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

(10) **DE 600 29 567 T2** 2007.09.20

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 159 799 B1**
(21) Deutsches Aktenzeichen: **600 29 567.2**
(86) PCT-Aktenzeichen: **PCT/US00/05098**
(96) Europäisches Aktenzeichen: **00 914 752.1**
(87) PCT-Veröffentlichungs-Nr.: **WO 2000/051286**
(86) PCT-Anmeldetag: **24.02.2000**
(87) Veröffentlichungstag der PCT-Anmeldung: **31.08.2000**
(97) Erstveröffentlichung durch das EPA: **05.12.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **26.07.2006**
(47) Veröffentlichungstag im Patentblatt: **20.09.2007**

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

(30) Unionspriorität:
259135 **26.02.1999** **US**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(73) Patentinhaber:
Authentidate Holding Corp., Schenectady, N.Y., US

(72) Erfinder:
BORROWMAN, D., Colin, Schenectady, NY 12303, US

(74) Vertreter:
Adolf - Lüken - Höflich - Sawodny Rechts- und Patentanwälte, 80807 München

(54) Bezeichnung: **DIGITALES DATENVERWALTUNGS-UND ABBILDHERSTELLUNGSSYSTEM UND VERFAHREN MIT GESICHERTER DATENMARKIERUNG**

Beschreibung

BEREICH DER ERFINDUNG

[0001] Diese Erfindung bezieht sich im Allgemeinen auf digitale Abbildungssysteme und im Speziellen auf digitale Dateiauthentifizierung.

HINTERGRUND DER ERFINDUNG

[0002] Digitales Abbilden bezeichnet die Darstellung und die Speicherung einer Abbildung oder eines Objekts als digitale Rasterabbildung. Digitales Abbilden wird immer öfter in vielen Industriezweigen verwendet, teilweise aufgrund der erhöhten Verfügbarkeit von Basistechnologien und teilweise aufgrund der vielen Vorteile gegenüber konventionellen Speichermethoden, darunter der reduzierte Speicherplatz, die erhöhte Zugriffsgeschwindigkeit, die gezielte Abrufbarkeit (z.B. Suchfunktionen), die Fähigkeit, bequem „mehrere" Kopien bzw. „Sicherungskopien" von Dokumenten zu machen, und die Fähigkeit, Dokumente schnell zu übertragen.

[0003] Im Fall von Originalpapierdokumenten scannen digitale Abbildungssysteme normalerweise das Dokument und speichern eine Darstellung des gescannten Dokuments als digitale Rasterabbildung. Es wird normalerweise ein optischer Scanner verwendet, um Abbildungen von Papierdokumenten zu scannen und als digitale Abbildung zu speichern. Die gescannten Abbildungen sind exakte Darstellungen des Originals (nur begrenzt durch das Auflösungsvermögen des Scanners) und sie können Handschriften, Signaturen, Fotos, Abbildungen usw. enthalten. Wahlweise können digitale Abbildungen aus Digitalkameras, medizinischen Abbildungsgeräten oder anderen Quellen ebenfalls in einem digitalen Abbildungssystem gespeichert werden.

[0004] Ein Nachteil der bekannten Abbildungstechnologie ist die inhärente Fähigkeit von digitalen Abbildungen, verändert werden zu können, zum Beispiel mit Betrugsabsicht Obwohl zum Beispiel an einem Originalpapierdokument unerlaubte Änderungen vorgenommen werden können, hinterlassen solche Veränderungen (Löschungen oder Hinzufügungen) normalerweise verräterische Beweise. Auf der anderen Seite können digitale Abbildungen solcher Dokumente verändert werden, ohne Beweise zu hinterlassen. Aus diesem Grund wird die Verwendung von digitalen Abbildungen, bei denen die Echtheit entscheidend ist und in Frage gestellt werden kann (z.B. im rechtlichen und medizinischen Bereich) oftmals nicht bevorzugt oder sie ist nicht gültig bzw. nicht zulässig und wird daher vermieden.

[0005] Da viele verschiedene digitale Abbildungsformate verfügbar sind, sind in jedem Fall die Daten potenziell veränderbar. Auch wenn das digitale Abbildungssystem nicht ausdrücklich eine Bearbeitungsfunktion bietet, können die Abbildungen mit einem Tool Dritter bearbeitet werden.

[0006] Eine mögliche Lösung ist die Verwendung von optischen Write-Once-, Read-Many („WORM")-Datenträgern, um digitale Abbildungen zu speichern. Ein Vorteil der WORM-Datenträgerspeicherung ist, dass die darauf enthaltenen Daten unveränderbar sind, da auf diese Datenträger nur einmal Daten geschrieben werden können. Diese Technik hat jedoch auch mehrere Nachteile. Beispielsweise können auf WORM-Datenträgern aufgezeichnete Daten von dem WORM-Datenträger der ursprünglichen Aufzeichnung auf wiederbeschreibbare Datenträger kopiert werden, geändert und dann auf neuen WORM-Datenträgern aufgezeichnet werden, ohne dass dieser Vorgang zurückverfolgt werden kann.

[0007] Außerdem können das Datum und die Uhrzeit der Datenaufzeichnung nicht mit Sicherheit bestimmt werden, und es kann nicht bestimmt werden, ob die Daten mit einem „Original" übereinstimmen, obwohl mit großer Sicherheit gesagt werden kann, dass Daten auf einem bestimmten WORM-Datenträger seit der Aufzeichnung auf diesem Datenträger nicht verändert wurden.

[0008] Ein bekannter Fortschritt in der Dateiüberprüfungstechnologie ist die Registrierung einer „elektronischen Signatur" einer digitalen Datei (Abbildung, Textverarbeitungsdokument, Audio- oder Videoclip usw.). Sie erlaubt einem Benutzer, eine Datei lokal auszuwählen und ein Programm lokal auszuführen, das von einem Dienstanbieter bereitgestellt wurde, um eine „elektronische Signatur" der digitalen Datei zu erstellen, die nur auf dem Dateiinhalt basiert.

[0009] Die Signatur wird zusammen mit einem vom Benutzer gewählten Dateinamen und ausgewählten Schlüsselwörtern auf die Seite des Anbieters hochgeladen und in einer Registrierungsdatenbank gespeichert, die vom Dienstanbieter unter einem Konto für den entsprechenden Benutzer verwaltet wird. Ein bestimmter Anbieter generiert ein „Registrierungszertifikat", in dem u.a. die Signatur angezeigt wird.

[0010] Die Überprüfung des Inhalts und des Vorlagedatums der digitalen Datei zu einem späteren Zeitpunkt erfordert den Online-Zugriff auf die Internetseite des Anbieters und den Abruf der vorherigen Registrierungsaufzeichnung durch den Dateinamen oder durch Schlüsselwörter. Die abgerufene Datenbankaufzeichnung zeigt die Dateisignatur und das ursprüngliche Datum an, an dem die Dateisignatur registriert wurde. Zur Vervollständigung der Überprüfung muss der Benutzer das elektronische Signaturprogramm in der zu überprüfenden Datei ausführen (erneut lokal) und die regenerierte Signatur mit der abgerufenen registrierten Signatur vergleichen, um zu bestimmen, ob die Signatur der fraglichen digitalen Datei mit der der ursprünglich registrierten Datei übereinstimmt.

[0011] Der Verwender hat nun die Bestätigung, dass die Signatur seiner Datei mit der Signatur einer Datei übereinstimmt, die zum angegebenen Zeitpunkt registriert wurde. EP-A-0516898 enthält einen elektronischen Notar, der überprüft, ob eine digitale Datei seit einem angegebenen Zeitpunkt verändert wurde.

ZUSAMMENFASSUNG UND ZWECK DER ERFINDUNG

[0012] Die vorangegangenen sowie andere Probleme und Defizite der Abbildungsauthentifizierung bei bekannten digitalen Abbildungssystemen werden gelöst und durch die vorliegende Erfindung wird durch sichere Abbildungskennzeichnung ein technischer Fortschritt bei der Bereitstellung digitaler Dateiauthentifizierung erzielt.

[0013] In vielerlei Hinsicht ist der Zweck der vorliegenden Erfindung, ein System und eine Methode zur digitalen Dateiverwaltung bereitzustellen, indem sie eine digitale Dateiauthentifizierung durch sichere Dateikennzeichnung ermöglicht.

[0014] Ein digitales Dateiverwaltungssystem in einer Ausführungsform wie der vorliegenden Erfindung beinhaltet Mittel für die Eingabe einer digitalen Datei und eine sichere Datums- und Uhrzeitreferenz, die Datums- und Uhrzeitinformationen enthält. Es wird ein Datums-/Uhrzeitwert generiert, der durch die Implementierung eines CRC-Algorithmus aus den sicheren Datums- und Uhrzeitinformationen abgeleitet wird. Aus der digitalen Datei selbst wird ein Abbildungswert ermittelt. Die digitale Datei wird mit den Datums- und Uhrzeitinformationen, dem Wert für Datum und Uhrzeit und dem Abbildungswert gekennzeichnet. Die gekennzeichnete digitale Datei wird anschließend gespeichert.

[0015] Alternative Ausführungsformen können Funktionen beinhalten wie das Generieren eines Datums- und Uhrzeitwerts und eines Abbildungswerts durch einen zyklischen Redundanzcode-Algorithmus, sowie das Transformieren des Datums- und Uhrzeitwertes und des Abbildungswertes durch eine mathematische Umformung und das Kennzeichnen der digitalen Datei mit den transformierten Werten.

[0016] In anderen Ausführungsformen ist die sichere Datums- und Uhrzeitreferenz eine lokale sichere Uhr.

[0017] In verschiedenen Ausführungen kann die digitale Datei aus einer Bilddatei, einer Textdatei oder aus jedem anderen Dateiformat bestehen.

[0018] Alternative Ausführungen der Erfindung ermöglichen die Eingabe einer digitalen Abbildung durch einen optischen Scanner zum Scannen einer Originalabbildung in eine digitale Abbildung oder direkt von Digitalkameras oder medizinischen Abbildungsgeräten. Die gekennzeichnete digitale Datei kann auch in optischen Speichern gespeichert werden.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0019] Die vorangegangenen und andere Funktionen und Vorteile der vorliegenden Erfindung werden anschaulicher mit Hilfe der folgenden detaillierten Beschreibung von exemplarischen Ausführungsformen dieser Erfindung, wie in den beiliegenden Zeichnungen illustriert, wobei

[0020] Fig. 1 eine Systemimplementierung der DocSTAR-Ausführung der vorliegenden Erfindung illustriert,

[0021] Fig. 2 ein Ablaufdiagramm der Dateikennzeichnung gemäß einer Ausführung der vorliegenden Erfindung darstellt,

[0022] Fig. 3 ein Ablaufdiagramm der Überprüfung der CRCs einer gespeicherten gekennzeichneten Abbildung gemäß einer Ausführung der vorliegenden Erfindung darstellt,

[0023] Fig. 4 ein Ablaufdiagramm der Einstellung der sicheren Uhr einer Ausführung der vorliegenden Erfindung darstellt,

[0024] Fig. 5 ein Ablaufdiagramm der Berechnung des Abbildungs-CRCs für Abbildungen im TIFF-Format gemäß einer Ausführung der vorliegenden Erfindung darstellt,

[0025] Fig. 6 ein Ablaufdiagramm der Berechnung des Datums-CRCs für Abbildungen im TIFF-Format gemäß einer Ausführung der vorliegenden Erfindung darstellt,

[0026] Fig. 7 ein Ablaufdiagramm der Berechnung des Abbildungs-CRCs für Abbildungen im JPEG-Format gemäß einer Ausführung der vorliegenden Erfindung darstellt, und

[0027] Fig. 8 ein Ablaufdiagramm der Berechnung des Datums-CRCs für Abbildungen im JPEG-Format gemäß einer Ausführung der vorliegenden Erfindung darstellt.

DETAILLIERTE BESCHREIBUNG DER ZEICHNUNGEN

[0028] Die folgende Beschreibung der vorliegenden Erfindung verwendet für illustrative Zwecke das Abbildungsauthentifizierungssystem Authentidate™, das im fertigen Dokumentverwaltungs- und Abbildungssystem DocSTAR™ enthalten ist, und von denen beide bei BitWiseDesigns, Inc., dem Zessionar für die vorliegende Erfindung, erhältlich sind. Während die DocSTAR-Ausführung der vorliegenden Erfindung auf die Speicherung, Kennzeichnung und Authentifizierung von Originalpapierdokumenten ausgerichtet ist, kann jede digitale Datei durch die Methode und das System der vorliegenden Erfindung wie beschrieben verarbeitet werden. Die folgende Erörterung mit Referenzen zur DocSTAR-Ausführung soll nicht beschränkend sein und sie dient illustrativen Zwecken hinsichtlich der Erklärungs- und Verständniserleichterung der vorliegenden Erfindung.

[0029] Fig. 1 illustriert eine exemplarische Ausführung der Implementierung des DocSTAR Dokumentverwaltungs- und Abbildungssystems der vorliegenden Erfindung.

[0030] Es wird ein DocSTAR-Systemhost **100** in Kommunikation mit einem Eingabegerät **110**, einem Speichergerät **120** und einer sicheren Uhrzeit- und Datumsreferenz **130** konfiguriert.

[0031] In dieser Ausführung wird der Systemhost **100** als IBM-PC oder IBM-Workstation implementiert, das Eingabegerät **110** ist ein optischer Scanner, das Speichergerät **120** ist ein optisches Speichergerät, und die sichere Uhrzeit- und Datumsreferenz **130** wird durch einen Hardwareschlüssel, der eine sichere Uhr beinhaltet, bereitgestellt.

[0032] Durch den optischen Scanner **110** werden Originalabbildungen gescannt. Die daraus resultierende digitale Abbildung wird vom Systemhost **100** gemäß der Methode der vorliegenden Erfindung verarbeitet, die im Folgenden noch näher beschrieben wird. Die Abbildung wird dann auf dem optischen Speichergerät **120** gespeichert und kann von dort zu einem späteren Zeitpunkt abgerufen werden.

[0033] Das Abbildungsauthentifizierungssystem der vorliegenden Erfindung arbeitet einmal auf die Art und Weise, dass zusätzliche unabhängige Daten mit jeder gespeicherten digitalen Datei aufgezeichnet werden. Diese zusätzlichen Daten beinhalten: Ein „echtes Datum", das von der sicheren Uhr (im Folgenden detailliert beschrieben) abgelesen wird, die nicht vom Benutzer einstellbar ist (Authentidate™), und eine Nummer, die aus einem zyklischen Redundanzcode-Algorithmus (CRC) der Abbildungsdaten abgeleitet ist (im Folgenden detaillierter beschrieben) und „Abbildungs-CRC" genannt wird, und ein CRC, der vom „echten Datum" abgeleitet wird und „Datums-CRC" genannt wird.

[0034] Diese zusätzlichen Daten werden innerhalb jeder digitalen Datei so bald wie möglich aufgezeichnet, nachdem das System die Abbildung erhalten hat (z.B. vom Scanner **110** in der DocSTAR-Ausführung). Wie im Folgenden noch detaillierter beschrieben wird, stimmt die erneute Berechnung des Abbildungs-CRC in der veränderten Abbildung nicht mit dem ursprünglichen, in diesem aufgezeichneten Abbildungs-CRC überein, wenn die Abbildung nach der Aufzeichnung von zusätzlichen Daten verändert wird.

[0035] Auf diese Weise kann eine Veränderung oder eine andere Gefährdung der Abbildung erkannt werden. Eine erneute Berechnung des Datums-CRC deckt die Veränderung von echten Daten ebenfalls auf die gleiche Weise auf.

[0036] Der Abbildungs-CRC und der Datums-CRC können jederzeit überprüft werden. Wenn der neu berechnete Wert und der aufgezeichnete Wert übereinstimmen, kann mit äußerster Sicherheit bestätigt werden, dass die gerade aufgezeichnete Abbildung an dem angegebenen Datum aufgezeichnet wurde und seitdem nicht auf irgendeine Art und Weise verändert wurde. Kein anderes bekanntes System, einschließlich der Papierablage, kann eine ähnliche Sicherheit bezüglich des Erstellungsdatums oder der Echtheit eines Dokuments bieten.

[0037] Mit Bezug auf Fig. 2 wird nun die Funktionsweise der vorliegenden Erfindung beschrieben.

[0038] Zuerst werden digitale Daten angefordert (entweder aus dem Speicher abgerufen oder vom Eingabegerät **110** erhalten) (Schritt **200**). Informationen zu Datum und Uhrzeit werden von der sicheren Uhr **130** erhalten (Schritt **202**). Die richtige Funktionsweise der sicheren Uhr wird bewertet. (Schritt **204**) Wenn die sichere Uhr funktioniert, werden die Daten zu Datum und Uhrzeit als von der Uhr abgelesen akzeptiert (in Schritt **202**). Wird ein Fehler der sicheren Uhr erkannt, wird eine Fehlermeldung zurückgegeben und die Abbildungsverarbeitung wird angehalten (Schritt **206**). Wenn die Uhr als funktionsfähig eingestuft wurde (in Schritt **204**), werden der digitalen Datei spezielle Tags (diese werden später weiter erläutert) und die Authentidate-Informationen (einschließlich Datum und Uhrzeit) hinzugefügt, und die CRC-Datenfelder werden auf 0 gesetzt (d.h. die Datenfelder werden mit Nullen ausgefüllt) (Schritt **208**).

[0039] Zwei errechnete Werte, die aus dem Abbildungsinhalt bzw. den Authentidate-Informationen abgeleitet werden, werden dann berechnet. Die errechneten Werte können auf jegliche Art und Weise berechnet werden, basierend auf Daten, die in der digitalen Datei enthalten sind, was die Erkennung von Datenverfälschungen ermöglicht, wie zum Beispiel einer Standardprüfsumme. In dieser Ausführung der vorliegenden Erfindung werden zyklische Redundanzcodes („CRC"), im Wesentlichen eine komplexere Prüfsummenberechnung, zur Ableitung der errechneten Werte verwendet. Jedoch ist auch jede andere Berechnungsmethode akzeptabel, die eine Zahl erzeugt, die von den Inhaltsdaten des Dokuments abgeleitet ist und die zur Erkennung von Datenverfälschungen geeignet ist.

[0040] In dieser Ausführung werden die errechneten Werte von einem bekannten CRC-Algorithmus generiert (der im Folgenden detailliert beschrieben wird), der sowohl auf dem Abbildungsinhalt als auch auf dem Authentidate ausgeführt wird und der einen Abbildungs-CRC bzw. einen Authentidate-CRC erstellt (Schritte **210**, **212**). Der Abbildungs-CRC und der Authentidate-CRC werden durch eine proprietäre mathematische Umformung für zusätzliche Sicherheit „transformiert" (wie im Folgenden noch näher beschrieben wird) und es wird ein Abbildungs-CRC' sowie ein Authentidate-CRC' erstellt (Schritt **214**).

[0041] Die Abbildungsdatei wird dann mit dem Abbildungs-CRC' und dem Authentidate-CRC' gekennzeichnet (Schritt **216**). Die gekennzeichneten digitalen Dateien werden vom optischen Speichergerät **120** auf einem optischen Medium gespeichert (Schritt **218**).

[0042] Die Echtheit der Abbildung und die Datums- bzw. Uhrzeitmarken können dann anschließend bestimmt werden, indem die in den digitalen Dateien gespeicherten errechneten Werte geprüft werden, wie in Fig. 3 gezeigt wird. Fig. 3 stellt ein exemplarisches Ablaufdiagramm dar, in dem eine Ausführung zur Überprüfung von CRCs in einer Abbildungsdatei beschrieben wird.

[0043] Der erste Schritt bei der Überprüfung von CRCs in einer digitalen Datei besteht darin, die speziellen Tag- und Datumsbereiche auszulesen und die gespeicherten Werte des Abbildungs-CRC bzw. des Datums-CRC abzurufen (Schritt **300**).

[0044] Wenn die CRC-Werte in der digitalen Datei nicht lokalisiert oder gelesen werden können (Schritt **302**), wurde die Abbildung entweder nicht korrekt gespeichert oder die Abbildung wurde verändert oder anderweitig verfälscht und es wird eine Fehlermeldung ausgegeben (Schritt **304**).

[0045] Wenn die speziellen Tags gefunden werden, werden die CRCs erneut für die digitale Datei und die Datumszeichenfolge berechnet (Schritt **306**).

[0046] Dieselben Algorithmen, die anfangs für die Berechnung der CRCs verwendet wurden, werden an dieser Stelle zu ihrer Regenerierung verwendet. Der neu errechnete Abbildungs-CRC wird transformiert und mit dem Abbildungs-CRC aus dem Tag verglichen (Schritt **308**). (Alternativ kann der gespeicherte Abbildungs-CRC vor dem Vergleich mit dem neu errechneten Wert rückwärts transformiert werden.) Wenn der neu errechnete CRC der digitalen Datei nicht mit dem im speziellen Tag gespeicherten Wert übereinstimmt, wird die Abbildung als geändert oder anderweitig verfälscht erkannt und es wird eine Fehlermeldung ausgegeben

(Schritt **310**). Wenn die gespeicherten und neu errechneten Abbildungs-CRCs positiv übereinstimmen, werden die Datums-CRCs getestet. Der neu errechnete Datums-CRC wird transformiert und mit dem aus dem Tag gelesenen Datums-CRC verglichen (Schritt **312**). (Alternativ kann der gespeicherte Datums-CRC vor dem Vergleich mit dem neu errechneten Wert rückwärts transformiert werden.) Wenn der neu errechnete Datums-CRC nicht mit dem gespeicherten Wert im speziellen Tag übereinstimmt, wird die Datumszeichenfolge als geändert oder auf sonstige Weise verfälscht erkannt und es wird eine Fehlermeldung ausgegeben (Schritt **314**). Wenn die Datums-CRCs übereinstimmen und an dieser Stelle beide Abbildungs-CRCs und Datums-CRCs positiv übereinstimmen, wird die digitale Datei als nicht geändert erkannt und somit authentifiziert (Schritt **316**).

[0047] Aus der vorangegangenen Beschreibung wird deutlich, dass die Verwendung einer sicheren, nicht verfälschbaren Uhr wesentlich für die vorliegende Erfindung ist. Sie dient als eine sichere Quelle für Datum und Uhrzeit, die nicht durch den Benutzer geändert werden kann. Mit Hilfe einer Batteriesicherung behält die sichere Uhr die Uhrzeit und das Datum auch dann bei, wenn der Computer ausgeschaltet wird.

[0048] Es kann entweder eine anwendungsspezifische Hardware oder ein kommerziell verfügbares Produkt verwendet werden, das eine sichere Uhr enthält. In beiden Fällen muss ein Mechanismus installiert sein, um betrügerische oder willkürliche Datums- und Uhrzeitanpassungen zu vermeiden.

[0049] In der DocSTAR-Ausführung wird ein kommerziell verfügbares Produkt verwendet, das eine sichere Uhr mit einem physischen Hardwareschlüssel verbindet (oft „Dongle" genannt). Der Hardwareschlüssel verbindet sich mit dem Parallelport des Computers und auf diesen kann mittels einer Anwendungsschnittstelle (API), die vom Hersteller bereitgestellt wird, zugegriffen werden.

[0050] Der zur Verwendung in der DocSTAR-Ausführung der vorliegenden Erfindung ausgewählte Hardwareschlüssel ist TIMEHASP-4 von Aladdin Knowledge Systems, LTD. Die Sicherheit des Hardwareschlüssels wird gewährleistet durch einen kundenspezifischen ASIC-Chip (Application Specific Integrated Circuit), einen einzigartigen Satz von Kennwörtern, die nur vom Systemanbieter (beispielsweise BitWise Designs, Inc., dem Zessionar dieses Patents und einem „Anbieter" des DocSTAR-Systems) benutzt werden sowie erweiterten Schutzalgorithmen und Fehlerbehebungtechnologien auf der Programmschnittstelle des Herstellers und Gerätetreibern. Dies bietet einen hohen Grad an Sicherheit für die sichere Uhr.

[0051] Die aktuelle Zeit und das aktuelle Datum werden während der Montage des DocSTAR-Host-Computers innerhalb des Hardwareschlüssels in die sichere Uhr werksprogrammiert. Obwohl auch jede andere Zeiteinstellung verwendet werden kann, wird die sichere Uhr in dieser Ausführung auf Greenwich Mean Time (GMT) eingestellt, womit vermieden wird, dass die Uhr auf verschiedene lokale Zeitzonen oder auf Sommerzeit umgestellt werden muss.

[0052] Es kann ein Mechanismus eingebaut werden, um Anpassungen der Uhr vorzunehmen bzw. die Uhr zurückzustellen, oder um kleine Ungenauigkeiten der Uhr zu korrigieren, die nach einiger Zeit auftreten können. Beispielsweise können das Datum und die Uhrzeit in der sicheren Uhr (wie in **Fig. 4** an einer Ausführung dargestellt) mittels eines speziellen Verwaltungsprogramms, das sich auf dem System eines Benutzers befindet, geändert werden. Jedoch erlaubt dieses Programm nur Änderungen des sicheren Datums und der sicheren Zeit, wenn der Benutzer einen korrekten Authentifizierungscode vom Systemanbieter (z.B. der Abteilung für technische Unterstützung von BitWise Designs, Inc., dem Zessionar dieses Patents) eingibt. Der Authentifizierungscode ändert nur das Datum und die Uhrzeit der sicheren Uhr von ihren aktuellen Werten auf die aktuelle GMT, die vom Systemanbieter verwaltet wird. Dies verhindert, dass der Benutzer die sichere Uhr willkürlich ändert und somit Abbildungen mit einer falschen und betrügerischen Uhrzeit und einem falschen Datum versehen kann.

[0053] Bei dieser Ausführung ist ein Authentifizierungscode erforderlich, um die sichere Uhr zu ändern. Um diesen Code zu erhalten, gibt ein Hilfstechniker auf dem System des Systemanbieters die Seriennummer des Hardwareschlüssels und das aktuelle Datum der sicheren Uhr in ein gesichertes, kundenspezifisches Programm ein (das „Eagle Call Tracking System"), das von BitWise Designs, Inc. verwaltet wird (Schritt **400**). Dieses Programm generiert einen Authentifizierungscode (Schritt **402**). Mit diesem Authentifizierungscode kann der Techniker oder Benutzer in der sicheren Uhr nur das Datum und die Uhrzeit ändern, die bei BitWise Designs, Inc. erstellt und verwaltet werden.

[0054] Der Authentifizierungscode in dieser Ausführung wird durch einen mathematischen Algorithmus festgelegt, der nur einen einzigen Code ergibt, wenn das aktuelle Datum der sicheren Uhr, die Seriennummer des Hardwareschlüssels und die gewünschten Änderungen von Datum und Uhrzeit eingegeben werden. Dieser

Authentifizierungscode ist in der Hinsicht von beschränkter Gültigkeit, dass er nicht an einem anderen Tag dazu funktioniert, das Datum und die Uhrzeit auf das Datum und die Uhrzeit zu ändern, die am Tag der Authentifizierung vergeben wurden.

[0055] Der Code wird beim Benutzer eingegeben (Schritt **404**). Die gewünschte Uhreinstellung wird beim Benutzer eingegeben (Schritt **406**). Das Verwaltungsprogramm auf dem Client-System bietet ein kleines Zeitfenster (**20** Sekunden), in dem jede eingegebene Zeit mit dem Authentifizierungscode übereinstimmt. Authentifizierungscodes werden intern für eine Zeit von 5 Minuten vor und 15 Minuten nach den angegebenen Uhrzeitänderungen errechnet. Wenn der gegebene Authentifizierungscode mit einem der Codes innerhalb des Zeiffensters übereinstimmt, wird der Authentifizierungscode als korrekt eingestuft und implementiert. So kann ein Bereichstechniker mehrere Minuten Verzögerung berücksichtigen, während der Authentifizierungscode übermittelt wird.

[0056] So wird die gewünschte Einstellung gegen den Authentifizierungscode geprüft, um zu bestimmen, ob der Code die gewünschten Änderungen von Datum und Uhrzeit authentifiziert (Schritt **408**). Wenn eine Ungültigkeit festgestellt wird, wird eine Fehlermeldung zurückgegeben und die Uhr wird nicht aktualisiert (Schritt **409**). Bei einer gültigen Anfrage erscheinen die aktuellen Änderungen der sicheren Uhr nicht, bis der Befehl „Uhr aktualisieren" auf der Benutzerseite eingegeben wird (Schritt **410**). So kann ein Bereichstechniker die Bereichsuhr genau mit der von BitWise Designs, Inc. verwalteten Uhr synchronisieren. Nachdem der Befehl „Uhr aktualisieren" ausgeführt wurde, wird der Authentifizierungscode erneut gegen die Informationen der Uhr geprüft, um sicherzustellen, dass er noch gültig ist (Schritt **412**). Wenn eine Ungültigkeit festgestellt wird, wird eine Fehlermeldung zurückgegeben, und die Uhr wird nicht aktualisiert (Schritt **413**). Die Uhr wird aktualisiert (Schritt **414**).

[0057] Alternativ können sichere Uhren vom Dienstanbieter in dessen Einrichtung (z.B. BitWise Designs, Inc.) neu programmiert werden, indem der Hardwareschlüssel direkt an ein ausgewiesenes Eagle System von BitWise Designs, Inc. angehängt wird und indem der Befehl zur Aktualisierung der sicheren Uhr eingegeben wird. Die Seriennummer des Hardwareschlüssels wird überprüft, und das Datum bzw. die Uhrzeit der sicheren Uhr werden auf GMT, die von BitWise Designs, Inc. verwaltet wird, aktualisiert.

[0058] Bei weiteren alternativen Ausführungen können Anpassungen der Uhr bei Ungenauigkeiten oder Einstellungen der Uhr als ein automatischer Vorgang implementiert werden, bei dem ein Benutzer eine Aktualisierung der Uhr von einer rechnerfernen Uhr auslösen kann. Jedoch kann hier der Benutzer nicht selbst die Uhr einstellen.

[0059] Die manuelle oder die automatische Methode zur Einstellung und Aktualisierung der Uhr, die oben beschrieben wurden, bewahren den Benutzer vor der willkürlichen oder betrügerischen Änderung der sicheren Uhr und verhindern somit, dass Abbildungen mit einer falschen Uhrzeit bzw. einem falschen Datum versehen werden.

[0060] Wie es bei aktuell erhältlichen Technologien zu erwarten ist, versagen die Batterien jeder Uhr irgendwann oder die Uhr kann mit der Zeit andere Schäden aufweisen. Diese Bedingungen werden vor der Verarbeitung der Abbildungen von Software getestet, um sicherzustellen, dass ungültige Daten, resultierend aus einer defekten Uhr (oder leeren Batterie), nicht in Abbildungen gespeichert werden und somit die Verlässlichkeit der Abbildungskennzeichnung nicht gefährdet wird. Im Falle eines Defektes der Uhr wird das Ablegen von Abbildungen deaktiviert, bis die Uhr repariert oder ersetzt wurde.

[0061] Die oben erwähnten, errechneten Werte mit Bezug zu Fig. 2 in der DocSTAR-Ausführung der vorliegenden Erfindung sind zyklische Redundanzcodes (CRCs). Der CRC ist ein 32-Bit großer, ganzzahliger Wert, der das Ergebnis der Durchführung des bekannten CRC-32-Algorithmus auf einem Datenblock darstellt. Der CRC-32-Algorithmus ist ein allgemeiner, gemeinfreier Algorithmus zur Erkennung von sogar winzigen Datenänderungen bei einer Reihe von Anwendungen. CRCs werden beispielsweise im Kommunikationsbereich verwendet, um zu überprüfen, ob Daten korrekt über Leitungen von unbekannter Qualität übermittelt wurden. Sie werden auch verwendet, um Verfälschungen komprimierter Daten zu erkennen, wie zum Beispiel bei der bekannten PKZIP-Anwendung. Eine der Stärken der CRCs besteht darin Datenveränderungen zu entdecken, die sonst unentdeckt bleiben würden. Wenn beispielsweise Bitfehler in einem gegebenen Datenblock erscheinen, ihre Summe jedoch zufällig die gleiche ist wie die der ursprünglichen Daten, bleibt dieser Fehler möglicherweise unentdeckt, wenn eine Standardprüfsumme verwendet wird. Der CRC-32-Algorithmus erkennt diese Art von Fehler, da der Ergebniscode nicht einfach eine Summe der zugehörigen Daten wie bei einer Standardprüfsumme ist.

[0062] An dieser Stelle wird keine technische Diskussion eines CRC-32-Algorithmus dargestellt. Es gibt viele Quellen von CRC-32-Algorithmen und Quellcodes in der Public Domain. Ein beispielhafter C++-Quellcode für einen CRC-32-Algorithmus, der in die DocSTAR-Ausführung der vorliegenden Erfindung implementiert wird, wird unten beschrieben. Wie zuvor beschrieben, ist die Verwendung des CRC für die vorliegende Erfindung nicht per se erforderlich und jede Berechnungsmethode ist akzeptabel, die von den Abbildungsdaten abgeleitet ist und für die Erkennung von Datenverfälschungen geeignet ist. Der exemplarische C++-Quellcode wird im Folgenden dargestellt:

```
long CRCTable[] =
    {
     0x00000000L,  0x77073096L,  0x0EE0E612CL,  0x990951BAL,
     0x076DC419L,  0x706AF48FL,  0x0E963A535L,  0x9E6495A3L,
     0x0EDB8832L,  0x79DCB8A4L,  0x0E0D5E91EL,  0x97D2D988L,
     0x09B64C2BL,  0x7EB17CBDL,  0x0E7B82D07L,  0x90BF1D91L,
     0x1DB71064L,  0x6AB020F2L,  0x0F3B97148L,  0x84BE41DEL,
     0x1ADAD47DL,  0x6DDDE4EBL,  0x0F4D4B551L,  0x83D385C7L,
     0x136C9856L,  0x646BA8C0L,  0x0FD62F97AL,  0x8A65C9ECL,
     0x14015C4FL,  0x63066CD9L,  0x0FA0F3D63L,  0x8D080DF5L,
     0x3B6E20C8L,  0x4C69105EL,  0x0D56041E4L,  0x0A2677172L,
     0x3C03E4D1L,  0x4B04D447L,  0x0D20D85FDL,  0x0A50AB56BL,
     0x35B5A8FAL,  0x42B2986CL,  0x0DBBBC9D6L,  0x0ACBCF940L,
     0x32D86CE3L,  0x45DF5C75L,  0x0DCD60DCFL,  0x0ABD13D59L,
     0x26D930ACL,  0x51DE003AL,  0x0C8D75180L,  0x0BFD06116L,
     0x21B4F4B5L,  0x56B3C423L,  0x0CFBA9599L,  0x0B8BDA50FL,
     0x2802B89EL,  0x5F058808L,  0x0C60CD9B2L,  0x0B10BE924L,
     0x2F6F7C87L,  0x58684C11L,  0x0C1611DABL,  0x0B6662D3DL,

     0x76DC4190L,  0x01DB7106L,  0x98D220BCL,  0x0EFD5102AL,
     0x71B18589L,  0x06B6B51FL,  0x9FBFE4A5L,  0x0E8B8D433L,
     0x7807C9A2L,  0x0F00F934L,  0x9609A88EL,  0x0E10E9818L,
     0x7F6A0DBBL,  0x086D3D2DL,  0x91646C97L,  0x0E6635C01L,
     0x6B6B51F4L,  0x1C6C6162L,  0x856530D8L,  0x0F262004EL,
     0x6C0695EDL,  0x1B01A57BL,  0x8208F4C1L,  0x0F50FC457L,
     0x65B0D9C6L,  0x12B7E950L,  0x8BBEB8EAL,  0x0FCB9887CL,
     0x62DD1DDFL,  0x15DA2D49L,  0x8CD37CF3L,  0x0FBD44C65L,
```

```
0x4DB26158L,  0x3AB551CEL,  0x0A3BC0074L,  0x0D4BB30E2L,
0x4ADFA541L,  0x3DD895D7L,  0x0A4D1C46DL,  0x0D3D6F4FBL,
0x4369E96AL,  0x346ED9FCL,  0x0AD678846L,  0x0DA60B8D0L,
0x44042D73L,  0x33031DE5L,  0x0AA0A4C5FL,  0x0DD0D7CC9L,
0x5005713CL,  0x270241AAL,  0x0BE0B1010L,  0x0C90C2086L,
0x5768B525L,  0x206F85B3L,  0x0B966D409L,  0x0CE61E49FL,
0x5EDEF90EL,  0x29D9C998L,  0x0B0D09822L,  0x0C7D7A8B4L,
0x59B33D17L,  0x2EB40D81L,  0x0B7BD5C3BL,  0x0C0BA6CADL,

0x0EDB88320L,  0x9ABFB3B6L,  0x03B6E20CL,  0x74B1D29AL,
0x0EAD54739L,  0x9DD277AFL,  0x04DB2615L,  0x73DC1683L,
0x0E3630B12L,  0x94643B84L,  0x0D6D6A3EL   0x7A6A5AA8L,
0x0E40ECF0BL,  0x9309FF9DL,  0x0A00AE27L,  0x7D079EB1L,
0x0F00F9344L,  0x8708A3D2L,  0x1E01F268L,  0x6906C2FEL,
0x0F762575DL,  0x806567CBL,  0x196C3671L,  0x6E6B06E7L,
0x0FED41B76L,  0x89D32BE0L,  0x10DA7A5AL,  0x67DD4ACCL,
0x0F9B9DF6FL,  0x8EBEEFF9L,  0x17B7BE43L,  0x60B08ED5L,
0x0D6D6A3E8L,  0x0A1D1937EL,  0x38D8C2C4L,  0x4FDFF252L,
0x0D1BB67F1L,  0x0A6BC5767L,  0x3FB506DDL,  0x48B2364BL,
0x0D80D2BDAL,  0x0AF0A1B4CL,  0x36034AF6L,  0x41047A60L,
0x0DF60EFC3L,  0x0A867DF55L,  0x316E8EEFL,  0x4669BE79L,
0x0CB61B38CL,  0x0BC66831AL,  0x256FD2A0L,  0x5268E236L,
0x0CC0C7795L,  0x0BB0B4703L,  0x220216B9L,  0x5505262FL,
0x0C5BA3BBEL,  0x0B2BD0B28L,  0x2BB45A92L,  0x5CB36A04L,
0x0C2D7FFA7L,  0x0B5D0CF31L,  0x2CD99E8BL,  0x5BDEAE1DL,

0x9B64C2B0L,  0x0EC63F226L,  0x756AA39CL,  0x026D930AL,
0x9C0906A9L,  0x0EB0E363FL,  0x72076785L,  0x05005713L,
0x95BF4A82L,  0x0E2B87A14L,  0x7BB12BAEL,  0x0CB61B38L,
0x92D28E9BL,  0x0E5D5BE0DL,  0x7CDCEFB7L   0x0BDBDF21L,
0x86D3D2D4L,  0x0F1D4E242L,  0x68DDB3F8L,  0x1FDA836EL,
0x81BE16CDL,  0x0F6B9265BL,  0x6FB077E1L,  0x18B74777L,
0x88085AE6L,  0x0FF0F6A70L,  0x66063BCAL,  0x11010B5CL,
0x8F659EFFL,  0x0F862AE69L,  0x616BFFD3L,  0x166CCF45L,
0x0A00AE278L,  0x0D70DD2EEL,  0x4E048354L,  0x3903B3C2L,
0x0A7672661L,  0x0D06016F7L,  0x4969474DL,  0x3E6E77DBL,
0x0AED16A4AL,  0x0D9D65ADCL,  0x40DF0B66L,  0x37D83BF0L,
0x0A9BCAE53L,  0x0DEBB9EC5L,  0x47B2CF7FL,  0x30B5FFE9L,
0x0BDBDF21CL,  0x0CABAC28AL,  0x53B39330L,  0x24B4A3A6L,
0x0BAD03605L,  0x0CDD70693L,  0x54DE5729L,  0x23D967BFL,
0x0B3667A2EL,  0x0C4614AB8L,  0x5D681B02L,  0x2A6F2B94L,
0x0B40BBE37L,  0x0C30C8EA1L,  0x5A05DF1BL,  0x2D02EF8DL

};

UINT32 CRCFileBlock(UINT16 hFile, UINT32 lOffset, UINT32 lLength, UINT32 lSeed)
{

    //CRC auf Dateiblock mit gegebenem Saatwert berechnen
```

```
        //0xFFFFFFFFL für ersten Saatwert verwenden
//gibt 0 bei Erfolg zurück, gibt 1Seed bei Fehler zurück

        int ret;
        char buffer[COPYBUFFERLEN];
        UINT32 lRemainLength;
        UINT16 uBlockSize;
        UINT32 lSourceOff;
        UINT32 lCRC;
        UINT16 i, index;

        lCRC = lSeed;

        if(lLength > COPYBUFFERLEN)
                uBlockSize = COPYBUFFERLEN;
        else
                uBlockSize = (UINT16)lLength;

        lRemainLength = lLength;
        lSourceOff = lOffset;

        while(lRemainLength) {
                ret = ReadFileBlock(buffer, hFile, lSourceOff, uBlockSize);
                if(ret)
                        return lSeed;

                for (i=0; i<uBlockSize; i++) {
                        index = (UINT16)(lCRC ^ buffer[i]) & (UINT16)0x000000FFL;
                        lCRC = ((lCRC >> 8) & 0x00FFFFFFL) ^ CRCTable[index];
                }
                lCRC = ~lCRC;

                lRemainLength -= uBlockSize;
                lSourceOff += uBlockSize;
                if(lRemainLength < uBlockSize)
                        uBlockSize = (UINT16)lRemainLength;
        }

        return lCRC;
}

UINT32 CRCBlock(char* buffer, UINT16 nLength, UINT32 lSeed)
{


        //CRC auf Dateiblock mit angegebenem Saatwert berechnen
        //0xFFFFFFFFL für ersten Saatwert verwenden
        //gibt 0 bei Erfolg zurück, gibt 1Seed bei Fehler zurück (ignoriert Fehler)
```

```
    UINT32 lCRC;
    UINT16 i, index;

    lCRC = lSeed;

    for (i=0; i<nLength; i++) {
        index = (UINT16)(lCRC ^ buffer[i]) & (UINT16)0x000000FFL;

        lCRC = ((lCRC >> 8) & 0x00FFFFFFL) ^ CRCTable[index];
    }
    lCRC = ~lCRC;
    return lCRC;
}
```

C++-Quellcodebeispiel zum Errechnen des CRC-32

[0063] Während bereits ein CRC-Wert allein verwendet werden kann, kann bei der vorliegenden Erfindung ein höheres Maß an Sicherheit erreicht werden, um die Echtheit einer Abbildung sicherzustellen. Dies geschieht durch das Hinzufügen einer mathematischen Umformung zum CRC-Wert. Wie schon gezeigt, befindet sich ein typischer Algorithmus zur Berechnung des CRC-32 in der Public Domain und ist daher leicht zugänglich. Aufgrund dieser Tatsache und im Zusammenhang mit den hier aufgeführten Details könnte jeder den CRC auf einer geänderten Abbildung errechnen, somit ein „Authentidate" fälschen und fälschlicherweise die Abbildung als echt und unverändert bestätigen. Bei der vorliegenden Erfindung wird der echte errechnete Abbildungs- oder Datums-CRC vor der Abbildungskennzeichnung mathematisch zu einem neuen Wert umgeformt. Die funktionalen Voraussetzungen für die Umformung sind, dass der Ergebniswert für jeden Eingabewert konsistent ist, und dass der Ergebniswert für jeden einzigartigen Eingabewert einzigartig ist. Die Umformung könnte beispielsweise in Form einer Permutation der Bitwerte der Eingabe, eines exklusiven ODER des Eingabewertes mit einer konsistenten, vorgegebenen „magischen" Zahl oder einer Kombination aus diesen Vorgängen geschehen.

[0064] Während die einzelne Umformungstechnik nicht als entscheidend anzusehen ist, sollte die bestimmte Technik, die zur Ausführung der Umformung in der Praxis dieser Erfindung verwendet wird, gegenüber dem Anbieter vertraulich gehandhabt werden, das heißt, es sollte eine „proprietäre Umformungstechnik" verwendet werden, da jede Aufdeckung oder Verbreitung der Methode wahrscheinlich die Systemsicherheit und die Effektivität des Systems gefährden würde.

[0065] Um ein einfaches Beispiel zu geben: Das Nichtsichern der proprietären Umformungstechnik würde im Wesentlichen gleichbedeutend sein mit dem Schützen einer Datei durch ein Kennwort und der anschließenden Weitergabe des Kennwortes.

[0066] Das Aufzeichnen von Informationen in Tags innerhalb digitaler Dateien erfordert Kenntnisse über die einzelnen digitalen Dateiformate und die Standards, die die Struktur ihrer Formate bestimmen. Diese Standards geben vor, wie Informationen in Dateien gespeichert werden, in welcher Reihenfolge, mit Hilfe welches Komprimierungsalgorithmus usw. Die meisten digitalen Dateiformate haben Bestimmungen für die Speicherung von Benutzerdaten in der digitalen Datei zusätzlich zu den Abbildungsdaten. Die Ausführung der DocSTAR-Dateiverwaltung und des Abbildungssystems der vorliegenden Erfindung verwendet für die Speicherung von (gescannten) bitonalen und farbigen Abbildungen bekannte TIFF-Formate (Tagged Image File) und JPEG-Formate (Joint Photographic Experts Group). Die Standards für TIFF- und JPEG-Abbildungsdateiformate ermöglichen die Einbeziehung von Benutzerdaten in der Abbildungsdatei in einer Weise, die die angezeigte Abbildung nicht beeinflusst. Die vorliegende Erfindung ist in der gleichen Weise auf andere Dateiformate anwendbar, die einen Mechanismus zur Speicherung von benutzerdefinierten Daten in der Datei haben oder einen Mechanismus zur Speicherung der Datei, die mit den benutzerdefinierten Daten gekennzeichnet ist, in einer untergeordneten Datei oder separaten Datenbank, z.B. für Textverarbeitungsdokumente, Tabellenkalkulationsprogramme, digitalisierte Audios oder Videos oder jede andere digitalisierte Datei.

[0067] Das bekannte TIFF-Format ist ein Dateiformat, in dem Abbildungsdaten in einer komprimierten Form zusammen mit den Informationen zu der Abbildung (Tags) gespeichert werden können, wie beispielsweise die

verwendete Komprimierungsmethode, Auflösung, Größe, Anzahl an Farben, Titel, Datum usw.

[0068] Ein geschriebener weltweiter Standard definiert das TIFF-Format in Bezug auf die zu verwendenden Tags, welche Tags optional sind, und wie bestimmte Tags verwendet werden. Die verwaltende Organisation des TIFF-Standards, Adobe Corporation, nimmt Anfragen bezüglich kundenspezifischer Tagnummern für Unternehmen an, die Anwendungen entwickeln, die Tags innerhalb der TIFF-Abbildung verwenden. Adobe weist einzelnen Unternehmen einzigartige Nummern zu, um Interferenzen zwischen Händlern zu vermeiden. BitWise Designs, Inc., dem Zessionar dieses Patents, wurden beispielsweise nach Anfrage eigene proprietäre Tagnummern zugewiesen und anderen Händlern werden ebenfalls ihre eigenen einzigartigen proprietären Tagnummern zugewiesen. Die Verwendung eines kundenspezifischen Tags ermöglicht die Speicherung eines kundenspezifischen Datenblocks. Die TIFF-Spezifikation fordert von Programmen, Tags zu ignorieren, die sie nicht kennen und die nicht in der Basisspezifikation enthalten sind. So können Abbildungen angesehen, angezeigt und gedruckt werden, die kundenspezifische Tags beinhalten, da die Abbildungsdateien immer noch der TIFF-Spezifikation entsprechen.

[0069] Im Falle von TIFF-Abbildungsdateien werden folgende TIFF-Abbildungstags verwendet:

Tag#	Verwendung
10 Dh	Dokumentname
10 Eh	Abbildungsbeschreibung
132 h	Datum/Uhrzeit
9244 h	BitWise DocSTAR kundenspezifischer Tag 1 kundenspezifischer Datenblock enthält proprietäre Informationen inschließlich: Abbildungs-CRC Authentidate-CRC

[0070] In Fig. 5 ist ein exemplarisches Ablaufdiagramm zur Berechnung eines Abbildungs-CRC für eine TIFF-Abbildungsdatei dargestellt. Die Berechnung eines Abbildungs-CRC für die TIFF-Abbildungsdatei erfordert die Berechnung eines CRC-32 auf einem gegebenen Datenblock mit Hilfe eines vorgegebenen 32-Bit-Saatwertes. Der anfängliche Saatwert wird auf –1 festgelegt (Schritt **500**). Die Routine arbeitet sich durch das Format der TIFF-Datei basierend auf dem Verzeichnis der Abbildungsdatei (Image File Directory, IFD) und berechnet den CRC-32 für jeden IFD-Eintrag und die zugehörigen Daten (Schritt **502**). Die Ergebnisse des vorherigen CRC-32 werden als Saat zum nächsten Schritt weitergegeben (Schritt **510**), bis alle IFD-Einträge durchlaufen wurden. (Schritt **506**) Alle Tags und Datenbereiche außer den folgenden werden verarbeitet (Schritt **508**):

Tag#	Beschreibung
0x010d	TIFFTAG_DOCUMENTNAME
0x010e	TIFFTAG_IMAGEDESCRIPTION
0x0132	TIFFTAG_DATETIME
0x9244	TIFFTAG_DOCSTARTAG1

[0071] Nach der Verarbeitung aller IFD-Einträge für die Datei (Schritt **506**) wird die proprietäre Umformungsmethode (wie oben beschrieben) verwendet, um den Ergebniswert des CRC in einen einzigartigen und sicheren Wert CRC' umzuformen (Schritt **512**). Der transformierte Abbildungs-CRC CRC' wird dann in der Abbildungsdatei gespeichert (Schritt **514**).

[0072] In Fig. 6 ist ein exemplarisches Ablaufdiagramm zur Berechnung eines Datums-CRC für eine TIFF-Abbildungsdatei dargestellt. Für die Berechnung des Datums-CRC für eine TIFF-Abbildungsdatei ist eine Routine erforderlich, die einen CRC-32 auf einem gegebenen Block von Daten berechnen kann und dazu einen gegebenen 32-Bit-Saatwert verwendet. Der anfängliche Saatwert wird auf den Wert des Abbildungs-CRC festgelegt (Schritt **600**). Das Programm liest den Tag 0x0132 TIFFTAG_DATETIME (Schritt **602**). Wenn der Tag DATETIME nicht gefunden und gelesen werden kann (Schritt **604**), wird eine Fehlermeldung zurückgegeben (Schritt **605**). Andernfalls wird ein CRC-32 für die Daten innerhalb des Tags DATETIME berechnet (Schritt **606**). Der Ergebnis-CRC wird dann mit Hilfe der proprietären Umformungstechnik in CRC' umgeformt (Schritt **608**) und in der Abbildungsdatei gespeichert (Schritt **610**).

[0073] Die Joint Photographic Experts Group entwickelte das nach ihr benannte Format und verwaltet die Standards für JPEG- und JPG-Dateiformate (oftmals auch JFIF -- JPEG-Dateiabbildungsformat genannt). Dieses Format wurde zur Speicherung und Übertragung von fotografischen Abbildungen entwickelt. Die verwen-

deten Komprimierungstechniken sind ideal dazu geeignet, feine Unterschiede zwischen Farben, wie bei einer Fotografie, zu speichern.

[0074] Wie bekannt ist, wird eine JPG-Datei interpretiert als eine Kette von Zeichen mit speziellen Bezeichnern (den so genannten „Markierungszeichen"), die verschiedene Elemente der Abbildungsinformationen und Abbildungsdaten voneinander trennen. Die genaue Bedeutung jedes Markierungszeichens ist an dieser Stelle nicht wichtig, außer, dass der JPG-Standard einen Satz von Markierungszeichen definiert, der von Herstellern für spezielle oder proprietäre Funktionen verwendet wird. Diese Markierungszeichen heißen „APPx", wobei „x" eine Zahl zwischen 0 und 9 darstellt.

[0075] Die vorliegende Erfindung fügt JPG-Dateien bei der Speicherung ein spezielles Markierungszeichen und einen speziellen Datenblock hinzu. In dieser Ausführung wird das Markierungszeichen „APP8" verwendet, aus dem einfachen Grund, dass dieses Markierungszeichen selten von anderen Herstellern verwendet wird. Dieses Markierungszeichen enthält verschiedene proprietäre Informationen, einschließlich:
Authentidate
Abbildungs-CRC
Authentidate-CRC

[0076] In Fig. 7 wird ein exemplarisches Ablaufdiagramm zur Berechnung eines Abbildungs-CRC für eine JPEG-Abbildungsdatei dargestellt. Für die Berechnung eines CRC für eine JPEG-Abbildungsdatei ist eine Routine erforderlich, die einen CRC-32 auf einem gegebenen Datenblock mit Hilfe eines vorgegebenen 32-Bit-Saatwertes berechnen kann. Der anfängliche Saatwert wird auf –1 festgelegt (Schritt **700**). Die Daten der Abbildungsdatei werden sequenzweise gelesen, und die Position des APP8 wird bestimmt und gelesen (Schritt **702**). Wenn das Markierungszeichen APP8 nicht gefunden und gelesen werden kann (Schritt **704**), wird eine Fehlermeldung zurückgegeben (Schritt **705**). Für alle Daten in der Datei wird vom Beginn der Datei bis zum (aber nicht einschließlich des) Markierungszeichen(s) APP8 ein CRC-32 berechnet (Schritt **706**). Das Ergebnis dieser Berechnung wird als Saat für die Berechnung eines CRC-32 für den Rest der Datei nach dem Markierungszeichen APP8 verwendet (Schritt **708**). Der Ergebnis-CRC wird mit Hilfe einer proprietären Umformungstechnik zu einem CRC' umgeformt (Schritt **710**). Der transformierte Abbildungs-CRC' wird dann in der Abbildungsdatei gespeichert. (Schritt **712**.)

[0077] In Fig. 8 wird ein exemplarisches Ablaufdiagramm zur Berechnung eines Datums-CRC für eine JPEG-Abbildungsdatei dargestellt. Für die Berechnung eines CRC für eine JPEG-Abbildungsdatei ist eine Routine erforderlich, die einen CRC-32 auf einem gegebenen Datenblock mit Hilfe eines vorgegebenen 32-Bit-Saatwertes berechnen kann. Der anfängliche Saatwert wird auf den Wert des Abbildungs-CRC festgelegt (Schritt **800**). Die Datei wird sequenzweise gelesen und die Position des APP8 wird bestimmt und gelesen (Schritt **802**). Wenn das Markierungszeichen APP8 nicht gefunden und gelesen werden kann (Schritt **804**), wird eine Fehlermeldung zurückgegeben (Schritt **805**). Innerhalb des APP8-Datenbereichs oder -blocks wird ein CRC-32 für die sichere Datenzeichenfolge berechnet (Schritt **806**). Der Ergebnis-CRC wird mit Hilfe einer proprietären Umformungstechnik in einen CRC' umgeformt (Schritt **808**). Der transformierte Datums-CRC' wird in der Abbildungsdatei gespeichert. (Schritt **810**.)

[0078] Die vorliegende Erfindung wurde in Bezug auf bestimmte Ausführungen derselben dargestellt und beschrieben. Es muss jedoch betont werden, dass die oben beschriebenen Ausführungen lediglich zur Illustration des Prinzips dieser Erfindung dienen und keine exklusiven Ausführungen darstellen. Um die Diskussion der vorliegenden Erfindung zu erleichtern, werden Originalpapierdokumente (z.B. Dokumente, Fotos usw.), die in digitale Abbildungen eingescannt werden, in der DocSTAR-Ausführung der vorliegenden Erfindung vorausgesetzt. Jedoch sollten Fachkundige wissen, dass die vorliegende Erfindung in der gleichen Weise auf jede digitale Datei anwendbar ist und es keinen Unterschied macht, woher diese Datei stammt oder wie sie generiert wurde (z.B. digitale Abbildungen aus Digitalkameras, medizinischen Abbildungsgeräten, Textverarbeitungsanwendungen, Tabellenkalkulationsanwendungen oder anderen Quellen).

[0079] Alternative Ausführungen, die Variationen der hier aufgelisteten Ausführungen beinhalten, können implementiert werden, um die Vorteile der vorliegenden Erfindung zu erreichen.

[0080] Es soll weiterhin betont werden, dass das Vorstehende und viele weitere Änderungen, Auslassungen und Ergänzungen möglicherweise von einer fachkundigen Person entwickelt werden, ohne vom Bereich der Erfindung abzuweichen.

[0081] Es ist daher beabsichtigt, dass die vorliegende Erfindung nicht auf die beiliegenden Ausführungen be-

grenzt wird, sondern in Übereinstimmung mit den folgenden Ansprüchen definiert wird.

Patentansprüche

1. Management- und Bildverarbeitungssystem für Digitaldateien, umfassend:
ein Mittel zur Eingabe einer Digitaldatei;
eine sichere Datums- und Uhrzeitreferenz, die Datums- und Uhrzeitinformationen liefert; gekennzeichnet durch:
ein Mittel zum Generieren eines von den Datums- und Uhrzeitinformationen abgeleiteten Datums-/Uhrzeitwerts, der einen zyklischen Redundanzcode-Algorithmus implementiert;
ein Mittel zum Generieren eines von der Digitaldatei abgeleiteten Bildwerts;
ein Mittel zum Markieren der Digitaldatei mit den Datums- und
Uhrzeitinformationen, dem Datums-/Uhrzeitwert und dem Bildwert; und
ein Mittel zum Speichern der markierten Digitaldatei.

2. System nach Anspruch 1, worin die sichere Datums- und Uhrzeitreferenz ein lokaler sicherer Block ist.

3. System nach Anspruch 1, worin das Mittel zum Generieren des Bildwerts einen zyklischen Redundanzcode-Algorithmus implementiert.

4. System nach Anspruch 1, das des weiteren Mittel zum Transformieren des Datums-/Uhrzeitwerts besitzt und wobei das Mittel zum Markieren die Digitaldatei mit dem transformierten Datums-/Uhrzeitwert markiert.

5. System nach Anspruch 4, worin das Mittel zum Transformieren des Datums-/Uhrzeitwerts eine mathematische Transformation ausführt.

6. System nach Anspruch 1, das des weiteren ein Mittel zum Transformieren des Bildwerts besitzt und wobei das Mittel zum Markieren die Digitaldatei mit dem transformierten Bildwert markiert.

7. System nach Anspruch 6, worin das Mittel zum Transformieren des Bildwerts eine mathematische Transformation durchführt.

8. System nach Anspruch 1, worin die Digitaldatei eine Bilddatei ist.

9. System nach Anspruch 1, worin die Digitaldatei eine Textdatei ist.

10. System nach Anspruch 1, worin die Digitaldatei eine Datei von einer Digitalkamera ist.

11. System nach Anspruch 1, worin die Digitaldatei von einer medizinischen Bildverarbeitungsvorrichtung stammt.

12. System nach Anspruch 1, worin die Digitaldatei eine von einer Computeranwendung generierte Datei ist.

13. System nach Anspruch 1, des weiteren ein Mittel zum Validieren einer markierten Datei enthaltend.

14. Verfahren zum Management und zur Bildverarbeitung einer Digitaldatei, folgende Schritte umfassend:
Bereitstellung einer Digitaldatei;
Bereitstellung von Datums- und Uhrzeitinformationen von einer sicheren Datums- und Uhrzeitreferenz einer lokalen Quelle, gekennzeichnet durch folgende Schritte:
Generieren eines von der Datums- und Uhrzeitreferenz abgeleiteten Datums-/Uhrzeitwerts, der einen zyklischen Redundanzcode-Algorithmus implementiert;
Generieren eines von der Digitaldatei abgeleiteten Bildwerts;
Markieren der Digitaldatei mit den Datums- und Uhrzeitinformationen, dem Datums-/Uhrzeitwert und dem Bildwert; und
Speichern der markierten Digitaldatei.

15. Verfahren nach Anspruch 14, worin das Mittel zum Generieren des Bildwerts eine zyklischen Redundanzcode-Algorithmus implementiert.

16. Verfahren nach Anspruch 14, des weiteren den Schritt der Transformation des Datums- und Uhrzeitwerts und des Markierens der Digitaldatei mit dem transformierten Datums- und Uhrzeitwert umfassend.

17. Verfahren nach Anspruch 14, des weiteren den Schritt der Transformation des Bildwerts und das Markieren der Digitaldatei mit dem transformierten Datums- und Uhrzeitwert umfassend.

18. Verfahren nach Anspruch 14, worin der Schritt zur Bereitstellung einer Digitaldatei das optische Scannen eines Originalbildes in ein Digitalbild umfasst.

19. Verfahren nach Anspruch 14, des weiteren die Neuberechnung des Datums-/Uhrzeitwerts und des Bildwerts und das Vergleichen der neu berechneten Werte mit den Datums-/Uhrzeit- bzw. Bildwerten, die in dem Bild markiert sind, umfassend.

Es folgen 15 Blatt Zeichnungen

Anhängende Zeichnungen

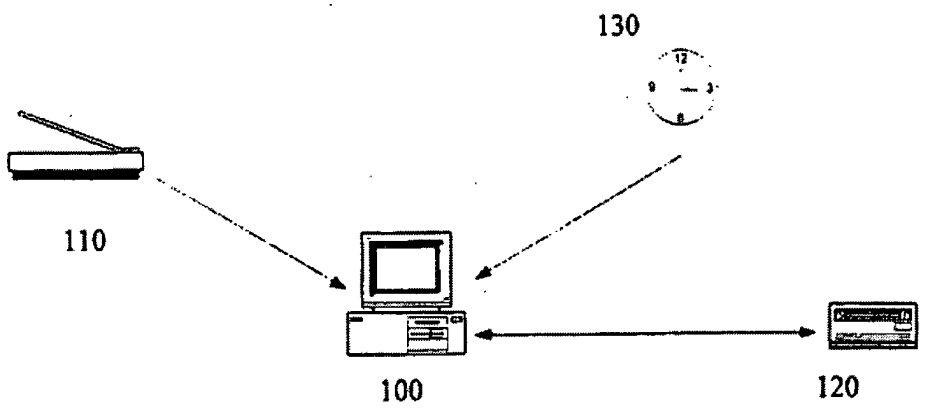


FIG. 1

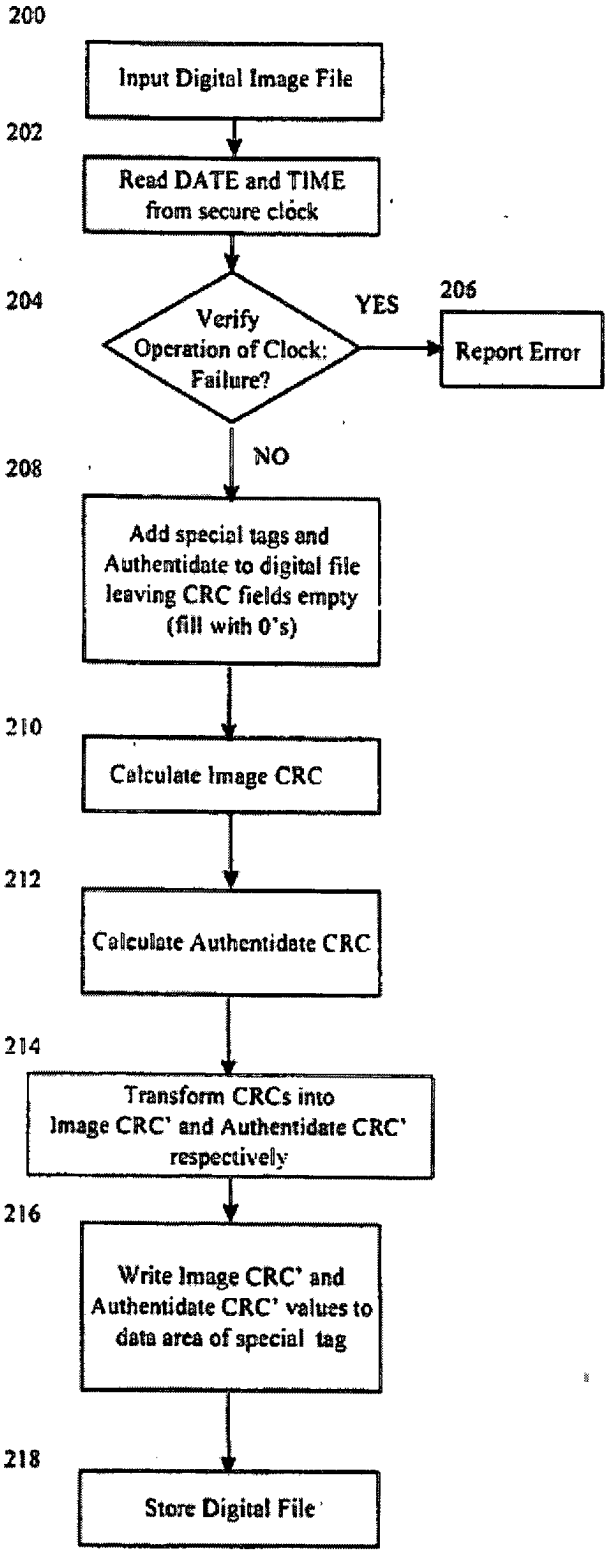

200
Input Digital Image File
202
Read DATE and TIME from secure clock
204
Verify Operation of Clock: Failure?
YES
206
Report Error
NO
208
Add special tags and Authentidate to digital file leaving CRC fields empty (fill with 0's)
210
Calculate Image CRC
212
Calculate Authentidate CRC
214
Transform CRCs into Image CRC' and Authentidate CRC' respectively
216
Write Image CRC' and Authentidate CRC' values to data area of special tag
218
Store Digital File

FIG. 2

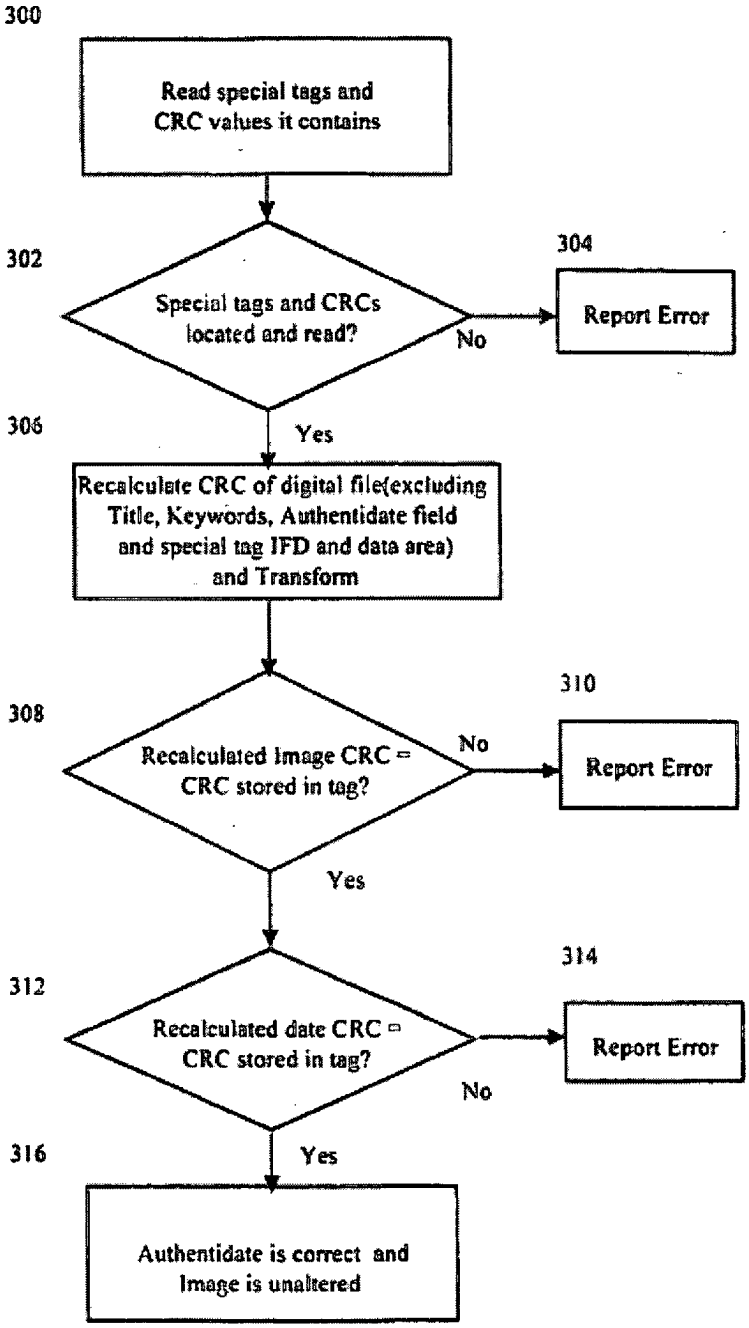

300
Read special tags and CRC values it contains
302
Special tags and CRCs located and read?
No
304
Report Error
Yes
306
Recalculate CRC of digital file(excluding Title, Keywords, Authentidate field and special tag IFD and data area) and Transform
308
Recalculated Image CRC = CRC stored in tag?
No
310
Report Error
Yes
312
Recalculated date CRC = CRC stored in tag?
No
314
Report Error
Yes
316
Authentidate is correct and Image is unaltered

FIG. 3

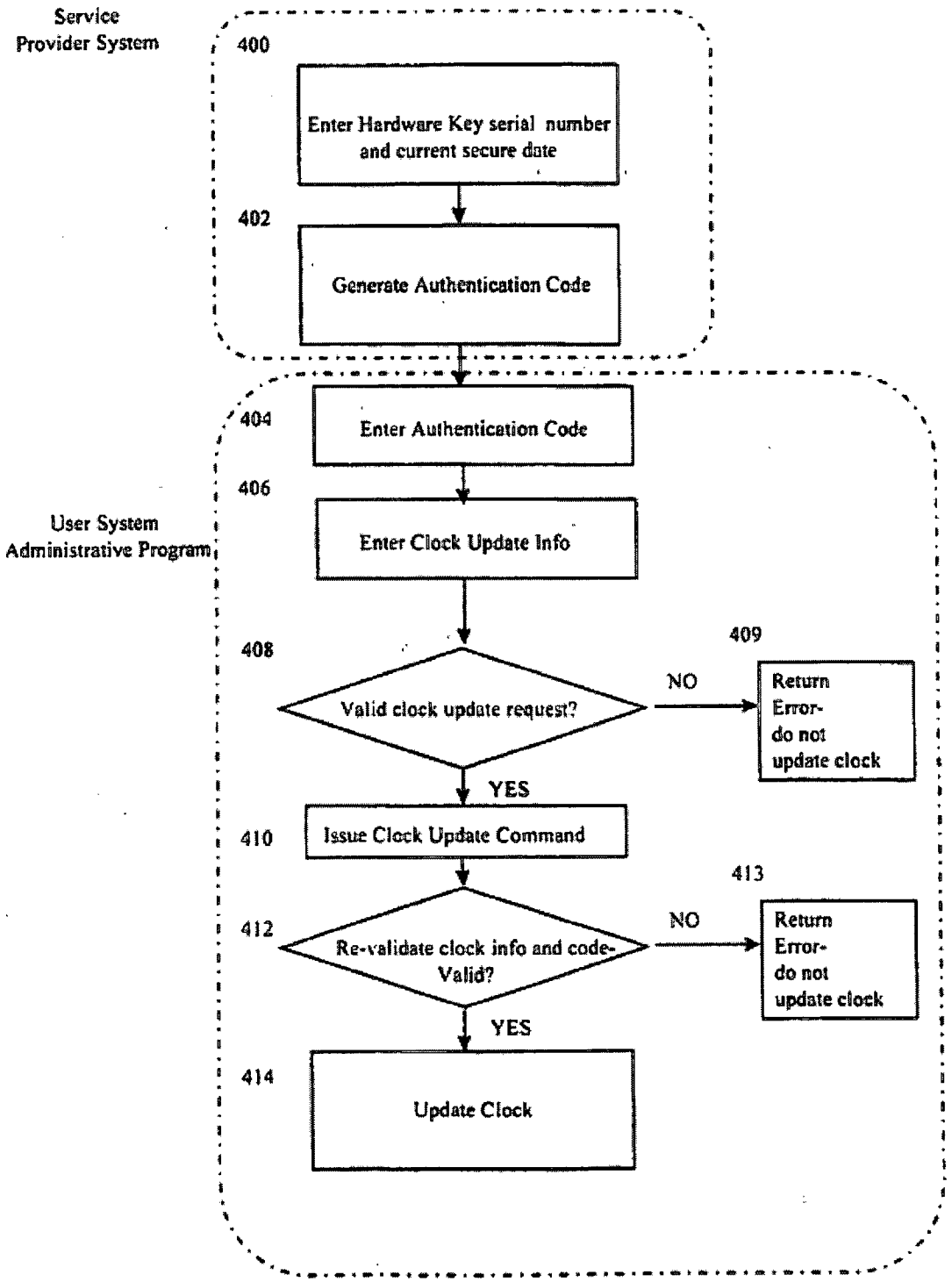

Service Provider System
400
Enter Hardware Key serial number and current secure date
402
Generate Authentication Code
User System Administrative Program
404
Enter Authentication Code
406
Enter Clock Update Info
408
Valid clock update request?
NO
409
Return Error- do not update clock
YES
410
Issue Clock Update Command
412
Re-validate clock info and code- Valid?
NO
413
Return Error- do not update clock
YES
414
Update Clock

FIG. 4

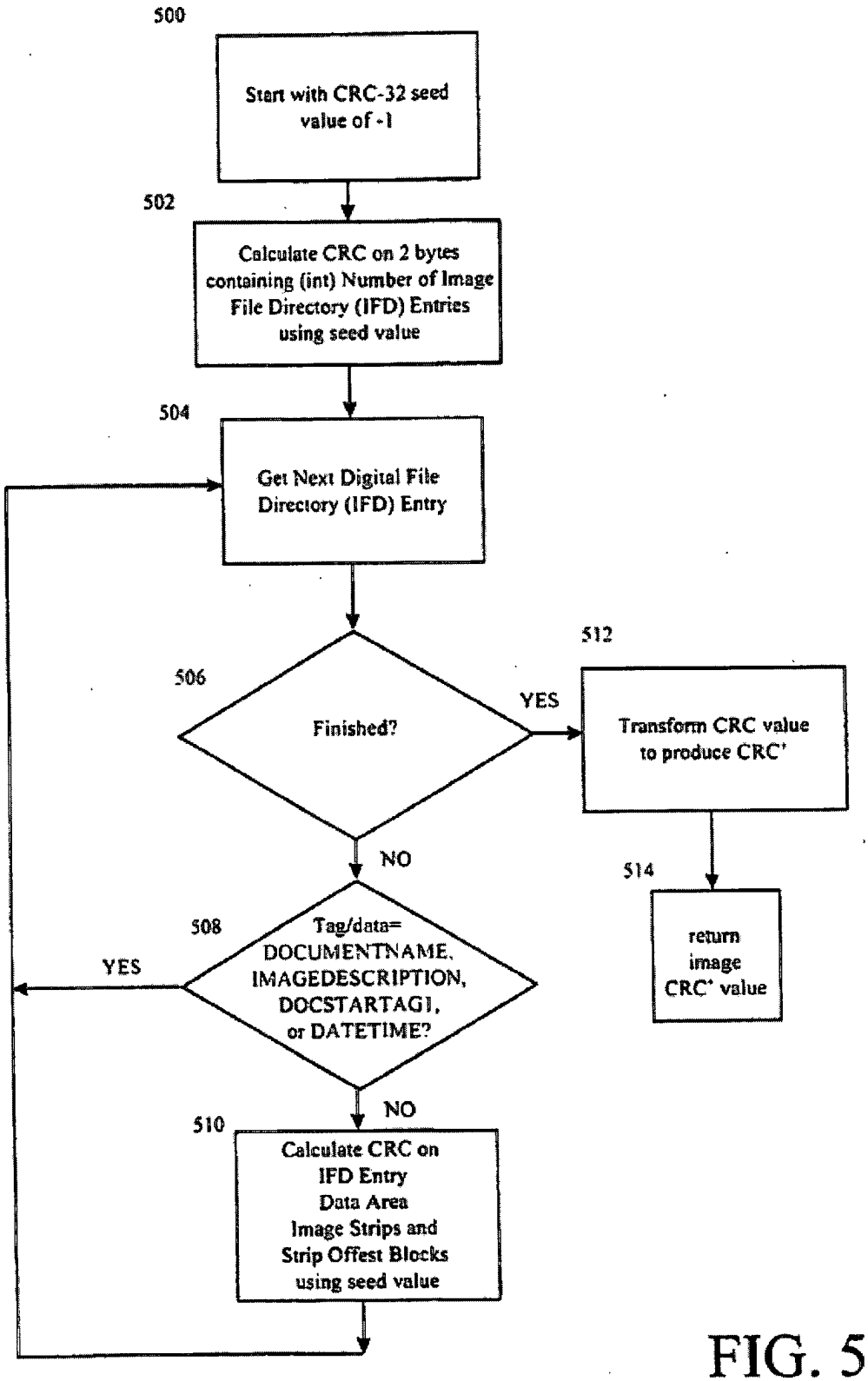

500
Start with CRC-32 seed value of -1
502
Calculate CRC on 2 bytes containing (int) Number of Image File Directory (IFD) Entries using seed value
504
Get Next Digital File Directory (IFD) Entry
506
Finished?
YES
512
Transform CRC value to produce CRC'
514
return image CRC' value
NO
508
Tag/data= DOCUMENTNAME, IMAGEDESCRIPTION, DOCSTARTAG1, or DATETIME?
YES
NO
510
Calculate CRC on IFD Entry Data Area Image Strips and Strip Offest Blocks using seed value

FIG. 5

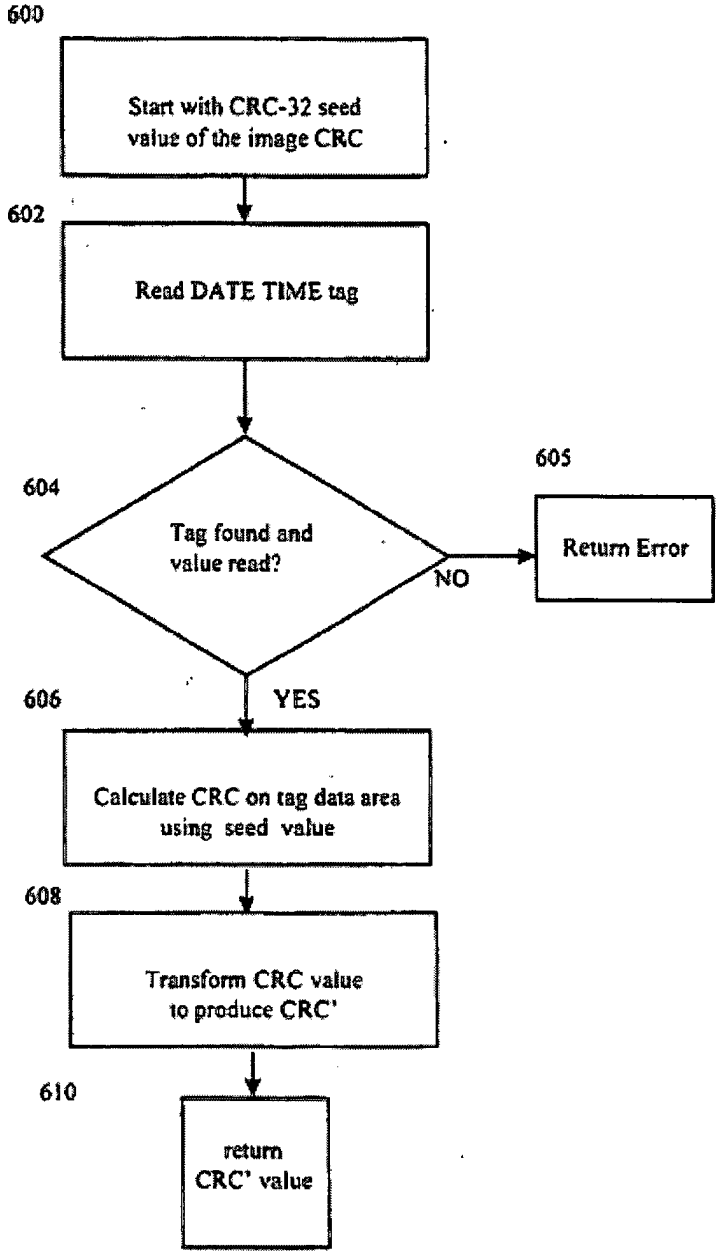

600
Start with CRC-32 seed value of the image CRC
602
Read DATE TIME tag
604
Tag found and value read?
NO
605
Return Error
YES
606
Calculate CRC on tag data area using seed value
608
Transform CRC value to produce CRC'
610
return CRC' value

FIG. 6

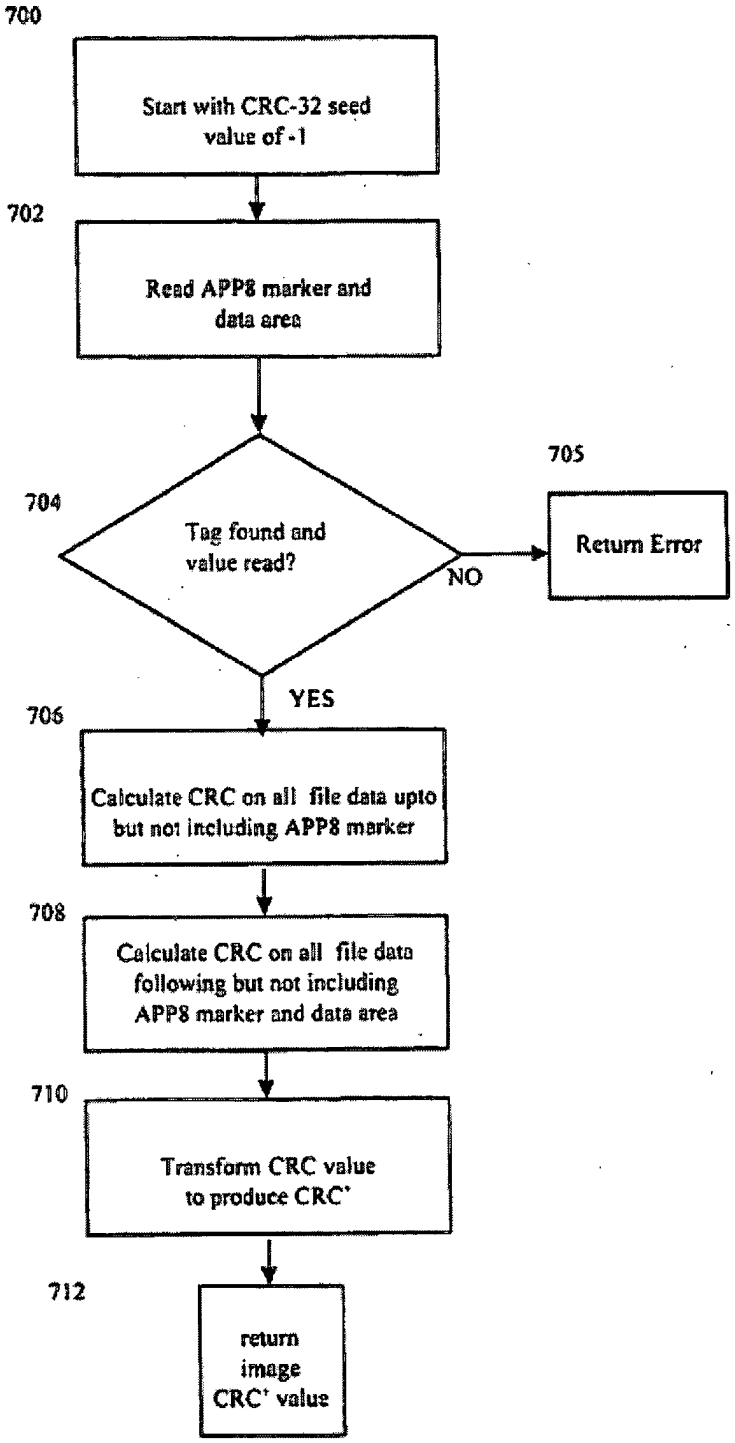

700
Start with CRC-32 seed value of -1
702
Read APP8 marker and data area
704
Tag found and value read?
NO
705
Return Error
YES
706
Calculate CRC on all file data upto but not including APP8 marker
708
Calculate CRC on all file data following but not including APP8 marker and data area
710
Transform CRC value to produce CRC'
712
return image CRC' value

FIG. 7

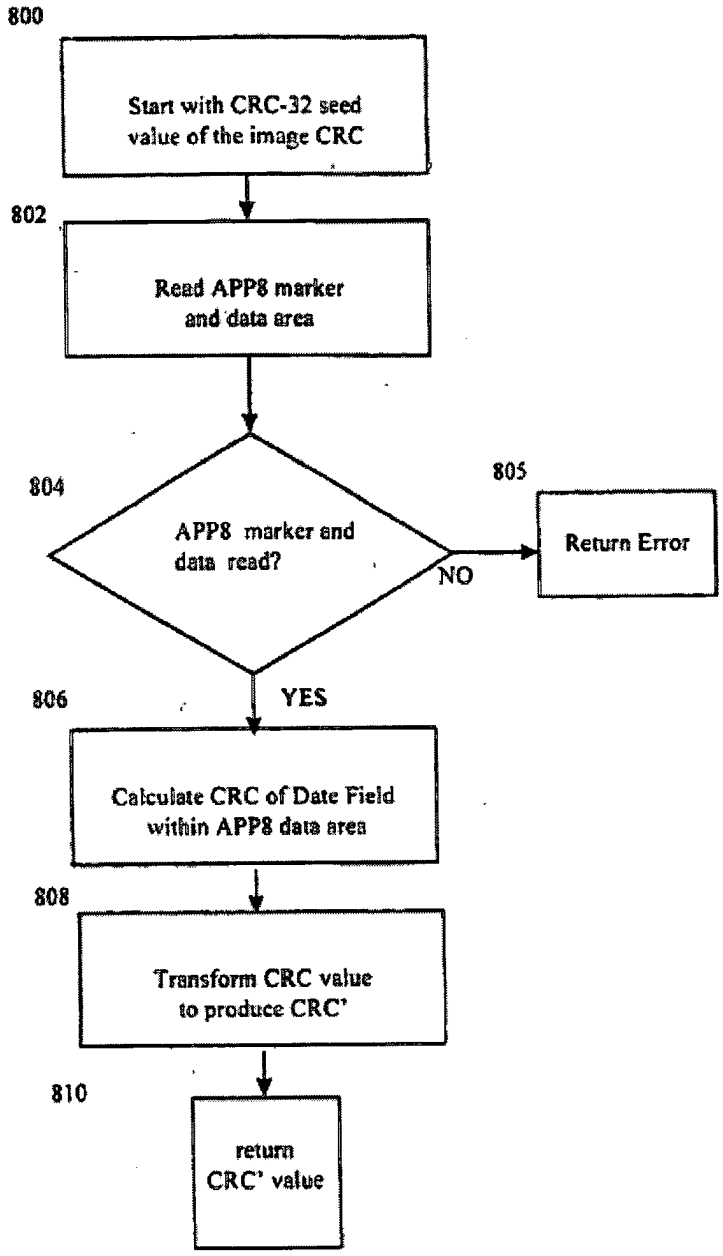
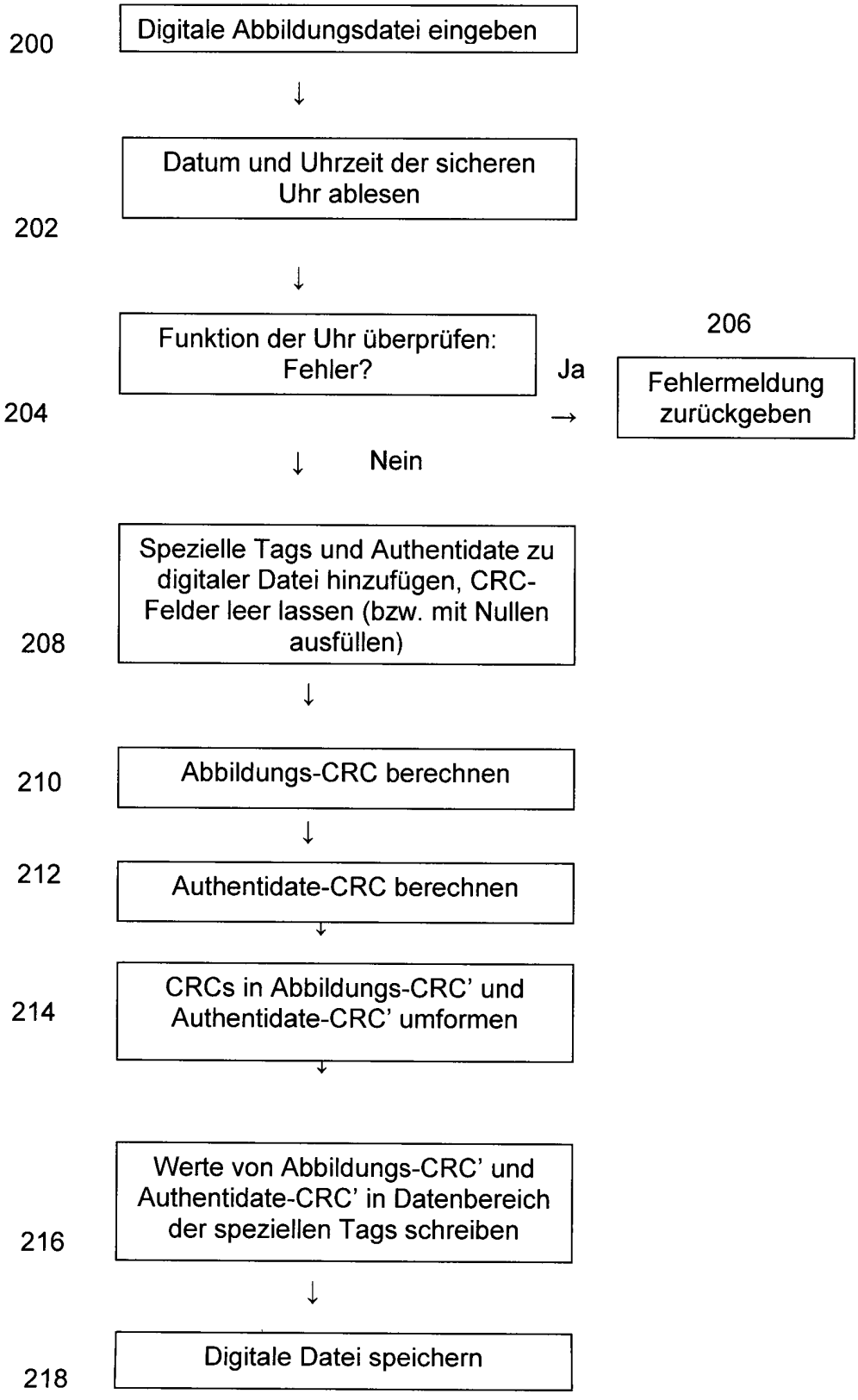

800
Start with CRC-32 seed value of the image CRC
802
Read APP8 marker and data area
804
APP8 marker and data read?
805
Return Error
NO
YES
806
Calculate CRC of Date Field within APP8 data area
808
Transform CRC value to produce CRC'
810
return CRC' value

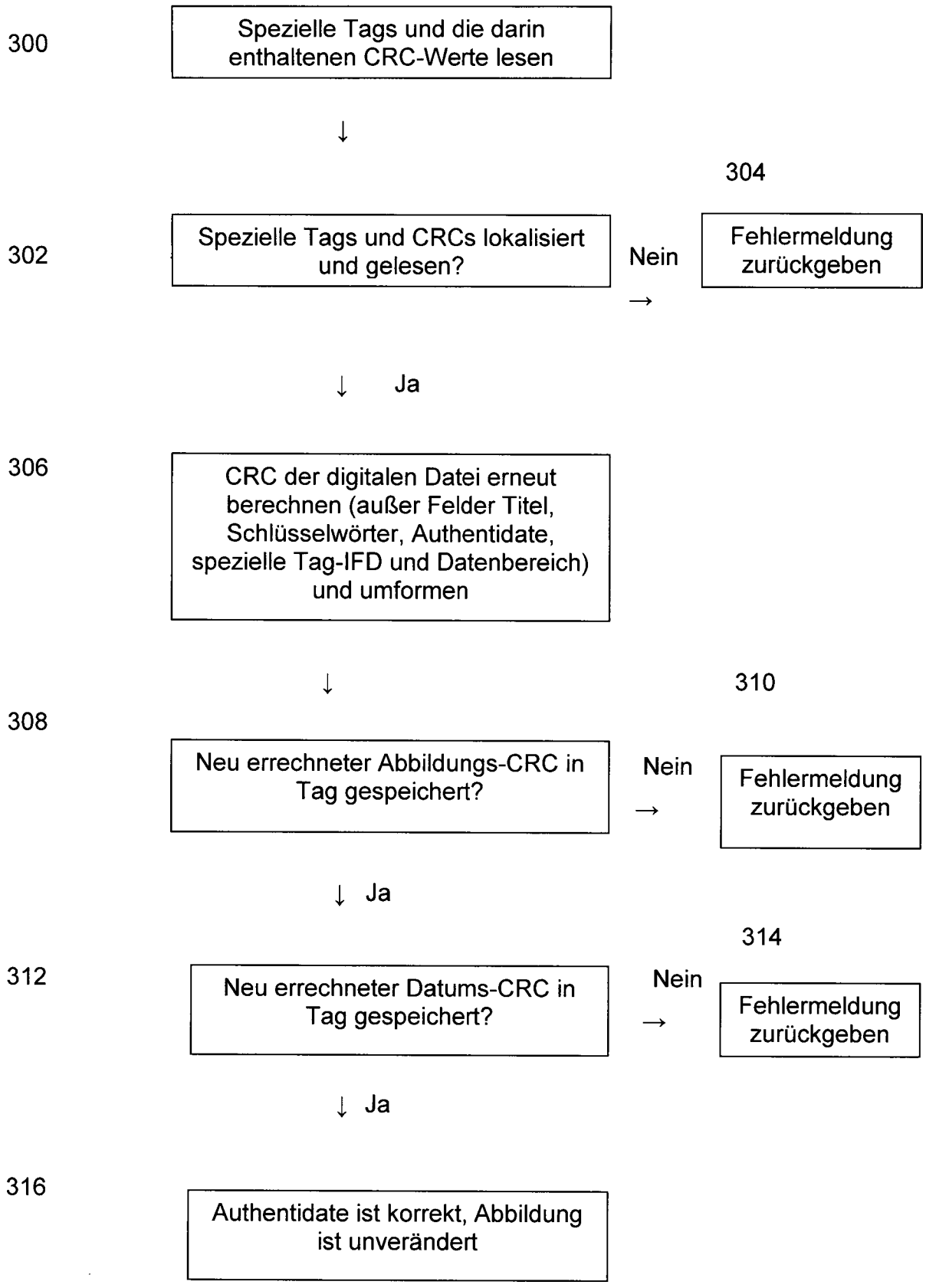
FIG. 8

Übersetzung der Textinhalte zu den Ablaufdiagrammen der Figuren 2 bis 8

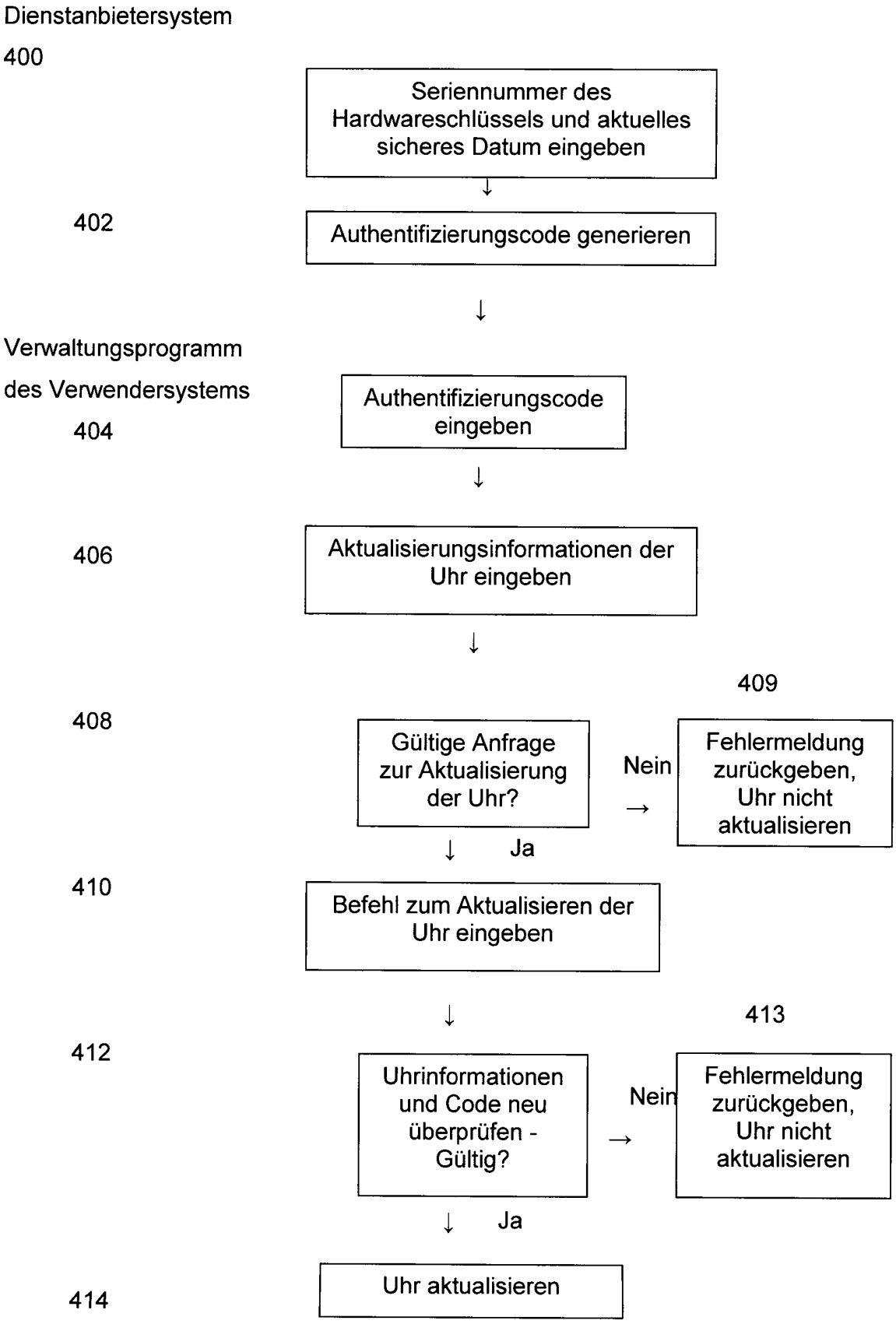
Figur 2



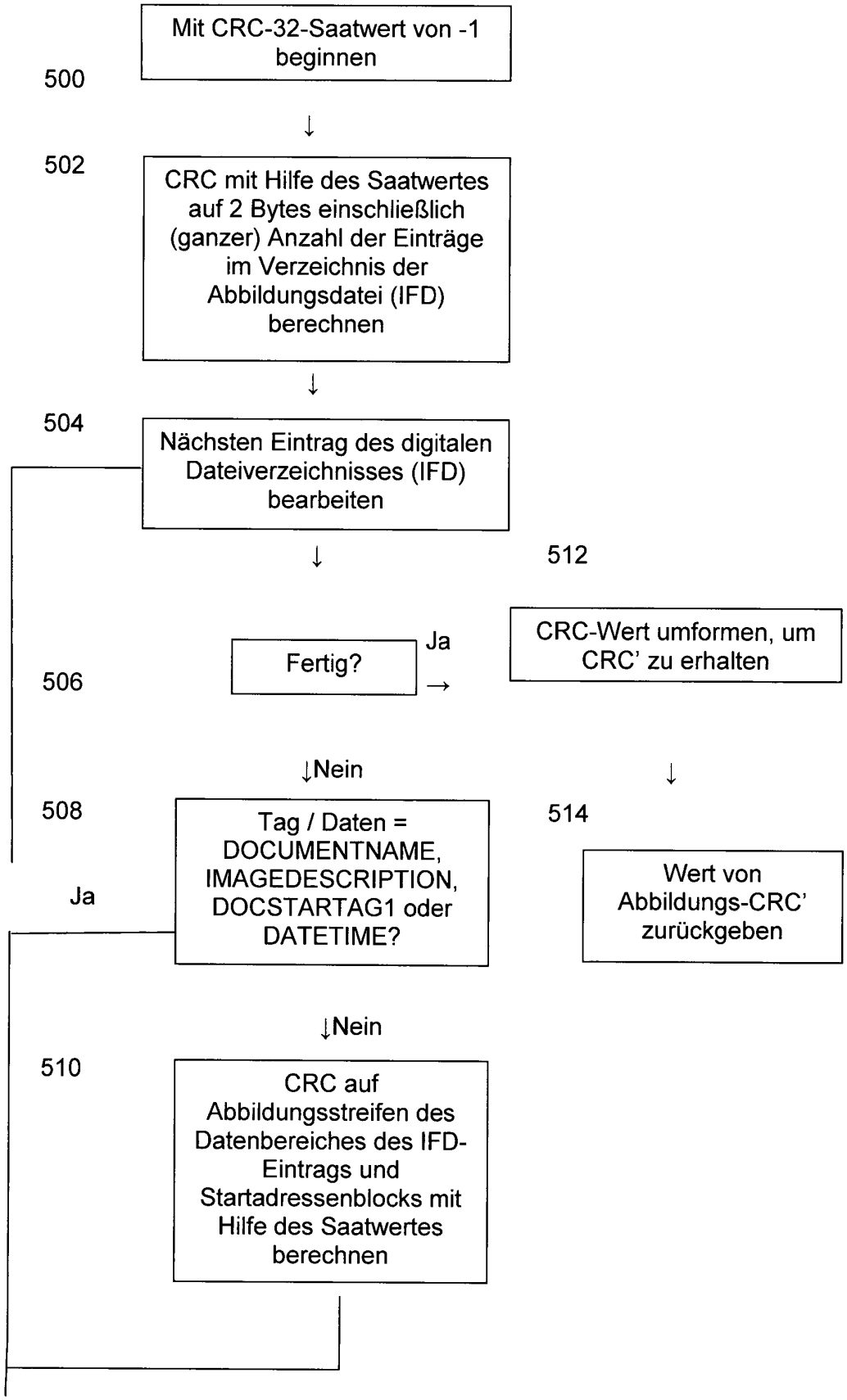
Figur 3


300
Spezielle Tags und die darin enthaltenen CRC-Werte lesen
304
302
Spezielle Tags und CRCs lokalisiert und gelesen?
Nein
Fehlermeldung zurückgeben
Ja
306
CRC der digitalen Datei erneut berechnen (außer Felder Titel, Schlüsselwörter, Authentidate, spezielle Tag-IFD und Datenbereich) und umformen
310
308
Neu errechneter Abbildungs-CRC in Tag gespeichert?
Nein
Fehlermeldung zurückgeben
Ja
314
312
Neu errechneter Datums-CRC in Tag gespeichert?
Nein
Fehlermeldung zurückgeben
Ja
316
Authentidate ist korrekt, Abbildung ist unverändert

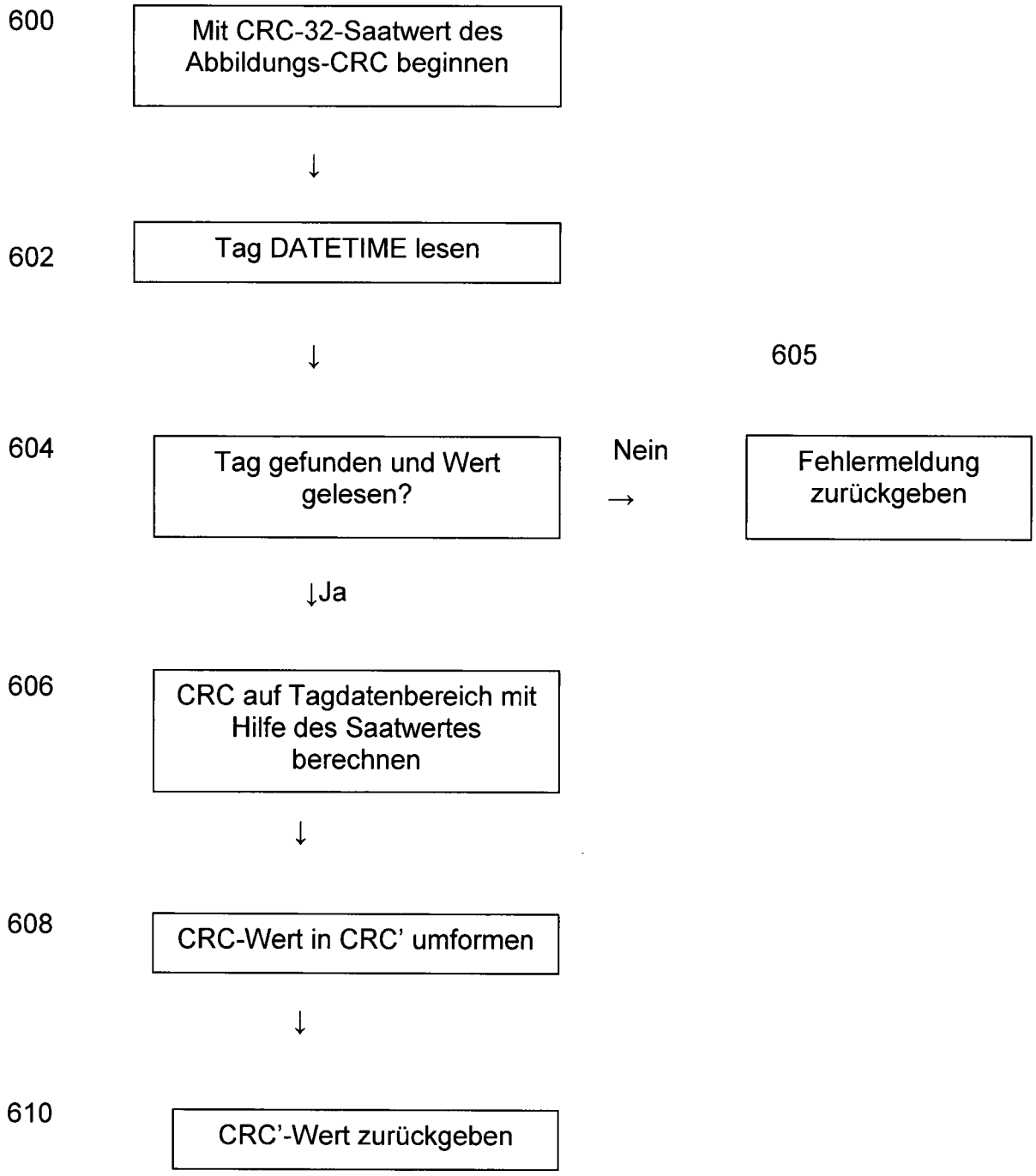
Figur 4


Dienstanbietersystem
400
Seriennummer des Hardwareschlüssels und aktuelles sicheres Datum eingeben
402
Authentifizierungscode generieren
Verwaltungsprogramm des Verwendersystems
404
Authentifizierungscode eingeben
406
Aktualisierungsinformationen der Uhr eingeben
409
408
Gültige Anfrage zur Aktualisierung der Uhr?
Nein
Fehlermeldung zurückgeben, Uhr nicht aktualisieren
Ja
410
Befehl zum Aktualisieren der Uhr eingeben
413
412
Uhrinformationen und Code neu überprüfen - Gültig?
Nein
Fehlermeldung zurückgeben, Uhr nicht aktualisieren
Ja
414
Uhr aktualisieren

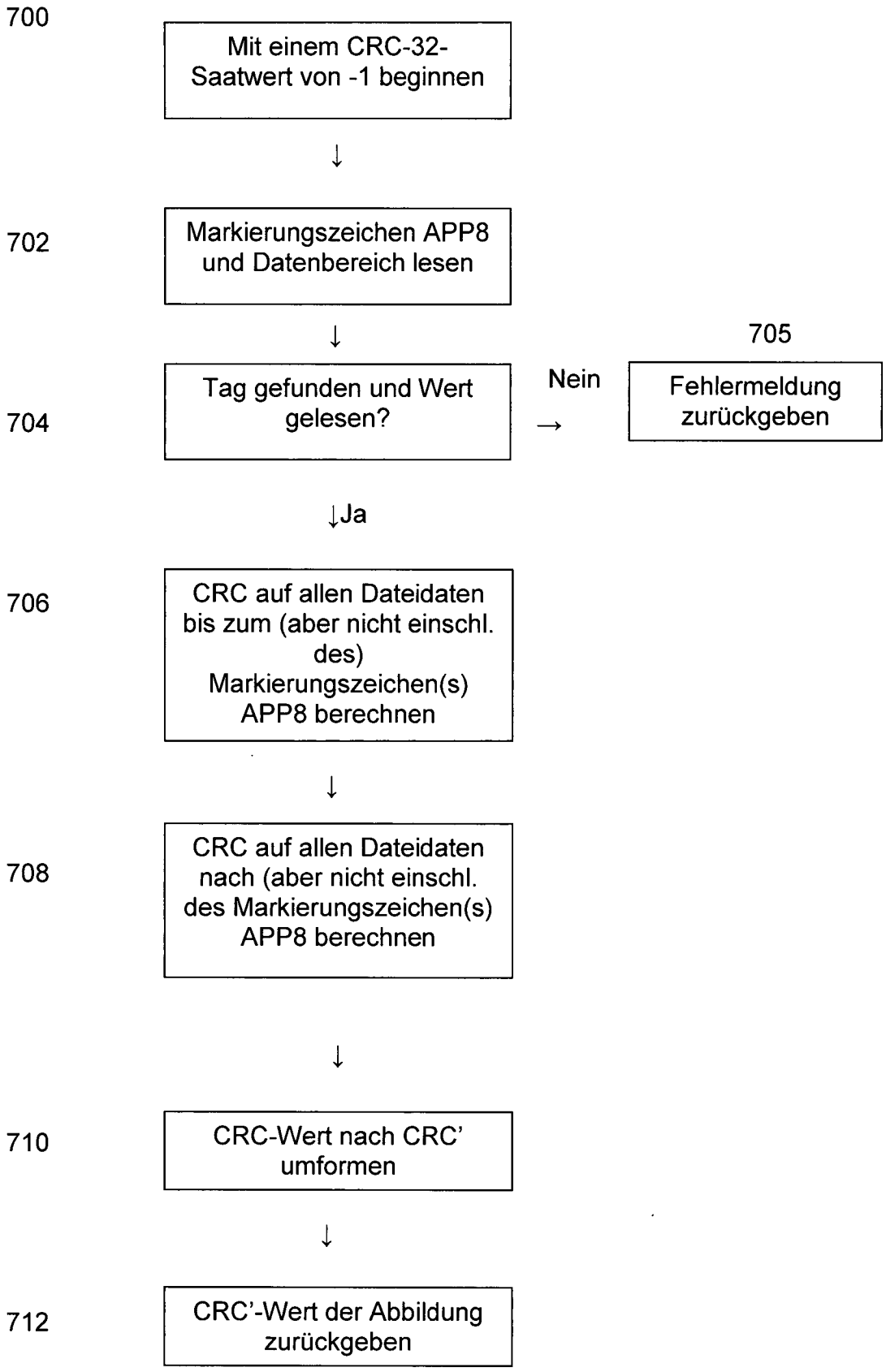
Figur 5


Mit CRC-32-Saatwert von -1 beginnen
500
502
CRC mit Hilfe des Saatwertes auf 2 Bytes einschließlich (ganzer) Anzahl der Einträge im Verzeichnis der Abbildungsdatei (IFD) berechnen
504
Nächsten Eintrag des digitalen Dateiverzeichnisses (IFD) bearbeiten
512
CRC-Wert umformen, um CRC' zu erhalten
Fertig?
Ja
506
Nein
508
Tag / Daten = DOCUMENTNAME, IMAGEDESCRIPTION, DOCSTARTAG1 oder DATETIME?
Ja
514
Wert von Abbildungs-CRC' zurückgeben
Nein
510
CRC auf Abbildungsstreifen des Datenbereiches des IFD-Eintrags und Startadressenblocks mit Hilfe des Saatwertes berechnen

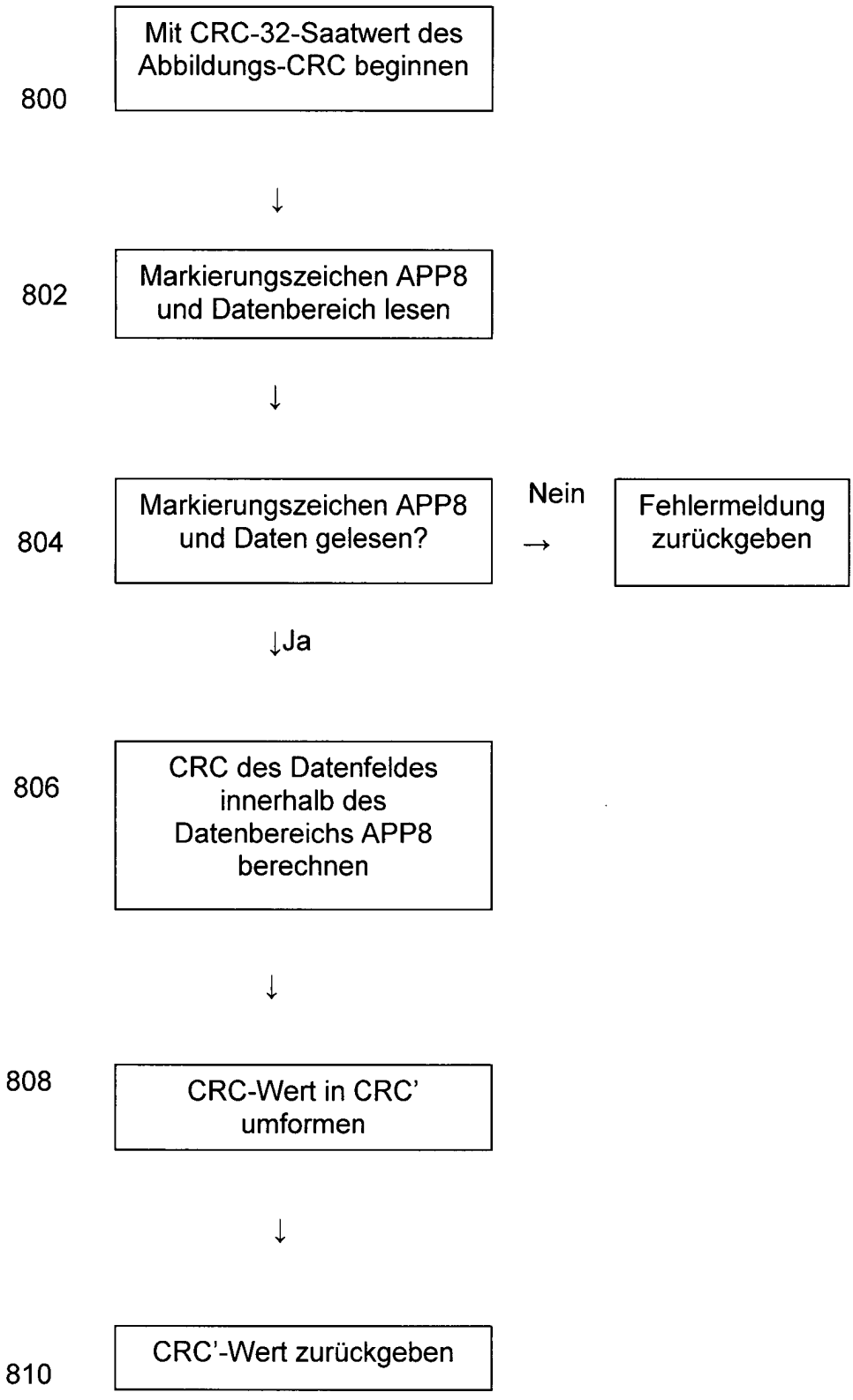
Figur 6


600
Mit CRC-32-Saatwert des Abbildungs-CRC beginnen
602
Tag DATETIME lesen
604
Tag gefunden und Wert gelesen?
Nein
605
Fehlermeldung zurückgeben
Ja
606
CRC auf Tagdatenbereich mit Hilfe des Saatwertes berechnen
608
CRC-Wert in CRC' umformen
610
CRC'-Wert zurückgeben

Figur 7


700
Mit einem CRC-32-Saatwert von -1 beginnen
702
Markierungszeichen APP8 und Datenbereich lesen
705
704
Tag gefunden und Wert gelesen?
Nein
Fehlermeldung zurückgeben
Ja
706
CRC auf allen Dateidaten bis zum (aber nicht einschl. des) Markierungszeichen(s) APP8 berechnen
708
CRC auf allen Dateidaten nach (aber nicht einschl. des Markierungszeichen(s) APP8 berechnen
710
CRC-Wert nach CRC' umformen
712
CRC'-Wert der Abbildung zurückgeben

Figur 8


800
Mit CRC-32-Saatwert des Abbildungs-CRC beginnen
802
Markierungszeichen APP8 und Datenbereich lesen
804
Markierungszeichen APP8 und Daten gelesen?
Nein
Fehlermeldung zurückgeben
Ja
806
CRC des Datenfeldes innerhalb des Datenbereichs APP8 berechnen
808
CRC-Wert in CRC' umformen
810
CRC'-Wert zurückgeben