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

(10) **DE 699 35 342 T2** 2007.11.29

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 110 401 B1**
(21) Deutsches Aktenzeichen: **699 35 342.4**
(86) PCT-Aktenzeichen: **PCT/US99/18417**
(96) Europäisches Aktenzeichen: **99 941 111.9**
(87) PCT-Veröffentlichungs-Nr.: **WO 2000/011870**
(86) PCT-Anmeldetag: **12.08.1999**
(87) Veröffentlichungstag der PCT-Anmeldung: **02.03.2000**
(97) Erstveröffentlichung durch das EPA: **27.06.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **28.02.2007**
(47) Veröffentlichungstag im Patentblatt: **29.11.2007**

(51) Int Cl.[8]: ***H04N 7/167*** (2006.01)
H04L 9/06 (2006.01)
H03M 7/30 (2006.01)

(30) Unionspriorität:

97264 P	**20.08.1998**	**US**
182933	**30.10.1998**	**US**

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

(73) Patentinhaber:
Sarnoff Corp., Princeton, N.J., US

(74) Vertreter:
Epping Hermann Fischer, Patentanwaltsgesellschaft mbH, 80339 München

(72) Erfinder:
REITMEIER, Glenn A., Yardley, PA 19067, US;
TINKER, Michael, Yardley, PA 19067, US

(54) Bezeichnung: **Sicheres Informationsverteilungssystem unter Verwendung von Segmentverschlüsselung**

Beschreibung

[0001] Die Erfindung betrifft Informationsverteilungssysteme und insbesondere Verfahren und Geräte zum Sichern von Informationen, die innerhalb eines Informationsverteilungssystems verteilt werden.

HINTERGRUND DER ERFINDUNG

[0002] In mehreren Kommunikationssystemen werden die zu übertragenden Daten so komprimiert, dass die verfügbare Bandbreite effizienter ausgenutzt wird. Zum Beispiel hat die Moving Pictures Experts Group (MPEG) mehrere Standards veröffentlicht, die sich auf digitale Datenübertragungssysteme beziehen. Der erste, bekannt als MPEG-1, bezieht sich auf den ISO-/IEC Standard 11172. Der zweite, bekannt als MPEG-2, bezieht sich auf den ISO-/IEC Standard 13818 und ist hier durch Referenz/Verweis berücksichtigt. Ein komprimiertes digitales Videosystem wird im Dokument A/53 des Digitalfernsehstandards des Advanced Television Systems Committee (ATSC) beschrieben.

[0003] Die oben erwähnten Standards beschreiben Techniken zur Verarbeitung und Handhabung von Daten, die gut für die Komprimierung und Übertragung von Video-, Audio- und anderen Informationsdaten, unter Verwendung von digitalen Kommunikationssystemen mit fester oder variabler Länge geeignet sind. Insbesondere komprimieren die oben erwähnten Standards und andere „MPEG-ähnliche" Standards und Techniken, veranschaulichend Videoinformationen, unter Verwendung von Intraframe-Codierungstechniken (wie z. B. Lauflängencodierung, Huffman-Codierung und dergleichen), sowie Interframe-Codierungstechniken (wie z. B. Vorwärts- und Rückwärts-Prädiktionscodierung, Bewegungskompensation und dergleichen). Insbesondere im Fall von Videoverarbeitungssystemen sind MPEG und MPEG-ähnliche Videoverarbeitungssysteme, durch die auf Prädiktion basierende Komprimierungscodierung von Videorahmen, mit oder ohne Intra- und/oder Interframe-Bewegungskompensations-Codierung, gekennzeichnet.

[0004] Derzeitige elektronische Verteilungssysteme finden typischerweise kein für die Zwecke von Informationsverteilungsanwendungen angemessenes Gleichgewicht zwischen Flexibilität und Sicherheit. Um z. B. die elektronische Verteilung von Kinofilmen (d.h. Film) und anderen Unterhaltungsvideoanwendungen zu ermöglichen, ist es erforderlich auf dynamische Weise „Trailer" (d.h. „kurze Vorschauen auf kommende Attraktionen") von Ort zu Ort – zusätzlich zu den Kinofilmen – in voller Länge zu verarbeiten. Bezüglich der Sicherheit ist es offensichtlich erforderlich, ein hohes Sicherheitsniveau zu integrieren, am besten unter Verwendung eines mehrschichtigen Sicherheitsansatzes, so dass wertvolles intellektuelles Eigentum, welches innerhalb des Systems übertragen wird, nicht gefährdet ist.

[0005] Daher besteht ein Bedürfnis nach sicheren und flexiblen Verfahren und Geräten für die Verteilung von Informationen, wie beispielsweise hochwertigen Kinofilmen, anderen Audio-Video-Informationen und weiteren Datenarten. Außerdem wird es als wünschenswert erachtet, verbesserte Sicherheit für verschiedene Medien, wie z. B. Digital Versatile Disk (DVD) oder andere Medien, bereitzustellen.

[0006] Vor dem Bereitstellen einer Zusammenfassung der vorliegenden Erfindung, wird hiermit die US-Patentschrift Nr. 5,479,512 (Weiss) als Prior Art Basis anerkannt. Weiss legt integrierte Komprimierung und Verschlüsselung (Concryption) von klaren Daten offen. Mindestens ein Komprimierungsschritt der klaren Daten wird durchgeführt, das Ergebnis dann in Segmente unterteilt und anschließend mindestens ein Verschlüsselungsschritt unter Verwendung von abgerufenen Segmentverschlüsselungscodes durchgeführt.

ZUSAMMENFASSUNG DER ERFINDUNG

[0007] Im Allgemeinen ausgedrückt, stellt die vorliegende Erfindung ein Verfahren und Gerät zum Sichern und, wahlweise, Verteilen eines Informationsflusses durch Unterteilen des Informationsflusses in eine Sammlung von Segmenten und dem Komprimierung der Segmente, Neuorganisieren der anderen Segmente und Verschlüsseln der Segmente, z. B. vor dem Verteilen der verschlüsselten Segmente an einen oder mehrere Nutzer innerhalb eines Informationsverteilungssystems, bereit. Alternativ kann der Informationsfluss komprimiert werden, bevor er in Segmente unterteilt wird.

[0008] Speziell stellt die Erfindung gemäß einem Aspekt ein Verfahren wie in Anspruch 1 beansprucht, gemäß einem anderen Aspekt ein Verfahren wie in Anspruch 2 beansprucht, gemäß eines anderen Aspekts ein Verfahren, wie in Anspruch 11 beansprucht, gemäß einem anderen Aspekt ein System, wie in Anspruch 13 beansprucht, und darüber hinaus gemäß einem anderen Aspekt, ein System wie in Anspruch 14 beansprucht, bereit.

[0009] In einer Ausführungsform der Erfindung wird ein Eingabeinformationsfluss in eine Sammlung von Informationssegmenten unterteilt, wobei die einzelnen Segmente dann komprimiert werden und auf eine nicht standardmäßige Weise (d.h. verwürfelt) angeordnet werden, um eine verwürfelte Sammlung von Informationssegmenten und eine damit verbundene Indextabelle zu erzeugen, die für die Verwendung beim Reorganisieren der Sammlung von Informationssegmenten in eine standardmäßige (d.h. nicht verwürfelte) Reihenfolge geeignet ist. Die ver-

würfelte Sammlung von Informationssegmenten und die damit verbundene Indextabelle werden verschlüsselt (unter Verwendung derselben oder anderer Verschlüsselungstechniken) und an einen oder mehrere Teilnehmer verteilt (unter Verwendung derselben oder anderer Verteilungskanäle). Optional wird die verwürfelte Sammlung von Informationssegmenten unter Verwendung einer Mehrzahl von Verteilungskanälen (d.h. Mehrwegeverteilung) und/oder zu einer Vielzahl von verschiedenen Zeiten (d.h. zeitlich gestaffelte Verteilung) verteilt.

[0010] Es wird angemerkt, dass die oben anerkannte US-Patentschrift Nr. 5,479,512 kein Neuorganisieren/Neusequenzieren/Verwürfeln der Segmente mit einem Index vor dem Verschlüsseln der Segmente nach Art der vorliegenden Erfindung offenbart oder angibt.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0011] Die Lehren der vorliegenden Erfindung können leicht verstanden werden durch Berücksichtigung der folgenden detaillierten Beschreibung, zusammen mit den beigefügten Zeichnungen, in denen:

[0012] Fig. 1 ein Informationsverteilungssystem **100**, einschließlich eines Gerätes gemäß der Erfindung darstellt;

[0013] Fig. 2 die graphische Darstellung einer Sammlung Informationssegmente, die in einer nicht standardmäßigen (d.h. verwürfelten) Reihenfolge angeordnet sind, und einer Indextabelle, die für die Verwendung beim Neuorqanisieren der Sammlung von Informationssegmenten in eine standardmäßige (d.h. nicht verwürfelte) Reihenfolge geeignet ist, darstellt;

[0014] Fig. 3 eine Fließroutine des Bearbeitungsverfahrens eines Informationslieferanten gemäß der Erfindung darstellt;

[0015] Fig. 4 ein Flussdiagramm eines teilnehmerseitigen Verfahrens zur Bearbeitung eines Informationsflusses gemäß der Erfindung darstellt; und

[0016] Fig. 5 eine schematische Darstellung einer geschichteten Sicherheitsumgebung, die von der Erfindung ermöglicht wird, darstellt.

[0017] Um das Verständnis zu erleichtern, wurden, wo möglich, identische Bezugszeichen verwendet, um identische Elemente, die den Figuren gemeinsam sind, zu kennzeichnen.

DETAILLIERTE BESCHREIBUNG

[0018] Die Erfindung wird im Kontext eines MPEG-ähnlichen Informationsverteilungssystems beschrieben. Es ist für Fachleute erkenntlich, dass die Erfindung auf viele Arten von Informationsverteilungssystemen anwendbar ist. Insbesondere ist die Erfindung bestens für den Schutz und die Verteilung von Informationsflüssen, die verbundene Sequenzen von Video- und/oder Audioinformationen, wie z. B. Kinofilme, Fernsehen und dergleichen umfassen, geeignet.

[0019] Fig. 1 stellt ein Informationsverteilungssystem **100**, einschließlich des Gerätes gemäß der Erfindung dar. Insbesondere stellt Fig. 1 ein Informationsverteilungssystem **100** dar, das eine Informationslieferantenanlage (**105**-**140**), Informationsverteilungskanäle (**145A** und **145B**) und eine Teilnehmeranlage (**150**-**175**) umfasst. Das Informationsverteilungssystem **100** empfängt einen Eingabeinformationsfluss IN', veranschaulicht einen audiovisuellen Informationsfluss wie z. B. einen Kinofilm-Videofluss und einen oder mehrere verbundene Audio- oder Datenflüsse. Der Eingabeinformationsfluss IN' wird von der Teilnehmeranlage verarbeitet, um einen sicheren Informationsfluss zu erzeugen, der mit der Teilnehmeranlage über den Informationsverteilungskanal/die Informationsverteilungskanäle gekoppelt ist. Der sichere Informationsfluss wird von der Teilnehmeranlage empfangen und verarbeitet, um einen Ausgabeinformationsfluss OUT' zu erzeugen, der den anfänglichen audio-visuellen Informationsfluss IN' umfasst.

[0020] In einer Ausführungsform der Erfindung wird ein Film oder ein anderes Programm als eine Sammlung in sich geschlossener MPEG-2-Sequenzen komprimiert, die eine nicht einheitliche Dauer und Größe (Anzahl der Bits) aufweisen können. Zur Verteilung/Lagerung können die Sequenzen beliebig neu angeordnet und eine Indextabelle aufgebaut werden, die Zeiger zu den Speicherstellen von Sequenzen, die in ihrer korrekten Darstellungssequenz geordnet sind, enthält. Die neu geordneten Sequenzen können unter Verwendung von standardmäßigen Verschlüsselungstechniken verschlüsselt werden. Die Indextabelle kann unter Verwendung derselben oder anderer Verschlüsselungstechniken getrennt verschlüsselt werden. Außerdem kann die Indextabelle unter Verwendung eines anderen Mediums verteilt werden. Zum Beispiel können die verschlüsselten und neu geordneten Sequenzen auf einer DVD-ROM verteilt werden, während die verschlüsselte Indextabelle von einem Online-Server in den Empfänger/Decodierer heruntergeladen wird. Alternativ könnte eine Chipkarte für die Indextabelle verwendet werden. Es sind viele Variationen möglich. Beim Empfänger wird die entschlüsselte Indextabelle verwendet, um das Direktzugriff-Auslesen der verschlüsselten Sequenzen vom Speichermedium zu steuern. Die Videosequenzen werden entschlüsselt, dekomprimiert und in ihrer richtigen Reihenfolge angezeigt.

[0021] Der Indextabellenansatz erzielt nicht nur

eine Verwürfelung, sondern stellt auch einen Ansatz zu einer flexiblen Unterbringung von Trailern bereit. Der neu geordnete Videospeicher, der an alle Standorte verteilt wird, enthält dann alle Trailer. Die Indextabelle, die an einen bestimmten Standort verteilt wird, kann die gewünschte Teilmenge von Trailern angeben. Auf diese Weise stellen sowohl der Indextabellen- als auch der Neuordnungsansatz eine mehrstufige Sicherheit und Flexibilität bei der Handhabung von Trailern bereit.

[0022] Es sollte angemerkt werden, dass im Umfang dieser Erfindung Video und Audio mit jeweils getrennten Indextabellen getrennt segmentiert und unabhängig voneinander neu geordnet werden können. Ähnlich können getrennte Videokomponenten (z. B. R, G und B) ebenfalls separat behandelt werden.

[0023] Die Informationslieferantenanlage innerhalb des Informationsverteilungssystems **100** von Abb. 1 umfasst ein optionales Pixeldomain-Codierungsmodul **105**, ein Segmentierungsmodul **110**, ein Komprimierungsmodul **115**, ein Neusequenzierungsmodul **130**, ein Informationsfluss-Verschlüsselungsmodul **135**, ein Indextabellen-Verschlüsselungsmodul **140** und eine Vielzahl optionaler Lieferanten-Speichermodule **122**, **124** und **126**.

[0024] Der optionale Pixeldomain-Codierer **105** empfängt und verarbeitet den Eingabeinformationsfluss IN' gemäß einer oder mehrerer von einer Vielzahl an Pixeldomain- (oder Audiodomain-) Verarbeitungstechniken. Diese Techniken werden unten mit Bezug auf Abb. 3 detaillierter beschrieben. Zum Beispiel kann der optionale Pixeldomain-Codierer **105** die Videoinformationen innerhalb des empfangenen Eingabeinformationsflusses IN' mit einem digitalen Wasserzeichen versehen, so dass Copyright-Vermerke, Quellenangabe und andere Informationen, die z. B. mit der zulässigen Verwendung und/oder dem zulässigen Eigentum, des Eingabeinformationsflusses IN', in Bezug stehen, eingefügt werden können. Der Pixeldomain-Codierer **105** erzeugt einen Pixel- (oder Audio-) Domain-codierten Informationsfluss IN, der mit dem Segmentierungsmodul **110** gekoppelt ist. Es sollte angemerkt werden, dass im Kontext dieser Offenbarung der Begriff „Pixeldomain" verwendet wird, um mehr als die Pixel- oder Basisbandvideo- oder Bildinformation zu bezeichnen. Der Begriff „Pixeldomain" wird verwendet, um zusätzlich Audio- und andere Informationen (d.h. Daten) zu bezeichnen, die mit der Pixel- oder Basisbandvideo- oder Bildinformation des zugrunde liegenden Informationsflusses, der verarbeitet wird, verbunden sind.

[0025] Das Segmentierungsmodul **110** unterteilt den codierten (oder nicht codierten) Informationsfluss IN in eine Vielzahl von Segmenten, um einen segmentierten Informationsfluss zu erzeugen. Der segmentierte Informationsfluss wird dann mit der Komprimierung **115A** gekoppelt und wahlweise in einem ersten Lieferanten-Speichermodul **122** abgelegt.

[0026] Das heißt, dass das Segmentierungsmodul **110** den Eingabeinformationsfluss IN in eine Vielzahl Informationssegmente gleicher oder unterschiedlicher Länge, gemäß einer oder mehrerer von einer Vielzahl an Kriterien „zerhackt". Die Kriterien werden unten mit Bezug auf Fig. 3 detaillierter beschrieben.

[0027] In einer Ausführungsform der Erfindung kann das Segmentierungsmodul **110** den Eingabeinformationsfluss IN, beliebig in Segmente von z. B. 1000 Paketen bis zu einem angemessenen Flusssplеiß-Ausgangspunkt „zerhacken". In einer anderen Ausführungsform der Erfindung stellt das Segmentierungsmodul **110** eine vordefinierte, ungefähre Anzahl von Rahmen (z. B. 100 oder 1000 Rahmen) innerhalb eines Videoflusses dar. Das ausgewählte Rahmensegment schließt diejenigen Rahmen ein, die unmittelbar einem Szenenschnitt vorausgehen (z. B. diejenigen Rahmen, die unmittelbar einem I-Bild vorausgehen). In einer weiteren Ausführungsform der Erfindung werden das Segmentierungsmodul **110**, eine ungefähre Anzahl von Videorahmen und die damit verbundenen Audiorahmen ausgewählt, so dass das Segment, das dadurch gebildet wird, alle Audiorahmen einschließt, die mit dem Videosegment verbunden sind (d.h. keine Audiorahmen in einem Segment, die mit Videorahmen in einem anderen Segment in Bezug stehen).

[0028] Es ist wünschenswert, dass Hinterlassen von „Anhaltspunkten" zum Verwürfelungsverfahren zu vermeiden, mit denen ein Hacker in der Lage sein könnte, die verschiedenen Segmente zusammenzusetzen. Zum Beispiel können Audiorahmen mit bekannten Verbindungen zu Videorahmen dazu verwendet werden, um die entsprechende Anordnung der Videorahmen zu rekonstruieren. Das heißt, dass Unterbrechungen in der Audiospur (d.h. ein Bruch inmitten einer Musiknote oder eines Tons) aufeinander abgestimmt werden können, um ein Videosegment zu rekonstruieren. Daher werden in einer Ausführungsform der Erfindung die Audiorahmen von den Videorahmen getrennt segmentiert.

[0029] Die Segmentgröße wird mit Bezug auf das gewünschte Sicherheitsniveau (d.h. mehrere oder kleinere Segmente ergeben größere Sicherheit), die Struktur der zugrunde liegenden Informationen (d.h. feste oder variable Bildgruppen, häufige Videoszenenschnitte und dergleichen) festgelegt.

[0030] Das Komprimierungsmodul **115A** komprimiert den segmentierten Informationsfluss, z. B. gemäß eines MPEG- oder eines anderen Komprimierungsschemas, je nach der Art der Information, die verteilt wird. Zum Beispiel kann für den Fall, dass der

Eingabeinformationsfluss einen Videoinformationsfluss und einen verbundenen Audioinformationsfluss (z. B. ein Bewegtbild) umfasst, das Komprimierungsmodul **115A** verwendet werden, um die Videoinformation gemäß einer MPEG-2-Komprimierungstechnik und die Audioinformation gemäß einer AC-3- oder einer anderen Audio-Codierungstechnik zu codieren. Das Komprimierungsmodul **115A** erzeugt einen komprimierten Informationsfluss, der mit dem Neusequenzierungsmodul **130** gekoppelt ist und wahlweise in einem zweiten Lieferanten-Speichermodul **124** abgelegt wird.

[0031] Es sollte angemerkt werden, dass die Reihenfolge des Segmentierungsmoduls **110A** und des Komprimierungsmoduls **115A** umgekehrt werden kann. Somit wird in Abb. 1 ein alternativer Verarbeitungsweg für den Eingabeinformationsfluss IN bereitgestellt, in dem ein Komprimierungsmodul **115B** verwendet wird, um den Eingabeinformationsfluss IN vor der Segmentierung durch ein Segmentierungsmodul **110B** zu verarbeiten.

[0032] Das Neusequenzierungsmodul **130** organisiert die komprimierten Informationssegmente gemäß einem vorbestimmten oder pseudozufälligen Muster neu. Das heißt, dass das Neusequenzierungsmodul **130** den komprimierten und segmentierten Informationsfluss „mischt", um einen neu organisierten oder neu sequenzierten, komprimierten und segmentierten Informationsfluss und eine damit verbundene Indextabelle zu erzeugen, die den Neusequenzierungsvorgang, der am komprimierten und segmentierten Informationsfluss durchgeführt wird, angibt. Das Neusequenzierungsmodul **130** sequenziert die zugrunde liegende Video- und/oder Audioinformation, gemäß einem oder mehreren von verschiedenen Kriterien, wie z. B. Szenengrenzen, Bildsequenz-Größe, zeitliche oder Rahmenverschiebungen, Rahmenzählung und dergleichen, neu. Der neusequenzierte, komprimierte und segmentierte Informationsfluss wird mit dem Informationsfluss-Verschlüsselungsmodul **135** gekoppelt, während die verbundene Indextabelle mit dem Indextabellen-Verschlüsselungsmodul **140** gekoppelt wird. Optional wird die Ausgabe des Neusequenzierungsmoduls **130** mit dem dritten lokalen Speichermodul **126** gekoppelt.

[0033] Für das Verständnis der vorliegenden Erfindung ist es entscheidend, zu beachten, dass der Zweck des Segmentierungsmoduls **110A** und des Neusequenzierungsmoduls **115A** darin liegt, auf eine anscheinend zufällige Weise, z. B. die Video- und/oder Audioinformation, die mit einem zugrunde liegenden Audio-Video-Informationsfluss verbunden ist, neu zu organisieren, so dass die Darstellungskontinuität der zugrunde liegenden Audio-Video-Information zerstört wird. Das heißt, dass das Segmentierungsmodul **110A** und das Neusequenzierungsmodul **115A** die zeitliche Kontinuität der zugrunde liegenden Audio-Video-Information auf eine Weise entfernen, welche die Audio-Video-Information für einen Raubkopierer oder einen unbefugten Teilnehmer unbrauchbar oder zumindest ungenießbar macht.

[0034] Das Informationsfluss-Verschlüsselungsmodul **135** verwürfelt den neu sequenzierten, komprimierten und segmentierten Informationsfluss unter Verwendung einer oder mehrerer bekannter Verwürfelungstechniken. Außerdem wird die Indextabelle, die vom Neusequenzierungsmodul **130** erzeugt wird, mit einem anderen Verschlüsselungsmodul **140** gekoppelt, wo sie auf eine von mehreren bekannten Arten verschlüsselt wird, um eine verschlüsselte Indextabelle zu erzeugen. Der verschlüsselte Informationsfluss (d.h. der verwürfelte, neu sequenzierte, komprimierte und segmentierte Informationsfluss) und die verschlüsselte Indextabelle werden mit der Informationsverbraucher- oder teilnehmerseitigen Anlage z. B. über ein Verteilungsnetz **145** und/oder ein alternatives Verteilungsnetz **145A** gekoppelt.

[0035] Das optionale erste **122**, zweite **124** und dritte **126** lokale Speichermodul **126** wird verwendet, um die Ausgabe des Segmentierungsmoduls **110A** (oder des Komprimierungsmoduls **115B**), die Ausgabe des Komprimierungsmoduls **115A** (oder des Segmentierungsmoduls **110B**) beziehungsweise die Ausgabe des Neusequenzierungsmoduls **130**, zu speichern. Die lokalen Speichermodule können verwendet werden, um z. B. derartige Informationen für die weitere Verarbeitung durch zusätzliche Verarbeitungsvorrichtungen (nicht gezeigt) abzulegen oder die Verarbeitung eines gesamten Informationsflusses bei jedem Schritt zu ermöglichen (z. B. um die gesamte Segmentierung eines empfangenen Eingabeinformationsflusses IN durchzuführen, dann die gesamte Komprimierung des segmentierten Informationsflusses durchzuführen und dann die gesamte Neusequenzierung des komprimierten und segmentierten Informationsflusses durchzuführen usw.). Optional kann die serverseitige Anlage als ein vorübergehender Puffer während einer „Ein-Schritt"-Verarbeitung eines Eingabeinformationsflusses IN (wie z. B. einer Direktübertragung eines Baseballspiels) verwendet werden.

[0036] Das Verteilungsnetz **145A** und das alternative Verteilungsnetz **145B** kann jedes beliebige einer Anzahl von Standardverteilungsnetzen wie z. B. Mikrowellenverbindungen, Glasfasernetze, Satellitenverbindungen, Kabelfernsehverbindungen, DVD, Internet, Rundfunk und dergleichen, umfassen.

[0037] In einer Ausführungsform der Erfindung wird ein alternatives Verteilungsnetz **145B** verwendet, um einige aller verwürfelten Sequenzen, die vom Verschlüsselungsmodul **135** erzeugt werden, zu transportieren. Das heißt, dass das alternative Vertei-

lungsnetz **145B** verwendet werden kann, um z. B. jeden fünften oder einen anderen Teil der verwürfelten Sequenzen, die vom Verschlüsselungsmodul **135** erzeugt werden, zu transportieren. Auf diese Weise wäre ein unbefugter Nutzer, der die Information, die vom Verteilungsnetz **145A** übertragen wird, auch im Fall eines Entzifferns der verschiedenen Verschlüsselungscodes und einer geeigneten Neusequenzierung der verwürfelten Segmente, nicht dazu in der Lage, alle der verwürfelten Segmente wieder aufzufinden. Somit bietet das alternative Verteilungsnetz **145B** eine zusätzliche Sicherheitsschicht innerhalb des Informationsverteilungssystems **100** von Abb. 1.

[0038] Die teilnehmerseitige Anlage innerhalb des Informationsverteilungssystems **100** von Abb. 1 umfasst ein lokales Speichermodul **155**, ein Verschlüsselungsmodul **150**, ein zweites Verschlüsselungsmodul **160**, ein Direktzugriffsmodul **165**, ein Dekomprimierungsmodul **170** und ein optionales Pixeldomain-Decodierungsmodul **175**.

[0039] Das lokale Speichermodul **155** empfängt die verwürfelten Sequenzen, die vom Verteilungsnetz **145A** und/oder **145B** transportiert werden, und speichert die verwürfelten Sequenzen. Das erste Entschlüsselungsmodul **150** wird verwendet, um die verschlüsselte Indextabelle, die vom Verteilungsnetz **145A** transportiert wird, zu entschlüsseln, um eine entschlüsselte Indextabelle zu erzeugen. Die entschlüsselte Indextabelle ist mit dem Direktzugriffsmodul **165** gekoppelt. Das zweite Entschlüsselungsmodul **160** greift auf das lokale Speichermodul **155** zu, um verwürfelte Sequenzen, die gespeichert sind, abzurufen und, als Antwort darauf, diese verwürfelten Sequenzen zu entschlüsseln. Die entschlüsselten verwürfelten Sequenzen (d.h. nicht verwürfelten Sequenzen) werden dann mit dem Direktzugriffsmodul **165** gekoppelt. Das Direktzugriffsmodul **165** verwendet die Indextabelleninformation, die vom ersten Entschlüsselungsmodul **150** empfangen wurde, um die entwürfelten Sequenzen, die vom Entschlüsselungsmodul **160** erhalten wurden, neu zu organisieren, um einen geeigneten sequenzierten Informationsfluss an einer Ausgabestelle zu erzeugen. Das heißt, dass die Ausgabe des Direktzugriffsmoduls **165** einen Informationsfluss umfasst, der eine Vielzahl von Segmenten aufweist, die auf eine Weise angeordnet sind, die Kontinuität innerhalb des zugrunde liegenden, veranschaulichten audiovisuellen Informationsflusses bereitstellt. Das Dekomprimierungsmodul **170** empfängt den Informationsfluss, der vom Direktzugriffsmodul **165** erzeugt wird, der korrekt angeordnete Informationssegmente umfasst, und dekomprimiert als Antwort darauf den empfangenen Informationsfluss, um einen oder mehrere Ausgabeinformationsflüsse zu erzeugen (d.h. einen Audio-Informationsfluss, einen Video-Informationsfluss und jeden beliebigen Hilfsdatenfluss). Der Ausgabeinformationsfluss OUT wird optional dem Pixeldomain-Decodierungsmodul **175** unterworfen, in dem ein Pixeldomain-Decodierungsverfahren erfolgt, das dem Pixeldomain-Codierungsverfahren, das vom Pixelcodierer **105** durchgeführt wird, entgegensteht.

[0040] Abb. 2 stellt eine graphische Darstellung der Sammlung von Informationssegmenten, die in einer nicht standardmäßigen (d.h. verwürfelten) Reihenfolge angebracht sind, sowie eine Indextabelle, die für die Verwendung beim Neuorganisieren der Sammlung von Informationssegmenten in eine standardmäßige (d.h. nicht verwürfelte) Reihenfolge geeignet ist, dar. In der graphischen Darstellung von Abb. 2 wird die Sammlung von Informationssegmenten in einem Speicher, wie z. B. der lokalen Speichereinheit **155** des Systems **100** von Abb. 1, abgelegt, und die Indextabelle umfasst eine Liste von Speicherstellen aus denen gelesen wird, um die ursprüngliche Reihenfolge der Informationssegmente zu rekonstruieren. Auf diese Weise sind unzulässig erhaltene verteilte Daten, die verwürfelt sind, nicht brauchbar, außer die Indextabelle wird ebenfalls erhalten.

[0041] Insbesondere stellt Abb. 2 eine Verbindung zwischen sechs Stellen (A-F) und sechs Sequenzen (Sequenz 1 – Sequenz 6) dar. Es sollte angemerkt werden, dass in Abb. 2 eine ovale Anzeige eines Speichermoduls, die eine Tabelle enthält, welche die Stellen und die Sequenzen verbindet, gezeigt wird. Insbesondere ist die Stelle A mit Sequenz 3 verbunden, Stelle B ist mit Sequenz 5 verbunden, Stelle C ist mit Sequenz 2 verbunden, Stelle D ist mit Sequenz 1 verbunden, Stelle E ist mit Sequenz 6 verbunden und Stelle F ist mit Sequenz 4 verbunden. Somit gibt eine Indextabelle, welche die folgende Sequenz (D, C, A, F, B, E) umfasst, an, dass die Sequenz, die im Speicher abgelegt ist, vor der Verwendung gemäß den oben beschriebenen Verbindungen abgerufen werden sollte, um einen geeignet sequenzierten Informationsfluss zu erzeugen.

[0042] Abb. 3 stellt eine Fließroutine eines Bearbeitungsverfahrens eines Informationslieferanten gemäß der Erfindung dar. Die Routine **300**, die in Abb. 3 dargestellt ist, ist auf das Verarbeiten eines Audio-Video-Flusses gerichtet, um einen segmentierten, codierten, neu sequenzierten und verschlüsselten Audio- und Video-Informationsfluss und die verbundene Indexinformation, die für die Neusequenzierung der Segmente geeignet ist, zu erzeugen.

[0043] Die Routine **300** wird bei Schritt **302** eingegeben und führt zu Schritt **304**. Bei Schritt **304** wird ein optionales Pixeldomain-Codierungsverfahren auf der Videoinformation innerhalb eines empfangenen Audio-Video-Informationsflusses durchgeführt. Zum Beispiel kann das Pixeldomain-Codierungsverfahren von Schritt **304** ein Wasserzeichenmarkierungsverfahren, ein Pixelverschlüsselungsverfahren, ein Lip-

pensynchronisierungs-Änderungsverfahren, ein Audiounterdrückungsverfahren oder ein Farbablösungsverfahren umfassen. Die Wasserzeichenmarkierung umfasst die Einfügung der Identifizierung einer Ausgabe innerhalb eines Videoabschnitts eines Informationsflusses, so dass das Copyright und andere Quellenangabeinformationen innerhalb eines verteilten Informationsflusses, eingeschlossen werden können. Die Pixelverschlüsselung umfasst jede beliebige aus einer Anzahl von Verschlüsselungstechniken, welche die Pixelinformation, ohne das entsprechende Pixelentschlüsselungsverfahren, unbrauchbar machen. Die Lippensynchronisierungs-Veränderung umfasst eine Änderung der Synchronisierung der Video- und der damit verbundenen Audioinformationen, auf der Grundlage eines zufälligen oder vorbestimmten zeitlichen Parameters, so dass Video und Audio nicht mehr synchronisiert sind, wobei die Darstellung des Audio-Video-Informationsflusses schwer beeinträchtigt wird. Die Audiounterdrückung umfasst Techniken zum Unterdrücken oder anderweitigen Verbergen von Audioinformationen von einem nachgeschalteten Audiodecodierer, so dass die Audioinformationen nur von einem Decodierer abgerufen werden können, der die neue Stelle oder die Codierungstechnik kennt, die verwendet wird, um die Audioinformationen zu verbergen. Die Farbablösung umfasst ein Verfahren zum Beseitigen oder Verbergen der Farbinformationen von einem nachgeschalteten Videodecodierer, so dass die Farbinformationen nur von einem Decodierer abgerufen werden können, der die Stelle oder die Technik kennt, die verwendet wird, um die Farbinformationen zu verbergen. Die Routine **300** führt dann zu Schritt **306**.

[0044] Bei Schritt **306** wird der Audio-Video-Informationsfluss in eine Vielzahl von benachbarten Informationsflusssegmenten unterteilt. Diese Segmente können hinsichtlich Szenenschnitt-Anhaltspunkten, zeitlichen Verschiebungsparametern, Rahmenzählungen, Bildsequenz-Struktur und dergleichen, festgestellt werden. Die Segmente können die gleiche oder im Wesentlichen, die gleiche Länge aufweisen, oder die Segmente können variable Längen aufweisen. Jedes Segment ist mit einer Segmentidentifizierung verbunden, so dass die ursprüngliche Segmentanordnung durch das Speichern der Segmentidentifizierungen mit einer Flussindextabelle gewahrt werden kann. Die Routine **300** führt dann zu Schritt **308**.

[0045] Bei Schritt **308** werden die Segmente z. B. gemäß der MPEG-2-Video- und verbundenen Audio-Komprimierungstechniken komprimiert. Da die Flusssegmente, die bei Schritt **306** erzeugt werden, typischerweise, hinsichtlich des Pufferverhaltens, in sich geschlossen sind, können die Komprimierungsverfahren, die bei Schritt **308** verwendet werden, parallel durchgeführt werden. Das heißt, dass zahlreiche audiovisuelle Flusssegmente unter Verwendung einer parallelen Verarbeitungs- oder parallelen Codierungstechnik, parallel komprimiert werden können. Andernfalls kann ein einzelnes MPEG- oder anderes Komprimierungsmodul verwendet werden, um jedes Flusssegment auf eine standardmäßige Weise zu verarbeiten, um einen komprimierten Ausgabefluss zu erzeugen, der eine Vielzahl von komprimierten Flusssegmenten umfasst. Die Routine **300** führt dann zu Schritt **310**. Bei Schritt **310** werden die komprimierten Flusssegmente neu sequenziert (d.h. „gemischt"), um einen neu sequenzierten, komprimierten Audio-Video-Informationsfluss und eine verbundene Indextabelle zu erzeugen. Die Indextabelle enthält Informationen, welche die neu sequenzierten Segmente mit der anfänglichen Sequenz von Segmenten in Bezug bringt, so dass die neu sequenzierten Informationsflusssegmente neu organisiert werden können, um die anfängliche Reihenfolge der Flusssegmente zu erzeugen. Die Routine **300** führt dann zu Schritt **312**.

[0046] Bei Schritt **312** wird jedes der neu sequenzierten Informationsflusssegmente verschlüsselt, um einen Informationsfluss zu erzeugen, der eine Vielzahl von verschlüsselten, neu sequenzierten Informationsflusssegmenten umfasst. Die Routine **300** führt dann zu Schritt **314**, wo die Indextabelle, die verwendet wird, um Verbindungen zwischen den Segmenten zu pflegen, selbst verschlüsselt wird. Die Routine **300** führt dann zu Schritt **316**. Bei Schritt **316** werden die verschlüsselten Informationsflusssegmente und die verschlüsselte Indextabelle, z. B. über ein Informationsverteilungsnetz verteilt. Die Routine **300** führt dann zu Schritt **318**, wo sie beendet wird.

[0047] Abb. 4 stellt ein Flussdiagramm eines teilnehmerseitigen Verfahrens zur Bearbeitung eines Informationsflusses gemäß der Erfindung dar. Insbesondere ist die Routine **400** von Abb. 4 darauf gerichtet, eine empfangene verschlüsselte Indextabelle und verschlüsselte Informationssegmente zu bearbeiten, um einen geeigneten sequenzierten audiovisuellen Informationsfluss für die nachfolgende Darstellung zu extrahieren. Die Routine **400** wird bei Schritt **402** eingegeben und geht zu Schritt **404** weiter.

[0048] Bei Schritt **404** wird eine verschlüsselte Indextabelle, die über ein Verteilungsnetz empfangen wird, entschlüsselt, um eine brauchbare Indextabelle bereitzustellen. Die Routine **400** führt dann zu Schritt **406**, wo eine Vielzahl von verschlüsselten Informationsflusssegmenten entschlüsselt wird, um entschlüsselte Informationsflusssegmente zu erzeugen. Es muss angemerkt werden, dass sich die entschlüsselten Informationsflusssegmente nicht in einer korrekten Sequenz, hinsichtlich der zugrunde liegenden audiovisuellen Informationen, befinden. Das heißt, die entschlüsselten Informationssegmente werden so „gemischt", dass die Darstellung der verschlüsselten Informationsflusssegmente (natürlich nach der

Dekomprimierung) zu einer unerwünscht unruhigen, zeitlich unterbrochenen audiovisuellen Darstellung führen würde. Die Routine **400** führt dann zu Schritt **408**.

[0049] Bei Schritt **408** wird auf die entschlüsselten Informationsflusssegmente, gemäß der Information innerhalb der entschlüsselten Indextabelle, zugegriffen. Insbesondere gibt die entschlüsselte Indextabelle eine korrekte zeitliche Reihenfolge oder Sequenz, für die entschlüsselten Informationsflusssegmente, an. Entschlüsselte Informationsflusssegmente werden z. B. von einem lokalen Speichermodul in einer korrekten zeitlichen oder sequentiellen Reihenfolge, wie von der entschlüsselten Indextabelle angegeben, abgerufen, um einen geeignet sequenzierten und komprimierten Informationsfluss zu erzeugen. Die Routine **400** führt dann zu Schritt **410**, wo der korrekt sequenzierte und komprimierte Informationsfluss dekomprimiert wird, um einen dekomprimierten audiovisuellen Informationsfluss zu erzeugen. Zum Beispiel ist das Dekomprimierungsverfahren bei Schritt **410**, dem Komprimierungsverfahren, das bei Schritt **308** der Routine **300** von Abb. 3 verwendet wird, entgegengesetzt. Die Routine **400** führt dann zu Schritt **412**.

[0050] Bei Schritt **412** wird ein optionales Pixeldomain-Decodierungsverfahren verwendet, um jede beliebige Pixeldomain-Codierung zu decodieren, die dem Informationsfluss bei Schritt **304** der Routine **300** von Abb. 3 übertragen wird. Die Routine **400** führt dann zu Schritt **414**, wo sie beendet wird.

[0051] Die oben beschriebene Erfindung stellt gleichzeitig sowohl Flexibilität als auch Sicherheit bei elektronisch gespeicherten Videoinformationen bereit. Die grundlegende Beobachtung ist, dass Videoinformationen, die in einer Direktzugriffs-Speichervorrichtung abgelegt sind, hinsichtlich ihres Darstellungsflusses neu sequenziert werden können, wenn sie auf eine geeignete Weise komprimiert werden. Im normalen Betrieb kann ein komprimiertes Video typischerweise nicht zerhackt und in Segmenten gespeichert werden, da die Verwendung einer doppeltgerichteten Bewegungsvorhersage und die Beschränkungen der weder über- noch unterlaufenden Ratenpuffer, einen derartigen Betrieb verbieten. Die MPEG-2-Syntax stellt jedoch sehr wohl Mechanismen bereit, um Abschnitte des Videoflusses, als in sich geschlossene Einheiten zu behandeln. Diese Mechanismen umfassen die Verwendung von I- und P-Rahmen-Bildsequenz-Strukturen (z. B. „IPP-PPPPI...") oder anderer „geschlossener" Bildsequenz-Strukturen (z. B. „IBBPBBPI...") und die Verwendung einer Spleißpunktsyntax, die periodische Punkte angibt, an denen die Puffer bis zu einem bekannten Zustand gefüllt sind. Die Erfindung stellt ein Gesamtsystem bereit, das sowohl Flexibilität als auch Sicherheit einschließt.

[0052] Es muss angemerkt werden, dass, falls die Segmente nicht in sich geschlossen sind (z. B. keine geschlossene Bildsequenz-Struktur vorliegt), der VBV-Pufferstatus an den Grenzen Informationen liefern würde, um beim Aufbrechen der Verwürfelung und der Wiederanordnung der geeigneten Video- oder Audiosequenz ohne den entschlüsselten Index von großer Hilfe zu sein.

[0053] Es ist wichtig anzumerken, dass die Erfindung sich mit Sicherheitsschwächen befasst, die mit den Kontinuitätsanzeigern wie z. B. der Audiokontinuität, dem VBV-Pufferstatus, den PTS- und DTS-Informationen und dergleichen verbunden sind. Diese Kontinuitätsanzeiger sind nützlich für diejenigen, die versuchen, die Sicherheit des Systems aufzubrechen und die „gesicherten" Daten abzurufen. Durch Isolieren oder Einkapseln dieser Kontinuitätsanzeiger innerhalb eines Segmentes und anschließendem Codieren des Segmentes sind die Kontinuitätsanzeiger bei der Decodierung des Segmentes nicht nützlich.

[0054] Abb. 5 stellt eine schematische Darstellung einer geschichteten Sicherheitsumgebung dar, die von der Erfindung ermöglicht wird. Insbesondere stellt Abb. 5 eine Reihe von konzentrischen Kreisen dar, welche die Sicherheitsschichten darstellen. Die verschiedenen Sicherheitsschichten wurden oben hinsichtlich Abb. 1-Abb. 4 detailliert beschrieben. Abb. 5 ist nützlich, um den ganzheitlichen und dennoch flexiblen Sicherheitsansatz, der von der Erfindung ermöglicht wird, zu verstehen.

[0055] Insbesondere wird eine erste Sicherheitsschicht von der Schicht **510** bereitgestellt, die eine Pixeldomain oder eine andere Basisband-Informationsdomain (z. B. Audio- oder Datendomain) verarbeitet. Wie bereits erörtert kann das beispielhafte Pixeldomainverfahren, z. B. ein digitales Wasserzeichen der Videoinformationen, das Einfügen von Copyright-Vermerken und anderer Pixeldomain-Sicherheitsmeldungen umfassen. Im Fall eines Informationsflusses, der einen Audio-Informationsfluss oder einen anderen Informationsfluss beinhaltet, umfasst das Pixeldomainverfahren natürlich ein Audiodomainverfahren oder ein anderes Datendomainverfahren.

[0056] Die Sicherheitsgesichtspunkte der Pixeldomain-Verarbeitungsschicht **510** werden durch die Flusssegmentierungs-Verarbeitungsschicht **520** erhöht. Die Sicherheitsgesichtspunkte der Flusssegmentierungs-Verarbeitungsschicht **520** werden durch die Flusssegment-Verwürfelungs- oder Neusequenzierungsschicht **530** erhöht. Die Sicherheitsgesichtspunkte der Flusssegment-Verwürfelungs- oder Neusequenzierungsschicht **530** werden durch die Verschlüsselungsschicht **540** einschließlich einer optionalen Index-Verschlüsselungsschicht **535** erhöht.

[0057] Außer den oben beschriebenen Sicherheitsschichten **510**-**540** werden zwei zusätzliche optionale Sicherheitsschichten bereitgestellt. Die erste der zusätzlichen optionalen Schichten umfasst eine Mehrwegeverteilungsschicht **550**, in der ein Informationsfluss, der gemäß einem oder mehreren der Verarbeitungsschritte **510** bis **540** verarbeitet wird, an einen oder mehrere Anwender über zahlreiche Signalwege übertragen oder verteilt wird. Zum Beispiel kann der verschlüsselte Index, der bei Schritt **535** erzeugt wird, über einen anderen Signalweg oder ein anderes Signalmedium, als die verschlüsselte Sequenz aus segmentierten oder neu verwürfelten Informationsrahmen, die bei Schritt **540** erzeugt wird, übertragen werden.

[0058] Die zweite der zusätzlichen optionalen Schichten umfasst die zeitlich gestaffelte Schicht **560**, in der Abschnitte des Informationsflusses, der gemäß einem oder mehreren der Verarbeitungsschritte **510** bis **540** verarbeitet wurde, an einen oder mehrere Informationsverbraucher auf eine zeitlich nicht sequentielle Weise übertragen werden. Das heißt, dass benachbarte Informationsflusssegmente zu verschiedenen Zeiten (d.h. auf eine zeitlich nicht sequentielle Weise) übertragen und vom/von den Informationsverbraucher/Informationsverbrauchern zeitlich neu zusammengefügt werden.

[0059] Im Falle eines einzelnen Übertragungskanals kann die zeitlich gestaffelte Sicherheitsschicht **560** aufgrund der innewohnenden Natur der zeitlichen Staffelung (d.h. innewohnende Nicht-Echtzeit-Verwendung eines einzelnen Kanals) nicht für die Echtzeit-Verteilung von sicheren Informationsflüssen verwendet werden. Zeitliche Staffelung, gekoppelt mit Mehrwegeverteilung, kann jedoch verwendet werden, um Echtzeit-Informationsflüsse zu verteilen. Wenn z. B. drei verschiedene Kommunikationskanäle verwendet werden, um verschlüsselte Informationssegmente zu verteilen, dann kann jeder der drei Kanäle verwendet werden, um verschlüsselte Informationssegmente zu verteilen, die um drei Segmente vom Informationssegment, das zuvor auf diesem Kanal übertragen wurde, versetzt sind. Von der Perspektive eines einzelnen Kanals ist jedes der übertragenen Informationssegmente zeitlich von einem vorhergehenden oder einem nachfolgenden Informationsflusssegment um die Zeit versetzt, die normalerweise mit der Übertragung der zwei dazwischen liegenden Informationsflusssegmente verbunden ist (d.h. die Zeit, die normalerweise der Übertragung der zwei Informationsflusssegmente, die von den anderen zwei Kanälen übertragen wird, zugewiesen wird, wird nicht von dem einen Kanal verwendet). Optional kann diese Totzeit mit Dummy-Informationen oder Informationen gefüllt werden, die wahrscheinlich Fehler erzeugen oder auf andere Weise dabei helfen, unbefugte Benutzer abzuschrecken.

[0060] In einer Ausführungsform der Erfindung werden ein oder mehrere Informationsverteilungskanäle verwendet, um eine Vielzahl von segmentierten Informationsflüssen zu übertragen. In dieser Ausführungsform der Erfindung sind die Informationssegmente, die mit jedem der Vielzahl von segmentierten Informationsflüssen verbunden sind, über die eine oder mehrere Informationen, die übertragen werden sollen, verschachtelt und zwischen einem oder mehreren Informationsverteilungskanälen verschachtelt. Die segmentierten Informationsflüsse können optional Verschlüsselungscodes teilen. Das Verschachtelungsverfahren kann fest oder dynamisch sein. Im Falle eines dynamischen Verschachtelungsverfahrens können Informationen, die für die Rekonstruktion der verschiedenen Informationsflüsse geeignet sind, innerhalb einer oder mehrerer Indextabellen bereitgestellt werden.

[0061] Während der Sicherheitsumfang, der von einer individuellen Sicherheitsschicht geleistet wird, grob von der relativen Position der individuellen Sicherheitsschicht dargestellt wird, muss angemerkt werden, dass jede Schicht auf eine andere Sicherheitsbedrohung ausgerichtet ist. Zum Beispiel richtet sich die Pixeldomain- (oder allgemeiner, die Basisband-Informationsdomain-) Schicht an die Identifizierung und/oder Verfolgung von unbefugter Informationsflussverwendung und/oder unbefugten Informationsflussverwendern. Die Segmentverwürfelungs- und Verschlüsselungsschichten richten sich an die Bedrohung von Hackern oder anderen unbefugten Verwendern, die Zugang zu nützlichen Daten innerhalb eines empfangenen Informationsflusses erlangen. Die Mehrfachkanalübertragungs- und zeitlichen Staffelungsschichten sind auf die physische Vermeidung des Empfangs von Informationsflüssen durch unbefugte Verwender ausgerichtet. Der gesamte geschichtete Ansatz richtet sich auf das Bereitstellen von selektiven Sicherheitsschichten, z. B. je nach der Empfindlichkeit der Information, die verteilt werden soll. Zum Beispiel kann es für unnötig erachtet werden, eine elektronische Programmzeitschrift zu sichern. Dagegen ist es absolut erforderlich, einen Premierenfilm, der für die spätere Vorführung an Kinos verteilt wird, zu sichern.

[0062] Obwohl verschiedene Ausführungsformen, welche die Lehren der vorliegenden Erfindung einschließen, hier detailliert gezeigt und beschrieben wurden, kann ein Fachmann leicht viele andere verschiedene Ausführungsformen entwickeln, die diese Lehren immer noch einschließen.

Patentansprüche

1. Verfahren zum Sichern eines Informationsflusses in einem Informationsverarbeitungssystem, eine Sequenz von Informationsrahmen umfassend, wobei das Verfahren die folgenden Schritte beinhaltet:

Segmentieren (**306**; **110A**) des Informationsflusses in eine Vielzahl von Informationsflusssegmente mit einer ersten Segmentsequenz, wobei jedes der Informationsflusssegmente eine Vielzahl von Informationsrahmen umfasst; dann
Komprimieren (**308**; **115A**) der Informationsrahmen, welche die Informationsflusssegmente bilden; dann
Neusequenzieren (**310**; **130**) der komprimierten Informationsflusssegmente, um einen neu sequenzierten Informationsfluss mit einer zweiten Segmentsequenz zu erzeugen, wobei die erste Segmentsequenz durch einen Index mit der zweiten Segmentsequenz verbunden ist; und dann
Verschlüsseln (**312**; **314**; **135**; **140**) des neu sequenzierten Informationsflusses und des Indexes.

2. Verfahren zum Sichern eines Informationsflusses in einem Informationsverarbeitungssystem, umfassend eine Sequenz von Informationsrahmen, wobei das Verfahren die folgenden Schritte umfasst:
Komprimieren (**308**; **115B**) des Informationsflusses; dann
Segmentieren (**306**; **110b**) des komprimierten Informationsflusses in eine Vielzahl von
Informationsflusssegmente mit einer ersten Segmentsequenz, wobei jedes der Informationsflusssegmente eine Vielzahl von Informationsrahmen umfasst; dann
Neusequenzieren (**310**; **130**) der komprimierten Informationsflusssegmente, um einen neu sequenzierten Informationsfluss mit einer zweiten Segmentsequenz zu erzeugen, wobei die erste Segmentsequenz durch einen Index mit der zweiten Segmentsequenz verbunden ist; und dann
Verschlüsseln (**312**; **314**; **135**; **140**) des neu sequenzierten Informationsflusses und des Indexes.

3. Das Verfahren nach Patentanspruch 1 oder Patentanspruch 2, weiter umfassend die folgenden Schritte:
Verteilen (**316**) des verschlüsselten neu sequenzierten Informationsflusses und des Indexes an einen oder an mehrere Informationsverbraucher.

4. Verfahren nach Anspruch 3, wobei der Schritt des Verteilens die folgenden Schritte umfasst:
Verteilen des verschlüsselten neu sequenzierten Informationsflusses über ein erstes Medium (**145B**); und
Verteilen des verschlüsselten Indexes über ein zweites Medium (**145A**).

5. Das Verfahren nach Patentanspruch 3, wobei die verschlüsselten und neu sequenzierten Informationsflusssegmente auf eine zeitlich unterbrochene Weise an den einen oder an mehrere Informationsverbraucher verteilt werden.

6. Das Verfahren nach Patentanspruch 4, wobei:
das erste Verteilungsmedium eine Vielzahl von Verteilungskanälen umfasst und jeder dieser Vielzahl von Verteilungskanälen eine entsprechende Vielzahl der verschlüsselten und neu sequenzierten Informationsflusssegmente verteilt.

7. Das Verfahren nach Patentanspruch 1 oder Patentanspruch 2, wobei:
ein erster komprimierter Informationsrahmen innerhalb jedes der Informationssegmente einen nicht vorhergesagten Informationsrahmen umfasst.

8. Das Verfahren nach Patentanspruch 1 oder Patentanspruch 2, wobei:
der Informationsfluss eine Vielzahl von Bilderrahmen und verbundenen Audiorahmen umfasst; und
jedes der Informationsflusssegmente eine entsprechende erste Vielzahl von Bilderrahmen und eine entsprechende zweite Vielzahl von Audiorahmen umfasst, wobei die erste Vielzahl von Bilderrahmen und die zweite Vielzahl von Audiorahmen für die Darstellung, im Wesentlichen während desselben Zeitraums, vorgesehen sind.

9. Das Verfahren nach Patentanspruch 1 oder Patentanspruch 2, wobei der Informationsfluss eine Vielzahl von Bilderrahmen und verbundenen Audiorahmen umfasst, und wobei der Schritt des Segmentierens die folgenden Schritte beinhaltet:
Segmentieren des Informationsflusses in eine Vielzahl von Bildinformations-Flusssegmente mit einer ersten Segmentsequenz, wobei jedes der Bildinformations-Flusssegmente eine Vielzahl von Bilderrahmen umfasst
Segmentieren des Informationsflusses in eine Vielzahl von Audioinformations-Flusssegmente mit einer dritten Segmentsequenz, wobei jedes der Audioinformations-Flusssegmente eine Vielzahl von Bilderrahmen umfasst.

10. Das Verfahren nach Patentanspruch 1 oder Patentanspruch 2, wobei
der Schritt des Komprimierens des Informationsflusses oder der Informationsrahmen eine Kontrollinformation erzeugt, die ein Verwendungsniveau eines Decodierpuffers angibt; und
der Schritt des Verschlüsselns einen Schritt des Verschlüsselns der Anhaltspunkte der Decodierpufferverwendung umfasst.

11. Verfahren zum Rückgewinnen von Informationsrahmen aus einem Informationsfluss, der gemäß dem Sicherungsverfahren jedes beliebigen der Ansprüche 1 bis 9 gebildet wird, wobei das Verfahren zum Rückgewinnen die folgenden Schritte beinhaltet:
Rückgewinnen (**404**) des Indexes, der die zweite Segmentsequenz mit der ersten Segmentsequenz verbindet;
Entschlüsseln (**406**) der verschlüsselten Informationsflusssegmente, um entsprechende entschlüsselte Informationsflusssegmente zu erzeugen

Neusequenzieren (**408A**, **408B**) der entschlüsselten Informationsflusssegmente unter Verwendung des zurück gewonnenen Indexes und
Dekomprimieren (**410A**, **410B**) der komprimierten Informationsrahmen, die innerhalb der entschlüsselten Informationsflusssegmente eingeschlossen sind, unter Verwendung eines Dekomprimierungsverfahrens, das mit dem Komprimierungsverfahren verbunden ist.

12. Das Verfahren nach Patentanspruch 11, wobei der Schritt des Neusequenzierens die folgenden Schritte beinhaltet:
Zugreifen von einem Direktzugriffsspeicher (**165A**, **165B**), der mindestens einige der entschlüsselten Informationsflusssegmente enthält, auf die entschlüsselten Informationsflusssegmente gemäß der ersten Segmentsequenz.

13. Informationsverarbeitungssystem, umfassend:
ein Segmentierungsmodul (**110A**), um einen Informationsfluss in eine Vielzahl von Informationsflusssegmente zu segmentieren, wobei die Informationsflusssegmente gemäß einer ersten Segmentsequenz angeordnet sind und jedes der Informationsflusssegmente eine Vielzahl von Informationsrahmen umfasst;
ein Komprimierungsmodul (**115A**), um die Informationsrahmen, welche die Informationsflusssegmente bilden, zu komprimieren;
ein Neusequenzierungsmodul (**130**), um gemäß einer zweiten Segmentsequenz neu zu organisieren, wobei die Informationsflusssegmente die komprimierten Informationsrahmen einschließen und die erste Segmentsequenz durch einen Index mit der zweiten Segmentsequenz verbunden ist; und
ein Verschlüsselungsmodul (**135**), um die neu sequenzierten Informationsflusssegmente und den Index zu verschlüsseln.

14. Informationsverarbeitungssystem, umfassend:
ein Komprimierungsmodul (**115B**), um den Informationsfluss zu komprimieren;
ein Segmentierungsmodul (**110B**), um den komprimierten Informationsfluss in eine Vielzahl von Informationsflusssegmenten zu segmentieren, wobei die Informationsflusssegmente gemäß einer ersten Segmentsequenz angeordnet sind und jedes der Informationsflusssegmente eine Vielzahl von Informationsrahmen umfasst;
ein Neusequenzierungsmodul (**130**), um gemäß einer zweiten Segmentsequenz neu zu organisieren, wobei die Informationsflusssegmente die komprimierten Informationsrahmen einschließen und die erste Segmentsequenz durch einen Index mit der zweiten Segmentsequenz verbunden ist; und
ein Verschlüsselungsmodul (**135**), um die neu sequenzierten Informationsflusssegmente und den Index zu verschlüsseln.

Es folgen 5 Blatt Zeichnungen

Anhängende Zeichnungen

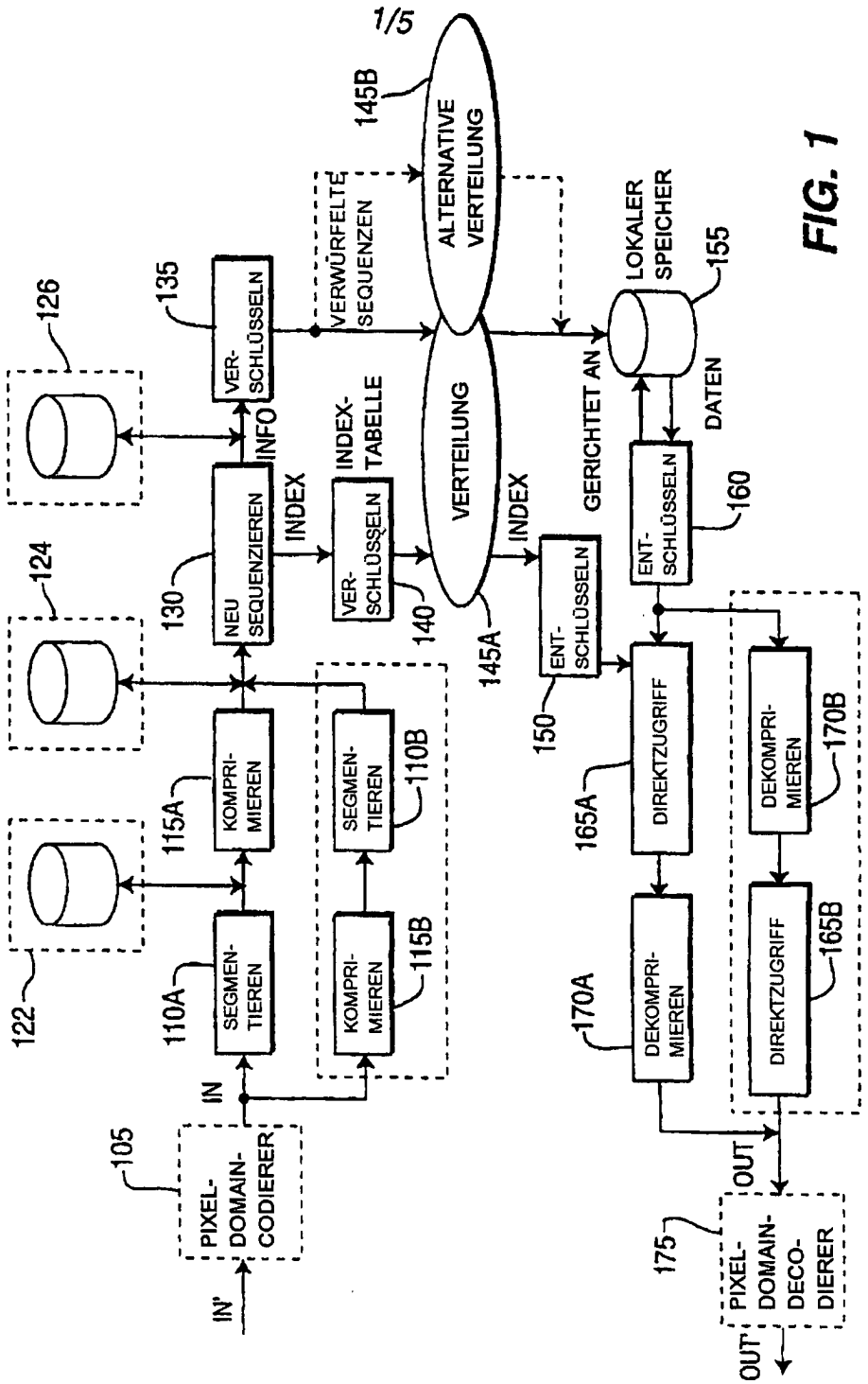

FIG. 1

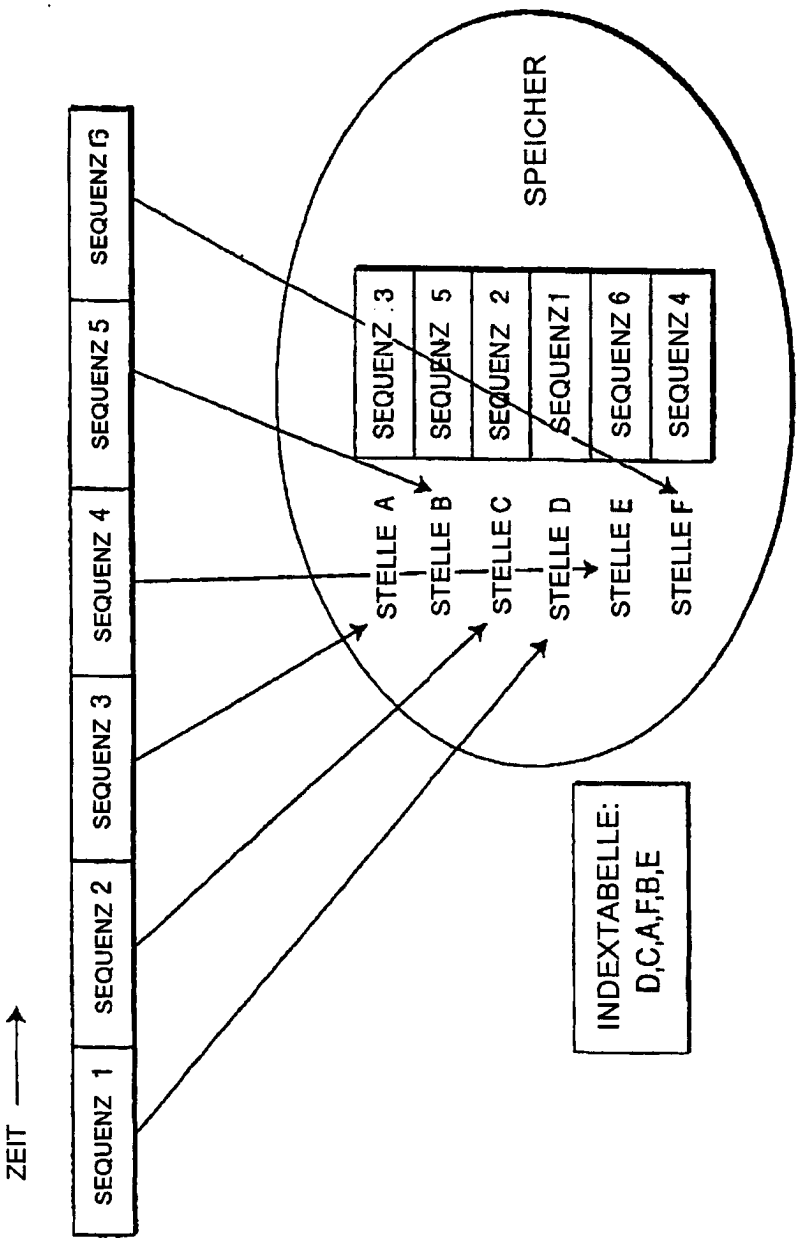
ZEIT
SEQUENZ 1
SEQUENZ 2
SEQUENZ 3
SEQUENZ 4
SEQUENZ 5
SEQUENZ 6
SPEICHER
SEQUENZ 3
SEQUENZ 5
SEQUENZ 2
SEQUENZ1
SEQUENZ 6
SEQUENZ 4
STELLE A
STELLE B
STELLE C
STELLE D
STELLE E
STELLE F
INDEXTABELLE:
D,C,A,F,B,E

FIG. 2

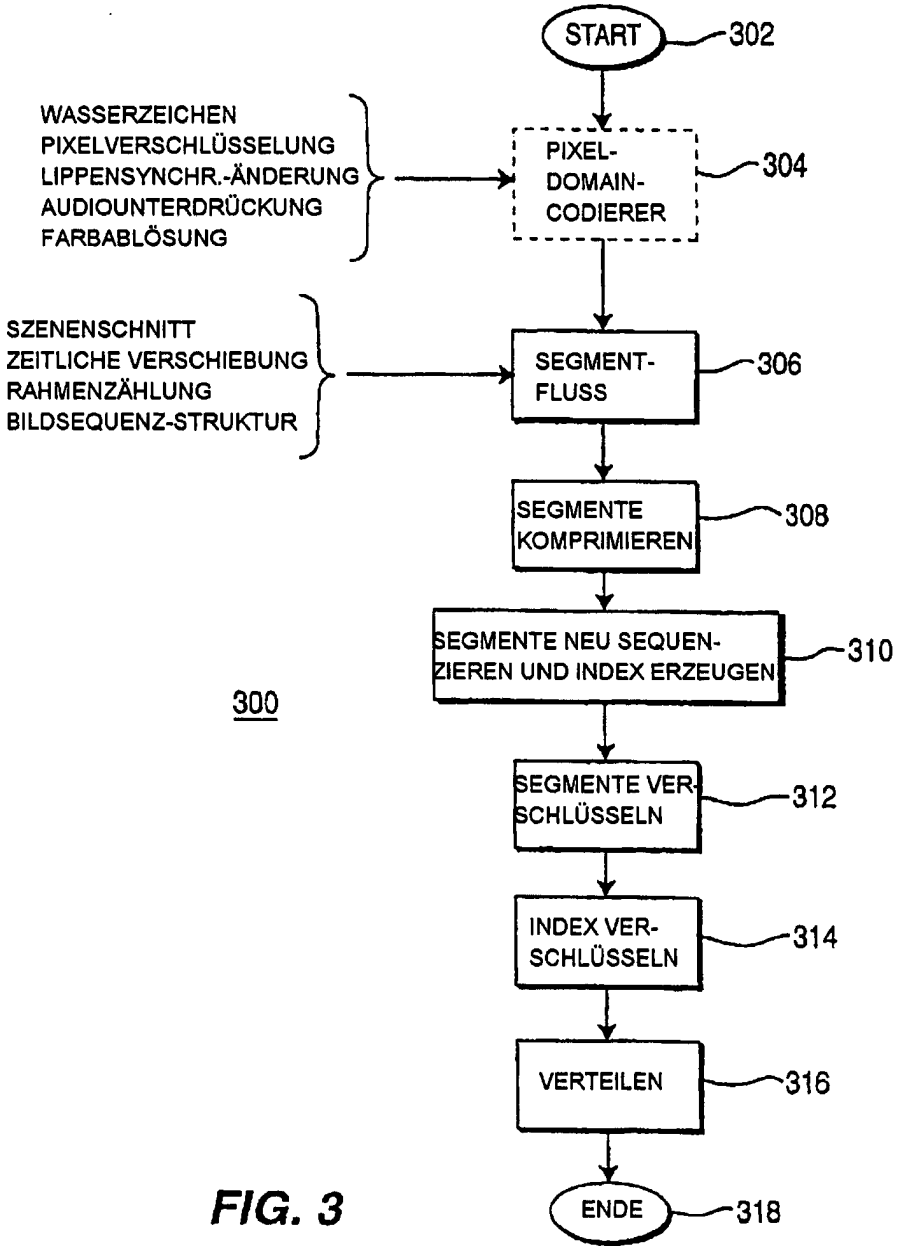
START
302
WASSERZEICHEN
PIXELVERSCHLÜSSELUNG
LIPPENSYNCHR.-ÄNDERUNG
AUDIOUNTERDRÜCKUNG
FARBABLÖSUNG
PIXEL-DOMAIN-CODIERER
304
SZENENSCHNITT
ZEITLICHE VERSCHIEBUNG
RAHMENZÄHLUNG
BILDSEQUENZ-STRUKTUR
SEGMENT-FLUSS
306
SEGMENTE KOMPRIMIEREN
308
SEGMENTE NEU SEQUEN-ZIEREN UND INDEX ERZEUGEN
310
300
SEGMENTE VER-SCHLÜSSELN
312
INDEX VER-SCHLÜSSELN
314
VERTEILEN
316
ENDE
318

FIG. 3

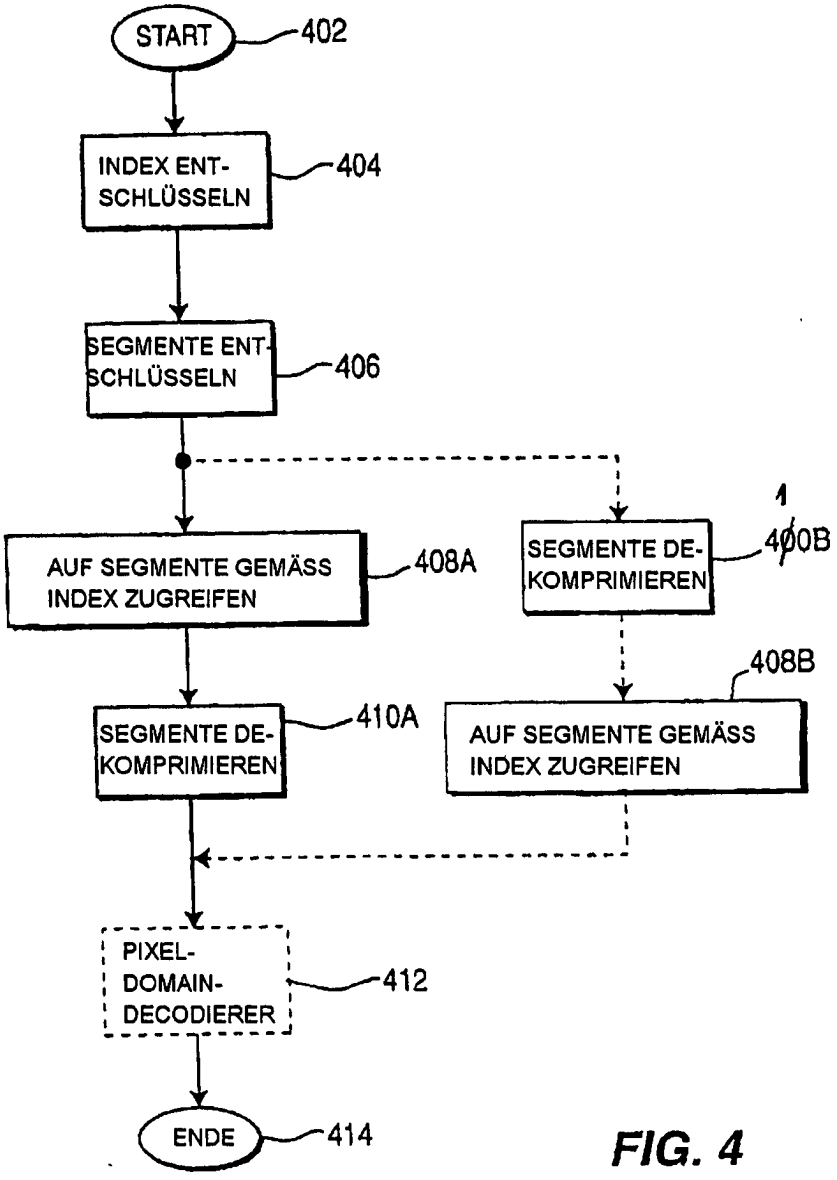
START
402
INDEX ENT-SCHLÜSSELN
404
SEGMENTE ENT-SCHLÜSSELN
406
AUF SEGMENTE GEMÄSS INDEX ZUGREIFEN
408A
SEGMENTE DE-KOMPRIMIEREN
410A
SEGMENTE DE-KOMPRIMIEREN
410B
AUF SEGMENTE GEMÄSS INDEX ZUGREIFEN
408B
PIXEL-DOMAIN-DECODIERER
412
ENDE
414

FIG. 4

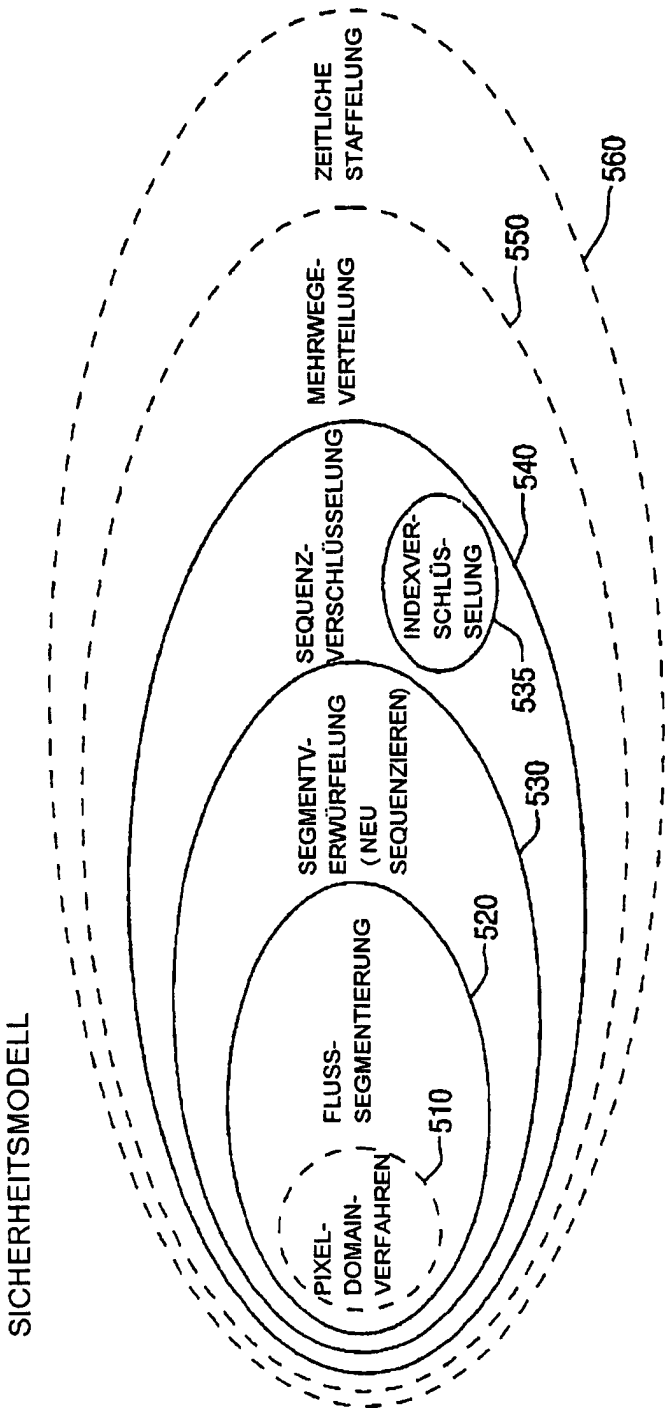
SICHERHEITSMODELL
PIXEL-DOMAIN-VERFAHREN
FLUSS-SEGMENTIERUNG
510
520
SEGMENTV-ERWÜRFELUNG (NEU SEQUENZIEREN)
530
SEQUENZ-VERSCHLÜSSELUNG
INDEXVER-SCHLÜS-SELUNG
535
540
MEHRWEGE-VERTEILUNG
550
ZEITLICHE STAFFELUNG
560

FIG. 5