(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 698 38 094 T2** 2008.04.03

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 963 637 B1**
(21) Deutsches Aktenzeichen: **698 38 094.0**
(86) PCT-Aktenzeichen: **PCT/IB98/02120**
(96) Europäisches Aktenzeichen: **98 959 116.9**
(87) PCT-Veröffentlichungs-Nr.: **WO 1999/035785**
(86) PCT-Anmeldetag: **28.12.1998**
(87) Veröffentlichungstag der PCT-Anmeldung: **15.07.1999**
(97) Erstveröffentlichung durch das EPA: **15.12.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **18.07.2007**
(47) Veröffentlichungstag im Patentblatt: **03.04.2008**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)

(30) Unionspriorität:
2098 **31.12.1997** **US**

(73) Patentinhaber:
Koninklijke Philips Electronics N.V., Eindhoven, NL

(74) Vertreter:
Volmer, G., Dipl.-Ing., Pat.-Anw., 52066 Aachen

(84) Benannte Vertragsstaaten:
DE, DK, FI, FR, GB, IT, NL, SE

(72) Erfinder:
EPSTEIN, Michael, NL-5656 AA Eindhoven, NL

(54) Bezeichnung: **ÜBERTRAGUNG VON REVISIONEN MIT DIGITALEN UNTERSCHRIFTEN**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

GEBIET DER ERFINDUNG

[0001] Die Erfindung bezieht sich auf das Gebiet der Kryptographie und insbesondere auf das kryptographische Zeitstempeln von Dokumenten, um deren Existenz zu einem bestimmten Zeitpunkt nachzuweisen.

HINTERGRUND DER ERFINDUNG

[0002] In vielen Situationen des täglichen Lebens müssen Menschen nachweisen, dass ein digitales Dokument (z.B. ein digital in einem Computersystem gespeichertes Dokument) zu einem bestimmten Zeitpunkt existierte. Das bedeutet, es kann notwendig sein, nachzuweisen, dass seit einem bestimmten Zeitpunkt, wie zum Beispiel dem geltend gemachten Erstellungsdatum oder dem Übertragungsdatum des Dokuments niemand das digitale Dokument verändert oder revidiert hat.

[0003] Ein Verfahren, einen solchen Nachweis zu liefern, ist bekannt als elektronische Beglaubigung oder Zeitstempeln (Timestamping). Es wird ein „Einweg-Hash" des Dokuments erstellt und der Hash-Wert unter Verwendung eines privaten Schlüssels des Urhebers des Dokuments verschlüsselt, um eine sogenannte digitale Signatur zu erstellen. Die Dokumentsignatur wird an einen elektronischen Notar oder einen Zeitstempler geschickt, der die digitale Signatur mit einem digitalen Zeitpunkt (digitale Darstellung des Zeitpunkts und des Datums) verbindet, um einen Zeitstempel zu erstellen, einen Hash-Wert des Zeitstempels bildet und den Hash-Wert des Zeitstempels unter Verwendung des digitalen privaten Schlüssels des elektronischen Notars verschlüsselt, um eine weitere digitale Signatur zu erstellen, die Zeitstempelsignatur genannt wird. Dann sendet der Notar eine den Zeitstempel und die Zeitstempelsignatur enthaltende Zertifizierung an den Verfasser. Jeder, der den öffentlichen Schlüssel des Notars besitzt, kann die Zeitstempelsignatur entschlüsseln und das Ergebnis mit einem Hash-Wert der Signatur des Verfassers und dem Zeitpunkt der Zertifizierung vergleichen, um nachzuweisen, dass die Signatur des Verfassers existierte, als die Zertifizierung erstellt wurde, und dass die Signatur des Servers und der Zeitpunkt der Zertifizierung ursprünglich zusammen von jemandem verschlüsselt wurden, der Zugriff auf den privaten Schlüssel des Notars hatte.

[0004] Das Beglaubigen digitaler Dokumente wird in der US-amerikanischen Patentschrift 5.136.646 beschrieben. Das Beglaubigen durch sichere Hardware in einem System wird in der US-amerikanischen Patentschrift 5.001.752 beschrieben. Public-Key-Kryptographie wird in „New Directions in Cryptography" von Diffie und Hellmann in IEEE Transactions On Information Theory, Band IT-22, November 1976, Seite 644-654 und in den US-amerikanischen Patentschriften 4.405.829 von Rivest und 4.868.877 beschrieben. Das Einweg-Hashing wird in „Collision-Free Hash Functions and Public Key Signature Schemes", Advances in Cryptology – Eurocrypt '87, Springer-Verlag, LNCS, 1988, Band 304, Seite 203-217 beschrieben.

[0005] Eine Ausführungsform eines Systems, in dem ein solches Verfahren verwendet werden kann, wird in der US-amerikanischen Patentschrift 5.347.579 beschrieben, in der ein Online-Tagebuchsystem beschrieben wird, das einen Tagebucheintrag durch Erstellen, Zeitstempeln, Authentifizieren und permanentes Speichern eines Bezugsdatenblocks zusammen mit jedem Tagebucheintrag archiviert. Ein archivierter Tagebucheintrag kann nur durch Einbringen des Originaltextes in Compartment-Codes, wie zum Beispiel Cross-out- oder Tear-out-Codes, verändert werden und durch Einbringen eines eingefügten Textes in Insertion-Codes, so dass der ursprüngliche Tagebucheintrag aus dem veränderten Tagebucheintrag wieder hergestellt werden kann. Der Bezugsdatenblock, der der ursprüngliche Tagebucheintrag, eine kanonische Version des ursprünglichen Tagebucheintrags oder eine Einweg-Verschlüsselung mit fester Länge des ursprünglichen Tagebucheintrags sein kann, kann nicht verändert werden und wird zum Authentifizieren des ursprünglichen Tagebucheintrags verwendet. Innerhalb des Authentifizierungsvorgangs werden zeitgestempelte Daten und die Signatur von einem Benutzer eingegeben. Handelt es sich bei den eingegebenen Daten um einen Arbeitsdatentext, dann werden die Daten entkleidet, um eine kanonische Version des Textes zu erstellen. Wird ein Public-key-Verfahren verwendet, dann wird ein herkömmliches Public-key-Verfahren eingesetzt. Anderenfalls wird eine Signatur anhand des entkleideten Textes und des angehängten Zeitstempels errechnet. Diese errechnete Signatur wird mit der Signatur in den archivierten Bezugsdaten verglichen, und bei Übereinstimmung wird ein Bestätigungssignal zurückgesandt; anderenfalls wird ein Signal zur Nichtbestätigung zurückgesandt.

ZUSAMMENFASSUNG DER ERFINDUNG

[0006] Die Erfindung hat zur Aufgab, Verfahren und Geräte für die Authentifizierung von Revisionen zu schaffen.

[0007] In den hierin beschriebenen Erfindungen werden ein Originaldokument und ein vom Originaldokument abgeleitetes revidiertes Dokument auf eine solche Weise signiert und beglaubigt, dass sowohl die Beziehung zwischen dem Originaldokument und dem revidierten Dokument als auch die Herkunft der Revision und optional der Zeitpunkt der Beglaubigung der Revision nachgewiesen werden können.

[0008] Bei einer Ausführungsform der Erfindung wird das Originaldokument signiert und beglaubigt; später wird das Dokument dann revidiert und die Revision und ihre Beziehung zum Originaldokument werden signiert und beglaubigt. Bei einer anderen Ausführungsform werden das Originaldokument und eine automatisch erzeugte Revision des Dokuments gleichzeitig signiert und beglaubigt. Dieses ermöglicht den Nachweis der Urheberschaft (Verfasserschaft) und des Zeitpunkts der Erstellung einer automatisch erzeugten Revision wie zum Beispiel einer verlustbehafteten Komprimierung von Informationen.

[0009] Andere Alternativen und Vorteile der Erfindung der Anmelderin werden beschrieben oder werden den Fachkundigen beim Durcharbeiten der nachfolgenden detaillierten Beschreibung unter Bezugnahme auf die folgenden Zeichnungen ersichtlich, die die Elemente der angehängten Ansprüche der Erfindungen darstellen.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0010] Die Fig. 1a-Fig. 1d zeigen einen Ablaufplan einer speziellen Ausführungsform der Erfindung zum Authentifizieren von Revisionen.

[0011] Die Fig. 2aFig. 2d zeigen einen weiteren Ablaufplan einer weiteren speziellen Ausführungsform der Erfindung zum Authentifizieren von Revisionen.

[0012] Die Fig. 3a-Fig. 3c stellen einen weiteren Ablaufplan einer speziellen Ausführungsform der Erfindung zum Authentifizieren von Revisionen dar.

[0013] Fig. 4 zeigt ein Beispiel einer Ausführungsform des Netzwerksystems der Erfindung.

[0014] Fig. 5 liefert zusätzliche Einzelheiten der Autorenstationen aus Fig. 4.

[0015] Fig. 6 zeigt zusätzliche Einzelheiten des sicheren Servers aus Fig. 4.

[0016] Fig. 7 stellt zusätzliche Einzelheiten des Hosts des Notars aus Fig. 4 dar.

[0017] Fig. 8 zeigt eine spezielle Ausführungsform von Geräten zum Programmieren des Systems aus **Fig.** 3.

DETAILLIERTE BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSFORM

[0018] Die Fig. 1a-Fig. 1d zeigen einen Ablaufplan einer speziellen Ausführungsform der Erfindung zum Authentifizieren von Revisionen. Fig. 1a zeigt eine erste Gruppe von Schritten **100** des Verfahrens, in dem eine in die Workstation des Verfassers geladene Software für das Erstellen und Signieren eines digitalen Dokuments sorgt, so dass andere die Herkunft des Dokuments authentifizieren können. Der Verfasser verfügt über einen privaten Schlüssel, der die digitalen Informationen verschlüsseln kann, und andere Parteien verfügen über einen öffentlichen Schlüssel zum Entschlüsseln der Informationen. Das heißt, der Verfasser hat den öffentlichen Schlüssel für die Öffentlichkeit zum Beispiel auf einem Server verfügbar gemacht, wo andere, die die Herkunft des Berichts (z.B. dass der Verfasser den Bericht erstellt hat) oder die Integrität des Berichts (d.h. dass der Bericht nach der Signatur nicht verändert wurde) nachprüfen möchten, auf den Bericht und den öffentlichen Schlüssel zugreifen können. In diesem ersten Abschnitt **100** der Erfindung, in Schritt **102**, erstellt ein Verfasser einen Bericht (digitales Dokument) unter Verwendung der Software, die auf die Workstation geladen ist, welche an einen Server in einem Netzwerk angeschlossen ist, und der Verfasser gibt einen Befehl zum Übergeben des Berichts an den Server ein.

[0019] Der Bericht enthält die Art von Informationen, von denen jemand möglicherweise nachprüfen möchte, ob sie ursprünglich vom Verfasser stammen und nicht verändert wurden. In Schritt **103** bildet die Workstation des Verfassers einen Hash-Wert des Berichts unter Verwendung eines speziellen Einweg-Hashing-Verfahrens. Der Einweg-Hash hat den Vorteil, dass er zum Decodieren des Dokuments nicht umgekehrt werden kann, so dass, selbst wenn das Dokument vertraulich oder privat wäre, der Hash-Wert nicht vertraulich bleiben müsste. In Schritt **104** verschlüsselt die Workstation den Hash-Wert unter Verwendung des privaten Schlüssels des Verfassers (oder des privaten Schlüssels der Workstation), um die Signatur des Verfassers für den Bericht zu erstellen. Der Zweck der Verschlüsselung besteht darin, den Nachweis zu liefern, dass der Verfasser der Ersteller des Berichts ist und dass der Bericht nicht durch andere verändert wurde. Die Verschlüsselung des Hash-Wertes dient nicht dazu, die Daten oder den Hash-Wert geheim zu halten, sondern dazu, die Integrität und die Herkunft nachzuweisen. Der Bericht kann andere Informationen, wie zum Beispiel den Titel, den Namen des Verfassers, die Kennung der Workstation, den Zeitpunkt der Erstellung enthalten oder sich darauf beziehen. Die Workstation kann, wenn gewünscht, den Bericht, den Hash-Wert und die Signatur relational in der Workstation speichern. Hierbei bedeutet relational nur, dass die Tatsache, dass der Bericht sich auf den Hash-Wert und die Signatur bezieht und umgekehrt, ebenfalls in der Workstation gespeichert wird. In Schritt **106** sendet (überträgt) die Workstation die Identifikation des Verfassers, den Titel des Berichts, den Bericht und die Signatur des Verfassers für den Bericht an den Server eines Kunden. Ist der Inhalt des Berichts vertraulich oder privat, dann wird vor der Übertragung eine si-

chere Verbindung zwischen der Workstation und dem Server hergestellt und bei dem Server handelt es sich um einen sicheren Server. In Schritt **107** bildet der Server einen Hash-Wert des Berichts und entschlüsselt die Signatur des Verfassers unter Verwendung des öffentlichen Schlüssels des Verfassers. Dann vergleicht der Server den Hash-Wert des Berichts mit der entschlüsselten Signatur, um zu überprüfen, ob sie zusammen passen. Passen sie zusammen, dann weiß der Server, dass die Signatur und der Bericht vom Verfasser stammen (oder zumindest von jemandem mit Zugriff auf den privaten Schlüssel des Verfassers), da die Signatur unter Verwendung des öffentlichen Schlüssels des Verfassers entschlüsselt wurde, und der Server weiß ebenfalls, dass die Signatur und der Bericht seit dem Signieren des Berichts durch den Verfasser nicht verändert wurden. In Schritt **108** speichert der Server den Bericht, die Identifikation (ID) des Verfassers und die Signatur des Verfassers relational im Speicher des Servers. Auch hierbei bedeutet relational (oder in Bezug auf) gespeichert nur, dass die Tatsache, dass die in Beziehung stehenden Elemente der Informationen Bezug zueinander haben, ebenfalls gespeichert wird.

[0020] In einer nächsten Gruppe von Schritten **110** in Fig. 1b erhält der Server einen Zeitstempel für den Bericht und speichert den Zeitstempel mit Bezug zum Bericht. In Schritt **112** sendet der Server die Signatur des Verfassers über das Netzwerk an ein Host-System des Notars. Alternativ könnte der Notar ein sicherer Teil der Hardware des Servers sein, zum Beispiel eine Vorrichtung mit einem privaten Schlüssel, den der Besitzer des Servers nicht kennt oder nicht herausfinden kann, ohne die Vorrichtung zu zerstören. Da die Signatur nicht vertraulich ist, ist für die Übertragung der Signatur keine hohe Sicherheit erforderlich. In Schritt **113** erstellt der Host einen Zeitstempel, der die Signatur des Verfassers, die Empfangszeit, die ID des Notars, die Sequenznummer und die ID des Kunden enthält. In Schritt **114** bildet der Notar einen Hash-Wert für den Zeitstempel. In Schritt **115** signiert der Notar den Hash-Wert des Zeitstempels unter Verwendung des privaten Schlüssels des Notars. In Schritt **116** speichert der Notar den Zeitstempel und die Signatur des Notars für den Bericht. In Schritt **117** überträgt der Notar den Zeitstempel und die Signatur des Notars an den Server. Ein oder mehrere vorherige und/oder nachfolgende Zeitstempel können auch als Paket an den Server des Kunden gesandt werden, so dass durch Kontaktieren der anderen in den Zeitstempeln identifizierten Kunden der ungefähre Zeitpunkt des Zeitstempels unabhängig überprüft werden kann. In Schritt **118** bildet der Server einen Hash-Wert für den Zeitstempel, um die Signatur des Notars zu überprüfen, und entschlüsselt die Signatur des Notars unter Verwendung des öffentlichen Schlüssels des Notars. In Schritt **119** vergleicht der Server die Ergebnisse und wenn eine Übereinstimmung vorliegt, dann ist der Zeitstempel überprüft. Das heißt, der Server erkennt, dass der Zeitstempel und die Signatur des Notars vom Notar stammen und nicht verändert wurden. In Schritt **120** speichert der Server den Zeitstempel, die Signatur des Notars und jegliche vorherigen und/oder nachfolgenden Zeitstempel mit Bezug zum Bericht.

[0021] In der nächsten Gruppe von Schritten **120** in Fig. 1c erhält ein Revisor (menschlicher Benutzer) eine Kopie des Berichts (Originaldokuments) zur Revision und überprüft dessen Herkunft und Integrität. In Schritt **122** fordert der Revisor den Originalbericht vom Server an. Es gibt viele Situationen, in denen jemand möglicherweise ein Dokument revidieren muss, zum Beispiel, um zusätzliche Materialien hinzuzufügen oder um Fehler zu korrigieren. Vorzugsweise teilt der Revisor dem Server mit, dass er vorhat, den Bericht zu revidieren, und der Server verweigert danach ein Übertragen des Berichts an irgendjemand anderen, der den Bericht anfordert, um ihn zu revidieren (d.h. der Bericht ist zur Revision gesperrt bis der Revisor die Revision vorlegt oder die Sperre anderweitig aufhebt). In Schritt **123** sendet der Server den Originalbericht, den Zeitstempel des Berichts und die Signatur des Notars an die Workstation des Revisors. In Schritt **124** bildet die Workstation des Revisors einen Hash-Wert des Zeitstempels und entschlüsselt unter Verwendung des öffentlichen Schlüssels des Notars die Signatur des Notars, um die Signatur des Notars zu überprüfen. Das heißt, wenn der Hash-Wert und die Entschlüsselung der Signatur übereinstimmen, dann erkennt der Revisor, dass die Signatur des Notars durch jemanden erstellt wurde, der Zugriff auf den privaten Schlüssel des Notars hat und dass die Informationen im Zeitstempel zum Zeitpunkt des Erstellens der Signatur existierten. Da der Zeitstempel die Signatur des Verfassers und den Zeitpunkt (einschließlich Datum), an dem die Signatur des Notars erstellt wurde, enthält, wird nachgewiesen, dass die Signatur des Verfassers zu diesem Zeitpunkt existierte. In Schritt **126** bildet die Workstation einen Hash-Wert des Berichts und entschlüsselt die Signatur des Verfassers (enthalten im Zeitstempel) unter Verwendung des öffentlichen Schlüssels des Notars und vergleicht die Ergebnisse, um die Signatur des Verfassers zu überprüfen. Das heißt, wenn der Hash-Wert und die Entschlüsselung der Signatur des Verfassers übereinstimmen, dann wurde der Bericht von jemandem signiert, der Zugriff auf den privaten Schlüssel des Verfassers hat und der Bericht wurde seit seiner Signierung nicht verändert.

[0022] In der letzten Gruppe von Schritten **130** dieser ersten Ausführungsform in Fig. 1d erstellt der Revisor eine Revision des Berichts und die Revision wird digital signiert, sicher gespeichert und digital beglaubigt. In Schritt **132** erstellt der Revisor eine Revision des Berichts und gibt einen Befehl zum Übergeben der Revision an den Server ein. In Schritt **133**

kombiniert die Workstation die Revision und den vorhergehenden Zeitstempel und bildet einen Hash-Wert der Kombination. Der Zweck des Kombinierens des Zeitstempels mit der Revision vor dem Signieren besteht darin, den Zusammenhang mit dem Originaldokument nachweisen zu können. Alternativ oder zusätzlich zum Zeitstempel könnten andere Informationen, die auf die Historie der Revision hindeuten, mit der Revision kombiniert werden, so zum Beispiel die Signatur des Originalberichts, ein Hash-Wert des Originalberichts, oder die Zeitstempelsignatur könnte in der Kombination enthalten gewesen sein. In Schritt **134** verschlüsselt die Workstation den Hash-Wert der Kombination unter Verwendung des privaten Schlüssels des Revisors (oder der Workstation), um die Signatur des Revisors zu erstellen. Die Workstation kann, falls gewünscht, die Revision, den Hash-Wert und die Signatur des Revisors speichern. In Schritt **135** sendet die Workstation die Revision, die Identifikation des Revisors, den Titel der Revision und die Signatur des Revisors an den Server. In Schritt **136** kombiniert der Server die Revision und den Zeitstempel des Originalberichts, bildet einen Hash-Wert der Kombination und decodiert die Signatur des Revisors unter Verwendung des öffentlichen Schlüssels des Revisors, um die Herkunft und die Integrität der Revision zu überprüfen. In Schritt **137** vergleicht der Server die entschlüsselte Signatur mit dem Hash-Wert, und wenn der resultierende Hash-Wert und die Entschlüsselung der Signatur des Revisors übereinstimmen, erkennt der Server, dass die Revision vom Revisor stammt, dass die Revision auf dem Originalbericht basiert und dass die Revision und die Signatur seit ihrer Signierung durch den Revisor nicht geändert wurden. In Schritt **138** speichert der sichere Server die Revision, die ID des Revisors, den Titel und die Signatur des Revisors mit Bezug zum Originalbericht. In Schritt **139** erhält der Server vom Notar einen Zeitstempel für die Signatur des Revisors und speichert den Zeitstempel mit Bezug zur Revision. Hierbei handelt es sich um denselben Zeitstempel-Vorgang wie oben in den Schritten **110** für den Originalbericht beschrieben. Nach diesem Vorgang werden zukünftige Revisionen auf ähnliche Weise auf der Grundlage der aktuellsten Revision erstellt, um die Historie der Revisionen zu dokumentieren.

[0023] Die Fig. 2a-Fig. 2d zeigen eine alternative spezielle Ausführungsform der Erfindung zum Authentifizieren von Revisionen. In einer ersten Gruppe von Schritte **160** in Fig. 2a erstellt der Verfasser ein Bild und überträgt das Bild zu einem Server, der das Bild für den Verfasser signiert und das Bild speichert. In Schritt **162** bedient der Verfasser einen Bildgeber, um ein Bild zu erstellen, und veranlasst ein Übergeben des Bildes an einen sicheren Server. Bei dem Bildgeber kann es sich um jegliche Art von Ausrüstung handeln, die ein Bild erstellt, wie zum Beispiel einen Page Scanner eines Unternehmens, einen medizinischen Scanner (Elektro-Kardiogramm/Angiogramm, Ultraschall-Bildgeber, Computertomographie, Magnetresonanzbildgeber, Röntgenbildscanner) oder um irgendein bekanntes Verfahren zum Erstellen von Bildern, und die Bilder können als Videobild und/oder als Audiobild vorliegen. In Schritt **163** überträgt der Bildgeber das Bild über eine sichere Verbindung an einen sicheren Server. Die Übertragung identifiziert den Verfasser oder das Bildgebunggerät. Der Server kann eine Sequenznummer zurücksenden, um dem Bildgeber den späteren Zugriff auf das Bild zu erleichtern. In Schritt **164** kombiniert der Server die ID des Bildgebers oder die ID des Verfassers mit dem Bild und bildet einen Hash-Wert der Kombination, um einen Bild-Hash zu erstellen, alternativ kann der Server die ID eines Scanners oder eines Verfassers mit einem Hash-Wert des Bildes kombinieren, um den Bild-Hash zu liefern. Bekannte Kombinierverfahren umfassen ein Anhängen der ID an den Bild-Hash oder eine Exklusiv-ODER-Verknüpfung der ID und des Bild-Hash. Alternativ könnte der Bildgeber oder Verfasser über spezielle Paare von privaten/öffentlichen Passwörtern (Schlüsseln) verfügen, die verwendet werden könnten, um die Herkunft des Bildes nachzuweisen, und somit müssten die IDs des Bildgebers oder des Verfassers nicht vor dem Hashing mit dem Bild kombiniert werden. In Schritt **166** verschlüsselt der Server die identifizierte Kombination unter Verwendung des privaten Schlüssels des Servers (oder der im Server gespeicherten privaten Schlüssel des Verfassers oder des Bildgebers), um die Signatur eines Bildes zu erstellen. In Schritt **167** speichert der Server das Bild, die ID des Bildgebers (oder die ID des Verfassers), die Sequenznummer des Bildes für den Bildgeber, den Bild-Hash und die Bildsignatur des Servers relational.

[0024] xxx In der nächsten Gruppe von Schritten **170** in Fig. 2b erhält der Server vom Notar einen Zeitstempel und eine Zeitstempelsignatur für das Bild. In Schritt **172** stellt der Server eine Verbindung mit dem Host-Netzwerk des Notars her und der Server sendet die Bildsignatur des Servers an den Host. In Schritt **174** erstellt der Host einen Zeitstempel für das Bild, der die Bildsignatur des Servers, die Empfangszeit, die ID des Notars, die Sequenznummer des Zeitstempels (diese unterscheidet sich von der Sequenznummer des Bildes) und die ID des Servers enthält. In Schritt **175** bildet der Host einen Hash-Wert des Zeitstempels des Bildes und in Schritt **176** signiert der Host den Zeitstempel-Hash unter Verwendung des privaten Schlüssels des Notars. In Schritt **177** speichert der Host den Zeitstempel des Bildes und die Bildsignatur des Notars. In Schritt **178** überträgt der Host ein Bildzertifikat, das den Zeitstempel des Bildes und die Bildsignatur des Notars enthält, an den Server. In Schritt **179** bildet der Server einen Hash-Wert des Zeitstempels des Bildes und decodiert die Bildsignatur des Notars unter Verwendung des öffentlichen Schlüssels des Notars, um die Inte-

grität und die Herkunft des Zeitstempels und der Signatur des Notars zu überprüfen. In Schritt **180** speichert der Server das Bildzertifikat des Notars mit Bezug zu den Sequenznummern der Bilder für den Bildgeber.

[0025] Im nächsten Abschnitt von Schritten **190** in Fig. 2c revidiert der Server automatisch das Bild und erhält einen beglaubigten Zeitstempel für die Revision. In Schritt **192** komprimiert der Server das Bild zu einer verlustbehafteten Kondensation. Ein Bitabbild wird zum Beispiel durch JPEG-Kompression zu einem bit-reduzierten Bild komprimiert, ein Audiobild wird unter Verwendung von MPEG-2 oder Dolby AC3 komprimiert oder ein Video kann unter Verwendung von MPEG-2 komprimiert werden. In Schritt **194** speichert der Server die Kondensation mit Bezug zur Sequenznummer des Bildes für den Bildgeber und andere zugehörige Informationen. In Schritt **196** kombiniert der Server die Kondensation und die Bildsignatur des Notars zum Beispiel durch gemeinsames Anhängen der beiden. In Schritt **198** bildet der Server einen Hash-Wert der Kombination, um den Hash der Kondensation zu erstellen. In Schritt **199** verschlüsselt der Server den Hash der Kondensation, um die Kondensationssignatur des Servers zu erstellen und in Schritt **200** speichert der Server den Hash der Kondensation und die Kondensationssignatur des Servers mit Bezug zur Kondensation. In Schritt **201** erhält der Server ein Kondensationszertifikat (d. h. Zeitstempel der Kondensation und Kondensationssignatur des Notars) vom Notar für die Kondensationssignatur des Servers und speichert das Kondensationszertifikat mit Bezug zur Kondensation. In Schritt **202** kann der Server das Originalbild löschen, um Speicherplatz zu sparen, aber natürlich bedeutet dies, dass ein Benutzer zumindest unabhängig von den Aufzeichnungen des sicheren Servers das Erstellungsdatum oder die Herkunft des Originalbildes nicht mehr nachweisen kann oder dass die Kondensation ein Produkt des Originalbildes ist. Das Löschen kann erforderlich werden, weil nicht komprimierte Bilder insbesondere die eines Videos, 100 mal so viel Speicherplatz benötigen wie das resultierende komprimierte Video und derart große Mengen Speicherplatz könnten nicht verfügbar oder vom Kunden nicht aufzubringen sein. Alternativ kann das Originalbild auf herausnehmbaren Band oder auf optischen Medien archiviert werden und Offline aufbewahrt oder sogar zur Langzeitspeicherung versandt werden.

[0026] In dem letzten Satz von Schritten **210** in Fig. 2d fordert ein Benutzer das Bild zur Bildbearbeitung auf einem Bildbetrachter an und das gespeicherte Bild wird zusammen mit beiden Zeitstempeln und beiden Signaturen des Notars bereitgestellt, so dass der Bildbetrachter die Herkunft und das Zertifizierungsdatum der Revision überprüfen kann, und dass, zumindest entsprechend den Aufzeichnungen auf dem sicheren Server, die Revision ein Produkt des Originalbildes ist. In Schritt **212** fordert der Benutzer unter Verwendung des Bildbetrachters das komprimierte Bild an. Der Bildbetrachter kann jede Art von Ausrüstung sein, die ein Abspielen des komprimierten Bildes für den Benutzer ermöglicht. Der Bildbetrachter ist nicht auf die visuelle Wiedergabe beschränkt und kann zum Beispiel ein Lautsprecher sein, der ein Audiobild abspielt. In Schritt **213** sendet der Server den Bild-Hash, die ID des Bildgebers, die Bildkondensation, beide entsprechenden Zeitstempel (einen für das Bild und einen für das komprimierte Bild) und ebenso beide Signaturen des Notars an den Bildbetrachter. In Schritt **214** bildet der Bildbetrachter einen Hash-Wert des Zeitstempels der Kondensation und entschlüsselt die Kondensationssignatur des Notars unter Verwendung des öffentlichen Schlüssels des Notars, um den digitalen Zeitpunkt und andere Informationen im Zeitstempel der Kondensation zu überprüfen. In Schritt **215** bildet der Bildbetrachter einen Hash-Wert des Zeitstempels des Bildes und entschlüsselt die Bildsignatur des Notars unter Verwendung des öffentlichen Schlüssels des Notars, um den Zeitstempel des Bildes zu überprüfen. In Schritt **216** kombiniert der Bildbetrachter den Hash der Kondensation und die Bildsignatur des Notars und bildet einen Hash-Wert der Kombination. und in Schritt **218** entschlüsselt der Bildbetrachter die Kondensationssignatur des Servers und vergleicht die Entschlüsselung mit dem Hash, um die Herkunft und die Integrität der Kondensation zu überprüfen. Der Bildbetrachter kann auch die Bildsignatur des Servers entschlüsseln und diese mit dem Bild-Hash vergleichen, um die Aufzeichnungen des sicheren Servers hinsichtlich der ID des Bildgebers gegenzuprüfen. Nach Überprüfen beider Zeitstempel kann der Bildbetrachter den Zeitpunkt des Zeitstempels des Bildes mit dem Zeitpunkt des Zeitstempels der Kondensation vergleichen, um zu überprüfen, dass die Zeitpunkte nahe bei einander liegen. In Schritt **218** dekomprimiert der Bildbetrachter das Bild. In Schritt **220** zeigt der Bildbetrachter dem Benutzer das dekomprimierte Bild, die ID des Bildgebers oder (die ID des Verfassers), den Zeitpunkt der Bildübergabe und den Zeitpunkt der Kondensation an.

[0027] Die Fig. 3a-Fig. 3c stellen eine andere Ausführungsform der Erfindung dar, in der ein Server ein Video automatisch und sofort nach Erhalt komprimiert, und einen Zeitstempel sowohl für den entsprechenden Erhalt des Videos als auch für die Komprimierung des Videos erhält. In einer ersten Gruppe **230** von Schritten in Fig. 3a wird das Video erstellt und an den Server übertragen. In Schritt **232** bedient der Verfasser den Video-Bildgeber, um das Video zu erstellen und das Video an den Server weiterzuleiten. Der Bildgeber kann jegliche Art von Ausrüstung zum Erstellen von Multimedia-Präsentationen sein, wie zum Beispiel eine Videokamera und ein Mikrofon. Das Video kann Tonkanäle und andere Daten sowie

Videobilder enthalten. Vorzugsweise wird auch ein Titel erstellt. In Schritt **233** komprimiert der Bildgeber zuerst das Video für die Übertragung. Der Bildgeber kann zum Beispiel das Video unter Verwendung von MPEG-2 oder einer anderen einfachen verlustbehafteten Komprimierung oder, was vorzuziehen ist, durch ein verlustloses Komprimierungsverfahren komprimieren. In Schritt **234** bildet der Bildgeber einen Hash-Wert der ersten Kondensation des Videos. Der Bildgeber kann auch, wie oben beschrieben, einen Hash-Wert anderer Informationen wie zum Beispiel der ID des Bildgebers oder der Sequenznummer des Bildes mit dem Bild-Hash bilden. In Schritt **235** verschlüsselt der Bildgeber den Hash-Wert mit dem privaten Schlüssel des Bildgebers (oder Verfassers), um das Video zu signieren. Der Bildgeber kann das Video, die erste Komprimierung, den Hash und die Signatur des Bildgebers speichern, zumindest bis der Server einen Nachweis des Erhalts sendet. In Schritt **236** überträgt der Bildgeber den Titel des Videos, die erste Kondensation und die Signatur an den Server. In Schritt **238** löscht der Bildgeber das Video, um Speicherplatz zu sparen und später, nach Erhalt der Empfangsbestätigung vom Server, löscht der Bildgeber die erste Kondensation des Videos. Alternativ kann die erste Kondensation auf dem Bildgeber archiviert werden, aber im Allgemeinen ist es üblich, nur die erste Kondensation wie nachfolgend beschrieben auf dem Server zu archivieren.

[0028] In einen zweiten Satz von Schritten **240** in Fig. 3b empfangt, überprüft und speichert der Server die erste Kondensation, erstellt eine zweite Komprimierung des Videos und erhält vom Notar einen Zeitstempel und eine Zeitstempelsignatur für die zweite Komprimierung. In Schritt **241** empfängt der Server die erste Kondensation des Videos, die Signatur des Bildgebers, den Titel, die ID des Bildgebers und möglicherweise andere dazugehörige Informationen und überträgt die Empfangsbestätigung zurück an den Bildgeber. In Schritt **242** bildet der Server einen Hash-Wert der ersten Kondensation des Videos und entschlüsselt die Signatur des Video-Bildgebers unter Verwendung des öffentlichen Schlüssels des Bildgebers und vergleicht die Entschlüsselung mit dem Hash, um die Herkunft und die Integrität der ersten Kondensation zu überprüfen. In Schritt **243** speichert der Server den Titel, die ID des Verfassers, die Signatur des Bildgebers und den Hash der ersten Kondensation relational. In Schritt **244** erstellt der Server sofort nach Überprüfen eine zweite Komprimierung des Videos, um eine zweite Kondensation zu erstellen. In Schritt **245** archiviert der Server die erste Kondensation des Videos, um Speicherplatz zu sparen und löscht die erste Kondensation aus dem Online-Speicher.

[0029] In Schritt **246** kombiniert der Server den Titel, die ID des Bildgebers, die ID des Verfassers, die Signatur des Bildgebers (oder die Signatur des Verfassers) und die zweite Kondensation und bildet einen Hash-Wert der Kombination. In Schritt **247** verschlüsselt der Server den Hash-Wert der Kombination unter Verwendung des privaten Schlüssels des Servers, um die Signatur des Servers für das zweite komprimierte Video zu erstellen. In Schritt **248** speichert der Server das zweite komprimierte Video und die Videosignatur des Servers relational zum Titel und der Signatur des Bildgebers und den zugehörigen Informationen. In Schritt **250** erhält der Server vom Notar einen Zeitstempel und die Signatur des Notars für die Signatur des Servers, überprüft den Zeitstempel und die Signatur des Notars und speichert den Zeitstempel und die Signatur des Notars mit Bezug zur zweiten Kondensation.

[0030] In einer letzten Gruppe von Schritten **260** für diese Ausführungsform in Fig. 3c wird das Video angefordert, überprüft und auf einer Anzeigevorrichtung betrachtet. In Schritt **262** fordert der Benutzer der Anzeigevorrichtung das Video vom Server an. In Schritt **263** sendet der Server die ID des Bildgebers, den Titel, die zweite Kondensation, den Zeitstempel des Notars (der die Signatur des Servers enthält) und die Signatur des Notars an die Anzeigevorrichtung. Der Hash-Wert der ersten Kondensation und die Signatur des Video-Bildgebers können auch gesandt werden, um die Herkunft des Videos gegenzuprüfen. In Schritt **264** entschlüsselt das Anzeigegerät die Signatur des Notars unter Verwendung des öffentlichen Schlüssels des Notars, bildet einen Hash-Wert des Zeitstempels und vergleicht die Ergebnisse, um den Zeitstempel zu überprüfen. In Schritt **265** führt die Anzeigevorrichtung die Kombination durch wie oben beschrieben und bildet einen Hash-Wert, um den Hash-Wert der zweiten Kondensation zu erstellen und entschlüsselt die Signatur des Servers unter Verwendung des öffentlichen Schlüssels des Servers und vergleicht die Ergebnisse, um die Herkunft und die Integrität der zweiten Kondensation zu überprüfen. Die Anzeigevorrichtung kann auch die Signatur des Bildgebers und den Hash-Wert der ersten Kondensation empfangen und dann die Signatur des Bildgebers entschlüsseln und das Ergebnis mit dem Hash-Wert der ersten Kondensation vergleichen, um die Aufzeichnungen des Servers für die Herkunft der ersten Kondensation gegenzuprüfen. Die Anzeigevorrichtung kann nicht unabhängig die Herkunft und die Integrität der ersten Kondensation überprüfen, ohne eine Kopie der ersten Kondensation zu erhalten. In Schritt **266** decodiert der Bildbetrachter (die Anzeigevorrichtung) die zweite Kondensation, um das dekomprimierte Video zu erstellen. In Schritt **267** schließlich betrachtet der Benutzer das Video auf der Anzeigevorrichtung. Der Benutzer kann auch in der Lage sein, andere Informationen über das Video, wie zum Beispiel die ID des Verfassers, die ID des Bildgebers, den Zeitpunkt der Erstellung der zweiten Kondensation und Informationen über den Zeitstempel des Notars zu betrachten.

[0031] Fig. 4 stellt ein Netzwerk **300** der Erfindung dar, in dem eine Vielzahl von Computerknoten über ein Kommunikationsnetzwerk von Kabeln und eine Kommunikationsausrüstung **301** miteinander verbunden sind. Die Netzwerkknoten enthalten einen lokalen Server **302** und einen Notar **303**. Eine Vielzahl von Autorenstationen **304**-**313** ist über das Kommunikationsnetzwerk mit dem Server verbunden und eine Vielzahl von Betrachtungsstationen **314**-**323** kann auch über das Kommunikationsnetzwerk mit dem Server verbunden werden. Die Autorenstationen verfügen über Ausrüstungen zum Erstellen von Dokumenten, wie zum Beispiel Röntgenstrahlen, Testdaten, Abtastungen, Video- und Audiobilder, Multimedia-Präsentationen und Geräte zum Übertragen der Dokumente an den Server, zum Anfordern der Dokumente vom Server und zum Revidieren derartiger Dokumente. Die Betrachtungsstationen dienen in erster Linie zum Anfordern digitaler Dokumente vom Server und zum Betrachten der Dokumente, können aber auch über einige begrenzte Möglichkeiten zum Revidieren der Dokumente, wie zum Beispiel Hinzufügen von Anmerkungen und Kommentaren, verfügen.

[0032] In Fig. 5 sind zusätzliche Details der Autorenstation **304** aus Fig. 4 dargestellt. Die Autorenstation enthält einen Prozessor **352**, wie zum Beispiel eine Zentraleinheit (CPU) oder einen eingebetteten Controller, der mit einem elektronischen Speicher **353** kommuniziert. Der Speicher enthält Programme, die den Betrieb des Prozessors steuern, und Puffer zum Speichern von Informationen, die über einen Eingangs- und/oder Ausgangs-Schaltkreis **354** (IOC) von Peripheriegeräten der Autorenstationen empfangen werden und zum Übertragen und Empfangen von Informationen von anderen Knoten des Netzwerks über den IOC **355**. Die Peripheriegeräte können zum Beispiel Folgende sein: eine Tastatur **356**, ein Zeigegerät, wie zum Beispiel eine Maus **357**, eine Videokamera **358**, ein Mikrofon **359**, ein Scanner **360** und ein Plattenspeicher **361**.

[0033] Der Speicher enthält das Programmmodul **370** zum Interagieren mit einem Benutzer, um ein Dokument, das in dem Puffer **371** gespeichert ist, zu erstellen und um den Vorgang zum Senden des Dokuments an den Server zu initiieren. Der Speicher enthält das Programmmodul **372**, um unter Verwendung eines Einweg-Hash einen Hash-Wert des Dokuments zu bilden und um den Hash-Wert unter Verwendung eines privaten Schlüssels **390** des Benutzers (Erstellers) oder eines privaten Schlüssels **390** der Station zu verschlüsseln, um eine digitale Signatur für das Dokument zu erstellen. Der Speicher kann auch ein Modul **373** zum Übertragen des Dokuments zusammen mit der Signatur an den Server enthalten. Das Programmmodul **375** kann verwendet werden, um das Dokument, den Hash-Wert und/oder die digitale Signatur im Speicher **361** zu speichern. Für Video- und Audiobilder enthält der Speicher ein Programmmodul **376**, um das Video in eine komprimierte Form zu codieren, wie zum Beispiel Motion JPEG oder MPEG-2 Video oder vorzugsweise ein verlustfreies Komprimierungsverfahren, und um die Komprimierung des Videos als ein weiteres Dokument im Puffer **371** zu speichern.

[0034] In dem Fall, wo eine digitale Signatur durch den Server erstellt wird, kann das Autorensystem ein Modul **377** zum Empfangen der Dokumentsignatur, eines Zeitstempels und einer Zeitstempelsignatur vom Server in den Puffer **371** enthalten und ein Modul **378**, um die Signatur zu überprüfen und um zu veranlassen, dass Modul **375** die Dokumentsignatur, den Zeitstempel und die Zeitstempelsignatur im Speicher **361** speichert.

[0035] Die Autorenstation kann auch zum Revidieren der Dokumente verwendet werden, um Revisionen zu erstellen, die an den Server zurückgesandt werden können. Das Programmmodul **370** kann von einem menschlichen Bildbetrachter verwendet werden, um ein Dokument vom Server anzufordern. Das Programmmodul **379** verhandelt den Empfang des Dokuments und der zugehörigen Zeitstempel und anderer Informationen vom Server, und das Programm **380** authentifiziert das Dokument. In einer Ausführungsform der oben beschriebenen Erfindung empfängt die revidierende Station zusätzlich zu dem Dokument einen Zeitstempel (wie unten beschrieben) und eine Signatur des Notars. Das Modul **380** enthält das Gerät **383**, um einen Hash-Wert des Zeitstempels zu bilden und um die Signatur des Notars unter Verwendung des öffentlichen Schlüssels **393** des Notars zu entschlüsseln, und das Modul **384** vergleicht die Ergebnisse, um die Herkunft des Zeitstempels zu überprüfen und um zu überprüfen, dass der Inhalt des Zeitstempels, der den digitalen Zeitpunkt enthält, nicht verändert wurde. Dann bildet das Programm **385** des Moduls **380** einen Hash-Wert des Dokuments und entschlüsselt die Signatur des Servers (oder des Verfassers) (enthalten im Zeitstempel) und vergleicht die Ergebnisse, um festzustellen, ob die Signatur des Servers für das Dokument bestimmt ist und um zu überprüfen, dass das Dokument seit der Signierung durch den Server nicht verändert wurde. Außerdem kann der Server dann auch, wenn es sich bei dem Dokument um eine Revision handelt, einen Hash-Wert des Originaldokuments, die Signatur des Servers (oder die des revidierenden Verfassers) für die Revision, einen weiteren Zeitstempel und die Signatur des Notars für das Originaldokument übertragen und das Modul **379** kann diese empfangen, und dann kann das Modul **385** den Zeitstempel für das Originaldokument wieder authentifizieren und dann die Signatur des Servers (enthalten im Zeitstempel) entschlüsseln und die Ergebnisse mit dem Hash-Wert des Originaldokuments vergleichen, um die Herkunft des Dokuments zu überprüfen. In eini-

gen der oben beschriebenen Ausführungsformen werden Informationen wie zum Beispiel die Signatur des Revisors oder eine vorhergehende Signatur des Notars vor dem Hashing und Verschlüsseln auch mit dem Dokument kombiniert, um die Signatur des Servers zu erstellen, und in diesen Fällen muss das Modul **385** die entschlüsselte Signatur mit einem Hash-Wert der entsprechenden Verbindung solcher Elemente vergleichen. Dann wird das Modul **386** zum Interagieren mit dem Benutzer verwendet, um das Dokument zu revidieren. Das Modul **384** bildet einen Hash-Wert der mit dem vorhergehenden Zeitstempel kombinierten Revision und verschlüsselt den Hash-Wert, um eine Signatur des Revisionsdokuments zu erstellen. Dann können die Revision und die Signatur der Revision auf ähnliche Weise wie bei dem Originaldokument gespeichert, sicher übertragen und überprüft werden.

[0036] In Fig. 6 sind zusätzliche Einzelheiten des Servers **302** aus Fig. 4 dargestellt. Der Server enthält einen Prozessor **402** wie zum Beispiel eine Zentraleinheit (CPU) oder einen eingebetteten Controller, der mit einem elektronischen Speicher **403** kommuniziert. Der Speicher enthält Programme, die den Betrieb des Prozessors steuern, und Puffer zum Speichern der vom Netzwerk empfangenen Informationen und der über einen Eingangs- und/oder Ausgangs-Schaltkreis **404** (ICO) zum Netzwerk übertragenen Informationen. Der IOC **404** dient zum Übertragen von Informationen zu anderen an das Netzwerk angeschlossenen Knoten und zum Empfangen von Informationen von diesen anderen Knoten. Der Server kann zum Beispiel ein Gateway-Server sein, der über einen IOC in einem Netzwerk mit lokalen Clients verbunden ist und über einen anderen IOC mit anderen Servern und/oder entlegenen Clients in einem anderen Netzwerk verbunden ist. Der IOC **405** wird zum Speichern von Informationen auf einen Plattenspeicher **406** verwendet, zum Abfragen gespeicherter Informationen, zum Senden von Informationen zur Archivierungsvorrichtung **407** und gelegentlich zum Abfragen archivierter Informationen.

[0037] Der Speicher enthält das Programmmodul **420**, das über den IOC **404** Dokumente zwischen dem Netzwerk und Bereichen des Puffers **421** kopiert. In einigen der oben beschriebenen Ausführungsformen empfängt der Server ein digital signiertes Dokument von einer Autorenstation. In einem solchen Fall führt das Programmmodul **423** einen Einweg-Hash am Dokument durch, entschlüsselt die digitale Signatur und vergleicht das Ergebnis, um zu überprüfen, dass das Dokument seit der digitalen Signierung nicht verändert wurde und dass die Herkunft des Dokuments korrekt ist. In einer anderen der oben beschriebenen Ausführungsformen empfangt der Server ein Dokument, das nicht über ein sicheres Netzwerk signiert wurde. In einem solchen Fall bildet das Programmmodul **423** einen Hash-Wert des Dokuments und verschlüsselt den Hash-Wert unter Verwendung entweder des privaten Schlüssels des Servers oder des privaten Schlüssels des Erstellers (oder der Autorenstation) (welcher in diesem Fall auf dem sicheren Server aufbewahrt wird). In einer anderen der Ausführungformen kombiniert ein Revisor die Revision mit einem Zeitstempel, dem Hash eines Zeitstempels oder der Signatur des Notars, bildet einen Hash-Wert der Kombination und verschlüsselt den Hash-Wert, um die Revision zu signieren. Auf diese Weise überprüft die Signatur der Revision nicht nur die Herkunft und die Integrität der Revision, sondern identifiziert auch das Originaldokument, von dem die Revision abgeleitet wurde. Der Revisor sendet dann die Revision und die Signatur der Revision an den Server. In einem solchen Fall entschlüsselt das Modul **423** im Server die Signatur der Revision, kombiniert die Revision mit dem Zeitstempel des Originaldokuments und jeglichen anderen Informationen auf dieselbe Weise wie der Revisor, bildet einen Hash-Wert der Kombination und vergleicht die Ergebnisse, um die Herkunft der Revision, die Herkunft des Originaldokuments und die Tatsache, dass die Revision seit der Signierung nicht verändert wurde, zu überprüfen.

[0038] In einer anderen der oben beschriebenen Ausführungsformen empfängt der Server eine nicht signierte Revision, und dann kann das Modul **423** die Revision mit einigen Angaben zur Herkunft des Originaldokuments (einem Hash-Wert des vorhergehenden Dokuments, der vorherigen Signatur des Verfassers, dem vorherigen Zeitstempel, dem Hash-Wert des vorherigen Zeitstempels oder der Signatur des vorherigen Zeitstempels) und einer Angabe zur Herkunft der Revision (ID des Revisors, ID der Workstation) kombinieren, bildet einen Hash-Wert der Kombination und verschlüsselt dann den Hash-Wert (d.h. signiert das Dokument) unter Verwendung entweder des privaten Schlüssels des Servers oder des privaten Schlüssels des Erstellers.

[0039] In einer noch anderen der oben beschriebenen Ausführungsformen empfangt der Server ein Dokument (wenn es nicht signiert ist, dann signiert das Programm **423** das Dokument) und dann erhält das Modul **425** einen Zeitstempel für das Dokument. Danach revidiert das Modul **420** automatisch das Dokument, bildet einen Hash-Wert der Kombination des Original-Zeitstempels und des revidierten Dokuments und signiert den Hash-Wert. Anschließend erhält das Modul **424** einen weiteren Zeitstempel für die automatische Revision.

[0040] In einer anderen der oben beschriebenen Ausführungsformen empfangt das Modul **422** ein Dokument, und das Modul **420** signiert das Dokument und (wenn keine Signatur mit dem Dokument empfangen wird) kombiniert das revidierte Dokument mit den identifizierenden Informationen, und dann revi-

diert das Modul **422** automatisch das Dokument, bildet einen Hash-Wert der Kombination und signiert den Hash-Wert. Danach erhält das Modul **424** einen Zeitstempel für die Signatur der automatischen Revision.

[0041] Nachdem das Dokument signiert wurde, sendet das Programmmodul **425** die Signatur an einen Notar, der einen Zeitstempel erstellt, der die Signatur des Servers, die ID des Servers, die Sequenznummer und einen digitalen Zeitpunkt (einschließlich Datum) umfasst, signiert den Zeitstempel (um eine Zeitstempelsignatur zu erstellen) und sendet den Zeitstempel und die Zeitstempelsignatur, die vom Modul **420** empfangen wurden, zurück. Danach bildet das Modul **424** einen Hash-Wert des Zeitstempels und entschlüsselt die digitale Signatur (unter Verwendung des öffentlichen Schlüssels des Notars), um zu überprüfen, dass der Zeitstempel vom identifizierten Notar stammt und dass der Zeitstempel seit seiner Signierung nicht verändert wurde.

[0042] Um Platz im Direktzugriffsspeicher **406** (Festplatte, DVD, DC-ROM) zu sparen, kopiert das Programmmodul **426** im Fall von revidierten Dokumenten alte Versionen von Dokumenten auf herausnehmbare Computermedien (z.B. Band), die aus dem Server herausgenommen werden, in einem Verfahren, das als Archivieren bekannt ist. Wird ein archiviertes Dokument angefordert, dann ist das Programm **426** dafür verantwortlich, das Archivierungsband in das Archivierungssystem **407** zu laden und die angeforderten Dateien auf dem Server wieder herzustellen.

[0043] In Fig. 7 sind zusätzliche Einzelheiten des Notars **303** aus Fig. 4 dargestellt. Der Notar enthält einen Prozessor **452**, wie zum Beispiel eine Zentraleinheit (CPU) oder einen eingebetteten Controller, der mit einem elektronischen Speicher **453** kommuniziert. Der Speicher enthält Programme, die den Betrieb des Prozessors steuern, und Puffer zum Speichern von Information, die vom Netzwerk empfangen wurden, und von Informationen, die über einen Eingangs- und/oder Ausgangs-Schaltkreis **454** (IOC) zum Netzwerk gesandt wurden. Der IOC **454** dient zum Übertragen von Informationen zu anderen mit dem Netzwerk verbundenen Knoten und zum Empfangen von Informationen von diesen anderen Knoten. Der IOC **455** wird zum Speichern der Zeitstempel und der Signaturen der Zeitstempel auf Disk **456** verwendet.

[0044] Der Speicher enthält das Programmmodul **470** zum Steuern des Empfangs von Dokumentsignaturen und der Übertragung von Zeitstempeln und Zeitstempelsignaturen. Wird die Signatur eines Notars angefragt, kopiert das Programm **470** die Dokumentsignaturen aus dem Netzwerk in Teilbereiche des Puffers **471**. Nach dem Erstellen der Zeitstempel und der Signaturen des Notars kopiert das Programm **470** den Zeitstempel und die Zeitstempelsignatur aus Teilbereichen des Puffers **471** in das Netzwerk. Das Programmmodul **472** liest die Signatur des Servers aus dem Puffer und erstellt einen Zeitstempel, der Folgendes umfasst: die Signatur des Servers, den Zeitpunkt, zu dem die Signatur des Servers empfangen wurde (in jedem Zeitformat), eine ID des Notars und eine Sequenznummer. Dann bildet das Modul **472** einen Hash-Wert des Zeitstempels und verschlüsselt den Hash-Wert mit dem privaten Schlüssel des Notars, um eine Zeitstempelsignatur des Notars zu erstellen. Danach bereitet das Modul **473** eine Übertragung des Zeitstempels und der Signatur des Notars vor und speichert die Zertifikatübertragung in den Puffer **471** und veranlasst, dass das Modul **470** das Zertifikat des Notars zurück zum Kunden überträgt. Das Programmmodul **474** kopiert auch den Zeitstempel und die Zeitstempelsignatur zusammen über den IOC **455** als eine Aufzeichnung der Zeitstempelsignatur auf die Festplatte **456**.

[0045] Wird die Überprüfung der Authentizität einer Zeitstempelsignatur angefordert, kann die Anforderung entweder die Dokumentsignatur, den Zeitstempel, die Zeitstempelsignatur oder die Sequenznummer bereitstellen. Der Notar enthält das Modul **476** zum Abrufen des Zertifikats (Zeitstempel und Signatur des Notars) aus dem Speicher **456** und kann das Modul **477** zum Vergleichen der in der Überprüfungsanforderung bereitgestellten Informationen mit den Informationen in der Aufzeichnung und zum Feststellen der Übereinstimmung der Informationen enthalten. Das Modul **478** bereitet dann eine Übertragung der Aufzeichnung des Zeitstempels und/oder der Ergebnisse des Vergleichs vor, um die Informationen zu authentifizieren, und speichert die Antwort im Puffer **471** und das Modul **470** überträgt die Antwort.

[0046] In Fig. 8 sind ein programmierbares Computersystem **500** und verschiedene Beispielgeräte zum Programmieren derartiger programmierbarer Computer dargestellt, die alle in Fachkreisen sind. Das Computersystem kann entweder durch Anschließen eines nicht-flüchtigen Speichers (z.B. ROM, PROM, EEPROM, Flash-Speicher, batteriegepufferter SRAM), der programmierte Strukturen für den programmierbaren Computer enthält, programmiert werden oder durch Bereitstellen von Signalen für den programmierbaren Computer, die dem Speicher des programmierbaren Computers zugeführt werden können, um programmierte Strukturen zu schaffen. Ein weiteres Computersystem **501**, wie zum Beispiel ein Internetserver, kann über ein Kommunikationsgerät **502** an das System **500** angeschlossen werden, um Signale zum Programmieren des Systems **500** zu liefern. Das Gerät **502** kann ein Kupfer- oder optisches Kabel enthalten, Radio, Infrarot oder ein Netzwerk wie Ethernet, ARCnet, Token Ring oder ein Modem und Telefonsystem. Ein Speicherlaufwerk **503**

kann über eingebaute Medien **504** verfügen und abnehmbar am System **500** angebracht sein oder das Laufwerk **503** kann im System **500** fest eingebaut sein und Signale vom abnehmbaren Computermedium **504** empfangen. Das System **500** kann eine Benutzerschnittstelle **505** und ein Programmeingabemodul **506** enthalten und schriftliche Materialien können bereitgestellt werden. Ein Benutzer kann die Signale unter Verwendung von Geräten (nicht gezeigt) der Benutzerschnittstelle, wie zum Beispiel Tastatur, Textscanner, Mikrofon, Kamera oder Strichcode-Lesegerät, eingeben. Die dem System **500** bereitgestellten Signale können in das Speicherlaufwerk **503** zum späteren Abruf in den flüchtigen Speicher **507** kopiert oder im nicht-flüchtigen Speicher **508** gespeichert werden, um ein programmiertes Gerät im Speicher zu schaffen. Alternativ kann das System durch Bereitstellen eines nicht-flüchtigen Speichers programmiert werden. Das System **500** kann einen Steckplatz **509** enthalten, in den eine Kassette **510** mit einem nicht-flüchtigen Speicher, wie zum Beispiel eine PC Flash-Speicherkarte, eingesetzt werden kann, um ein programmiertes Gerät zu schaffen. Das System **500** kann eine Buchse **511** enthalten, in die ein nicht-flüchtiges Paket **512** eingesetzt werden kann, um ein programmiertes Gerät zu schaffen. Das System **500** kann mit einem integrierten nicht-flüchtigen Speicher **508** hergestellt werden, um ein programmiertes Gerät zu schaffen. Die programmierten Strukturen umfassen Programme und andere Daten im Speicher, die einen Mikroprozessor **513** und I/O-Prozessoren, z.B. **114**, des programmierbaren Computers, steuern, um Computervorgänge auszuführen. Das Computersystem kann eine Workstation, ein Modem, eine PC-Karte, ein Drucker oder ein anderes per Software aufrüstbares Bauteil sein. Andere bekannte Verfahren zum Programmieren eines Computersystems können ebenfalls verwendet werden.

[0047] Die Erfindung wurde unter Bezugnahme auf spezielle Ausführungsformen einschließlich des besten Verfahrens zum Ausführen der Erfindung und mit genügend Details beschrieben, damit jeder Fachkundige die Erfindung ausführen und anwenden kann. Die Fachkundigen können diese Ausführungsformen modifizieren oder andere Ausführungsformen im Rahmen der Erfindung schaffen, und somit beschränkt die Beschreibung die vorliegende Erfindung nicht auf die beschriebenen Ausführungsformen. Die Erfindung wird nur durch die nachstehenden angehängten Ansprüche beschränkt.

Text in der Zeichnung

Fig. 4

Authoring station – Autorenstation
Local server – lokaler Server
Viewing station – Betrachtungsstation
Communications – equipment Kommunikationsausrüstung
Certifier – Zertifizierer

Fig. 5

Camera – Kamera
KBD – Tastatur
Pointer – Zeigegerät
Microphone – Mikrofon
Scanner – Scanner
IOC – Eingangs-/Ausgangs-Schaltkreis
CPU – Zentraleinheit
Network – Netzwerk
Disk store – Plattenspeicher
Memory – Speicher
Buf – Puffer
Prog – Programmmodul
Server pub key – Server öffentlicher Schlüssel
Autor priv key – Verfasser privater Schlüssel
Notary pub key – Notar öffentlicher Schlüssel
Author pub key – Verfasser öffentlicher Schlüssel
Authoring station – Autorenstation

Fig. 6

Network – Netzwerk
IOC – Eingangs-/Ausgangs-Schaltkreis
CPU – Zentraleinheit
Memory – Speicher
Prog – Programmmodul
Buf – Puffer
Server priv key – Server privater Schlüssel
Certifier pub key – Zertifizierer öffentlicher Schlüssel
Server pub key – Server öffentlicher Schlüssel
Author pub key – Verfasser öffentlicher Schlüssel
Server – Server
Disk – Platte
Archival device – Archivierungsvorrichtung

Fig. 7

Network – Netzwerk
IOC – Eingangs-/Ausgangs-Schaltkreis
CPU – Zentraleinheit
Memory – Speicher
Prog – Programmmodul
Buf – Puffer
Notary pub key – Notar öffentlicher Schlüssel
Notary priv key – Notar privater Schlüssel
Hard disk – Festplatte
Time stamp & signature – Zeitstempel & Signator

Fig. 8

Host computer – Host-Computer
Communication – Kommunikation
I/O – E/A
ROM – ROM
PROC – Prozessor
RAM – RAM

Programmable computer – Programmierbarer Computer
PC card – PC-Karte
Perm mem – Permanentspeicher
Storage drive – Speicherlaufwerk
User interface – Benutzerschnittstelle
Media – Medien

Patentansprüche

1. Computernetzwerk (**300**), das Folgendes umfasst:
ein Computersystem eines Benutzers (**304**, **350**), das dem Benutzer den Zugang zu dem Netzwerk ermöglicht, das Folgendes umfasst:
Mittel (**356**-**360** und **370**) zum Bereitstellen eines Originaldokuments;
Mittel (**372**, **422**), um eine Dokumentsignatur vom Originaldokument zu erstellen; und
Mittel (**355**, **374**), um die Signatur des Originaldokuments zu übertragen;
ein sicheres Computersystem (**303**, **450**), das Folgendes umfasst:
Mittel (**454**, **470**), um eine Dokumentsignatur vom Benutzersystem zu empfangen;
Mittel (**472**), um einen Zeitstempel bereit zu stellen, der die Dokumentsignatur und einen digitalen Zeitpunkt, an dem das Dokument empfangen wurde, enthält; und
Mittel (**437**, **454**, **470**), um den Zeitstempel zum Benutzersystem zu übertragen;
wobei das Benutzersystem weiterhin Folgendes umfasst:
Mittel (**377**, **355**, **375**, **384**), um einen Zeitstempel für das Originaldokument zu empfangen und zu speichern;
Mittel (**386**) zum Revidieren des Originaldokuments, um ein revidiertes Dokument zu erstellen, und
Mittel (**387**), um eine revidierte Dokumentsignatur in Abhängigkeit vorn revidierten Dokument zu erstellen;
und in dem die Mittel (**355**, **373**) zum Übertragen der Dokumentsignatur dafür geeignet sind, die revidierte Dokumentsignatur zu übertragen;
das Computernetzwerk enthält darüber hinaus Mittel (**377**, **378**, **424**, **472**, **476**, **477**, **383**, **384** und **485**), um den Zeitstempel zu authentifizieren; und
dadurch gekennzeichnet, dass die revidierte Dokumentsignatur auch vom Zeitstempel des Originaldokuments abhängig ist.

2. Netzwerk nach Anspruch 1, in dem das Mittel zum Authentifizieren des Zeitstempels Folgendes umfasst:
einen privaten Schlüssel (**490**) zum Verschlüsseln der Daten in dem sicheren System;
einen öffentlichen Schlüssel (**491**), der in der Lage ist, die vorher unter Verwendung des privaten Schlüssels verschlüsselten Daten zu entschlüsseln;
Mittel (**472**), um unter Verwendung des privaten Schlüssels in dem sicheren System eine Zeitstempelsignatur vom Zeitstempel zu erstellen;
Mittel (**473**), um die Zeitstempelsignatur zum Benutzersystem zu übertragen;
Mittel (**383**), um die Zeitstempelsignatur unter Verwendung eines öffentlichen Schlüssels auf dem Benutzersystem zu entschlüsseln;
Mittel (**384**), um den Zeitstempel oder einen Hash-Wert des Zeitstempels mit der entschlüsselten Zeitstempelsignatur auf dem Benutzersystem zu vergleichen, um festzustellen, ob der Zeitstempel authentisch ist.

3. Netzwerk nach Anspruch 1, in dem die Mittel zum Authentifizieren des Zeitstempels Folgendes umfassen:
sicheren Speicher (**456**) zum Speichern des Zeitstempels auf dem sicheren System;
Mittel (**425**), um den Zeitstempel vom Benutzersystem zum sicheren System zu übertragen;
Mittel (**475**), um den Zeitstempel vom sicheren Speicher in das sichere System abzurufen;
Mittel (**476**), um den abgefragten Zeitstempel und den übertragenen Zeitstempels zu vergleichen; und
Mittel (**477**), um abhängig vom Vergleich ein Authentifizierungssignals oder ein Authentifizierungs-Fehlersignals vom sicheren System zum Benutzersystem zu übertragen.

4. Netzwerk nach Anspruch 1, in dem die Mittel zum Authentifizieren des Zeitstempels Folgendes umfassen:
Mittel (**472**), um eine erste Zeitstempelsignatur vom Zeitstempel unter Verwendung eines privaten Schlüssels im sicheren System zu erstellen;
Mittel (**470**, **473**), um den Zeitstempel und die erste Zeitstempelsignatur zum Benutzersystem zu übertragen;
Mittel, um den Zeitstempel zum sicheren System zurückzusenden;
Mittel (**473**), um eine zweite Zeitstempelsignatur vom zurückgesandten Zeitstempel auf dem sicheren System zu erstellen;
Mittel, um die zweite Zeitstempelsignatur zum Benutzersystem zu übertragen; und
Mittel (**383**), um die erste Zeitstempelsignatur mit der zweiten Zeitstempelsignatur zu vergleichen, um die Authentizität des Zeitstempels zu überprüfen.

5. Netzwerk nach Anspruch 1, in dem:
die Übertragung vom sicheren Server einen vorhergehenden Zeitstempel und eine vorhergehende Zeitstempelsignatur sowie einen nachfolgenden Zeitstempel und eine nachfolgende Zeitstempelsignatur enthält, wobei jeder Zeitstempel die Identifikation des Kunden enthält;
das Benutzersystem den vorhergehenden und den nachfolgenden Zeitstempel und die Signatur speichert; und
die Mittel zum Authentifizieren des Zeitstempels geeignet sind, um mit dem vom nachfolgenden Zeit-

stempel identifizierten Kunden zu kommunizieren und um eine Kopie des nachfolgenden Zeitstempels und der Zeitstempelsignatur vom nachfolgenden Kunden zu erhalten.

6. Netzwerk nach Anspruch 1, in dem das Mittel zum Revidieren des Dokuments das Dokument automatisch bei Erhalt des Dokuments revidiert.

7. Netzwerk nach Anspruch 1, in dem das Computersystem des Benutzers eine Autoren-Workstation (**350**) zum Erstellen des Dokuments enthält und einen sicheren Server (**400**) zum Speichern des Dokuments, der Dokumentsignatur und des Zeitstempels des Dokuments.

8. Computersystem (**304**, **350**), das Folgendes umfasst:
Mittel (**356**, **360** und **370**) zum Bereitstellen eines Originaldokuments;
Mittel (**372**, **422**), um eine Dokumentsignatur vom Originaldokument zu erstellen;
Mittel (**386**) zum Revidieren des Originaldokuments, um eine revidiertes Dokument zu erstellen; und
Mittel (**387**), um abhängig vom revidierten Dokument eine revidierte Dokumentsignatur zu erstellen;
dadurch gekennzeichnet, dass die revidierte Dokumentsignatur auch von der Signatur des Originaldokuments abhängt.

9. Computersystem (**304**, **350**) nach Anspruch 8, das Folgendes umfasst:
Mittel (**355**, **374**), um die Signatur des Originaldokuments zu einem sicheren Computersystem (**303**, **450**) zum Zeitstempeln zu übertragen;
Mittel (**377**, **355**, **375**, **384**), um vom sicheren Computersystem einen Zeitstempel für das Originaldokument zu empfangen und zu speichern; wobei der Zeitstempel die Signatur des Originaldokuments und einen digitalen Stempelzeitpunkt enthält, der angibt, wann der Zeitstempel erstellt wurde; und
in dem die Signatur des revidierten Dokuments vom digitalen Stempelzeitpunkt im Zeitstempel für das Originaldokument abhängig ist.

10. Computernetzwerk, das Folgendes umfasst:
Mittel (**356**-**360** und **370**) für einen Verfasser, um ein Originaldokument auf einer für den Benutzer zugänglichen Station zu erstellen;
Mittel (**355**, **374**) zum Übertragen des Originaldokuments auf einen sicheren Server;
Mittel (**372**, **422**) zum Erstellen einer Signatur für das Originaldokument;
Mittel (**423**), um die Signatur für den Nachweis zu verwenden, dass das Dokument nicht geändert wurde und zum Identifizieren des Benutzers oder der Station;
Mittel (**420**, **422**) zum Übertragen der Signatur des Originaldokuments vom sicheren Server an einen Notar;
Mittel (**472**) zum Bereitstellen eines Zeitstempels beim Notar, der die Signatur des Originaldokuments und einen digitalen Zeitpunkt enthält, der den Zeitpunkt angibt, an dem die Signatur vom Notar empfangen wurde;
Mittel (**470**, **473**) zum Übertragen des Zeitstempels an den sicheren Server;
Mittel (**424**) zum Überprüfen, dass der Zeitstempel authentisch ist;
Mittel (**422**) zum Revidieren des Originaldokuments;
Mittel (**422**) zum Erstellen einer Signatur für das revidierte Dokument in Abhängigkeit vom revidierten Dokument;
dadurch gekennzeichnet, dass die Signatur für das revidierte Dokument auch vom Originaldokument abhängig ist, wobei die Tatsache, dass das revidierte Dokument anhand des Originaldokument erstellt wurde, überprüft werden kann.

11. Verfahren zum Betrieb eines Computernetzwerks, das die folgenden Schritte umfasst:
Bereitstellen (**122**) eines Originaldokuments auf einem Benutzersystem;
Erstellen (**132**) eines revidierten Dokuments in Abhängigkeit vom Originaldokument;
Erstellen (**133**) einer Signatur eines revidierten Dokuments, einschließlich Hashing des revidierten Dokuments, um einen Fingerabdruck eines Dokuments zu erstellen, und Verschlüsseln des Fingerabdrucks des Dokuments;
Übertragen (**135**) der Signatur des revidierten Dokuments vom Benutzersystem zu einem sicheren Computersystem;
Bereitstellen (**174**) eines Zeitstempels für das revidierte Dokument, wobei der Zeitstempel die Signatur des revidierten Dokuments und einen digitalen Zeitpunkt enthält, der angibt, wann der Zeitstempel erstellt wurde;
Übertragen (**212**) des Zeitstempels vom sicheren System zum Benutzersystem, wobei der Zeitstempel die Signatur des revidierten Dokuments enthält;
Feststellen (**218**), ob der Zeitstempel authentisch ist; und
Feststellen (**218**), ob die Signatur des revidierten Dokuments im Zeitstempel authentisch ist, abhängig vom Vergleich zwischen einer Entschlüsselung der Signatur des revidierten Dokuments und einem Hash-Wert des revidierten Dokuments;
dadurch gekennzeichnet, dass das Erstellen des Fingerabdrucks des Dokuments das Hashing des revidierten Dokuments zusammen mit Informationen umfasst, die angeben, dass das revidierte Dokument anhand des Originaldokuments erstellt wurde, und dadurch, dass das Feststellen, ob die Signatur des revidierten Dokuments authentisch ist, beinhaltet, dass festgestellt wird, ob das revidierte Dokument anhand des Originaldokuments erstellt wurde, was das Hashing (**216**) des revidierten Dokuments zusammen mit dem Originaldokument umfasst, das Informationen zum Wiederherstellen des Fingerabdrucks des Doku-

ments angibt.

12. Verfahren nach Anspruch 11, in dem der Schritt zum Feststellen, ob der Zeitstempel authentisch ist, die nachfolgenden Schritte umfasst:
Speichern des Zeitstempels in einem sicheren Speicher des sicheren Systems;
Übertragen des Zeitstempels vom Benutzersystem zum sicheren System;
Vergleichen des Zeitstempels des Benutzersystems mit dem Zeitstempel im sicheren Speicher;
Übertragen der Ergebnisse des Vergleichs an das Benutzersystem; und
abhängig von den Ergebnissen des Vergleichs Feststellen, ob der Zeitstempel authentisch ist.

13. Verfahren nach Anspruch 11, in dem der Schritt des Feststellens, ob der Zeitstempel authentisch ist, die nachfolgenden Schritte umfasst:
Bereitstellen eines privaten Schlüssels auf dem sicheren System;
Verschlüsseln des Zeitstempels, um eine Signatur eines Zeitstempels auf dem sicheren System zu erstellen;
Übertragen der Zeitstempelsignatur vom sicheren System zum Benutzersystem;
Übertragen des Zeitstempels und der Zeitstempelsignatur vom Benutzersystem zum sicheren System;
Verschlüsseln des Zeitstempels unter Verwendung des privaten Schlüssels, um eine Signatur zum Überprüfen des Zeitstempels zu erstellen;
Vergleichen der Zeitstempelsignatur mit der Signatur zum Überprüfen des Zeitstempels; und
abhängig von den Ergebnissen des Vergleichs Feststellen, ob der Zeitstempel authentisch ist.

14. Verfahren nach Anspruch 11, in dem der Schritt des Feststellens, ob der Zeitstempel authentisch ist, die nachfolgenden Schritte umfasst:
Bereitstellen eines privaten Schlüssels auf dem sicheren System;
Verschlüsseln des Zeitstempels, um eine Signatur eines Zeitstempels unter Verwendung des privaten Schlüssels auf dem sicheren System zu erstellen;
Übertragen der Zeitstempelsignatur vom sicheren System zum Benutzersystem;
Bereitstellen eines öffentlichen Schlüssels für den privaten Schlüssel auf dem Benutzersystem;
Entschlüsseln der Zeitstempelsignatur unter Verwendung des öffentlichen Schlüssels;
Vergleichen der Signatur des verschlüsselten Zeitstempels mit dem Zeitstempel oder dem Ergebnis des Verarbeitens des Zeitstempels; und
abhängig vom Vergleich Feststellen, ob der Zeitstempel authentisch ist.

15. Verfahren nach Anspruch 11, in dem der Schritt des Feststellens, ob der Zeitstempel authentisch ist, Folgendes umfasst:
Übertragen der Information, die den Kunden eines nachfolgenden Zeitstempels identifizieren, an das Benutzersystem;
Übertragen des Zeitstempels für das revidierte Dokument an den nachfolgenden Kunden;
Kommunizieren mit dem nachfolgenden Kunden, um den Zeitstempel für das revidierte Dokument mit dem Zeitstempel für das an den nachfolgenden Kunden übertragene, revidierte Dokument zu vergleichen.

16. Verfahren nach Anspruch 11, in dem
das Erstellen des Fingerabdrucks des revidierten Dokuments das Hashing des revidierten Dokuments zusammen mit Informationen umfasst, die die Herkunft des revidierten Dokuments angeben; und
das Feststellen, ob die Signatur des revidierten Dokuments authentisch ist, das Feststellen, ob das revidierte Dokument von solcher Herkunft ist, umfasst, was das Hashing des revidierten Dokuments zusammen mit den Informationen umfasst, die die Herkunft angeben, um den Fingerabdruck des Dokuments wieder herzustellen.

17. Verfahren nach Anspruch 11, in dem die das Originaldokument angebenden Informationen von der Signatur des Originaldokuments abhängig sind.

18. Verfahren nach Anspruch 11, in dem die das Originaldokument angebenden Informationen von der Herkunft des Originaldokuments abhängig sind.

19. Verfahren nach Anspruch 11, in dem:
das Verfahren weiterhin das Erhalten eines Zeitstempels für das Originaldokument umfasst; und
die die Herkunft angebenden Informationen von einem Stempelzeitpunkt des Zeitstempels für das Originaldokument abhängig sind.

20. Verfahren nach Anspruch 11, in dem
Informationen, die die Identität des Verfassers der Revision des revidierten Dokuments angeben, in dem Hash-Wert der Revision enthalten sind, und
das Feststellen, ob die Signatur des revidierten Dokuments authentisch ist, das Hashing des revidierten Dokuments mit den Informationen umfasst, die den Verfasser identifizieren.

21. Verfahren zum Revidieren eines Dokuments, das Folgendes umfasst:
Eingeben (**192**) eines revidierten Dokuments in ein für den Revisor zugängliches System;
Übertragen (**123**) des Dokuments, eines Zeitstempels für das Dokument und einer Zeitstempelsignatur für das Dokument von einem sicheren System an das für den Revisor zugängliche System;
automatisches (**124**) Verwenden eines öffentlichen Schlüssels eines Notars zum Überprüfen, dass der Zeitstempel und die Zeitstempelsignatur von dem im Zeitstempel aufgeführten Notar erstellt wurden und dass der Zeitstempel nicht verändert wurde;
automatisches (**126**) Verwenden eines öffentlichen

Schlüssels eines Erstellers zum Überprüfen, dass eine Dokumentsignatur in dem Zeitstempel vom Ersteller erstellt wurde und dass das Dokument seit der Erstellung der Signatur nicht verändert wurde;
Revidieren des Dokuments in das revidierte Dokument, wenn die Überprüfung erfolgreich war;
Übertragen des revidierten Dokuments vom für den Revisor zugänglichen System zum sicheren Server;
Übertragen (**172**) einer Signatur eines revidierten Dokuments an einen Notar;
Erstellen (**174**) eines Zeitstempels eines revidierten Dokuments, der die Signatur des revidierten Dokuments und einen Zeitstempel enthält, der angibt, wann der Notar die Signatur des revidierten Dokuments erhalten hat;
Verwenden (**176**) eines privaten Schlüssels des Notars, um eine Signatur für den Zeitstempel des revidierten Dokuments zu erstellen;
Übertragen (**178**) des Zeitstempels und der Zeitstempelsignatur für das revidierte Dokument zurück an den Server;
Speichern (**180**) des revidierten Dokuments, des Zeitstempels für das revidierte Dokument und der Zeitstempelsignatur für das revidierte Dokument in einem sicheren Speicher auf dem sicheren Server; und
dadurch gekennzeichnet, dass das Verfahren Folgendes umfasst:
Verwenden (**134**) eines privaten Schlüssels eines Erstellers der Revision, um die Signatur des revidierten Dokuments für das revidierte Dokument unter Verwendung von Informationen zum Überprüfen, dass das revidierte Dokument anhand des Dokuments erstellt wurde, zu erstellen.

22. Verfahren zum automatischen Revidieren eines Dokuments, das Folgendes umfasst:
Übertragen eines Originaldokuments von einem Autorensystem an das System des Kunden;
automatisches Speichern (**194**) eines revidierten Dokuments, das auf einem Kundensystem anhand des Originaldokuments im System des Kunden erstellt wurde;
Übertragen (**172**) der Signatur eines revidierten Dokuments für das revidierte Dokument vom System des Kunden an ein elektronisches Notarsystem;
Erstellen (**174**) einer Aufzeichnung eines Zeitstempels für das revidierte Dokument, die die Signatur des revidierten Dokuments und einen digitalen Zeitpunkt enthält, der angibt, warm der Notar das Dokument erhalten hat;
Verwenden (**176**) eines privaten Schlüssels des Notars zum Verschlüsseln des Zeitstempels, um eine digitale Signatur für den Zeitstempel zu erstellen;
Speichern (**177**) des Zeitstempels und der Zeitstempelsignatur im elektronischen Notarsystem;
Übertragen des Zeitstempels und der Zeitstempelsignatur zum Kunden;
Speichern des Zeitstempels und der Zeitstempelsignatur im System des Kunden; und
dadurch gekennzeichnet, dass das Verfahren Folgendes umfasst:
Verwenden (**166**) eines privaten Schlüssels zum Erstellen der Signatur des revidierten Dokuments mit Informationen zum Überprüfen, dass das revidierte Dokument anhand des Originaldokuments erstellt und seit dem Signieren der Revision nicht geändert wurde.

Es folgen 10 Blatt Zeichnungen

Anhängende Zeichnungen

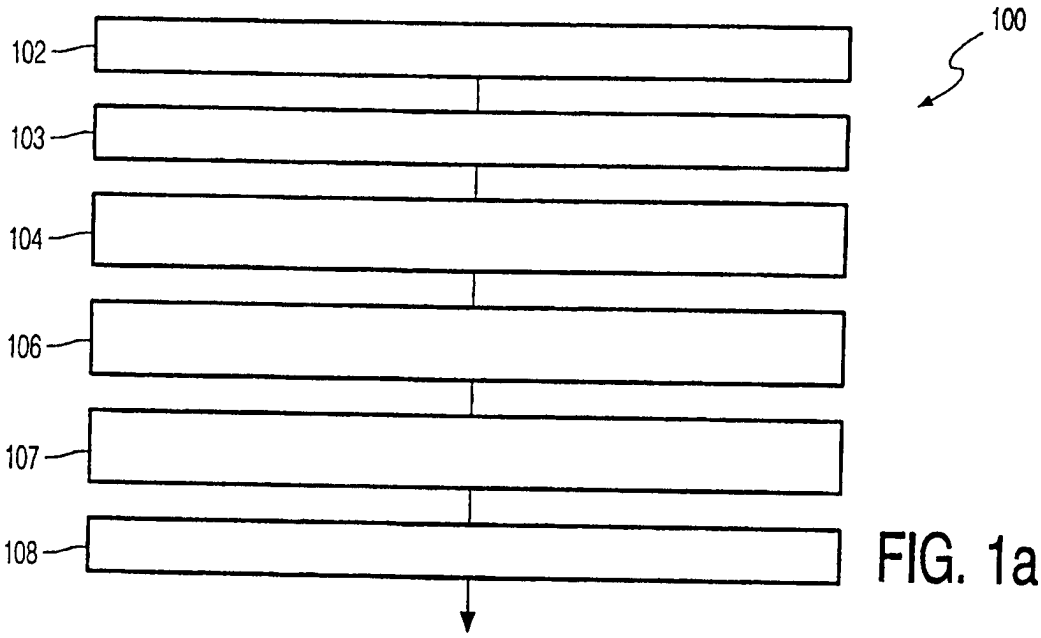

FIG. 1a

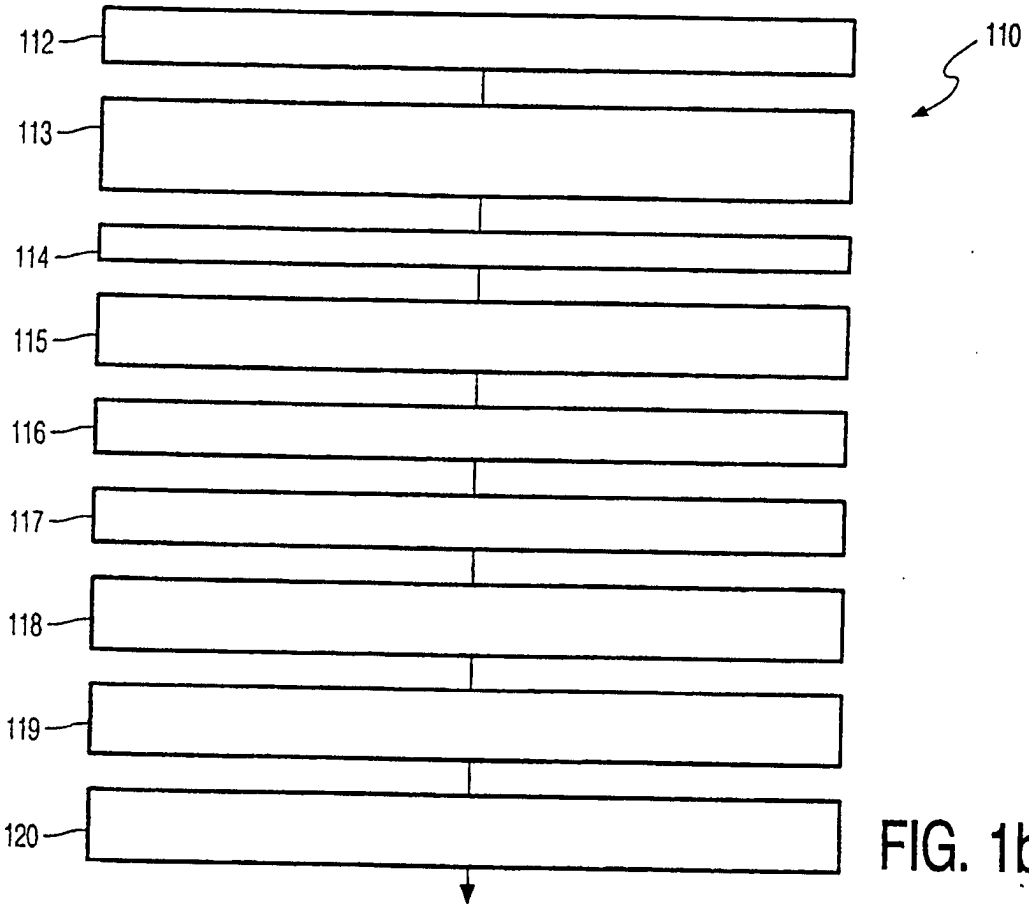

FIG. 1b

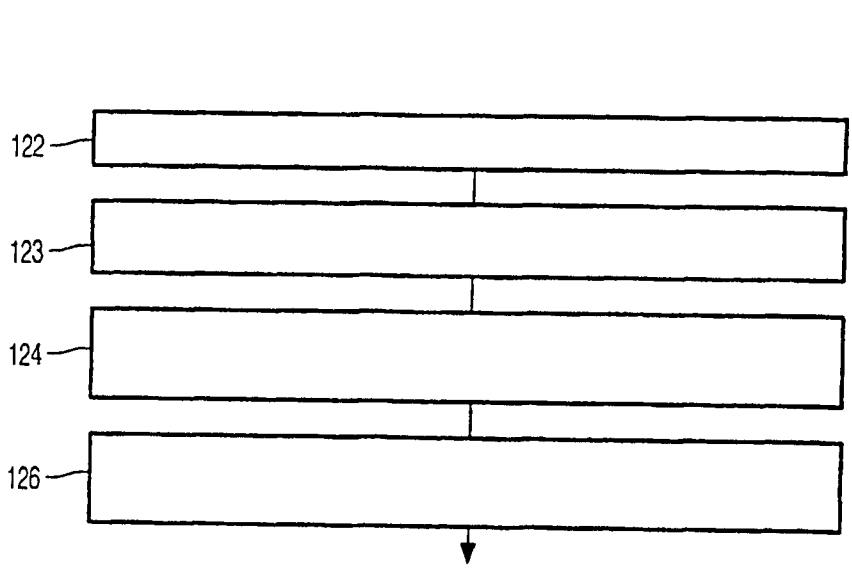

FIG. 1c

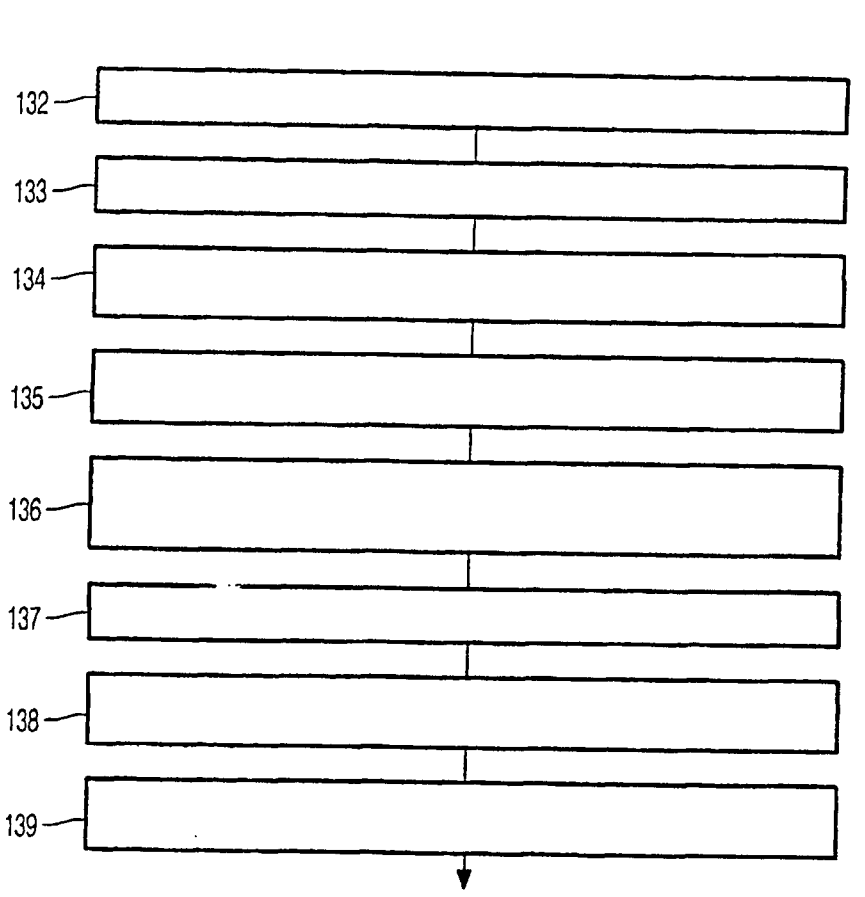

FIG. 1d

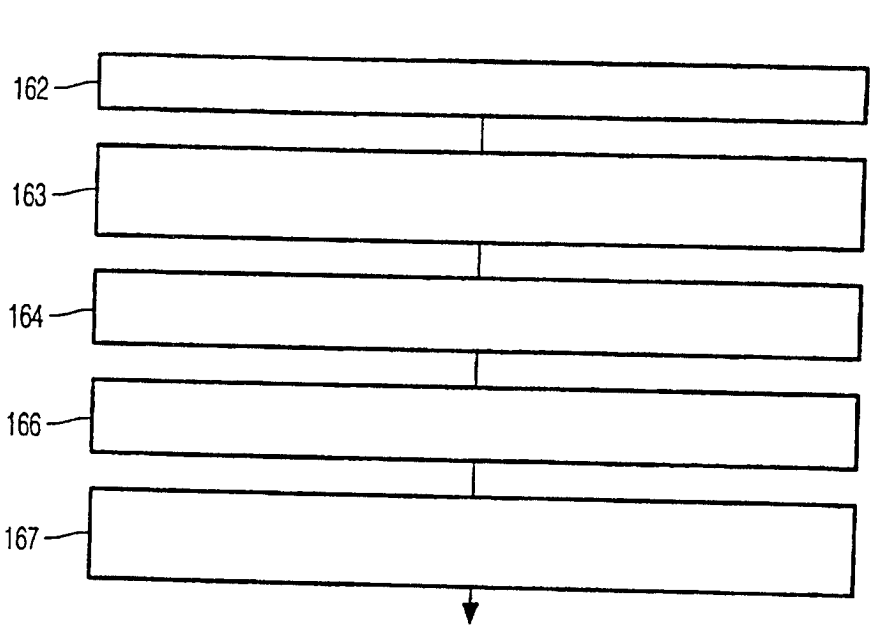

FIG. 2a

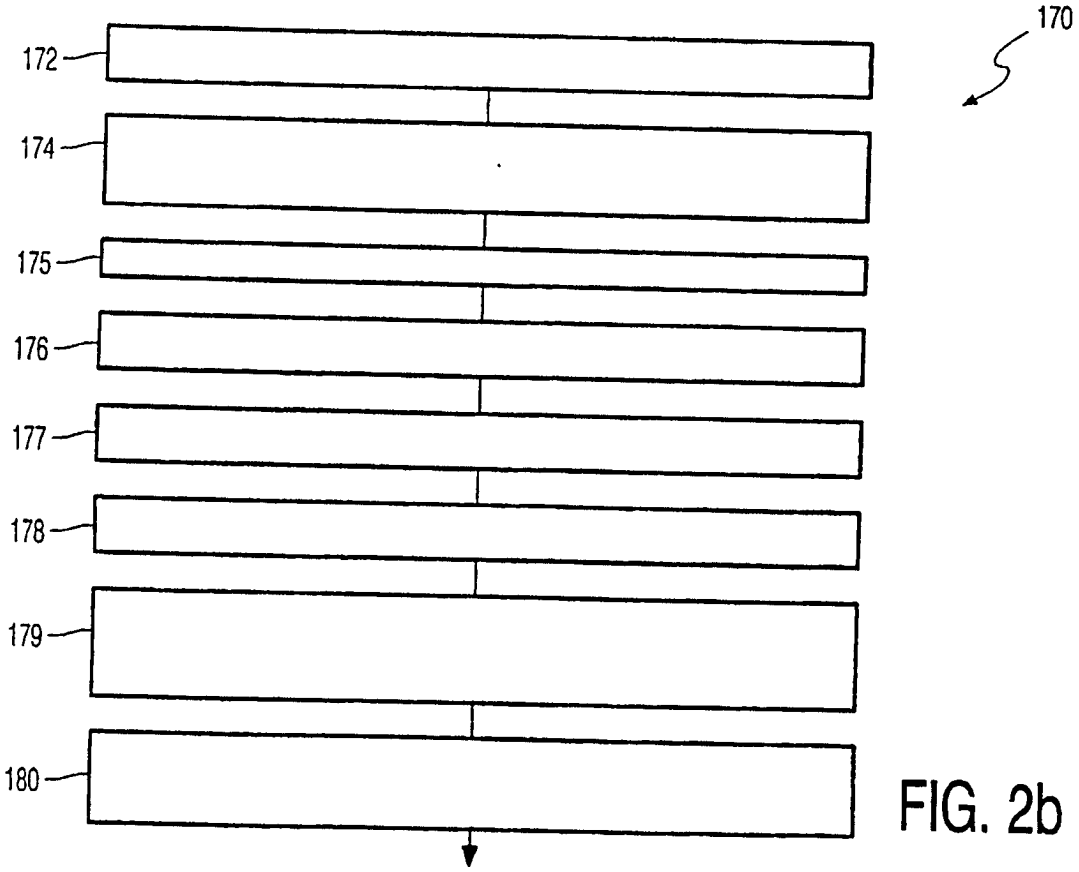

FIG. 2b

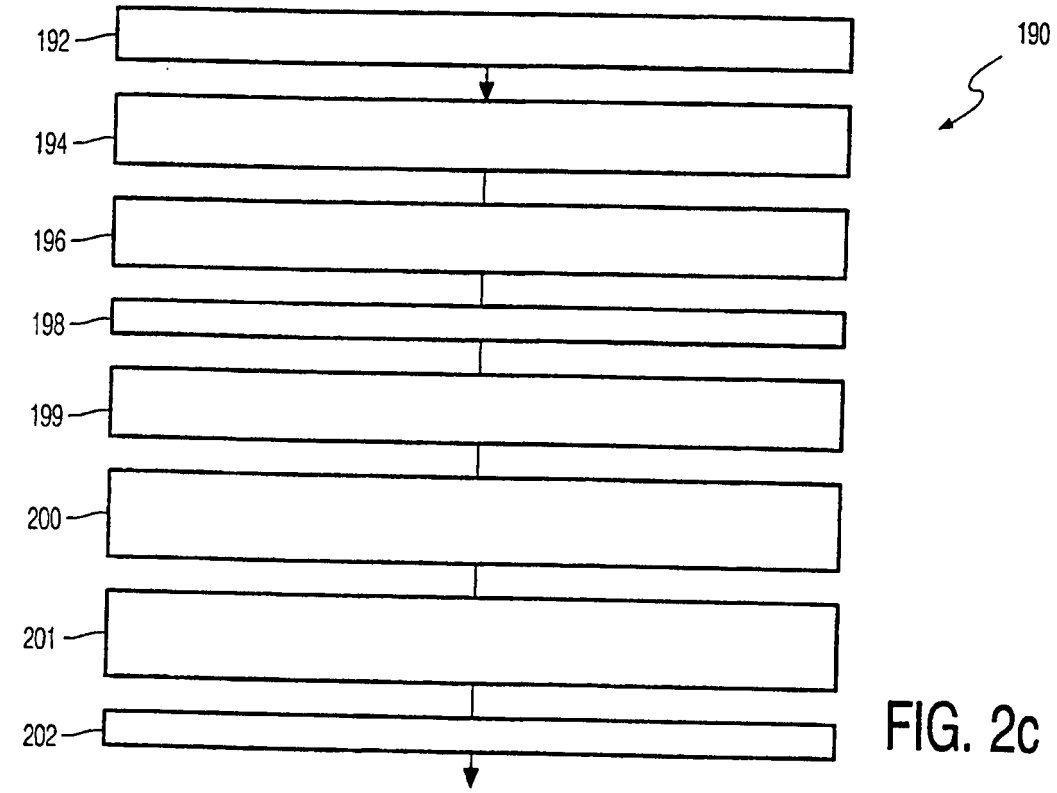
192
194
196
198
199
200
201
202
190

FIG. 2c

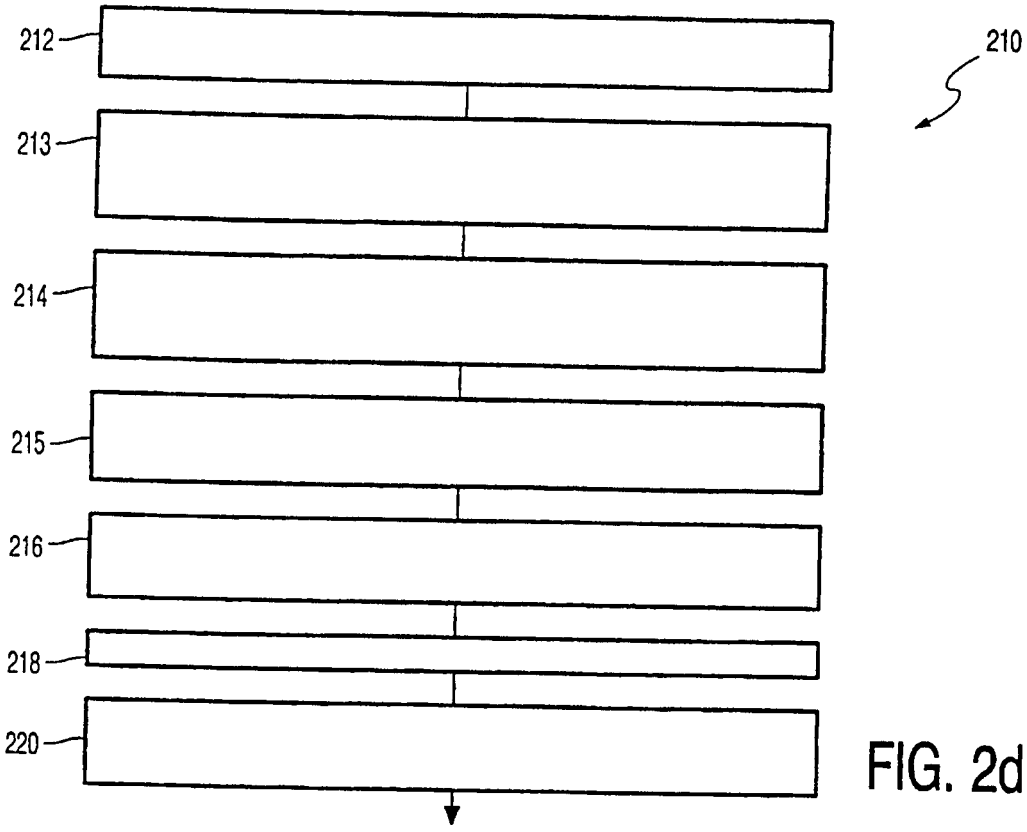
212
213
214
215
216
218
220
210

FIG. 2d

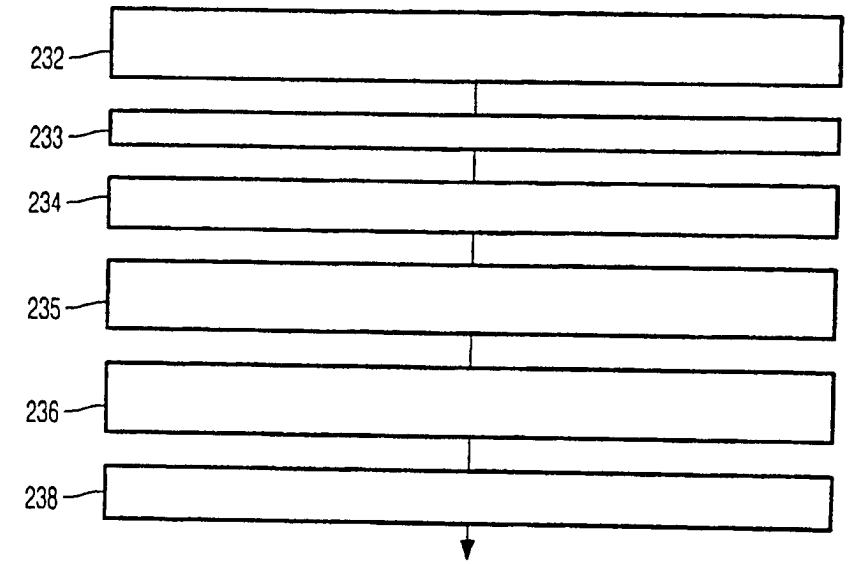
230
232
233
234
235
236
238

FIG. 3a

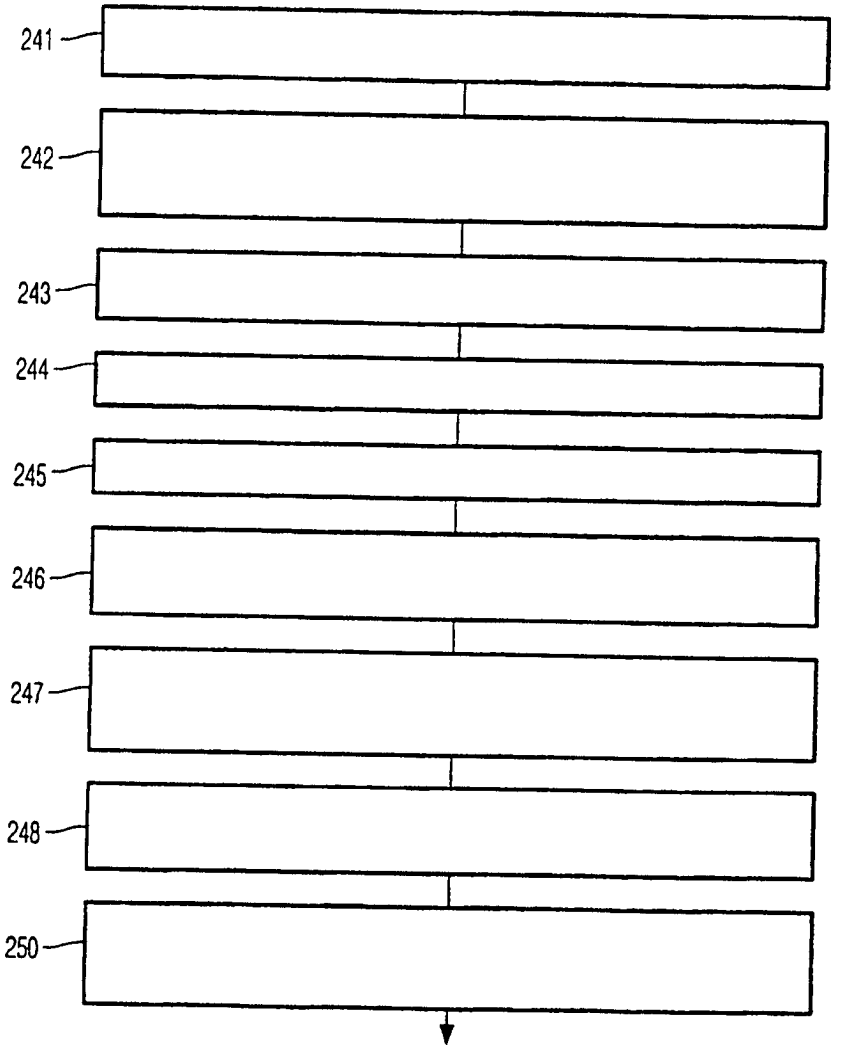
240
241
242
243
244
245
246
247
248
250

FIG. 3b

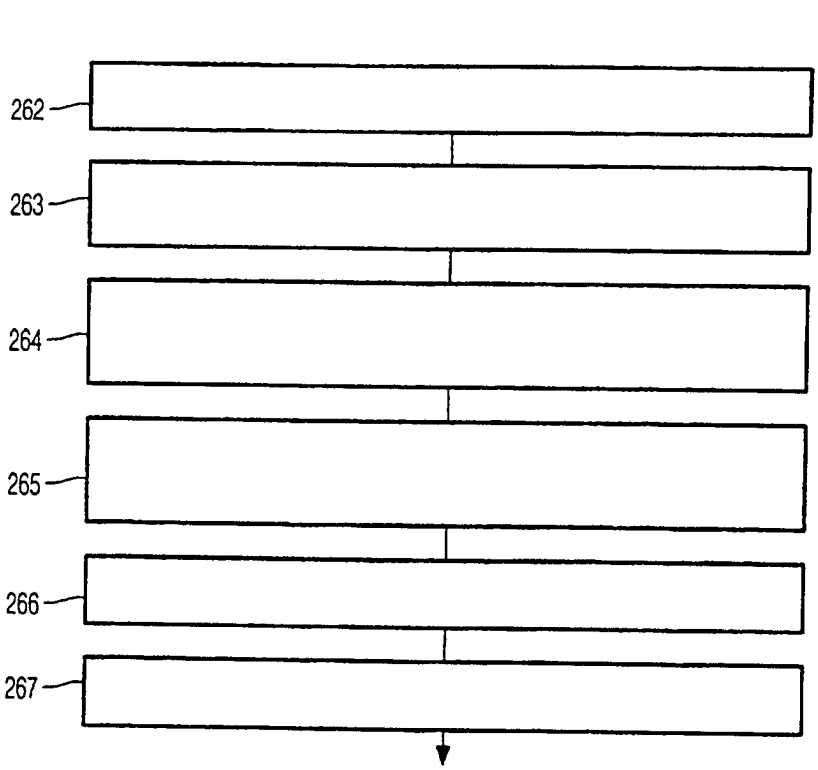
260
262
263
264
265
266
267

FIG. 3c

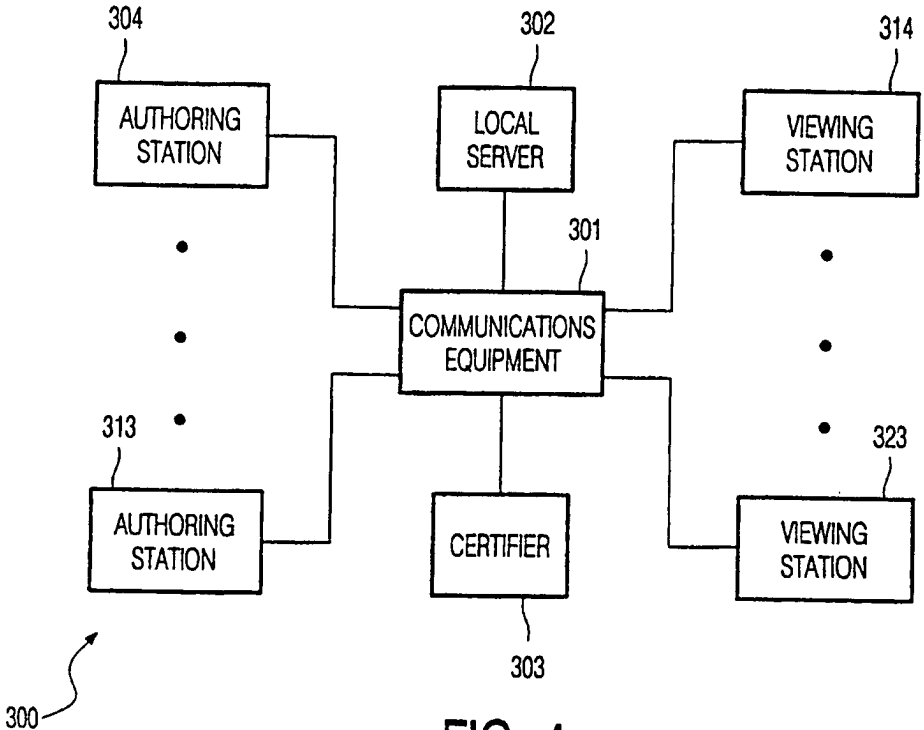
304
302
314
AUTHORING STATION
LOCAL SERVER
VIEWING STATION
301
COMMUNICATIONS EQUIPMENT
313
323
AUTHORING STATION
CERTIFIER
VIEWING STATION
303
300

FIG. 4

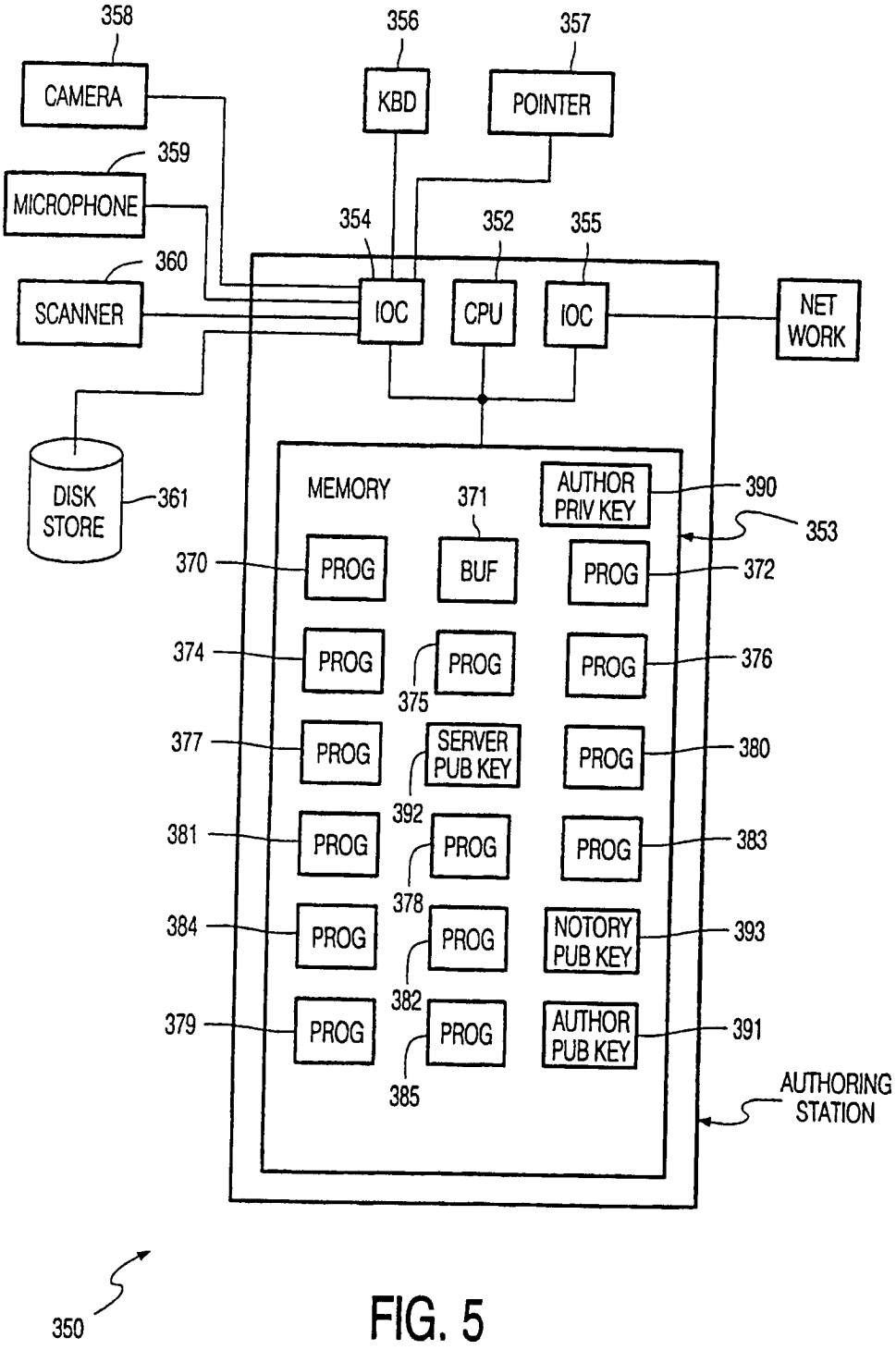
358
CAMERA
356
KBD
357
POINTER
359
MICROPHONE
354
352
355
360
SCANNER
IOC
CPU
IOC
NET WORK
DISK STORE
361
MEMORY
371
AUTHOR PRIV KEY
390
353
370
PROG
BUF
PROG
372
374
PROG
PROG
PROG
376
375
377
PROG
SERVER PUB KEY
PROG
380
392
381
PROG
PROG
PROG
383
378
384
PROG
PROG
NOTORY PUB KEY
393
382
379
PROG
PROG
AUTHOR PUB KEY
391
385
AUTHORING STATION
350

FIG. 5

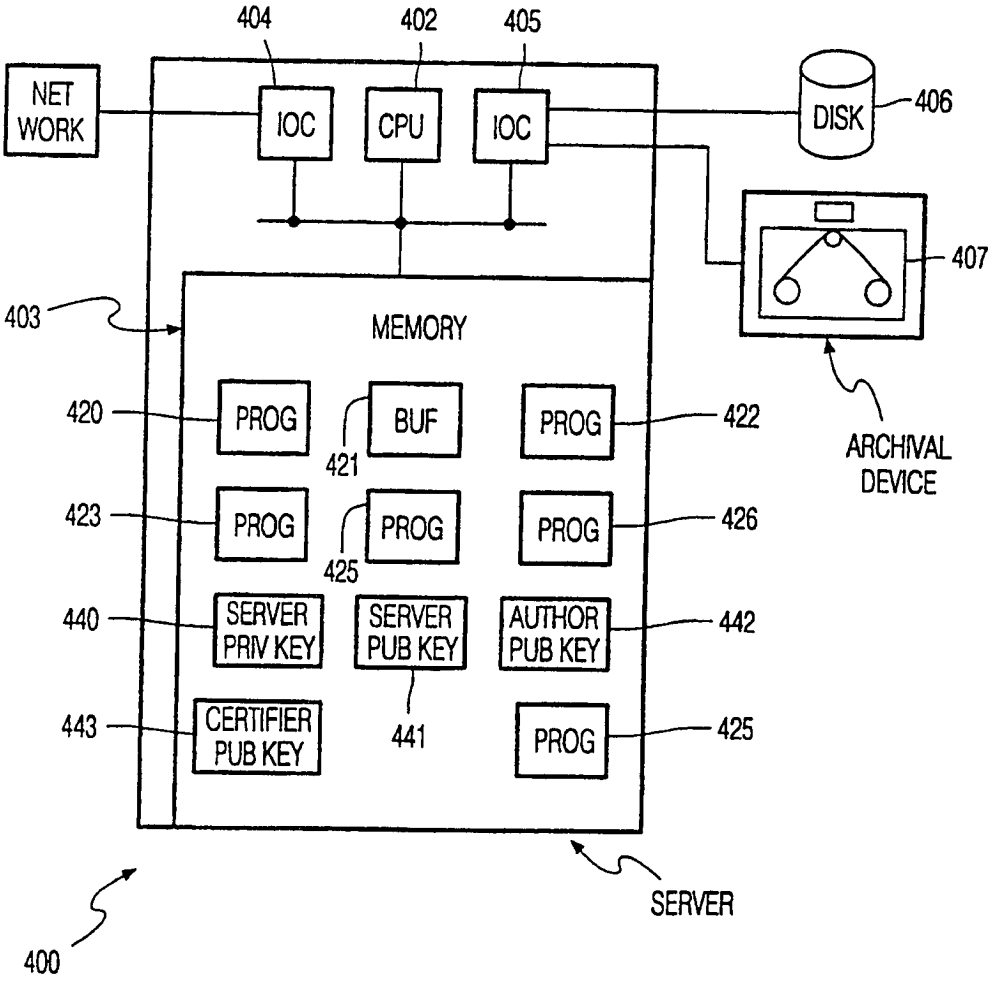
404
402
405
NET WORK
IOC
CPU
IOC
DISK
406
407
403
MEMORY
420
PROG
BUF
421
PROG
422
423
PROG
PROG
425
PROG
426
440
SERVER PRIV KEY
SERVER PUB KEY
AUTHOR PUB KEY
442
443
CERTIFIER PUB KEY
441
PROG
425
ARCHIVAL DEVICE
SERVER
400

FIG. 6

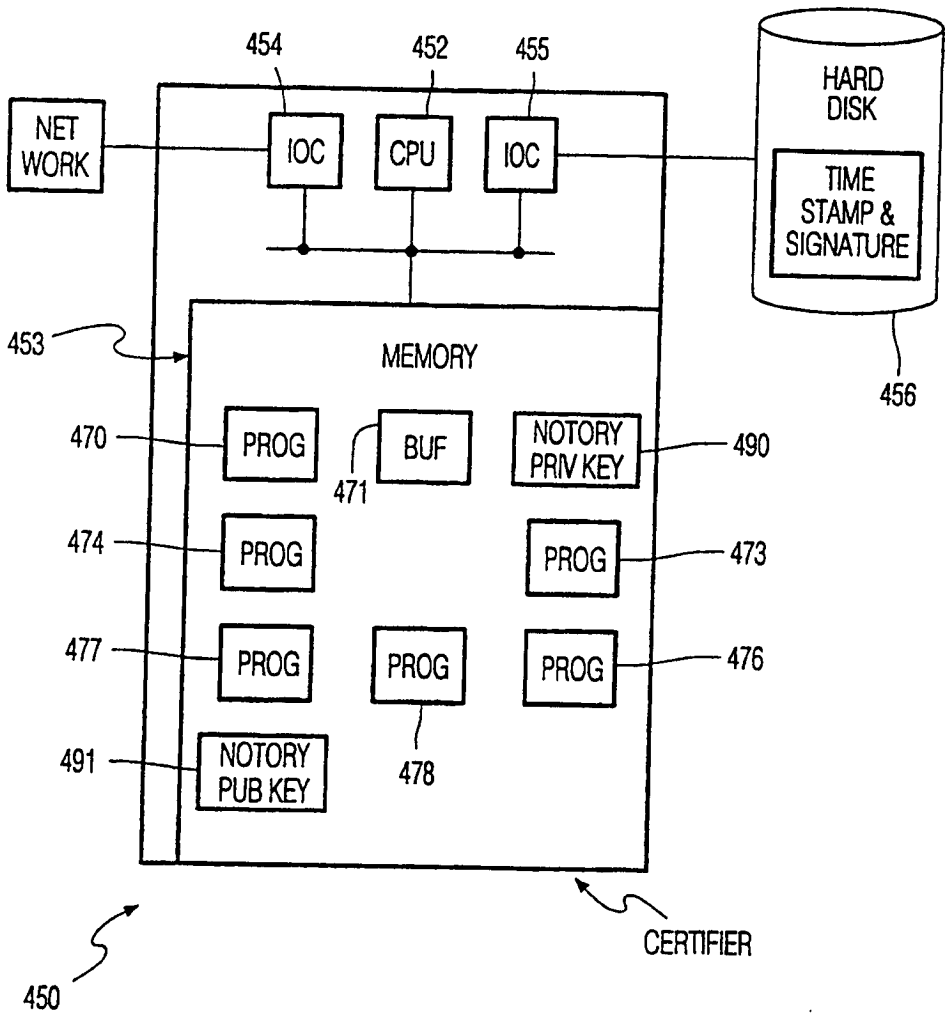
454
452
455
NET WORK
IOC
CPU
IOC
HARD DISK
TIME STAMP & SIGNATURE
456
453
MEMORY
470
PROG
BUF
471
NOTORY PRIV KEY
490
474
PROG
PROG
473
477
PROG
PROG
PROG
476
491
NOTORY PUB KEY
478
CERTIFIER
450

FIG. 7

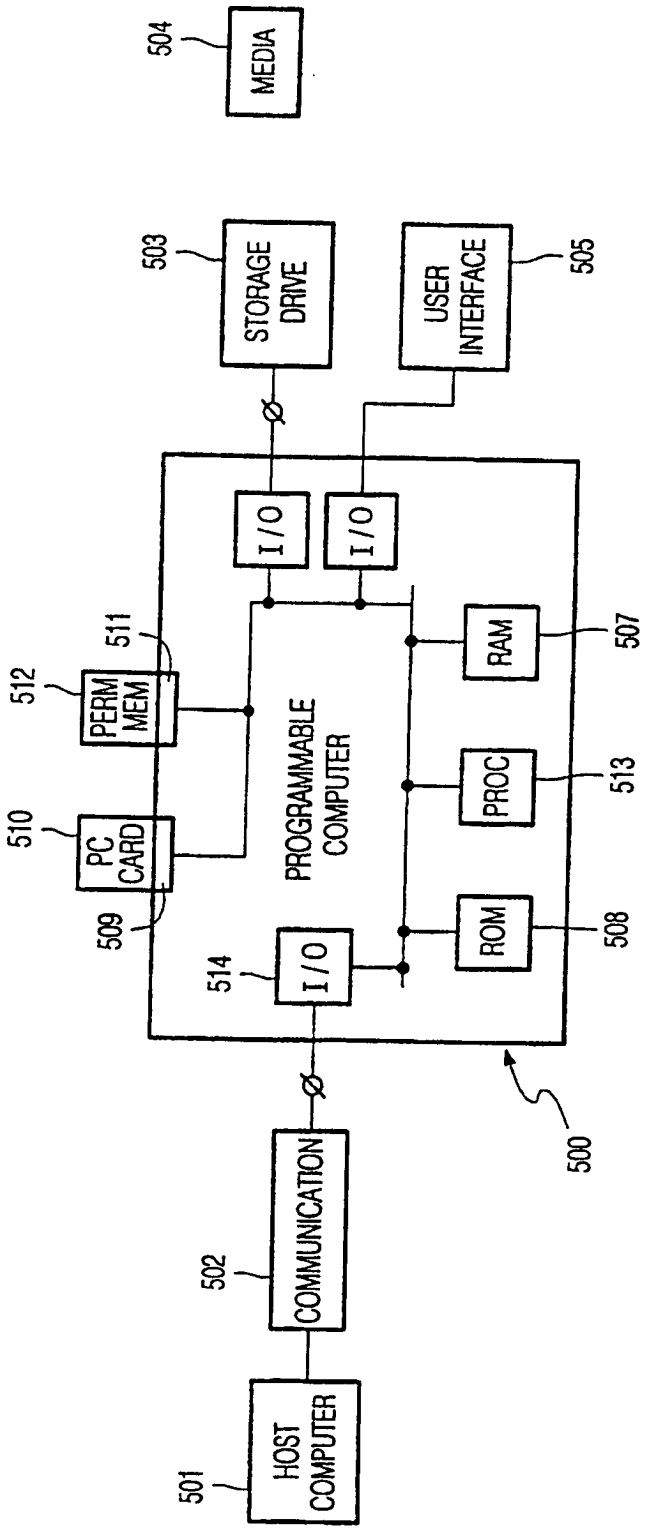
504
MEDIA
503
STORAGE DRIVE
USER INTERFACE
505
I/O
I/O
511
512
PERM MEM
RAM
507
PROGRAMMABLE COMPUTER
510
PC CARD
PROC
513
509
514
I/O
ROM
508
500
COMMUNICATION
502
HOST COMPUTER
501

FIG. 8