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

(10) **DE 697 31 316 T2** 2006.02.23

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 966 839 B1**
(21) Deutsches Aktenzeichen: **697 31 316.6**
(86) PCT-Aktenzeichen: **PCT/US97/05532**
(96) Europäisches Aktenzeichen: **97 917 839.9**
(87) PCT-Veröffentlichungs-Nr.: **WO 97/038531**
(86) PCT-Anmeldetag: **03.04.1997**
(87) Veröffentlichungstag der PCT-Anmeldung: **16.10.1997**
(97) Erstveröffentlichung durch das EPA: **29.12.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **20.10.2004**
(47) Veröffentlichungstag im Patentblatt: **23.02.2006**

(51) Int Cl.[8]: ***H04N 7/167*** (2006.01)
H04N 1/44 (2006.01)
H04N 5/76 (2006.01)
H04K 1/00 (2006.01)
H04L 9/00 (2006.01)
G09C 3/00 (2006.01)
H04N 1/32 (2006.01)

(30) Unionspriorität:
627441 **04.04.1996** **US**

(73) Patentinhaber:
Flashpoint Technology, Inc., Peterborough, N.H., US

(74) Vertreter:
Einsel und Kollegen, 38102 Braunschweig

(84) Benannte Vertragsstaaten:
BE, DE, FR, GB, IE

(72) Erfinder:
STEINBERG, Eran, San Francisco, US

(54) Bezeichnung: **BILDMARKIERUNG UND -AUTHENTIFIZIERUNG IN EINER KAMERA**

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

Hintergrund der Erfindung

Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich ganz allgemein auf die Bildauthentifizierung und insbesondere auf ein Verfahren und eine Vorrichtung in einer Kamera zum nicht zerstörenden Markieren eines Bildes und zum Schaffen von Bildauthentifizierungsdaten bei dem Vorgang der Bildbeschaffung.

Kurze Beschreibung des Standes der Technik

[0002] Das Verhindern von unautorisierter Benutzung und das damit verwandte Problem der Authentifizierung von Dokumenten und Bildern ist ein Problem, das bereits in der Vergangenheit angesprochen wurde. In dem Bereich der unautorisierten Benutzung benötigen Fotografen zum Ausstellen ihrer Bilder für einen möglichen Verkauf einen Zustand, der von der Verwendung des Bildes vor einem Vertragsabschluss abschreckt. Beispiele schließen auch das Fotografieren auf Vorrat und Bildbanken ein. In einem Versuch zum Verhindern unautorisierter Benutzung kann ein Fotograf eine Markierung (typischerweise als "Wasserzeichen" benannt) auf einer Kopie des Bildes anbringen, um von seiner Benutzung abzuschrecken. Auch dann besteht stets das Risiko, dass jemand in den Besitz des Originals kommen kann. Ein besonderes Problem existiert auf dem Gebiet der digitalen Fotografie, in der das Konzept einer "Original"-Fotografie höchst fragwürdig ist, aufgrund der Möglichkeit der Bildbearbeitung.

[0003] Auf dem Gebiet der Authentifizierung erfordert eine zuverlässige Geldversorgung ein Verfahren zum Authentifizieren der Währung. Unterschriften auf zahlreichen Typen von Dokumenten benötigen eine Authentifizierung, wobei die Bemühungen von der Verwendung eines öffentlichen Notars für amtliche Dokumente bis zu dem Vorzeigen eines Führerscheins bei dem Verkaufspersonal in einem Laden reicht. Eine Bildidentifizierung wird in vielen Gebieten eingesetzt, aber es fehlt ihr grundsätzlich eine Einrichtung zum Zusichern, dass das Bild tatsächlich die Person zeigt, die auf andere Weise identifiziert wurde, beispielsweise auf einem Führerschein oder einer Sicherheitsplakette/-karte. Das Problem mit einer Bildidentifizierung ist eines der Sicherstellung, dass das Bild auf der Karte das Original ist. Ohne ein Verfahren des Prüfens der Bildauthentifizierung können falsche Identifikationen durch einen Austausch des Bildes vorgenommen werden, nachdem das Originalbild aufgenommen wurde. Ein besonderes Problem besteht bei der modernen digitalen Fotografie, die einem Benutzer eine weiträumige und leichte Flexibilität beim Bearbeiten von Bildern durch Pixelmanipulation zur Verfügung stellt, und auf diese Weise das bereits oben erwähnte Problem wieder hervorzieht, das betrifft, was als Original gegenüber einem modifizierten oder manipulierten Bild berücksichtigt werden sollte. Ein Verfahren zum Authentifizieren eines Bildes besteht darin, physisch ein Bild in einer Weise zu markieren, die es sehr schwierig macht, es zu reproduzieren, sodass ein Bild nur unter einem bestimmten Winkel angesehen werden kann, wie dies in dem US-Patent 5,468,581 von Coe et al. beschrieben ist. Das US-Patent 5,410,642 von Hakamatsuka et al. beschreibt ein Verfahren zum Herstellen einer Identitätskarte mit einem Einprägen über einem Foto und einem Anbringen eines Codes an der Identitätskarte. Das US-Patent 5,420,924 von Berson et al. beschreibt das Herausziehen eines Informationsabschnittes aus einem digitalen Bild und dessen Platzieren auf einer Seite einer Identitätskarte mit dem Foto auf der anderen. Das Foto kann dann auf anschließende Änderungen durch das Dekodieren der Daten auf der Rückseite und das Anzeigen und das Überlagern des sich ergebenden Bildes mit dem Foto überprüft werden, um visuell Unterschiede anzuzeigen.

[0004] Der Nachteil der vorstehenden Verfahren der Authentifizierung von Bildern besteht darin, dass sie das Hinzufügen von Authentifizierungsindikatoren zu einem Bild oder zu Daten eines Bildes mit einbeziehen, das bereits in einer sichtbaren Form existiert. Diese Verfahren werden verwendet, um spätere Änderungen am Bild zu prüfen. Das Problem mit diesen Verfahren besteht darin, dass eine beliebige Menge an Zeit zwischen dem Erzeugen des Originalbildes und dem Einschließen der Authentifizierungsdaten vergehen kann, und sie daher keinen Weg des Sicherstellens der Authentizität des angenommenen Originals darstellen. Mit anderen Worten gibt es keine Garantie, dass das Ausgangsbild nicht manipuliert wurde, bevor die Authentifizierungsmarkierung angebracht wurde. In ähnlicher Form laufen in einer Situation, in der eine sichtbare Markierung auf einem Bild platziert wird, um von der unautorisierten Benutzung abzuschrecken, existierende Verfahren, die eine Marke auf einer Kopie zum Anzeigen anbringen, das Risiko, dass jemand in den Besitz des Originals kommt.

[0005] Es besteht ganz klar ein großes Bedürfnis für ein Verfahren und eine Vorrichtung zum Markieren eines Bildes und zum Erzeugen von Authentifizierungsdaten zu der Zeit der Beschaffung des Bildes, um das Erfordernis zum vorab Erzeugen und Speichern eines sichtbaren Originals zu umgehen, das durch nicht autorisierte Personen interpretiert werden könnte.

[0006] Die US-A-5,499,294 offenbart ein Authentifizierungssystem in einer Digitalkamera, das Aufnehmen von Ausgangsbilddaten mit der Digitalkamera, das Erzeugen von ersten Authentifizierungsdaten

aus den Ausgangsbilddaten mit dem Authentifizierungssystem innerhalb der Digitalkamera, wobei die ersten Authentifizierungsdaten für die Zwecke des Vergleiches mit aus zweiten Bilddaten erzeugte zweiten Authentifizierungsdaten dienen, um festzustellen, ob die zweiten Bilddaten identisch mit den Ausgangsbilddaten sind, und das Verschlüsseln der ersten Authentifizierungsdaten mit dem Authentifizierungssystem innerhalb der Digitalkamera, um verschlüsselte erste Authentifizierungsdaten zu erzeugen und um die verschlüsselten ersten Authentifizierungsdaten zu den Ausgangsbilddaten als Ausgabe aus der Digitalkamera zuzuordnen.

Kurzfassung der Erfindung

[0007] Es ist daher eine Aufgabe der vorliegenden Erfindung, ein Verfahren vorzuschlagen, mit dem die Authentizität eines Originalbildes sichergestellt werden kann.

[0008] Es ist eine weitere Aufgabe der vorliegenden Erfindung, eine Kamera vorzuschlagen, die Daten für die Bildauthentifizierung in dem Vorgang des Aufnehmens des Bildes erzeugt.

[0009] Es ist außerdem eine weitere Aufgabe der vorliegenden Erfindung, eine Software zum Authentifizieren eines Bildes vorzuschlagen.

[0010] Es ist eine andere Aufgabe der vorliegenden Erfindung, ein Verfahren und eine Vorrichtung zum Markieren von Bilddaten innerhalb einer Kamera vorzuschlagen.

[0011] Es ist eine weitere Aufgabe der vorliegenden Erfindung, eine Markierung von Bilddaten innerhalb einer Kamera vorzusehen und einen Zugang zu dem Originalbild durch eine Verwendung eines Passwortes zu schaffen.

[0012] Diese Aufgaben werden erreicht durch ein Verfahren gemäß dem Anspruch 1 und eine Vorrichtung gemäß dem Anspruch 10.

[0013] Kurz gesagt, schließt eine bevorzugte Ausführungsform der vorliegenden Erfindung eine Kamera mit einem eingebauten Mikroprozessorsystem ein, das so programmiert ist, dass es ein Eingangspasswort und eine Kennung von einem Zentralrechner (Hostcomputer) erhält. Die Kamera ist so aufgebaut, dass sie die Kennung in Kombination mit einer Umwandlungsformel benutzt, um ein aufgenommenes Ausgangsbild in einer nicht zerstörenden Weise zu markieren, um modifizierte Bilddaten zu bilden und die Kennung an den Bildkopf anzufügen. Die Kamera erzeugt außerdem Bildauthentifizierungsdaten für den Vergleich mit entsprechenden Daten eines fraglichen zweiten Bildes, um festzustellen, ob das zweite Bild das gleiche oder unterschiedlich von dem Ausgangsbild ist. Dieser Vorgang des Markierens und des Erzeugens von Authentifizierungsdaten geschieht insgesamt während des Aufnehmens und bevor irgendwelche Bilddaten in einem Medium gespeichert werden, von welchem einer Person anschließend Daten zugänglich wären. Die Kamera nimmt dann die Authentifizierungsdaten und speichert sie gemeinsam mit den Daten des markierten Bildes in einem Speicher für die anschließende Übertragung an den Hostcomputer. Die bevorzugte Ausführungsform der Authentifizierung begreift das Erzeugen eines Kontrollsummenwertes ein, was das Hinzufügen von Pixelwerten aus jeder Bildzeile und jeder Bildspalte mit umfasst. Diese Summen werden dann in einer Nachschlagetafel für zukünftige Verwendung beim Vergleichen mit dem Resultat der gleichen Kontrollsummenberechnung gespeichert, die mit einem fraglichen Bildwert in zukünftiger Zeit vorgenommen wird. Das Ausgangsbild kann man nur beim Vorlegen des Passwortes betrachten.

[0014] Ein Vorteil der vorliegenden Erfindung besteht darin, dass die Authentifizierungsdaten während eines Vorgangs der Aufnahme des Bildes innerhalb einer Kamera erzeugt werden, bevor irgendeine Möglichkeit zum Manipulieren mit den Bilddaten besteht.

[0015] Ein weiterer Vorteil der vorliegenden Erfindung besteht darin, dass ein Ausgangsbild während des Vorgangs der Aufnahme innerhalb der Kamera markiert wird, bevor irgendeine Möglichkeit zum Anschauen des Bildes besteht.

[0016] Ein weiterer Vorteil der vorliegenden Erfindung besteht darin, dass ein Ausgangsbild nur durch das Vorlegen eines Passwortes angesehen werden kann, was es für eine unautorisierte Person praktisch unmöglich macht, das Ausgangsbild zu sehen. Die Möglichkeit zum Entziffern oder zum Eliminieren der Marke ist nur durch das technische Raffinement der Verschlüsselungsverfahren und durch die Komplexität der Authentifizierungsverfahren begrenzt.

[0017] Ein anderer Vorteil der vorliegenden Erfindung besteht darin, dass sie markierte, gesicherte Bilder zur Verfügung stellt, die für die Verkaufsförderung eingesetzt werden können und dabei Bedenken hinsichtlich nicht autorisierter Verwendung minimieren.

In den Zeichnungen

[0018] Fig. 1 stellt ein Kamerasystem gemäß der vorliegenden Erfindung dar;

[0019] Fig. 2 ist ein Blockschema von größeren Kamerateilen;

[0020] Fig. 3 ist ein detailliertes Blockschema des

Systems aus Fig. 1 entsprechend der vorliegenden Erfindung;

[0021] Fig. 4 ist eine Bitmap-Veranschaulichung eines digitalen Bildes, das mit einer Digitalkamera aufgenommen wurde;

[0022] Fig. 5 ist eine Veranschaulichung des digitalen Bildes aus Fig. 4 mit einem darüber gelegten Wasserzeichen mit 50% Lichtundurchlässigkeit;

[0023] Fig. 6 ist eine Veranschaulichung des digitalen Bildes aus Fig. 4 mit einem weißen Wasserzeichen;

[0024] Fig. 7 ist eine Veranschaulichung des digitalen Bildes aus Fig. 4 mit einem insgesamt schwarzen Zeichen;

[0025] Fig. 8 ist eine Veranschaulichung des digitalen Bildes aus Fig. 4 mit einem "negativen" Zeichen.

[0026] Fig. 9 demonstriert die Erzeugung einer Markierung;

[0027] Fig. 10 ist eine Veranschaulichung eines vereinfachten Feldes aus dreifarbigen Pixeldaten;

[0028] Fig. 11 ist eine Tabelle, die die Umwandlung von Bilddaten in modifizierte Bilddaten unter Verwendung einer Kennung zeigt;

[0029] Fig. 12 ist eine vereinfachte Veranschaulichung der mit einer Kennung modifizierten Bilddaten aus Fig. 9;

[0030] Fig. 13 ist ein Blockschema, das den Vorgang des Umwandelns von Bilddaten in durch eine Kennung modifizierte Daten zeigt;

[0031] Fig. 14 ist ein Blockschema, das weitere Details des Vorgangs zeigt, die in die Authentifizierung des Blockes **82** aus Fig. 3 involviert sind;

[0032] Fig. 15 ist ein Blockschema, das ein Verfahren zum Erzeugen einer Kontrollsumme veranschaulicht;

[0033] Fig. 16 zeigt ein Ausgangsbild, das in Gruppen von Zeilen und Spalten mit angemerkten Authentifzierungsdaten unterteilt ist; und

[0034] Fig. 17 zeigt ein verändertes Bild, das in Gruppen von Zeilen und Spalten mit angemerkten Authentifizierungsdaten unterteilt ist.

Beschreibung einer bevorzugten Ausführungsform

[0035] Unter Bezugnahme auf Fig. 1 der Zeichnung zeigt diese eine Veranschaulichung des Betriebes einer Kamera und eines Systems entsprechend der vorliegenden Erfindung. Vorhanden sind eine Kamera **10**, ein Zentralrechner (Hostcomputer) **12** und ein Drucker **14**. Verschiedene Kommunikationseinrichtungen zwischen der Kamera **10** und dem Computer **12** sind gezeigt, einschließlich einer Kabelanordnung **16**, die die Kamera **10** und den Computer **12** über Verbinder **18** und **20** miteinander verbindet. Die Kommunikation kann auch unter Verwendung eines scheibenförmigen Informationsträgers **22** vorgenommen werden, beispielsweise einer PCMCIA-Karte zur Verwendung mit Karten-/Scheiben-/Schlitzen **24**, **26**. Auch ausgestrahlte Signale können für die Kommunikation verwendet werden, wie dies durch Übertragungselemente **28**, **30** angedeutet ist. Außerdem kann Information auch zusätzlich durch Verbindungen **32**, **34** zu einem Modem für eine Übertragung durch ein Telefonsystem übermittelt werden. Der Computer **12** ist dargestellt, wie er mit dem Drucker **14** über eine Kabelanordnung **36** und Verbinder **38**, **40** verbunden ist.

[0036] Die Kamera ist für eine nicht zerstörende Markierung eines Ausgangsbildes aufgebaut und angeordnet, sowie zum Erzeugen von Bildauthentifizierungsdaten aus einem Ausgangsbild. Der gesamte Systemvorgang beginnt mit der Erzeugung einer Kennung und eines Passwortes durch die Verwendung des Zentralrechners (Hostcomputers) **12**. Die Kennung und das Passwort werden in die Kamera geladen, wo die Kennung durch die Kamera in Kombination mit einer vorbestimmten Formel verwendet wird, um Ausgangsbilddaten zu modifizieren, das heißt, das Ausgangsbild so zu markieren, dass es eine unautorisierte Verwendung hindert. Die Kennung und das Passwort werden in die Kamera **10** durch eine der oben erörterten Kommunikationsverfahren geladen. Nach der Annahme des Passwortes und der Kennung und in Abhängigkeit von einer Betätigung durch den Benutzer nimmt die Kamera **10** ein Bild auf und erzeugt Ausgangsbilddaten, die dann als Teil des Aufnahmevorgangs in Daten eines markierten Bildes modifiziert werden, entsprechend der von dem Hostcomputer zugeführten Kennung und einer vorbestimmten Formel. Die Kennung und die Formel können dann verschlüsselt und in einem Bildkopf für die spätere Übertragung zu einem Hostcomputer zur Verwendung in der Rekonstruktion des Ausgangsbildes nach der Vorlage eines Passwortes verwendet werden. Alternativ kann eine Markierungsnachschlagetafel vorbereitet werden, die die Adresse und die Pixelfarbwerte für jedes Pixel enthält, das gemäß der Kennung ersetzt worden ist. Diese Tabelle kann dann wie in dem Bildkopf gespeichert, verschlüsselt werden, um später in einen Hostcomputer zur Rekonstruktion des Ausgangsbildes nach Vorlage eines Passwortes geladen zu werden.

[0037] Die Kamera **10** erzeugt außerdem Bildauthentifizierungsdaten, die in einer bevorzugten Aus-

führungsform eine Kontrollsumme sind, die aus Daten in der Form einer Kontrollsummennachschlagetafel (Look up table LUT) bestehen. Die Authentifizierungsdaten werden aus den Ausgangsbilddaten zum Zweckes des Vergleiches mit und zum Beweisen der Authentizität von einem beliebigen fraglichen späteren Bild, das heißt von zweiten Bilddaten erzeugt. Die Authentifizierungsdaten und die Kennung und die Formel (oder die Markierungsnachschlagetafel) werden dann durch die Kamera **10** verschlüsselt, um verschlüsselte Authentifizierungsdaten und eine verschlüsselte Kennung und Formel (oder eine verschlüsselte Nachschlagetafel) zu bilden, welche als "Kopf' an die Daten des markierten Bildes angeschlossen werden, und nach einem Befehl eines Benutzers werden sie mit den Daten des markierten Bildes auf den Hostcomputer **12** geladen.

[0038] Es gibt viele Wege, Authentifizierungsdaten aus Ausgangsbilddaten zu erstellen. Die ganzen oder Teile der Bilddaten können gemäß einem weiten Bereich von Formeln modifiziert werden und die Ergebnisse können zum Vergleich mit entsprechenden Daten eines fraglichen Bildes gespeichert werden, um festzustellen, ob es das gleiche oder ein unterschiedliches zum Ausgangsbild ist.

[0039] Der Geist der vorliegenden Erfindung schließt alle diese vielen Wege ein, die einem Fachmann klar sein werden.

[0040] Nach dem Erhalt der verschlüsselten Authentifizierungsdaten, der verschlüsselten Kennung und der Formel (oder der verschlüsselten Nachschlagetafel) und der Daten des markierten Bildes auf dem Hostcomputer kann ein Benutzer das markierte Bild ausdrucken oder es speichern oder es anzeigen. Nach der Eingabe des Passwortes kann ein Benutzer den Computer erfolgreich anweisen, die Markierung zu entfernen und das Ausgangsbild anzuzeigen. Die Authentifizierungsdaten werden durch den Hostcomputer verwendet, um festzustellen, ob ein fragliches zweites Bild das gleiche wie das Ausgangsbild ist. Um dies vorzunehmen, führt der Hostcomputer eine Authentifizierungsdaten-berechnung mit dem zweiten Bild durch und vergleicht die sich ergebenden zweiten Authentifizierungsdaten mit den (ersten) Authentifizierungsdaten des Ausgangsbildes. Der Vorgang der Authentifizierung der Daten der bevorzugten Ausführungsform (Kontrollsummenbildung) wird ebenso zeigen, wo sich zwei Bilder unterscheiden. Dies wird in den folgenden Beschreibungen mit den verschiedenen Figuren der Zeichnung vollständig erklärt werden.

[0041] Fig. 2 zeigt ein Blockschema der größeren Betriebsabschnitte einer Digitalkamera. Diese schließt eine Bildaufnahmevorrichtung **44** in Verbindung über einen Bus **46** mit einem Prozessor **48** ein. Der Prozessor speichert über einen Bus **52** Daten in einem Speicher **50**, der auch einen ROM-Speicher für grundsätzliche Vorgänge einschließt. Die Eingabe und die Ausgabe von Daten wird durch eine der oben beschriebenen verschiedenen Einrichtungen vorgenommen, einschließlich einer Kabelverbindung **54** über einen Bus **56**, einen Karten-/Scheiben-Schlitz **58** über einen Bus **60**, einen Übermittler **62** über einen Bus **64**, oder eine Modemverbindung (nicht in Fig. 2 dargestellt). Steuerungen **42** sind mit dem Prozessor über einen Bus **56** verbunden gezeigt.

[0042] Die Bildaufnahmevorrichtung **44** schließt Komponenten ein, die für Fachleute gut bekannt sind und nicht im Detail gezeigt werden müssen, um die Erfindung durchzuführen. Die Aufnahmevorrichtung **44** schließt eine optische Bildaufnahme ein, wie beispielsweise einen Ladungstransportspeicher (charged coupled device CCD) und einen Analog/Digital-Schaltkreis zum Umwandeln der analogen CCD-Signale in eine digitale Form für den Prozessor **48**.

[0043] Die Ausgangsbilddaten werden vorübergehend in Registern gespeichert, beispielsweise im Prozessor **48**, und in Inkrementen zugegriffen und verarbeitet. Die Register sind sicher und stellen keine Langzeitspeicherung oder einen bleibenden Speicher zur Verfügung, der für eine Person zugänglich wäre, um die Inhalte herauszuziehen. Die Kamera zieht die Daten aus den Registern und wandelt sie unter Verwendung der Kennung und der Formel in markierte Bilddaten (Daten eines markierten Bildes) um, und wie bereits erwähnt, wird alternativ eine Markierungsnachschlagetafel mit den Adressen und den Farbwerten der durch die Markierung modifizierten Pixel des Ausgangsbildes erzeugt. Die Nachschlagetafel (oder die Kennungsformel) ist dann verschlüsselt und in dem Speicher abgelegt. Gemäß der vorstehenden Beschreibung wird das Platzieren einer Markierung auf einem Bild in einer kontinuierlichen Folge/Vorgang vorgenommen, der sauber als Teil des Bildaufnahmevorganges beschrieben werden kann. Die Daten des markierten Bildes und die verschlüsselte Nachschlagetafel (oder die verschlüsselte Kennung) werden dann in dem Speicher **50** niedergelegt.

[0044] In ähnlicher Form werden die Ausgangsbilddaten in Inkrementen aus dem Register herausgezogen, um Authentifizierungsdaten zu erzeugen, die dann verschlüsselt werden, um verschlüsselte Authentifizierungsdaten zu bilden. Die sicher verschlüsselten Authentifizierungsdaten werden dann in dem Speicher **50** niedergelegt. Die verschlüsselten Authentifizierungsdaten, die verschlüsselte Nachschlagetafel (oder die verschlüsselte Kennung und Formel) werden dann in einem "Kopf" zu den Daten des markierten Bildes platziert, die dann in den Hostcomputer geladen werden können, wo das markierte Bild betrachtet werden kann und nach der Vorlage eines

Passwortes auf die Markierungsnachschlagetafel (oder die Kennung und die Formel) zugegriffen werden kann und das Ausgangsbild wieder hergestellt und betrachtet werden kann.

[0045] Die verschlüsselten Authentifizierungsdaten sind ähnlich zugänglich nach Vorlage eines Passwortes, um die Auswertung eines fraglichen Bildes zu erlauben, um festzustellen, ob es das gleiche wie das Original ist. Alternativ können die Authentifizierungsdaten an den Hostcomputer in unverschlüsselter Form übertragen werden, ohne dass ein Passwort für die Verwendung erforderlich ist.

[0046] Unter Bezugnahme auf Fig. 3 wird ein detaillierteres Blockschema des von der Kamera und dem System aus Fig. 1 durchgeführten Vorganges veranschaulicht. Gemäß einem Block **68** wird ein Hostcomputer mit einer "Set up"-Software geladen, die es einem Benutzer erlaubt, eine Markierung und eine korrespondierende Kennung (Block **70**) und ein Passwort (Block **72**) zu erzeugen. Diese Information wird entweder gesichert (Block **74**) und später geladen (Block **76**), oder direkt in die Kamera **10** geladen (Block **76**, **78**). Der Block **80** zeigt die Annahme des Passwortes durch die Kamera wie auch die Aktivierung der Kamera durch den Benutzer und den anschließenden Bildaufnahmevorgang einschließlich des Umwandelns der analogen Bilddaten in digitale Daten. Block **82** schließt die Vorgänge des Umwandelns der Ausgangsbilddaten gemäß der Kennung (Kennungsdaten) ein, um die Markierung auf dem Ausgangsbild zu platzieren, das heißt, um markierte Bilddaten zu bilden. Der Block **82** schließt auch die Verschlüsselung der Kennung und der Formel ein, das Erzeugen der Markierungsnachschlagetafel und einer verschlüsselten Markierungsnachschlagetafel und schließt den Vorgang des Erzeugens von Bildauthentifizierungsdaten aus einem Ausgangsbild ein. Die Authentifizierungsdaten werden aus den Ausgangsbilddaten zur Verwendung beim Vergleichen mit der gleichen Berechnung von entsprechenden Daten einer fraglichen anschließenden oder das heißt, zweiten Bilddaten berechnet, um festzustellen, ob die anschließenden Bilddaten die gleichen wie die Ausgangsdaten sind. Die bevorzugte Ausführungsform der Authentifizierungsdaten ist eine Kontrollsumme, die aus einer Tafel enthaltend die Summe von Daten aus jeder Zeile und Spalte der Ausgangsbilddaten besteht. Block **82** schließt auch die Verschlüsselung von Authentifizierungsdaten ein, um verschlüsselte Authentifizierungsdaten zu erzeugen.

[0047] Block **84** zeigt den Vorgang des Sicherns der verschlüsselten Authentifizierungsdaten, der markierten Bilddaten und der verschlüsselten Markierungsnachschlagetafel. Die verschlüsselten Authentifzierungsdaten und die verschlüsselte Nachschlagetafel (oder die verschlüsselte Kennung und die Formel) können als Kopf an den Daten des markierten Bildes platziert werden. Der Block **86** zeigt den Vorgang des Übertragens der Daten auf den Hostcomputer.

[0048] Wenn die vorgenannten Daten auf den Computer übertragen sind, kann der Benutzer das markierte Bild (Blocks **88**, **90**) anzeigen, drucken oder speichern. Nach der Eingabe des Passwortes (Block **92**) kann die Markierung entfernt werden (Block **94**) und das Ausgangsbild kann gedruckt, angezeigt oder gespeichert werden (Block **96**). Der Benutzer kann auch die Authentifizierungsdaten mit den Authentifizierungsdaten eines anschließenden Bildes (Block **98**) vergleichen, um festzustellen, ob das anschließende Bild sich vom Original unterscheidet.

[0049] Fig. 4 veranschaulicht das Konzept eines digitalen Bildes **100** als ein Feld von Pixeln (Bildelementen) **102**, wobei jedes Quadrat ein Pixel repräsentiert. In dieser Figur wird jedes Pixel als eine "Bitmap" dargestellt, das heißt, entweder als "ein" (weiß) oder als "aus" (schwarz). Tatsächlich repräsentiert im Falle der Farbfotografie wie in den folgenden Figuren beschrieben jedes Pixel drei Ausgaben, jeweils eine für Rot, Blau und Grün, wobei jede Ausgabe mehrere Niveaus (beispielsweise 256 Schattierungen für jede Farbe) zur Verfügung stellt.

[0050] Die Quadrate in der Fig. 4 sind zur Erleichterung der Darstellung groß. In ähnlicher Form zeigt Fig. 5 das Konzept, eine Markierung auf einem Bild anzuordnen, um Daten **104** eines markierten Bildes zu erzeugen, was als Lichtundurchlässigkeit von 50% dargestellt ist. In diesem Fall ist ein "C im Kreis" (Copyright) gefolgt von einer "9" und einer "6" auf dem Ausgangsbild aufgebracht, um Daten **104** eines markierten Bildes zu erzeugen. Eine derartige Markierung wird üblicherweise als ein "Wasserzeichen" bezeichnet. In ähnlicher Form veranschaulicht Fig. 6 eine insgesamt weiße Markierung, Fig. 7 veranschaulicht eine insgesamt schwarze Markierung, und Fig. 8 repräsentiert eine negative Markierung. Die Tabelle der zur Umwandlung aus den Ausgangdaten in die markierten Daten verwendeten Umwandlungselemente wird als "Kennung" bezeichnet, die Elemente bearbeiten den roten, grünen und blauen Inhalt eines jeden Pixels und die Pixellichtundurchlässigkeit.

[0051] Die Kennung kann erzeugt werden, um eine Markierung vorzusehen, die insgesamt schwarz, insgesamt weiß, eine Schattierung dazwischen ist, oder jedes Pixel der Markierung kann ein Negativ der Ausgangspixeldaten sein, ebenso wie viele andere Umwandlungen, beispielsweise einschließlich der Multiplizierung von Farben, die für Fachleute klar sein wird.

[0052] Die Fig. 5 und Fig. 6 veranschaulichen beispielsweise die gleiche grundsätzliche Markierung

(Wasserzeichen) mit den gleichen Grundfarben (weiß) und unterschiedlicher Lichtundurchlässigkeit. In Fig. 5 ist das Wasserzeichen zu 50% lichtundurchlässig, während es in der Fig. 6 vollständig lichtundurchlässig ist. Die Grundfarbe ist hier die Farbe der Markierung, die beispielsweise wie in der Fig. 6 insgesamt weiß oder wie in der Fig. 7 insgesamt schwarz sein kann. Fig. 8 veranschaulicht eine Alternative zu diesem Verfahren, in welcher das Wasserzeichen als ein Negativ des Bildes bei 100%-iger Lichtundurchlässigkeit definiert wird.

[0053] Fig. 9 veranschaulicht die verschiedenen Dinge, die bei der Erzeugung einer Kennung gebildet werden müssen, aus welcher die Kamera gemeinsam mit der Formel die Markierung erzeugt, wie im Folgenden vollständig erörtert werden wird. Ein Text **106**, Zeichnungen **108**, eine Positionierung **110** und eine Lichtundurchlässigkeit **112** müssen als Information festgelegt werden. Die Textinformation schließt die Auswahl aus der Drucktype **114**, der Größe **116**, der Farbe **118** und die Auswahl einer Textzeile **120** ein. Die Zeichnungsinformation **108** schließt die Auswahl aus einer Bitmap **122**, einer Größe **124** und einer Farbe **126** ein. Die Positionierung **110** benötigt die Festlegung der Koordinaten **128** und der Orientierung **130** der Markierung auf dem Ausgangsbild. Die Lichtundurchlässigkeit **112** begreift die Feststellung ein, welcher Prozentsatz **132** einer jeden Ausgangsbildpixelfarbe oder, das heißt Schattierung modifiziert werden soll. Eine 100%-ige Änderung bedeutet, dass keine Ausgangsbilddaten erhalten bleiben. Die Grundfarbe (**134**) bedeutet, die Farbe der Markierung, oder beispielsweise alles weiß (wie in Fig. 6), alles schwarz (Fig. 7) oder ein Negativ (Fig. 8).

[0054] Der Block **136** zeigt das Erfordernis an, dass die zu modifizierenden Pixel in ein Feld oder eine Nachschlagetafel zu bringen sind, welche Vorgehensweise auch als "Rastern" bezeichnet werden kann.

[0055] Die Vorbereitung der Kennung und ihre Verwendung beim Erzeugen von Daten eines markierten Bildes kann vielleicht am besten mit einem übermäßig vereinfachten Beispiel erläutert werden, das leicht dargestellt werden kann. Nehmen wir an, dass das Feld aus der Fig. 10 die Ausgangsbilddaten darstellt, die aus einem 4 × 4 Feld aus 16 Pixeln bestehen. Die X-Koordinaten **140** und die Y-Koordinaten **142** eines jeden Pixels werden vermerkt und den Pixeln werden Nummern **144** von 1 bis 16 gegeben, die in der oberen linken Ecke eines jeden Quadrates positioniert werden, welches ein Pixel repräsentiert. Ein Satz aus drei Farbziffern wird in jedem Quadrat platziert, das die Farbe des Pixels angibt. Die erste Ziffer zeigt die Intensität des roten Inhalts, die zweite des grünen und dritte des blauen an.

[0056] Um eine Markierung auf dem in Fig. 10 wiedergegebenen Bild zu platzieren, wird eine Kennung von dem Hostcomputer empfangen und zusammen mit einer Formel oder einer Umwandlungsgleichung benutzt, um einen neuen Satz an Farbziffern zu berechnen.

[0057] Die Formel und die Kennung können von verschiedener Art sein und jede Art kann potentiell verwendet werden, um eine beliebige Anzahl unterschiedlicher Markierungen zu bekommen. Eine der einfachsten davon wäre es, eine erste Nachschlagetafel auf dem Hostcomputer vorzubereiten, die die Adresse, die Farbwerte und die Lichtundurchlässigkeit für jedes Pixel der Markierung enthält. Die Kamera kann dann einfach die entsprechenden Ausgangsbildpixelwerte und die der Markierung ersetzen und eine Markierungsnachschlagetafel erzeugen, die die Werte der Ausgangsbilddaten für die Pixel in der Markierung enthält. Die Markierungsnachschlagetafel könnte wie oben erläutert dann verschlüsselt und als ein Kopf an den Daten des markierten Bildes platziert werden. In einem derartigen einfachen Fall könnte die Kennung die Werte der Pixel in der Markierung darstellen und die Umwandlungsgleichung würde einfach die Farbwerte der Pixel in der Markierung mit denen der Kennung/Markierung gleichsetzen. Eine kompliziertere Umwandlung kann ebenfalls verwendet werden, sowie die in der Fig. 11 veranschaulichte, in welcher die Spalte **148** die Pixelzahl angibt, die Spalte **150** die Pixelkoordinaten angibt und die Spalte **152** die Kennungsziffern **154** angibt, wobei die Ziffern symbolisch durch die Buchstaben Rd, Gd, Bd und Op dargestellt werden. Diese Ziffern werden in einer Umwandlungsgleichung (Formel) verwendet, um auf jedes Pixel des Ausgangsbildes angewandt zu werden, um Daten eines markierten Bildes zu erzeugen. Die gleichen Ziffern und die Gleichung können später durch den Hostcomputer verwendet werden, um nach Erhalt des korrekten Passwortes die Ausgangsbilddaten aus den Daten des markierten Bildes zu errechnen. Rd ist eine Ziffer, die zur Berechnung des roten Inhalts des markierten Bildes verwendet wird, und Gd und Bd werden in ähnlicher Weise für grün und blau verwendet. Der Wert Op ist eine Ziffer, die die Lichtundurchlässigkeit angibt, das heißt, wie viel von der Ausgangsbildfarbe erlaubt wird, in dem speziellen Pixel erhalten zu bleiben. Alternativ kann eine komplizierte Formel verwendet werden, um die Markierung zu erzeugen, und eine einfache Nachschlagetafel kann verwendet werden, um diese zu entfernen oder umgekehrt. Außerdem kann das Wasserzeichen oder seine Formel innerhalb der Bilddaten versteckt werden. Alle diese Möglichkeiten fallen in den Bereich des Konzeptes für Kennung und Formel/Gleichung und sind in der vorliegenden Erfindung enthalten.

[0058] Eine komplizierte Umwandlungsgleichung kann eine größere Sicherheit schaffen. Um den Code zu "knacken" müsste eine Person in irgendeiner

Form sowohl die Umwandlungsnachschlagetafel als auch die Formel/Umwandlungsgleichung ermitteln. Der Geist der vorliegenden Erfindung schließt jede Kombination aus Umwandlungstafelziffern und Umwandlungsgleichung ein. Die spezielle Umwandlungsgleichung, die in der Fig. 11 verwendet ist, lautet:

Rt = Rundungswert (der kleinere Wert von {255, (Ri + Rd) × Op})

[0059] Der Prozessor **48** verwendet die Gleichung (Formel) und die Kennungswerte in der Umwandlungs-LUT (Spalte **152**) aus Fig. 11, um diese auf die Ausgangsbilddaten aus Fig. 10 anzuwenden, die in der Spalte **154** in Fig. 11 aufgelistet sind, um die Daten des markierten Bildes zu berechnen, die in der Spalte **156** in Fig. 11 aufgelistet sind. Zur Vollständigkeit der Beschreibung sind diese modifizierten Daten in Feldform in der Fig. 12 dargestellt, wobei die Pixeldaten die gleichen wie in der Fig. 10 sind, abgesehen dort, wo sie durch die Umwandlungsgleichung und die Kennung in den Pixeln 6, 10 und 11 modifiziert sind. Zum leichteren Vergleich sind diese in der Fig. 11 in der Spalte **156** aufgelistet, die zeigt, dass die einzigen modifizierten Pixel die Nummern 6, 10 und 11 sind, die eine L-förmige Markierung im Ausgangsbild bilden.

[0060] Das Blockschema aus Fig. 13 fasst ein bevorzugtes Verfahren zum Erzeugen der Daten des markierten Bildes zusammen, in welchem der Prozessor nur auf diejenigen Pixel wirkt, die als Teil der Markierung angezeigt sind. Beispielsweise wären im Falle der Fig. 10 bis Fig. 12 die einzigen Pixel in der Umwandlung LUT die Pixel 6, 10 und 11 der "L"-Markierung. In der Fig. 13 zeigt der Block **158** den Prozessor **48**, wie er ein "Passwort" erhält, das sofern korrekt die Umwandlungstätigkeit beginnt. Der Block **158** zeigt auch die Eingabe der Ausgangsbilddaten und der Kennung LUT an. Entsprechend dem Block **160** wird ein Pixel in der Kennung (der Markierung in ihrer bevorzugten Ausführungsform) ausgewählt und durch den Block **162** wird auf die entsprechenden Bildfarbdaten zugegriffen. Der Block **164** zeigt dann den Ersatz der Ausgangsbilddaten Ri, Gi, Bi durch die Daten Rt, Gt, Bt des markierten Bildes an. Der Vorgang wird dann wiederholt, bis alle Pixel in der Markierung/Kennung ersetzt sind; die Wiederholung wird durch den Pfeil **166** angezeigt. Obwohl das einfache Beispiel eine Markierung verwendet (das durch die Pixel 6, 10, 11 gebildete "L"), kann die Kennung so vorbereitet werden, dass sie mit jedem Prozentsatz von Pixeln aus dem Ausgangsbild arbeitet, einschließlich von 100% von diesen, um jede gewünschte Modifizierung der Ausgangsbilder zu erzeugen, und dieses ist in der vorliegenden Erfindung eingeschlossen.

[0061] Die Gesamtvorgänge der durch den Block **82** in der Fig. 3 gekennzeichneten Bildauthentifizierung werden noch vollständiger in dem Blockschemabild in der Fig. 14 beschrieben. Die erforderlichen Eingaben werden im Block **168** vermerkt und schließen das Bild ein, aus dem die Bilddaten erzeugt werden, das Passwort, und die Kennung oder die Kennung LUT. Der Block **170** hat mit der Erzeugung der durch die Kennung modifizierten Bilddaten zu tun. Die Kennung wird dann als Teil des Sicherheitsvorganges verschlüsselt (Block **172**), da die Kennung zusammen mit der Umwandlungsgleichung für die Umwandlung des Bildes aus dem Original in die modifizierte (markierte) Form und zurück erforderlich ist.

[0062] Das Passwort (Block **168**) wird ebenso benötigt, um den Vorgang der Entschlüsselung der verschlüsselten Kennungsnachschlagetafel (LUT) zu starten, wenn das Ausgangsbild durch die Verwendung auf dem Hostcomputer wieder gespeichert werden soll.

[0063] Der Block **174** aus der Fig. 14 schließt die Erzeugung von Authentifizierungsdaten ein, die ein Satz von Daten sind, der aus den Ausgangsbilddaten berechnet und als Authentifizierungsnachschlagetafel beiseite gesetzt ist, um mit einem anschließenden Bild als eine Überlagerung verglichen zu werden, um für mögliche Änderungen an dem Ausgangsbild geprüft zu werden. Die Authentifizierungsdaten können ebenfalls verschlüsselt werden, wie dies durch den Block **176** vermerkt ist, oder sie können alternativ auch ohne eine Verschlüsselung an den Hostcomputer übertragen werden. Die verschlüsselten oder nicht verschlüsselten Authentifizierungsdaten und die verschlüsselte Kennung werden dann in einer Datei als Kopf für die Daten des markierten Bildes platziert. Dies ist in den Blöcken **178** und **180** vermerkt, und das "Zurückgeben" in Block **180** zeigt das Sichern "innerhalb der Kamera" (Block **84** aus Fig. 3) und/oder das Übertragen an einen Hostcomputer (Block **86** aus Fig. 3) an.

[0064] Das Erzeugen von Authentifizierungsdaten kann auf viele Weise geschehen. Komplexere Verfahren sichern eine dichtere Sicherheit und minimieren die Zufallsmöglichkeit eines geänderten Bildes, das nicht durch die Authentifizierungsdaten angezeigt wird. Wie die Umwandlungsgleichung schließt der Geist der Erfindung die vielen Wege zur Erzeugung der Authentifizierungsdaten ein. Die grundsätzliche Idee ist es, die ganzen oder Teile der Bilddaten zu verschlüsseln oder diese in irgendeiner Form zu modifizieren und sie für eine zukünftige Bezugnahme zu speichern, um sie mit den Ergebnissen der gleichen Berechnung zu vergleichen, die auf einem späteren Bild vorgenommen werden, um zu sehen, ob das spätere Bild das gleiche oder ein anderes als das Original ist.

[0065] Die bevorzugte Ausführungsform der Au-

thentifizierungsdaten besteht in Kontrollsummendaten, die durch das einfache Addieren der Farbziffern von ausgewählten Gruppen aus Zeilen und Spalten der Ausgangsbilddaten vorbereitet werden, und das Speichern dieser Werte in einer LUT zum Vergleich mit den Ergebnissen des gleichen Additionsvorgangs, das mit einem fraglichen Bild vorgenommen wird, um mit dem Original verglichen zu werden. Die Zahl der Zeilen in einer bestimmten Gruppe kann eins oder mehr betragen, und jede Gruppe kann entweder die gleiche Zahl von Zeilen oder eine unterschiedliche Zahl besitzen. Eine besondere Ausführungsform einer Kontrollsummenberechnung ist als Blockschemabild in Fig. 15 veranschaulicht, die eine Reihe von Blöcken **182** zum Addieren von Pixelfarbwerten in Zeilen von Pixeln zeigt, um horizontale Kontrollsummen zu erzeugen und eine Reihe von Blöcken **184** zum Addieren von Pixelfarbwerten von Spalten von Pixeln, um vertikale Kontrollsummen zu erzeugen. Der Buchstabe "n" in der Fig. 15 wird verwendet, um die Zahl einer Spalte anzugeben. Der Buchstabe "m" wird verwendet, um die Zahl einer Zeile anzugeben. Das m-te Pixel in einer Spalte "n" wird als Y_{mn} angegeben. In ähnlicher Form wird das n-te Pixel in der Zeile m als X_{mn} bezeichnet. Die Verwendung von sowohl X als auch Y zum Identifizieren eines Pixels dient zum Unterscheiden zwischen einer Zeilenaddition gegenüber einer Spaltenaddition. Tatsächlich ist das Pixel X_{mn} das gleiche wie das Pixel Y_{mn}, beispielsweise ist X_{23} das Pixel in der 2. Zeilen nach unten und in der 3. Spalte nach rechts, was das gleiche Pixel ist wie X_{23}, welches das Pixel in der 3. Spalte nach rechts und der 2. Zeile nach unten ist. Die Gesamtzahl an Zeilen (die Bildhöhe) wird als MM bezeichnet und die Gesamtzahl an Spalten (Bildbreite) wird mit NN bezeichnet. In dem Beispiel aus Fig. 15 schreitet der Vorgang vertikal um die Ziffer M, das heißt, jede M-te Reihe wird ausgewählt und er schreitet horizontal um die Ziffer N, das heißt jede N-te Spalte wird ausgewählt.

[0066] Eine detaillierte Beschreibung der Erzeugung der vertikalen Kontrollsummen wird nunmehr gegeben. Der Block **186** gibt das Setzen des Spaltenindikators "n" auf Null. Eine große Schleife wird dann durch den Entscheidungsblock **188**, den Entscheidungsblock **202** und die Wiederholungsschleife (Return) **204** angezeigt. Der Block **188** und die Wiederholungsschleife (Return) **204** zeigen an, dass der Vorgang solange fortgesetzt wird wie n kleiner ist als die Gesamtzahl der Spalten NN. Jeder Umlauf rund um die Schleife verarbeitet eine weitere Spalte, wie dies durch den Block **202** angezeigt wird, der die Spaltenziffer n auf "n + N" setzt, also um N inkrementiert. N kann eine ausgewählte Zahl sein, die größer oder gleich 1, aber kleiner als NN ist. Kleinere Werte von N geben eine feinere Auflösung und ergeben eine genauere Kontrollsumme. Der Block **190** setzt die Zeilenzahl m und die gesamte Kontrollsumme S für die Spalten auf 0. Die Blöcke **192** bis **198** und die Wiederholungsschleife (Return) **199** geben das Addieren der Farbwerte eines jeden ausgewählten Pixels in der Spalte n an, wenn das spezielle Pixel Y_{mn} in der Spalte durch Inkrementieren der Zeilenzahl m um den Inkrementwert M ausgewählt ist. Der Block **192** zeigt an, dass die Schleife fortgesetzt wird, bis die Zeile m größer oder gleich MN ist. Der Block **194** zeigt, dass das spezielle Pixel Y_{mn} addiert wird, und der Block **196** zeigt die aktuelle Addition des neuen Pixelwertes Y_{mn} zur Summe S an. Dieser Vorgang wird für jeden der drei Farbwerte vorgenommen, wobei die Zahl den Vorgang für jede Farbe angibt. Der Block **198** inkrementiert das nächste ausgewählte Pixel in der Spalte durch Inkrementieren der Zeilenzahl m durch den Inkrementwert M. Der Pfad **199** zeigt die fortgesetzte Arbeitsweise der Blöcke **192** bis **198** bis die Zeilenzahl m größer oder gleich MM ist. An diesem Punkt wird die gesamte Kontrollsumme "Kontrollsumme (Yn) = S" für die Spalte n gespeichert oder verschlüsselt und gespeichert, welcher Vorgang durch den Block **200** angezeigt ist. Der Block **202** gibt dann die Auswahl der nächsten Spalte durch inkrementieren von n durch den Wert N an. Das Verfahren des in den Blöcken **196** und **216** angegebenen Summierens könnte eine weitere Definition erfordern. Ein bevorzugtes Verfahren des Aufsummierens schließt das Trunkieren ein, um die Größe der Zahlen zu begrenzen, wie dies in den Blöcken **196** und **216** angegeben ist. Beispielsweise bedeutet "Mod 256**"**, dass das Register bis 255 zählt und dann wieder zur "0" zurückkehrt, ähnlich wie das Dezimalsystem, das von 1 bis 9 zählt und dann wieder zur "0" zurückkehrt, und nur die letzte Zahl aufrechterhält. Beispielsweise wäre 256 mod 256 zugleich "0", 257 mod 256 wäre "1", 513 mod 256 wäre "1".

[0067] Die Berechnung der horizontalen Kontrollsummen durch die Blöcke **182** ist genau der gleiche Vorgang wie für die vertikalen Kontrollsummen, abgesehen davon, dass die Blöcke **206** bis **222** die passenden unterschiedlichen Zeilen- und Spaltenbezeichnungen wie für die Zeilenaddition angeben. Da diese Vorgehensweise andererseits die gleiche wie für die vertikale Vorgehensweise ist, ist eine detaillierte Wiederholung der Blockfunktionen hier nicht erforderlich.

[0068] Der Block **224** zeigt das Speichern der Kontrollsummen oder der verschlüsselten Kontrollsummen. In der bevorzugten Ausführungsform werden die Kontrollsummen oder verschlüsselten Kontrollsummen in einem Bildkopf platziert.

[0069] Alternativ oder zusätzlich zu dem Speichern der ausgewählten Zeilen und Spalten können die Gesamtfarbwertsummen für ausgewählte Pixel des gesamten Feldes addiert werden. Der sich ergebende Satz von drei Farbziffern (R, G, B) kann dann mit den entsprechenden Summen für ein fragliches/zweites Bild verglichen werden, um anzugeben, ob das zwei-

te Bild das gleiche wie das erste ist. Falls die Summen für die zwei Bilder unterschiedlich sind, beweist dies folgerichtig, dass das zweite Bild ein anderes als das erste ist. Andererseits, falls die Summen die gleichen sind, so ist dieser Test lediglich eine Anzeige dafür, dass keine Änderungen vorgenommen wurden und er ist nicht zwingend, da ein Pixel erhöht und ein anderes um den gleichen Betrag gesenkt worden sein könnte. Authentifizierungsdaten unter Einschluss von individuellen Zeilen- und Spaltensummen werden bevorzugt, da sie eine genauere Prüfung ergeben und auch erzählen können, wo ein bestimmter Defekt oder eine Änderung aufgetreten ist, wobei ein Defekt an einem Schnitt von einer Zeile und einer Spalte oder von Gruppen von Zeilen und Spalten die in Abweichung sind.

[0070] Wie vorstehend erörtert, können andere Berechnungsverfahren für Authentifizierungsdaten mit einem Originalbild vorgenommen werden, um Daten zu erzeugen, die ein Bild auf Authentizität prüfen können. Die verschiedenen Berechnungen werden für Fachleute klar sein, sie werden alle als Authentifizierungsdaten hierin unter Bezug genommen und in den Ansprüchen, abgesehen von der Beschreibung der bevorzugten "Kontrollsummen"-Ausführungsform.

[0071] Ein Verfahren zum Verwenden von Zeilen- und Spaltenauthentifizierungsdaten zum Auffinden des Ortes einer Bildveränderung wird in den Fig. 16 und Fig. 17 dargestellt. Das Verfahren schließt das Durchführen von Berechnungen gemäß einer vorbestimmten Formel auf Zeilen von Pixeln oder Gruppen von Zeilen und von Spalten von Pixeln oder Gruppen von Spalten ein. Beispielsweise zeigt Fig. 16 ein in Gruppen von Zeilen von Pixeln wie beispielsweise 228 und in Gruppen von Spalten von Pixeln wie beispielsweise 230 unterteiltes Ausgangsbild **226**. Aus jeder dieser Gruppen können Authentifizierungsdaten gewonnen werden. Die Berechnung kann in beliebiger Form wie vorstehend beschrieben durchgeführt werden und muss keine individuellen Zeilen oder Spalten von Pixeln innerhalb einer Gruppe einschließen. Außerdem müssen die Gruppen nicht von gleicher Größe sein.

[0072] Die sich ergebenden Authentifizierungsdaten können verwendet werden, um den Bereich einer Bildveränderung zu lokalisieren, die Genauigkeit der Lokalisierung hängt von der Größe der Gruppen ab. Die Kästen **232** längs der Oberseite und die Kästen **233** längs der linken Seite des Bildes enthalten die Zeilenziffern **234** und Spaltenziffern **236**. Die Ziffern **238** unterhalb der Zeilenziffern **234** bilden einen ersten Satz von Zeilenauthentifizierungsdaten, und die Ziffern **240** unterhalb der Spaltenziffern **236** bilden einen ersten Satz von Spaltenauthentifizierungsdaten.

[0073] Fig. 17 zeigt ein Bild **242**, welches das Bild **226** aus der Fig. 16 in einer geänderten Form ist. Der Ort der Veränderung kann durch einen Vergleich des zweiten Satzes der Zeilenauthentifizierungsdaten **244** mit einem ersten Datensatz **238** und eines zweites Satzes von Spaltenauthentifizierungsdaten **246** mit einem ersten Datensatz **240** beobachtet werden. Der Schnitt der Zeile des zweiten Satzes an Zeilendaten und einer Spalte des zweiten Satzes von Spaltendaten, die beide sich von den entsprechenden Zeilen aus dem ersten Satz von Zeilendaten und dem ersten Satz von Spaltendaten unterscheiden, bildet den Bereich **248** des Bildes, in dem eine Veränderung vorgenommen wurde. Im Beispiel in der Fig. 17 kann man erkennen, dass die Authentifizierungsdaten für die Spalte 603 des Originalbildes 147 beträgt, während die entsprechenden Authentifzierungsdaten für die Spalte 603 des geänderten Bildes 58 lauten. Ein Vergleich der Zeilendaten zeigt, dass die Daten für die Zeile 613 von 69 in 131 geändert wurden. Da die anderen Daten nicht geändert wurden, ist die Änderung auf den Bereich **248** beschränkt, der durch den Schnitt der Zeile 613 mit der Spalte 603 gebildet wird.

[0074] Obwohl vorstehend ein bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung beschrieben wurde, ist es verständlich, dass bestimmte Modifikationen oder Veränderungen für Fachleute klar sein werden.

[0075] Was beansprucht wird, ist:

Patentansprüche

1. Verfahren zur Authentifizierung eines Bildes unter Verwendung einer Digitalkamera mit folgenden Schritten:
(a) Initialisieren eines Authentifizierungssystems in der Digitalkamera mit einem von einem Benutzer programmierbaren Passwort für die Verschlüsselung;
(b) Aufnehmen von Ausgangsbilddaten mit der Digitalkamera;
(c) Erzeugen von ersten Authentifizierungsdaten aus den Ausgangsbilddaten mit dem Authentifizierungssystem innerhalb der Digitalkamera, wobei die ersten Authentifizierungsdaten für die Zwecke des Vergleiches mit aus zweiten Bilddaten erzeugten zweiten Authentifizierungsdaten dienen, um festzustellen, ob die zweiten Bilddaten identisch mit den Ausgangsbilddaten sind; und
(d) Verschlüsseln der ersten Authentifizierungsdaten mit dem Authentifizierungssystem innerhalb der Digitalkamera, um verschlüsselte erste Authentifizierungsdaten zu erzeugen und um die verschlüsselten ersten Authentifizierungsdaten zu den Ausgangsbilddaten als Ausgabe aus der Digitalkamera zuzuordnen, wobei die ersten Authentifizierungsdaten aus der Digitalkamera in unverschlüsselter Form unzugänglich sind und die Ausgangsbilddaten aus der Digitalkamera ohne ihre zugeordneten verschlüsselten ersten Authentifizierungsdaten unzugänglich sind.

2. Verfahren nach Anspruch 1, in welchem die ersten Authentifizierungsdaten die Daten einer Kontrollsumme sind.

3. Verfahren nach Anspruch 2, in welchem die Daten der Kontrollsumme durch das Addieren von Farbnummern aus ausgewählten Gruppen von Zeilen und Spalten aus den Ausgangsbilddaten, und durch das Speichern von Werten der Zeilen und Spalten der Ausgangsbilddaten in einer Nachschlagetafel vorbereitet werden.

4. Verfahren nach Anspruch 1, das zusätzlich aufweist:
(a) das Übertragen der verschlüsselten ersten Authentifizierungsdaten an ein externes Gerät;
(b) das Entschlüsseln der verschlüsselten ersten Authentifizierungsdaten in Abhängigkeit von einer Eingabe des Passwortes durch den Benutzer zum Bilden der ersten Authentifizierungsdaten; und
(c) das Vergleichen der ersten Authentifizierungsdaten mit den zweiten Authentifizierungsdaten zum Feststellen, ob die zweiten Bilddaten identisch zu den Ausgangsbilddaten sind.

5. Verfahren nach Anspruch 4, in welchem das Erzeugen der ersten Authentifizierungsdaten einschließt
(a) das Durchführen einer ersten Zeilenberechnung entsprechend einer vorbestimmten Formel mit Gruppen von ein oder mehreren Zeilen aus Pixeln, um einen ersten Satz an Zeilenauthentifizierungsdaten zu bilden; und
(b) das Durchführen einer ersten Spaltenberechnung entsprechend einer vorbestimmten Formel mit Gruppen von ein oder mehreren Spalten aus Pixeln, um einen ersten Satz an Spaltenauthentifizierungsdaten zu bilden,
wobei der erste Satz aus Zeilendaten mit einem zweiten Satz aus Zeilendaten verglichen werden kann, der sich aus einer mit den zweiten Bilddaten durchgeführten Zeilenberechnung ergibt, und wobei der erste Satz aus Spaltendaten mit einem zweiten Satz aus Spaltendaten verglichen werden kann, der sich aus einer mit den zweiten Bilddaten durchgeführten Spaltenberechnung ergibt,
und wobei die Position einer Änderung in den zweiten Bilddaten durch einen Schnitt einer geänderten Gruppe von Zeilen des zweiten Satzes aus Zeilendaten mit einer geänderten Gruppe von Spalten des zweiten Satzes aus Spaltendaten festgestellt wird.

6. Verfahren nach Anspruch 1, in welchem das Passwort von einem externen Gerät erhalten wird.

7. Verfahren nach Anspruch 1, in welchem das Erzeugen und das Verschlüsseln während des Aufnehmens der Ausgangsbilddaten durchgeführt wird, wodurch es keinen Schritt gibt, der das Speichern von unverschlüsselten ersten Authentifizierungsdaten in einer Form erlaubt, aus der eine nichtautorisierte Person Zugang zu den ersten Authentifizierungsdaten erhalten könnte.

8. Verfahren nach Anspruch 1, in welchem die Authentifizierung die Verwendung eines Markierungssystems zum Markieren eines Bildes aufweist, in welchem Schritt (a) aufweist:
– das Initialisieren des Markierungssystems in einer Digitalkamera mit beim Markieren des Bildes verwendeten Kennungen und des vom Benutzer programmierbaren Verschlüsselungspassworts; und in welchem Schritt (c) aufweist:
– das Umwandeln der Ausgangsbilddaten in markierte Bilddaten mit dem Markierungssystem, wobei die Umwandlung die Verwendung der Kennungen und einer Konvertierungsformel einschließt, um die Ausgangsbilddaten in die markierten Bilddaten umzuwandeln.

9. Verfahren nach Anspruch 8, weiter aufweisend: das Erhalten des Passwortes durch die Digitalkamera aus einem externen Gerät.

10. Digitalkamera, die eine Bildauthentifizierung zur Verfügung stellt, aufweisend:
(a) ein Authentifizierungssystem in der Kamera,
(b) eine Einrichtung zum Aufnehmen der Ausgangsbilddaten;
(c) eine Einrichtung zum Erzeugen von ersten Authentifizierungsdaten aus den Ausgangsbilddaten mittels des Authentifizierungssystems innerhalb der Kamera, wobei die ersten Authentifizierungsdaten für die Zwecke des Vergleiches mit aus zweiten Bilddaten erzeugten zweiten Authentifizierungsdaten dienen, um festzustellen, ob die zweiten Bilddaten identisch mit den Ausgangsbilddaten sind; und
(d) eine Einrichtung zum Verschlüsseln der ersten Authentifizierungsdaten mit dem Authentifizierungssystem innerhalb der Kamera, um verschlüsselte erste Authentifizierungsdaten zu erzeugen und um die verschlüsselten ersten Authentifizierungsdaten zu den Ausgangsbilddaten als Ausgabe aus der Kamera zuzuordnen;
dadurch gekennzeichnet,
dass
(e) das Authentifizierungssystem vom Benutzer mittels eines vom Benutzer ausgewählten Verschlüsselungspassworts programmierbar ist;
(f) die ersten Authentifizierungsdaten aus der Kamera in unverschlüsselter Form unzugänglich sind und die Ausgangsbilddaten aus der Kamera ohne ihre zugeordneten verschlüsselten ersten Authentifizierungsdaten unzugänglich sind.

11. Digitalkamera nach Anspruch 10, außerdem aufweisend: eine Einrichtung zum Übertragen der ersten verschlüsselten Authentifizierungsdaten an ein externes Gerät.

12. Digitalkamera nach Anspruch 11, in welcher die Einrichtung zum Erzeugen der ersten Authentifizierungsdaten einschließt
(a) eine Einrichtung zum Durchführen einer ersten Zeilenberechnung entsprechend einer vorbestimmten Formel mit Gruppen von ein oder mehreren Zeilen aus Pixeln, um einen ersten Satz an Zeilenauthentifizierungsdaten zu bilden; und
(b) eine Einrichtung zum Durchführen einer ersten Spaltenberechnung entsprechend einer vorbestimmten Formel mit Gruppen von ein oder mehreren Spalten aus Pixeln zum Bilden eines ersten Satzes von Spaltenauthentifizierungsdaten,
wodurch in dem externen Gerät der erste Satz aus Zeilendaten mit einem zweiten Satz aus Zeilendaten verglichen werden kann, der sich aus einer mit den zweiten Bilddaten durchgeführten Zeilenberechnung ergibt, und der erste Satz aus Spaltendaten mit einem zweiten Satz aus Spaltendaten verglichen werden kann, der sich aus einer mit den zweiten Bilddaten durchgeführten Spaltenberechnung ergibt, und wobei die Position einer Veränderung in den zweiten Bilddaten durch einen Schnitt einer veränderten Gruppe von Zeilen aus dem zweiten Satz an Zeilendaten mit einer veränderten Gruppe von Spalten aus dem zweiten Satz an Spaltendaten festgestellt wird.

13. Digitalkamera nach Anspruch 10, außerdem aufweisend: eine Einrichtung zum Erhalten des Passworts aus einem externen Gerät

14. Digitalkamera nach Anspruch 10, in welcher die ersten Authentifizierungsdaten temporär in einer Registereinrichtung vor dem Verschlüsseln gehalten werden, wodurch es keinen ersten Authentifizierungsschritt gibt, der das Speichern von unverschlüsselten Daten in einer Form erlaubt, aus der eine nichtautorisierte Person Zugang zu den ersten Authentifizierungsdaten erhalten könnte.

15. Digitalkamera nach Anspruch 10, in welcher die ersten Authentifizierungsdaten die Daten einer Kontrollsumme sind.

16. Digitalkamera nach Anspruch 15, in welcher die Einrichtung zum Erzeugen von ersten Authentifizierungsdaten eine Einrichtung zum Vorbereiten der Daten der Kontrollsumme mittels Addierens von Farbnummern aus ausgewählten Gruppen aus Zeilen und Spalten der Ausgangsbilddaten, und durch das Speichern von Werten der Zeilen und Spalten der Ausgangsbilddaten in einer Nachschlagetafel einschließt.

17. Digitalkamera nach Anspruch 10, in welcher das Authentifizierungssystem ein Markierungssystem ist, das Kennungen vorsieht, die zum Markieren des Bildes verwendet werden, und in welcher die Einrichtung zum Erzeugen eine Einrichtung zum Umwandeln der Ausgangsbilddaten mittels des Markierungssystems in markierte Bilddaten durch Verwendung der Kennungen und einer Umwandlungsformel zum Umwandeln der Ausgangsbilddaten in die markierten Bilddaten aufweist.

18. Digitalkamera nach Anspruch 17, außerdem aufweisend:
eine Einrichtung zum Empfangen des Passworts von einem externen Gerät.

Es folgen 14 Blatt Zeichnungen

Anhängende Zeichnungen

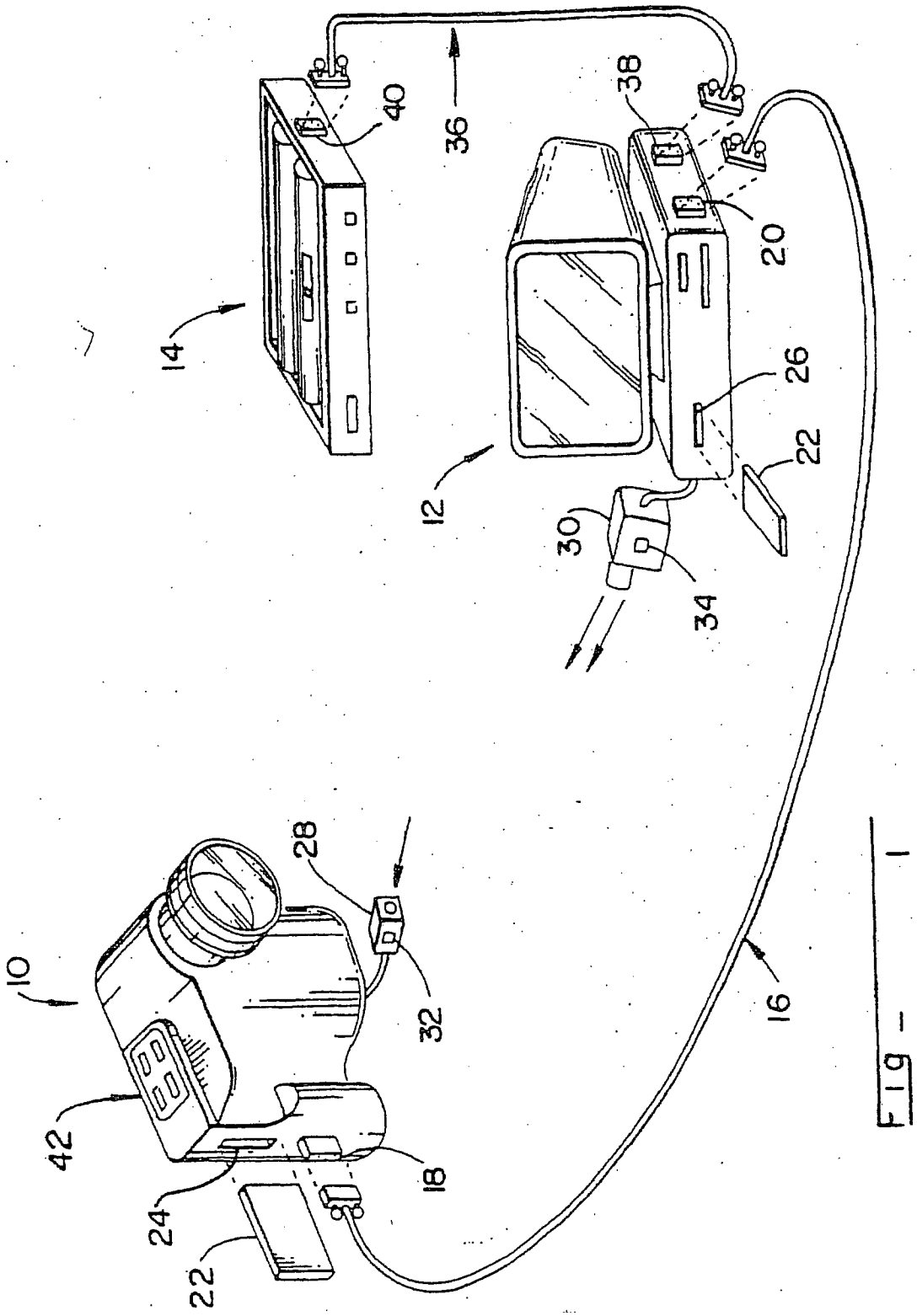


Fig. 1

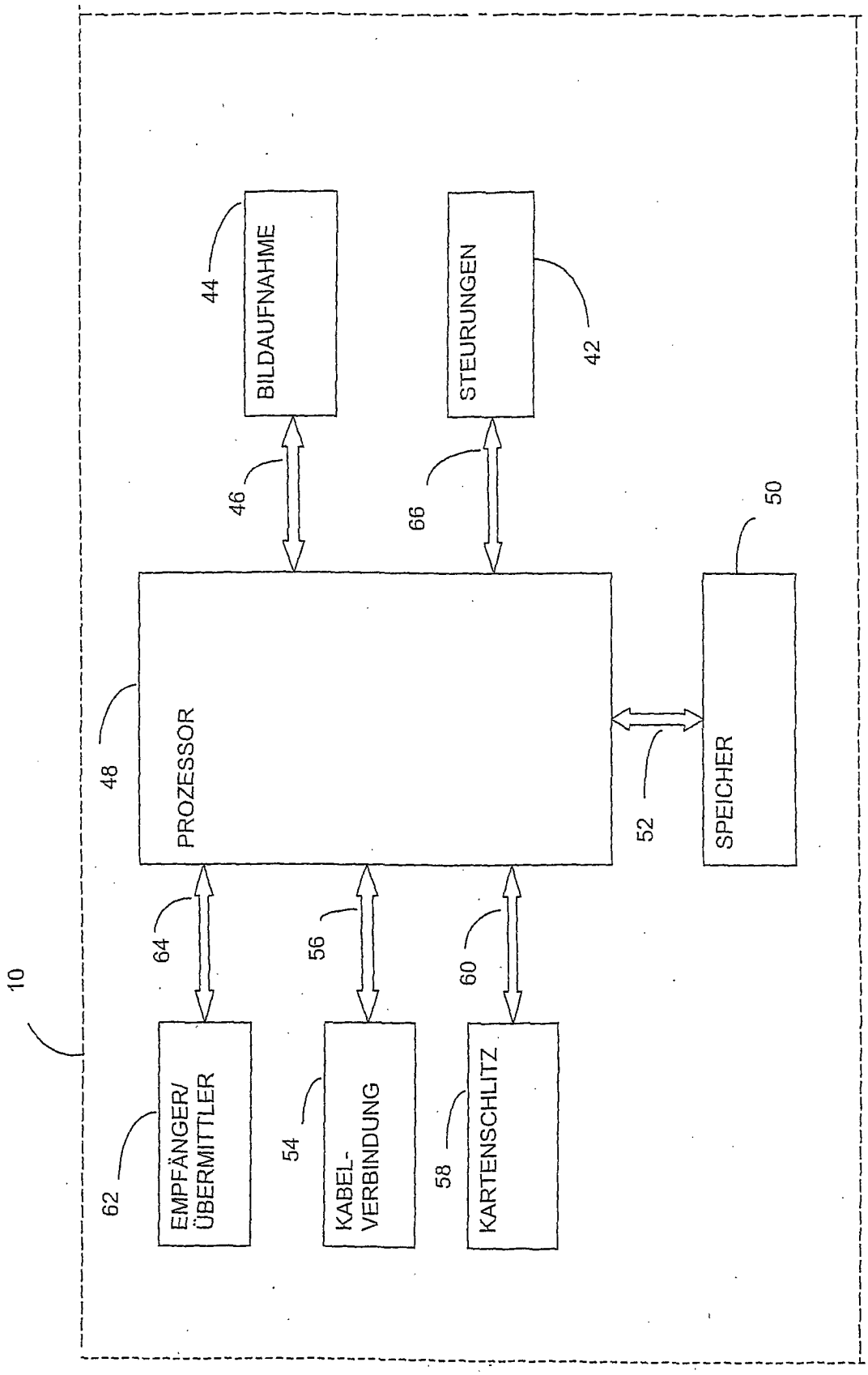

10
PROZESSOR
48
BILDAUFNAHME
44
STEURUNGEN
42
SPEICHER
50
46
66
52
64
56
60
EMPFÄNGER/
ÜBERMITTLER
62
KABEL-
VERBINDUNG
54
KARTENSCHLITZ
58

Fig. 2

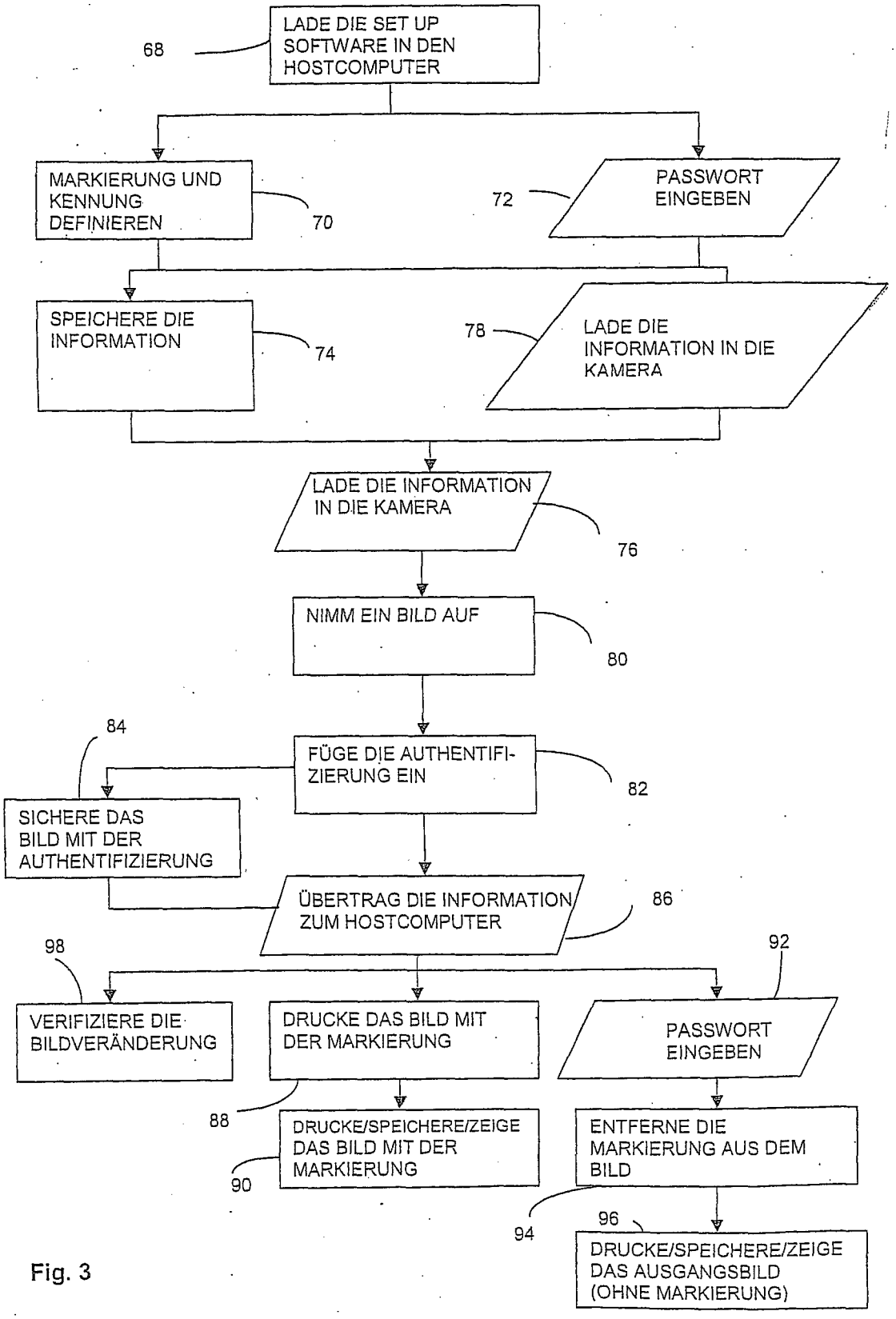

LADE DIE SET UP SOFTWARE IN DEN HOSTCOMPUTER
68
MARKIERUNG UND KENNUNG DEFINIEREN
70
PASSWORT EINGEBEN
72
SPEICHERE DIE INFORMATION
74
LADE DIE INFORMATION IN DIE KAMERA
78
LADE DIE INFORMATION IN DIE KAMERA
76
NIMM EIN BILD AUF
80
FÜGE DIE AUTHENTIFIZIERUNG EIN
82
84
SICHERE DAS BILD MIT DER AUTHENTIFIZIERUNG
ÜBERTRAG DIE INFORMATION ZUM HOSTCOMPUTER
86
98
92
VERIFIZIERE DIE BILDVERÄNDERUNG
DRUCKE DAS BILD MIT DER MARKIERUNG
PASSWORT EINGEBEN
88
DRUCKE/SPEICHERE/ZEIGE DAS BILD MIT DER MARKIERUNG
90
ENTFERNE DIE MARKIERUNG AUS DEM BILD
94
96
DRUCKE/SPEICHERE/ZEIGE DAS AUSGANGSBILD (OHNE MARKIERUNG)

Fig. 3

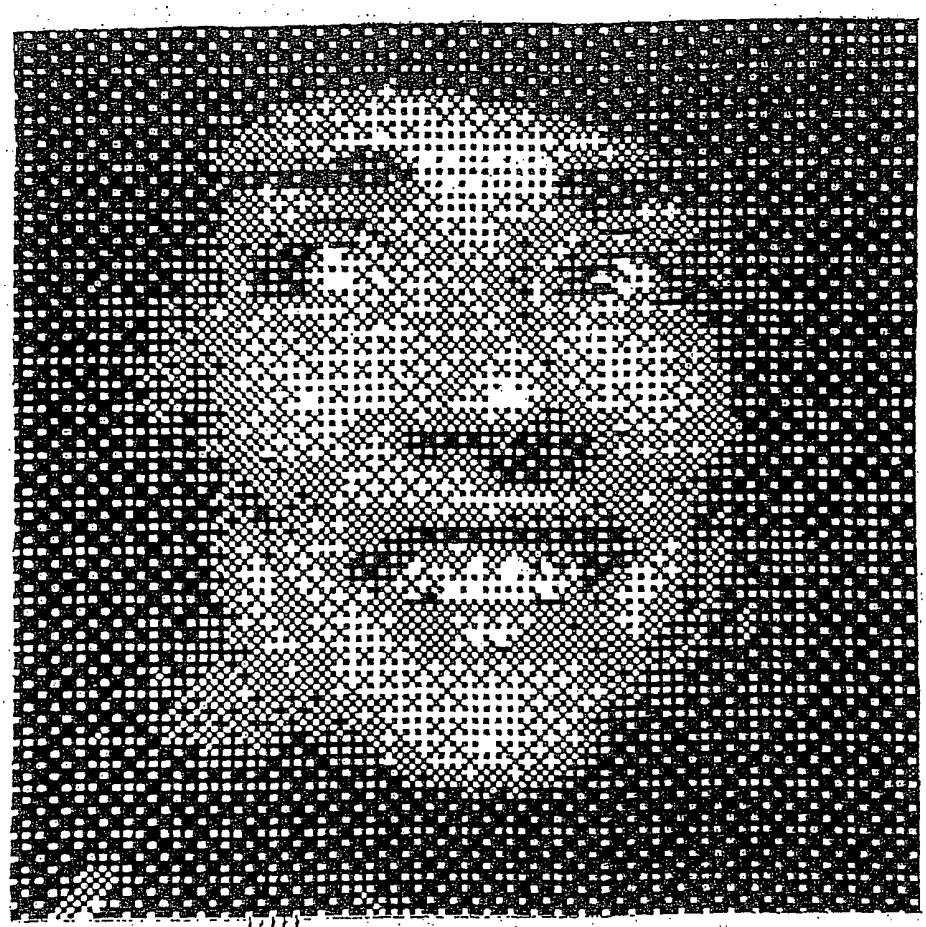


Fig. 4

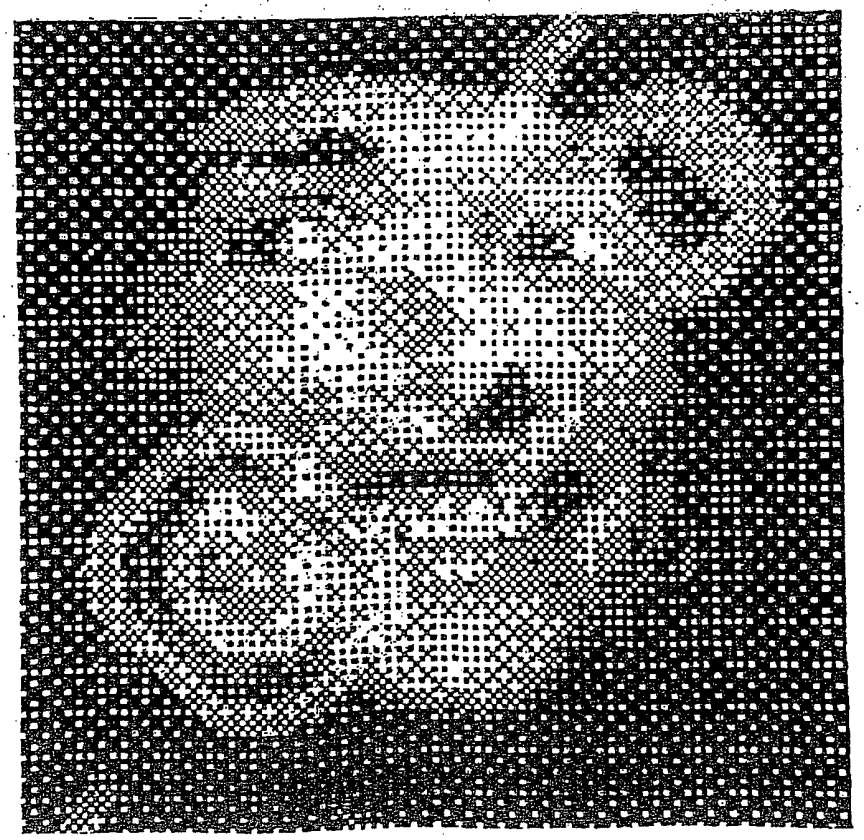


Fig. 5

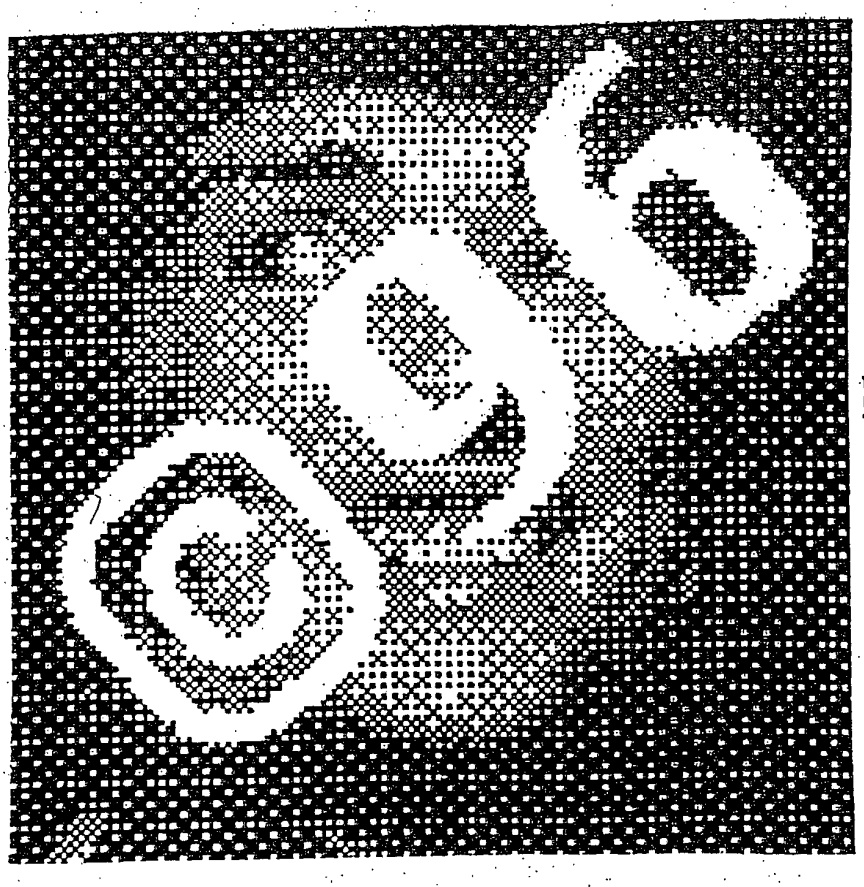


Fig- 6

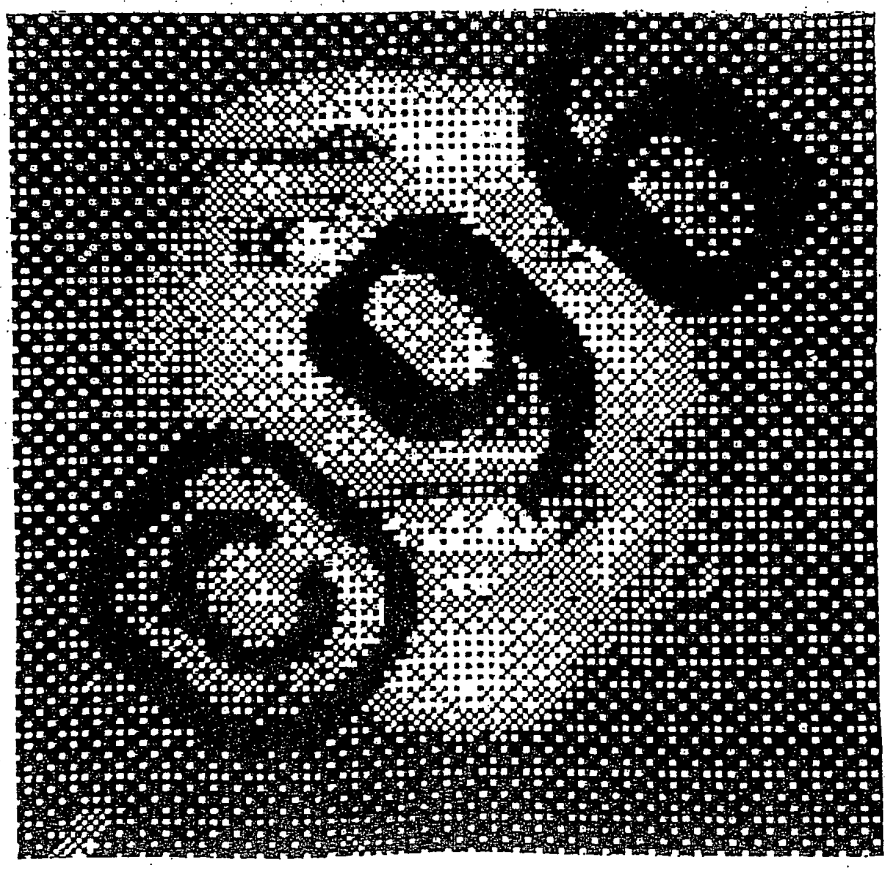


Fig- 7

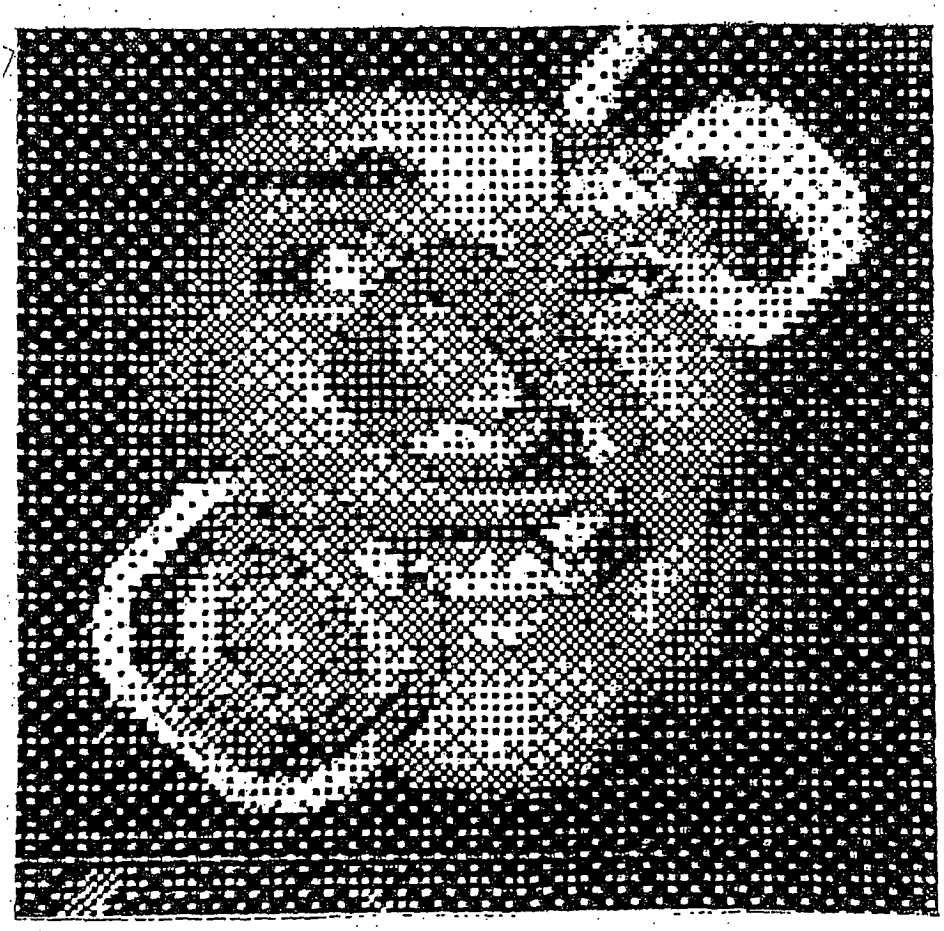
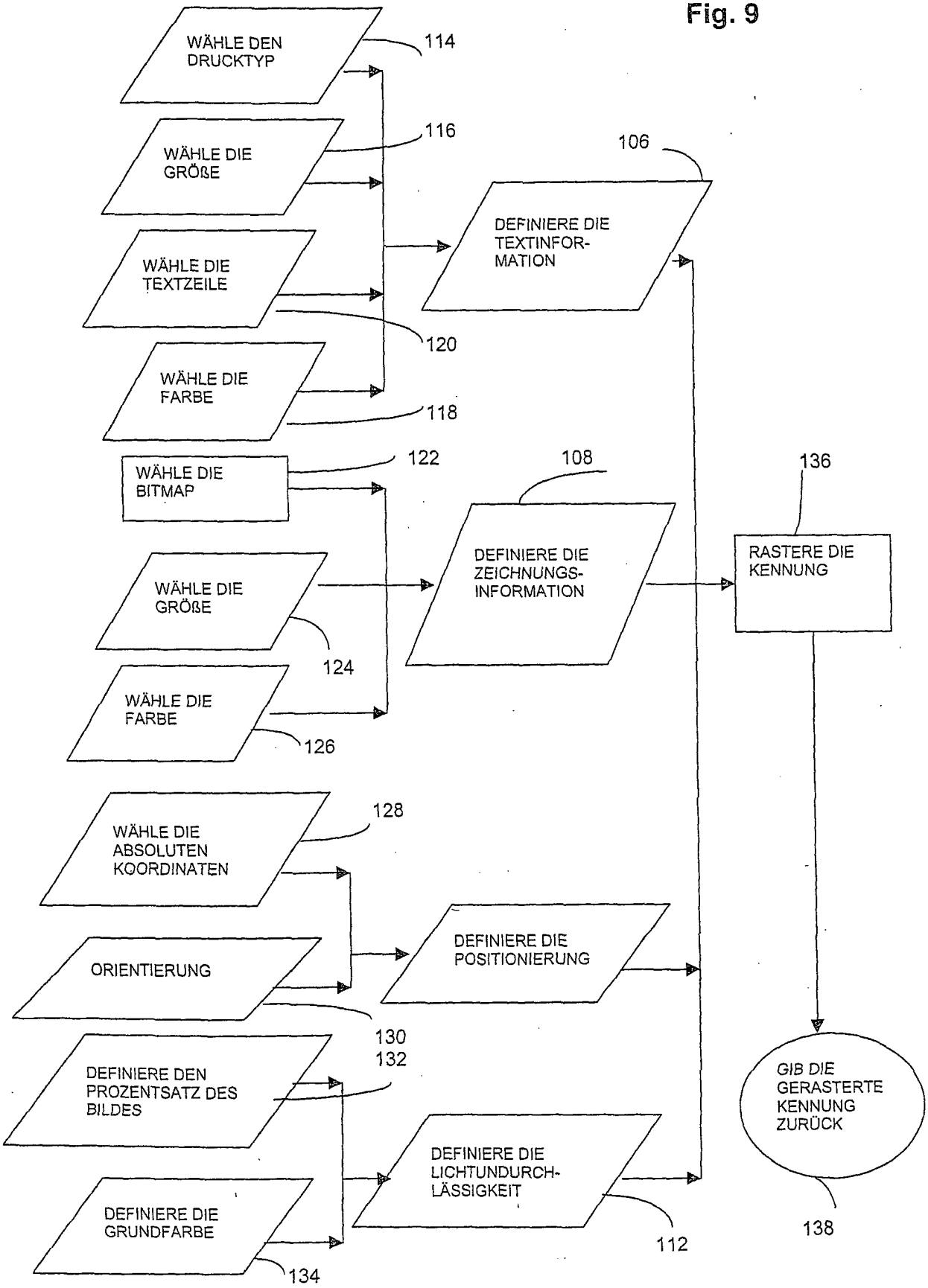


Fig. 8

Fig. 9


WÄHLE DEN DRUCKTYP
114
WÄHLE DIE GRÖßE
116
106
DEFINIERE DIE TEXTINFOR-MATION
WÄHLE DIE TEXTZEILE
120
WÄHLE DIE FARBE
118
WÄHLE DIE BITMAP
122
108
136
DEFINIERE DIE ZEICHNUNGS-INFORMATION
RASTERE DIE KENNUNG
WÄHLE DIE GRÖßE
124
WÄHLE DIE FARBE
126
128
WÄHLE DIE ABSOLUTEN KOORDINATEN
DEFINIERE DIE POSITIONIERUNG
ORIENTIERUNG
130
132
DEFINIERE DEN PROZENTSATZ DES BILDES
GIB DIE GERASTERTE KENNUNG ZURÜCK
DEFINIERE DIE LICHTUNDURCH-LÄSSIGKEIT
DEFINIERE DIE GRUNDFARBE
112
134
138

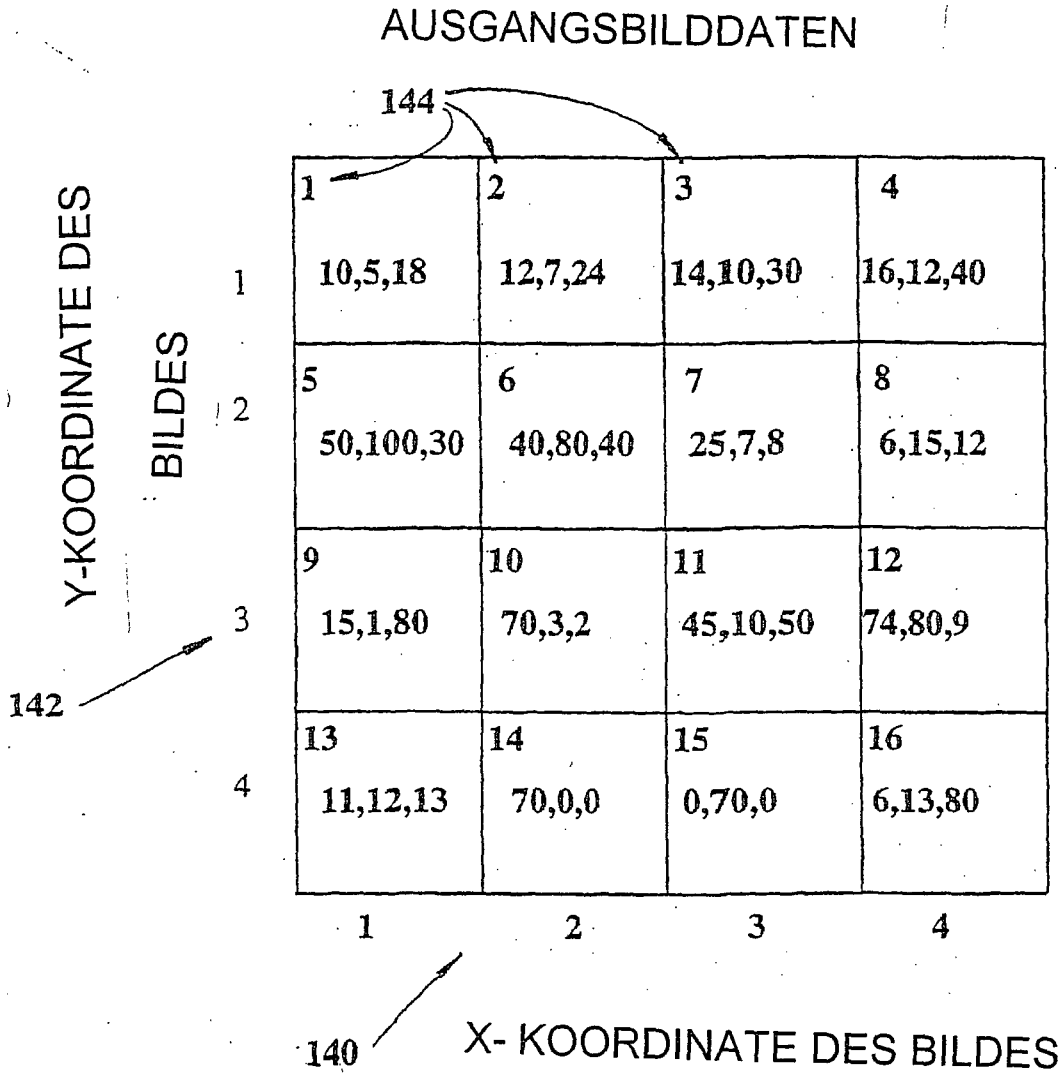

AUSGANGSBILDDATEN
144
Y-KOORDINATE DES BILDES
142
140
X- KOORDINATE DES BILDES
1
2
3
4
1 10,5,18
2 12,7,24
3 14,10,30
4 16,12,40
5 50,100,30
6 40,80,40
7 25,7,8
8 6,15,12
9 15,1,80
10 70,3,2
11 45,10,50
12 74,80,9
13 11,12,13
14 70,0,0
15 0,70,0
16 6,13,80

Fig - 10

148 150 156 154 152

PIXEL-NR.	KOORDINATEN X, Y	DIGITALER WERT DER MARKIERTEN BILDDATEN (Rt, Gt, Bt)	DIGITALER WERT DER BILDDATEN (Ri, Gi, Bi)	DIGITALER WERT DER KENNUNG (Rd, Gd, Bd, Op)
1	1,1	10, 5, 18	10, 5, 18	0, 0, 0, 1
2	2,1	12, 7, 24	12, 7, 24	0, 0, 0, 1
3	3, 1	14, 10, 30	14, 10, 30	0, 0, 0, 1
4	4, 1	16, 12, 40	16, 12, 40	0, 0, 0, 1
5	1, 2	50, 100, 30	50, 100, 30	0, 0, 0, 1
6	2, 2	255, 80, 40	40, 80, 40	255, 0, 0, 1
7	3, 2	25, 7, 8	25, 7, 8	0, 0, 0, 1
8	4, 2	6, 15, 12	6, 15, 12	0, 0, 0, 1
9	1, 3	15, 1, 80	15, 1, 80	0, 0, 0, 1
10	2, 3	70, 255, 2	70, 3, 2	0, 255, 0, 1
11	3, 3	45, 10, 255	45, 10, 50	0, 0, 255, 1
12	4, 3	74, 80, 9	74, 80, 9	0, 0, 0, 1
13	1, 4	11, 12, 13	11, 12, 13	0, 0, 0, 1
14	2, 4	70, 0, 0	70, 0, 0	0, 0, 0, 1
15	3,4	0, 70, 0	0, 70, 0	0, 0, 0, 1
16	4, 4	6, 13, 80	6, 13, 80	0, 0, 0, 1

Fig. 11

MODIFIZIERTE BILDDATEN

Y-KOORDINATE DES BILDES 2	1	2	3	4
1	1 10, 5, 18	2 12, 7, 24	3 10, 10, 30	4 16, 12, 40
2	5 50,100,30	6 255,80,40	7 25,7,8	8 6,15,12
3	9 15,1,80	10 70,255,2	11 45,10,255	12 74,80,9
4	13 11,12,13	14 70,0,0	15 0,70,0	16 6,13,80

X-KOORDINATE DES BILDES 2

Fig - 12

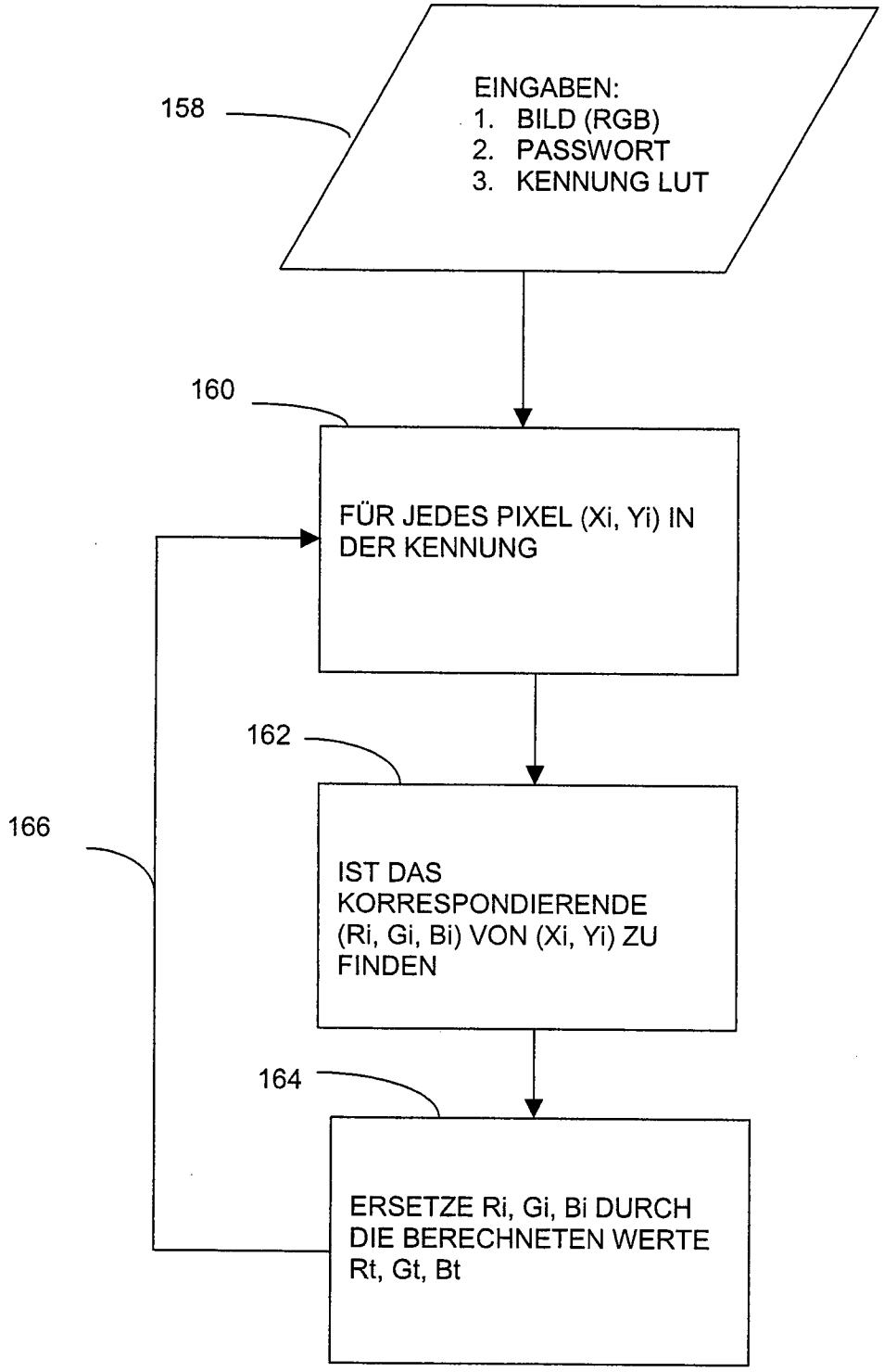

158
EINGABEN:
1. BILD (RGB)
2. PASSWORT
3. KENNUNG LUT
160
FÜR JEDES PIXEL (Xi, Yi) IN DER KENNUNG
162
IST DAS KORRESPONDIERENDE (Ri, Gi, Bi) VON (Xi, Yi) ZU FINDEN
164
ERSETZE Ri, Gi, Bi DURCH DIE BERECHNETEN WERTE Rt, Gt, Bt
166

Fig. 13

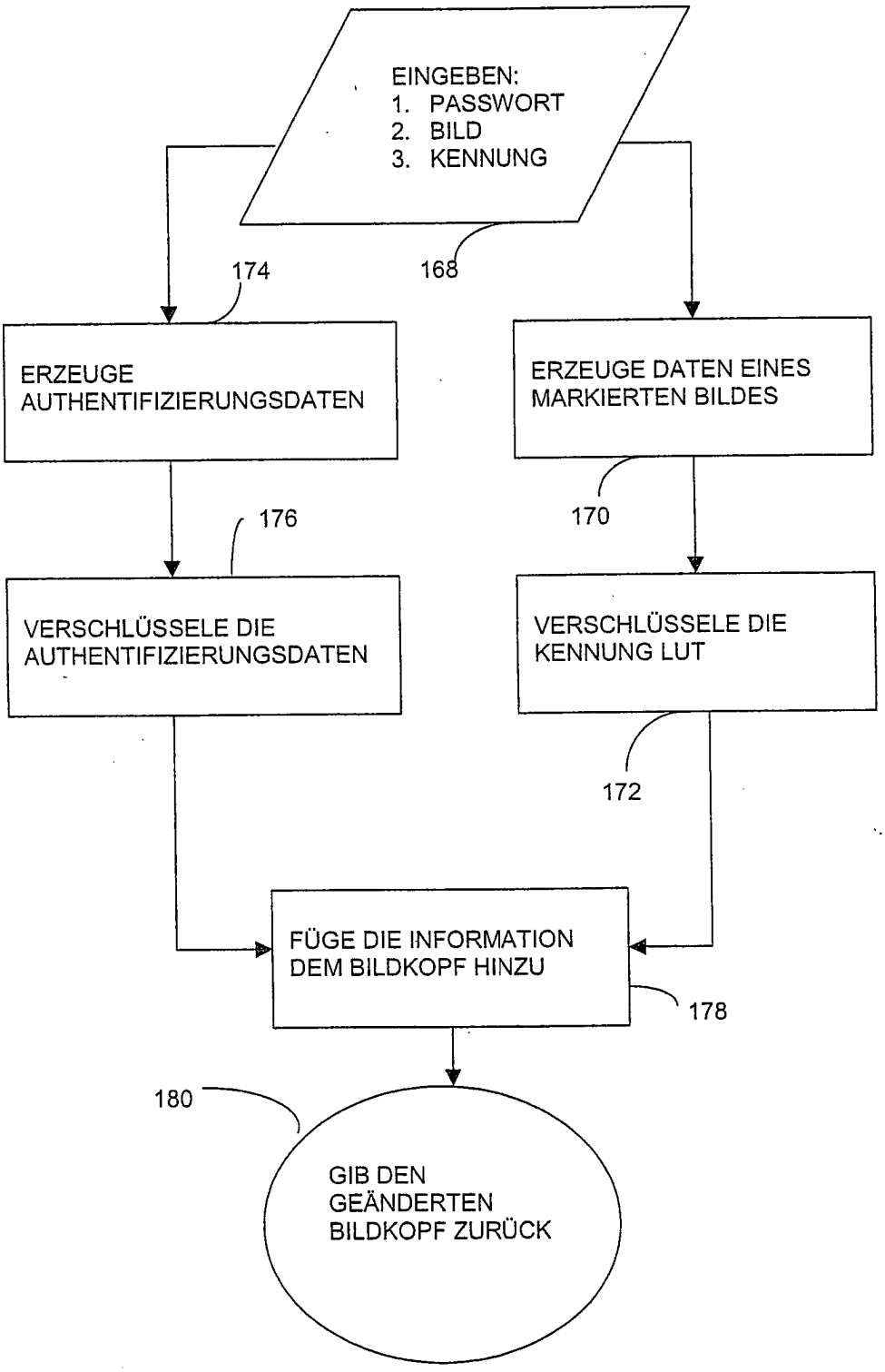
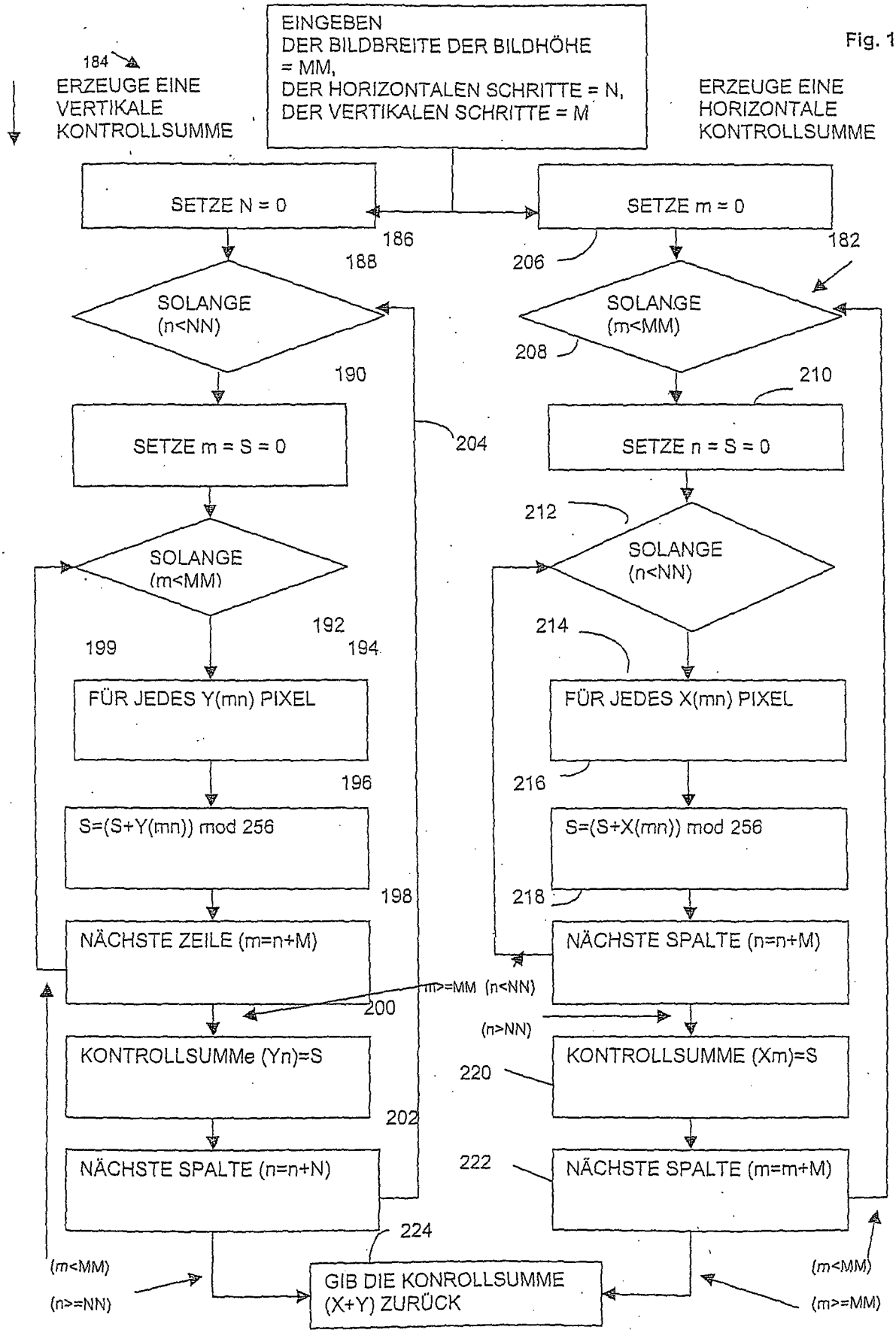

EINGEBEN:
1. PASSWORT
2. BILD
3. KENNUNG
168
174
ERZEUGE AUTHENTIFIZIERUNGSDATEN
ERZEUGE DATEN EINES MARKIERTEN BILDES
170
176
VERSCHLÜSSELE DIE AUTHENTIFIZIERUNGSDATEN
VERSCHLÜSSELE DIE KENNUNG LUT
172
FÜGE DIE INFORMATION DEM BILDKOPF HINZU
178
180
GIB DEN GEÄNDERTEN BILDKOPF ZURÜCK

Fig. 14

Fig. 15


EINGEBEN
DER BILDBREITE DER BILDHÖHE
= MM,
DER HORIZONTALEN SCHRITTE = N,
DER VERTIKALEN SCHRITTE = M
184
ERZEUGE EINE
VERTIKALE
KONTROLLSUMME
ERZEUGE EINE
HORIZONTALE
KONTROLLSUMME
SETZE N = 0
SETZE m = 0
186
188
206
182
SOLANGE
(n<NN)
SOLANGE
(m<MM)
208
190
210
SETZE m = S = 0
204
SETZE n = S = 0
212
SOLANGE
(m<MM)
SOLANGE
(n<NN)
192
214
199
194
FÜR JEDES Y(mn) PIXEL
FÜR JEDES X(mn) PIXEL
196
216
S=(S+Y(mn)) mod 256
S=(S+X(mn)) mod 256
198
218
NÄCHSTE ZEILE (m=n+M)
NÄCHSTE SPALTE (n=n+M)
m>=MM (n<NN)
200
(n>NN)
KONTROLLSUMMe (Yn)=S
KONTROLLSUMME (Xm)=S
220
202
NÄCHSTE SPALTE (n=n+N)
222
NÄCHSTE SPALTE (m=m+M)
224
(m<MM)
(n>=NN)
GIB DIE KONROLLSUMME
(X+Y) ZURÜCK
(m<MM)
(m>=MM)

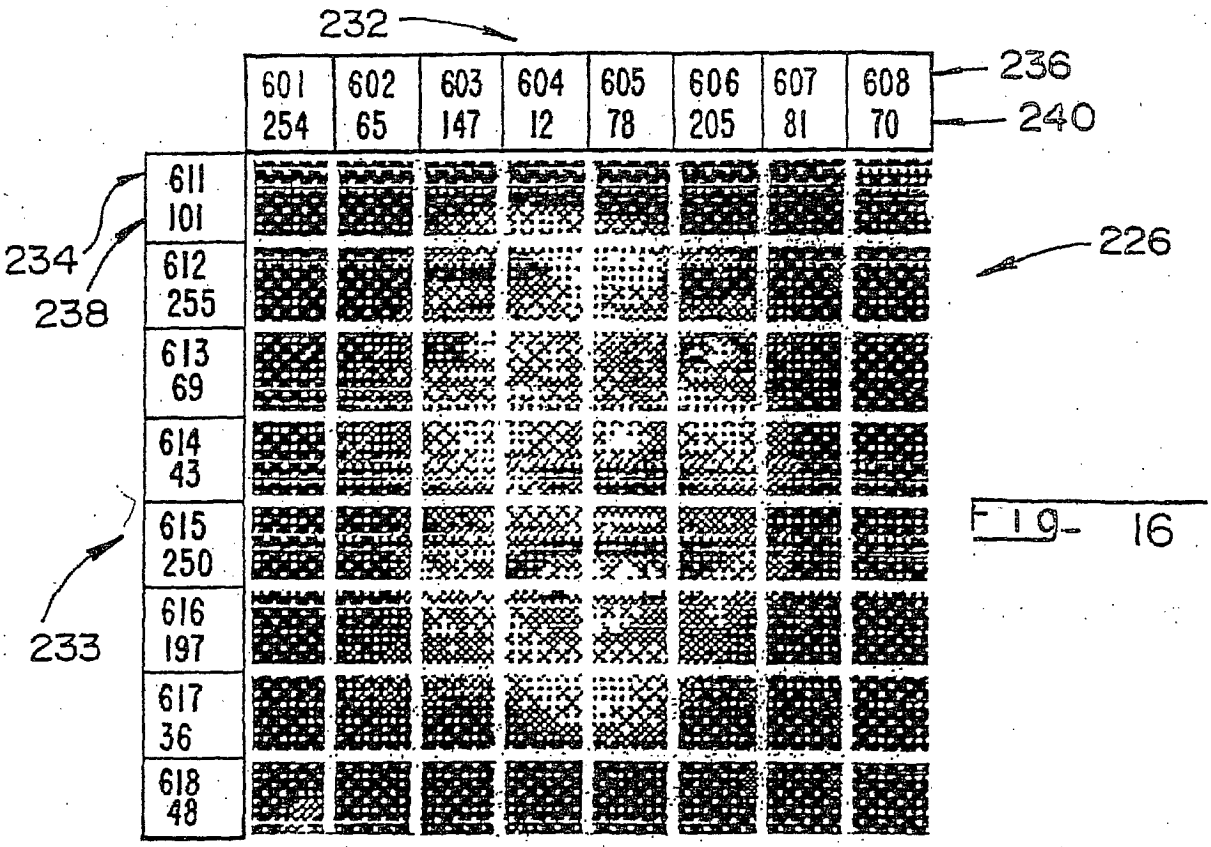

232
601 254
602 65
603 147
604 12
605 78
606 205
607 81
608 70
236
240
611 101
612 255
613 69
614 43
615 250
616 197
617 36
618 48
234
238
226
233

Fig. 16

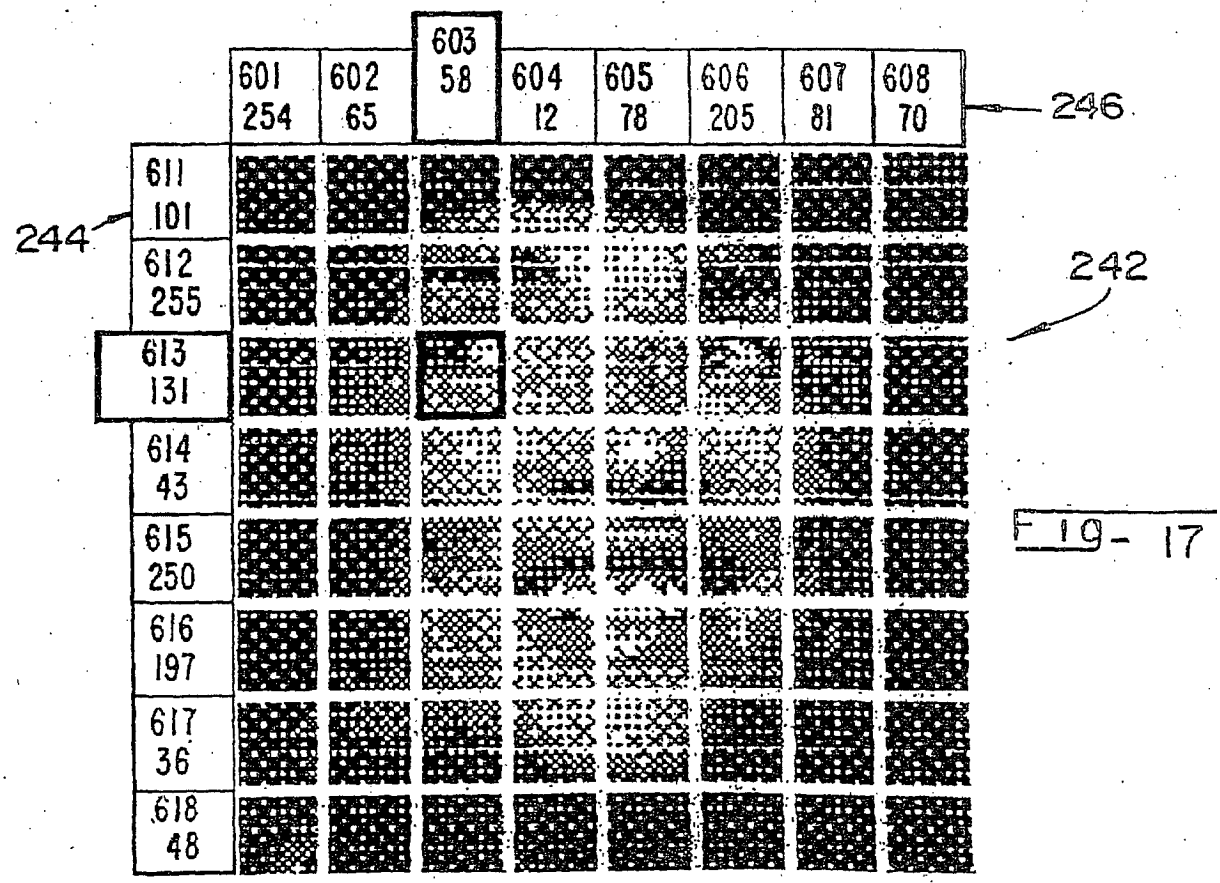

601 254
602 65
603 58
604 12
605 78
606 205
607 81
608 70
246
611 101
612 255
613 131
614 43
615 250
616 197
617 36
618 48
244
242

Fig. 17