with the earlier determined remanent noise.

If this information is obtained in a "single shot" measurement, then the results will obviously include both electronics noise as well as the remanent noise attributable to the particles' orientation. As this "noise" or "remanent noise" is electronically determined as an analog signal, this information may then be digitized and recorded with about a hundred to two hundred digital bits of information as may be representationally shown as code 46 in Figure 3. In experiments, the inventors have made multiple measurements and averaged their results in order to eliminate the electronics noise present in the measured wave form. However, there was observed a high correlation coefficient when the two sets of data, i.e. single shot and averaged, were compared thereby demonstrating that a single shot reading could readily be used in comparison to an averaged set of data in commercial application. The normalized cross correlation coefficient r is used where

$$r = \frac{\sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N} (x_i - \bar{x})^2 \sum_{i=1}^{N} (y_i - \bar{y})^2}}$$

as explained by the inventors in their earlier published article mentioned above.

In order to recover or measure the "fingerprint" or remanent noise, the process is similarly repeated and, when comparing two single shot wave forms, a smaller

correlation therebetween was experienced. However, the correlation experienced with two single shot wave forms was significant and clearly demonstrated this method's feasibility for commercial application as well.

As shown in Figure 24, the portion of the signal used for fingerprinting is very small with respect to the rest of the recorded signal. As shown in Figure 25, the encircled portion or fingerprint from Figure 24 may be amplified to show in greater detail the waveform. In Figure 26, a correlation using the present invention produces a definable "peak" which verifies the existence of the fingerprint in the medium.

As shown in Figure 5, a practical implementation for the subject invention includes a magnetic data card 48 which has a magnetic stripe 50 thereon with magnetic stripe 50 being encoded with a code 52 representative of a fingerprint of a region 54 of magnetic stripe 50. Thus, as the magnetic data card 48 is "swiped" through a card reader 56, the card reader 56 may read the code 52 to determine the stored fingerprint data, read the fingerprint at region 54 of the magnetic stripe 50, compare them for a match, and if they match then authenticate magnetic data card 48 as a genuine card which has not been altered and which may be approved. Alternatively, the fingerprint need not be stored on the card but may instead be stored centrally, as in a data base elsewhere.

As shown in Figure 10, a schematic block diagram for a magnetic fingerprint prototype includes a read head 100 for reading the magnetic medium 102 which may be on a credit card or passcard 104 as previously described. A magnetic trigger circuit 106 (including the gain circuit shown in Figure 23) pulses on a logic element 108 which activates an analog to digital converter 110 (including a reference voltage generator shown in Figure 22) to convert the output from read head 100, V_s, into a stream of digital data which is stored in a memory 112. A

microcontroller 114 then processes the data and compares it with the original fingerprint in order to authenticate the credit card or passcard 104. The magnetic trigger circuit 106 is shown in greater detail in Figure 11. It includes a preamp 116 (shown in greater detail in Figure 15) which amplifies the output from read head 100 to produce, through a set of analog comparators (see Figure 14) with thresholds produced by threshold generators (see Figure 20), a positive pulse output 118 and a negative pulse output 120, as shown by the timing graph in the lower half of Figure 11. The logic 108 may be implemented as shown in Figure 12 by connection to an IBM PC through connector 122. A memory element 124 is shown in greater detail in Figure 13, trigger circuits 126 are more completely shown in Figure 14, and preamp circuits 128 are shown in Figure 15. A block diagram 130 for a magnetic fingerprint device is shown in Figure 16 which is arranged for implementation in a custom integrated circuit.

In many of the implementations of the present invention, the speed at which the magnetic medium is propelled past a recording head, card reader, or the like is fixed both when the magnetic fingerprint is first measured and, later, when the magnetic fingerprint is read in order to verify or authenticate its validity. Some examples of this fixed reading speed include the speed at which a floppy disk is rotated in a computer, the speed at which a VCR tape is played, the speed at which an audio cassette tape is played, the motorized reading of an ATM card, etc. This is even true for certain credit card applications where motorized card readers could be implemented. However, there are also other applications for which a controlled speed cannot be expected. Perhaps the most prevalent situation known today is the widely used credit card readers which require a retail clerk to "swipe" the card through a reading track.

For those situations wherein the speed of the magnetic medium is variable, or different from when the fingerprint was first determined, the inventors have developed a number of methodologies to ensure that data corresponding to the magnetic fingerprint are captured and used in the verification process. This helps eliminate improper rejections of valid credit cards, passcards, and the like. For clarity, these various methodologies will now be explained with respect to a credit card having a magnetic stripe. However, it should be understood that these methodologies are equally applicable to any application wherein the speed of the magnetic medium is variable or potentially variable from that of the original fingerprinting step.

With the magnetic fingerprint whose block diagram is shown in Figure 10, a series of data points, perhaps 150, are taken between the two trigger pulses recorded in the magnetic medium. As shown with the magnetic trigger circuit of Figure 11, the signal "POS PULSE" becomes active when the "center" of a sufficiently large positive going pulse is detected. Similarly, the signal "NEG PULSE" is active when a sufficiently large negative going pulse is detected. The derivative of the incoming signal is taken using an active differentiator (shown in greater detail in Figure 19) in order to locate the center of the pulse. By locating the center of the pulse, the distance between the center of the pulses which define the fingerprint area is thus fixed and represents a distance which is reliably ascertainable every time the credit card is swiped through a credit card reader. A level sensitive detection is also performed but this is only to help guard against false trigger events. The A to D converter samples at a fixed rate such as F_{s1}. Thus, the spacing between samples is delta x_1 where delta x_1 is equal to V_1 (velocity of the credit card) divided by F_{s1} (the sampling rate). If the sampling frequency F_{s1} is a few hundred

kHz, then delta x_1 is on the order of one micron. The number of samples taken, P (perhaps 150), is counted and may be recorded on the credit card as the fingerprint. In order to improve the reliability, several readings of the magnetic fingerprint may be made and then averaged in order to eliminate the effects of head noise, electronic circuit noise, and any other noise other than the magnetic microstructure noise of the magnetic medium. This completes the process of determining the fingerprint for a credit card.

When the card is in use, and its fingerprint is desired to be authenticated, it is necessary to sample the same region of the magnetic medium of the card which was sampled at the time of its fingerprinting. Furthermore, the distance between sample points must be the same as it was when the card was fingerprinted and, in our example, this distance is delta x_1. Although it is desired for this to be exactly the same, the inventors have found that some variance, up to a few percent, may be acceptable. The sampling interval is determined both by the sampling frequency of the A to D converter and the velocity at which the credit card moves past the read head. For manual card reading applications, the vast majority presently in use, retail store keepers are virtually assured to swipe the cards at different rates through the card readers. One solution for obtaining samples at the same intervals as the original sample interval is to greatly oversample. In other words, a sampling rate is chosen which is much greater than F_{61}. This creates a new sampling interval delta x_2 which produces many more samples, perhaps 100 times more, than were taken in the original fingerprinting process. In other words, instead of 150 samples, 15,000 samples may be taken. This requires that only every Mth sample be utilized in order to provide the same data set. M may be chosen as the ratio of Q/P where P is the number of samples taken between the two triggering pulses at the time

of fingerprinting and Q is the number of samples taken at the point of sale using an oversampling frequency F_{s2}. Since the distance between the trigger events does not change, and the ratio of F_{s1} to F_{s2} is known, the velocity of the card as it is swiped at the retail store location compared to its velocity at the time of fingerprinting may be readily determined. With this oversampling technique, it may be readily shown mathematically that oversampling by a factor of approximately 100 will result in an effective sampling interval at the point of sale which will be within 2% of the original sampling interval for velocities which are as much as five times greater than the velocity used at the time that the fingerprint was determined. If necessary, an even greater oversampling rate would accommodate even larger velocity ratios.

The work by the inventors in prototyping the present invention indicate that a digital word size as small as three bits for encoding the value of the fingerprint samples may be sufficient to obtain acceptable results using the proposed correlation analysis technique. This small word size suggests that a custom integrated circuit (IC) may be designed to conduct this correlation. It is well known in the art (for example see the literature on sigma-delta conversion) that n-bit words at a rate r_1 can be constructed from a one-bit data stream provided that the data rate of the one-bit data stream is significantly higher than the rate r_1. In its simplest form, the word length can be increased by one bit for every factor of four in the oversampling rate. Moreover, it is highly likely that in the case of the proposed correlation technique it might not be necessary to construct the n-bit data word. If that is the case, performing the correlations on a one-bit data stream is trivial. For the case of one-bit data, and signals with a zero mean (such as with magnetic medium noise), the

correlation coefficient r is given by the following expression

$$r = \sum_{i=0}^{N-1} x_i \, y_i$$

Therefore, this correlation analysis can be performed by using a simple up/down counter 132 as shown in Figure 17. As shown therein, the read head 100 has its output amplified by a preamplifier 116 which feeds a high sampling rate analog comparator 134 for the x_i input into logic gate 136. The original fingerprint data, in a one-bit data stream, is input in synchronism such that the logic gate 136 output goes positive when the bits match and negative when they don't. The output of the up/down counter 132 is compared against some threshold which, if in excess of the threshold indicates a match with the original fingerprint.

Just as it is possible to take a one-bit data stream at a high rate and construct an n-bit word at a lower rate, the inverse is also feasible. In other words, at the time of creation, the magnetic medium to be fingerprinted could be sampled with a four-bit A to D converter, for example. The fingerprint data can then be stored in four-bit words. At the point of authentication, the four-bit data samples could be translated into a one-bit data stream at the higher rate, such as is implemented in recent model CD players. This four-bit data stream is then correlated with the one-bit data stream emanating from the analog comparator 134.

Still another methodology to ensure the capture of data samples corresponding to those used during the original fingerprinting process involves, essentially, measuring the velocity of the credit card and adjusting the sampling rate to match that velocity. More exactly, two transitions or other fiduciary mark may be placed on the

card which are a fixed distance D apart. The time it takes for the card to be pulled from the first transition to the second transition defines the velocity that the card is being pulled through the reader. The sampling rate may then be adjusted to match that velocity which relies on the assumption that the velocity that the card will travel for the second interval will match that of the first interval. As these distances are only a few hundred microns, this assumption is reliable. This technique does not require any oversampling which therefore minimizes the amount of memory required to store the data points collected during the verification or card read step. In implementing this approach, a phase locked loop may be utilized where the input frequency is divided by a factor M and the feedback loop is divided by a factor N such that N over M times $F_{reference}$ equals F_s (sampling frequency). The factors M and N may be chosen depending upon the other parameters of the system, such as the sample size, expected sampling frequency, distance D, etc. As noted, this technique provides the advantage of eliminating oversampling which reduces the required memory. It does suffer from a disadvantage in that a velocity measurement must be made over a very small physical region, several hundred microns, which may present accuracy problems. Also, this does increase the amount of magnetic stripe which must be dedicated to the fingerprinting technique of the present invention although even with this doubling in length, still a minute fraction of the magnetic stripe of a credit card is being used.

As mentioned previously, credit card readers which are motorized, or which otherwise standardize the velocity at which the card is pulled through the reader could be used to eliminate this sampling and matching problem. Furthermore, it is possible to combine several of the methodologies to thereby form a hybrid methodology which might provide the best results. For example, the credit

card reader might be designed to match the sampling interval which, as explained above, ideally eliminates the requirement for oversampling. However, oversampling may also be used in conjunction with interval matching to ensure that variations may be corrected for.

As shown in Figure 6, a computer 58 has a floppy disk drive 60 for reading floppy diskettes 62, all as is well known in the art. As still another implementation of the inventors' device, the software recorded on floppy diskette 62 may first require that the floppy disk drive 60 read a designated region of the magnetic medium comprising floppy diskette 62 to determine its fingerprint, compare that fingerprint with the fingerprint stored in the program resident in floppy diskette 62, and if they match permit computer 58 to run the application program stored on floppy diskette 62. If the program stored on floppy diskette 62 is not the original floppy diskette, then the application program will not be run as the measured fingerprint will not match the fingerprint stored in data contained in the floppy diskette 62. In a variation of this implementation, a single, archival, copy of floppy diskette 62 may be permitted should the program resident in floppy diskette 62 allow it to run if the measured fingerprint is either a match with the fingerprint stored, or is its first non-match. The non-match fingerprint would then also be stored in the application software resident in floppy diskette 62 such that the program would recognize the original floppy diskette 62 and a second floppy diskette as used by a user to create this backup, archival, copy.

In still another implementation of the present invention, a magneto-optic disc player 64 has a disc 66 placed in its tray 68 and ready for play upon retraction of tray 68. However, disc 66 may have its fingerprint stored to match the disc medium. Should magneto-optic disc player 64 have the appropriate circuitry for precon-

ditioning play of disc 66 with a comparison of the measured and recorded fingerprints, unauthorized copying of disc 66 may be prevented. Similarly, any taped copies made from disc 66 would necessarily have the incorrect fingerprint stored therein and its subsequent play would also be prohibited should the tape playback unit have an appropriate circuit for preconditioning play based on matching stored and measured fingerprints.

As shown in Figure 8, still another implementation of the invention includes measuring and storing the appropriate fingerprint on a cassette or digital tape 70, with a cassette tape player 72 having the necessary circuitry for measuring and comparing the recorded and measured fingerprints to pre-condition play, as explained above.

In still another implementation of the present invention, as shown in Figure 9 a VCR 74 has a VCR tape 76 ready for insertion therein. Using the present invention, a fingerprint can readily be measured and encoded onto the VCR tape for comparison by appropriate circuitry contained within VCR 74. Thus, if appropriately configured, the VCR would not play back a tape unless it was authentic or original.

There are various changes and modifications which may be made to the invention as would be apparent to those skilled in the art. However, these changes or modifications are included in the teaching of the disclosure, and it is intended that the invention be limited only by the scope of the claims appended hereto.

The claims defining the invention are as follows:

1. A device for fingerprinting an object for the later determination of its identity, said object including at least in part, a magnetic medium portion, said device having means for determining a remanent noise for said medium portion, said remanent noise comprising a fingerprint for said object, and means for recording said remanent noise for later comparison with the later determination of said remanent noise to thereby identify said object.

2. The device of claim 1 wherein said recording means has means for recording said fingerprint on said object.

3. The device of claim 2 wherein said recording means includes means for recording said remanent noise in said magnetic medium portion in machine readable form.

4. The device of claim 3 further comprising means for encrypting said remanent noise prior to recording said remanent noise by said recording means.

5. The device of claim 4 wherein said object is a magnetic data card, and said magnetic medium portion is a magnetic stripe on said magnetic data card.

6. The device of claim 5 wherein said remanent noise is encrypted with a trap door function.

7. The device of claim 5 wherein said object is a computer diskette, and said magnetic medium portion comprises a portion of said computer diskette.

8. The device of claim 7 wherein said remanent noise is encrypted with a trap door function.

9. The device of claim 5 wherein said object is a magneto-optic disc, and said magnetic medium portion comprises a portion of said magneto-optic disc.

10. The device of claim 9 wherein said remanent noise is encrypted with a trap door function.

11. The device of claim 5 wherein said object is a magnetic recording tape, and said magnetic medium portion comprises a portion of said magnetic recording tape.

12. The device of claim 11 wherein said remanent noise is encrypted with a trap door function.

AUSTRALIAN PATENT OFFICE

13. The device of claim 2 wherein said magnetic medium portion comprises a label affixed to said object.

14. An object having its fingerprint recorded for the later verification of its identity, said object having a magnetic medium portion, said fingerprint comprising a remanent noise for said magnetic medium portion.

15. The object of claim 14 wherein said fingerprint is recorded on said object.

16. The object of claim 15 wherein said remanent noise is recorded in said magnetic medium portion in machine readable form.

17. The object of claim 16 wherein said recorded remanent noise is encrypted.

18. The object of claim 14 wherein said object is a magnetic data card, and said magnetic medium portion is a magnetic stripe on said magnetic data card.

19. The object of claim 18 wherein said remanent noise is encrypted with a trap door function.

20. The object of claim 14 wherein said object is a computer diskette, and said magnetic medium portion comprises a portion of said computer diskette.

21. The object of claim 20 wherein said remanent noise is encrypted with a trap door function.

22. The object of claim 14 wherein said object is a magneto-optic disc, and said magnetic medium portion comprises a portion of said magneto-optic disc.

23. The object of claim 22 wherein said remanent noise is encrypted with a trap door function.

24. The object of claim 14 wherein said object is a magnetic recording tape, and said magnetic medium portion comprises a portion of said magnetic recording tape.

25. The object of claim 24 wherein said remanent noise is encrypted with a trap door function.

26. The object of claim 14 wherein said magnetic medium portion comprises a label affixed to said object.

27. The device of claim 1 wherein said determining means includes means for DC saturating a region of said magnetic medium and means for reading a residual

AUSTRALIAN PATENT OFFICE

magnetization over said region, said residual magnetization comprising said remanent noise.

28. The device of claim 27 wherein said region comprises a linear portion extending between about 30 micrometers and about 4300 micrometers.

29. The device of claim 27 wherein said determining means further comprises means for averaging a plurality of residual magnetization readings, said average comprising said fingerprint.

30. The device of claim 1 wherein said determining means comprises a conventional magnetic recording head.

31. A device for authenticating an object having a fingerprint recorded, said object having a magnetic medium portion, said fingerprint comprising a remanent noise for said medium portion, said device including means for reading said recorded fingerprint, means for translating said remanent noise from said fingerprint, means for determining a remanent noise directly from said magnetic medium portion, and means for comparing said translated remanent noise with said determined remanent noise to determine whether they match, thereby authenticating said object.

32. The device of claim 31 wherein said object has its fingerprint recorded thereon.

33. The device of claim 31 wherein said fingerprint is recorded in said magnetic medium portion in machine readable form.

34. The device of claim 33 wherein said fingerprint is encrypted, and said translation means includes means for de-crypting said fingerprint.

35. The device of claim 34 wherein said object is a magnetic data card, said magnetic medium portion is a magnetic stripe on said magnetic data card.

36. The device of claim 35 wherein said remanent noise is encrypted with a trap door function.

37. The device of claim 31 wherein said object is a computer diskette, and said magnetic medium portion comprises a portion of said computer diskette.

38. The device of claim 37 wherein said remanent noise is encrypted with a trap door function.

AUSTRALIA PATENT OFFICE

39. The device of claim 31 wherein said object is a magneto-optic disc, and said magnetic medium portion comprises a portion of said magneto-optic disc.

40. The device of claim 39 wherein said remanent noise is encrypted with a trap door function.

41. The device of claim 31 wherein said object is a magnetic recording tape, and said magnetic medium portion comprises a portion of said magnetic recording tape.

42. The device of claim 41 wherein said remanent noise is encrypted with a trap door function.

43. The device of claim 31 wherein said magnetic medium portion comprises a label affixed to said object.

44. A method for authenticating an object, said object including at least in part a magnetic medium portion, said object having a fingerprint recorded, said fingerprint comprising a previously determined remanent noise for said medium portion, said method comprising the steps of:

determining a remanent noise directly from said medium portion,

reading said fingerprint, and

comparing said determined remanent noise with said fingerprint.

45. The method of claim 44 wherein said fingerprint comprises a machine readable representation of said previously determined remanent noise, and the step of reading includes the step of reading said fingerprint with a machine.

46. The method of claim 45 wherein said fingerprint comprises an encrypted representation of said previously determined remanent noise, and further comprising the step of de-crypting said fingerprint.

47. A method for fingerprinting an object for the later determination of its identity, said object including at least in part a magnetic medium portion, said method comprising the steps of determining a remanent noise for said medium portion, said remanent noise comprising said fingerprint, and recording said fingerprint on said object

AUSTRALIA PATENT OFFICE

for the later comparison thereof with the later determination of said remanent noise.

48. The method of claim 47 further comprising the step of encrypting said fingerprint prior to recording .

49. A device for authenticating an object having a fingerprint recorded, said object having a magnetic medium portion, said recorded fingerprint comprising a signal corresponding to a first read of a remanent noise in said magnetic medium portion, means for determining said fingerprint by a second read of said remanent noise in said magnetic medium portion, and means for comparing said recorded fingerprint with said determined fingerprint including means for compensating for differences in data obtained by said first read and said second read to determine whether said fingerprints match, thereby authenticating said object.

50. The device of claim 49 wherein said compensating means includes means for compensating for differences between a speed at which each of said first read and said second read is performed.

51. The device of claim 50 wherein said speed compensation means includes means for adjusting a sampling rate at which said second read is performed.

52. The device of claim 51 wherein said adjusting means includes means for measuring the speed of said second read and comparing it with the speed of said first read.

53. The device of claim 50 wherein said speed compensation means includes means for oversampling said remanent noise during at least said second read.

54. The device of claim 53 wherein said speed compensation means includes means for adjusting a rate of said oversampling.

55. The device of claim 50 wherein each of said recorded and determined fingerprints comprises a digital sample of said remanent noise, and wherein said speed compensation means includes means for creating for said second read a digital sample approximately 100 times larger than the digital sample of said first read.

AUSTRALIA PATENT OFFICE

56. A method for authenticating an object, said object including at least in part a magnetic medium portion having a fingerprint, said fingerprint comprising a remanent noise for said magnetic medium portion previously determined by a first read thereof, said method comprising the steps of:

determining a remanent noise directly from said magnetic medium portion by a second read thereof,

comparing said determined remanent noise with said previously determined remanent noise, and

compensating for differences in data obtained by

said first read and said second read to determine whether said fingerprints match, thereby authenticating said object.

57. The method of claim 56 wherein the step of compensating further includes the step of compensating for differences between a speed at which each of said first read and said second read is performed.

58. The method of claim 57 wherein the step of speed compensating further includes the step of adjusting a sampling rate at which said second read is performed.

59. The method of claim 58 wherein the step of adjusting includes the steps of measuring the speed of said second read and comparing it with the speed of said first read.

60. The method of claim 57 wherein the step of speed compensating further includes the step of oversampling said remanent noise during at least said second read.

61. The method of claim 60 wherein the step of speed compensating further includes the step of adjusting a rate of oversampling.

62. The method of claim 57 wherein each of said previously determined remanent noise and said determined remanent noise comprises a digital sample of said remanent noise, and wherein the step of speed compensating further comprises the step of creating for said second read a digital sample approximately 100 times larger than the digital sample of said first read.

AUSTRALIA PATENT OFFICE

63. An object having its fingerprint recorded for the later verification of its identity, said object having a magnetic medium portion, said fingerprint comprising a remanent noise for said magnetic medium portion determined by a first read of said magnetic medium portion, and data related to said read being recorded in association with said fingerprint for later use in compensating for differences between a speed of a subsequent read and the speed of said first read.

64. The object of claim 63 further comprising a plurality of spaced timing marks on said magnetic medium portion so that a speed of said magnetic medium portion may be determined during a read.

65. A security card with a fingerprint for limiting access to a controlled access environment, said security card having a magnetic medium portion, said fingerprint comprising a remanent noise for said magnetic medium portion, said security card being validated to permit access only upon a match of a subsequent determination of said fingerprint with a previously determined fingerprint.

66. The security card of claim 65 further comprising a data bit recorded on said magnetic medium portion, a value of said data bit corresponding to a placement of said fingerprint on said magnetic medium portion.

67. The security card of claim 66 wherein said fingerprint is randomly located on said magnetic medium portion.

68. An object having its fingerprint recorded for the later verification of its identity, said object having a magnetic medium portion, said fingerprint comprising a remanent noise for said magnetic medium portion, and at least one data bit recorded on said magnetic medium portion, a value of said data bit corresponding to a location of said fingerprint.

69. The object of claim 68 wherein said fingerprint is recorded on said magnetic medium portion, said data bit thereby pointing to a location on said magnetic medium portion.

AUSTRALIA PATENT OFFICE

70. The object of claim 69 wherein said fingerprint is randomly located on said magnetic medium portion.

71. A device for fingerprinting an object, substantially as herein described with reference to Figs. 10 and 11.

72. A device for fingerprinting an object, substantially as herein described with reference to Figs. 12, 13, 14 and 15.

73. A device for fingerprinting an object, substantially as herein described with reference to Fig. 16.

74. A method of authenticating an object, substantially as herein described with reference to Figs. 10 and 11.

75. A method of authenticating an object, substantially as herein described with reference to Figs. 12, 13, 14 and 15.

76. A method of authenticating an object, substantially as herein described with reference to Fig. 16.

DATED this Fourteenth Day of May 1997

Washington University

Patent Attorneys for the Applicant

SPRUSON & FERGUSON

AUSTRALIA PATENT OFFICE

FIG. 1.

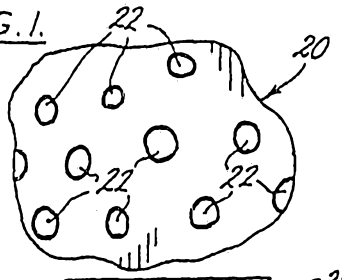


FIG. 2.

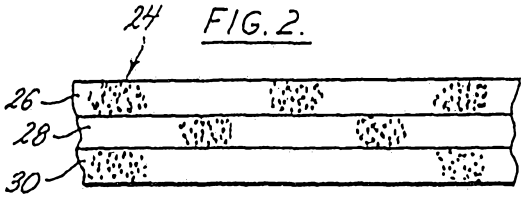


FIG. 4.

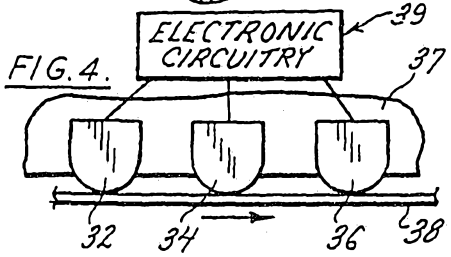
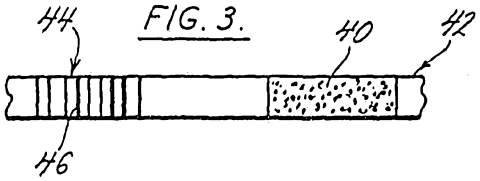


FIG. 3.



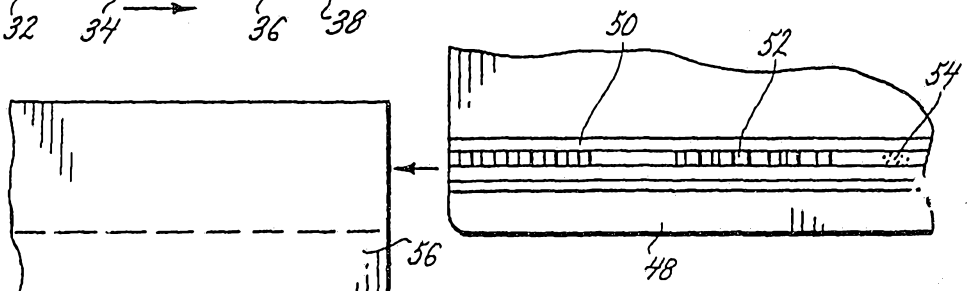
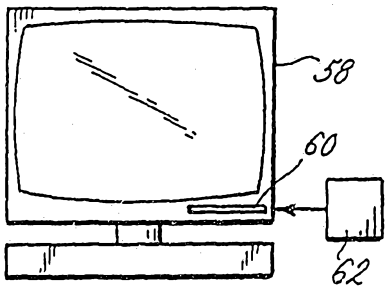


FIG. 5.



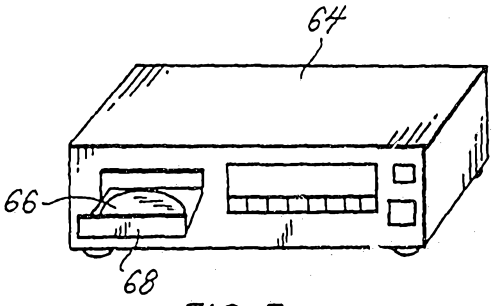


FIG. 7.

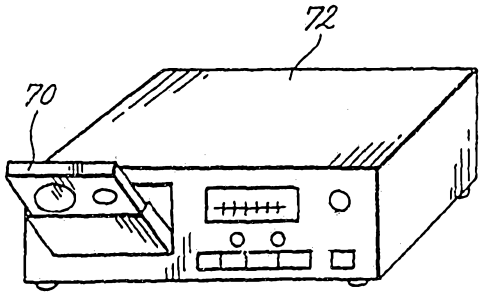


FIG. 8.

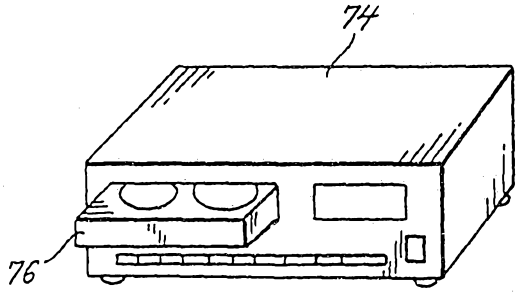


FIG. 9.

BLOCK DIAGRAM OF MAGNETIC FINGERPRINT PROTOTYPE

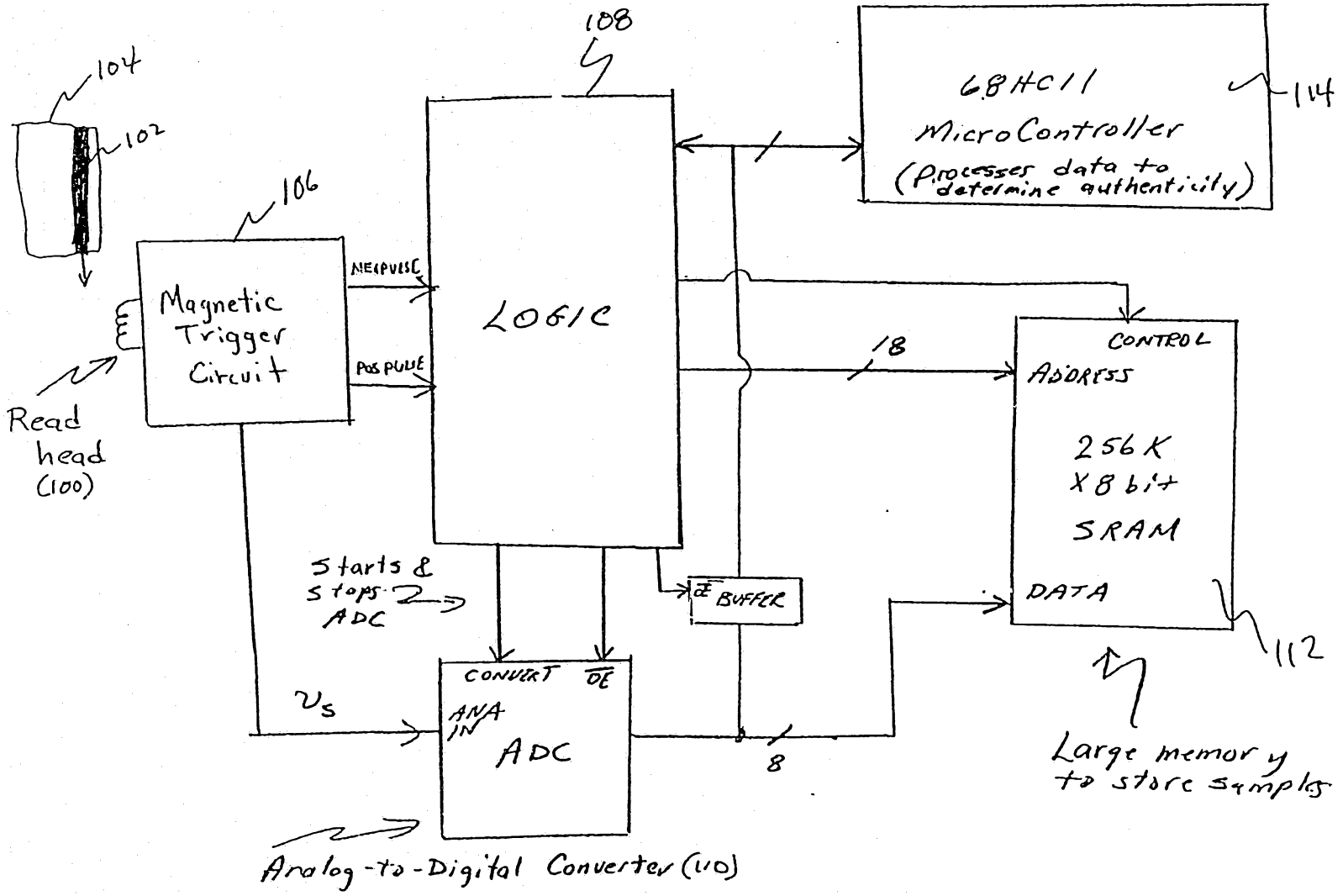
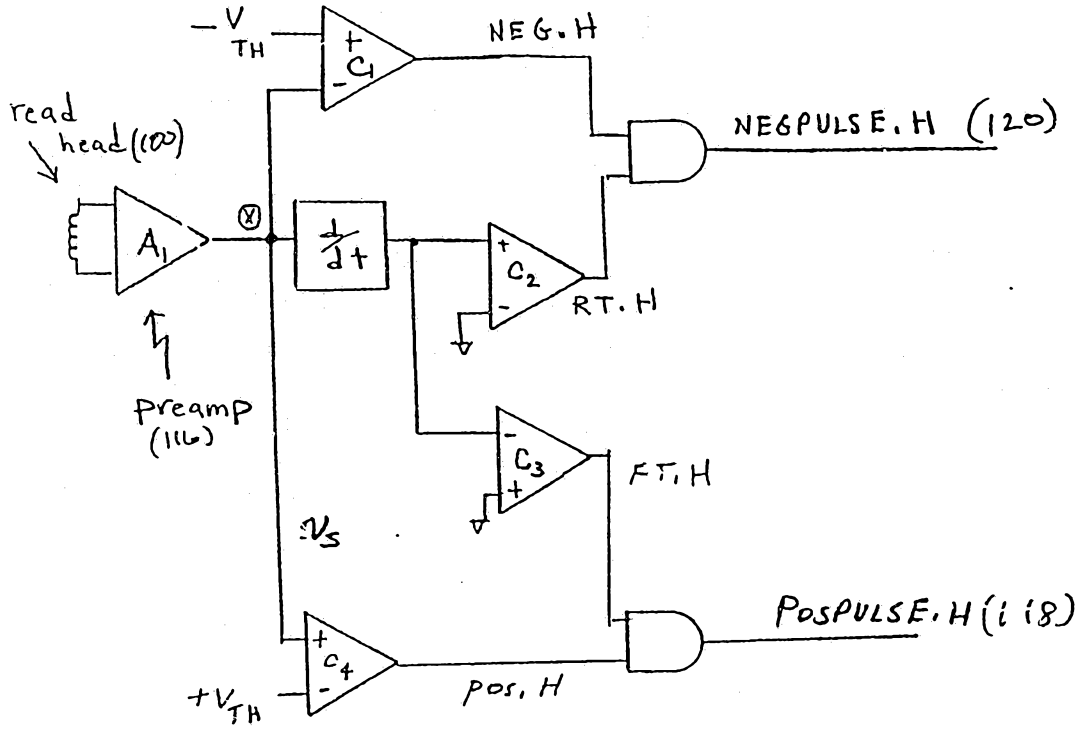
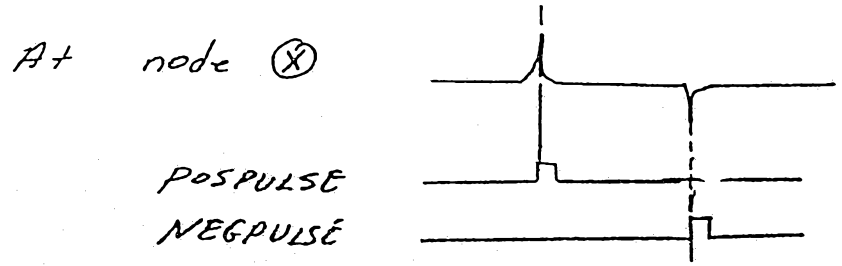


Fig 10

Magnetic Trigger Circuit





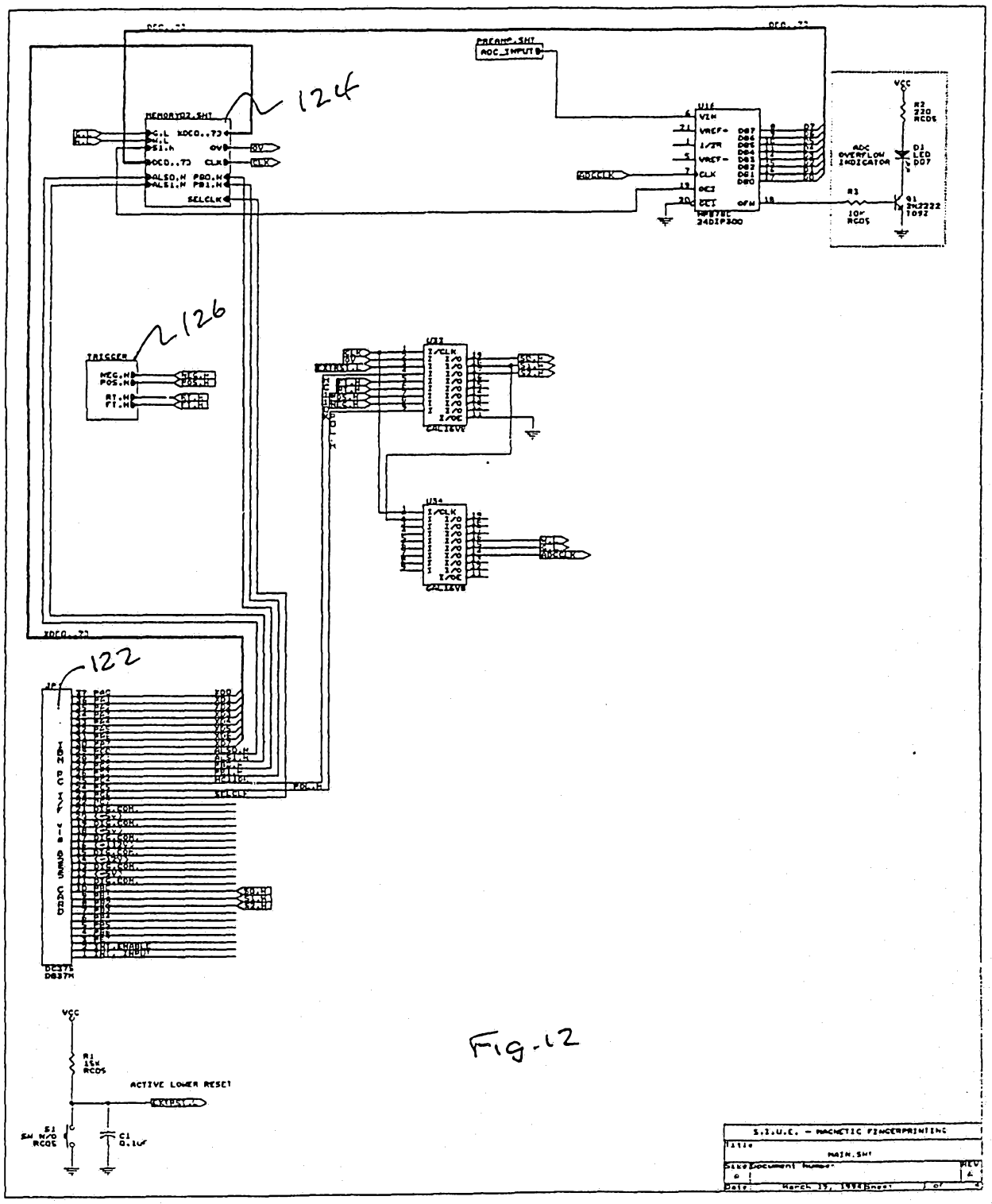
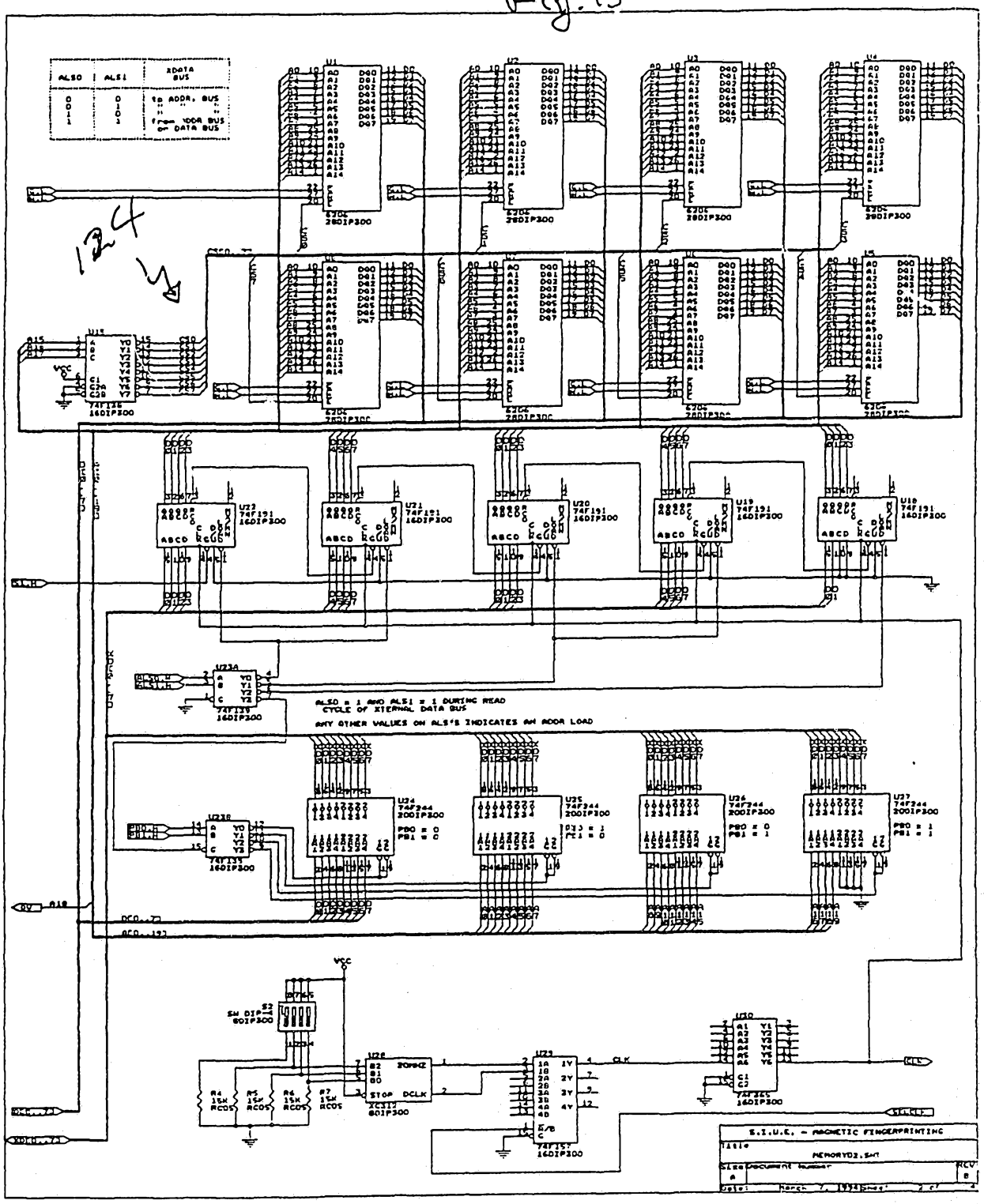

124
126
122
ACTIVE LOWER RESET
S.I.U.E. - MAGNETIC FINGERPRINTING
MAIN.SHT

Fig. 12

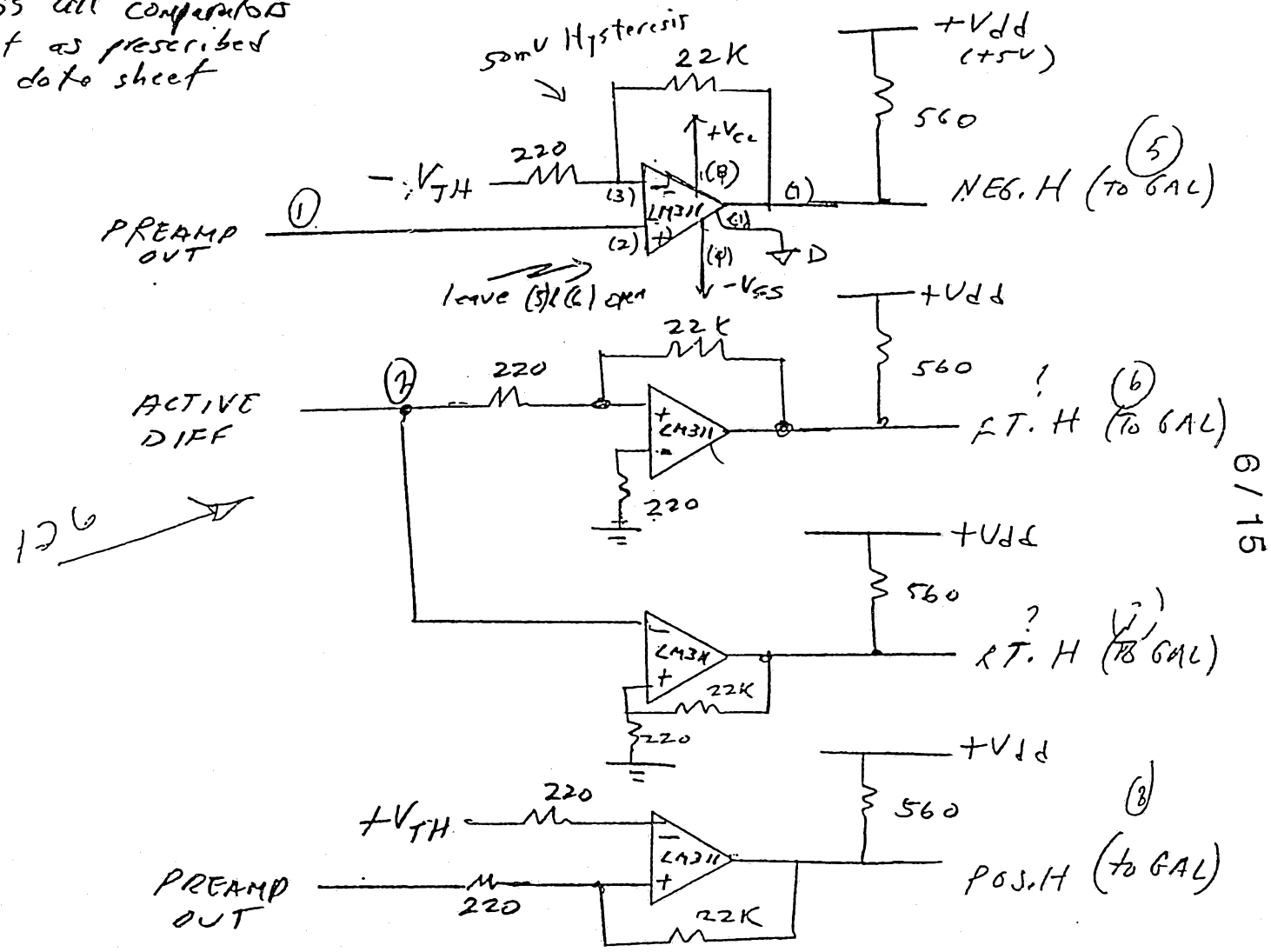
Fig. 13


ALSO | ALS1 | XDATA BUS
0 | 0 | to ADDR. BUS
0 | 1 | "
1 | 0 | "
1 | 1 | from XDATA BUS or DATA BUS
124
ALSO = 1 AND ALS1 = 1 DURING READ CYCLE OF XTERNAL DATA BUS
ANY OTHER VALUES ON ALS'S INDICATES AN ADDR LOAD
S.I.U.C. - MAGNETIC FINGERPRINTING
MEMORY02.SCH

TRIGGER CKT

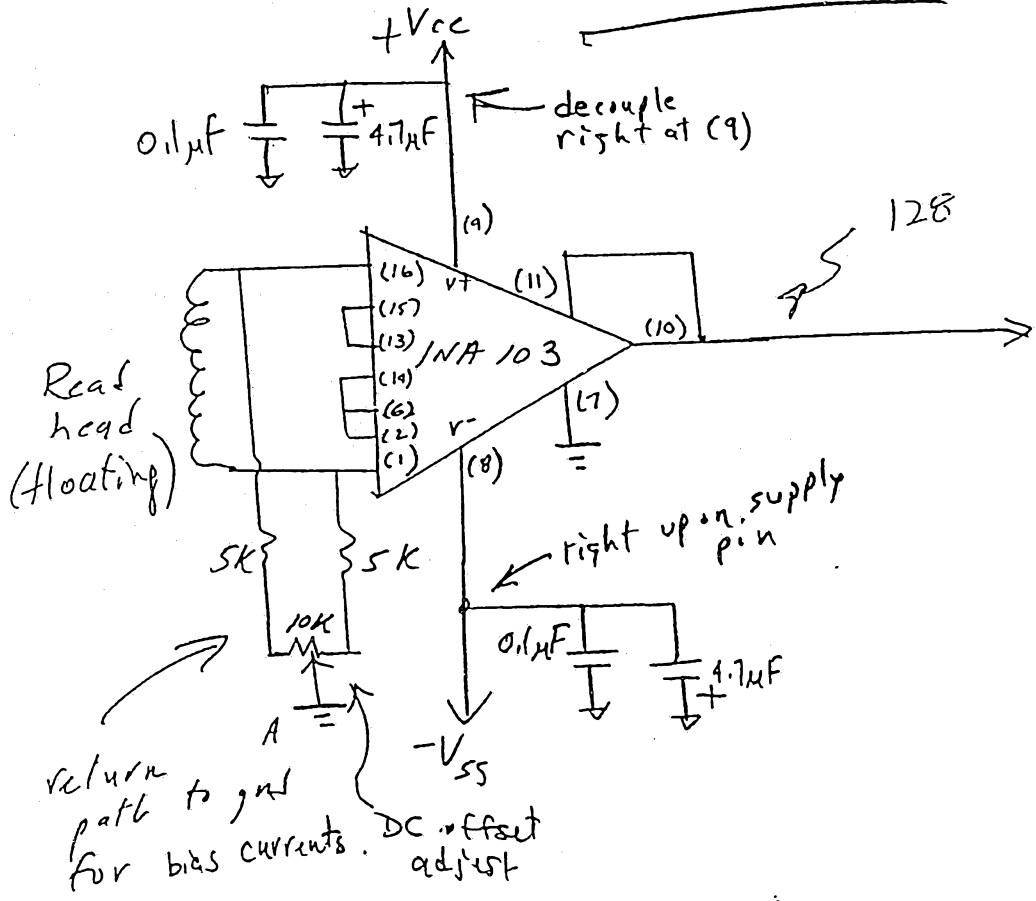
Fig. 14

Bypass all comparators
Layout as prescribed
in data sheet



PREAMP

Fig. ~~15~~ 15



Use suggested layout in data sheet!

Gain of ~x100

Very Good CMRR

Read head connected to preamp using twisted pair shielded cable.
Ground shield at preamp gnd

IC Solution

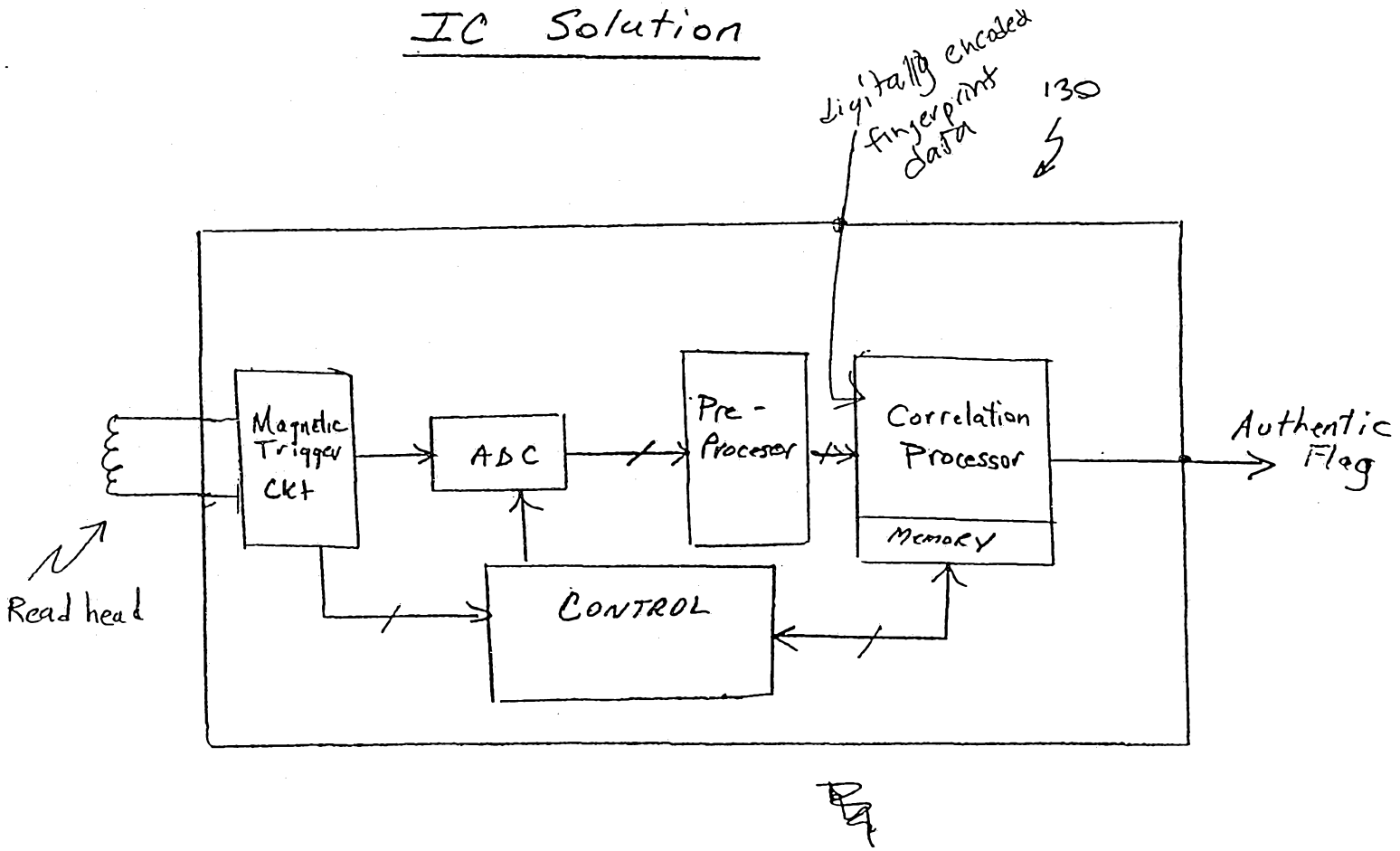


Fig. 16.

Figure 16

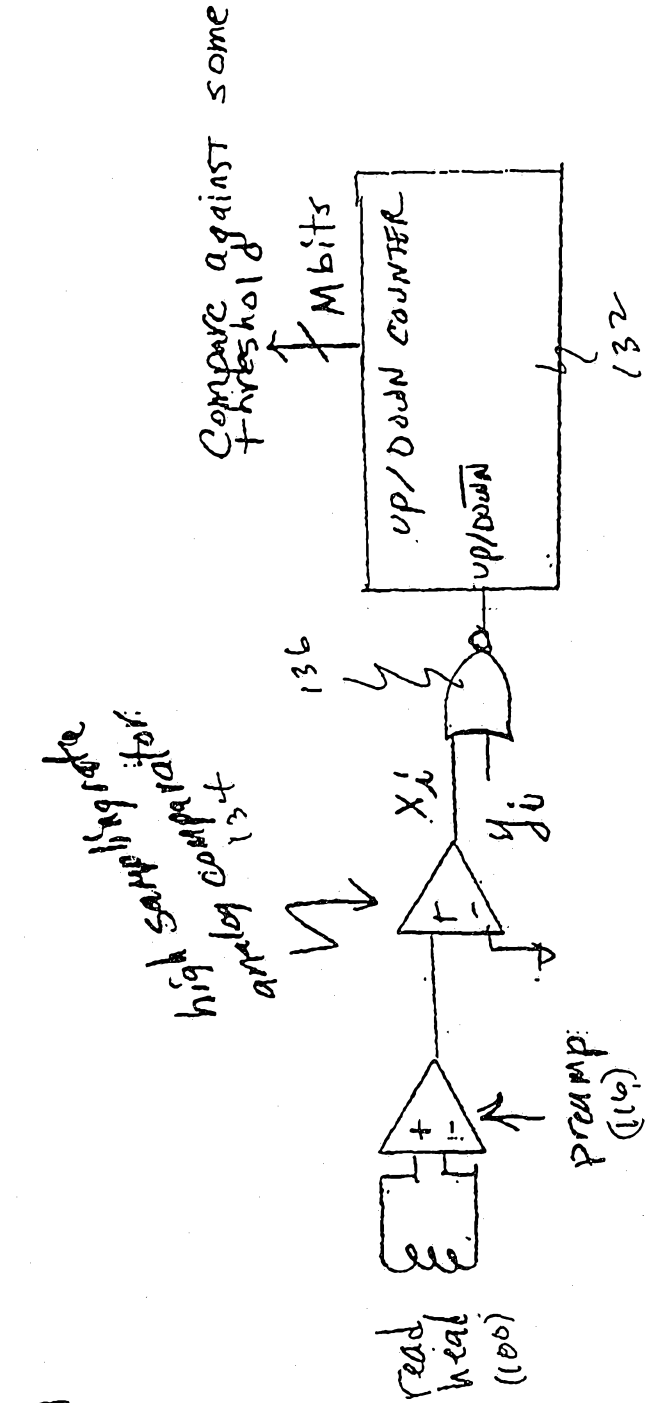

Compare against some threshold
M bits
up/down counter
up/down
132
136
high sampling rate analog comparator
134
Xi
Yi
read head (100)
preamp (110)

Fig. 7

ACTIVE DIFFERENTIATOR

Fig. 19

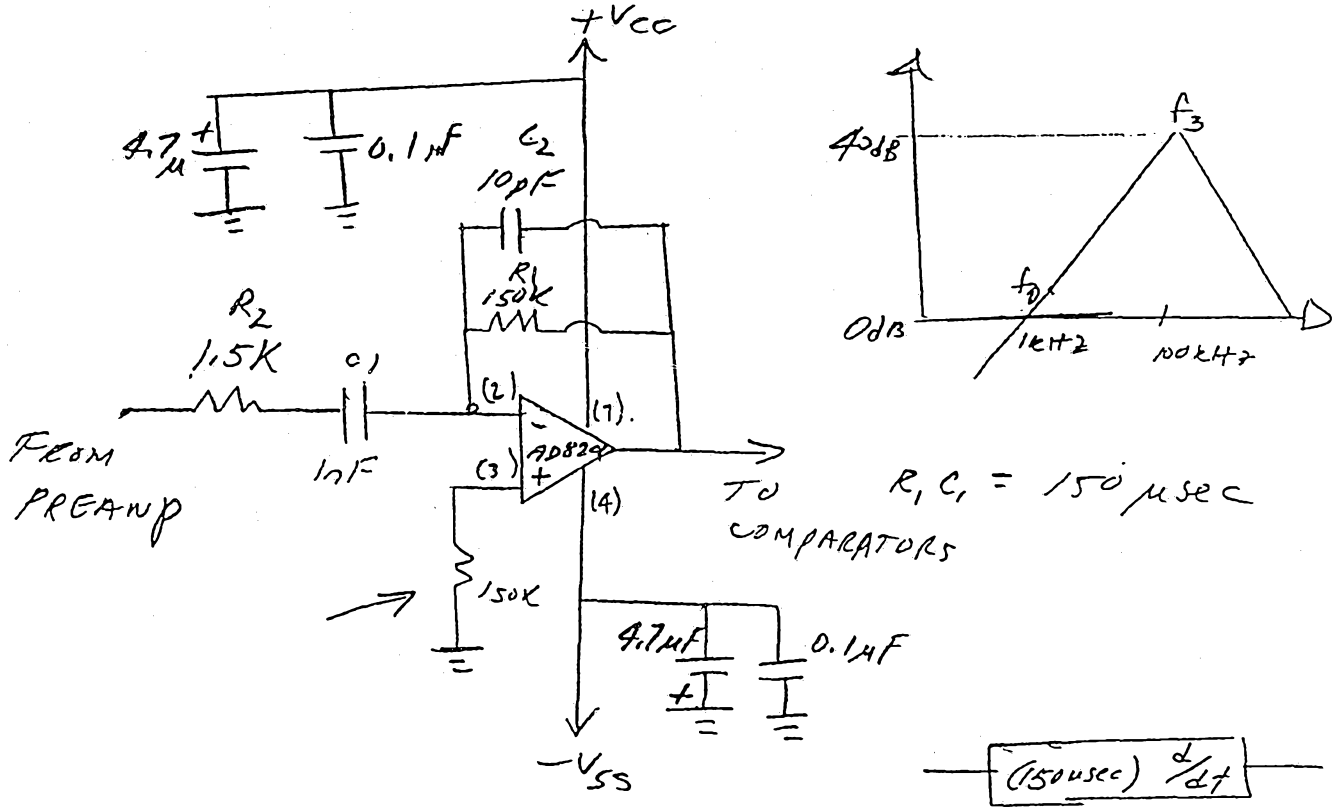


Fig. 20

THRESHOLD GENERATORS

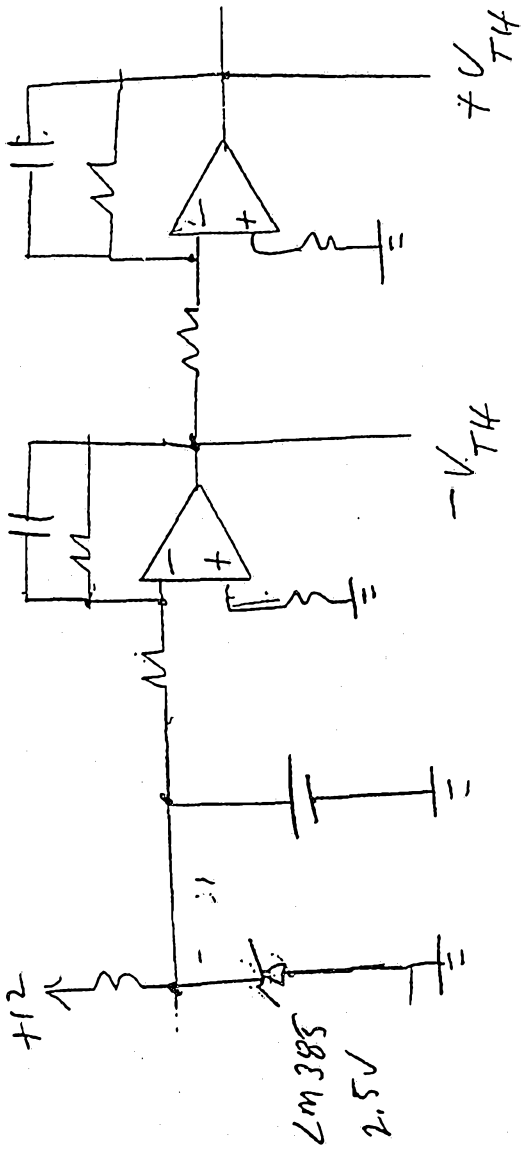


Fig. 22

ADC Reference Generator

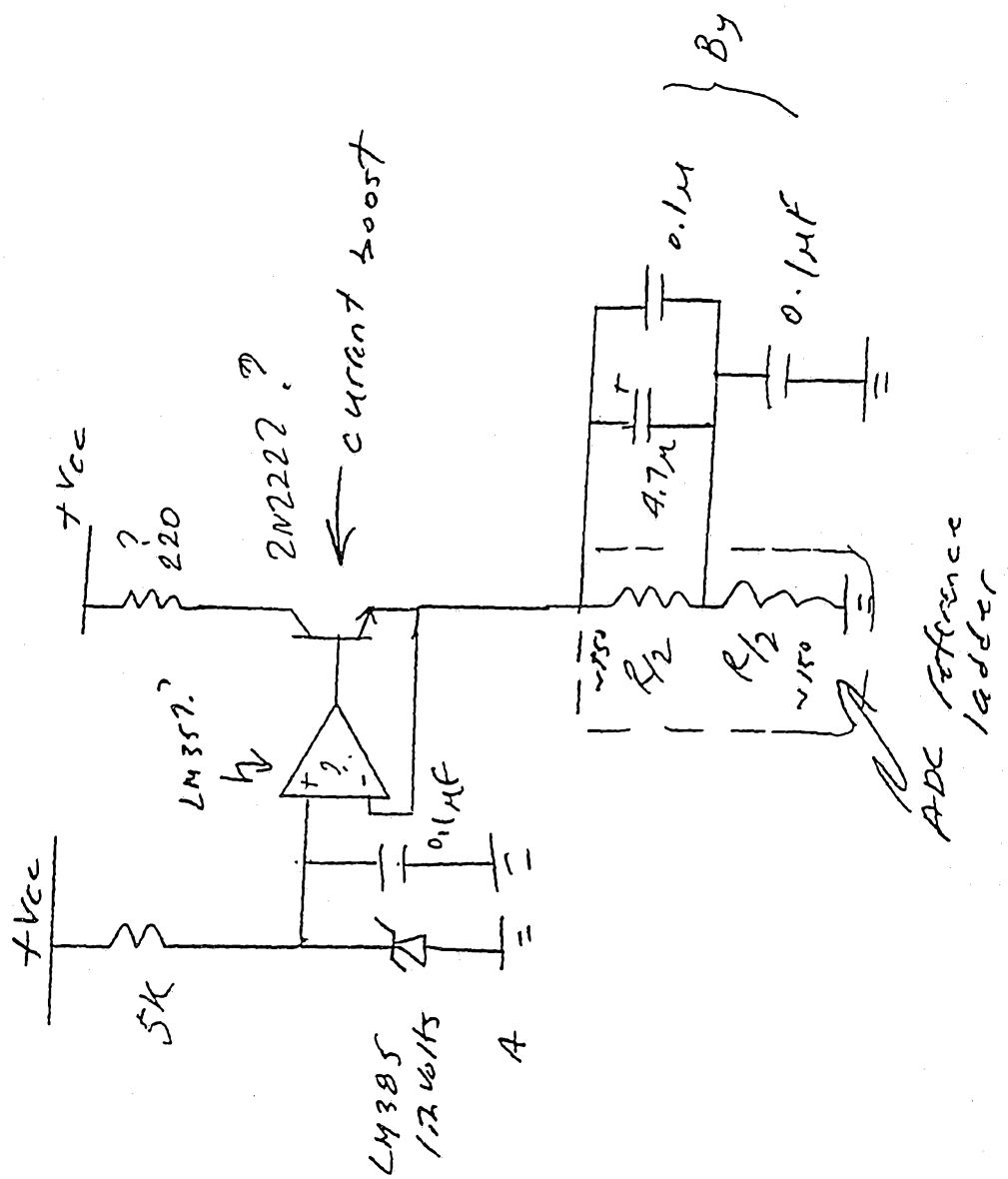
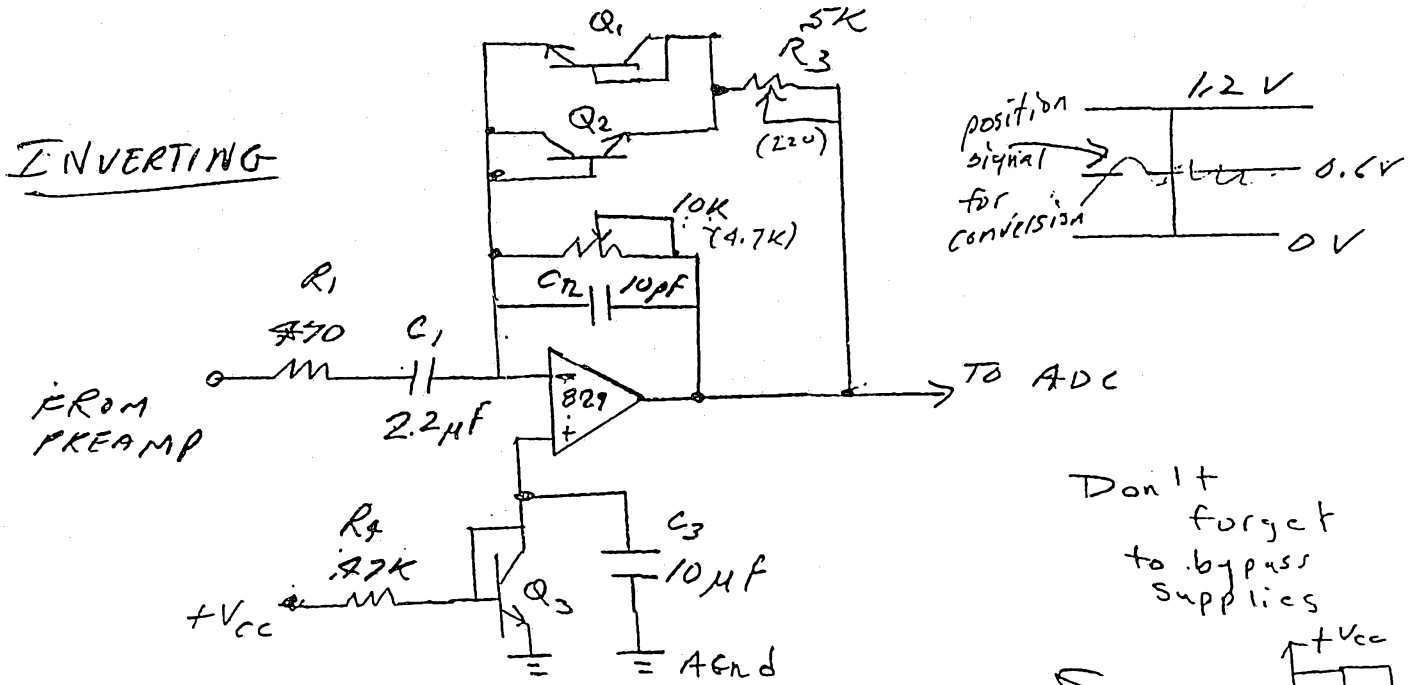
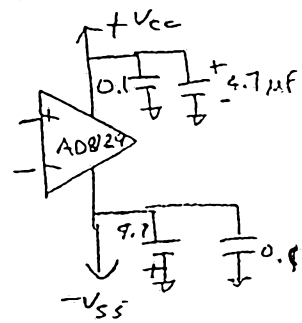


Fig 23

INVERTING



Don't forget to bypass supplies

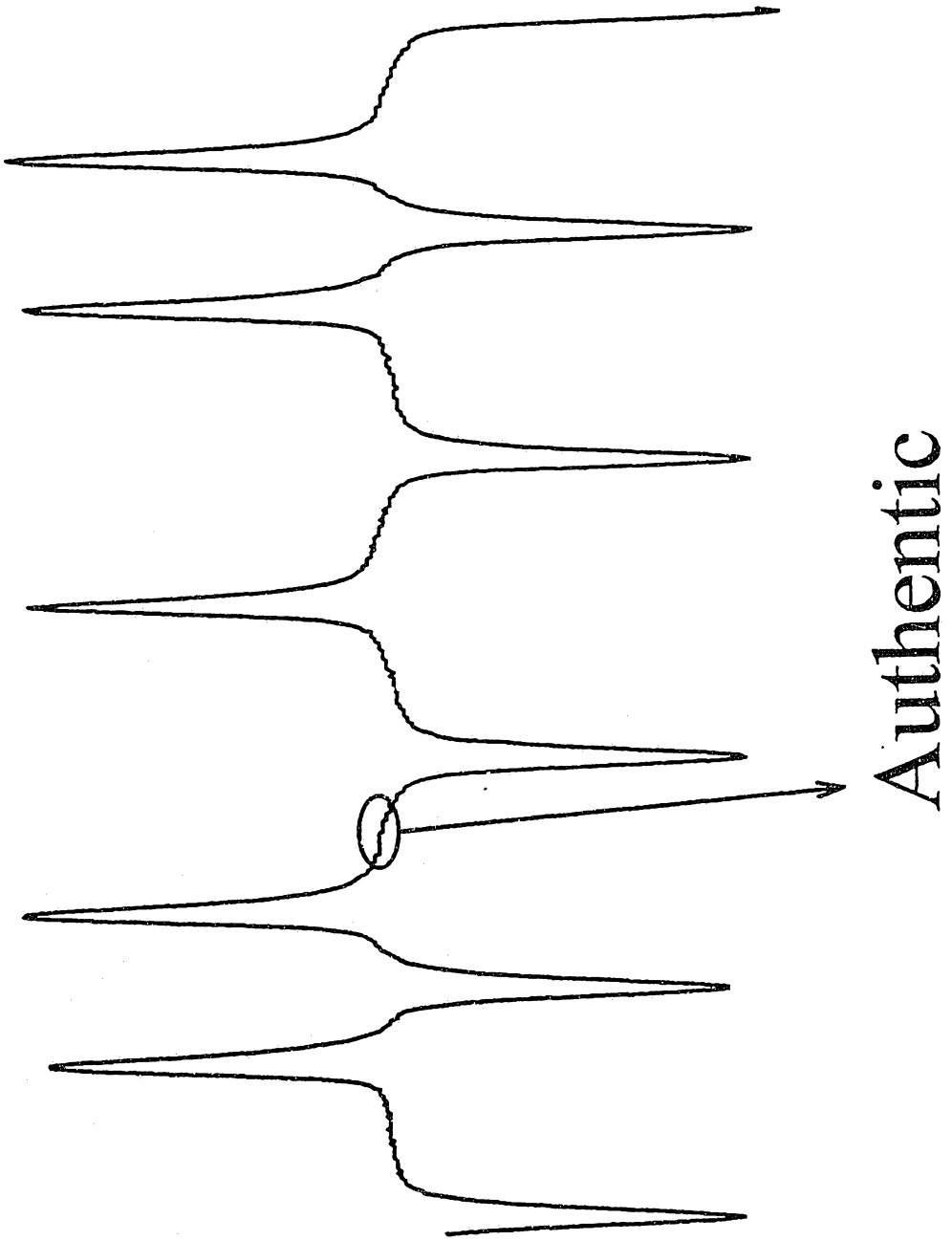


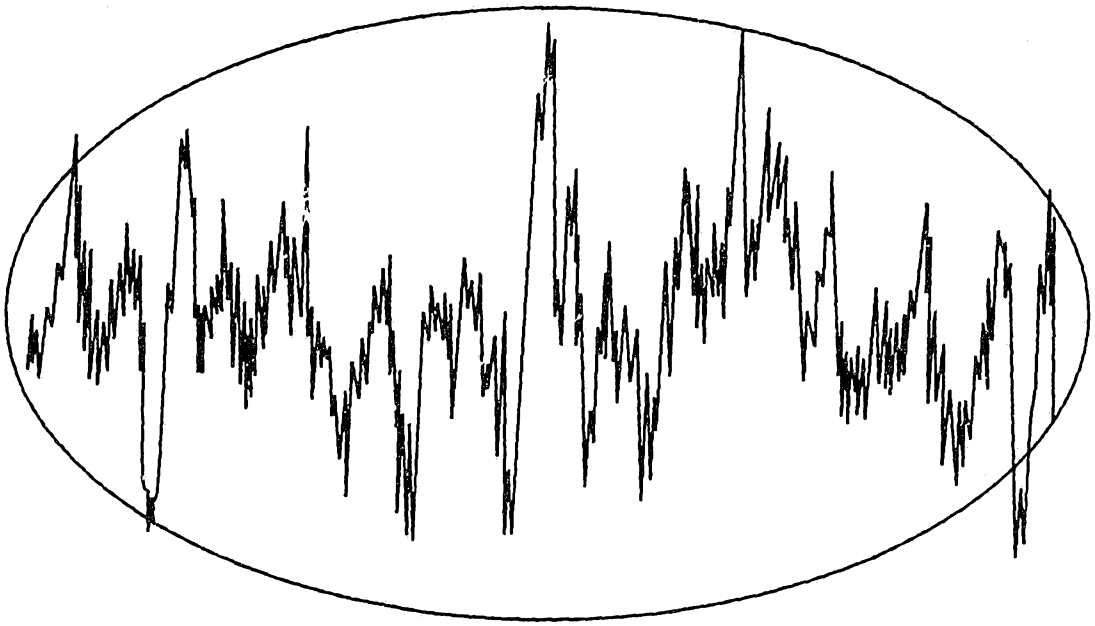
Q_1, Q_2, Q_3 are 2N2369

↑ fast switching small jncn cap

~20 dB (300 Hz – 1 MHz, 0V ≤ out ≤ 1.2V)

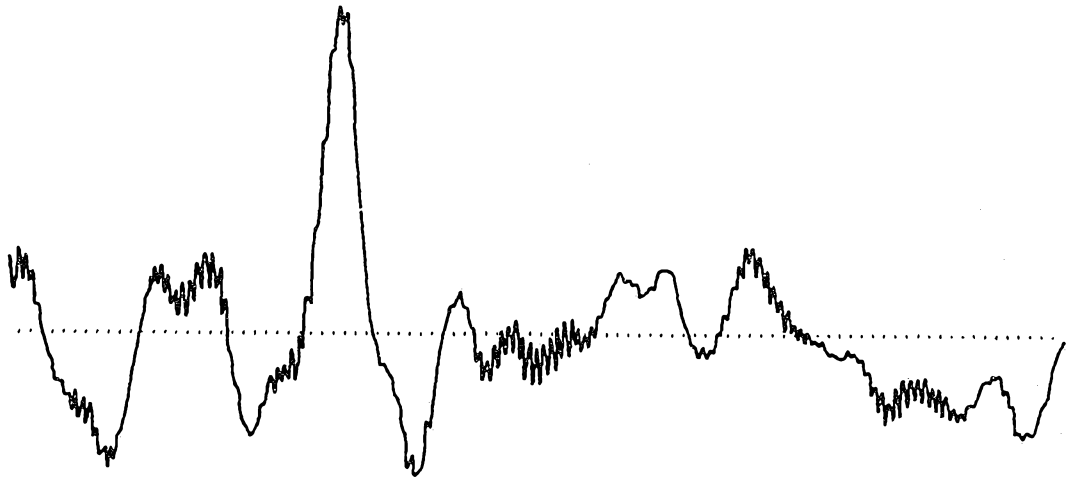
Fig. 24





MAGNETIC FINGERPRINT

FIG. 25



CORRELATION WITH MATCH

FIG. 26

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/03917

A. CLASSIFICATION OF SUBJECT MATTER

IPC(5) :G06K 7/00
US CL :380/4; 235/440
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/4; 235/440
235/380; 437, 448, 493

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US, A, 4,837,426 (PEASE, ET AL.) 06 JUNE 1989. See column 5, lines 10-18	1-48
X	US, A, 4,806,740 (GOLD ET AL.) 21 FEBRUARY 1989. See column 2, lines 49-64	1-48

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

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 15 JULY 1994	Date of mailing of the international search report AUG 03 1994
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer DAVID CAIN Telephone No. (703) 308-0463

Form PCT/ISA/210 (second sheet)(July 1992)*