(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4860149号
(P4860149)

(45)発行日　平成24年1月25日(2012.1.25)　(24)登録日　平成23年11月11日(2011.11.11)

(51)Int.Cl.			F I		
H04N	7/26	(2006.01)	H04N	7/13	Z
H04N	7/16	(2011.01)	H04N	7/16	Z
H04N	1/387	(2006.01)	H04N	1/387	

請求項の数 3　(全 19 頁)

(21)出願番号	特願2004-520106 (P2004-520106)
(86)(22)出願日	平成15年7月9日 (2003.7.9)
(65)公表番号	特表2005-533410 (P2005-533410A)
(43)公表日	平成17年11月4日 (2005.11.4)
(86)国際出願番号	PCT/US2003/021592
(87)国際公開番号	WO2004/006168
(87)国際公開日	平成16年1月15日 (2004.1.15)
審査請求日	平成18年7月4日 (2006.7.4)
(31)優先権主張番号	60/394,630
(32)優先日	平成14年7月9日 (2002.7.9)
(33)優先権主張国	米国(US)
(31)優先権主張番号	60/394,922
(32)優先日	平成14年7月9日 (2002.7.9)
(33)優先権主張国	米国(US)

(73)特許権者　505013158
カレイドスケイプ・インコーポレイテッド
ＫＡＬＥＩＤＥＳＣＡＰＥ，　ＩＮＣ．
アメリカ合衆国９４０８５－４１１７カリフォルニア州サニーベイル、ポトレロ・アベニュー４４０番
(74)代理人　100105924
弁理士　森下　賢樹
(72)発明者　スティーブン・ワトソン
カナダ、エム６ジー・２ワイ４、オンタリオ、トロント、クリントン・ストリート６５番

最終頁に続く

(54)【発明の名称】デジタルコンテンツマーキング方法、デジタルコンテンツ内のフィンガープリントを検出する方法、デジタルコンテンツ、デジタルコンテンツに透かしを入れる装置、透かしを入れたデジタル

(57)【特許請求の範囲】

【請求項１】

データが埋め込まれた符号化デジタルコンテンツ内の一組の符号化ブロックを決定するステップと、

それぞれが前記一組の符号化ブロックのうちの一つの符号化ブロックに関連付けられている、複数の可能な代替ブロックを特定するステップと、

前記複数の可能な代替ブロックから一つの代替ブロックのサブセットを選択し、前記代替ブロックのサブセットに関連付けられた複数の符号化ブロックに代えて、前記代替ブロックのサブセットを前記デジタルコンテンツ内に挿入することによって、前記デジタルコンテンツ内にフィンガープリントを埋め込むステップとを含み、

前記可能な代替ブロックのそれぞれは、関連付けられた符号化ブロックの可変長コード（ＶＬＣ）の改変であり、関連付けられた符号化ブロック内の第１の可変長コードのビット長を増加させる第１の改変と、前記第１の可変長コードのビット長の増加分と等しい量、関連付けられた符号化ブロック内の第２の可変長コードのビット長を減少させる第２の改変とを含み、

前記可能な代替ブロックのそれぞれは、前記関連づけられた一つの符号化ブロックのビット長と等しいビット長であることを特徴とする、フィンガープリントされたデジタルコンテンツを生成する方法。

【請求項２】

データストリーム内において、前記符号化ブロックを含むオリジナルブロックを、前記

代替ブロックを含む代替パケットによって置換するステップ、をさらに含む、請求項１に記載の方法。
【請求項３】
前記決定ステップでは、パケット化されたデータストリーム内のパケットの境界にまたがるブロックを排除する、請求項１に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、デジタルコンテンツの配布に関する。
【背景技術】
【０００２】
例えば、映画などのメディアストリームのためのデジタルコンテンツの配布は、いくつかの問題を受ける。１つの問題は、簡単にデジタルコンテンツの正確なコピーを作成できるため、それをする権限を有しているかいないかにかかわらず、いかなる受取人もそのコンテンツを再配付可能となることである。権限なく配布される惧れがなく、デジタルコンテンツ、特にメディアストリームのためのデジタルコンテンツを配布可能となることは有利であろう。これは、デジタルコンテンツを、例えば、コンピュータネットワーク、あるいは、（例えば、要求に応じて、あるいは今後の要求を予測して、あるいは他の何かに応じて）エンドビューアへ配布するための他の技術など、通信リンクを用いて配布することが所望されるとき、特に有利であろう。
【０００３】
１つの既知の解決策は、デジタルコンテンツに、コンテンツの権限のない配布者を識別可能となる「フィンガープリント」を付けることで、結果として、できるならば潜在的な権限のない配布者を思いとどまらせようとするものである。しかしながら、デジタルコンテンツのフィンガープリンティングは、以下を含むいくつかの既知の問題を受ける。（１）　そのメディアストリームの提示は、オリジナルのコンテンツを改変することにより、劣化する場合があること。（２）その受取人が、フィンガープリントを改変あるいは消去することにより、改ざんしてしまうこともあること。もしくは、（３）　特に、複数の権限のない再配布者が、これらの複数の受取人が利用可能な情報を用いて、フィンガープリントが改変あるいは消去されたコピーを製造するために結託している場合は、権限がないという十分な確証のある再配布者の決定は困難となること。
【０００４】
他の問題は、フィンガープリントが、オリジナルのメディアストリームの配布、デコーディング、あるいは提示を妨げるかもしれないことである。特に、オリジナルのメディアストリームが、例えば、ＭＰＥＧ‐２フォーマットなどのように、映画用の既知のフォーマットを用いて符号化されているときは、一本の映画でさえ、含まれているデータ量はかなり大きくなる場合がある。
【発明の開示】
【発明が解決しようとする課題】
【０００５】
特定のフィンガープリントされたデジタルコンテンツが配布目的のためにフィンガープリントを変えられないよう、オリジナルのＭＰＥＧ符号化（オリジナルのメディアストリームのパケット化を含む）ストラクチャーを保持することは、どのようなフィンガープリンティング方法にも有利であろう。特に、以下を保証することは有利となろう。（１）フィンガープリントされたデジタルコンテンツの長さが、オリジナルのデジタルコンテンツの長さと同じであること、および、（２）フィンガープリントされたデジタルコンテンツを再計算する必要もなく、さらに、フィンガープリントされたデジタルコンテンツについての多量の中間状態の情報を維持する必要もなく、ネットワークコミュニケーションの技術を使用する時などのように、デジタルコンテンツの送付を中断および再開することができること。

【課題を解決するための手段】
【０００６】
本発明の１つの態様は、メディアストリーム内に情報を埋め込む方法である。この方法は以下を含んでいる。（１）　情報を埋め込むために、そのメディアストリーム内部の１組の位置を選択すること、（２）それらの位置を作成するために、１組の可能な改変を選択すること、および、（３）　可能な改変のサブセットを作成すること。位置および可能な改変の組は、本明細書では「透かし」と呼ばれる場合もある。実際の改変のサブセットは、本明細書では「フィンガープリント」と呼ばれる場合もある。
【０００７】
本方法は、１つは、同一メディアストリームのオリジナルバージョンであり、また１つは、同一メディアストリームの代替バージョンであるといった、同一のメディアストリームの代替バージョンが存在する１組の位置を決定する。本明細書では「オリジナルの映画」および「代替映画」（「代替映画」）と呼ぶことがあり、あるいは、メディアストリーム内の特定のブロックを「オリジナルのブロック」および「代替ブロック」（「代替ブロック」）と呼ぶこともある。１つより多い代替映画あるいは代替ブロックが、１ビットより多い情報が各位置で埋め込可能となるよう、各位置を決定することができる。したがって、こうした各位置は、１ビット以上の情報を埋め込むことができ、この埋め込まれたビットは、その位置にオリジナルの映画あるいは代替映画が選択されているか否かに対応している。
【０００８】
方法の態様は、メディアストリームの配布における変化が全くないよう、改変を選択することを含んでいる。例えば、（１）そのメディアストリームを表わすデジタルコンテンツのパケット化、あるいは、（２）メディアストリームの音声部分のビデオ部分との同期化。好適な実施例では、変更のない配布は、例えば、ＭＰＥＧで符号化された映画の個々のブロックなどのような、そのメディアストリームを表わすデジタルコンテンツの部分の長さに全く変更を加えることなく実行可能である。
【０００９】
好適な実施例では、この方法は、そのメディアストリーム用デジタルコンテンツのＭＰＥＧ‐２符号化内の、１組のイントラ符号化されたブロックを決定することを含んでいる。イントラ符号化された各ブロックは、そのブロックに対するＤＣＴ係数のための１組のランレベルの符号化された値を有している。本方法は、オリジナルの組の値と少しでも違っている代替組の値があるか否か、さらに、符号化されたブロックのビット長が変わっていないかを決定する。したがって、こうした各ブロックは、埋め込まれた情報に対する位置、およびその位置に対する改変の双方を提供して、結果的に、埋め込み可能な情報値を少なくとも１ビット提供する。代替的実施例では、ブロックの代わりにマクロブロックを使用してもよい。
【００１０】
この好適な実施例は、以下の選択を有することができよう、（１）２以下の値などの、任意の個々のブロック内で変更されるランレベルの符号化された値の数；（２）＋／－１レベルなどの、変更される任意のランレベルの符号化された値に対する改変の量；および（３）２４以下の量子化スケールなどの、変更される任意のランレベルの符号化された値に対しても、許容される量子化量。
【００１１】
好適な実施例では、本方法は、代替ブロックを選択可能なそれらのブロックを認識すること、ランダムあるいは擬似ランダム効果に対応して、各ブロックで特定の代替ブロックを選択することを含んでいる。このタイプの効果により、フィンガープリントを「取り消す」ためにランレベルを研究しようと試みるアタックに対し、フィンガープリントが抵抗することを補助可能となる。また、それは、透かしをコンテンツの空間周波数の比較的大きな範囲にわたって広げるのを補助してもよく、アタックへの抵抗を補助する一方で、視覚効果をさらに減少させる。したがって、透かしを入れられる各映画に対して、それに透

かしを入れた特定の代替映画は、代替ブロッをオリジナルのブロックに再符号化することにより、または、ブロックを代替ブロックに再符号化することにより、情報の埋め込みをリバースするようなアタックに対しても抵抗力を有している。なぜなら、アタッカーは、これらの代替ブロック、あるいはこれらのオリジナルブロックを容易には知り得ないからである。

【００１２】

好適な実施例の方法は、また、メディアストリームを表わすデジタルコンテンツに対するパケット化されたデータストリーム内部のパケットの境界にまたがる位置にあるブロックを除外する。代替ブロックは、こうしたまたがるブロックを選択しないことが好ましい。なぜならこれらのブロックにアクセスすると、パケット化されたデジタルコンテンツの解析にかかわることになり、自明でない予見、およびメディアストリームを表わすデジタルコンテンツの分析をしなければならなくなるからである。したがって、この最適化により、本発明の好適な実施例の実現が単純化される。

【００１３】

本発明は映画に限定されるものではなく、例えば、アニメーションあるいは音声などの、他のデジタルコンテンツおよびメディアストリームに対しても適用可能であるのみならず、例えば、写真あるいはイラストなどの静止メディアに対しても、さらにデータベースあるいは情報の他のコレクションに対しても適用可能である。

【発明を実施するための最良の形態】

【００１４】

以下の説明では、本発明の好適な実施例は、好適な処理ステップおよびデータストラクチャーに関して説明されている。本技術分野の技術者ならば、この出願の熟読の後に、本発明の実施例は、１つ以上の汎用プロセッサ、あるいは専用プロセッサ、あるいは、特定の処理ステップならびに本明細書で説明されるデータストラクチャーに適当な他の回路を用いて実行可能であり、さらに、特定の処理ステップの実行およびデータストラクチャーは、過度の実験あるいはさらなる発明を必要としないことを認めるであろう。

【００１５】

語彙

次の用語は、以下で説明するように、本発明の態様に関連し、あるいは関係している。これらの用語の一般的な意味の記述は、制限を意図するものではなく、説明を意図しているに過ぎない。

【００１６】

「デジタルコンテンツ」というフレーズは、エンドビューアへの提示のために、メディアストリームあるいは他の情報を表示することを意図した、デジタルフォーマットのデータを説明する。「デジタルコンテンツ」は、例えば、メッセージヘッダー情報などのパッケージング情報とは区別される。

【００１７】

「メディアストリーム」というフレーズは、一連のフレームもしくはフィールドを含む映画、あるいは一連の音声を含むオーディオなど、連続した提示を意図する情報を説明する。本明細書に使用されているように、「メディアストリーム」というフレーズは、パケットを用いて連続的に送信し、コンテンツ全体が到着する前に再生を始める、音声と画像の「ストリーミングメディア」の標準的な意味より広い意味を有している。むしろ、本明細書で用いられているように、「メディアストリーム」は、連続して届けらなければならないといういかなる特定の要件も存在しない。また、本明細書で説明するように、メディアストリームは、写真あるいはイラストなどのような静止したメディアと同様に、例えば、アニメーションあるいは音声などのような、提示のための他の情報を指す場合もあるし、情報のデータベースおよび他のコレクションを指す場合もある。

【００１８】

「情報をメディアストリームに埋め込む」というフレーズは、そのメディアストリームを表示し、さらに、後に検出可能な形式で埋め込まれた情報を含む、そのメディアストリ

ームのための１組のデジタルコンテンツを生成することを説明する。

【００１９】

「透かし」という用語は、情報をそのデジタルコンテンツに埋め込むことができる、デジタルコンテンツのためのスキーマを説明する。本明細書で説明するように、アタッカーは、本発明により提供される透かしを容易には取り外すことができない。しかしながら、本明細書で説明するような透かしの概念は、十分に一般的であるため、アタックに対して抵抗力を持たない透かしも含み得る。本明細書で説明するように、本発明により提供される透かしは、そのメディアストリーム内部に、情報が埋め込まれる１組の位置、および情報を埋め込むことで、これらの各位置にほどこされる可能な改変の双方を含んでいる。しかしながら、本明細書で説明するような透かしの概念は、十分に一般的であるため、情報を埋め込む他の技術を用いた透かしも含み得る。

【００２０】

「フィンガープリント」という用語は、少なくとも１人の指定されたデジタルコンテンツの受取人を識別し得る程度の、情報の特定の組を説明する。本明細書で説明するように、共謀した複数のアタッカーは、本発明により提供されるフィンガープリントを容易には取り除くことができず、あるいは、彼らのうちの少なくとも１人がデジタルコンテンツの権限のない配布者として検出されるのを防ぎ得ない。しかしながら、本明細書で説明するようなフィンガープリントの概念は、十分に一般的であるため、取り除きに対してそれほど抵抗力を持たず、もしくは、デジタルコンテンツの権限のない配布者を検出するような能力を提供しないフィンガープリントも含み得る。本明細書で説明するように、本発明により、提供されるフィンガープリントはメディアストリーム内部に、透かしにより識別される各位置にほどこされる特定の組の改変を含んでいる。しかしながら、本明細書で説明するようなフィンガープリントの概念は、十分に一般的であるため、情報を埋め込み、その埋め込まれた情報を検出し、さらにデジタルコンテンツの権限のない配布者を検出する、他の技術を用いるフィンガープリントを含み得る。

【００２１】

「適応」という用語は、送り主がデジタルコンテンツを受取人へ届ける処理を説明する。本明細書で説明するように、送り主は、そのデジタルコンテンツのコピーを解読し、さらにそのデジタルコンテンツにより表されるメディアストリームに情報を埋め込み（したがって、そのデジタルコンテンツを部分的にフィンガープリントする）、そして、その部分的にフィンガープリントされたデジタルコンテンツを再暗号化する。送り主は、この適応されたデジタルコンテンツを受取人に送る。

【００２２】

「エンドビューア」というフレーズは、メディアストリーム用のデジタルコンテンツのデコードを受け、さらにメディアストリームの提示を受けると考えられる、メディアストリームの受取人を説明する。

【００２３】

「デコード」という用語は、符号化されたフォーマットのメディアストリームのデジタルコンテンツに応答して、メディアストリームの提示の形式でのデータを生成することを説明する。本明細書で説明するように、符号化されたフォーマットは、ＭＰＥＧ‐２などの業界基準の符号化されたフォーマットを含んでいてもよい。しかしながら、本明細書で説明するようなデコードの概念は、十分に一般的であるため、メディアストリームのための他の符号化フォーマットも含み得る。

【００２４】

「提示」という用語は、例えば、映画を見る（あるいは、他の感覚）ためのオーディオおよびビジュアル情報などのような、メディアストリームを見るための形式で情報を生成することを説明する。本明細書で説明するように、映画の提示は、映画のフレームあるいはフィールドのビジュアルディスプレイのみならず、その映画に関連付けられたサウンドトラックのオーディオ提示も含み得る。しかしながら、本明細書で説明するような提示の概念は、十分に一般的であるため、オーディオ、ビジュアル、あるいはその他を含む、エ

ンドビューアが受け取る情報の生成のための、他の様々な形式を含み得る。

【００２５】

「オリジナルの映画」および「代替映画」というフレーズは、１つは、本発明の態様を用いるシステムへ導入されるそのメディアストリームのオリジナルバージョンであり、そして、他の１つは、オリジナルの映画に応じて生成された、同一メディアストリームの代替バージョンであるといった、同一メディアストリームの代替バージョンを説明する。同様に、「オリジナルブロック」および「代替ブロック」というフレーズは、オリジナルの映画あるいは代替映画内の、同一の個々のブロックあるいはマクロブロックの各代替バージョンを説明する。本明細書で説明するように、オリジナルの映画と代替映画との間の違いは、代替映画が、あらゆる点において、オリジナルの映画の代わりとなり得るので、履歴的である。同様に、任意の１つのオリジナルブロックと、その関連する代替ブロックとの間の違いも、代替ブロックが、あらゆる点においてオリジナルブロックの代わりとなり得るので、履歴的である。

【００２６】

「ＭＰＥＧ」というフレーズは、ＩＳＯ／ＩＥＣ（国際標準化機構／国際電気標準会議）のワーキンググループである、「動画専門家グループ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）」の頭文字語である。「ＭＰＥＧ‐１」、「ＭＰＥＧ‐２」、および「ＭＰＥＧ‐４」というフレーズは、それぞれ、ＩＳＯ／ＩＥＣ　１１１７２、ＩＳＯ／ＩＥＣ　１３８１８、およびＩＳＯ／ＩＥＣ　１４４９６ドキュメント内に詳しく説明されている、メディアコンテンツを符号化する技術を指している。本発明は、ＭＰＥＧでの使用に限定されるものではなく、さらに、これらの用語は、同様の性質であるか、あるいはそうでないかにかかわらず、他の符号化技術を含むように広く解釈されるべきである。

【００２７】

「イントラ符号化されたブロック」という用語は、イントラ符号化されたマクロブロックの一部であるブロックを指している。イントラ符号化されたブロックおよびマクロブロックは、ＭＰＥＧ技術の技術分野ではよく知られた用語である。

【００２８】

これらの用語および概念の拡張を含む本発明の他の、およびさらなるアプリケーションは、この出願を熟読した後には、当業者にとれば明白であろう。これらの他の、およびさらなるアプリケーションは本発明の範囲および趣旨の一部であり、またこれらは、当業者にとれば、さらなる発明あるいは過度な実験を伴うことなく、明白であろう。

【００２９】

システムの要素

図１は、デジタルコンテンツに透かしを入れ、フィンガープリントをほどこすシステムのブロック図を示している。

【００３０】

システム１００は、ビデオ配布ネットワーク１１０を含んでいる。ビデオ配布ネットワーク１１０は、少なくとも１つの注入オリジン１２０、および多くのエンドビューア施設１３０を含んでいる。

【００３１】

１．注入オリジンからエンドビューア施設への配布

注入オリジン１２０は、ビデオ配布ネットワーク１１０外部のソースから、メディアストリーム用のデジタルコンテンツ１２１を受けとる。好適な実施例では、これらのソースは、例えば、映画プロダクションスタジオ、テレビスタジオ、ラジオまたはテレビのネットワークシンジケータなどのような、コンテンツプロデューサーあるいはコンテンツアグリゲータを含んでいてもよい。必要であれば、注入オリジン１２０は、デジタルコンテンツ１２１をフォーマットし、それに透かしを入れ、さらに、注入オリジン１２０での記憶のためにそれを暗号化する。好適な実施例では、注入オリジン１２０は、本明細書で説明されるように、透かしを入れ、フィンガープリントをほどこす方法を使用する。

【００３２】
好適な実施例では、注入オリジン１２０は、少なくともインストラクションを実行することができるプロセッサ、デジタルコンテンツおよびインストラクションを格納するためのメモリ、およびネットワークインタフェースを含んでいる。
【００３３】
ビデオ配布ネットワーク１１０は、各々が、個々に、あるいは連携して、注入オリジン１２０からエンドビューア施設１３０への、デジタルコンテンツ１２１を受け取り、格納し、および配布するために作用可能な、キャッシュ装置１１１のネットワークを含んでいる。好適な実施例では、エンドビューアからの要求は、ビデオ配布ネットワーク１１０に、エンドビューア施設１３０へデジタルコンテンツ１２１を配布するように促し、したがって、配布用の「プル」モデルが使用される。しかしながら、代替的実施例では、注入オリジン１２０あるいは他の装置は、ビデオ配布ネットワーク１１０に、デジタルコンテンツ１２１をエンドビューア施設１３０へ配布するよう促すことも可能であり、したがって、代替的に、「プッシュ」モデルあるいは配布用の他のモデルを用いることも可能である。
【００３４】
好適な実施例では、キャッシュ装置１１１は、１次キャッシュ１１２、中間キャッシュ１１３、およびリーフキャッシュ１１４を含む、層状配布システム内に配列される。１次キャッシュ１１２は、デジタルコンテンツ１２１を注入オリジン１２０から直接受け取る。中間キャッシュ１１３は、デジタルコンテンツ１２１を、１次キャッシュ１１２、あるいは、ネットワークトポロジー的に注入オリジン１２０により近い、他の中間キャッシュ１１３から受け取る。リーフキャッシュ１１４は、デジタルコンテンツ１２１を、中間キャッシュ１１３から、あるいは、可能であれば１次キャッシュ１１２から受け取り、デジタルコンテンツ１２１をエンドビューア施設１３０へ直接配布する。
【００３５】
好ましくは（すなわち、好適な実施例では）、各キャッシュ装置およびエンドビューア施設は、少なくともインストラクションを実行可能なプロセッサ、デジタルコンテンツおよびインストラクションを格納するメモリ、およびネットワークインタフェースを含んでいる。
【００３６】
好適な実施例では、ビデオ配布ネットワーク１１０は、インターネット、あるいは、その機密保護サブセットのような冗長通信ネットワークを含んでいる。しかしながら、本発明のコンテキストでは、任意の特定の通信技術を使用するビデオ配布ネットワーク１１０のための、いかなる特定の要件も存在していない。代替的実施例では、デジタルコンテンツ１２１のコピーを、注入オリジン１２０から、ビデオ配布ネットワーク１１０を通して最終的にエンドビューア施設１３０へ配送可能ないかなる通信技術も適当であろう。
【００３７】
好適な実施例では、ビデオ配布ネットワーク１１０を用いるデジタルコンテンツ１２１の配布は、デジタルコンテンツ１２１のコピーが、複数のキャッシュ装置１１１に記録され、および維持され、さらに、注入オリジン１２０からエンドビューア施設１３０への１つより多い経路を用いて配送し得ることを提供する。
【００３８】
第１例については、デジタルコンテンツ１２１のコピーは、注入オリジン１２０から２つの異なる中間キャッシュ１１３（ＡおよびＢ）へ、さらに、これらの中間キャッシュ１１３（ＡおよびＢ）から複数のエンドビューア施設１３０へ配送可能である。これらの中間キャッシュ１１３（Ａ）のうちの１つが、後にそのデジタルコンテンツ１２１のコピーを破棄する場合には、さらにエンドビューア施設１３０へ配送するために、他の中間キャッシュ１１３（Ｂ）から他のコピーを受け取ることができる。
【００３９】
第２例については、デジタルコンテンツ１２１の異なる部分が、注入オリジン１２０か

ら異なる中間キャッシュ１１３（ＡおよびＢ）へ配送され、次いで、これらの中間キャッシュ１１３（ＡおよびＢ）から同一エンドビューア施設１３０へ配送されることができる。これは、例えば、ビデオ配布ネットワーク１１０内部の通信リンクエラー、あるいは代替的にユーザの動作などにより、デジタルコンテンツ１２１を注入オリジン１２０からエンドビューア施設１３０へ送る作業が中断された場合に発生し、後に再開され、完了される。

【００４０】

２．　各受取人へのビデオ配布ネットワークを用いた配布

ビデオ配布ネットワーク１１０内の任意の送り主が、任意の受取人に対して、いつデジタルコンテンツ１２１を配送しても、送り主は、その受取人に対してデジタルコンテンツ１２１の適応を実行する。適応では、送り主は、そのデジタルコンテンツのコピーを復号化し、そのデジタルコンテンツを部分的にフィンガープリントし、さらにその部分的にフィンガープリントされたデジタルコンテンツを再暗号化することにより、情報を、そのデジタルコンテンツにより表示されるメディアストリーム内に埋め込む。

【００４１】

好適な実施例では、適応は、キャッシュ装置１１１とエンドビューア施設１３０の双方を含む、あらゆる受取人に対して実行される。これは、たとえ、それらの注入オリジン１２０からの距離が、同一あるいは同様であっても、キャッシュ装置１１１間の転送も含むことになろう。しかしながら、本発明の文脈では、代替的実施例において、ビデオ配布ネットワーク１１０の何らかの部分が、デジタルコンテンツ１２１を復号化し、あるいは再暗号化することなく、伝送することができるよう、適応が全ての可能な受取人に対して実行されるための、いかなる特定の要件も存在していない。

【００４２】

復号化と再暗号化には、異なるキーが使用されるのが好ましい。さらに、復号化と再暗号化には、異なる暗号スキームを使用することも可能である。代替的に、同一のキー、スキーム、あるいはその双方も使用可能である。

【００４３】

したがって、上述したように、結果として、個々のエンドビューア施設１３０が、複数の受取人に対して部分的にフィンガープリントされたデジタルコンテンツ１２１を受け取ることは可能である。しかしながら、いずれにせよ、好適な実施例では、個々のビューアを検出するためにフィンガープリンティング方法（例えば、フィンガープリントされたデジタルコンテンツの複数の受取人の間の共謀を検出する技術を用いるなど）が提供されている。

【００４４】

個々のエンドビューア施設１３０が、暗号化され、およびフィンガープリントされたデジタルコンテンツ１２１を受け取ると、その施設は、そのデジタルコンテンツ１２１をローカルビデオライブラリ１３１内へ記録する。ローカルビデオライブラリ１３１は、デジタルコンテンツ１２１を、後に１つ以上の再生要素１３２へ配布するために、暗号化され、およびフィンガープリントされた形式で保存する。エンドビューアによる要求に応答して、ローカルビデオライブラリ１３１は、デジタルコンテンツ１２１を、デジタルコンテンツ１２１が、実質的に同時に復号化され、さらに、視聴のためにエンドビューアへ提示される、１つ以上の再生要素１３２へ配布する。

【００４５】

システム１００の１つの可能な実現についてのさらなる詳細は、２００３年1月３１日に出願された、関連出願である米国特許出願第１０／３５６，６９２号「デジタルコンテンツの並行配布およびフィンガープリンティング（Ｐａｒａｌｌｅｌ　Ｄｉｓｔｒｉｂｕｔｉｏｎ　ａｎｄ　Ｆｉｎｇｅｒｐｒｉｎｔｉｎｇ　ｏｆ　Ｄｉｇｉｔａｌ　Ｃｏｎｔｅｎｔ）」（コレンズ（Ｃｏｌｌｅｎｓ）他）で議論されている。

【００４６】

動作方法

図２は、本発明に従う、ＭＰＥＧ符号化と、代替ブロック（すなわち、代替ブロック）の生成を示す。本発明は、ＭＰＥＧ符号化デジタルコンテンツでの使用に限定されない。ＭＰＥＧの文脈での本発明の以下の議論を読んだ後は、デジタル符号化の当業者であるなら、過度の実験あるいはさらなる発明を要することなく、本発明を異なる符号化スキームおよびデータタイプに適用することができるだろう。

【００４７】

図２では、デジタルコンテンツのフレーム２００が、ＭＰＥＧ規格に従って処理される。説明の目的のために、このフレームはＲＧＢ、ＣＭＹＫ、あるいは何らかの他のフォーマットでのイメージフレームとして示されている。本発明はまた、他のタイプのデジタルコンテンツに適用可能である。

【００４８】

フレーム自体の中のデータを処理可能である。フレーム自体の中のデータが処理される場合、そのフレームは「イントラ符号化されている」と呼ばれる。

【００４９】

代替的に、そのフレームに対して予測されるデータとそのデータの相違を処理可能である。フレームデータの予測は、前のフレーム内のデータ、あるいは、前のフレームと後に続くフレームの双方のデータに基づくことが可能である。前者の場合は、このフレームは「予測」フレームと呼ばれている；後者の場合は、このフレームは「双方向」フレームと呼ばれている。

【００５０】

本発明の好適な実施例は、イントラ符号化フレームのみに適用される；しかしながら、この場合にはこうした必要はない。

【００５１】

フレーム２００は、１６×１６画素マクロブロック２１０に分割される。そして、各マクロブロックは、輝度マクロブロック２２０およびクロミナンスマクロブロック２２５に分解される。図２は、４：２：０クロミナンスフォーマットを示している。このフォーマットでは、輝度マクロブロックは４つの８×８ブロックを含み、クロミナンスマクロブロックは２つの８×８ブロックを含んでいる。肉眼は、輝度変化ほどクロミナンス変化に敏感ではないので、クロミナンスデータには低解像度を用いることができる。様々なダウンサンプリング技術のいずれであれクロミナンスブロックを決定可能である。

【００５２】

他のクロミナンスフォーマットでは、異なるサイズの各クロミナンスマクロブロックが使用可能である。例えば、４：２：２フォーマットでは、各クロミナンスマクロブロックは４つの８×８ブロック含み、さらに４：４：４フォーマットでは、各クロミナンスマクロブロックは８つの８×８ブロックを含んでいる。

【００５３】

次に、各ブロックの輝度およびクロミナンスデータが処理される。ブロックを処理するために、離散コサイン変換（ＤＣＴ）がそのブロックに適用され、１組の８×８ＤＣＴ係数２３０をもたらす。

【００５４】

その後、ＤＣＴ係数が量子化される。量子化は、全てのＤＣＴ係数を整数によりブロックに対して分割し、いかなる残余も破棄することを伴っている。この処理により、ゼロの係数の間に点在する、いくつかの非ゼロ係数がもたされる。係数が分割されるこの整数は、ブロックに対する量子化レベルである。量子化により、精度は若干の損失をもたらす；しかしながら、可能な量子化の程度に応じて、精度の損失は、エンドビューアにとり容認可能であろう（少しでも気付かれるなら）。量子化の便益は、高度なデータ圧縮が可能となることである。

【００５５】

そして、ブロックに対して量子化されたデータは、パターン２４０などのジグザグパターンでブロックをラン（ｒｕｎ）することにより順序付けられる。この順序付けは、ゼロ

の連続で分離されるレベルと呼ばれる、非ゼロ係数の系列をもたらす。図２では、こうした系列は、参照数字２５０で表現的に示されている。

【００５６】

レベルおよびゼロの系列は、ランレベル符号化と呼ばれる処理を通して数の対のリストに変換される。このリスト内の数の対は、参照番号２６０で表される、ランレベルコードと呼ばれている。各対の第１数はランにおいてレベルに先行するゼロの数を表し、さらに、各対の第２数はレベルを表す。このようにして、例えば、ＡおよびＢが各レベルに対する値として、レベルとゼロの系列（Ａ　０　０　０　０　０　Ｂ　０　０）は、対（０，Ａ）および（５，Ｂ）などに変換可能である。

【００５７】

圧縮を改良するために、ランレベルコードは、ハフマンコードなどの何らかの適応型符号化スキームを通して符号化される。このタイプの符号化スキームは、結果的に、各ランレベルコードに対して長さの異なる２進コードとなる。この理由で、結果として生じるコードは、可変長コード（ＶＬＣ）と呼ばれる。図２では、長さの異なるＶＬＣ２７０は、長さの異なるダッシュにより表されている。

【００５８】

ＶＬＣ２７０は、４つの可変長コードを表す４本のダッシュを含んでおり、これは順番に、輝度あるいはクロミナンスデータの単一の８×８画素ブロックに対する、量子化されたＤＣＴ係数のための４つのランレベルコードを表している。ブロックは、より短い、あるいはより長い長さの、より少ない、あるいはより多くのこうしたＶＬＣにより表されることができよう。

【００５９】

上で議論したように、フレームのＶＬＣへの変換は、ダウンサンプリングおよび量子化にかかわる；その結果、ＶＬＣは正確なフレームデータを表さない。本発明は、ほとんど同一の、しかし完全には同一でない方法でフレームを表す、フレームに対するＶＬＣの１つ以上の交互の組を決定することにより、この事実を利用する。これらのＶＬＣの交互の組は、本発明に従う代替ブロックを形成する。ＶＬＣのオリジナルの組は、オリジナルブロックと呼ばれている。

【００６０】

代替ブロックのための、若干のあるいは全てのＶＬＣは、オリジナルブロック内のＶＬＣとは異なる長さを有している場合もあろう。しかしながら、本発明に従えば、代替ブロックに対するＶＬＣの全長は、オリジナルブロックに対するＶＬＣの全長と等しくなるべきである。これは、図２において表示的に示されており、そこでは、代替ブロック２８０に対するＶＬＣの全長は、オリジナルブロック２９０に対するＶＬＣ２７０の全長と等しい。

【００６１】

図３は、本発明に従うパケット化の保存を示している。

【００６２】

図３では、データストリーム３００は、ヘッダー３２０内の制御データなどに加えてＶＬＣのオリジナルブロック３１０を含んでいる。各ブロック内のＶＬＣの可変数および長さは、ブロック３１０内の破線で表されている。

【００６３】

データストリーム３００は、パケット化されたデータストリーム３３０と同様のメディアストリームとしての提示のためにパケット化される。このパケット化されたデータストリームは、それ自身のパケットヘッダー３４０と、データストリーム３００からの全てのデータを含むパケット３５０を含んでいる。パケットの境界は、図３においてパケット化されたデータストリーム３３０とデータストリーム３００との間の縦線により示したように、データストリーム３００内のいかなる場所にも発生させることが可能である。したがって、パケット境界は、ブロック３１０およびヘッダー３２０で発生可能である。

【００６４】

データストリーム３６０は、データストリーム３００内の若干のブロックの代替ブロック３７０を含んでいる。これらの代替ブロックは、データをデータストリーム内に埋め込むために、対応するオリジナルブロックの代わりに、データストリーム内へ挿入することができる。

【００６５】

図２について議論したように、代替ブロックに対するＶＬＣの全長は、対応するオリジナルブロックに対するＶＬＣの全長と等しい。しかしながら、個々のＶＬＣの数、サイズ、あるいはその両方は、総合的ブロック長が変化しない限り、オリジナルブロックのものと異なることができる。これらの変化は、ブロック３７０の破線により表されている。

【００６６】

代替ブロックの長さが、それに対応するオリジナルブロックの長さに適合しているので、代替ブロックを伴うパケットを、オリジナルブロックを伴うパケットと置換することにより、代替ブロックを、パケット化されたデータストリーム３３０内へ代入可能である。

【００６７】

しかしながら、代替ブロックが２つのパケットにまたがっている場合は、代替ブロックによる置換は、パケット化されたデータストリームの重要な予見および分析を必要とすることになろう。したがって、本発明の好適な実施例は、データの埋め込み可能な位置から、パケットの境界にまたがるブロックを排除している。言い換えれば、代替ブロックは、パケット化されたデータストリーム内のパケットの境界にまたがるブロックを許可しないことが好ましい。

【００６８】

次に、位置選択のための、およびこれらの位置に対する代替ブロックのための、好適な技術の特定の細部について議論する。デジタルコンテンツの特定のアイテムに対する可能な位置および代替ブロックの組は、そのデジタルコンテンツに対して透かしを形成する。これらの可能な代替ブロックのいくつか、あるいは全てが挿入されているコンテンツのコピーは、完全に、あるいは部分的にフィンガープリントされていると言われる。

【００６９】

図４は、情報が埋め込まれるであろう１組の位置でデジタルコンテンツに透かしを入れ、フィンガープリントをほどこす方法のフロー図を示している。

【００７０】

１．透かし入れ

これらの位置でのブロック位置および代替ブロックの組は、ＭＰＥＧの文脈での位置および可能な改変の組の特定の例である。概して、これらの位置でのこうした位置および可能な改変の組は、本発明に従う透かしを形成する。ステップ４０１およびステップ４０２は、この透かしの作成ステップである。これらのステップは、注入オリジン１２０で実行されるのが好ましい。

【００７１】

ステップ４０１では、情報を埋め込む位置がデジタルコンテンツ内で選択される。好適な実施例では、このデジタルコンテンツは、ＭＰＥＧ‐１、ＭＰＥＧ‐２、あるいはＭＰＥＧ‐４（以下では、まとめて単にＭＰＥＧと言及する）に符号化されたデジタル映画であってもよい。以下のステップは、符号化されたデジタル映画の文脈で説明されている。しかしながら、本発明は、他のデジタルコンテンツにも等しく適用可能であり、さらに、これらのステップのアプリケーションは、さらなる発明、あるいは過度の実験を必要とはしないだろう。

【００７２】

位置は、輝度あるいはクロミナンスＤＣＴ係数のいずれかの８×８ブロックであるのが好ましいが、こうした係数の１６×１６マクロブロックであってもよい。本発明は、完全にイントラ符号化されたマクロブロックである位置で使用可能であるが、位置は、イントラ符号化されたマクロブロックのブロックであるのが好ましい。ブロックとイントラ符号化されたマクロブロックは、ＭＰＥＧ符号化技術ではよく知られている。

【００７３】
本発明は、例えば、ウェーブレットあるいは、輝度もしくはクロミナンス情報が、なんらかの変換されたドメイン（例えば、非ＭＰＥＧ符号化スキームにおける）に提示されるいかなる他の変換など、ＤＣＴ以外の変換からの係数を含む他のブロックに適用可能であり、あるいは、ＲＧＢデータ、ＣＭＹＫデータ、ＹＵＶデータに変換、および、より一般的に、メディアストリームの提示に役立つ情報がデジタルコンテンツで表示される、いかなる変換にも適用可能である。本技術分野の技術者ならば、この出願の熟読の後に、本発明の範囲および趣旨の中で、本質的に色空間および基礎機能のいかなる組合せも実行可能となり得て、さらに、過度の実験あるいはさらなる発明を必要としないことを認めるであろう。

【００７４】
パケット化されたデジタルコンテンツの場合は、パケットの境界にまたがるブロックは、情報を埋め込むために可能な位置から排除されるのが好ましい。

【００７５】
位置はまた、ブロックの代替バージョンがあり、位置に対して可能な改変を選択するよう、ステップ４０２で議論した評価基準を満たしているような形で選択される。したがって、ステップ４０１は、ステップ４０２に関連して起こるのが好ましい。

【００７６】
ステップ４０２では、ブロックに対する可能な改変が選択される。デジタルコンテンツのパケット化および同期を維持するために、これらの改変は、情報が埋め込まれる位置（すなわち、ブロック）でのデジタルコンテンツの長さへ、いかなる変化も伴わないことが好ましい。

【００７７】
ＭＰＥＧのコンテキストでは、各ブロックは、そのブロックに対する離散コサイン変換（ＤＣＴ）係数のためのランレベル符号化値の組を有している。本発明は、オリジナルの値の組と少しだけ異なっている代替の値の組があるか否か、さらにそれが符号化されたブロックのビット長を変えないかどうかを決定する。したがって、こうした各ブロックは、情報を埋め込む位置とその位置に対する改変の双方を提供し、その結果、埋め込み可能な情報の少なくとも１ビットを提供する。代替的実施例では、各マクロブロックがブロックの代わりに使用されている。

【００７８】
より詳細には、ＭＰＥＧでは、クロミナンスおよび輝度ブロックは、ピクセルデータ値の離散コサイン変換を表すランレベルコードに対応する可変長コード（ＶＬＣ）を用いて符号化される。これらのＶＬＣはハフマンコードであり、それはデータ圧縮の非常に効率的な方法を提供する。しかしながら、異なる各ブロックに対する結果としてのデータは、異なる長さを有している場合もある。

【００７９】
したがって、情報を埋め込む位置で一定のブロック長を維持するためには、ブロックに対するＶＬＣのいかなる変化も、正味の長さとゼロの差にならなければならない。これは、いくつかの方法で達成可能である。

【００８０】
第１に、１つのＶＬＣは、同一長を有する他のＶＬＣの代わりをすることができよう。第２に、オリジナル、および、代用されたＶＬＣの合計の長さが等しい状態で、１つより多いＶＬＣが、等しい数のＶＬＣの代わりをすることもできよう。例えば、５と６の長さを有する２つのＶＬＣは、４と７の長さを有するＶＬＣの代わりに用いることができよう。第３に、１つ以上のＶＬＣを追加し、あるいは削除することができよう。視覚インパクトを減少するためには、追加および削除は、１のレベルでＶＬＣに限定されるのが好ましい。他の技術と同様、これらの３つの技術の組合せが利用可能である。

【００８１】
ブロックに対する２つより多いＶＬＣが変化する場合は、人為ストラクチャーは、たと

え非常に低いレベルの認知であれ、ビューアにより目視されるものとなろう。したがって、代替ブロックは、ＶＬＣに対する２つの変化からもたらされるブロックに限定されるのが好ましい。

【００８２】

デジタルコンテンツの提示への視覚インパクトを制限するために、識別された位置のデータへの変化は、ランレベルコード内の１つのレベル値により増加し、あるいは減少するのが好ましい。加えて、ＭＰＥＧは、ランレベルコードにより表されるデータの量子化に関係している。量子化スケール（ＱＳ）が２４より高いなら、１のレベル変化でさえ、提示において容認できない歪みをもたらすことになる。したがって、２４以下の量子化スケールを有するブロックのみが、代替ブロックの形成に使用されるのが好ましい。

【００８３】

要するに、好適な実施例では、以下の評価基準は、オリジナルブロックに対する可能な改変（すなわち、代替ブロック）を識別するために使用される：

・ブロックは、イントラ符号化されたマクロブロックの一部分である

・ブロックは、プラスあるいはマイナス１のレベルの値により変化可能な、１つか２つのランレベルコードを含んでいる。ランレベルにおけるその変化は、変化していないレベルに対するＶＬＣと同一の長さを有するＶＬＣをもたらす。（２つのランレベルコードが変化する場合、ＶＬＣの長さの合計だけが等しい必要がある）

ブロックの量子化スケールは２４以下である。

【００８４】

経験的に、典型的なＭＰＥＧ符号化されたデジタル映画は、これらの評価基準を満たす、およそ１億の適当な位置を含んでいるのがわかっている。

【００８５】

以上の評価基準の使用が好適な実施例である一方、本発明は、これらの評価基準に限定されない。したがって、本発明の代替的実施例は、イントラ符号化されていないマクロブロック内部に含まれるブロックを含む、いかなるタイプのブロックからも代替ブロックが作成可能であり、さらに、１つのブロック内の２つのＶＬＣを変更し、追加し、あるいは削除することが可能であり、１つのレベルより大きなレベル内の変化を使用可能であり、さらに、２４より大きい量子化スケールを有するブロックから代替ブロックを作成可能である。他の変化も、本発明の範囲から逸脱することなく可能である。

【００８６】

図５は、代替ブロックを決定するステップ４０２での、ブロック内の可能な改変を識別するために使用可能な再帰的技術のフロー図を示している。非再帰的技術を含む他の異なる技術は、ステップ４０２の実行において、本発明から逸脱することなく、使用可能である。

【００８７】

再帰的技術では、順番に、それ自体の他の例をコールする初期処理が開始される。したがって、この処理のコールされた例は、処理の他の例をコールすることなども可能である。図５では、この再帰的コールは破線として示されている。

【００８８】

初期処理は、ステップ５０１におけるブロックに対するＶＬＣの第１の許可された変更を作成する。ＶＬＣの変更に対して確立された、量子化レベルおよび他の任意の要件に対する評価基準を満たしている場合、ＶＬＣの変更が許可される。その後、ステップ５０２では、処理は、ブロックに対して変更されたＶＬＣの長さのネット変化がゼロであるか否かを確認するようチェックする。ネット変化（再帰的処理を任意にコールすることにおける変更からの変化を含んでいる）がゼロである場合、可能な代替ブロックが見出されたことになる。可能な代替ブロックは、ステップ５０３で可能な代替ブロックのリストに追加される。ネット変化がゼロでない場合は、この変化はステップ５０４で記載（ｎｏｔｅ）される。

【００８９】

この処理は、そのポイントまでのネット変化をパスして、ステップ５０７でそれ自体の他の例を、再帰的にコールする。再帰的にコールされた処理は、ブロックに対するＶＬＣの次の可能な変更から開始する。この次の変更とは、第１もしくは現在のＶＬＣの他の変更、あるいは次のＶＬＣの変更であることもあろう。

【００９０】

この処理は、そのブロックの終端に達するまで、再帰的コールを続ける。処理の１つによりブロックの終端に達すると、この処理のためのフローは、ステップ５０５により、再帰的処理が戻るステップ５０６へ分流される。ここで、戻り処理をコールした処理は、ステップ５０８で続けられ、そのブロック内のＶＬＣの次に許可可能な変更がなされる。この全再帰的処理は、初期処理が、そのブロックの終端に達するまで続く。

【００９１】

以上の再帰的処理の理解の一助に、例を挙げることにする。この例では、２回の変化のみが、ブロックに対する３つのＶＬＣの各々に試みられている。例を単純化するために、すべての変更が許可されていると仮定する。これらの変化は、Ａ＋１、Ａ－１、Ｂ＋１、Ｂ－１、Ｃ＋１、およびＣ－１と示されている。この例では、以下の順序のＶＬＣ変更は、正味の長さの変化がゼロであるとチェックされる：（Ａ＋１），（Ａ＋１，Ｂ＋１），（Ａ＋１，Ｂ＋１，Ｃ＋１），（Ａ＋１，Ｂ＋１，Ｃ－１），（Ａ＋１，Ｂ－１），（Ａ＋１，Ｂ－１，Ｃ＋１），（Ａ＋１，Ｂ－１，Ｃ－１），（Ａ＋１，Ｃ＋１），（Ａ＋１，Ｃ－１），（Ａ－１），（Ａ－１，Ｂ＋１），（Ａ－１，Ｂ＋１，Ｃ＋１），（Ａ－１，Ｂ＋１，Ｃ－１），（Ａ－１，Ｂ－１），（Ａ－１，Ｂ－１，Ｃ＋１），（Ａ－１，Ｂ－１，Ｃ－１），（Ａ－１，Ｃ＋１），（Ａ－１，Ｃ－１），（Ｂ＋１），（Ｂ＋１，Ｃ＋１），（Ｂ＋１，Ｃ－１），（Ｂ－１），（Ｂ－１，Ｃ＋１），（Ｂ－１，Ｃ－１），（Ｃ＋１），および（Ｃ－１）．

【００９２】

図５の再帰的技術は、所与のブロックに対する、全ての可能な代替ブロックを見出すために使用可能である。しかしながら、代替的実施例では、この技術は、いったんある程度の数の可能な代替ブロックが見出されたり、あるいはいったん単一の代替ブロックが見出された場合でも停止可能である。複数の可能な代替ブロックが見出された場合は、１つ以上の可能な代替ブロックが、例えば、擬似ランダムに、可能な代替ブロックから選択可能であろう。他の変形形態も可能であり、本発明の範囲内にとどまっている。

【００９３】

２．　フィンガープリンティング

図４に戻って、フィンガープリンティングはステップ４０３で実行される。フィンガープリンティングは、情報をデジタルコンテンツに埋め込むために、選択された位置で改変のいくつかを実際に作成する処理である。ＭＰＥＧの文脈では、改変は、いくつかのオリジナルブロックに代えて代替ブロックを使用することにより作成される。

【００９４】

ブロックに対して１つの代替ブロックが見出された場合、その位置へ１ビットを埋め込むのにその代替ブロックが使用可能である。例えば、１組の位置および可能な改変がいったん決定されると、その位置でオリジナルブロックを使用することにより、その位置へ「０」を埋め込み可能であり、その位置で代替ブロックを使用することにより、「１」を埋め込み可能である。データを埋め込む他の構成も使用可能である。

【００９５】

さらに、選択された位置で、ブロックに対して１つより多い代替ブロックが見出される場合、それらの代替ブロックは、その位置で１ビットより多くを埋め込むのに使用可能である。例えば、オリジナルブロックが「００」を表し、第１代替ブロックが「０１」を表し、第２代替ブロックが「１０」を表し、さらに第３代替ブロックが「１１」を表すことが可能である。さらに、複数の代替ブロックを使用する他のスキームも可能である。

【００９６】

ステップ４０３では、デジタルコンテンツ内の選択された位置のいくつかにおいて、代

替ブロックをオリジナルブロックの代わりに用いることにより、情報（すなわち、ビット）がデジタルコンテンツ内へ埋め込まれる。デジタルコンテンツの配布においては、複数の異なる点で変化を受けるのは、位置のサブセットのみであるのが好ましい。例えば、第１サブセットは１次キャッシュ１１２で変化を受け、第２サブセットが中間キャッシュ１１３で変化を受け、第３サブセットがリーフキャッシュ１１４で変化を受ける、などが可能である。概して、少なくともいくつかの「０」（あるいは、符号化スキームに依存する他の値）が利用可能な位置へ埋め込まれるので、各サブセット内のすべての位置が変更されるというわけではないことになる。

【００９７】

３．フィンガープリント情報の抽出

フィンガープリンティングが重要であるのは、埋め込まれた情報を抽出可能であるからに他ならない。図６は、デジタルコンテンツ内のフィンガープリントから、埋め込まれた情報を抽出する方法のフロー図を示している。データは、図６に示したステップを実行可能な計算装置で抽出可能である。こうした計算装置は、少なくとも、デジタルコンテンツを格納し、さらにステップを実行するインストラクションを格納するプロセッサおよびメモリを含んでいるのが好ましい。

【００９８】

ステップ６０１では、デジタルコンテンツの特定のアイテムに対する透かしが決定される。この透かしは、デジタルコンテンツの特定のアイテム用のそれらの位置に、１組の位置と可能な改変（例えば、代替ブロック）を含んでいる。

【００９９】

透かし自体は、エンドユーザに配布されるデジタルコンテンツには含まれていないのが好ましい。したがって、デジタルコンテンツについての識別情報に基づいて、透かしは注入ポイント１２０から検索されるのが好ましい。こうした識別情報の例には、コンテンツのタイトル、改訂番号、シリアル番号などが含まれる。

【０１００】

識別情報は、それ自体、何らかの強健な方式でデジタルコンテンツ内に埋め込まれているか、あるいはデジタルコンテンツから自明であることが好ましい。例えば、ＭＰＥＧ符号化された映画の場合は、識別情報は映画のタイトルであることもあり、これは、映画の内容から自明である。他の識別情報も利用可能である。

【０１０１】

透かしがいったん検索されると、ステップ６０２で、透かしにより決定される情報を埋め込む選択位置を検査可能である。位置は、透かしにより特定される可能な改変に従って、各位置のうちのいずれが改変されたかを決定するために検査される。

【０１０２】

次に、ステップ６０３では、改変（例えば、代替ブロック）が存在しているか、あるいは存在していないかの検査から、埋め込まれた情報を抽出可能である。例えば、存在している改変がデジタルの「１」を表し、存在していない改変がデジタルの「０」を表すことができる。本発明から逸脱することなく、他の符号化スキームが使用可能である。

【０１０３】

各々の埋め込まれたビット情報は、デジタルコンテンツ内に何度も埋め込まれるのが好ましい。これにより、いくつかの位置で改変の喪失あるいは変造があっても、埋め込まれた情報は喪失しないことになる。

【０１０４】

加えて、デジタルコンテンツ内の位置の順序は、既知であるがランダム（あるいは、擬似ランダム）な何らかの方式で埋め込まれた情報における、ビットの順序に関連しているのが好ましい。この埋め込み情報の混ぜ合わせは、埋め込まれた情報への権限のないアクセス、あるいは変造の防止を補助する。

【０１０５】

検査されるデジタルコンテンツは、故意にあるいは偶発的に改変されたこともあろう。

結果として、デジタルコンテンツ内のいかなる所与のブロックも、コンテンツの透かしからのオリジナルブロックあるいは代替ブロックのどちらとも、正確には整合しないこともあろう。この問題を処理するために、例えば、ＶＬＣから得られるＤＣＴ係数のベクトルスペースなど、何らかのベクトルスペース内の対応するオリジナルブロックからの各ブロックの距離が計算可能であろう。その後、オリジナルブロックあるいは代替ブロックの何らかの距離以内にあるブロックは、これらのブロックに整合するとみなすことができよう。埋め込まれたデータの各ビットが何度も埋め込まれている場合、埋め込まれたデータを計算するために、十分なビットが抽出されることになろう。

【０１０６】

本発明の一般性

代替ブロックの生成は、デジタルコンテンツに対して使用される符号化のタイプに依存していない。一般的な意味で、本発明の透かし入れ技術およびフィンガープリントをほどこす技術は、連続の、あるいはアナログの物理処理をモデル化する、いかなるディジタルデータにも適用可能である。本発明は、ＭＰＥＧ－ハフマンコード化、あるいは他の完全に異なる符号化スキームを使用しているか否かに関係なく、ＭＰＥＧの何らかのバージョン－により符号化された、デジタル化された音声データ、測定データ、ビデオデータ、他のマルチメディアデータなどに適用可能である。データを埋め込むために、デジタルコンテンツ内の位置を選択し、さらに、選択された位置へほどこされる可能な改変を選択するために、本発明の技術はこのデジタル化されたデータのいずれにも使用可能であり、その間ずっと、データのパケット化が保存される。

【０１０７】

さらには、本発明は、メディアストリームの配布以外およびデジタルコンテンツの配布以外のアプリケーションにも役立ち、十分な一般性を有している。例えば、本発明は、また、概して、データセットのセキュリティ、あるいはそれらのデータセットの受取人を識別することが所望されているアプリケーションに役立つ。

【０１０８】

このように、本明細書には、好適な実施例が開示されているが、本発明の概念、範囲、および趣旨内に留まりながらも、多くの変形形態が可能である。これらの変形形態は、本明細書を熟読するならば、当業者には明白になろう。

【図面の簡単な説明】

【０１０９】

【図１】デジタルコンテンツに透かしを入れ、フィンガープリントをほどこすシステムのブロック図である。

【図２】本発明に従う、ＭＰＥＧ符号化と、代替ブロックの生成を示す図である。

【図３】本発明に従う、パケット化の保存を示す図である。

【図４】情報が埋め込まれることになる１組の位置で、デジタルコンテンツに透かしを入れ、フィンガープリントをほどこす方法のフロー図である。

【図５】本発明に従う、代替ブロックを決定するために、ブロック内の可能な改変を識別するために使用可能な再帰的技術のフロー図である。

【図６】情報をデジタルコンテンツに埋め込むフィンガープリントの検出方法のフローチャートを示す図である。

【図１】

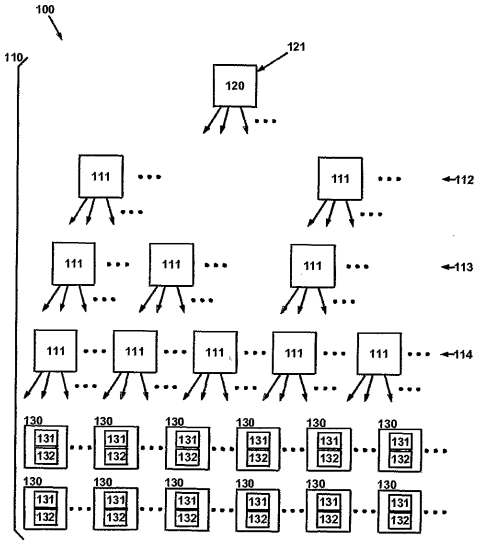
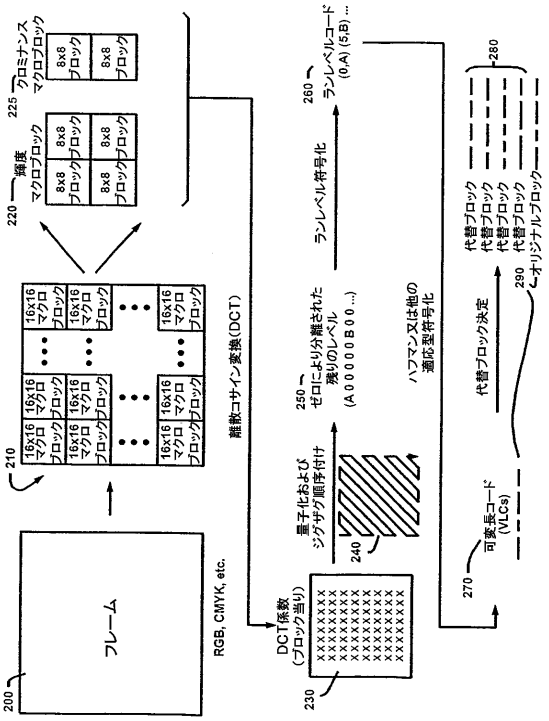
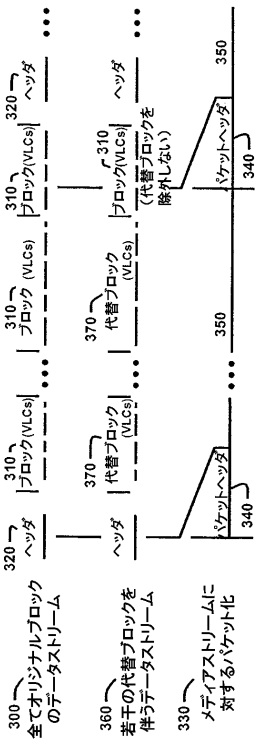


Fig. 1

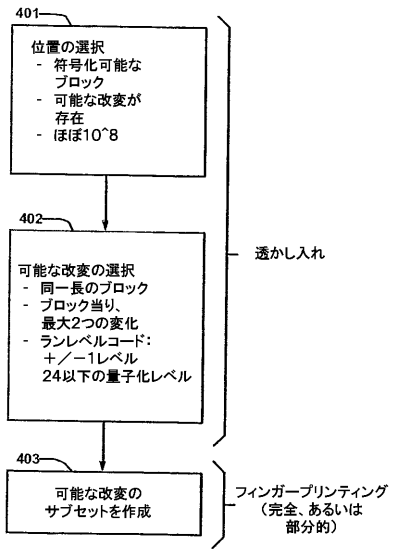
【図２】



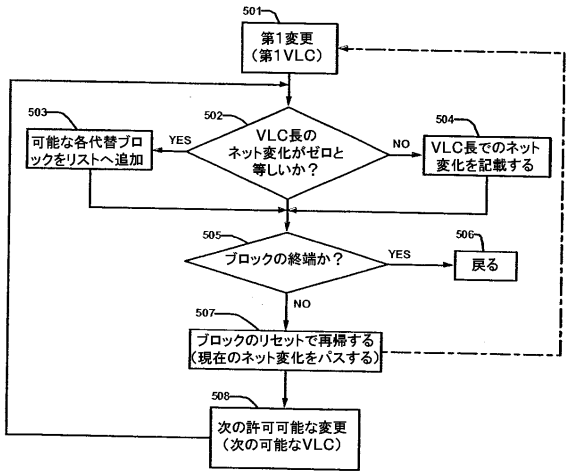
【図３】



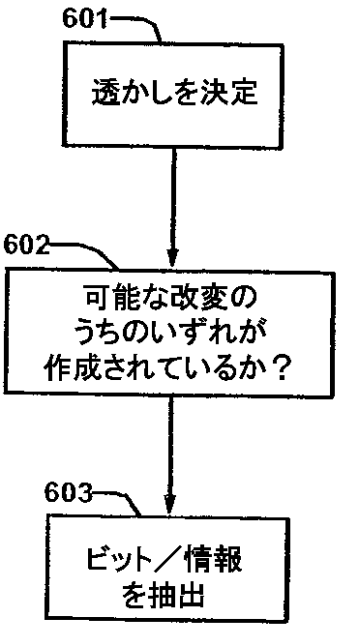
【図４】



【図５】


501
第1変更
（第1VLC）
502
VLC長の
ネット変化がゼロと
等しいか？
YES
503
可能な各代替ブロ
ックをリストへ追加
NO
504
VLC長でのネット
変化を記載する
505
ブロックの終端か？
YES
506
戻る
NO
507
ブロックのリセットで再帰する
（現在のネット変化をパスする）
508
次の許可可能な変更
（次の可能なVLC）

【図６】


601
透かしを決定
602
可能な改変の
うちのいずれが
作成されているか？
603
ビット／情報
を抽出

フロントページの続き

(31)優先権主張番号 60/394,588
(32)優先日 平成14年7月9日(2002.7.9)
(33)優先権主張国 米国(US)
(31)優先権主張番号 10/356,322
(32)優先日 平成15年1月31日(2003.1.31)
(33)優先権主張国 米国(US)

前置審査

(72)発明者 ダニエル・エイ・コレンズ
カナダ、エヌ２ケイ・３ゼット８、オンタリオ、ウォータールー、ボナビスタ・ドライブ７９０番
(72)発明者 ケビン・フイ
カナダ、エヌ２エム・５イー４、オンタリオ、キッチェナー、ウエスト・アベニュー３０８－２９番
(72)発明者 マイケル・エイ・マルコム
アメリカ合衆国８１６１２コロラド州アスペン、ポスト・オフィス・ボックス７６６７

審査官 川崎 優

(56)参考文献 特開平１１－３４１４５０（ＪＰ，Ａ）
国際公開第０１／０１９０７１（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04N 7/16-173,7/24,26-68,1/387,40-41
G06F 21/24

(54)【発明の名称】デジタルコンテンツマーキング方法、デジタルコンテンツ内のフィンガープリントを検出する方法、デジタルコンテンツ、デジタルコンテンツに透かしを入れる装置、透かしを入れたデジタルコンテンツにフィンガープリントをほどこす装置、デジタルコンテンツ内のフィンガープリントを検出する装置、およびインストラクションを含む情報を格納するメモリ