



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 198 81 919 B4** 2009.01.02

(12)

Patentschrift

(21) Deutsches Aktenzeichen: **198 81 919.6**
(86) PCT-Aktenzeichen: **PCT/US98/00786**
(87) PCT-Veröffentlichungs-Nr.: **WO 1998/031123**
(86) PCT-Anmeldetag: **09.01.1998**
(87) PCT-Veröffentlichungstag: **16.07.1998**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **02.12.1999**
(45) Veröffentlichungstag
der Patenterteilung: **02.01.2009**

(51) Int Cl.⁸: **H04L 9/00** (2006.01)

Innerhalb von drei Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(30) Unionspriorität:
08/780,772 09.01.1997 US

(73) Patentinhaber:
Washington University, St. Louis, Mo., US

(74) Vertreter:
TER MEER STEINMEISTER & Partner GbR
Patentanwälte, 81679 München

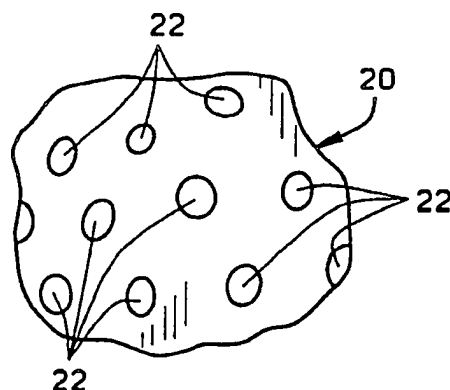
(72) Erfinder:
Indeck, Ronald S., Olivette, Mo., US; Muller, Marcel W., St. Louis, Mo., US; Morley jun., Robert E., St. Louis, Mo., US

(56) Für die Beurteilung der Patentfähigkeit in Betracht
gezogene Druckschriften:
US 53 65 586 A
US 49 85 614 A

(54) Bezeichnung: **Verfahren und Vorrichtung zum Erstellen von Fingerabdrücken und zum Authentifizieren verschiedener magnetischer Medien**

(57) Hauptanspruch: Verfahren zum Authentifizieren eines Objekts, wobei das Objekt wenigstens teilweise ein magnetisches Medium (212) enthält, wobei das Verfahren die folgenden Schritte umfasst:

- Auswählen mehrerer Abschnitte (A, B, C, D) des magnetischen Mediums (212), wobei wenigstens zwei der ausgewählten Abschnitte (A, B, C, D) unterschiedliche Abschnitte (A, B, C, D) umfassen,
- Erhalten von remanenten Rauschdaten von den ausgewählten Abschnitten (A, B, C, D) und
- Vergleichen der von den ausgewählten Abschnitten (A, B, C, D) erhaltenen remanenten Rauschdaten mit einer vorausgehenden Bestimmung davon, um somit zu bestimmen, ob das Objekt authentisch ist, wobei der Auswahl-schritt das Auswählen wenigstens zweier überlappender Abschnitte (A, B) des magnetischen Mediums (212) enthält.



Beschreibung**Hintergrund und Zusammenfassung der Erfindung**

[0001] Die Quellen des Rauschens in einem von einem magnetischen Aufzeichnungsmedium ausgelesenen Signal wurden untersucht und identifiziert. Wie in dem US-Patent Nr. 5.546.462 offenbart ist, dessen Offenbarung hier durch Literaturhinweis eingefügt ist, umfaßt eine dieser Quellen die Irregularitäten und Defekte in der Mikrostruktur des magnetischen Mediums selbst. Seit vielen Jahre besteht die Vorstellung, daß das von dieser Quelle erzeugte Rauschen ebenso wie das von anderen identifizierten Quellen erzeugte Rauschen zufällig ist und zu seiner Bestimmung lediglich der statistischen Untersuchung unterliegt. Die Erfinder haben bewiesen, daß diese Rauschkomponente statt dessen deterministisch, d. h. dauerhaft und wiederholbar, ist, wobei es vollständig von der Kopf-Medium-Position und von der magnetischen Vorgeschichte des Mediums abhängt. Wie von den Erfindern durchgeführte Experimente bestätigen, sind die beobachteten ausgelesenen Signale, wenn kein Signal auf das Medium geschrieben wurde und es lediglich Gleichfeldern ausgesetzt wurde, nahezu völlig gleich. Der magnetische Beitrag zu dem ausgelesenen Signal ergibt sich unter diesen Umständen aus den räumlichen Schwankungen der Magnetisierung des Mediums: den magnetischen Domänen, der Welligkeit, den lokalen Fluktuationen des Anisotropiefelds und der Sättigungsmagnetisierung. Diese lokalen Eigenschaften werden ihrerseits durch die Morphologie und die magnetischen Eigenschaften der einzelnen Körner, die die Domäne bilden und sich nach der Ablagerung nicht ändern, beeinflußt. Somit ist das an einer festen Stelle auf einem magnetischen Medium gemessene Rauschen von einem nominal gleichförmig magnetisierten Gebiet reproduzierbar. Wie durch die Erfinder gezeigt wurde, kann ein magnetisches Medium gleichfeldmäßig gesättigt und dann zur Bestimmung seines remanenten Zustands oder remanenten Rauschens gelesen werden. Durch Vergleich des remanenten Rauschens nach einer positiven Gleichfeldsättigung mit dem remanenten Rauschen nach einer negativen Gleichfeldsättigung haben die Erfinder bestätigt, daß dieses remanente Rauschen eine Funktion der magnetischen Mikrostruktur ist. Es wurde gefunden, daß diese Signalformen virtuelle "Spiegelbilder" voneinander sind, wobei auf diese Weise eine enge Korrelation bewiesen wurde. Ähnlich wurden weitere Methodiken verwendet, um zu bestätigen, daß das remanente Rauschen deterministisch und wiederholbar ist und mit der physikalischen Mikrostruktur des magnetischen Mediums selbst in Zusammenhang steht. Das von der dauerhaften Mikrostruktur herrührende remanente Rauschen zeigt identifizierbare Merkmale, die nach praktisch jeder magnetischen Vorgeschichte für diese dauerhafte Mikrostruktur charakteristisch sind. Siehe Spatial Noise Phenomena of Longitudinal

Magnetic Recording Media von Hoinville, Indeck und Muller, IEEE Transactions on Magnetics, Bd. 28, Nr. 6, November 1992, dessen Offenbarung hiermit durch Literaturhinweis eingefügt ist.

[0002] Im Gebiet besteht seit langem ein Bedarf an einem Verfahren und an einer Vorrichtung zum zuverlässigen Identifizieren oder Erstellen eines Fingerabdrucks verschiedener Arten von Objekten einschließlich der breiten Vielfalt der bespielten magnetischen Medien, die derzeit in den Vereinigten Staaten und in der gesamten Welt vermarktet und/oder verteilt werden. Beispiele dieser magnetischen Medien umfassen jene, die in der Unterhaltungsindustrie hergestellt und verkauft werden einschließlich magnetischer und magnetooptischer Platten und Bänder, Kassettenbänder, Bänder für Zweirollen-Magnetbandgeräte, Videobänder usw. Ein nochmals weiterer Hauptmarkt in bezug auf bespielte magnetische Medien ist der gewaltige Umfang der routinemäßig auf Floppy-Disketten und Digitalbändern verkauften und/oder verteilten Computerprogramme. Magnetische Medien werden außerdem für weitere Zwecke, bei denen es wichtig ist, die Originale identifizieren und authentifizieren zu können, einschließlich Videobändern, Kassettenbändern und weiteren Aufzeichnungen auf magnetischen Medien einschließlich Bandaufnahmen von Telefongesprächen, Videoaufzeichnungen krimineller Aktivitäten und weiterer solcher Untersuchungs- und Dokumentationsanwendungen, verwendet. Ein nochmals weiteres Beispiel eines Bedarfs im Gebiet für die Authentifizierung und Bestätigung aufgezeichneter magnetischer Medien liegt im Gebiet der magnetischen Datenkarten. Beispiele magnetischer Datenkarten umfassen die wohlbekannte Kreditkarte sowie Bankautomatenkarten, Debitkarten, Sicherheits- oder ID-Karten, Massentransitkarten, Telefonkarten und selbst Flugzeugtickets oder andere Gutscheine, auf denen sich Magnetstreifen für die magnetische Aufzeichnung der Daten befinden. Wie im Gebiet wohlbekannt ist, besitzt praktisch jede magnetische Datenkarte einen Magnetstreifen mit eingespielten magnetischen Daten, der zum Aufzeichnen der Kundenkontonummer oder weiterer solcher Identifizierungsdaten verwendet wird. Durch Fälschung und durch anderes betrügerisches Kopieren gehen jährlich gewaltige Geldsummen verloren, wobei Systeme verwendet werden, die praktisch weggelassen werden könnten, falls eine Vorrichtung und eine Methodik zur zuverlässigen Authentifizierung und Bestätigung der Identität einer magnetischen Datenkarte vor deren Anerkennung für ihre zugeordnete Transaktion realisiert werden könnten.

[0003] Bespielte magnetische Medien sind nur eines der Vielzahl der Objekte, für die eine zuverlässige Identifizierung oder das Erstellen von Fingerabdrücken erforderlich ist. Gewaltige Geldsummen gehen jährlich außerdem durch die Fälschung oder durch das betrügerische Kopieren und durch die be-

trügerische Verwendung von Papierdokumenten wie etwa von Schecks, Bankwechseln, Zahlungsanweisungen und weiteren verkäuflichen oder unverkäuflichen Finanzinstrumenten einschließlich Bürgschaften, Aktienzertifikaten usw. verloren. Falls diese verschiedenen Typen von Papierdokumenten während der Verarbeitung durch die Finanzmärkte authentifiziert werden könnten, könnten ihre Fälschungen vor dem Verrechnen einer besonderen Transaktion erfaßt werden.

[0004] Das explosionsartige Wachstum des Internet und weiterer Computernetze und -datenbanken haben außerdem zu einem nochmals weiteren Gebiet geführt, auf dem eine zuverlässige Bestätigung oder Authentifizierung erforderlich ist. Typischerweise werden autorisierten Anwendern wiederverwendbare Kennwörter zugewiesen, wobei der Zugang zum Netz davon abhängig gemacht wird, ob der Anwender das zugewiesene wiederverwendbare Kennwort eingeben kann. Diese Methodik besitzt jedoch wenigstens zwei signifikante Nachteile. Da das Netz den Zugang für irgendeinen Anwender, der das Kennwort für eine entsprechende Kontonummer eingeben kann, bereitstellt, können zunächst gewissenlose Anwender ein einziges Konto und Kennwort gemeinsam nutzen, was dem Netz häufig zum finanziellen Schaden gereicht. Zum Beispiel könnte ein Anwender für den Zugang zum Internet einen monatlichen Pauschal tariff zahlen und dann die zugewiesene Kontonummer und das zugewiesene Kennwort mit anderen gemeinsam nutzen, so daß mehrere Anwender auf das Internet zugreifen, während nur eine einzige Gebühr gezahlt wurde. Abgesehen von krassen Fällen, wie etwa dann, wenn für ein einziges Konto 25 Stunden an einem Tag registriert werden, ist diese Art des betrügerischen Zugangs häufig schwer, wenn nicht unmöglich zu erfassen.

[0005] Ein weiterer Nachteil für wiederverwendbare Kennwörter sowohl für Online- als auch für Offline-Computernetze und -Datenbanken rührt von dem zunehmenden Auftreten des Online-Abhörens und des elektronischen Lauschens her. Dort, wo ein Computernetz oder eine Computerdatenbank proprietäre oder anderweitig geheime Informationen enthält, können eine Anwenderkontonummer und das entsprechende Kennwort z. B. während der Eingabe durch den Anwender in das Netz abgehört werden. Die abgefangene Kontonummer und das abgefangene Kennwort können dann nachfolgend zum Zugang zu dem Netz und somit zum Abwehren der durch das wiederverwendbare Kennwort gelieferten Sicherheit verwendet werden. Ähnlich kann dort, wo einem Anwender eine Rechnung auf der Grundlage dessen gestellt wird, wie lange oder wie oft der Anwender auf das Netz zugreift, das Abfangen und der Gebrauch des wiederverwendbaren Kennworts durch Dritte zu Rechnungsstellungen an den Anwender für den unberechtigten Gebrauch durch andere führen. Somit

werden ein Verfahren und eine Vorrichtung benötigt, die sowohl die gemeinsame Nutzung als auch den unberechtigten Gebrauch rechtmäßiger Netz- und Datenbankkonten durchkreuzen können.

[0006] Computer-Hardware- und -Software-Hersteller benötigen in dieser Richtung eine Einrichtung zum zuverlässigen Identifizieren der Käufer, die vom Hersteller technische Unterstützung begehren. Häufig machen die Hersteller den Zugang zu der üblicherweise telephonisch gelieferten technischen Unterstützung von der Fähigkeit des Kunden abhängig, für die gekaufte Hardware oder Software, für die die technische Unterstützung benötigt wird, bestimmte Informationen zu liefern. Bevor die technische Unterstützung gegeben wird, fragen Software-Hersteller die Anrufer z. B. routinemäßig nach der auf der Floppy-Diskette befindlichen laufenden Nummer und möglicherweise nach dem Namen des registrierten Käufers. Diese Informationen können jedoch durch den Käufer mit anderen gemeinsam genutzt werden, wobei sie oftmals im Internet mit jedermann gemeinsam genutzt werden. Im Ergebnis geben die Hersteller häufig an Personen, die die Software raubkopiert haben, eine technische Unterstützung, ohne daß eine Zahlung an den Hersteller für die raubkopierte Software oder für die geleistete technische Unterstützung erfolgen würde.

[0007] Ein nochmals weiterer Bedarf an einer zuverlässigen Identifizierung und an einer Fernidentifizierung rührt von der zunehmenden Verwendung von Online-Computernetzen zur Ausführung von Geschäftstransaktionen her. Immer mehr Informationen sowie Erzeugnisse werden online wie etwa über das Internet verkauft, wobei viele Käufer für diese Transaktionen mit Kreditkarten zu zahlen wünschen. Die Online-Verwendung von Kreditkarten erfordert jedoch, daß der Käufer die Kreditkarteninformationen wie etwa die Kontonummer an den Verkäufer überträgt, wobei für den Käufer ein ernsthaftes Risiko besteht, daß die Kreditkarteninformationen abgehört und betrügerisch durch andere verwendet werden. Da der Verkäufer üblicherweise keine Möglichkeiten besitzt, aus der Ferne zu bestätigen, daß der Käufer die den gelieferten Kreditkarteninformationen entsprechende Kreditkarte wirklich besitzt, besteht eine verwandte Besorgnis für den Online-Verkäufer darin, daß die gelieferten Kreditkarteninformationen gestohlen sein könnten.

[0008] Den Erfindern sind einige bestimmte, auf das Verifizieren oder Authentifizieren verschiedener Objekte gerichtete Bemühungen bekannt. In Verbindung damit wird in einem Artikel mit dem Titel Novel Applications of Cryptography in Digital Communications von Omura, IEEE Communications Magazine, Mai 1990, ein Verfahren zum Authentifizieren von Papierdokumenten offenbart. Wie darin beschrieben ist, besteht die Grundidee darin, einen eindeutigen "Finger-

abdruck" des Papiers zu messen und es unter Verwendung des geheimen Schlüssels des Herstellers z. B. eines Aktienzertifikats zu unterschreiben (zu verschlüsseln). Der Fingerabdruck wird dadurch erhalten, daß ein schmaler, starker Lichtstrahl längs einer Linie auf dem Papier verschoben wird, während die durch das Papier geleitete Lichtstärke gemessen wird. Die durch das eindeutige zufällige Muster der Papierfasern längs der Linie bestimmte Lichtstärkefunktion bildet den Fingerabdruck des besonderen Blatts Papier. Dieser Fingerabdruck wird dann durch die geheime Verschlüsselungsfunktion digitalisiert und verschlüsselt. Der verschlüsselte Fingerabdruck wird dann in digitaler Form wie etwa als ein Bar-Code getrennt auf das Papier gedruckt. Zu einem späteren Zeitpunkt kann die Authentizität des Aktienzertifikats mit einer nicht geheimen öffentlichen Entschlüsselungsfunktion zum Entschlüsseln der verschlüsselten Daten auf dem Papier und zum Rekonstruieren der darauf aufgezeichneten Stärkefunktion oder des darauf aufgezeichneten Fingerabdrucks bestätigt werden. Als nächstes wird die tatsächliche Stärkefunktion des Aktienzertifikats gemessen. Falls diese neu gemessene Stärkefunktion mit der aus den verschlüsselten Daten rekonstruierten Stärkefunktion übereinstimmt, kann das Dokument als authentisch erklärt werden. Dieses System nutzt ein wohlbekanntes Sicherheitssystem, das als Schlüsselsystem mit einem öffentlichen Schlüssel bezeichnet wird. Dieses System verwendet eine Falltür-Einweg-Funktion. Ein Anwender wählt einen geheimen Schlüssel (die Falltür), wobei das Verfahren, nachdem es die Falltür-Einweg-Funktion auf die Daten angewendet hat, einen zum Decodieren verwendeten Algorithmus bestimmt, den es öffentlich bekannt macht. Die Falltür-Einweg-Funktion wird außerdem zum Erzeugen der verschlüsselten Nachricht verwendet. Jeder andere Anwender kann dann die ursprüngliche Nachricht durch Anwenden des Algorithmus auf das Kryptogramm verstehen. Da nur der Absender Kenntnis von diesem Algorithmus hat, kann in diesem System niemand anders eine der Falltür des Absenders zuzuschreibende öffentlich lesbare Nachricht erzeugen. Dies verhindert den simplen Versuch, den beispielten Fingerabdruck in der Weise zu fälschen, daß er mit dem Fingerabdruck eines gefälschten Dokuments übereinstimmt.

[0009] Ein weiteres Beispiel eines Versuchs im Stand der Technik, Objekte mit einem Fingerabdruck zu versehen oder fälschungssicher zu machen, ist in dem US-Patent Nr. 4.806.740 beschrieben. Wie darin gezeigt ist, ist auf einem Objekt wie etwa auf einem Aktienzertifikat ein Streifen eines magnetischen Mediums mit einer von der Ungleichförmigkeit des Papiers, von dem Verfahren des Aufbringens des magnetischen Mediums auf dem Dokument und von der Streuung der magnetischen Teilchen in dem Medium herrührenden variablen Dichte aufgebracht. Die Dichteschwankungen werden während des Aufbrin-

gens des magnetischen Mediums zufällig erzeugt, was, da diese Dichteschwankungen zum Identifizieren des Dokuments feststehend und wiederholbar sind, ein eindeutiges Dokument liefert. Außerdem wird auf das Dokument ein zweiter Magnetstreifen aufgetragen, wobei dieser Magnetstreifen aber aus einem Medium besteht, das gemäß wohlbekannten Standards auf dem Aufzeichnungsgebiet eng spezifiziert und gut kontrolliert wird, um einen Teil eines magnetischen Lese/Schreib-Systems zu bilden. Im Betrieb wird der nicht gleichförmige Magnetstreifen gelöscht und auf ihm eine aus einem linearen Gleichfeldsignal oder aus einem linearen Wechselfeldsignal oder aus einem linearen Vormagnetisierungssignal bestehende Standardaufnahme aufgezeichnet. Nach dem Aufzeichnen tastet ein weiterer Kopf die magnetische Charakteristik des aufgezeichneten Magnetstreifens ab, wobei diese in ein digitales, maschinenlesbares Format übersetzt und dann in einer einfachen Schreibfunktion getrennt auf dem zweiten Magnetstreifen aufgezeichnet wird. Zur Authentifizierung wird das Aktienzertifikat unter einem weiteren Satz von Köpfen hindurchgeführt, der zunächst die digital aufgezeichnete maschinenlesbare Darstellung des abgetasteten Rauschsignals liest, während dann ein zweiter Satz von Köpfen den Magnetstreifen mit der variablen Dichte dadurch liest, daß er ihn zunächst löscht, die gleiche Standardrauschfunktion aufzeichnet und dann das Ausgangssignal der aufgezeichneten Rauschfunktion abtastet, während es durch den Magnetstreifen mit der variablen Dichte "gestört wird". Falls es mit der aufgezeichneten Darstellung davon übereinstimmt, wird das Dokument als authentisch und original erklärt. Bei dem Verfahren des 740er-Patents muß somit auf dem Dokument ein Magnetstreifenpaar aufgetragen werden, während ein (als Rauschen bezeichnetes) besonderes Signal aufgezeichnet, gemessen und dann sein Ausgangssignal digital aufgezeichnet werden muß. Um die Zufälligkeit seines Ausgangssignals sicherzustellen, muß außerdem einer der Magnetstreifen in einer von dem Aufzeichnungsindustriestandard verschiedenen und zufälligen Weise aufgetragen werden. Diese Schritte machen es schwierig und unzuverlässig das Verfahren des 740er-Patents zu realisieren.

[0010] Ein weiteres Beispiel eines Versuchs des Standes der Technik, ein magnetisches Medium zum Authentifizieren von Kreditkarten, Dokumenten und dergleichen zu verwenden, findet sich in Pease u. a., US-Patent Nr. 4.985.614. Dadurch, daß es sich auf makroskopische, im folgenden als "Makro"-Variationen in einem magnetischen Medium und auf ihre Wirkung auf ein in einer Ausführung darauf aufgezeichnetes "Verstärkungs"-Signal oder in einer zweiten Ausführung auf ein selbständig aufgezeichnetes "Verstärkungs"-Signal konzentriert, ist das Konzept des 614er-Patents tatsächlich recht ähnlich zu dem des oben diskutierten 740er-Patents. Bei beiden Ausführungen werden diese "Makro"-Variationen

durch ein drei- bis neunmaliges (in der zweckmäßigen Ausführung fünfmaliges) Lesen einer ausgewählten Länge von etwa 2,6 Zoll eines Magnetstreifens und anschließendes Korrelieren der gesammelten Datenpunkte zum "Herausmitteln" der Wirkungen des Kopfrauschens, des elektrischen Rauschens sowie irgendeines weiteren Nicht-Medium-Rauschens bestimmt. Diese Korrelation führt zu einem "repräsentativen Profil", das die Varianzen darstellt, die durch diese Makrowirkungen für ein Signal bewirkt würden, falls es auf diesem 2,6-Zoll-Abschnitt des Magnetstreifens aufgezeichnet würde. Falls diese Schwankungen zum Erzeugen einer zuverlässigen Korrelation nicht signifikant genug sind, was ein Fehlen signifikanter makroskopischer Ungleichförmigkeiten in dem Medium zeigt, wird das Medium verworfen. Dies ist ein Anzeichen, daß das Medium von der Spezifikation her mit einer zu geringen Schwankung hergestellt wurde oder anderweitig keine möglicherweise infolge eines Herstellerwasserzeichens oder dergleichen vorhandene genügende Schwankung auf der Makroebene besitzt, um für ein aufgezeichnetes Signal zuverlässig erfaßbare und wiederholbare Schwankungen zu erzeugen. Das 614er-Patent legt außerdem nahe, daß das Makroebenenrauschen dadurch verstärkt werden kann, daß lokal die augenscheinlichen magnetischen Charakteristiken des Streifens wie etwa durch Anbringen magnetischer Symbole auf dem unter dem magnetischen Gebiet liegenden Substrat oder durch Prägen ausgewählter Gebiete des magnetischen Materials, um eine gewisse Menge des Materials physikalisch zu verschieben, lokal geändert werden. Da die gemessenen Rauschpegel signifikante Wirkungen auf die Spitzen eines aufgezeichneten Verstärkungssignals haben, wird eine einfache Spitzenerfassungs- und Halteschaltung, wie sie zum Sammeln der Daten ausreichend ist, gelehrt, und wird ein einfacher "Vergleich" des beispielten "repräsentativen Profils" mit den momentan abgetasteten Datenpunkten, wie er ausreichend ist, um zu bestimmen, ob das Medium authentisch ist, gelehrt. Somit konzentriert sich das 614er-Patent nicht nur auf die Verwendung des Makroebenenrauschens, sondern es wird angenommen, daß seine zum Realisieren eines Makroebenen-Rauschensors offenbarte Vorrichtung und Methodik keinen zuverlässigen Mikrostruktur-Rauschebenen-Fingerabdruck erzeugen und seine Existenz zu einem späteren Zeitpunkt zum Authentifizieren eines Originals überprüfen kann.

[0011] Außerdem ist eine Vorrichtung zum Bestätigen der Identität eines Anwenders vor dem Gewähren des Zugangs zu einem Computersystem oder -netz bekannt. Die Vorrichtung umfaßt ein an einen autorisierten Anwender des Netzes ausgegebenes "Token" sowie ein entsprechendes "Zugangssteuermodul", das bei einem Netz-Host, bei einem Betriebssystem oder bei einer weiteren Kommunikationsvorrichtung liegt. Sowohl das Token als auch das

Zugangssteuermodul erzeugen alle sechzig Sekunden eindeutige, einmalige "unvorhersagbare" Zugangscodes. Um Zugang zu dem Netz zu erlangen, muß ein Anwender den auf dem Token angezeigten momentanen Code eingeben. Der Netzzugang wird gewährt, wenn der eingegebene Code mit dem durch das entsprechende Zugangssteuermodul gleichzeitig erzeugten Code übereinstimmt. Auf diese Weise kann die Identität des Anwenders dadurch fern bestätigt werden, daß bestätigt wird, daß der Anwender zu dem Zeitpunkt, zu dem er den Zugang anfordert, das Token besitzt. Die signifikanten Nachteile in diesem System bestehen darin, daß das Netz für jeden autorisierten Anwender ein Zugangssteuermodul und ein Token erwerben, d. h. kaufen, muß, wobei dann die autorisierten Anwender zusätzlich zu den zahlreichen weiteren magnetischen Datenkarten und Identifizierungskarten, die die durchschnittliche Einzelperson trägt, die Token tragen müssen. Da jedes Token und sein entsprechendes Zugangssteuermodul alle sechzig Sekunden genau den gleichen Code erzeugen, besagt dies außerdem, daß ein vorbestimmter Algorithmus verwendet wird, wobei es weiter besagt, daß ein "Knacken" des Algorithmus nicht jenseits des Bereichs des Möglichen liegt. Da das von dem autorisierten Anwender getragene Token zum Erzeugen und Anzeigen des Zugangscodes Elektronik und einen Bildschirm verwendet, hängt der zuverlässige Betrieb des Tokens außerdem vom Batteriestrom ab.

[0012] Die US 5,365,586 A beschreibt ein Verfahren und eine Vorrichtung zur Authentifizierung eines magnetischen Mediums. Hierbei umfaßt eine praktische Umsetzung für die Authentifizierung eines magnetischen Mediums durch ihre deterministische Rauschkomponente, eine magnetische Datenkarte, welche einen Magnetstreifen darauf aufweist, wobei der Magnetstreifen mit einem Strichcode versehen ist, welcher einen Fingerabdruck eines Bereichs des Magnetstreifens darstellt. Somit kann, wenn die magnetische Datenkarte durch einen Kartenleser gezogen wird, der Kartenleser den Strichcode lesen, um die gespeicherten Fingerabdruckdaten zu bestimmen, den Fingerabdruck im den Bereich des Magnetstreifens bestimmen, und diesen mit den gespeicherten Fingerabdruckdaten vergleichen, um aufgrund des Vergleichs die magnetische Datenkarte zu authentifizieren. Hierbei müssen die Fingerabdruckdaten nicht auf der Karte selbst gespeichert werden, sondern können statt dessen auch an einem anderen Ort abgelegt sein.

[0013] Die US 4,985,614 A beschreibt eine Vorrichtung und ein Verfahren zur Authentifizierung eines Objekts. Hierbei werden die Irregularitäten eines magnetischen Materials verstärkt und dazu verwendet, ein Objekt, das das entsprechende Material trägt, eindeutig zu identifizieren. Dabei wird, wenn ein gelöscht Magnetstreifen eines magnetischen Materi-

als durch einen Lesekopf gezogen wird, diese verbleibende Charakteristik des magnetischen Materials gemessen und in ein einzigartiges zeitabhängiges Spannungsprofil umgewandelt. Dieses Spannungsprofil kann gespeichert werden, um eine spätere Authentifizierung des Objekts zu ermöglichen. Der magnetische Bereich kann auch mit zwei oder mehreren vermischten Materialien mit unterschiedlichen Eigenschaften gebildet werden. Somit kann ein magnetischer Bereich mit zwei oder mehreren Materialien verwendet werden, um einen magnetischen Bereich mit zwei verschiedenen meßbaren Profilen zu erzeugen. Solch eine Anordnung schafft einen besonders hohen Grad an Sicherheit.

[0014] Um diese und weitere Probleme im Stand der Technik zu lösen, haben die Erfinder ein Verfahren und eine Vorrichtung zum Verwenden der eindeutigen, deterministischen, remanenten Rauschcharakteristik eines magnetischen Mediums infolge seiner magnetischen Mikrostruktur entwickelt, um nicht nur Dokumente, sondern weitere Objekte und wichtiger das magnetische Medium selbst in der Weise mit einem Fingerabdruck zu versehen, daß es identifiziert und authentifiziert werden kann. Dieses erfindungsgemäße Verfahren beruht auf der Entdeckung, daß die mikroskopische Struktur des magnetischen Mediums selbst eine dauerhaft zufällige Anordnung von Mikromerkmalen und somit deterministisch ist. Mit anderen Worten, die physikalische Mikrostruktur des Aufzeichnungsmediums bleibt, sobald es hergestellt wurde, für alle herkömmlichen Aufzeichnungsverfahren fest. In Medien, die aus Partikeln bestehen, ändert sich die Position und die Orientierung jedes Zeichens in dem Bindemittel für irgendein Anlegen eines Magnetfelds nicht; in Dünnschichtmedien bleiben die mikrokristallinen Orientierungen und Korngrenzen der Schicht während des Aufzeichnungs- und Reproduktionsverfahrens stationär. Es ist die Magnetisierung in jedem dieser festen Mikromerkmale, die gedreht oder modifiziert werden kann, um die Grundlage des magnetischen Aufzeichnungsverfahrens zu bilden. Falls ein Gebiet eines magnetischen Mediums in einer Richtung durch ein starkes angelegtes Feld gesättigt ist, hängt die remanente Magnetisierung stark von der Mikrostruktur des Mediums ab. Dieser remanente Zustand ist für irgendeinen Punkt des magnetischen Mediums deterministisch. Die Dimension jedes Teilchens oder Korns in dem Medium beträgt Hunderte oder Tausende von Ångström. Infolge ihrer kleinen Größe enthält ein kleines Gebiet der magnetischen Oberfläche eine sehr große Anzahl dieser physikalischen Subjekte. Obgleich das Herstellungsverfahren normalerweise Bemühungen zum Ausrichten dieser Teilchen einschließt, gibt es immer eine gewisse Streuung der einzelnen Orientierungen und Positionen. Die tatsächlichen Abweichungen sind für irgendein Gebiet der Medienoberfläche eindeutig, was diese Orientierung zu einer Unterschrift oder zu einem "Fingerabdruck" dieses Mediums

macht. Das absichtliche oder unabsichtliche Reproduzieren dieser Verteilung ist praktisch unmöglich, da dies eine präzise Manipulation der Orientierung der zahlreichen Teilchen auf der Submikrometerebene mit sich bringen würde. Somit kann die Orientierung einer großen Menge von Teilchen auf einen bestimmten Abschnitt einer magnetischen Oberfläche dieses Medium eindeutig identifizieren. In Experimenten haben die Erfinder gefunden, daß das remanente Rauschen von einer Länge von zwischen etwa 30 Mikrometern und 4300 Mikrometern momentan genügend Daten liefert, um ein magnetisches Medium mit einem "Fingerabdruck" zu versehen. Dies kann mit den 66.040 Mikrometern (2,6 Zoll) an Länge verglichen werden, die in dem Verfahren des oben diskutierten 614er-Patents zum Erstellen eines Fingerabdrucks eines magnetischen Mediums unter Verwendung des Makrorauschens erforderlich sind.

[0015] Im wesentlichen ist die vorliegende Erfindung geschickt einfach und an die Realisierung durch herkömmliche magnetische Meßwandler, wie sie momentan im Großen und Ganzen in praktisch jeder durch die Öffentlichkeit verwendeten Lese- oder Les-/Schreib-Vorrichtung zu finden sind und verwendet werden, angepaßt. Solche Beispiele umfassen Kreditkartenleser, Abspieler für magnetooptische Platten, Kassettenabspieler, VCRs sowie Personal Computer. Außerdem kann ein billiger Kartenleser an praktisch irgendeine Vorrichtung oder an praktisch irgendein Verfahren angeschlossen werden, wobei der Kartenleser als ein "Pfortner" verwendet wird, um die Eingabe oder den Zugang nur durch jene zu ermöglichen, die eine gültige Zugangskarte zur Authentifizierung übergeben können. Der Kartenleser kann außerdem zum Ermöglichen der Genehmigung von Online-Kreditkarten-Transaktionen verwendet werden. Infolge der relativ geringen Menge des zum Erreichen eines genauen Fingerabdrucks erforderlichen "magnetischen Mediums" erstreckt sich die Anwendung der vorliegenden Erfindung weit über die oben diskutierten magnetischen Aufzeichnungsoberflächen hinaus. Zum Beispiel besitzen die auf Bankschecks aufgetragenen magnetischen Nummern eine ausreichende Länge, um einen genauen "Fingerabdruck" für jeden einzelnen Scheck zu ermöglichen.

[0016] In seiner einfachsten Realisierung braucht ein herkömmlicher Aufzeichnungskopf lediglich einen bestimmten Abschnitt eines magnetischen Mediums gleichfeldmäßig zu sättigen und dann das verbleibende Restrauschen zu "lesen" oder "abzuspielen". Zweckmäßig kann der Fingerabdruck von einem Gebiet zwischen zwei aufgezeichneten magnetischen Übergängen, die sich auf dem Medium bereits an ihrer Stelle befinden, erhalten werden. Dieses remanente Rauschen, bei dem es sich um ein analoges Signal handelt, kann dann auf dem Medium selbst oder anderswo in einem maschinenlesbaren Format

und in Abhängigkeit von der besonderen Anwendung möglicherweise unter Verwendung einer Falltürfunktion digitalisiert und aufgezeichnet werden. Somit kann das magnetische Medium mit seinem Fingerabdruck selbst "markiert" werden. Mit Ausnahme dessen, daß in den sicherheitssensitiveren Anwendungen der digital aufgezeichnete Fingerabdruck unter Verwendung eines öffentlich bekannten Schlüssels entschlüsselt werden muß, wird die Bestätigung oder Authentifizierung dieses magnetischen Mediums durch einfaches Umkehren dieses Verfahrens erreicht. Sollte das gemessene remanente Rauschen mit dem aufgezeichneten remanenten Rauschen übereinstimmen, ist das magnetische Medium authentifiziert.

[0017] Bei der Verwendung des Verfahrens und der Vorrichtung der Erfinder gibt es viele Abwandlungen, die die Gesamtheit seiner Anwendungen erweitern. So brauchen z. B. einige Anwendungen, wie etwa, wenn die codierten Objekte z. B. nicht öffentlich verteilt und statt dessen nur für die Zwecke des Anwenders identifiziert werden, die Verwendung einer Falltürfunktion nicht zu erfordern. Ein solches Beispiel wäre zur Verwendung mit Inventarpositionen. Andere Beispiele umfassen jene Anwendungen der magnetischen Medien, die nicht an das Aufzeichnen von Daten oder Informationen darauf angepaßt sind. Zum Beispiel enthält ein Bankscheck längs seiner Unterkante magnetische Zahlen, die zum Verarbeiten des Bankschecks in den verschiedenen Phasen in dem Scheckverrechnungssystem der Finanzwelt verwendet werden. An einem oder an mehreren beliebigen ausgewählten Punkten in diesem System kann ein Fingerabdruck verwendet werden, um zu überprüfen, ob der Scheck gültig und keine Fälschung ist. Bei dieser Anwendung kann der Bankscheck durch die ausgebende Institution während der Ausgabe der Bankschecks zu ihrem Gebrauch an die Kontoinhaber mit einem Fingerabdruck versehen werden. Dies wird die verbreitete Fälschung von Bankschecks unter Verwendung von auf den Scheck aufgedruckten entweder richtigen oder falschen Kontoinhaberinformationen beseitigen. Auf diese Weise können kommerzielle Bankinstitute sicherstellen, daß nur ihre abgedruckten und autorisierten Schecks durch ihre Kontoinhaber verwendet und durch das Scheckverrechnungssystem eingelöst werden. Diese Anwendung des Fingerabdruckverfahrens der Erfinder würde einen signifikanten Anteil des Betrugs im kommerziellen Banksystem beseitigen.

[0018] Die Verwendung der vorliegenden Erfindung des Erstellens eines Fingerabdrucks würde bei anderen Finanzinstrumenten über das Aufdrucken von Kontonummern, Urkundennummern und weiteren identifizierenden Anzeichen oder Daten mit Magnetfarbe und deren Lesen während der Verarbeitung dieser Finanzinstrumente viele weitere Arten von Betrug, Fälschung und dergleichen mit einer minimalen

Unterbrechung oder Modifizierung momentan verwendeter Dokumentationsparadigmen beseitigen. Aktienzertifikate, Wertpapierzertifikate, Inhaberoptionen, Wertpapiercoupons, Schatzwechsel und weitere Finanzinstrumente könnten zum Beseitigen ihrer Fälschung mit einem Fingerabdruck versehen werden. Das Lesen und Bestätigen des Fingerabdrucks wird leicht zur gleichen Zeit erledigt, zu der während der Verarbeitung des Instruments durch die verschiedenen Punkte in den Finanzmärkten die magnetische Urkundennummer, Kontonummer, ID-Nummer oder andere Nummern auf dem Instrument gelesen werden. Durch die Verwendung der besonderen bereits realisierten Numerierung und der bereits realisierten Leser kann dieses erhöhte Niveau des Authentizitätsschutzes bei einer minimalen Änderung der Verarbeitungsmaschinerie erreicht werden. Als solches sind die Vorrichtung und das Verfahren der Erfinder für die Anpassung in dieser besonderen Anwendung einzigartig geeignet.

[0019] Eine nochmals weitere Anwendung betrifft den "Kopierschutz" von in Massen verteilter Anwendungssoftware. Während der Jahre wurden viele Systeme für den Kopierschutz öffentlich verteilter Disketten mit eingespielter Software versucht und fast einheitlich verworfen. Dies ist aus vielen Gründen geschehen, einschließlich des Problems, daß nahezu alle zuvor realisierten Kopierschutzsysteme den Lauf der Software auf dem Anwendercomputer stören. Mit der vorliegenden Erfindung kann ein Kopierschutzsystem realisiert werden, das den Lauf der Software nicht stört, während es lediglich eine Vorbedingung für den Lauf des ansonsten normal geschriebenen Codes liefert. In dieser Realisierung kann ein Software-Programm den Computer, auf dem es läuft, zunächst anweisen, einen Fingerabdruck eines bestimmten Abschnitts der gekauften Diskette oder des gekauften Bands zu lesen und ihn mit einer bespielten Version des gleichen Fingerabdrucks zu vergleichen. Falls die Fingerabdrücke übereinstimmen, kann die Software gestatten, daß der Computer die Anwendungs-Software weiter liest und realisiert. Falls der durch den Computer erfaßte Fingerabdruck jedoch nicht mit dem in der Software gespeicherten Fingerabdruck übereinstimmt, kann die Software selbst das weitere Lesen des Programms sperren und seine Realisierung verhindern. Dies würde absolut verhindern, daß ein Anwender eine Kopie eines Programms zur Verwendung durch jemand anderen erstellt. Dieses System kann außerdem leicht modifiziert werden, um einem Anwender das Erstellen eines einzelnen Archivs oder einer Sicherungskopie zu ermöglichen, so daß der Fingerabdruckvergleich ermöglicht, daß die erste Kopie mit dem nicht übereinstimmenden Fingerabdruck läuft, während sie dann verhindert, daß irgendwelche weiteren Kopien mit nicht übereinstimmenden Fingerabdrücken laufen. Als ein zusätzliches Schutzniveau können in der Software zuvor bestimmte Fingerabdrücke für mehrere

Abschnitte einer Diskette gespeichert werden, wobei die Software in der Weise konfiguriert werden kann, daß sie jedesmal, wenn sie läuft, einen Fingerabdruck von einem anderen Gebiet der Diskette liest und überprüft. Diese Realisierung wird leicht erreicht und versieht die Anwendungs-Software mit einem zuverlässigen, billigen "Kopierschutz", wobei an der gewaltigen Anzahl der bereits in den Händen der Verbraucher befindlichen Computer nur minimale Hardware-Änderungen erforderlich sind.

[0020] Eine nochmals weitere signifikante Anwendung der vorliegenden Erfindung betrifft das Authentifizieren von Kreditkarten unter Verwendung des auf den meisten Hauptkreditkarten bereits realisierten einzelnen Magnetstreifens. Dies kann wieder mit dem 614er-Patent verglichen werden, das vorschlägt, daß wegen der erforderlichen 2,6 Zoll-Streifenlänge, die zum Erhalten eines einzelnen Makrofingerabdrucks vorgesehen werden müssen, ein zweiter Streifen hinzugefügt wird. Wie oben erläutert wurde, würde das gleiche Verfahren zum Messen des "Fingerabdrucks" für einen Abschnitt des Magnetstreifens und dann zum Aufzeichnen einer digitalisierten Form des Fingerabdrucks auf dem Magnetstreifen verwendet werden. Jedesmal, wenn die Karte zum Bestätigen ihrer Authentizität verwendet wird, würde dann ein Kreditkartenleser erfordern, daß der bespielte Fingerabdruck mit einem gemessenen Fingerabdruck übereinstimmt. Obgleich bereits eine große Anzahl von Kreditkarten in Umlauf ist, unterliegen diese Karten routinemäßig dem Verfall, so daß in den Händen der Öffentlichkeit eine kontinuierliche Ersetzung dieser Karten stattfindet. Somit könnte die installierte Basis der Kreditkarten im Laufe der Zeit leicht in jene, die "mit Fingerabdrücken" versehen wurden, umgewandelt werden. Außerdem könnte zu einer schnellen Realisierung des "Fingerabdruck"-Systems eine existierende Kartenbasis während des Gebrauchs mit "Fingerabdrücken" versehen werden. Dies könnte während des nächsten Gebrauchs jeder Karte durch jeden Karteninhaber geschehen.

[0021] Als eine Alternative oder Verbesserung zu dieser Anwendung der vorliegenden Erfindung können die Fingerabdrücke für ein gesamtes Gebiet oder für mehrere Gebiete eines Magnetstreifens bestimmt und in einer zentralen Datenbank gespeichert werden. Wenn der Verbraucher die Karte danach z. B. online verwenden möchte, kann der Verkäufer die Kreditkarte dadurch, daß er den Fingerabdruck für einen ausgewählten Abschnitt des Magnetstreifens anfordert und ihn mit den zuvor gespeicherten Daten vergleicht, authentifizieren und bestätigen, daß der Verbraucher die Karte besitzt. Unter Verwendung eines billigen Kartenlesers und möglicherweise geeigneter Software kann der Anwender das remanente Rauschen für den ausgewählten Abschnitt des Magnetstreifens lesen und diese Informationen zur Über-

prüfung an den Online-Verkäufer senden. Durch den Verkäufer oder durch den Kreditkartenausgeber kann für Authentifizierungszwecke jedesmal, wenn die Kreditkarte des Verbrauchers verwendet wird, ein anderer oder ein zusätzlicher Abschnitt der Karte ausgewählt werden. Auf diese Weise wird der vom Käufer an den Verkäufer gesendete Überprüfungsfingerabdruck jedesmal, wenn die Karte authentifiziert wird, geändert, so daß ein Online-Abhören und elektronisches Lauschen zum "Stehlen" eines Fingerabdrucks und zum Anpassen an die Kontonummer unschädlich und unwirksam gemacht werden. Falls der übertragene Fingerabdruck abgehört wird, ist er für praktisch alle nachfolgenden Transaktionen nutzlos.

[0022] Dieser Aspekt der vorliegenden Erfindung wurde aus der Erkenntnis der Erfinder heraus entwickelt, daß von einem magnetischen Medium mit einer endlichen Länge oder mit einem endlichen Oberflächeninhalt eine große und praktisch unbegrenzte Anzahl von Fingerabdrücken erhalten werden kann. Im Fall einer Kreditkarte kann z. B. jedesmal, wenn die Karte zum Erzeugen eines eindeutigen Fingerabdrucks authentifiziert wird, ein anderer Abschnitt des Magnetstreifens (oder ein anderer Abschnitt eines der mehreren Spuren des Magnetstreifens) ausgewählt werden, wobei sich der ausgewählte Abschnitt überschneiden oder nicht überschneiden kann und die gleiche Länge oder nicht die gleiche Länge wie der zuvor ausgewählte Abschnitt haben kann. Außerdem können mehrere Abschnitte des Magnetstreifens ausgewählt und die remanenten Rauschen daraus gelesen werden, wobei dann die remanenten Rauschen von den mehreren Abschnitten für Bestätigungszwecke zu einem einzigen Fingerabdruck zusammengesetzt werden. Die remanenten Rauschen von mehreren Abschnitten des Magnetstreifens können außerdem wie etwa durch Addieren, Subtrahieren oder Mitteln der mehreren remanenten Rauschen linearkombiniert werden, um einen Hybrid-Fingerabdruck zu erzeugen, der nicht das remanente Rauschen für irgendeinen Einzelabschnitt des magnetischen Mediums darstellt. Dies würde verhindern, daß z. B. ein elektronischer Lauscher im Laufe der Zeit die remanenten Rauschdaten für einen wesentlichen Abschnitt des magnetischen Mediums sammelt. Im Fall der magnetischen Datenkarten kann zum weiteren Erhöhen der Anzahl der verfügbaren Rauschcodes ein zweiter Magnetstreifen auf der Karte aufgetragen werden. Durch Anwenden irgendeiner oder einer Kombination dieser mehreren Methodiken kann aus dem magnetischen Medium eines Objekts eine anscheinend unbegrenzte Anzahl von Fingerabdrücken abgeleitet werden, so daß jedesmal, wenn das Objekt authentifiziert wird, ein anderer Fingerabdruck verwendet werden kann.

[0023] Obgleich dieser Aspekt der vorliegenden Erfindung oben für Kreditkarten beschrieben wurde, ist er, wie unten ausführlicher diskutiert wird, ebenso gut

auf weitere Anwendungen wie etwa auf die Fernauthentifizierung von Netzanwendern vor der Gewährung des Zugangs zu einem Computernetz anwendbar. Falls irgendein Risiko besteht, daß ein gesendetes Kennwort abgehört und nachfolgend durch einen nicht autorisierten Teilnehmer verwendet werden könnte, kann das Netz dadurch, daß es jedesmal, wenn der Anwender den Zugang zu dem Netz anfordert, einen oder mehrere verschiedene Abschnitte der magnetischen Zugangskarte eines Anwenders auswählt, einmalige, nicht wiederverwendbare Rauschcodes verwenden. In einer nochmals weiteren Anwendung kann ein Computer-Hardware- oder -Software-Hersteller sicherstellen, daß technische Unterstützung nur an die tatsächlichen Käufer der Erzeugnisse des Herstellers gegeben wird. Bevor ein Software-Hersteller ein Computerprogramm auf einer Floppy-Diskette auf der Einzelhandelsebene verkauft, können z. B. die remanenten Rauschdaten für mehrere Abschnitte oder für ein gesamtes Gebiet der Diskette gesammelt und gespeichert werden. Wenn danach ein vorgeblicher Käufer der Software technische Unterstützung begehrt, kann der Software-Hersteller seine Unterstützung an die Voraussetzung knüpfen, daß der vorgebliche Käufer in der Lage ist, unter Verwendung eines Computers das remanente Rauschen von einem durch den Hersteller ausgewählten Abschnitt der Diskette zu lesen, wobei der Computer die remanenten Rauschdaten für den Käufer anzeigen kann, damit er sie liest und an den Hersteller berichtet. Diese Auswahl kann jedesmal, wenn technischen Unterstützung angefordert wird, geändert werden, um zu verhindern, daß Unterstützung für Einzelpersonen geleistet wird, die die Software nicht gekauft, sondern raubkopiert haben.

[0024] In einer nochmals weiteren Anwendung kann die vorliegende Erfindung wie etwa in sogenannten Chipkarten mit einer Datenbank oder mit einem Prozessor verbunden werden. Diese kreditkartenähnlichen Vorrichtungen enthalten tatsächlich möglicherweise zusätzlich zu den Standard-Kreditkarten-Magnetstreifen einen kartenintegrierten elektronischen Speicher und/oder Mikroprozessor. Dieser Speicher oder Mikroprozessor kann alle Arten von Informationen einschließlich Geldersatzdaten enthalten. Zum Beispiel sind derzeit eine große Anzahl dieser Chipkarten weltweit als Guthaben-Telephonkarten im Gebrauch, die zuvor mit einem Geldbetrag geladen werden, der durch einen Münzfernsprecher belastet wird. Die Karten werden so lange verwendet, bis ihr zuvor geladener Geld-Gegenwert erschöpft ist, wobei sie dann verworfen werden. Obgleich zum Schutz gegen Betrug verschiedene Sicherheitsmethodiken entwickelt wurden, sind diese der Brechung ausgesetzt. Da die vorliegende Erfindung lediglich von der magnetischen Mikrostruktur des besonderen magnetischen Mediums abhängt, ist sie als ein einzigartiges Sicherheitssystem für Chipkarten geeignet. Im Gebrauch könnte der magnetische Fingerabdruck auf

dem Magnetstreifen oder in dem auf dem Chip befindlichen Chipkartenspeicher gespeichert werden. In Verbindung mit einer Falltürfunktion könnte ohne Zugang zu der Falltürfunktion keine betrügerische Karte erzeugt werden, wobei jede Transaktion an einem lokalen Kartenleser schnell im voraus, ohne mit einer zentralen Verrechnungsverkehr-Behörde zu telefonieren, autorisiert werden könnte.

[0025] In einer Erweiterung auf alle Kreditkarten- und Chipkartenanwendungen können die Fingerabdruckdaten zusammen mit jeder Transaktion in der Weise gespeichert werden, daß ein vollständiger Datensatz oder eine vollständige Spur erzeugt wird, der bzw. die die Vorgeschichte einer besonderen Karte verfolgt. Das momentan üblicherweise verwendete System, bei dem eine Anzahl betrügerischer Karten mit einer richtigen, aber gestohlenen Kontonummer erzeugt werden, könnte somit entweder durchkreuzt oder effektiv verfolgt werden. Eine weitere Sicherheitsebene integriert die zufällige Positionierung eines aufgezeichneten Fingerabdrucks z. B. auf einer magnetischen Datenkarte. Diese Position könnte eine Funktion der Kartenummer sein. Zum Beispiel könnte der Kartenummernmodul "P" die Leseelektronik zu einem besonderen Datenbit weisen, um das herum oder in dessen Nähe der aufgezeichnete maschinenlesbare Fingerabdruck gefunden wird.

[0026] Wie oben erwähnt wurde, betrifft eine weitere signifikante Kategorie von Anwendungen die Verwendung der vorliegenden Erfindung in ihrer Pfortnerfunktion. Die vorliegende Erfindung schafft eine einzigartige und zuverlässige Lösung für irgendein System, irgendein Netz, irgendein Verfahren, irgendeine Maschine, irgendeinen Ort oder irgendeine weitere Funktion, für die erwünscht ist, daß der Zugang nur auf jene, die autorisiert sind, beschränkt ist. In ihrer einfachsten Realisierung kann eine Zugangskarte mit einem Magnetstreifen erzeugt werden, der gemäß der vorliegenden Erfindung mit einem Fingerabdruck versehen ist. Obgleich die Beispiele bezüglich der Verwendung einer Zugangskarte diskutiert werden, ist selbstverständlich, daß gemäß der hier gegebenen Lehre irgendein magnetisches Medium ähnlich verwendet werden kann. Als solches sollen alle weiteren solchen Beispiele und Realisierungen in der vorliegenden Erfindung enthalten sein, wobei selbstverständlich ist, daß sie in dem Begriff "Zugangskarte" enthalten sind. Diese Zugangskarte kann dann zu einer persönlichen ID-Karte werden, die durch Speichern des besonderen magnetischen Fingerabdrucks der verwendeten Karte nicht nur zum Steuern des Zugangs, sondern auch zum Identifizieren der besonderen Person, die auf den Dienst, die Funktion usw. zugreift, verwendet werden kann. Es können leicht zahlreiche Beispiele betrachtet werden. Zum Beispiel kann der Zugang zu einem Computernetz über ein Fernterminal unter Verwendung einer Zugangskarte der vorliegenden Erfindung ge-

steuert werden. Dies könnte durch die Verwendung einer Diskette realisiert werden, die leicht in irgendein Floppy-Disk-Laufwerk eingesetzt werden kann, das irgendeinen oder mehrere der Fingerabdrücke auf der Diskette authentifizieren könnte. Alternativ könnte ebenso ein billiger, an das Lesen einer Zugangskarte angepaßter Kartenleser verwendet werden. In beiden Fällen könnten zum Überwinden der Sicherheitsrisiken des Online-Abhörens und des elektronischen Lauschens in der gleichen Weise, wie es oben zuvor für die magnetischen Datenkarten beschrieben wurde, jedesmal, wenn Zugang begehrt wird, andere Abschnitte des Magnetstreifens verwendet werden.

[0027] Viele weitere Anwendungen könnten die Zugangskarte der zweckmäßigen Ausführung ebenso verwenden. Zum Beispiel könnte einem Bankkassierer eine Zugangskarte übertragen werden, die dann dazu verwendet werden könnte, alle durch den Kassierer eingegebenen Transaktionen zu verfolgen und somit zuverlässiger gegen Kassiererbetrug zu schützen. Die Myriade der durch Geschäfte, Krankenversicherungen, Universitäten, Krankenhäuser sowie weitere Organisationen oder Einrichtungen verwendeten Identifizierungskarten könnten leicht eine Zugangskarte annehmen und verwenden, um die Anwender ihrer Dienste, Einrichtungen usw. sicherer zu identifizieren und im voraus zu autorisieren. Nicht nur existierende Anwendungen wären einer Ersetzung mit der Zugangskarte der vorliegenden Erfindung leicht zugänglich, sondern wegen des hohen Grads der durch die vorliegende Erfindung gelieferten Sicherheit könnten weitere, neue Dienste und Systeme realisiert werden. Dies kann gut zur Erzeugung nationaler Datenbanken, nationaler ID-Karten sowie weiterer, universeller Realisierungen der Kreditkarten oder Zugangskarten führen. Dies trifft insbesondere zu, wenn ein System nicht nur den magnetischen Fingerabdruck einer besonderen Zugangskarte, sondern außerdem eine oder mehrere zusätzliche Sicherheitsüberprüfungen wie etwa eine Bild-ID, eine persönliche Identifikationsnummer (PIN) oder ein möglicherweise verschlüsseltes Kennwort, einen menschlichen Fingerabdruck, ein (derzeit auf Kreditkarten aufgedrucktes) Hologramm oder eine weitere solche Methodik, die somit das Zugangskartensystem faktisch unüberwindlich machen würde, verwendet. Mit einer solchen Sicherheit wären Einzelpersonen eher bereit, solche ausführlichen persönlichen Informationen, Finanzinformationen sowie Gesundheitsinformationen, wie sie diese Systeme durchführbar machen würden, zu übergeben.

[0028] Obwohl die Hauptvorteile und -merkmale der vorliegenden Erfindung oben beschrieben wurden und mehrere Beispiele gegeben wurden, kann ein besseres Verständnis der Erfindung unter Bezug auf die Zeichnung und auf die folgende ausführliche Beschreibung der zweckmäßigen Ausführungen erlangt werden.

Kurzbeschreibung der Zeichnung

[0029] [Fig. 1](#) ist eine vergrößerte repräsentative Darstellung der mikroskopischen Struktur eines Gebiets des magnetischen Mediums;

[0030] [Fig. 2](#) ist eine vergrößerte Darstellung mehrerer Spuren eines magnetischen Mediums mit repräsentativ darauf gezeigten mikroskopischen Strukturen;

[0031] [Fig. 3](#) ist eine Teilansicht einer Spur eines magnetischen Mediums mit einem darauf aufgezeichneten Fingerabdruck im maschinenlesbaren Code;

[0032] [Fig. 4](#) zeigt drei herkömmliche, an die zugeordnete Elektronik angeschlossene Meßwandler, mit einem darunter laufenden magnetischen Medium;

[0033] [Fig. 5](#) ist eine Teilansicht einer Kreditkarte mit darauf codierten Fingerabdruckdaten zum Lesen durch einen Kreditkartenleser;

[0034] [Fig. 6](#) zeigt einen Personal Computer mit einer Computerdiskette zum Einsetzen in sein Floppy-Disk-Laufwerk;

[0035] [Fig. 7](#) ist eine perspektivische Ansicht eines Abspielers für magnetooptische Platten mit einer magnetooptischen Platte in seinem Einschubfach;

[0036] [Fig. 8](#) ist ein Kassettenabspieler, der ein Kassettenband zum Abspielen darin zeigt;

[0037] [Fig. 9](#) ist eine perspektivische Ansicht eines VCR mit einem zum Einsetzen bereiten Band;

[0038] [Fig. 10](#) ist ein Blockschaltplan einer Bestätigungsschaltung für magnetische Fingerabdrücke;

[0039] [Fig. 11](#) ist ein Blockschaltplan eines Teils der in [Fig. 10](#) gezeigten magnetischen Auslöseschaltung;

[0040] [Fig. 12](#) ist ein Stromlaufplan der in der magnetischen Auslöseschaltung nach [Fig. 11](#) verwendeten Komparatoren;

[0041] [Fig. 13](#) ist ein Stromlaufplan der in der Realisierung nach [Fig. 11](#) verwendeten Vorverstärkerschaltung;

[0042] [Fig. 14](#) ist ein Blockschaltplan einer zur Realisierung in einer integrierten Schaltung eingerichteten Bestätigungsschaltung für magnetische Fingerabdrücke;

[0043] [Fig. 15](#) ist ein Stromlaufplan einer Korrelationschaltung für Ein-Bit-Datenströme;

[0044] [Fig. 16](#) ist ein Stromlaufplan eines aktiven Differenzierers;

[0045] [Fig. 17](#) ist ein Stromlaufplan des Schwellwertgenerators;

[0046] [Fig. 18](#) ist eine graphische Darstellung einer Auslesung eines magnetischen Kreditkartenstreifens;

[0047] [Fig. 19](#) ist eine vergrößerte Ansicht des eingekreisten Abschnitts der Signalform in [Fig. 18](#);

[0048] [Fig. 20](#) ist eine Signalform, die die Korrelation der zwei ausgelesenen Signale als eine Funktion des relativen Laufzeitunterschieds dazwischen angibt;

[0049] [Fig. 21](#) ist eine vergrößerte Ansicht eines Teils eines Finanzinstruments wie etwa eines Bankschecks, die ausführlich die Verwendung der Magnetintennummerierung in der vorliegenden Erfindung zeigt;

[0050] [Fig. 22](#) ist eine Ansicht einer magnetischen Datenkarte mit einem Magnetstreifen, von der eine praktisch unbegrenzte Anzahl von Fingerabdrücken abgeleitet werden kann;

[0051] [Fig. 23](#) ist eine Ansicht einer magnetischen Datenkarte mit einem für die Authentifizierung der Datenkarte vorgesehenen zweiten Magnetstreifen; und

[0052] [Fig. 24](#) ist ein Blockschaltplan einer Realisierung der vorliegenden Erfindung zur Fernauthentifizierung von Kreditkarten zum Ermöglichen von sicheren Online-Kreditkarten-Transaktionen.

Ausführliche Beschreibung der zweckmäßigen Ausführungen

[0053] Der Begriff "magnetisches Medium", wie er hier verwendet wird, sollte so verstanden werden, daß er sich auf irgendeine Substanz, auf irgendein Material, auf irgendeine Oberfläche oder auf irgendein anderes physikalisches Objekt, das über sein Magnetfeld abgetastet werden kann, bezieht, wobei dieses Magnetfeld entweder intrinsisch oder induziert sein kann. Wie oben angemerkt wurde, gibt es viele klassische Beispiele magnetischer Medien, die in einem engen Sinn als diese Oberflächen angesehen werden können, wobei sie so beschaffen sind, daß sie die Codierung von Informationen wie etwa Daten, Musik und dergleichen mit magnetischen, analogen oder digitalen Daten aufnehmen können. Jedoch gibt es weitere in der Definition der Erfinder enthaltene Beispiele wie etwa durch ein Spray oder durch Lithographie oder durch weitere Verfahren auf einer Oberfläche aufgetragene Magnetintinte, Photo-

kopierverfahren, die einen elektrostatisch aufgetragenen Toner verwenden, die Suspension von Metallspänen oder von anderen magnetisierbaren Teilchen in verschiedenen Flüssigkeiten wie etwa in Farbe, die auf einer Oberfläche aufgetragen werden kann und dann trocknet, um die Metallspäne zu fixieren, und selbst jene Materialien, die keinen äußeren Fluß besitzen, die aber, wenn sie z. B. getaktet werden, ein extern abtastbares Feld erzeugen. Mit dem Verständnis dieser Definition für den Begriff "magnetisches Medium" wird an nochmals weitere physikalische Beispiele einschließlich irgendwelcher Papierdokumente mit darauf aufgetragener Magnetintinte, wie etwa Schecks, Bankwechsel, Postanweisungen sowie weitere verkäufliche oder unverkäufliche Finanzinstrumente wie etwa Wertpapiere, Aktienzertifikate usw. erinnert.

[0054] Wie in [Fig. 1](#) gezeigt ist, ist ein Gebiet des magnetischen Mediums **20** mit mehreren mikrokristallinen Strukturen **22** in einem zufälligen Muster gebildet. Jede mikrokristalline Struktur **22** besteht aus Teilchen oder Körnern, deren Durchmesser von Hunderten bis zu Tausenden von Ångström schwankt. Um diese physikalischen Mikrostrukturen zu zeigen, ist die Ansicht nach [Fig. 1](#) stark vergrößert und verstärkt. Obgleich das in [Fig. 2](#) gezeigte magnetische Medium **24** selbst aus den im Gebiet wohlbekannten Spuren **26**, **28**, **30** bestehen kann, erstrecken sich die mikrokristallinen Strukturen, wie in [Fig. 2](#) gezeigt ist, über das gesamte magnetische Medium. Obgleich er schematisch als getrennte Gebiete gezeigt ist, kann ein magnetischer Fingerabdruck von irgendeinem Abschnitt des Mediums **24** erhalten werden.

[0055] Nunmehr mit Bezug auf die [Fig. 3](#) und [Fig. 4](#) sind mehrere an einem Kopftransport **37** angebrachte herkömmliche Schreibköpfe **32**, **34**, **36** gezeigt, wobei ein laufendes magnetisches Medium **38** steuerbar an den Schreibköpfen **32**, **34**, **36** vorbei angetrieben wird, wobei all dies im Gebiet wohlbekannt ist. Diese Schreibköpfe **32-36** können irgendein im Gebiet bekannter magnetischer Meßwandlerkopf oder magnetooptischer Meßwandlerkopf einschließlich Meßwandlern mit mehreren Spulen zum Lesen mehrerer Spuren sein. Die Schreibköpfe **32-36** sind, wie im Gebiet wohlbekannt ist, sämtlich an eine elektronische Schaltungsanordnung **39** zum Steuern und Lesen ihrer Eingangssignale und Ausgangssignale und zur weiteren Verarbeitung der Signale zum Abspielen oder zur anderweitigen Verwendung angeschlossen. Obgleich in [Fig. 4](#) nur drei Köpfe **32**, **34**, **36** gezeigt sind, ist für den Durchschnittsfachmann im Gebiet selbstverständlich, daß ebensogut irgendeine Anzahl vorgesehen werden kann und, wie hier gelehrt wird, zur Realisierung der Lehren der vorliegenden Erfindung erforderlich sein kann. Die Erfinder haben ebenfalls einen Prototyp konstruiert, der die Betriebsfähigkeit eines Aspekts der Erfindung unter Verwendung eines einzigen Kopfs beweist. Wie in [Fig. 3](#) ge-

zeigt ist, kann der magnetische "Fingerabdruck" in einem bestimmten Gebiet **40** eines in [Fig. 3](#) gegenständlich als ein Dünnschichtband gezeigten magnetischen Dünnschichtmediums **42** in einem digitalisierten, maschinenlesbaren Code **46** oder dergleichen an einer zweiten Position **44** auf dem magnetischen Dünnschichtmedium **42** aufgezeichnet werden. Alternativ kann der magnetische Fingerabdruck auf dem gleichen Abschnitt des Mediums, von dem er bestimmt wurde, oder in einer benachbarten Spur aufgezeichnet werden.

[0056] Als ihre zweckmäßige Ausführung haben die Erfinder eine Methodik zum Lesen oder Bestimmen des für ein Gebiet eines magnetischen Mediums, das "mit einem Fingerabdruck versehen wird", charakteristischen remanenten Mikrostrukturrauschens verwendet. Zweckmäßig liegt dieses Gebiet in der Größenordnung von mehreren zehn bis zu Tausenden von Mikrometern. Das Gebiet wird gleichfeldmäßig gesättigt und dann zum Bestimmen seines remanenten Rauschens einem "Lese"-Schritt unterworfen. Obgleich dies die zweckmäßige Ausführung ist, ist selbstverständlich, daß sich der Fingerabdruck unabhängig davon, ob auf dem Medium aufgezeichnet wurde oder nicht, immer dort befindet. Streng genommen ist es somit nicht erforderlich, daß der ausgewählte Abschnitt des Mediums, der den Fingerabdruck enthält, jedesmal, wenn der Fingerabdruck bestimmt wird, gleichfeldmäßig gesättigt oder in der gleichen Polarität gleichfeldmäßig gesättigt wird. Statt dessen ist es nur wichtig, daß das remanente Rauschen in einer Weise bestimmt wird, die sein erfolgreiches Korrelieren mit einem früher bestimmten remanenten Rauschen ermöglicht.

[0057] Falls das remanente Rauschen für einen bestimmten Abschnitt des magnetischen Mediums in einer "Einzel"-Messung erhalten wird, enthalten die Ergebnisse sowohl das elektronische als auch das der Teilchenorientierung zuzuschreibende remanente Rauschen. Da dieses "Rauschen" oder "remanente Rauschen" elektronisch als ein Analogsignal bestimmt wird, können diese Informationen dann digitalisiert und, wie gegenständlich als der Code **46** in [Fig. 3](#) gezeigt werden kann, mit zwischen etwa mehreren zehn bis zu Tausenden von Digitalbits an Informationen aufgezeichnet werden. Um das in der gemessenen Signalform anwesende elektronische Rauschen zu beseitigen, haben die Erfinder in den Experimenten mehrere Messungen vorgenommen und ihre Ergebnisse gemittelt. Beim Vergleich der zwei Datensätze, d. h. des Einzeldatensatzes und des gemittelten Datensatzes, wurde jedoch ein hoher Korrelationskoeffizient beobachtet, was somit bewies, daß in einer kommerziellen Anwendung leicht eine Einzelablesung verwendet werden kann. Wie von den Erfindern in ihrem obenerwähnten zuvor veröffentlichten Artikel erläutert wurde, wird der normierte Kreuzkorrelationskoeffizient r mit:

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

verwendet. Beim Authentifizieren des magnetischen Mediums zu einem späteren Zeitpunkt wird das Verfahren ähnlich wiederholt, wobei beim Vergleich der zwei Einzelsignalformen eine geringere Korrelation zwischen ihnen erfahren wurde. Jedoch war die mit den zwei Einzelsignalformen erfasste Korrelation signifikant und bewies klar die Durchführbarkeit dieses Verfahrens auch für die kommerzielle Anwendung.

[0058] [Fig. 18](#) zeigt das vom Lesen eines magnetischen Kreditkartenstreifens erhaltene Signal. Wie darin gezeigt ist, ist der zum Erhalten eines einzelnen Fingerabdrucks verwendete Abschnitt des Signals in bezug auf den Rest des Signals sehr klein. In der zweckmäßigen Ausführung der Erfinder werden für Fingerabdruckzwecke zwischen vier und acht Abschnitte des ausgelesenen Signals verwendet, wobei jeder verwendete Abschnitt Null-Bit-Daten darstellt. Jedoch ist selbstverständlich, daß zum Erstellen des Fingerabdrucks und zur Authentifizierung ebenfalls mehr, weniger und andere Abschnitte des ausgelesenen Signals verwendet werden können. Wie in [Fig. 19](#) gezeigt ist, kann der eingekreiste Abschnitt oder Fingerabdruck aus [Fig. 18](#) verstärkt werden, um die Signalform ausführlicher zu zeigen.

[0059] Infolge von derzeit mit der Indizierung magnetischer Meßwandler verknüpften Toleranzen kann eine gewisse Unsicherheit bestehen, ob der bei der ursprünglichen Bestimmung des Fingerabdrucks gelesene Abschnitt des Mediums genau der gleiche Abschnitt ist, der gelesen wird, wenn der Fingerabdruck nachfolgend für Vergleichszwecke bestimmt wird. Aus diesem Grund müssen die zwei ausgelesenen Signale möglicherweise mehrmals miteinander korreliert werden, wobei die ausgelesenen Signale jedesmal in bezug aufeinander verschoben werden, um die relative Position zwischen den Signalen zu bestimmen, die die größte Korrelation liefert. [Fig. 20](#) zeigt das Ergebnis eines solchen Verfahrens, wobei eine definierbare "Spitze" zeigt, wann die Korrelation am stärksten ist und wann somit das ursprüngliche und das nachfolgende ausgelesene Signal ausgerichtet sind.

[0060] Wie in [Fig. 5](#) gezeigt ist, umfaßt eine praktische Realisierung für die betreffende Erfindung eine magnetische Datenkarte **48**, auf der sich ein Magnetstreifen **50** befindet, wobei der Magnetstreifen **50** mit einem Code **52** codiert wird, der einen zuvor für ein Gebiet **54** des Magnetstreifens **50** bestimmten Fingerabdruck darstellt. Wenn die magnetische Datenkarte **48** durch einen Kartenleser **56** "geschlagen"

wird, kann der Kartenleser **56** somit den Code **52** zum Bestimmen der gespeicherten Fingerabdruckdaten lesen und erforderlichenfalls übersetzen, den Fingerabdruck im Gebiet **54** des Magnetstreifens **50** erneut bestimmen, sie auf eine Übereinstimmung hin vergleichen und, wenn sie übereinstimmen, die magnetische Datenkarte **48** als eine echte Karte, die nicht geändert wurde und anerkannt werden kann, authentifizieren. Alternativ braucht der Fingerabdruck nicht auf der Karte gespeichert zu werden, sondern kann statt dessen wie anderswo in einer Datenbank zentral gespeichert werden. Der Fingerabdruck kann außerdem sowohl auf der Karte als auch in einer zentralen Datenbank gespeichert werden, wobei der auf der Karte gespeicherte Fingerabdruck zur sofortigen Verarbeitungspunkt-Authentifizierung der Karte verwendet werden kann, während die in der zentralen Datenbank gespeicherten Fingerabdruckdaten, wie unten ausführlicher diskutiert wird, zur Fernauthentifizierung der Karte verwendet werden können. Nochmals ferner können die remanenten Rauschdaten für mehrere Abschnitte des Magnetstreifens oder für ein gesamtes Gebiet des Streifens zum Ermöglichen der Fernauthentifizierung in einer Datenbank gespeichert werden. Jedesmal, wenn die Karte authentifiziert wird, kann zum Vergleich mit den gespeicherten Fingerabdruckdaten ein anderer Abschnitt des Magnetstreifens gelesen werden. Wie in [Fig. 23](#) gezeigt ist, kann die Datenkarte in dieser Ausführung mit einem zweiten Magnetstreifen zum Erhalten der Fingerabdruckdaten versehen werden.

[0061] Wie in [Fig. 10](#) gezeigt ist, enthält ein schematischer Blockschaltplan für eine magnetische Fingerabdruck-Authentifizierungsvorrichtung einen Lesekopf **100** zum Lesen des magnetischen Mediums **102**, das sich, wie zuvor beschrieben wurde, auf einer Kreditkarte oder Zugangskarte **104** befinden kann. Eine magnetische Auslöseschaltung **106** taktet an einem Logikelement **108**, was ermöglicht, daß der Speicher **112** die durch einen Analog-Digital-Umsetzer **101** aus dem Strom der Daten V_s von dem Lesekopf erzeugten Digitaldaten speichert. Ein Mikrocontroller **114** verarbeitet dann die Daten und vergleicht sie mit dem zuvor bestimmten Fingerabdruck, um die Kreditkarte oder Zugangskarte **104** zu authentifizieren. In [Fig. 11](#) ist ein Teil der magnetischen Auslöseschaltung **106** ausführlicher gezeigt. Sie enthält einen (in 13 ausführlicher gezeigten) Vorverstärker **116**, der das Ausgangssignal von dem Lesekopf **100** verstärkt, um über einen (in [Fig. 16](#) gezeigten) aktiven Differenzierer sowie über eine Menge von Analogkomparatoren (siehe [Fig. 12](#)) mit durch einen Schwellwertgenerator (siehe [Fig. 17](#)) erzeugten Schwellwerten ein positives Impulsausgangssignal **118** und ein negatives Impulsausgangssignal **120** zu erzeugen, wie sie durch den Zeitablaufgraphen in der unteren Hälfte von [Fig. 11](#) gezeigt sind. In [Fig. 14](#) ist ein Blockschaltplan **130** für eine magnetische Fingerabdruckvorrichtung, die so beschaffen ist, daß sie in

einem nutzerangepaßten integrierten Schaltung realisiert werden kann, gezeigt.

[0062] In vielen Realisierungen der vorliegenden Erfindung ist die Geschwindigkeit, mit der das magnetische Medium an einem Schreibkopf, an einem Kartenleser oder dergleichen vorbei vorwärts getrieben wird, sowohl dann, wenn der magnetische Fingerabdruck erstmals gemessen wird, als auch später, wenn das magnetische Medium zum Bestätigen seiner Authentizität gemessen wird, festgelegt. Einige Beispiele dieser festen Lesegeschwindigkeit umfassen die Geschwindigkeit, mit der eine Floppy-Disk in einem Computer gedreht wird, die Geschwindigkeit, mit der ein VCR-Band abgespielt wird, die Geschwindigkeit, mit der ein Audio- oder Digitalkassettenband abgespielt wird, das motorisierte Auslesen einer ATM-Karte, das Verarbeiten von Bankschecks durch automatische Vorrichtungen usw. Dies trifft selbst auf bestimmte Kreditkartenanwendungen, bei denen motorisierte Kartenleser realisiert sind, zu. Jedoch gibt es außerdem weitere Anwendungen, für die eine gesteuerte Geschwindigkeit nicht zu erwarten ist. Die heutzutage vielleicht geläufigste Situation sind die weithin verwendeten Kreditkartenleser, die erfordern, daß ein Einzelhandelsverkäufer die Karte durch eine Lesespur "schlägt". Für diese Situationen, in denen die Geschwindigkeit, mit denen das magnetische Medium gelesen wird, variabel oder verschieden von der ist, mit der die ersten Fingerabdruckdaten bestimmt wurden, haben die Erfinder eine Anzahl von Methodiken entwickelt, um sicherzustellen, daß die den zuvor bestimmten magnetischen Fingerabdrücken entsprechenden Daten erfaßt und in dem Bestätigungsverfahren verwendet werden. Dies hilft, falsche Zurückweisungen gültiger Kreditkarten, Zugangskarten und dergleichen zu beseitigen. Der Klarheit halber werden diese verschiedenen Methodiken nicht mit Bezug auf eine Kreditkarte mit einem Magnetstreifen erläutert. Jedoch ist selbstverständlich, daß diese Methodiken ebensogut auf irgendeine Anwendung anwendbar sind, bei der die Geschwindigkeit, mit der das magnetische Medium gelesen wird, variabel oder anderweitig von der Geschwindigkeit, mit der die Fingerabdruckdaten zuvor bestimmt wurden, verschieden ist.

[0063] Um den magnetischen Fingerabdruck mit der Authentifizierungsvorrichtung, deren Blockschaltplan in [Fig. 10](#) gezeigt ist, ursprünglich zu erfassen, wird zwischen zwei auf dem magnetischen Medium aufgezeichneten Auslöseimpulsen eine Reihe von Datenpunkten, vielleicht 150, verwendet. Wie bei der magnetischen Auslöseschaltung nach [Fig. 11](#) gezeigt ist, wird das Signal "POS PULSE" aktiv, wenn die "Mitte" eines hinreichend großen positiv werdenden Impulses erfaßt wird. Ebenso wird das Signal "NEG PULSE" aktiv, wenn ein hinreichend großer, negativ werdender Impuls erfaßt wird. Um die Mitte des Impulses zu lokalisieren, wird unter Verwendung

des in [Fig. 16](#) gezeigten aktiven Differenzierers die Ableitung des ankommenden Signals genommen. Durch das Lokalisieren der Mitte des Impulses wird somit die Entfernung zwischen der Mitte der Impulse, die die brauchbare Fingerabdruckfläche definieren, festgelegt, wobei sie eine Entfernung darstellt, die jedesmal, wenn die Kreditkarte durch einen Kreditkartenleser geschlagen wird, zuverlässig ermittelt werden kann. Durch die Komparatoren C_1 und C_2 wird außerdem eine pegelsensitive Erfassung ausgeführt, wobei diese aber nur dazu dient, gegen falsche Auslöseereignisse schützen zu helfen. Der A/D-Umsetzer tastet mit einer festen Rate wie etwa F_{s1} ab. Somit ist der physikalische Abstand zwischen den abgetasteten Abschnitten des Mediums Δx_1 , wobei Δx_1 gleich V_1 (die Geschwindigkeit der Kreditkarte) dividiert durch F_{s1} (die Abtastfrequenz) ist. Falls die Abtastfrequenz F_{s1} einige hundert Kilohertz und die Geschwindigkeit der Karte etwa 0,5 m/s beträgt, liegt Δx_1 in der Größenordnung von einem Mikrometer. Die Anzahl der verwendeten Abtastwerte P (vielleicht 150) wird abgezählt und kann zusammen mit einer digitalen Darstellung des bestimmten Fingerabdrucks auf der Kreditkarte oder anderswo aufgezeichnet werden. Um die Zuverlässigkeit zu verbessern, können mehrere Ablesungen des magnetischen Fingerabdrucks erzeugt und dann gemittelt werden, um die Wirkungen des Kopfrauschens, des elektronischen Schaltungsrauschens und irgendeines weiteren, von dem magnetischen Mikrostrukturrauschens des magnetischen Mediums verschiedenen Rauschens zu beseitigen. Dies schließt das Verfahren, eine Kreditkarte mit einem Fingerabdruck zu versehen, ab.

[0064] Wenn die Karte in Gebrauch ist und wenn einer ihrer Fingerabdrücke zu authentifizieren gewünscht wird, muß das gleiche Gebiet des magnetischen Mediums der Karte, das zu dem Zeitpunkt abgetastet wurde, als die Karte mit ihrem Fingerabdruck versehen wurde, abgetastet werden. Außerdem muß die Entfernung zwischen den Abtastpunkten die gleiche sein wie die, als die Karte mit einem Fingerabdruck versehen wurde, wobei diese Entfernung in unserem Beispiel Δx_1 ist. Obgleich erwünscht ist, daß sie genau gleich ist, haben die Erfinder gefunden, daß eine gewisse Varianz von bis zu wenigen Prozent akzeptabel sein kann. Wie oben angegeben wurde, wird das Abtastintervall sowohl durch die Abtastfrequenz des A/D-Umsetzers als auch durch die Geschwindigkeit, mit der die Kreditkarte am Lesekopf vorbeiläuft, bestimmt. Für manuelle Kartenleseanwendungen, die große Mehrheit, die derzeit im Gebrauch ist, ist praktisch gewährleistet, daß die Einzelhandelsladenverkäufer die Karten mit verschiedenen Raten durch die Kartenleser schlagen. Eine Lösung für das nachfolgende Erhalten von Abtastwerten in dem ursprünglichen Abtastintervall besteht in dem starken Überabtasten. Dies kann entweder softwaremäßig oder hardwaremäßig geschehen. Mit anderen

Worten, wird eine Abtastfrequenz F_{s2} gewählt, die wesentlich größer als F_{s1} ist. Dies erzeugt ein neues Abtastintervall Δx_2 , das wesentlich mehr Abtastwerte, vielleicht 100mal mehr als in dem ursprünglichen Fingerabdruckverfahren genommen wurden, erzeugt. Mit anderen Worten können anstelle von 150 Abtastwerten 15.000 Abtastwerte genommen werden. Dies erfordert die Verwendung nur jedes M . Abtastwerts zum Erzeugen des gesamten Datensatzes. M kann als das Verhältnis von Q/P gewählt werden, wobei P die Anzahl der zwischen zwei Auslöseimpulsen zum Zeitpunkt des Erstellens des Fingerabdrucks verwendeten Abtastwerte und Q die Anzahl der nachfolgend während der Authentifizierung unter Verwendung einer Überabtastfrequenz F_{s2} verwendeten Abtastwerte ist. Da sich die Entfernung zwischen den Auslöseimpulsen nicht ändert und die Abtastfrequenz F_{s2} bekannt ist, kann die Geschwindigkeit der Karte während des Schlagens in der Einzelhandelsladeneinrichtung leicht bestimmt werden. Mathematisch kann leicht gezeigt werden, daß das Überabtasten mit diesem Überabtastverfahren um einen Faktor von etwa 100 zu einem Satz von Abtastwerten führt, die für Geschwindigkeiten, die sogar fünfmal größer als die Geschwindigkeit sind, die verwendet wurde, als der Fingerabdruck zuvor bestimmt wurde, am Verkaufspunkt ein effektives Abtastintervall besitzen, das innerhalb von 2% des ursprünglichen Abtastintervalls liegt. Erforderlichenfalls kann eine noch stärkere Überabtastfrequenz an noch größere Geschwindigkeitsverhältnisse anpassen.

[0065] Die Arbeit durch die Erfinder an den Prototypen der vorliegenden Erfindung zeigte, daß eine digitale Wortgröße von sogar drei Bits zum Codieren des Fingerabdruckabtastwerts ausreichend sein kann, um unter Verwendung des vorgeschlagenen Korrelationsanalyseverfahrens akzeptable Ergebnisse zu erhalten. Diese kleine Wortgröße legt nahe, daß zum Durchführen dieser Korrelation eine relativ kleine nutzerangepaßte integrierte Schaltung (IC) erwünscht sein kann. Auf dem Gebiet ist wohlbekannt (siehe z. B. die Literatur über die Sigma-Delta-Umsetzung), daß n -Bit-Wörter mit einer Rate von r_1 unter der Voraussetzung, daß die Datenrate des Ein-Bit-Datenstroms signifikant höher als die Rate r_1 ist, aus einem Ein-Bit-Datenstrom konstruiert werden können. Siehe z. B. An Integrated Binary Correlator Module, Jespers u. a., IEEE Journal, Juni 1983. In ihrer einfachsten Form kann die Wortlänge für jeden Faktor von vier in der Überabtastfrequenz um ein Bit erhöht werden. Außerdem ist es sehr wahrscheinlich, daß im Fall des vorgeschlagenen Korrelationsverfahrens das Konstruieren des n -Bit-Datenworts möglicherweise nicht erforderlich ist. Wenn das der Fall ist, ist das Ausführen der Korrelationen an einem Ein-Bit-Datenstrom trivial. Für den Fall von Ein-Bit-Daten und von Signalen mit einem Mittelwert null (wie etwa beim Rauschen des magnetischen Mediums) ist der Korrelationskoeffizient r durch den folgenden Ausdruck gegeben

ben:

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

[0066] Somit kann diese Korrelationsanalyse unter Verwendung eines einfachen Auf/Ab-Zählers **132**, wie er in [Fig. 15](#) gezeigt ist, ausgeführt werden. Wie darin gezeigt ist, wird das Ausgangssignal des Lesekopfs **100** durch einen Vorverstärker **116** verstärkt. Um für die Daten einen Mittelwert null sicherzustellen, wird am Ausgang des Vorverstärkers **116** ein Hochpaßfilter (HPF) **117** bereitgestellt. Das HPF **117** speist einen Analogkomparator **134** mit einer hohen Abtastrate für das Eingangssignal X_1 in ein XOR-Logikgatter **136**. Die ursprünglichen Fingerabdruckdaten werden synchron in einem Ein-Bit-Datenstrom für den Eingang Y_1 bereitgestellt, so daß der Ausgang des XOR-Logikgatters **136** tief wird, wenn die Bits übereinstimmen, während er hoch wird, wenn sie nicht übereinstimmen. Zum Auslösen der richtigen Zustandsänderungen wird für den Zähler ein durch die Logik **108** erzeugtes Takteingangssignal bereitgestellt. Das Ausgangssignal des Auf/Ab-Zählers **132** wird mit einem gewissen Schwellwert verglichen, welches, falls es den Schwellwert übersteigt, eine Übereinstimmung mit dem ursprünglichen Fingerabdruck angibt.

[0067] Ebenso, wie ein Ein-Bit-Datenstrom mit einer hohen Rate genommen und ein n-Bit-Wort mit einer niedrigen Rate konstruiert werden kann, ist das Umgekehrte ebenfalls möglich. Mit anderen Worten, kann das magnetische Medium zum Zeitpunkt des Erstellens des Fingerabdrucks z. B. mit einem Vier-Bit-A/D-Umsetzer abgetastet werden. Die Fingerabdruckdaten können dann in Vier-Bit-Wörtern gespeichert werden. Wie es etwa in vielen CD-Spielern realisiert ist, können die Vier-Bit-Daten-Abtastwerte während der Authentifizierung in einen Ein-Bit-Datenstrom mit der höheren Rate übersetzt werden. Dieser übersetzte Ein-Bit-Datenstrom wird dann mit dem von dem analogen Komparator **134** ausgehenden Ein-Bit-Datenstrom korreliert.

[0068] Eine nochmals weitere Methodik, um sicherzustellen, daß die Erfassung der Datenabtastwerte jener entspricht, die während des ursprünglichen Verfahrens des Erstellens des Fingerabdrucks verwendet wurde, umfaßt im wesentlichen das Messen der Geschwindigkeit der Kreditkarte und das Einstellen der Abtastrate in der Weise, daß sie mit dieser Geschwindigkeit übereinstimmt. Genauer können auf der Karte zwei durch eine feste Entfernung D voneinander getrennte Übergänge oder andere Vertrauenszeichen angebracht werden. Die Zeit, die die Karte benötigt, um von dem ersten Übergang zu dem zweiten Übergang gezogen zu werden, definiert die Geschwindigkeit, mit der die Karte durch den Leser gezogen wird. Die Abtastrate kann in der Weise eingestellt werden, daß sie mit dieser Geschwindigkeit

übereinstimmt, was auf der Voraussetzung beruht, daß die Geschwindigkeit, mit der sich die Karte nach dem zweiten Übergang bewegt, mit der Geschwindigkeit übereinstimmt, mit der sie sich zwischen dem ersten und zweiten Übergang bewegt hat. Dieses Verfahren erfordert keinerlei Überabtastung und minimiert somit die Menge des zum Speichern der während des Bestätigungs- oder Authentifizierungsverfahrens gesammelten Datenabtastwerte erforderlichen Speichers. Es wurde jedoch gezeigt, daß das Überabtasten um einen Faktor zwei und das anschließende Deformieren oder Dezimieren um zwei eine verbesserte Leistung liefert. Bei der Realisierung dieses Zugangs kann eine Phasenkoppelschleife verwendet werden, wobei die Eingangsfrequenz durch einen Faktor M und die Rückkoppelschleife durch einen Faktor N geteilt wird, so daß N durch M mal F_{Referenz} gleich F_s (die Abtastfrequenz) ist. Die Faktoren M und N können in Abhängigkeit von den weiteren Parametern des Systems wie etwa von der Größe der Abtastwerte, der erwarteten Abtastfrequenz, der Entfernung D usw. gewählt werden. Wie angemerkt wurde, bietet dieses Verfahren den Vorteil, das Überabtasten zu beseitigen, was den erforderlichen Speicher reduziert. Es leidet dadurch an einem Nachteil, daß die Geschwindigkeitsmessung über ein sehr kleines physikalisches Gebiet, vielleicht mehrere hundert Mikrometer, ausgeführt werden muß, was Genauigkeitsprobleme bieten kann.

[0069] Wie zuvor erwähnt wurde, können zum Minimieren dieses Abtast- und Anpassungsproblems Kreditkartenleser, die motorisiert sind oder die die Geschwindigkeit, mit der die Karte durch den Leser gezogen wird, anderweitig standardisieren, verwendet werden. Außerdem können mehrere der Methodiken kombiniert werden, um somit eine Hybridmethodik zu bilden, die für eine besondere Anwendung die besten Ergebnisse liefert. Zum Beispiel kann der Kreditkartenleser so beschaffen sein, daß er eine Anpassung an das Abtastintervall vornimmt, was, wie oben erläutert wurde, idealerweise die Forderung nach der Überabtastung beseitigt. Jedoch kann das Überabtasten in Verbindung mit der Intervallanpassung außerdem verwendet werden, um sicherzustellen, daß irgendwelche Abweichungen korrigiert werden.

[0070] Wie in [Fig. 6](#) gezeigt ist, besitzt ein Computer **58** ein Floppy-Disk-Laufwerk **60** zum Lesen einer Floppy-Diskette **62**, wobei all dies im Gebiet wohlbekannt ist. Als eine nochmals weitere Realisierung der vorliegenden Erfindung kann ein auf der Floppy-Diskette **62** aufgezeichnetes Software-Programm (das in eine Speichervorrichtung in dem Computer **58** kopiert und von dieser aus laufen kann) zunächst erfordern, daß das Floppy-Disk-Laufwerk **60** ein bezeichnetes Gebiet des magnetischen Mediums der Diskette liest, um ihren Fingerabdruck zu bestimmen, diesen Fingerabdruck mit den in dem Programm gespeicherten Fingerabdruckdaten vergleicht und, falls sie

übereinstimmen, zuläßt, daß der Computer **58** das Anwendungsprogramm laufen läßt. Falls die Floppy-Diskette **62** nicht die ursprüngliche, gekaufte Floppy-Diskette ist, läuft das Anwendungsprogramm nicht, da der gemessene Fingerabdruck nicht mit den in dem Programm gespeicherten Fingerabdruckdaten übereinstimmt. In einer Abwandlung dieser Realisierung kann eine einzelne Archivkopie der Floppy-Diskette **62** zulässig sein, wobei das Programm in der Weise konfiguriert wird, daß es läuft, falls der gemessene Fingerabdruck entweder eine Übereinstimmung mit den gespeicherten Fingerabdruckdaten oder die erste Nichtübereinstimmung ist. Die ersten Nichtübereinstimmungs-Fingerabdruckdaten würden dann ebenfalls in dem Software-Programm gespeichert, so daß das Programm nachfolgend die ursprüngliche Floppy-Diskette **62** oder eine zweite Floppy-Diskette, d. h. die Sicherungs-, Archivkopie, erkennen würde. Als ein zusätzliches Niveau des Kopierschutzes kann das Programm unter der Voraussetzung, daß es gespeicherte Fingerabdruckdaten für mehrere Abschnitte oder für ein gesamtes Gebiet des magnetischen Mediums der ursprünglichen Diskette enthält, in der Weise konfiguriert werden, daß es jedesmal, wenn das Software-Programm laufen gelassen wird, vielleicht zufällig, einen anderen oder zusätzlichen Abschnitt des magnetischen Mediums der Diskette auswählt. Ähnlich kann ein Software-Programm auf einem Digitalband gespeicherte remanente Rauschdaten für einen oder für mehrere Abschnitte des Digitalbands für die nachfolgende Authentifizierung des Bands besitzen.

[0071] In einer nochmals weiteren Realisierung der vorliegenden Erfindung besitzt ein Abspieler **64** für magnetooptische Platten, wie in [Fig. 7](#) gezeigt ist, eine in seinem Einschubfach **68** liegende Platte **66** zum Abspielen beim Zurückziehen des Einschubfachs **68**. Auf der Platte **66** kann jedoch ein zuvor bestimmter Fingerabdruck gespeichert sein. Sollte der magnetooptische Plattenspieler **64** die richtige Schaltungsanordnung zum Vorbedingungs-Abspiel der Platte **66** bei einer positiven Korrelation der gemessenen und der bespielten Fingerabdrücke besitzen, kann ein nicht autorisiertes Kopieren der Platte **66** verhindert werden. Ähnlich wären auf irgendwelchen von der Platte **66** hergestellten Bandkopien notwendig die falschen Fingerabdruckdaten gespeichert, wobei ihr nachfolgendes Abspiel, sollte die Bandabspieleinheit eine geeignete Schaltung zum Vorbedingungs-Abspiel auf der Grundlage der Übereinstimmung der gespeicherten und der gemessenen Fingerabdrücke besitzen, ebenfalls verhindert würde.

[0072] Wie in [Fig. 8](#) gezeigt ist, umfaßt eine nochmals weitere Realisierung der Erfindung das Messen und Speichern eines geeigneten Fingerabdrucks auf einer Kassette oder auf einem Digitalband **70** mit einem Kassettenabspieler **72**, der, wie oben erläutert wurde, die erforderliche Schaltungsanordnung zum

Messen und Vergleichen der bespielten und gemessenen Fingerabdrücke als eine Vorbedingung für das Abspielen besitzt. In einer nochmals weiteren Realisierung der vorliegenden Erfindung, wie sie in [Fig. 9](#) gezeigt ist, besitzt ein VCR **74** ein zum Einsetzen in ihn bereites VCR-Band **76**. Unter Verwendung der vorliegenden Erfindung kann ein Fingerabdruck leicht gemessen und auf dem VCR-Band für ein durch eine in dem VCR **74** enthaltene geeignete Schaltungsanordnung ausgeführtes nachfolgendes Authentifizierungsverfahren codiert werden. Wenn der VCR entsprechend konfiguriert ist, würde er somit ein Band nicht abspielen, wenn es nicht authentisch oder original ist.

[0073] Wie in [Fig. 21](#) gezeigt ist, umfaßt eine nochmals weitere Realisierung der vorliegenden Erfindung ihren Gebrauch mit einem magnetischen Medium, das, wie etwa ein typischer Bankscheck **200**, bei dem die mehreren Magnettintennummern **202** längs der Unterkante des Bankschecks **200** jeweils ein zum Erstellen eines Fingerabdrucks verwendbares "magnetisches Medium" enthalten, nicht an das Codieren von Informationen darauf angepaßt ist. Zum Beispiel enthält das Bezugszeichen **203** genügend Magnetintinte, die hinreichend lang ist, um für sie einen Fingerabdruck zu bestimmen. Zu diesem Zweck kann irgendeines der Standardzeichen an irgendeiner Stelle verwendet werden. Zur Anpassung an die an den verschiedenen Positionen auf dem Bankscheck **200** verwendeten veränderlichen Nummern könnte außerdem sogar eine zusätzliche Ziffer allein für Authentifizierungszwecke hinzugefügt werden. Da sich die besonderen Datenbits von Bank zu Bank, von Scheckkonto zu Scheckkonto usw. unterscheiden, würde die Verwendung des Bezugszeichens **203** oder einer zusätzlichen Ziffer das Einführen und Erhalten einer gewissen Gleichförmigkeit ermöglichen. Die digitale Darstellung des gemessenen Fingerabdrucks könnte dann auf dem Bankscheck zur sofortigen Verarbeitungspunkt-Authentifizierung des Schecks in verschiedenen Phasen des Scheckverrechnungssystems aufgezeichnet werden. Wie andere auf dem Scheck **200** vorhandene Daten können die digitalen Fingerabdruckdaten außerdem verschlüsselt oder verschleiert werden. Alternativ oder zusätzlich können die gemessenen Fingerabdruckdaten zur nachfolgenden Wiedergewinnung während des Authentifizierungsverfahrens in einer zentralen Datenbank gespeichert werden.

[0074] Dieses gleiche Verfahren kann für weitere Finanzinstrumente einschließlich Aktienzertifikaten, Wertpapieren, Wertpapiercoupons, Inhaberoobligationen, Postanweisungen, Geschenkzertifikaten kommerzieller Einzelhandelsunternehmen usw. verwendet werden. Da der Hauptzweck dieser Arten magnetischer Medien ein anderer als für das magnetische Aufzeichnen von Informationen darauf ist, besteht von diesen magnetischen Medien allgemein die Vor-

stellung als magnetische Nichtaufzeichnungsmedien. Mit anderen Worten, wird jede mit Magnettinte auf der Unterkante eines Bankschecks aufgetragene Dezimalzahl in einem Umriß aufgetragen, der selbst dem Befördern von Informationen, d. h. von einer Dezimalzahl, dienen soll. Es ist nicht beabsichtigt, daß auf diesen Magnettintenzahlen weitere Daten aufgezeichnet werden. Statt dessen sollen die Magnettintenzahlen selbst während der Verarbeitung des Schecks gelesen werden. Dies kann als eine Untergruppe des Begriffs "magnetisches Medium" angesehen werden, die magnetische Aufzeichnungsmedien enthält, auf denen zusätzliche Informationen magnetisch aufgezeichnet werden sollen. Beispiele magnetischer Aufzeichnungsmedien einschließlich magnetooptischer Platten und Bänder, Kassettenbänder, Zweiröllengerät-Bänder, Videobänder, Computer-Floppy-Disketten, Kreditkarten sowie ATM-Karten usw. werden oben gegeben. Die Erfinder gehen von der Vorstellung aus, daß ihre Erfindung mit allen Arten magnetischer Medien, einschließlich sowohl Aufzeichnungsmedien als auch Nichtaufzeichnungsmedien, wie sie hier erläutert wurden, leicht verwendbar ist.

[0075] In vielen der oben offenbarten Beispiele wurden die Daten, die einen ursprünglich gemessenen Fingerabdruck darstellen, um die Verarbeitungspunkt-Authentifizierung des magnetischen Mediums, d. h. die sofortige Autorisierung einer physikalisch zur Zahlung an einen Einzelhändler übergebenen Kreditkarte, zu ermöglichen, auf dem magnetischen Medium selbst aufgezeichnet. Jedoch kann die Verarbeitungspunkt-Authentifizierung anstelle auf der Kreditkarte auch dort ausgeführt werden, wo diese Fingerabdruckdaten in einer zentralen Datenbank gespeichert werden. Nicht anders als in anderen in einer derzeit weitverbreiteten Weise unter Verwendung von Kreditkartenlesern ausgeführten Kreditkarten-Verrechnungsverfahren könnte der Einzelhändler somit jedesmal, wenn eine Kreditkarte physikalisch zur Zahlung übergeben wird, auf die zentrale Datenbank zugreifen.

[0076] Ein nochmals weiterer Aspekt der vorliegenden Erfindung stützt sich auf das Speichern der ursprünglichen Fingerabdruckdaten in einer fernen oder zentralen Datenbank, um in einer Weise, die die früheren Risiken des Online-Datenabhörens, des elektronischen Lauschens und des gemeinsamen Nutzens von Zugangsdaten durch gewissenlose Anwender überwindet, eine Online-Verwendung von Kreditkarten und einen sicheren Zugriff auf Computernetze, auf Datenbanken und auf eine technische Unterstützung vorzusehen. In ihrer einfachsten Realisierung kann ein Objekt wie etwa eine magnetische Datenkarte oder eine Floppy-Diskette, das wenigstens teilweise ein magnetisches Medium besitzt, für mehrere Abschnitte oder für ein gesamtes Gebiet des Mediums remanente Rauschdaten besitzen, die be-

stimmt wurden, bevor das Objekt ausgegeben, verkauft oder anderweitig für die Öffentlichkeit verfügbar gemacht wurden. Zur nachfolgenden Wiedergewinnung, wenn das Objekt fernauthentifiziert werden soll, können diese remanenten Rauschdaten dann z. B. in einer zentralen Datenbank gespeichert werden. Einige Beispiele dessen, wo die Fernauthentifizierung nützlich ist, umfassen die Fernauthentifizierung der Kreditkarte eines Online-Anwenders durch einen Online-Dienstanbieter, die Fernauthentifizierung der Zugangskarte eines Netzanwenders durch das Netz sowohl die Fernauthentifizierung einer gekauften Floppy-Diskette durch einen Software-Hersteller als eine Vorbedingung für das Leisten einer technischen Unterstützung.

[0077] Wenn eine Einzelperson z. B. Zugang zu einem Computernetz wünscht, kann das Netz den Zugang von der Vorbedingung abhängig machen, daß der Anwender die Fingerabdruckdaten für einen oder für mehrere ausgewählte Abschnitte einer magnetischen Zugangskarte erfolgreich übertragen kann. In dieser Ausführung übermittelt das Netz an den Anwender zunächst einen Auswahlbefehl, der einen bestimmten Abschnitt oder bestimmte Abschnitte der magnetischen Zugangskarte angibt, für die das remanente Rauschen bestimmt werden soll. Der Computer des Anwenders bestimmt dann das remanente Rauschen für den ausgewählten Abschnitt des Mediums und übermittelt einen dafür repräsentativen digitalen oder anderen Code an das Netz. Unterdessen gewinnt das Netz aus einer zentralen Datenbank die zuvor gespeicherten remanenten Rauschdaten für den ausgewählten Abschnitt der magnetischen Zugangskarte dieses Anwenders wieder. Falls die durch den Anwender gelieferten Fingerabdruckdaten mit den wiedergewonnenen remanenten Rauschdaten für den ausgewählten Abschnitt des magnetischen Mediums korrelieren, wird das magnetische Medium authentifiziert und wird bestätigt, daß es der Anwender besitzt. Dementsprechend wird dem Anwender Zugang zu dem Netz gewährt.

[0078] Das nächste Mal, wenn der Anwender Zugang zu dem Netz wünscht, wird eine ähnliche Operation ausgeführt, wobei aber höchstwahrscheinlich durch das Netz für Authentifizierungszwecke ein anderer oder zusätzlicher Abschnitt der magnetischen Zugangskarte ausgewählt wird. Mit anderen Worten, kann zur Auswahl des während jedes Authentifizierungsverfahrens verwendeten Abschnitts des magnetischen Mediums ein zufälliger oder sich nicht wiederholender Auswahlalgorithmus verwendet werden. Da sichergestellt ist, daß die gelieferten Daten nur für diesen Zugangsversuch gültig sind, wird auf diese Weise irgendein elektronisches Lauschen oder Online-Datenabhören der durch den Anwender an das Netz gelieferten Fingerabdruckdaten unschädlich gemacht. Sollten die Fingerabdruckdaten durch einen Dritten abgehört oder anderweitig erhalten werden,

sollte der Dritte die abgehörten Daten nachfolgend nicht zum Zugang zu dem Netz verwenden können. Falls ein solcher Versuch unternommen wird, wird durch das Netz das remanente Rauschen für einen anderen oder für einen zusätzlichen Abschnitt der magnetischen Zugangskarte des autorisierten Anwenders angefordert, wobei der Dritte auf diese Anforderung nicht erfolgreich reagieren kann.

[0079] Dieser Zugang zur Fernauthentifizierung geht von der Erkenntnis der Erfinder aus, daß von dem remanenten Rauschen eines magnetischen Mediums mit einer endlichen Länge oder mit einem endlichen Oberflächeninhalt eine sehr große Anzahl von Fingerabdrücken abgeleitet werden kann. Zum Beispiel kann von dem Magnetstreifen der in [Fig. 22](#) gezeigten magnetischen Datenkarte eine große Anzahl von Fingerabdrücken abgeleitet werden. Jedesmal, wenn die magnetische Datenkarte **210** fernauthentifiziert wird, kann ein anderer Abschnitt des Magnetstreifens **212** ausgewählt werden. Wenn die magnetische Datenkarte **210** z. B. für den Zugang zu einem Online-Computernetz verwendet wird, kann das Netz zur Fernauthentifizierung der magnetischen Datenkarte **210** einen Abschnitt "A" des Magnetstreifens **212** auswählen. Wenn der Anwender die von dem remanenten Rauschen für den Abschnitt "A" abgeleiteten Fingerabdruckdaten liefert und wenn dieser Code mit den durch das Netz aus einer zentralen Datenbank wiedergewonnenen zuvor gespeicherten remanenten Rauschdaten für den Abschnitt "A" der magnetischen Datenkarte **210** korreliert, wird die Karte authentifiziert und der Zugang gewährt. Wenn der Anwender nachfolgend wieder Zugang zu dem Netz begehrt, wählt das Netz für Fernauthentifizierungszwecke einen anderen Abschnitt des Magnetstreifens **212** wie etwa den von dem Abschnitt "A" vollkommen verschiedenen Abschnitt "C" oder den Abschnitt "B", der sich mit dem zuvor ausgewählten Abschnitt "A" überschneidet, oder den Abschnitt "D", der eine kleinere Leselänge als der Abschnitt "A" besitzt. Außerdem kann der Magnetstreifen mehrere Spuren umfassen, wobei das Netz jedesmal, wenn die magnetische Datenkarte fernauthentifiziert wird, zufällig einen anderen Abschnitt einer oder mehrerer der Spuren auswählen kann.

[0080] Es ist selbstverständlich, daß [Fig. 22](#) nicht maßstabgerecht gezeichnet ist, und daß die Länge des ausgewählten Abschnitts des magnetischen Datenstreifens, um das für den ausgewählten Abschnitt gemessene remanente Rauschen mit einer vorausgehenden Bestimmung davon erfolgreich zu korrelieren, wie oben festgestellt wurde, lediglich zwischen etwa 30 und 4.300 Mikrometern zu betragen braucht. Dadurch, daß jedesmal, wenn die magnetische Datenkarte **210** fernauthentifiziert wird, routinemäßig ein anderer Abschnitt des Magnetstreifens **212** ausgewählt wird, wobei sich der ausgewählte Abschnitt mit einem zuvor ausgewählten Abschnitt überschnei-

den oder nicht überschneiden kann, wobei er die gleiche, im wesentlichen die gleiche oder eine signifikant andere Länge als ein zuvor ausgewählter Abschnitt haben kann, kann somit von einem einzelnen Magnetstreifen **212** eine große Anzahl von Fingerabdrücken abgeleitet werden, wobei jeder Fingerabdruck einen einmaligen, nicht wiederverwendbaren Zugangscode für den Zugang zu dem Computernetz darstellen kann. In diesem Beispiel kann das Netz zum Auswählen des für Fernauthentifizierungszwecke zu verwendenden Abschnitts des Magnetstreifens **212** einen zufälligen, nicht wiederholenden Zugang oder irgendeinen anderen Auswahlalgorithmus verwenden.

[0081] Obgleich das Auswählen eines einzelnen, aber verschiedenen Abschnitts des Magnetstreifens **212** jedesmal, wenn die magnetische Datenkarte **210** authentifiziert wird, für die Mehrzahl der Anwendungen dieser Ausführung der vorliegenden Erfindung eine hinreichend große Anzahl von Fingerabdrücken liefert, kann durch das Zusammensetzen von Fingerabdrücken aus den für mehrere Abschnitte des Magnetstreifens **212** bestimmten remanenten Rauschdaten eine noch größere Anzahl von Fingerabdrücken erzeugt werden. Zum Beispiel kann das Netz den fernen Anwender mit einem Auswahlbefehl auffordern, der die remanenten Rauschdaten für jeden der sich überschneidenden Abschnitte "A" und "B" anfordert. Als Antwort auf diese Anforderung kann der Kartenleser des fernen Anwenders das remanente Rauschen für jeden Abschnitt messen, wobei er diese gemessenen remanenten Rauschen zu einem einzelnen Fingerabdruck zusammenfaßt. Das Netz vergleicht dann diesen durch den Anwender gelieferten Fingerabdruck mit einem aus früheren Bestimmungen der remanenten Rauschen für die ausgewählten sich überschneidenden Abschnitte "A" und "B" zusammengesetzten Fingerabdruck. Ähnlich können zum Erzeugen zusätzlicher Fingerabdrücke mehrere sich nicht überschneidende Abschnitte oder mehrere Abschnitte mit unterschiedlichen Leselängen oder sogar mehrere Abschnitte mit unterschiedlichen Längen, von denen sich einige überschneiden und einige sich nicht überschneiden, oder irgendeine andere Kombination mehrerer Abschnitte verwendet werden. Somit ist selbstverständlich, daß für eine gegebene Anwendung zum Erzeugen der Fingerabdruckdaten in Abhängigkeit lediglich von den akzeptablen Übertragungs- und/oder Verarbeitungszeiten und Speicheranforderungen mehr als zwei Abschnitte und tatsächlich irgendeine Anzahl von Abschnitten des Magnetstreifens **212** verwendet werden können.

[0082] Um eine noch höhere Sicherheit zu schaffen, kann von mehreren Abschnitten des Magnetstreifens **212** ein Hybrid-Fingerabdruck abgeleitet werden, wobei die Digitaldaten der für die mehreren ausgewählten Abschnitte gemessenen remanenten Rauschen wie etwa durch Addieren, Subtrahieren, Mitteln usw.

in der Weise linearkombiniert werden, daß kein einzelner Abschnitt der Hybrid-Fingerabdruckdaten eine Ähnlichkeit zu den von nur einem ausgewählten Abschnitt erhaltenen remanenten Rauschdaten zeigt. Der Hybrid-Fingerabdruck wird dann zum Vergleich mit der gleichen Linearkombination der gespeicherten remanenten Rauschdaten für die ausgewählten Abschnitte an das Netz übertragen.

[0083] Obgleich die Erfinder diese verschiedenen Methodiken zum Ableiten zahlreicher Fingerabdrücke von einem magnetischen Medium mit einer endlichen Länge oder mit einem endlichen Oberflächeninhalt entwickelt haben, ist selbstverständlich, daß die Lehren der vorliegenden Erfindung ebenfalls durch die Verwendung einer sehr kleinen Anzahl von Fingerabdrücken für Authentifizierungszwecke realisiert werden können. Falls ein Computernetz z. B. jedesmal, wenn die Zugangskarte authentifiziert wird, abwechselnd die remanenten Rauschdaten von einem von nur zwei Abschnitten der magnetischen Zugangskarte eines Anwenders anfordert, und falls die durch den Anwender an das Netz übertragenen Fingerabdruckdaten abgehört werden, besteht, wenn das Netz die Zugangskarte während irgendwelcher nachfolgenden Zugangsversuche authentifiziert, nur eine Wahrscheinlichkeit von 50 Prozent, daß die abgehörten Daten nutzbar sind. Je größer die Anzahl der Fingerabdrücke ist, die für Authentifizierungszwecke ausgewählt werden können, desto größer ist natürlich die Sicherheit.

[0084] Um einem Dritten, der den Auswahlbefehl abhört, das Ermitteln des Abschnitts oder der Abschnitte des magnetischen Mediums des Anwenders, für den bzw. für die die remanenten Rauschdaten übertragen werden, zu erschweren, wenn nicht sogar unmöglich zu machen, kann der von dem Netz an den Anwender übertragene Auswahlbefehl für eine nochmals höhere Sicherheit verwürfelt oder verschlüsselt werden. Ähnlich können die Fingerabdruckdaten vor der Übertragung verwürfelt oder verschlüsselt werden. Diese Zugänge machen in Verbindung mit jedem der oben diskutierten Zugänge ferner irgendeinen Versuch durch einen Dritten, im Laufe der Zeit die remanenten Rauschdaten für wesentliche Abschnitte der magnetischen Datenkarte oder eines anderen Mediums eines Anwenders zu sammeln, zunichte.

[0085] Dort, wo die magnetische Datenkarte die wohlbekannte Kreditkarte ist, legt die vorliegende Erfindung vor dem Verrechnen einer besonderen Transaktion zwei sichere Verfahren zum Authentifizieren einer Kreditkarte nahe. Die zuvor auf der Kreditkarte aufgezeichneten Fingerabdruckdaten können zur Verarbeitungspunkt-Authentifizierung verwendet werden, wobei die Kreditkarte zur Bezahlung einer besonderen Transaktion physikalisch durch den Kreditkarteninhaber an einen Einzelhändler

übergeben wird. Alternativ, oder wenn die Einzelperson ihre Kreditkarte wie etwa online oder per Telefon fern von dem Einzelhändler verwendet, kann der Verkäufer seine Akzeptanz der Kreditkartenzahlung an die Vorbedingung knüpfen, daß die Einzelperson erfolgreich die Fingerabdruckdaten für einen oder für mehrere Abschnitte des Magnetstreifens liefern kann. Durch die Verwendung dieser Methodiken kann die weitverbreitete betrügerische Verwendung gestohlener Kreditkartennummern drastisch reduziert, wenn nicht vollständig beseitigt werden.

[0086] Um die Anzahl der Fingerabdrücke, die von der Datenkarte erhalten und gespeichert werden könnten, zu erhöhen, kann die magnetische Datenkarte, wie oben erwähnt wurde, außerdem mit einem zweiten Magnetstreifen versehen werden. Ein Abschnitt eines Magnetstreifens oder beider Magnetstreifen einschließlich einer Spur oder mehrerer der mehreren Spuren kann für Authentifizierungszwecke reserviert und möglicherweise zu einem Authentifizierungsgebiet bestimmt werden, oder es kann ein gesamter Streifen in dieser Weise bestimmt werden. Eine solche magnetische Datenkarte **215** mit zwei Magnetstreifen **216**, **218** ist in [Fig. 23](#) gezeigt. Zweckmäßig wird der erste Magnetstreifen **216** zum Aufzeichnen von Standarddaten, wie es im Gebiet wohlbekannt ist, verwendet, während der zweite Streifen **218** zur Bestimmung der remanenten Rauschdaten daraus für Authentifizierungszwecke reserviert ist. Die remanenten Rauschdaten für einen oder für beide Magnetstreifen **216**, **218** können außerdem auf einem oder auf beiden Streifen und/oder in einer Datenbank zur nachfolgenden Verwendung während eines Bestätigungsverfahrens bestimmt und aufgezeichnet werden.

[0087] [Fig. 24](#) zeigt eine Realisierung der Lehren der vorliegenden Erfindung für den Fall der Kreditkartentransaktionen. Wenn ein ferner Anwender **220** unter Verwendung einer Kreditkarte **224** Waren oder Dienste von einem Online-Geschäft **222** kaufen möchte, bestätigt das Online-Geschäft **222** dadurch, daß es mit der Kreditkartengesellschaft **226** des Anwenders Kontakt aufnimmt, zunächst, daß der ferne Anwender **220** die Kreditkarte **224** besitzt und daß die Kreditkarte eine gute Bonität besitzt. Das Online-Geschäft **222** löst diese Transaktion dadurch aus, daß es an die Kreditkartengesellschaft eine Transaktionsanforderung **228** sendet, wobei diese Informationen über den fernen Anwender wie etwa den Namen, die Kreditkartennummer usw. des Anwenders liefert. Diese in der Transaktionsanforderung **228** gelieferten Informationen werden dann zur Auswahl eines oder mehrerer Abschnitte des Magnetstreifens **232** der Kreditkarte **224** für Authentifizierungszwecke an eine Auswahlrichtung **230** geliefert. Die Auswahlrichtung gibt ein Auswahlsignal **234** aus, das über das Online-Geschäft **222** an den fernen Anwender geliefert wird, während es zum Wiedergewinnen

der zuvor bestimmten remanenten Rauschdaten für den ausgewählten Abschnitt des Magnetstreifens aus der Datenbank **238** an eine Wiedergewinnungseinrichtung **236** geliefert wird. Unterdessen verarbeitet der ferne Anwender das Auswahlsignal **234** und bestimmt unter Verwendung eines Lesers **240** das remanente Rauschen für den ausgewählten Abschnitt des Magnetstreifens. Wo durch das Auswahlsignal **234** mehrere Abschnitte des Magnetstreifens spezifiziert sind und, wie oben diskutiert wurde, zum Erzeugen eines Hybrid-Fingerabdrucks verwendet werden sollen, wird das Ausgangssignal des Lesers **240** zum Ausführen dieses Verfahrens an einen Kombinator **242** geliefert. Der Kombinator **242** liefert dann die Hybrid-Fingerabdruckdaten **244** an das Online-Geschäft **222**, das diese Daten seinerseits an die Kreditkartengesellschaft **226** liefert. Die Kreditkartengesellschaft verarbeitet die zuvor bestimmten remanenten Rauschdaten für die ausgewählten Abschnitte des Magnetstreifens ähnlich mit einem Kombinator **246**, der den gleichen Algorithmus wie der Kombinator **242** verwendet, wobei er ein Hybrid-Fingerabdruck-Datensignal **248** an einen Komparator **250** ausgibt. Der Komparator **250** vergleicht die durch den fernen Anwender gelieferten Fingerabdruckdaten mit den aus der Datenbank **238** erhaltenen Fingerabdruckdaten und liefert, wenn diese Daten korrelieren, an das Online-Geschäft **222** ein Authentifizierungssignal **252**, das angibt, daß die Kreditkarte **224** tatsächlich authentisch ist.

[0088] In allen oben und unten offenbarten Beispielen können die durch das Netz oder durch das Online-Geschäft, durch die zentrale Datenbank oder durch die ferne Einzelperson oder durch den fernen Anwender ausgeführten Funktionen einschließlich der Erzeugung des Auswahlbefehls, der Bestimmung der Fingerabdruckdaten, der Wiedergewinnung der gespeicherten remanenten Rauschdaten und der Korrelation der gemessenen Fingerabdrücke mit den gespeicherten Fingerabdrücken sämtlich mit geeigneten Computersystemen und mit herkömmlichen magnetischen Meßwandlern ausgeführt werden. Das Realisieren der Lehren der vorliegenden Erfindung unter Verwendung eines herkömmlichen Computersystems und geeigneter Software ist eine Frage der üblichen Sachkenntnis.

[0089] Im Fall der Zugangskarten für den Zugang zu sicheren Computersystemen oder Datenbanken könnte die Zugangskarte eine Diskette sein, wobei das System eine Datenbank zuvor für mehrere Abschnitte der Diskette bestimmter remanenter Rauschdaten enthält. Alternativ kann die Zugangskarte eine magnetische Datenkarte und sogar eine Mehrzweck-Zugangskarte/Kreditkarte sein.

[0090] Ebenso wie eine Computer-Diskette, wie oben beschrieben wurde, als eine Zugangskarte verwendet werden kann, kann ein Hardware- oder Soft-

ware-Hersteller, der Computer-Software kommerziell verteilt, vor dem Verkauf oder vor dem anderweitigen Verteilen einer Diskette an die Öffentlichkeit die remanenten Rauschdaten für mehrere Abschnitte der Floppy-Diskette speichern. Falls danach ein vorgeblicher Käufer der Software von dem Software-Hersteller technische Unterstützung begehrt, kann der Software-Hersteller die remanenten Rauschdaten für einen oder für mehrere Abschnitte der gekauften Diskette anfordern, um zu bestätigen, daß die Diskette die authentische, original gekaufte Diskette ist. Um dieses Verfahren zu erleichtern, kann der Software-Hersteller zunächst eine laufende Nummer oder weitere Kennzeichen für die Diskette anfordern, die der Hersteller zum Indizieren einer zentralen Datenbank und zum Wiedergewinnen der zuvor für diese Diskette bestimmten remanenten Rauschdaten verwenden kann. Die gekaufte Diskette enthält zweckmäßig eine Software zum Messen der remanenten Rauschdaten in irgendeinem ausgewählten Abschnitt der Diskette. Falls die durch den Käufer gemessenen und übertragenen remanenten Rauschdaten mit den von dem Hersteller wiedergewonnenen remanenten Rauschdaten korrelieren, wird die Diskette als authentisch erklärt. Alternativ können die zuvor bestimmten remanenten Rauschdaten verschlüsselt und auf der Diskette gespeichert werden. Während des Authentifizierungsverfahrens kann der Anwendercomputer das für einen durch den Anwender ausgewählten Abschnitt der Diskette gemessene remanente Rauschen zusammen mit den dem ausgewählten Abschnitt entsprechenden verschlüsselten Daten senden. Der Hersteller kann dann die gespeicherten Daten entschlüsseln und sie mit dem gemessenen remanenten Rauschen vergleichen, um zu bestätigen, daß die Diskette authentisch ist. Beide Verfahren zum Fernauthentifizieren der Diskette durch einen Software-Hersteller können in der gleichen Weise, wie es oben in bezug auf magnetische Datenkarten diskutiert wurde, online ausgeführt werden.

[0091] Wo ein vorgeblicher Käufer technische Unterstützung per Telefon begehrt, kann der Software-Hersteller den vorgeblichen Käufer zunächst bitten, die remanenten Rauschdaten für einen bestimmten Abschnitt der Diskette wie etwa "RQ5" zu liefern. Der Käufer kann dann "RQ5" in seinen Computer eingeben, wobei die mit der gekauften Diskette gelieferte Authentifizierungs-Software diese Anforderung übersetzen und das remanente Rauschen für einen besonderen Abschnitt der Diskette bestimmen kann und dann auf dem Computermonitor einen für den Menschen lesbaren Code liefern kann, der das bestimmte remanente Rauschen darstellt. Der Käufer kann dann den für den Menschen lesbaren Code über das Telefon dem Software-Hersteller vorlesen, so daß der Hersteller diesen Code mit dem zuvor bestimmten remanenten Rauschen vergleichen kann, um somit die Käuferdiskette, bevor technische Unterstützung geleistet wird, zu authentifizieren. Das

nächste Mal, wenn der Käufer technische Unterstützung begehrt, kann für Authentifizierungszwecke ein anderer oder ein zusätzlicher Abschnitt der Diskette ausgewählt werden. Somit kann der für den Menschen lesbare Code jedesmal, wenn der Käufer technische Unterstützung begehrt, geändert werden. Auf diese Weise können die Software-Hersteller ihre Kosten für die Lieferung der technischen Unterstützung auf die tatsächlichen Käufer ihrer Software oder wenigstens auf die Einzelpersonen, die eine gekaufte Diskette physikalisch besitzen, beschränken. Obgleich diese Ausführung und viele weitere Ausführungen der betreffenden Erfindung mit Bezug auf besondere Arten magnetischer Medien wie etwa auf Disketten, Bänder, Kreditkarten, Zugangskarten usw. beschrieben wurden, ist selbstverständlich, daß diese Ausführungen ebenso auf andere hier beschriebene Arten magnetischer Medien sowie auf irgendeine andere Art eines magnetischen Mediums, das dem gleichen oder einem ähnlichen Zweck dient, anwendbar sind. Zum Beispiel kann im Fall der durch die Software-Hersteller geleisteten technischen Unterstützung die Software statt dessen z. B. auf einem Digitalband geliefert werden, wobei zum Authentifizieren des Bands vor dem Leisten der technischen Unterstützung die gleichen obenbeschriebenen Methodiken verwendet werden können. Durch dauerhaftes Befestigen eines magnetischen Mediums wie etwa eines magnetischen Etiketts an dem Objekt kann zum Realisieren jeder der oben diskutierter Ausführungen die vorliegende Erfindung außerdem auf Objekte erstreckt werden, die ursprünglich kein magnetisches Medium enthalten. Zum Beispiel könnte ein Funktelefon zur Fernauthentifizierung des Telefons und zur Verhinderung der Verwendung irgendwelcher illegaler Klone davon mit einem Magnetetikett oder mit einem anderen magnetischen Medium versehen werden.

[0092] Für den Fachmann im Gebiet ist klar, daß an der Erfindung verschiedene Änderungen und Modifizierungen vorgenommen werden können. Diese Änderungen oder Modifizierungen sind jedoch in der Lehre der Offenbarung enthalten, wobei die Erfindung lediglich durch den Umfang der hierzu beigefügten Ansprüche und ihrer Entsprechungen beschränkt werden soll.

Patentansprüche

1. Verfahren zum Authentifizieren eines Objekts, wobei das Objekt wenigstens teilweise ein magnetisches Medium **(212)** enthält, wobei das Verfahren die folgenden Schritte umfasst:

- Auswählen mehrerer Abschnitte (A, B, C, D) des magnetischen Mediums **(212)**, wobei wenigstens zwei der ausgewählten Abschnitte (A, B, C, D) unterschiedliche Abschnitte (A, B, C, D) umfassen,
- Erhalten von remanenten Rauschdaten von den ausgewählten Abschnitten (A, B, C, D) und

- Vergleichen der von den ausgewählten Abschnitten (A, B, C, D) erhaltenen remanenten Rauschdaten mit einer vorausgehenden Bestimmung davon, um somit zu bestimmen, ob das Objekt authentisch ist, wobei der Auswahlsschritt das Auswählen wenigstens zweier überlappender Abschnitte (A, B) des magnetischen Mediums **(212)** enthält.

2. Verfahren nach Anspruch 1, bei dem der Auswahlsschritt das Auswählen wenigstens zweier Abschnitte (A, B, C, D) des magnetischen Mediums **(212)** mit ungleichen Leselängen enthält.

3. Verfahren nach Anspruch 1 oder 2, das ferner die folgenden Schritte umfasst:

- lineares Kombinieren der von den mehreren ausgewählten Abschnitten (A, B, C, D) erhaltenen remanenten Rauschdaten, und
- lineares Kombinieren der zuvor für die mehreren ausgewählten Abschnitte (A, B, C, D) bestimmten remanenten Rauschdaten, wobei der Schritt des Vergleichens das Vergleichen der Linearkombinationen enthält, um somit zu bestimmen, ob das Objekt authentisch ist.

4. Verfahren zum Authentifizieren eines Objekts, wobei das Objekt wenigstens teilweise ein magnetisches Medium **(212)** enthält, wobei das Verfahren die folgenden Schritte umfasst:

- Auswählen mehrerer Abschnitte (A, B, C, D) des magnetischen Mediums **(212)**, wobei wenigstens zwei der ausgewählten Abschnitte (A, B, C, D) unterschiedliche Abschnitte (A, B, C, D) umfassen,
- Erhalten von remanenten Rauschdaten von den ausgewählten Abschnitten (A, B, C, D) und
- Vergleichen der von den ausgewählten Abschnitten (A, B, C, D) erhaltenen remanenten Rauschdaten mit einer vorausgehenden Bestimmung davon, um somit zu bestimmen, ob das Objekt authentisch ist, wobei der Auswahlsschritt das Auswählen wenigstens zweier Abschnitte (A, B, C, D) des magnetischen Mediums **(212)** mit ungleichen Leselängen enthält.

5. Verfahren nach Anspruch 4, bei dem der Auswahlsschritt das Auswählen wenigstens zweier überlappender Abschnitte (A, B) des magnetischen Mediums **(212)** enthält.

6. Verfahren nach Anspruch 4 oder 5, das ferner die folgenden Schritte umfasst:

- lineares Kombinieren der von den mehreren ausgewählten Abschnitten (A, B, C, D) erhaltenen remanenten Rauschdaten, und
- lineares Kombinieren der zuvor für die mehreren ausgewählten Abschnitte (A, B, C, D) bestimmten remanenten Rauschdaten, wobei der Schritt des Vergleichens das Vergleichen der Linearkombinationen enthält, um somit zu bestimmen, ob das Objekt authentisch ist.

7. Verfahren zum Authentifizieren eines Objekts, wobei das Objekt wenigstens teilweise ein magnetisches Medium (**212**) enthält, wobei das Verfahren die folgenden Schritte umfasst:

- Auswählen mehrerer Abschnitte (A, B, C, D) des magnetischen Mediums (**212**), wobei wenigstens zwei der ausgewählten Abschnitte (A, B, C, D) unterschiedliche Abschnitte (A, B, C, D) umfassen,
- Erhalten von remanenten Rauschdaten von den ausgewählten Abschnitten (A, B, C, D),
- lineares Kombinieren der von den mehreren ausgewählten Abschnitten (A, B, C, D) erhaltenen remanenten Rauschdaten und lineares Kombinieren der zuvor für die mehreren ausgewählten Abschnitte (A, B, C, D) bestimmten remanenten Rauschdaten, und
- Vergleichen der Linearkombinationen von den ausgewählten Abschnitten (A, B, C, D) erhaltenen remanenten Rauschdaten mit einer vorausgehenden Bestimmung davon, um somit zu bestimmen, ob das Objekt authentisch ist.

8. Verfahren nach Anspruch 7, bei dem der Auswahlschritt das Auswählen wenigstens zweier überlappender Abschnitte (A, B) des magnetischen Mediums (**212**) enthält.

9. Verfahren nach Anspruch 7 oder 8, bei dem der Auswahlschritt das Auswählen wenigstens zweier Abschnitte (A, B, C, D) des magnetischen Mediums (**212**) mit ungleichen Leselängen enthält.

Es folgen 9 Blatt Zeichnungen

Anhängende Zeichnungen

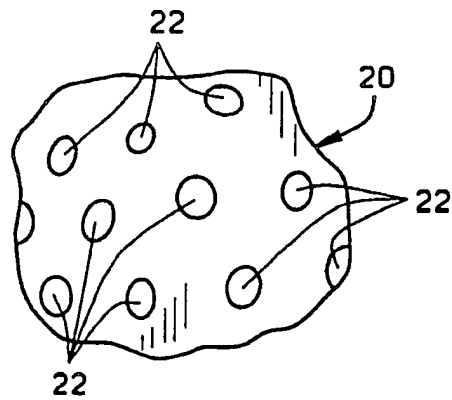


FIG. 1

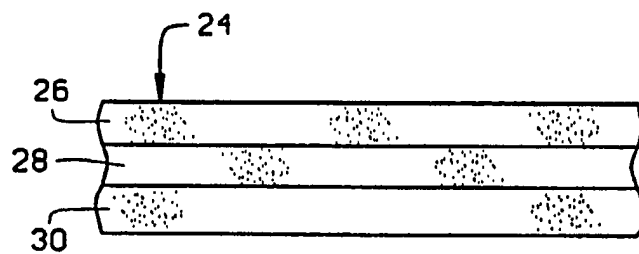


FIG. 2

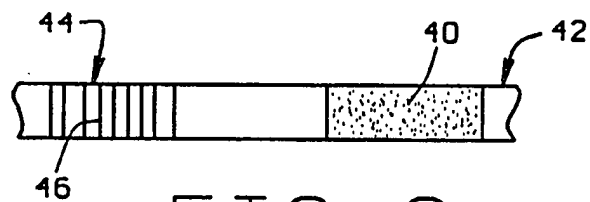


FIG. 3

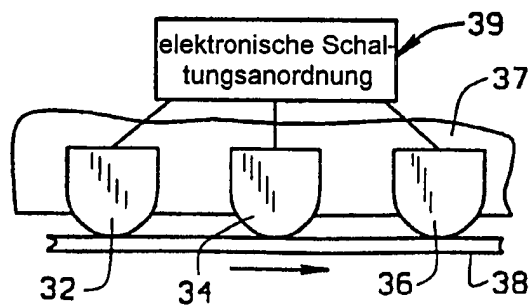


FIG. 4

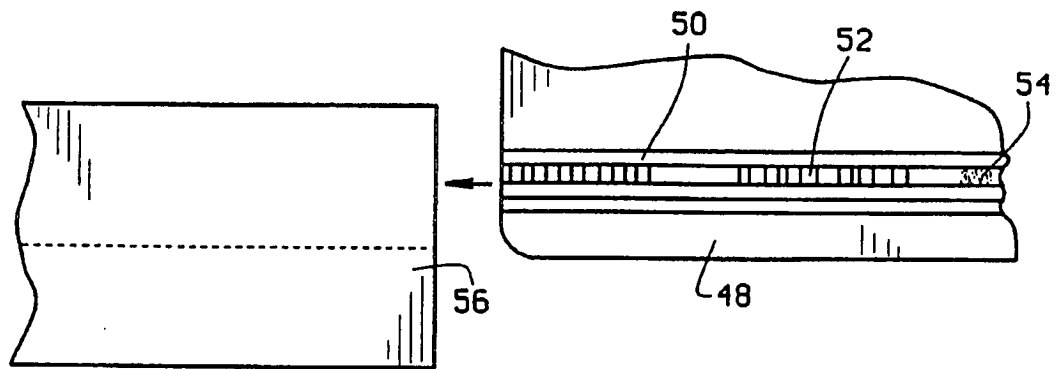


FIG. 5

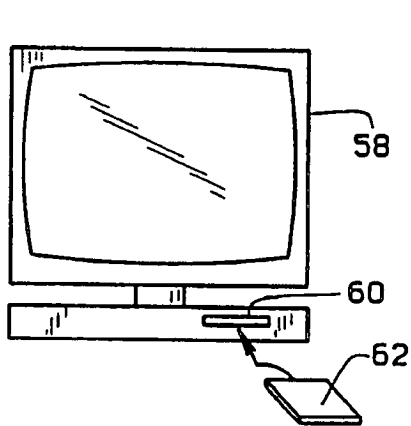


FIG. 6

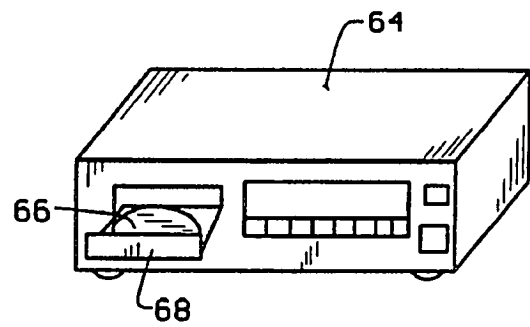


FIG. 7

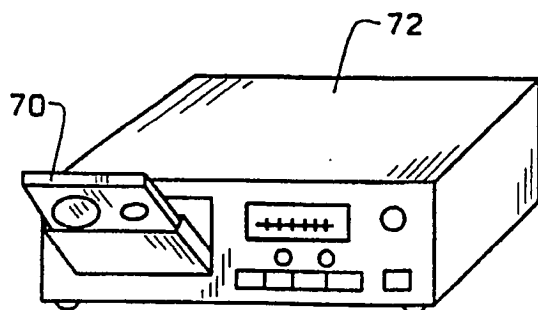


FIG. 8

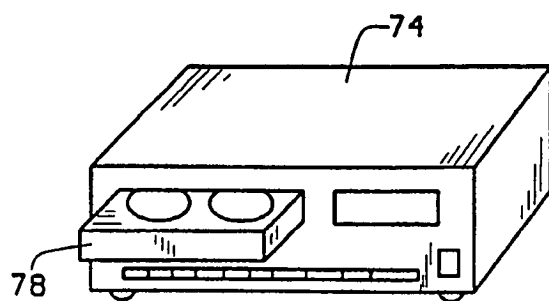


FIG. 9

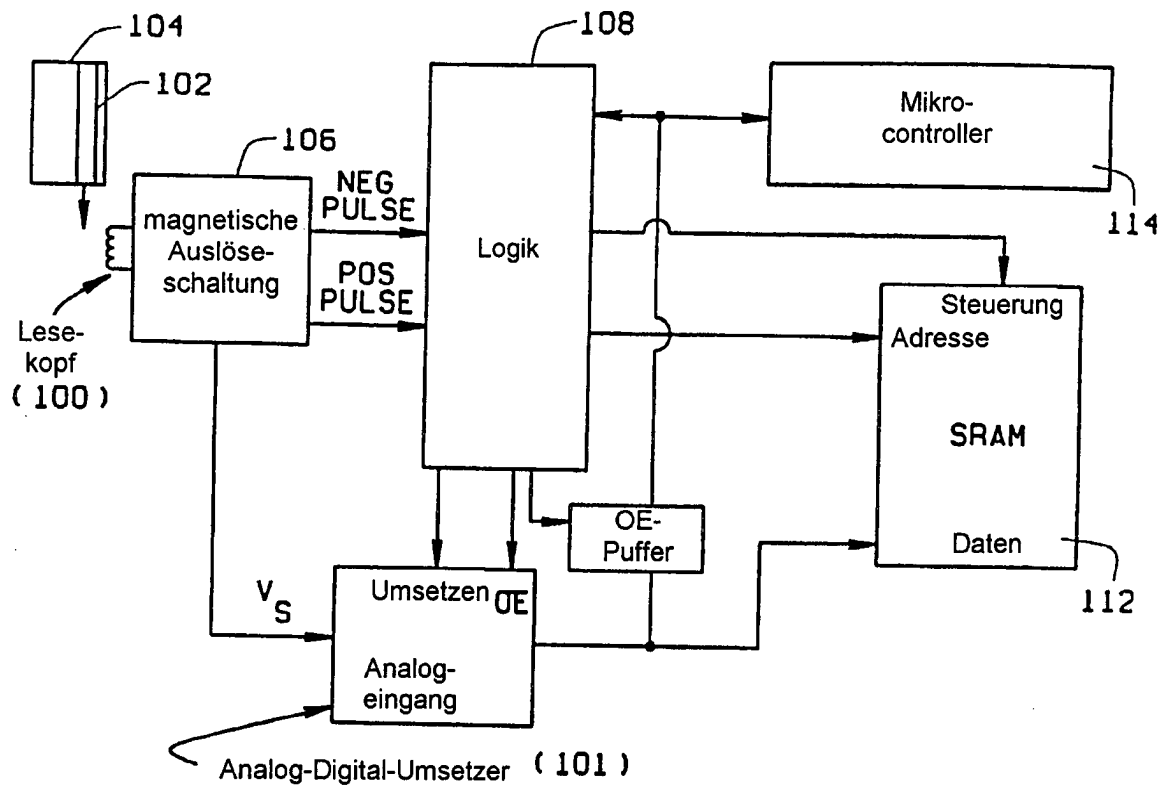


FIG. 10

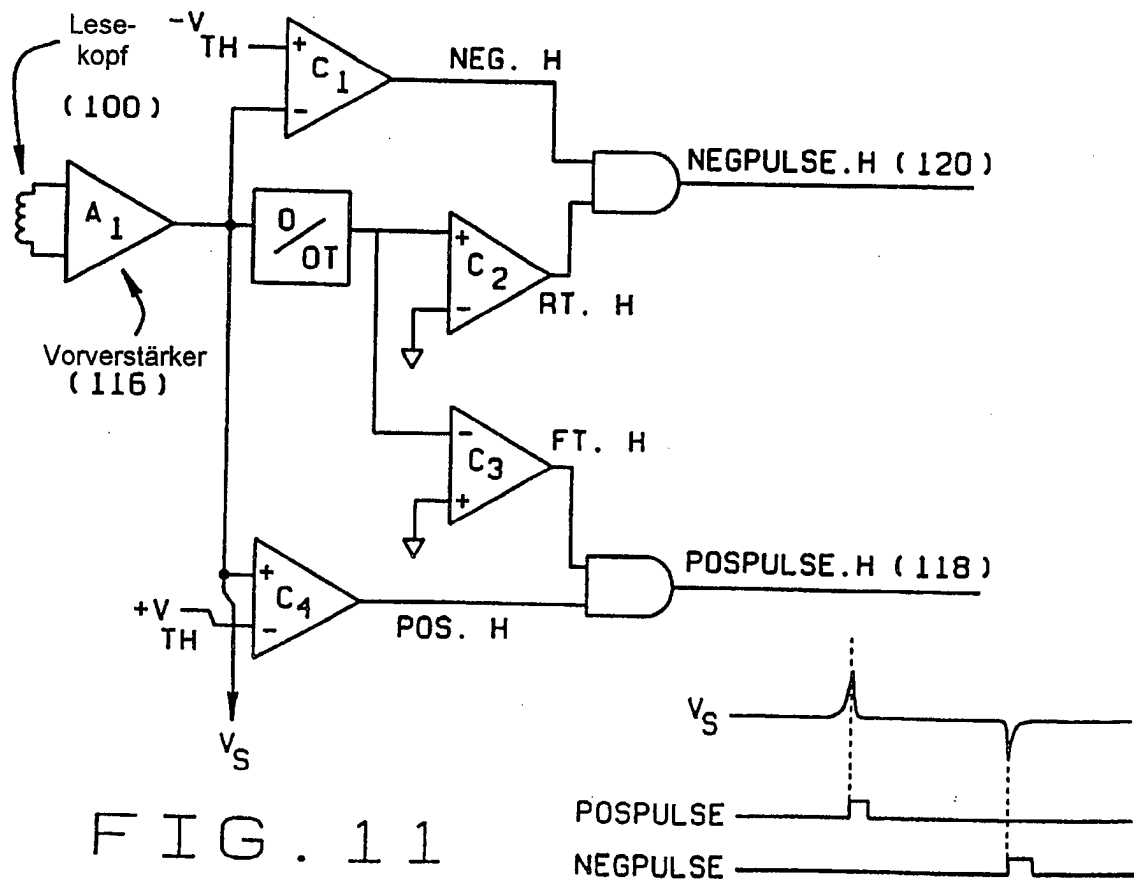


FIG. 11

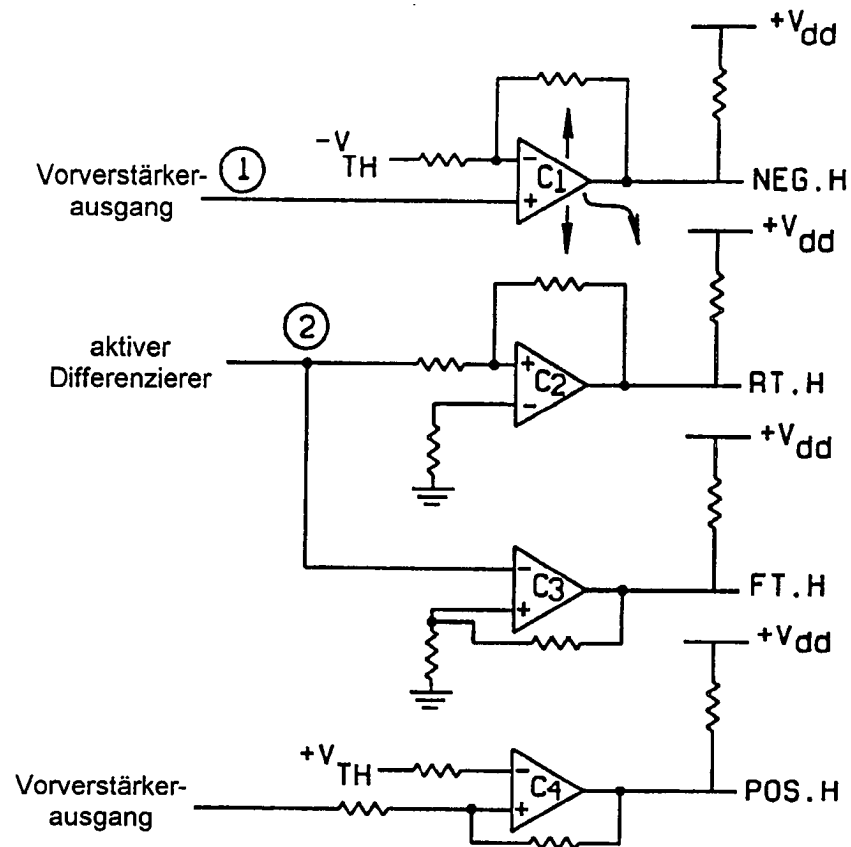


FIG. 12

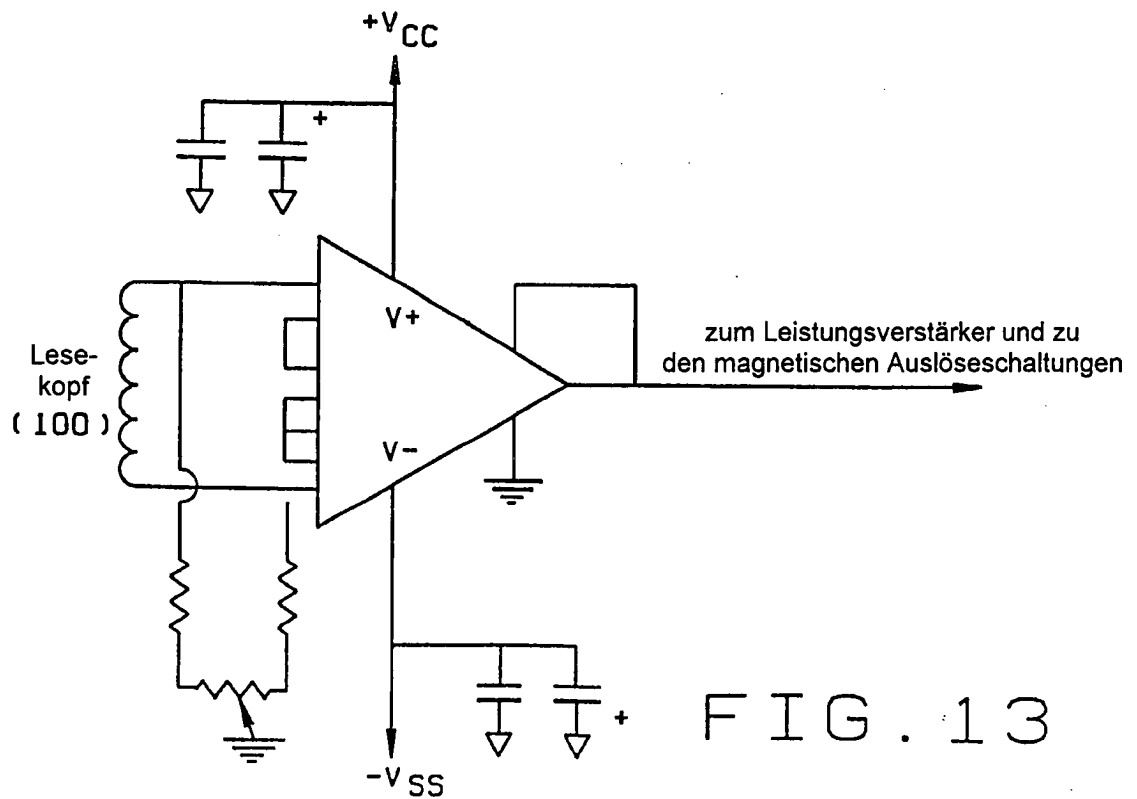


FIG. 13

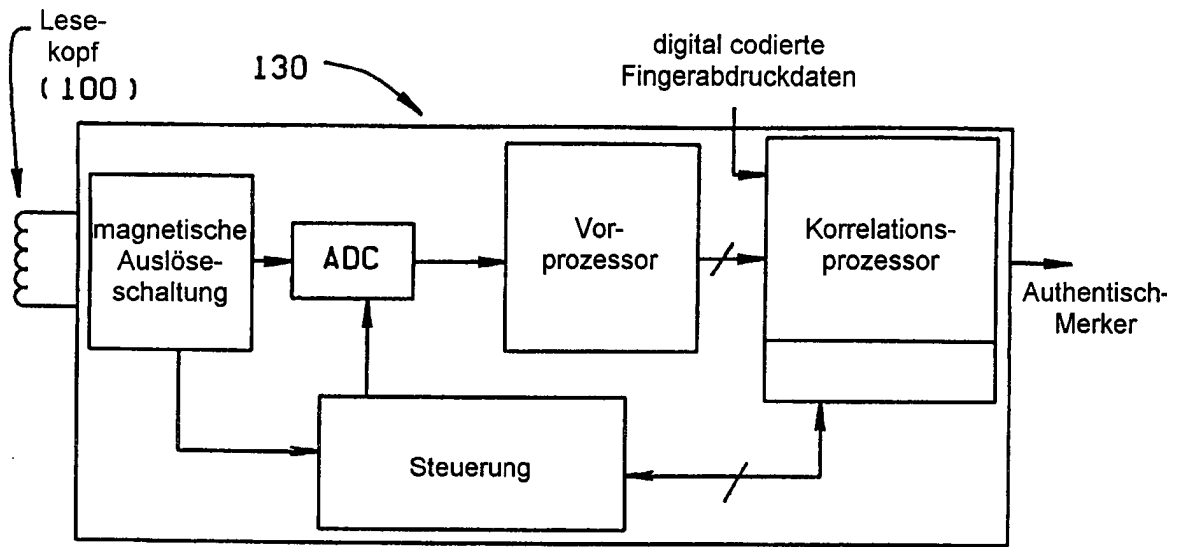


FIG. 14

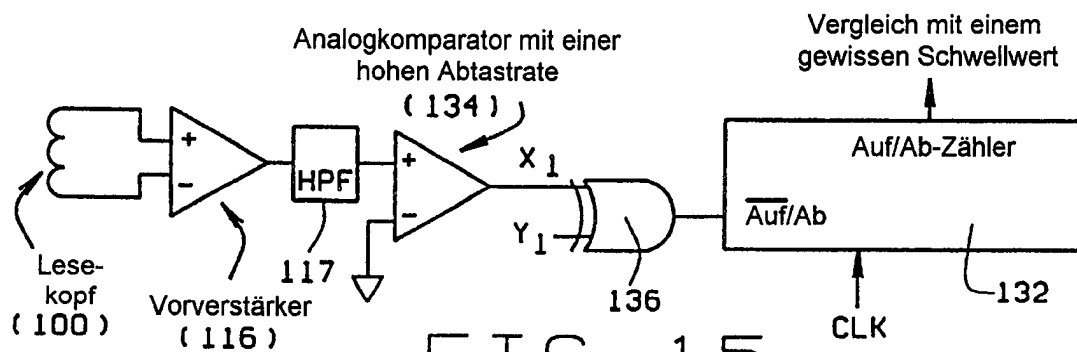


FIG. 15

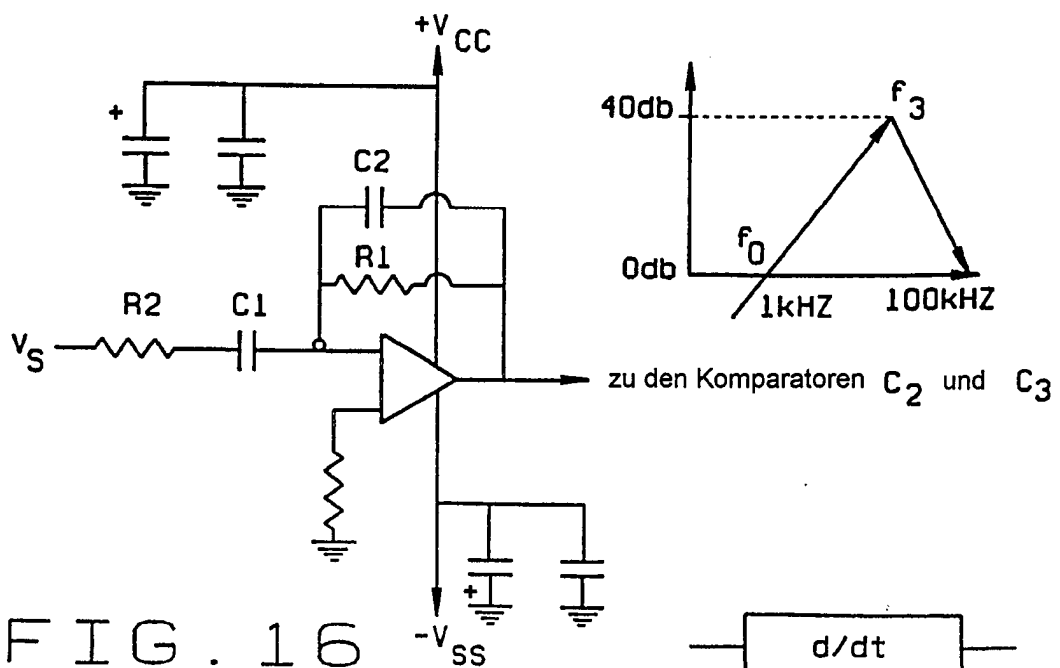


FIG. 16

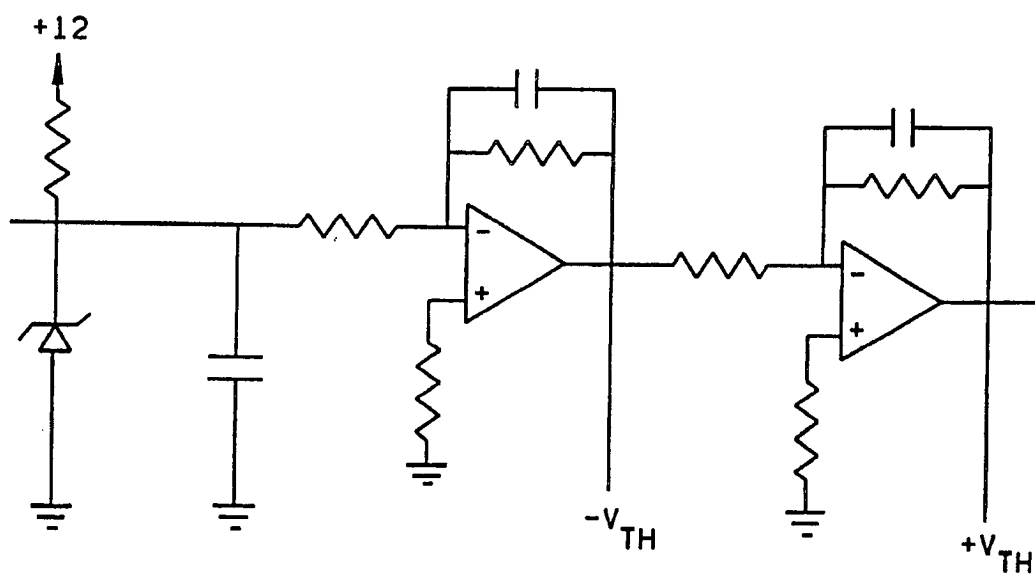


FIG. 17

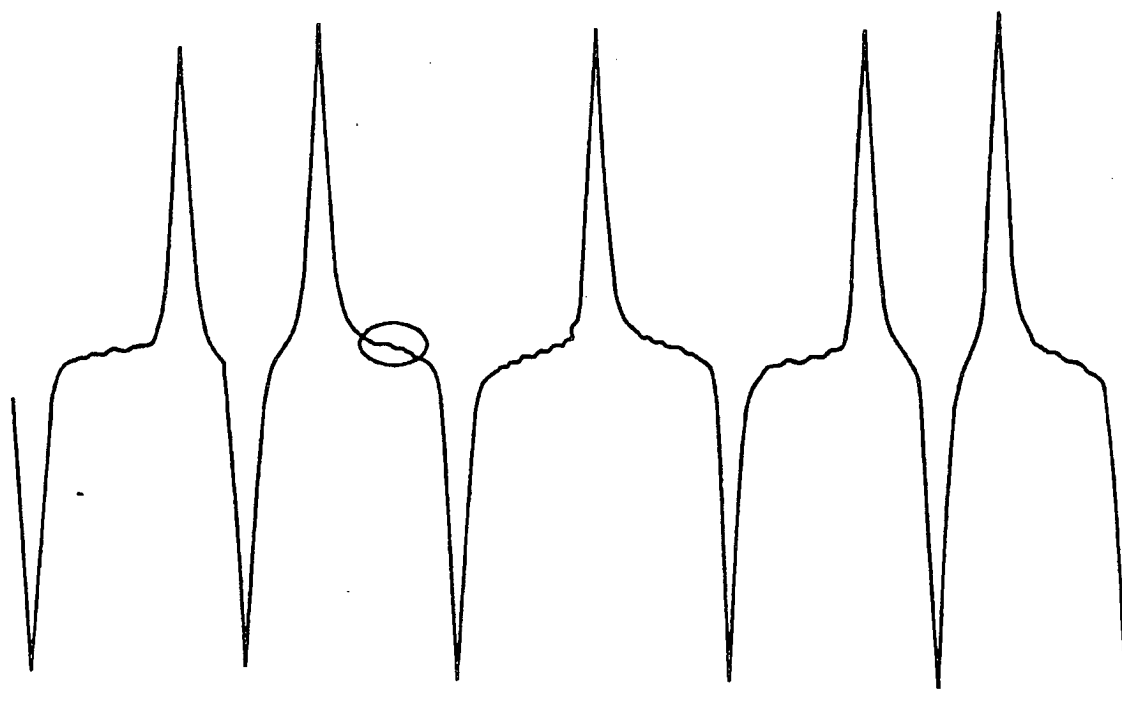
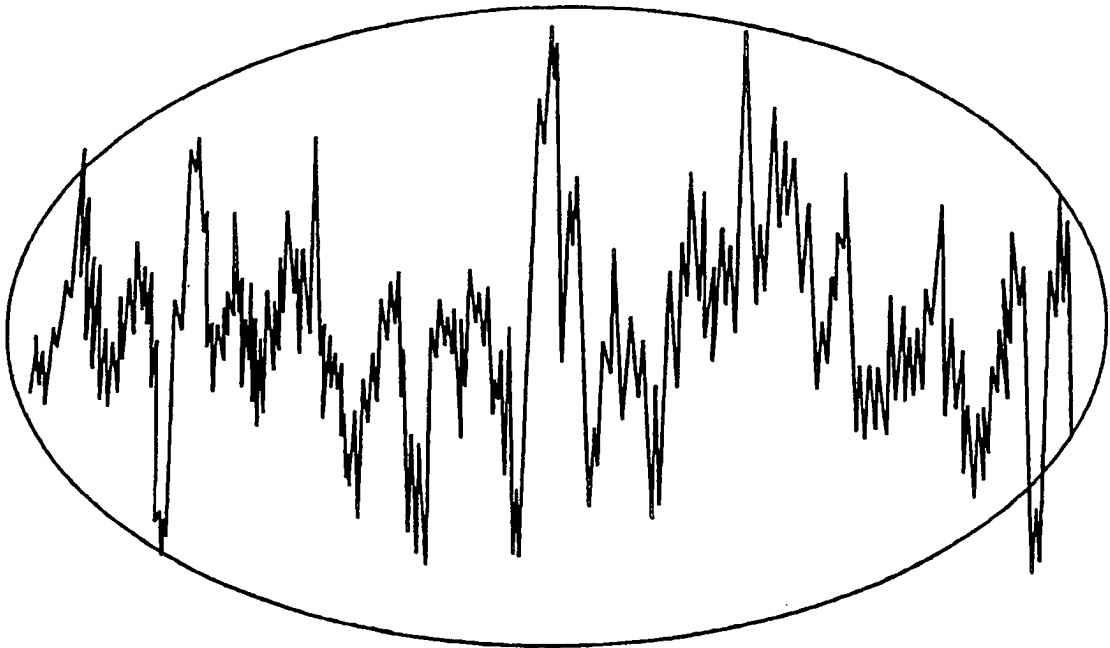
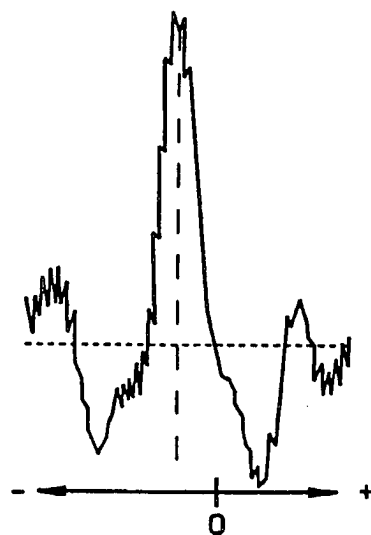


FIG. 18



magnetischer Fingerabdruck

FIG. 19



Laufzeitunterschied

FIG. 20

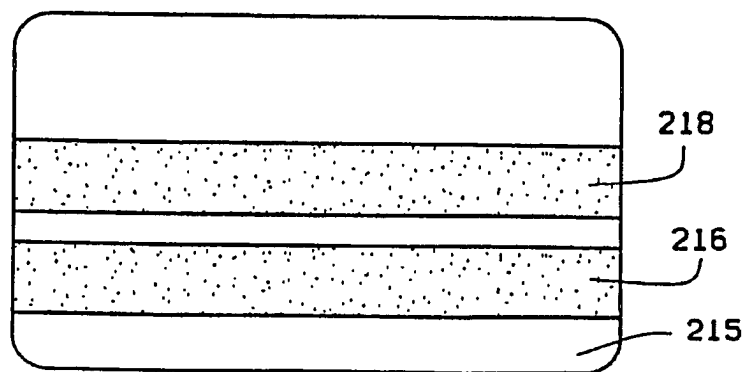
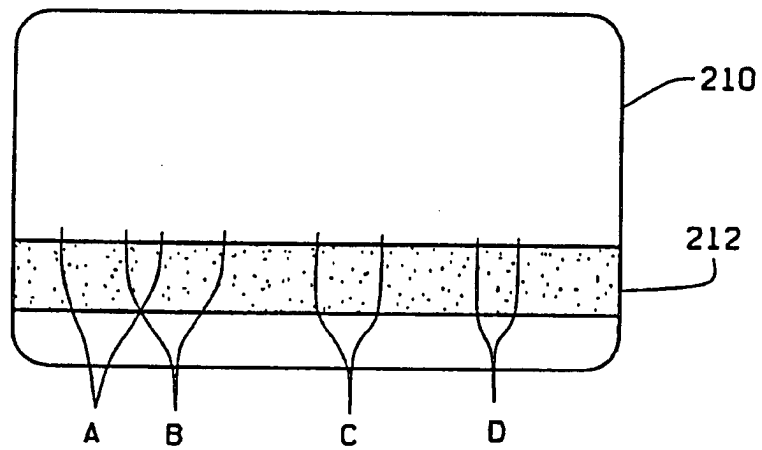
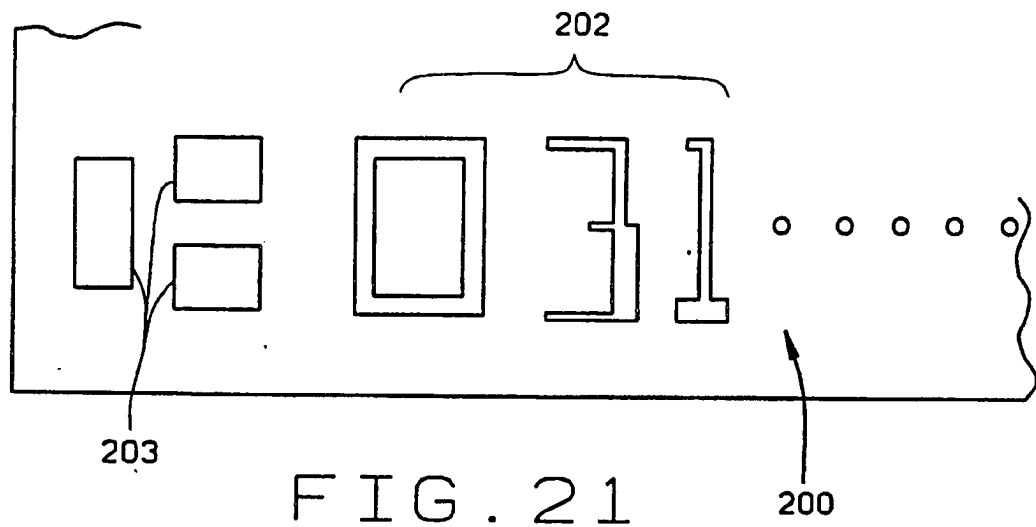


FIG. 23

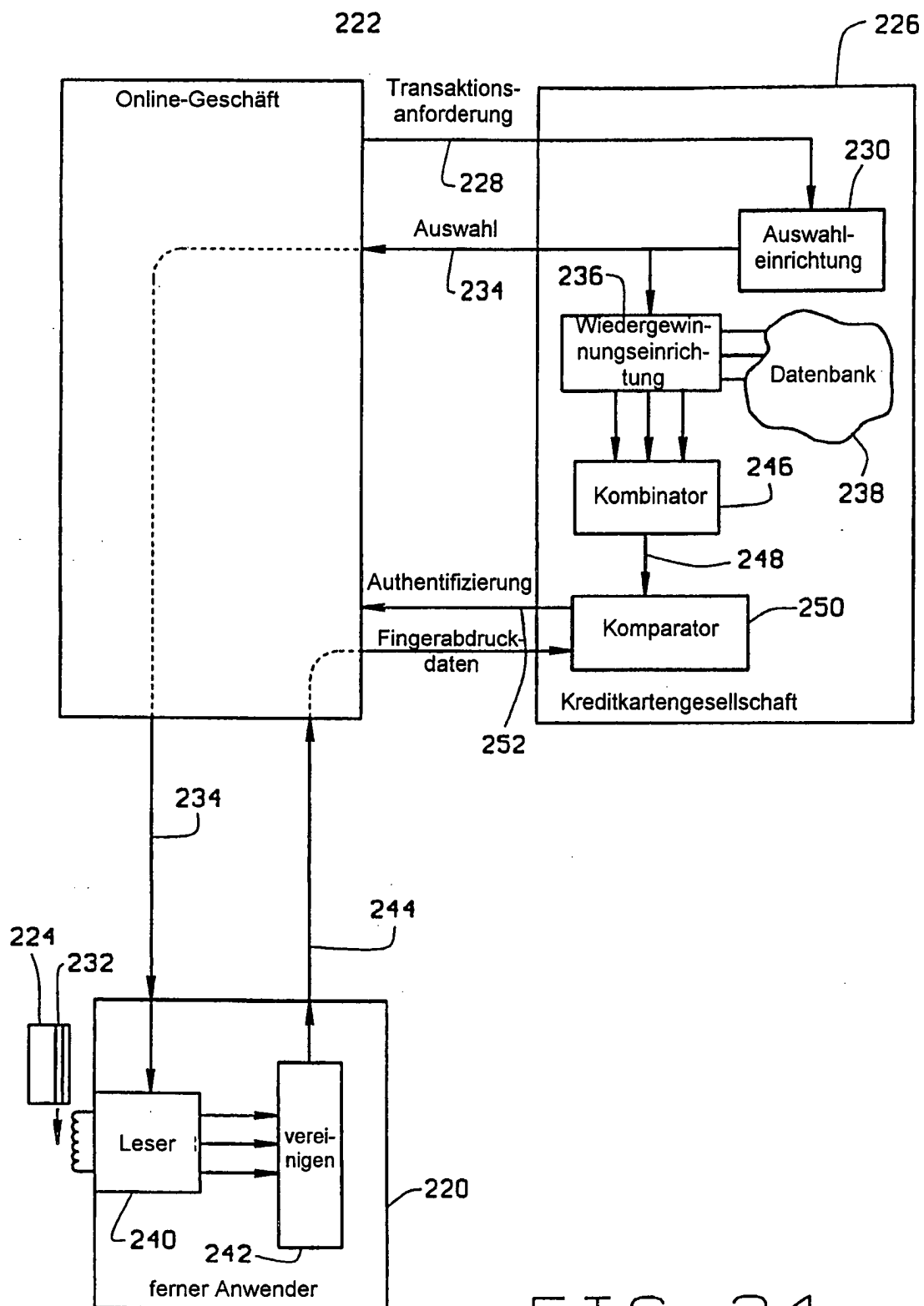


FIG. 24