

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4572085号
(P4572085)

(45) 発行日 平成22年10月27日 (2010.10.27)

(24) 登録日 平成22年8月20日 (2010.8.20)

(51) Int. Cl. F I
H O 4 N 7 / 1 6 7 (2006.01) H O 4 N 7 / 1 6 7 Z

請求項の数 8 (全 21 頁)

(21) 出願番号	特願2004-109417 (P2004-109417)	(73) 特許権者	500046438
(22) 出願日	平成16年4月1日 (2004.4.1)		マイクロソフト コーポレーション
(65) 公開番号	特開2004-310097 (P2004-310097A)		アメリカ合衆国 ワシントン州 9805
(43) 公開日	平成16年11月4日 (2004.11.4)		2-6399 レッドモンド ワン マイ
審査請求日	平成19年4月2日 (2007.4.2)		クロソフト ウェイ
(31) 優先権主張番号	10/405,970	(74) 代理人	100077481
(32) 優先日	平成15年4月1日 (2003.4.1)		弁理士 谷 義一
(33) 優先権主張国	米国 (US)	(74) 代理人	100088915
			弁理士 阿部 和夫
		(72) 発明者	シュ ビン
			アメリカ合衆国 55436 ミネソタ州
			エディナ クレセント ドライブ 59
			15

最終頁に続く

(54) 【発明の名称】 スケーラブルなマルチメディアに関する完全にスケーラブルな暗号化

(57) 【特許請求の範囲】

【請求項 1】

基本層および拡張層を有するスケーラブル・マルチメディア・ストリームを暗号化する方法であって、

前記マルチメディア・ストリームのセグメントの少なくとも一部の基本層コンテンツから第1のキーを取り出すこと、

前記第1のキーを使用して前記セグメントの前記基本層コンテンツの一部を置き換えること、

前記セグメントの前記基本層の少なくとも一部および前記セグメントの前記拡張層の少なくとも一部を、前記第1のキーを使用して暗号化すること、および

チェーン&サム暗号化技術あるいはブロック暗号による暗号化技術を使用して、前記基本層の前記コンテンツの少なくとも一部の、暗号化されるべき前記基本層の少なくとも一部の暗号化前のメッセージ認証コードの少なくとも一部を備えるハッシュ値あるいはハッシュ値の合計から、前記第1のキーの少なくとも一部を生成すること

を備え、

前記基本層の一部を置き換えることは、

暗号化されるべき前記基本層の一部を、前記暗号化前のメッセージ認証コード (pre-MAC) に置き換え、

前記基本層のデータサイズの増大を防ぎ、前記暗号化されたスケーラブル・マルチメディア・ストリームのスケーラビリティを維持する

10

20

ことを備え、

前記暗号化前のメッセージ認証コードは、可逆性を有し、暗号化されたメッセージ認証コードが暗号化解除され元の基本層コンテンツに復元することを可能にすることを特徴とする方法。

【請求項 2】

前記スケーラブル・マルチメディア・ストリームの全体を暗号化するグローバル・キーであり、前記基本層コンテンツおよび前記拡張層コンテンツのうちの一つあるいは両方を暗号化するための、第 2 のキーを使用することを備えることを特徴とする請求項 1 に記載の方法。

【請求項 3】

オブジェクト・ヘッダを除いて、前記基本層の全てのエントロピー符号化マルチメディア・データを符号化することを備えることを特徴とする請求項 1 に記載の方法。

【請求項 4】

前記基本層の各フレームから一つまたは複数のビット・セットだけを選択的に暗号化することを備え、ビット・セットは、フレーム間 DC 係数ビットの離散コサイン値、または DC T の DC 差分ビットの離散コサイン値、または離散コサイン変換係数の符号ビット、または離散コサイン伝達係数の符号ビット、または動きベクトルの符号ビット、または動きベクトル剰余の符号ビットを備えることを特徴とする請求項 1 に記載の方法。

【請求項 5】

前記スケーラブル・マルチメディア・ストリームの全体を暗号化するグローバル・キーである第 2 のキーを使用して前記基本層を暗号化すること、

前記第 1 のキーと前記第 2 のキーを暗号器に入力し、前記拡張層内の離散コサイン変換係数の符号ビットと XOR 演算されるビット・シーケンスを生成することによって前記拡張層を暗号化すること

を備えることを特徴とする請求項 1 に記載の方法。

【請求項 6】

ランダム・ビット・シーケンスを生成して前記暗号器に追加入力し、前記ビット・シーケンスを生成すること、

擬似ランダム・ビット・シーケンスを生成して前記暗号器に追加入力し、前記ビット・シーケンスを生成すること、

フレーム・カウントをオブジェクト・ヘッダに追加し、前記フレーム・カウントを前記暗号器に追加入力して、ビット・シーケンスを生成すること

のうちの一つを備えることを特徴とする請求項 5 に記載の方法。

【請求項 7】

XOR 演算を実行して、選択的に暗号化された拡張層を生成することを備え、

前記 XOR 演算は、

前記ビット・シーケンスからの第 1 のビットアレイと、

前記基本層あるいは前記拡張層のフレームからの離散コサイン変換係数の符号ビットの、対応する第 2 のアレイ、あるいは

前記基本層あるいは前記拡張層のフレームからのテンポラル・ビデオ・オブジェクト・プレーン動きベクトルの対応する第 2 のアレイ

との間に適用される

ことを特徴とする請求項 5 に記載の方法。

【請求項 8】

ビット・シーケンスを使用して前記基本層を暗号化することを備え、前記基本層を暗号化するための前記ビット・シーケンスは、前記拡張層を暗号化するための前記ビット・シーケンスと異なり、前記拡張層を暗号化するための前記ビット・シーケンスは、ビット・シーケンスにシードを送り込むことによって生成されることを特徴とする請求項 5 に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、一般に、マルチメディア保護に関し、より具体的には、スケーラブルなマルチメディアに関する完全にスケーラブルな暗号化に関する。

【背景技術】

【0002】

スケーラブル・ビデオ・コーディングは、マルチメディア・コンテンツに対して、それが多くの異なるアプリケーションおよび環境に適合させることができるように、柔軟性および適応性付与する。スケーラブルなマルチメディア・フォーマットには、とりわけ、いくつかのMPEGストリーム・フォーマット、および「スケーラブル・メディア適合および堅牢なトランスポート」(SMARTおよびSMART++) (例えば、非特許文献1、非特許文献2、非特許文献3、および非特許文献4を参照)が含まれる。

【0003】

MPEG-4は、個々のデバイスにスケーラビリティを提供するのにプロファイルを採用している。1つのそのようなMPEG-4プロファイルは、「Simple」プロファイルと呼ばれている。「Simple」は、「Simple Scalable」などの他のプロファイルが拡張層を追加してスケーラビリティを提供することができる、ビデオ基本層を提供する。「Advance Simple」と呼ばれる別のプロファイルは、「Simple」プロファイルにいくつかのコーディング・ツールを追加することによって四角形ビデオ・オブジェクト・コーディング(rectangular video object coding)を実行する。この「Advance Simple」プロファイルは、最新のMPEG-4コーディング効率ツールを有してはいるが、スケーラビリティを全く提供しない。「Advance Simple」基本層に細粒度の(fine-grained)拡張層を追加することによってスケーラブル・ビデオコーディング・スキームを提供するさらに別のMPEG-4プロファイルは、「Fine Granularity Scalability」(FGS)と呼ばれている。FGSは標準になっている。

【0004】

これらのスケーラブルMPEG-4プロファイルで使用される基本層は、ビットレートの下限でスケーラブルでない形でエンコードされる。FGSプロファイルは、同じ拡張層で可能なビットレートの範囲内の各ビットレートに関して最適なビデオ品質を実現しようと努める低いビットレートの基本層から予測された拡張層を含む。拡張層は、スケーラブルな形でエンコードされる。すなわち、フレームの残りの離散コサイン変換(DCT)係数が、最上位ビットから最下位ビットまでビット・プレーンごとに(bit-plane wise)圧縮される。ビデオは、MPEG-4 FGSによって1回だけ圧縮される。ビデオがネットワークを介して伝送される際、伝送ネットワークに必要とされる帯域幅が不足しているようなことがあれば、サーバは、最下位ビットに関連する拡張層データを破棄することができる。その他の速度シェーピング操作(rate shaping operation)も、圧縮または展開に頼ることなく、圧縮された拡張層データに対して直接に実行することができる。前述したFGSプロファイルを本明細書でMPEG-4 FGS、または単に「FGS」と呼ぶ。

【0005】

様々なスケーラブルMPEG-4プロファイルに準拠するマルチメディア・ストリームに関するマルチメディア暗号化技術は、理想的には、スケーラブルでないコーデックにおいて望ましい特徴と同じ特徴を有する。すなわち、高いセキュリティ、低い複雑性、低い圧縮オーバーヘッド、エラー耐性(error resilience)、速度シェーピング適合性、およびランダム再生能力である。次に、これらのいくつかをより詳細に説明する。

【0006】

セキュリティは、マルチメディア暗号化の必要不可欠な要件である。軍事プロセスや銀行業務プロセスなどのよりクリティカルなアプリケーションに関する他のタイプの暗号化と比べると、マルチメディア暗号化は、軍事データおよび銀行業務データと比べて、暗号化されるべき(ビデオ)データが比較的大量であること、およびデータの価値が特質上低

10

20

30

40

50

いことを含め、それ自身の特有の問題を有する。

【0007】

あらゆる暗号化プロセスまたは暗号化解除プロセスは、処理オーバーヘッドを付加するので、低い複雑性は、特徴付ける機能である。マルチメディア・ストリームは、比較的大量のデータを有するので、多くのアプリケーションにおいて、暗号化システムの複雑性が、非常に低いことが望ましいか、または必須であり、多くのアプリケーションは、通常ユーザの限られた設備上で大量のマルチメディア・データのリアルタイムの暗号化解除を、必要とするので、特に暗号化解除中、暗号化システムの複雑性が、非常に低いことが望ましいか、または必須である。

【0008】

また、暗号化は、圧縮アルゴリズムのコーディング効率を低下させること、または既に圧縮済みのファイルにバイトを追加することによって圧縮効率に不可避に影響を及ぼすので、圧縮オーバーヘッドも、特徴付ける機能である。したがって、圧縮オーバーヘッドは、マルチメディア暗号化アルゴリズムに対して理想的に最小限に抑えられる。

【0009】

エラー復元力は、マルチメディアの格納中および伝送中に障害が生じるので、暗号化にとって重要である。ワイヤレス・ネットワークは、伝送エラーで有名である。データパケットが、輻輳、バッファ・オーバーフロー、およびその他のネットワークの不完全さに起因して失われる可能性がある。暗号化スキームは、理想的には、ビット・エラーおよびパッケージ損失に対する復元力を有さなければならない。また、暗号化スキームは、ビット・エラーからの迅速な回復、およびパッケージ損失からの高速の再同期、を可能にして広範なエラー伝搬を防止することも行わなければならない。多くのマルチメディア暗号化アルゴリズムは、通常、完璧な伝送環境の下で設計されており、伝送中にビット・エラーまたはパッケージ損失が生じた場合、大幅な知覚的な劣化 (perceptual degradation) を伝搬させる。

【0010】

速度シェーピング (Rate shaping) とは、様々な条件に合うように伝送ビットレート (1秒間のストリーム内のビット数) を変更する能力のことである。コンテンツ所有者からユーザへのマルチメディア・ストリーム配信中、多くの中間ステージが、通常、そのデータを処理する。例えば、コーディング変換 (transcoding) により、伝送帯域幅の変動に適合するように、またはアプリケーション要件にさえ適合するようにビットレートが変更される可能性がある。データが暗号化されている場合、それらの中間ステージは、データを処理するために、通常、暗号化キーおよび暗号化解除キーを呼び出して、暗号化解除のサイクルおよび暗号化のサイクルを実行しなければならない。このことは、暗号化の秘密が、それらの中間ステージと共有されなければならないので、処理オーバーヘッドを増大させ、セキュリティを低下させる。

【0011】

前述したセキュリティの特徴に関連して、しばしば、デジタル著作権管理 (DRM) のためにマルチメディア・ストリームを暗号化することが望ましい。そのような暗号化は、コンテンツ所有者が、マルチメディア・コンテンツのライセンス供与などの著作権およびその他の所有権を行使するのを手助けすることができる。

【0012】

スケーラブルでないビデオを暗号化する多くのアルゴリズムが提案されてきている。最も単純明快な方法は、圧縮されたストリームに対して、あたかもそれがテキスト・データであるかのように同じ形で、DESなどの標準の暗号化スキームを適用する素朴なアルゴリズムである (非特許文献5参照)。素朴なアルゴリズムは、通常、処理されるべき大量のビデオ・データに起因して大きい処理オーバーヘッドを有する。素朴なアルゴリズムは、最低限のエラー復元力しか有さず、暗号化テキストに対して直接に速度シェーピングを行うことを可能にしない。

【0013】

10

20

30

40

50

別の方法として、ビデオ・ストリーム構造を活用し、圧縮されたビデオ・データの一部だけを暗号化する選択的アルゴリズム（非特許文献6および非特許文献7参照）が提案されている。暗号化される部分的データは、Iフレーム、Iフレームに加えてPフレーム内およびBフレーム内のすべてのIブロック、またはそのIブロックのDC係数とより低いAC項とすることが可能である。Iフレームだけを暗号化することは、Pフレーム内およびBフレーム内で公開されたIブロック、ならびにフレーム間の相関に起因して、十分なセキュリティを提供しない（非特許文献5参照）。

【0014】

暗号化されるべきデータを減少させる方法として、Iフレームのかたまりに関して偶数インデックスにおけるバイトだけを暗号化し、残りを、奇数インデックスの付いたサブシーケンスを偶数インデックスの付いたサブシーケンスとXOR演算した結果で置き換える方法（非特許文献8参照）が提案されている。

10

【0015】

別の選択的アルゴリズムとして、すべてのDCT係数の符号ビットを擬似ランダムに変更する方法（非特許文献9参照）、またはIブロックのDC係数の差分値(differential value)の符号ビット、および動きベクトルの差分値の符号ビットを擬似ランダムに変更する方法（非特許文献10参照）も提案されている。

【0016】

第3の手法は、一部の圧縮パラメータにスクランブルをかけたり、またはコードワードをシャッフル(shuffle)したりして、許可のないユーザが正しい展開(圧縮解除)を行うのを防止するスクランブル・アルゴリズムである。単純なスキームは、2Dブロックを1Dベクトルにマップするのに、通常のジグザグの順序ではなく、ランダムな置き換えを使用する（非特許文献11参照）。動きベクトルおよび選択されたDCT係数を、エントロピー・コーディングを行う前にシャッフルすることができる（非特許文献12および非特許文献13参照）。

20

【0017】

VLC(可変長コーディング)も、フォーマットに準拠する形でシャッフルすることができる（非特許文献14参照）。以上のスキームは、データの統計的特性を変化させ、これにより、圧縮効率を低下させる。ビット・オーバーヘッドを被ることなく機能するスキームも提案されている。圧縮ビットストリームのコードワードを空間的にシャッフルする方法（非特許文献15参照）も提案されている。

30

【0018】

前述したスキームの一部、およびその他のスキーム、例えば、ほとんどのスクランブル・アルゴリズムも、MPEG-4 FGSに同様に適用可能であるが、スケーラブルでないマルチメディア向けに開発されているほとんどの暗号化スキームは、スケーラブル・マルチメディアに適用された場合、しばしば、スケーラビリティの特徴を、減じるか、または損なう。そのような暗号化されたスケーラブル・ストリームにスケーラブル操作を提供するために、中間伝送ステージは、しばしば、ストリームを暗号化解除し、コーディング変換および/またはビット削減(bit reduction)などの速度シェーピングを適用した後、ストリームを再暗号化しなければならない。したがって、スケーラビリティの特徴を保ちながら、スケーラブル・マルチメディア・ストリームを暗号化するための技術が必要とされている。

40

【0019】

スケーラブル・フォーマット向けに特に設計されたスキームが、最近、報告されている。ウィー(Wee)他が、暗号化解除なしにコーディング変換を可能にするセキュアなスケーラブル・ストリーミング(SSS)スキームを提案している（非特許文献16参照）。MPEG-4 FGSに関して、この手法は、ヘッダ・データを除き、基本層と拡張層の両方においてビデオ・データを暗号化する。中間ステージがRD最適ビットレート削減を実行するように速度歪曲最適(rate distortion optimal)(RD最適)カットオフ・ポイントに関するヒントを暗号化されていないヘッダの中に挿入しなければならない。暗号

50

化細粒度 (Encryption granularity) は、ビデオ・ストリームがパケット化されている仕方に依存する。より正確には、各パケットに暗号化が適用される。これは、暗号化が S S S において適用される場合、パケット・サイズが分かっていることを意味する。S S S において暗号化が行われた後、パケット・サイズの変更は、全く許されない。現実のアプリケーションでは、1つのタイプの伝送チャンネル向けに設計されたパケット・サイズは、別のタイプの伝送チャンネルには適切でない可能性がある。例えば、ワイヤレス伝送のためのビデオ・パケット・サイズは、チャンネルにエラーが生じやすいため、小さくしなければならない。インターネット伝送の場合、インターネットに関するエラー率は非常に小さいので、ビデオパケットは、効率的な伝送のために大きくななければならない。その伝送チャンネルに最適なパケット・サイズに変更することを望むいずれの中間ステージも、S S S における暗号化解除／再暗号化サイクルに依存する必要がある。

10

【0020】

G r o s b o i s 他が、J P E G 2 0 0 0 のイメージ圧縮標準のためのスケーラブル認証—アクセス制御スキームを提案している (非特許文献 17 参照)。このスキームは、ビットストリーム内の情報の変更および挿入に基づいている。キー付ハッシュ値 (keyed hash value) が、高周波数帯域ウェーブレット係数の符号を擬似ランダムに反転させるのに使用される擬似ランダム・シーケンスを生成するのに使用される。階層化されたアクセス構造 (layered access structure) が、異なるアプリケーションに対する適合を可能にしている。このスキームの大きな欠点の 1 つは、暗号化解除を助ける追加の情報の挿入にあり、これにより、圧縮効率を低下させている。

20

【0021】

【非特許文献 1】ワシントン州レッドモンド市のマイクロソフト・コーポレーションの<<http://research.microsoft.com/im/>>

【非特許文献 2】Feng Wu, Shipeng Li, Ya-Qin Zhang, "A framework for efficient progressive fine granular scalable video coding", IEEE Trans. on Circuits and Systems for Video Technology, vol. 11, no. 3, pp. 332-344, 2001

【非特許文献 3】Xiaoyan Sun, Feng Wu, Shipeng Li, Wen Gao, Ya-Qin Zhang, "Macroblock-based temporal-SNR progressive fine granularity scalable video coding", IEEE International Conference on Image Processing (ICIP), pp. 1025-1028, Thessaloniki, Greece, October, 2001

30

【非特許文献 4】Yuwen He, Feng Wu, Shipeng Li, Yuzhuo Zhong, Shiqiang Yang, "H.26L-based fine granularity scalable video coding", ISCAS 2002, vol. 4, pp. 548-551, Phoenix, USA, May 2002

【非特許文献 5】I. Agi and L. Gong, "An Empirical Study of Secure MPEG Video Transmissions," Proc. Symp. Network & Distributed System Security, 1996, pp. 137-144

【非特許文献 6】T. B. Maples and G. A. Spanos, "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-time Video," Proc. 4th Int. Conf. Computer Communications & Networks, 1995

【非特許文献 7】J. Meyer and F. Gadekast, "Security Mechanisms for Multimedia Data with the Example MPEG-1 Video," <http://www.gadegast.de/frank/doc/secmeng.pdf>, 1995

40

【非特許文献 8】L. Qiao and K. Nahrstedt, "Comparison of MPEG Encryption Algorithms," Int. J. Computers & Graphics, Special Issue: "Data Security in Image Communication and Network", vol. 22, no. 3, 1998)

【非特許文献 9】C. Shi and B. Bhargava, "A Fast MPEG Video Encryption Algorithm," Proc. of ACM Multimedia'98, 1998, pp. 81-88

【非特許文献 10】C. Shi and B. Bhargava, "An Efficient MPEG Video Encryption Algorithm," IEEE Proc. 17th Symp. Reliable Distributed Systems, 1998, pp. 381-386

【非特許文献 11】L. Tang, "Method for Encrypting and Decrypting MPEG Video Data

50

Efficiently," Proc. ACM Multimedia'96, 1996, pp. 219-230

【非特許文献12】W. Zeng and S. Lei, "Efficient Frequency Domain Video Scrambling for Content Access Control," Proc. ACM Multimedia'99, 1999, pp. 285-294

【非特許文献13】W. Zeng and S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video," IEEE Trans. Multimediaに掲載予定の予稿

【非特許文献14】J. Wen, M. Severa, W. Zeng, M. H. Luttrell, and W. Jin, "A Format-compliant Configurable Encryption Framework for Access Control of Video," IEEE Trans. Circuits & Systems for Video Technology, vol. 12, no. 6, 2002, pp. 545-557

【非特許文献15】W. Zeng, J. Wen, and M. Severa, "Fast Self-synchronous Content Scrambling by Spatially Shuffling Codewords of Compressed Bitstreams," IEEE Int. Conf. Image Processing, 2002, vol. 3, pp. 169-172 10

【非特許文献16】S. J. Wee and J. G. Apostolopoulos, "Secure Scalable Streaming Enabling Transcoding Without Decryption," IEEE Int. Conf. Image Processing, 2001, vol. 1, pp. 437-440

【非特許文献17】Raphael Grosbois, Pierre Gergelot, and Touradj Ebrahimi, "Authentication and Access Control in the JPEG 2000 compressed domain," Proc. of SPIE 46th Annual Meeting, Applications of Digital Image Processing XXIV, San Diego, 2001

【非特許文献18】Mariusz H. Jakubowski, Ramarathnam Venkatesan, "The Chain & Sum Primitive and Its Applications to MACs and Stream Ciphers", EUROCRYPT'98, pp. 281-293, 1998 20

【発明の開示】

【発明が解決しようとする課題】

【0022】

上述したように、ウィー（Wee）他が、暗号化解除なしにコーディング変換を可能にするセキュアなスケーラブル・ストリーミング（SSS）スキームを提案しているが、このスキームにおいては、その伝送チャンネルに最適なパケット・サイズに変更することを望むいずれの中間ステージも、SSSにおける暗号化解除／再暗号化サイクルに依存する必要があるという欠点を有している。 30

【0023】

また、上述したように、Grosbois他が、JPEG2000のイメージ圧縮標準のためのスケーラブル認証・アクセス制御スキームを提案しているが、暗号化解除を助ける追加の情報の挿入を必要として、これが、圧縮効率を低下させるという大きな欠点を有している。

【課題を解決するための手段】

【0024】

本発明は、スケーラブル・マルチメディアについて完全にスケーラブルに暗号化するための例示的なシステムおよび関連する方法を含む。本発明を使用して暗号化されたスケーラブル・ビットストリームは、暗号化された形態で、スケーラブルな機能（scalable features）の完全な機能性を保つ。例示的なスケーラブル暗号化は、スケーラブル圧縮効率およびエラー復元力を低下させることなく、暗号化テキストに対して、コーディング変換、速度シェーピング、およびその他の操作を直接に行うことを可能にする。本発明は、例えば、MPEG-4 FGS、MPEG-4 FGST、SMART、およびSMART++ストリームを含むスケーラブル・マルチメディア・ストリームに適用することができる。 40

【0025】

例示的なスケーラブル方法は、基本層だけを暗号化する。別の例示的なスケーラブル方法は、スケーラブル・マルチメディア・ストリームの基本層と拡張層をともに暗号化する。基本層は、軽いセキュリティ要件に関して選択的に暗号化すること、またはより厳格なセキュリティ要件のために完全に暗号化することができる。 50

【発明を実施するための最良の形態】

【0026】

概要

本発明は、新たに採用されたMPEG-4 Fine Granularity Scalability (FGS) ビデオ・コーディング標準、およびSMARTビデオオーディオ・コーディングのような他のスケーラブル・マルチメディア・コーディング・スキームを遵守するビットストリームなどのスケーラブル・マルチメディアを、完全にスケーラブルに暗号化するためのシステム、および関連する方法を含む。これらのスケーラブル・ビットストリームは、異なる伝送ニーズおよびアプリケーションニーズに対する、同ストリームの、容易で柔軟性のある適合を可能にする完全なスケーラビリティを提供する。本発明は、暗号化解除されたスケーラブル・ビットストリームのスケーラビリティの特徴を保つように努める暗号化技術を提供する。そのような例示的なシステム、および関連する方法は、スケーラブル・マルチメディア・コーディング・スキームを介する暗号化ベースのデジタル権利管理(DRM)に役立つ。

10

【0027】

本発明の一態様によれば、比較的低い複雑性を有する例示的な方法が、デジタル権利管理などのアプリケーションのためにスケーラブル・ビットストリームを暗号化するように提供される。この例示的な方法は、暗号化された暗号化テキストを直接使用して完全なFGS機能を可能にする。これにより、ビットストリームに対する中間操作中に、ビットストリームを暗号化解除する必要性が阻止される。本発明を使用して、動的な環境にビットストリームを適合させるプロセスまたはデバイス(例えば、限られた帯域幅を有するネットワークに合うようにストリームのビットレートを低減するネットワーク・デバイス)などの中間ステージは、暗号化テキストを暗号化解除することなく、コーディング変換、速度シェーピング、および再パケット化、などのFGS操作を実行することができる。暗号化サイクルおよび暗号化解除サイクルが、伝送中に各中間デバイスによって繰り返される必要がないので、キーおよびその他の秘密が中間ステージと共有されることもなく、より良好なセキュリティを維持することができる。これにより、中間ステージにかかる処理負荷が大幅に軽減され、例示的なスケーラブル暗号化システムの終端間セキュリティ(end-to-end security)が向上する。また、例示的な暗号化システム200は、細粒度も保ち、切り捨て(truncation)や他の速度シェーピング操作が行われた場合でも、残りのFGSがRD最適化されたビデオ・ストリームであるようにする。

20

30

【0028】

さらに、例示的な暗号化のシステムおよび方法は、スケーラブル圧縮効率、ならびに伝送パケット損失とビット・エラーに対するエラー復元力、に対する低下を全く生じさせない。また、例示的なシステムおよび方法は、暗号化されたストリームのランダム・アクセスおよびリバース再生(reverse play)も可能にする。

【0029】

例示的なスケーラブル暗号化システムの概要

図1は、基本層106、および基本層106に基づく拡張層108から成るスケーラブル・マルチメディア・コンテンツ102に対する例示的なスケーラブル暗号化システム100を示している。システム100は、基本層106を受け取り、少なくとも1つのキーまたは秘密(secret)を使用して、基本層106を、選択的に暗号化された、または完全に暗号化された基本層212に変換する、基本層エンクリプタ(encryptor)104を含む。拡張層108は、元の(すなわち、暗号化されていない)スケーラブル・マルチメディア・コンテンツ102の完全なスケーラビリティを保つために暗号化されない。

40

【0030】

図2は、異なるスキームで、基本層106と拡張層108をともに暗号化する別の例示的なスケーラブル暗号化システム200を示している。例示的なシステム200は、例示的な暗号化エンジン204を有する例示的なマルチメディア・デバイス202を含む。暗号化エンジン204は、拡張層エンクリプタ208と通信するように結合された基本層エ

50

ンクリプタ104を含む。

【0031】

例示的なマルチメディア・デバイス202は、基本層106および少なくとも1つの拡張層108を有するスケーラブル・マルチメディア・コンテンツ102、例えば、スケーラブルMPEG-4FGSビットストリームを受け取り、例示的な暗号化エンジン204を使用してそのマルチメディア・コンテンツ102を暗号化して、スケーラブル暗号化されたマルチメディア・コンテンツ210にする。例示的な暗号化エンジン204は、マルチメディア・コンテンツ102の基本層106と拡張層108をともに受け取り、基本層コンテンツに基づく少なくとも1つのキー、秘密、および／またはその他の情報（例えば、以下に説明する「基本層キー」）を使用して、拡張層108を、選択的に暗号化された
10
拡張層214に変換する。コンテンツ・ベースの基本層キーに加えて、他の情報およびグローバル・キーも暗号化に使用することができる。グローバル・キーは、フレーム全体、セル、ストリーム・セグメント、またはストリームを暗号化するのに使用される任意の情報である。通常、グローバル暗号化解除キーは、ビデオ全体、ムービー等に関するマルチメディア・ストリームの暗号化をロック解除するための暗号化解除秘密を指す。複数のキー、情報、および秘密は、ストリーム暗号キーと呼ぶことが可能であり、あるいは実際に結合されてストリーム暗号キーになることも可能である。

【0032】

本明細書で、FGSビットストリームは、スケーラブル・マルチメディア・コンテンツ102の例として使用する。FGSは、マルチメディア・コンテンツ102を1つの基本
20
層106に分割し、以下の例では、1つの拡張層108に分割する。FGSプロファイルにおいて、FGSビデオ・オブジェクト・プレーン(plane)モード(FGS VOP)は、基本層106を拡張層VOPの予測のための基準ソースとして使用し、FGSテンポラル・ビデオ・オブジェクト・プレーン・モード(FGS temporal video object plane mode; FGST VOP)は、拡張層VOPに関して基本層106からの順方向予測、逆方向予測、または双方向予測を使用することができる。

【0033】

例示的な暗号化エンジン

図3は、図2の例示的な暗号化エンジン204をより詳細に示している。マルチメディア・コンテンツ102から基本層106を受け取る（かつ／または取り出す）基本層エン
30
クリプタ104が、マルチメディア・コンテンツ102から1つまたは複数の拡張層108を受け取る（かつ／または取り出す）拡張層エンクリプタ208と通信するように結合されている。例示的な暗号化エンジン204は、着信するマルチメディア・コンテンツ102に加えて、1つまたは複数のグローバル・キー318、またはその他の暗号化情報を受け取ることができる。

【0034】

基本層エンクリプタ

例示的な暗号化エンジン204の1つの実装では、基本層エンクリプタ104は、図示するとおり、制御論理308と通信するように結合されたコンテンツ・ベースのキー・ジェネレータ302、ストリーム暗号器(cipher)304、および乱数発生器306などの
40
例示的なスケーラブル暗号化を実行するコンポーネントを有する。

【0035】

1つの実装では、この例示的な暗号化エンジン204は、「C&S暗号化」と呼ばれるJakubowskiおよびVenkatesanによる暗号化技術の変形を使用する（参照により本明細書に組み込まれている非特許文献18）。C&S暗号化は、合計を伴う全般的なブロックの連鎖(universal block chaining with sum)、またはチェーン(chain)とサム(sum)のプリミティブ（略してC&S）を表わし、これらは、データを暗号化するため、および認証するために組み合わせて適用される。このプリミティブは、合計するステップに適用される「弱い」CBCタイプの暗号化であり、ビデオ・ストリーム内のデータのブロックを暗号化するためのストリーム暗号器のフロントエンドとして使用さ
50

れる。

【0036】

例示的な暗号化エンジン204によって実行されるにつれ、入力データのシーケンス、例えば、基本層コンテンツ（数百の「機械ワード」から成る、またはそれに類似した）のビデオ・フレームまたはビデオ・セルを表わすマルチメディア・コンテンツ102のセグメントが、CBCタイプのプリミティブによって処理される。プリミティブにおいて、暗号（cipher）が、交互に適用される1対の可逆な汎用ハッシュ関数（invertible hash functions）によって置き換えられる。基本層コンテンツの出力ワードは、合計され、フレーム内またはセル内の最後の「ワード」の次に（next-to-last "word"）に書き込まれる。「pre-MAC」（「MAC」は、メッセージ認証コードの略語である）と呼ばれる最後の2つのワードは、ブロック暗号（cipher）で暗号化される。このpre-MAC値は、黙示的に、基本層コンテンツに関するMAC値であり、拡張層108を暗号化するためのキーのコンテンツ・ベースの部分の役割をすること、ならびに基本層106自体を暗号化するためのコンテンツ・ベースの情報312の役割をすることも可能である。pre-MACは、基本層キー310として使用される場合、ストリーム暗号器304、314の少なくとも1つを同期させるため、ストリーム暗号キー316を生成するため、または基本層暗号器304を使用する擬似ランダム・ワンタイム・パッド（one-time pad）を計算して大量（bulk）の基本層コンテンツの残りの部分を暗号化するために、直接に、または間接的に使用することができる。

10

【0037】

例示的な暗号化エンジン204は、大量のデータを暗号化することができるが、暗号化は、1回だけ（基本層106および拡張層108ごとに）適用するだけでよく、例えば、この暗号化は、FGSスキームにおいて1回限りの圧縮が実行されるのと同時に、適用することができる。例示的なC&S暗号化は、他の暗号化ルーチンと比べて比較的低い複雑性を有するので、暗号化（および暗号化解除）は、比較的高速である。例示的な暗号化エンジン204によって適用される暗号化は、通常、圧縮効率あるいはエラー復元力に対する低下を生じさせない。

20

【0038】

速度を高めるため、基本層暗号104は、基本層キー310、例えば、pre-MACの暗号化に関して、DESの代わりにRC5、AES、または他のブロック暗号を使用することができる。例示的なC&S暗号化は、コンテンツ・ベースのキー・ジェネレータ302が、暗号化されるべきデータの一部を置き換えるキーを生成するので、フレーム内、セル内等でデータ・サイズを増大させない。通常の実装では、基本層キー310は、pre-MACであり、pre-MACは、フレーム、セル、ビデオ等に関するグローバル暗号化キー318とともに、マルチメディア・データの大部分、すなわち、基本層コンテンツからの暗号化セルの残りの部分を暗号化するストリーム暗号器304（通常、RC4などの暗号化アルゴリズムを使用し、かつ／または含む）に送り込まれる。（pre-MACは、前述したとおり、RC5を使用して別個に暗号化して、MACを形成する速度を高める。）MACは、デクリプタ（decrypter）（図示せず）が後に、暗号化を逆操作（リバース）させて、ビット・エラーが無い場合に、元のプレーン・テキストを取り出すことができるように、可逆性を有する。ストリーム暗号キー316は、グローバル暗号化キー318と、暗号化されるべきデータの一部の、1つまたは複数のハッシュ値として理解することができるpre-MACとの両方に依存するので、暗号化セキュリティは非常に強力である。言い換えれば、ごくわずかな違いだけを有する2つの異なるコンテンツは、同じグローバル暗号化キー318を繰り返し使用していても、異なる暗号化テキストに暗号化される。

30

40

【0039】

基本層106は、選択的に、または完全に暗号化することができる。例示する選択的暗号化モードでは、各フレームに関して、例えば、基本層ビットのセットのDC値、すなわち、intra_dc_coefficientおよびdct_dc_difference

50

t i a l、D C T係数の符号ビット、動きベクトルh o r i z o n t a l _ m v _ d a t aおよびv e r t i c a l _ m v _ d a t aの符号ビット、および／または動きベクトル残h o r i z o n t a l _ m v _ r e s i d u a lおよびv e r t i c a l _ m v _ r e s i d u a lが抽出されて、暗号化、例えば、前述した例示的な変更されたC & S暗号化を使用して、暗号化されるべきベクトルが形成される。次に、暗号化テキストが、基本層106内の元のデータに置き換わるように元のフィールドに戻される。例示的な完全暗号化モードでは、V O Pヘッダを除き、基本層106内のエントロピー・コーディングされたビデオ・データが、各フレームに関して、例えば、例示的なC & S暗号化を使用して暗号化される。

【0040】

10

完全暗号化モード、または選択的暗号化モードのいずれでも、基本層暗号化は、マルチメディア・データのエントロピー・コーディングに悪影響を及ぼさないことに留意されたい。例示的なC & S暗号化は、暗号化されるデータのサイズを保つので、例示的な暗号化は、F G S圧縮効率に全く悪影響を与えない。以上に説明した選択的暗号化モードは、完全にM P E G - 4 F G Sに適合するということも注目に値する。

【0041】

以上の例示的な実装では、基本層エンクリプタ104は、暗号化解除を実行するのに先立ってフレーム全体に関して十分なデータを集めることを必要とするアプリケーションまたはデバイスに対して暗号化を実行し続けることが可能である。そのようなアプリケーションまたはデバイスは、基本層フレーム全体をバッファに入れ、それぞれの暗号化されたフィールドに関して位置とビット数を憶えていなければならない、あるいは、基本層フレームのデータを2回（暗号化解除のために1回、展開のために1回）、構文解析しなければならない。例示的なC & S暗号化は、これらのタイプのアプリケーションおよびデバイスの一部に関して妥当でない可能性がある。代替の例示的な実装として、E C B (Electronic Codebook) モード、C B C (Cipher Block Chaining) モード、またはO C B (Offset Codebook) モードなどの様々なモードで使用されるR C 4などのストリーム暗号、またはD E S、A E S、R C 5などのブロック暗号は、完全暗号化モードあるいは選択的暗号化モードの何れかに対して例示的なC & S暗号化と置き換えることができる。

20

【0042】

次に、乱数発生器306は、各フレームに関して異なる乱数を生成することに使用される。乱数は、各基本層フレームのヘッダ内に挿入することができ、そのフレームに関して暗号化されるデータとX O R演算するために各フレーム内で異なるランダム・ビットを生成するストリーム暗号器304への入力として、またはフレームに関して暗号化されるデータを暗号化するためのブロック暗号化への入力として、グローバル暗号化キー318と結合することができる。通常の長さのビデオの場合、32ビットの乱数は、ビデオ内のすべてのフレームに関する十分な容量を提供するはずであり、そうである場合、圧縮効率に影響を与えるオーバーヘッドは、1基本層フレーム当たり32ビットである。32ビットの乱数により、實際上、各ビデオ・フレームを暗号化する繰り返しのないランダムなシーケンスが確実になる（良好な品質の乱数発生器が使用される場合、確率の非常に小さい乱数の衝突が生じない限り）。R C 4は、膨大な数の可能な状態を有するので、R C 4を例示的なC & S暗号化の代わりに使用することにより、暗号化されたコンテンツのセキュリティを確実にすることができる。また、挿入された乱数も、次に説明する拡張層108の暗号化において基本層キー310として（例えば、p r e - M A Cの代わりに）使用される。

30

40

【0043】

拡張層エンクリプタ

図1に示すとおり、最も単純な例示的な実装は、拡張層を暗号化しないでおくことである。拡張層108は、基準としての基本層106からのビデオ・オブジェクト・プレーン（V O P）から予測されるか、または導出されるので、一部のアプリケーションにおいてマルチメディア・コンテンツ102全体を保護するのに、基本層106を保護するだけで

50

十分である。この例示的な実装では、暗号化された基本層 2 1 2、および暗号化されていない基本層 1 0 6 から予測された、または導出された暗号化されていない拡張層 1 0 8 を含む「暗号化された」マルチメディア・ストリーム 1 1 0 が生成される。

【0044】

それぞれの個々の VOP の観点からは、そのような例示的な実装は、非常にセキュアであるように思える。暗号化解除キーなしでは、暗号化された基本層 2 1 2 と暗号化されていない拡張層 1 0 8 の両方から再構成されたフレームは、全く有用な情報を含まない。しかし、VOP から成るビデオの全体的な観点からは、異なる結論が明白である。

【0045】

QCIF ビデオが、およそ每秒 1.0 Mb の総ビットレートで、低いビットレート（およそ每秒 50 Kb）の基本層 1 0 6 と拡張層 1 0 8 に圧縮され、基本層 1 0 6 からのピクセル値がゼロ（または別の固定の値）に設定され、再構成された FGS ビデオが再生された場合、以下の観察がなされる可能性がある。まず、それぞれの個々の再構成されたフレームが検査された場合、各フレームは、非常にランダムであり、有用な情報をあまり抽出することができない。再構成されたビデオが再生された場合、動くオブジェクトの輪郭は容易に可視可能である。より重要なこととして、そのような動くオブジェクト、およびオブジェクトの動きが、人間の目によって正しく、意味ある形で観察される。多くのアプリケーションにおいて、ビデオ暗号化から漏れるそのようなビデオ情報は、許容できない可能性がある。この現象は、おそらく、ビデオ内の隣接するフレーム間の強い相関によって説明される。基本層 1 0 6 内の基準フレームが強く相関している場合、一続きの拡張層フレームにより、基本層エンクリプタ 1 0 4 が意図するよりもはるかに多くの情報が明かされる。したがって、基本層 1 0 6 の暗号化だけでは、多くのアプリケーションに対して多くのタイプのスケラブル・マルチメディア・コンテンツ 1 0 2 を暗号化するのに十分でない可能性がある。

【0046】

図 3 を参照すると、例示的な暗号化エンジン 2 0 4 の中に含まれる代替の例示的な拡張層エンクリプタ 2 0 8 が、ランダム・ビット・エンジン 3 2 0 の中に含まれる前述した拡張層暗号器 3 1 4 を含む。また、例示的な拡張層エンクリプタ 2 0 8 は、フレーム・マネージャ 3 2 2、フレーム・バッファ 3 2 4、フレーム・ビットマスク・バッファ 3 2 6、フレーム & ビットマスク・コンバイナ（combiner）3 2 8、および再同期情報マネージャ、または「s y n c h マネージャ」3 3 0 も含み、以上すべては、図示するとおり、制御論理 3 3 2 と通信するように結合されている。フレーム・マネージャ 3 2 2 は、VOP マネージャ 3 3 4 およびフレーム・カウンタ 3 3 6 をさらに含むことが可能である。ランダム・ビット・エンジン 3 2 0 は、シード（seed）マネージャ 3 3 8 を含む。例示的な拡張層エンクリプタ 2 0 8 は、追加のコンポーネント、または図示した例よりも少ないコンポーネントを含むことも可能である。次に、例示的な拡張層エンクリプタ 2 0 8 の機能の簡単な概要を提示し、続いて、より詳細な説明を提示する。

【0047】

簡単に述べると、例示的な拡張層エンクリプタ 2 0 8 は、1 つの実装において、拡張層 1 0 8 内の DCT 係数の符号ビットをランダムなビット・シーケンスまたは擬似ランダムなビット・シーケンスと XOR 演算することにより、拡張層 1 0 8 を選択的に暗号化する。マルチメディア・ストリームの各フレームは、異なるフレームに同じランダム・シーケンスを適用して暗号化のセキュリティに脆弱性を生じさせることを回避するために、異なるランダム・ビット・シーケンスを使用する。MP EG-4 FGS T の実装の場合、動きベクトルも、DCT 係数と同様のやり方で暗号化される。次に、例示的な拡張層エンクリプタ 2 0 8 の動作をより詳細に説明する。

【0048】

拡張層 1 0 8 の例示的なスケラブル暗号化は、前述した基本層 1 0 6 の暗号化によって相当に容易になる。p r e-MAC などの基本層キー 3 1 0 が、基本層エンクリプタ 1 0 4 から拡張層エンクリプタ 2 0 8 に通信され、グローバル暗号化キー 3 1 8 とともにラ

10

20

30

40

50

ンダム・ビット・エンジン 320 に送り込まれる。(複数の基本層フレームに基づく F G S T V O P のケースでは、各基本層フレームからの基本層キー 310 を、グローバル暗号化キー 318 とともにランダム・ビット・エンジン 320 に送り込むことが可能である。)ランダム・ビット・エンジン 320 内部の、かつ/またはランダム・ビット・エンジン 320 に関連する拡張層暗号 314 は、R C 4 などの技術を使用して、拡張層 108 内の D C T 係数の符号ビットと X O R 演算されるランダム・ビット・シーケンスを生成する。ランダムなビット・シーケンスまたは擬似ランダムなビット・シーケンスと拡張層 108 内の D C T 係数との X O R 演算を実行することの詳細を以下により十分に説明する。

【0049】

ランダム・ビット・エンジン 320 内のシード・マネージャ 338 により、拡張層 108 のフレームを暗号化するためにランダム・ビット・エンジン 320 によって生成されたのと同じビット・シーケンスが、基本層 106 の選択的暗号化において基本層 106 の対応するフレームを暗号化するためにも使用されることがないことが確実にされる。ビット・シーケンスは、擬似ランダムとすることが可能であり、したがって、繰り返し可能であり、複数のフレームに対する同じビット・シーケンスの適用により、セキュリティが危うくなる。ランダム・ビット・エンジン 320 は、シード・マネージャ 338 を使用して、暗号化を危うくする擬似ランダム・シーケンスの繰り返しを防止する。これを達成することができる 1 つのやり方は、固定のストリング、多くの場合に拡張層の一部である固定のストリングを、シーケンスをランダムにするシードとして拡張層暗号器 314 に送り込むことによる方法である。

【0050】

ランダム・ビット・エンジン 320 によって(例えば、そこに含まれる拡張層暗号器 314 によって)生成されたランダム・ビットは、フレーム・マネージャ 322 によって特定された操作中の (operative) ビデオ・フレーム内の関連するビット配列に対応するアレイまたは 2 値マトリックスに編成される。このアレイまたは 2 値マトリックスは「フレーム・ビットマスク」または「ビットマスク」と呼ばれることがある。1 つの実装では、フレーム・ビットマスク・バッファ 326 が、ランダムに生成されたビットから構成されるフレーム・ビットマスクを保持する間、フレーム・バッファ 324 は、拡張層 108 のフレームを保持することに使用できる。フレーム & ビットマスク・コンバイナ 328 は、拡張層フレーム内の D C T 係数符号ビットをフレーム・ビットマスク内の対応するランダム・ビットと X O R 演算する。言い換えれば、拡張層 108 内の D C T 係数の符号ビットは、拡張層 108 内に出現した場合、フレーム・ビットマスク内の同じ位置のランダム・ビットと X O R 演算される。フレーム & ビットマスク・コンバイナ 328 によって生成されたスケーラブル暗号化された拡張層 214 の伝送中にパケット損失が生じている場合、受信パケットは、パケットを失っているにも関わらず、暗号化解除のための正しいランダム・ビットに容易に再編成することができる。

【0051】

テンポラル・拡張フレーム内のすべての D C T 係数に関してビット・プレーン・コーディングを使用することも可能であり、これは、F G S T テンポラル・スケーラビリティ (F G S T temporal scalability; F G S T) と呼ばれる。F G S V O P および F G S T V O P は、単一の拡張層か、または 2 つの別々の拡張層に編成することができる。各 F G S T V O P は、例えば、基本層からの順方向予測、逆方向予測、または双方向予測を使用してコーディングすることができる。再同期用マーカーが s y n c h マネージャ 330 によって F G S ストリームの中に挿入されて、ビット・エラーまたはパケット損失が生じた場合にエラー伝搬を抑えることが可能である。また、エラー復元力の目的で、拡張層内でビット・プレーン区切り f g s _ b p _ s t a r t _ c o d e を再同期マーカーとして使用することも可能である。

【0052】

F G S T V O P の例示的なスケーラブル暗号化の場合、動きベクトルが暗号化されたビットのセットに追加される。この例示的な暗号化は、基本層の選択的暗号化に関して前

10

20

30

40

50

述したのと同様である。動きベクトルのビットは、DCT符号ビットと同じやり方で拡張層暗号器314を使用して暗号化される。

【0053】

図4に示すとおり、ヘッダ406、408をそれぞれ有する複数のFGST VOP 402、404が、同じ基本層フレーム410を自らの基本VOP 412のソースとして使用する可能性がある。前述したランダム・ビット・エンジン320が、同じ基本層フレーム410に基づき、異なるFGST VOPに対して同じランダム・ビットを生成するようなことがあれば、セキュリティが危うくなることが生じる。VOPマネージャ334が、フレーム・カウンタ336によって生成されたフレーム・カウント416、418をFGST VOPヘッダ406、408に挿入する。このフレーム・カウント416、418が拡張層暗号器314に（例えば、RC4を使用して）送られ、同じ基本層フレーム410に基づくFGST VOP 402、404のそれぞれに関して異なるランダム・ビットが生成されるようにする。異なる基本フレームに対して、他の情報が拡張層暗号器314に送られ、重複（duplication）を防止するので、異なる基本層フレームに基づく異なるグループのFGST VOPに関して、同じフレーム・カウント・シーケンスを再使用すること、または再スタートすることができる。つまり、基本層キー310は、各基本層フレーム410に対して異なっている。ほとんどのアプリケーションにおいてフレーム・カウンタ336が効果的に動作するのに、1つのFGST拡張層フレーム当たり2ビットまたは3ビットのオーバーヘッドで十分である。暗号化されたマルチメディア・コンテンツ210の伝送中に中間ステージ内で実行されるいくつかのプロセスにより、タイム・スタンプが変更される可能性があるので、VOPマネージャ334によって挿入されるフレーム・カウント416、418は、タイム・スタンプよりも効果的である。また、FGST VOP 402、404の一部を含むパケットが伝送中にドロップされた場合、暗号化解除エンティティが受信されたFGST VOP 402、404の暗号化解除のために正しいランダム・ビットを生成することが、フレーム・カウント416、418により可能になる。

【0054】

例示的な拡張層エンクリプタ208は、元の暗号化されていない拡張層108のエラー復元力を保ち、FGS圧縮によって提供されるすべてのスケーラブルな拡張層操作を可能にする。

【0055】

例示的な暗号化エンジン204の一部の実装では、基本層暗号器304と拡張層暗号器314は、同一のモジュールまたはルーチンとすることが可能である。図示した実装では、暗号プロセスが基本層106と拡張層108の両方の暗号化に関連して行われることを強調するため、基本層暗号器304と拡張層暗号器314を別々のエンティティとして示している。

【0056】

例示的な方法

図5は、例示的なスケーラブル暗号化方法500を示している。この例示的なスケーラブル暗号化方法500は、図2および3に示した例示的な暗号化エンジン204のようなデバイスによって実行されることが可能である。この流れ図では、動作が個々のブロック内に要約されている。動作は、プロセッサによって実行されることが可能なハードウェアおよび／またはマシン可読命令（ソフトウェアまたはファームウェア）で実行されることが可能である。

【0057】

ブロック502で、スケーラブル・マルチメディア・ストリームの基本層フレームが暗号化される。

【0058】

ブロック504で、スケーラブル・マルチメディア・ストリームの拡張層が、基本層内のコンテンツの少なくとも一部に基づくキーを使用して暗号化される。

【0059】

図6は、別の例示的なスケーラブル暗号化方法600を示している。この例示的なスケーラブル暗号化方法600は、図2および3に示した例示的な暗号化エンジン204のようなデバイスによって実行されることが可能である。この流れ図では、動作が個々のブロック内に要約されている。この動作は、ハードウェアおよび／またはプロセッサによって実行されることが可能なマシン可読命令（ソフトウェアまたはファームウェア）で実行されることが可能である。

【0060】

ブロック602で、第1のキーを使用してスケーラブル・マルチメディア・ストリームの基本層が暗号化される。

10

【0061】

ブロック604で、ランダムなビット・シーケンスまたは擬似ランダムなビット・シーケンスが、基本層コンテンツの一部から少なくとも部分的に導出された第1のキーおよび第2のキーを使用して生成される。第1のキーは、通常、暗号化されているマルチメディア・ストリーム全体に関するグローバル・キーであり、第2のキーは、通常、現在のフレームの拡張層、または現在のフレームの基本層を基準とするFGST VOPだけを暗号化するための基本層キーである。

【0062】

ブロック606で、拡張層内のDCT係数の符号ビットが、ランダム・ビット・シーケンスからのビットとXOR演算される。

20

【0063】

例示的な暗号化のセキュリティ

視覚効果もシステムセキュリティもともに、マルチメディア暗号化方法によって付与されるセキュリティにおける要因である。視覚効果は、暗号化されたマルチメディア・ストリームからユーザがどれだけの有用な情報を導出することができるかに関わる。システムセキュリティは、受動的攻撃および能動的攻撃に対して暗号化されたストリームが示す抵抗力の量に関わる。

【0064】

セキュリティに関して、テキスト暗号化とは異なり、マルチメディア暗号化は、攻撃者が利用することができる強い相関をプレーン・テキスト・ビデオ内に含む可能性がある。テキスト暗号化における攻撃の成功は、普通、テキスト全体の一部またはすべてが完全に逆操作（リバース）されることを必要とするのに対して、マルチメディア暗号化における攻撃は、暗号化の部分的な、またはおおよその逆操作（リバース）が成功することしか必要としない可能性がある。言い換えれば、暗号化されたビデオにおいて、ビデオ・フレーム内、およびビデオ・フレーム間のデータのすべての部分が重要（relevant）であるのではなく、したがって、元のビデオのおおよその回復により、暗号化されたストリームから相当な量の情報がもたらされる可能性がある。様々なアプリケーションは、セキュリティ障害に関して異なる基準を有する。

30

【0065】

前述した例示的な完全な暗号化とは異なり、前述した基本層106に関する例示的な選択的暗号化は、暗号化されたマルチメディア・コンテンツ210内にいくらかの見える構造を残す。人間の目は、静止部分と動く部分の間の違いを見分けることができる。他方、前述した例示的な完全な暗号化方法は、ほとんどすべての視覚的に識別することができる構造を暗号化されたマルチメディア・コンテンツ210から削除する。完全に暗号化された基本層212、および選択的に暗号化された拡張層214を含む例示的な完全に暗号化されたマルチメディア・コンテンツ210は、暗号化解除されない限り、視覚的にランダムに見え、役立たない。

40

【0066】

例示的なスケーラブル完全暗号化モードと例示的なスケーラブル選択的暗号化モードとともに、コンテンツ依存入力（例えば、基本層キー310）が基本層暗号器304および

50

／または拡張層暗号器 3 1 4 に送り込まれるために各フレームの暗号化が異なるという理由で、既知のプレーン・テキスト攻撃に対して堅牢である。他のタイプの攻撃に対する堅牢性は、選択的暗号化モードと完全暗号化モードでは異なる。例示的なスケーラブル完全暗号化モードの場合、セキュリティの量は、暗号化のために基本層暗号器 3 0 4 内で使用される潜在的なアルゴリズムに依存する。例示的な C & S 技術が使用される場合、この技術が、セキュアな暗号化を提供する。他方、例示的なスケーラブル選択的暗号化モードは、使用される状態の数が限られていることに起因して、それほどセキュアでない可能性がある。

【0067】

暗号化のために選択されたビットが、実現されるセキュリティの量に影響を与える可能性がある。例えば、DC 係数の暗号化だけでは、依然として視覚的に識別可能な、暗号化されたフレームの端部が残される。AC 係数に関する符号ビットの暗号化は、ゼロでない AC 係数に対してだけ実行することができる。動きベクトルの場合、フレームに関する動きベクトルの数は限られているので、それらの符号ビットに対する暗号化は、総当たり攻撃 (brute force attack) を受けた状態では、あまりセキュアでない。動きベクトルの残余に対する暗号化も、動きベクトルの剰余に関して使用されるビットの数が、普通、非常に少ないので (例えば、1 フレーム当たり 2 ビット)、あまりセキュリティを強化することにならない。すなわち、動きベクトルの剰余が正しくレンダリングされても、誤ってレンダリングされても、多くの変化、または知覚的破損が生じさせない。

【0068】

一部の実装では、例示的な選択的暗号化は、MPEG-4 FGS などの一部のスケーラブル・スキームとの完全な適合性 (compatibility) を提供するが、軽量のセキュリティしか提供しない。ただし、多くのマルチメディア・ストリーム 102 は、レンダリングされたビデオが、普通、低い情報価値しか有さないエンターテインメントアプリケーションにおける使用に向けられているので、例示的な選択的暗号化は、ビデオのコピーを正当に購入するよりもビデオを暗号化解除することの方が攻撃者に高くつくようにしながら、早さとスケーラビリティを提供する。したがって、例示的な選択的暗号化は、多くのアプリケーションに関して実行可能なソリューション (viable solution) である。

【0069】

実験結果

例示的な暗号化エンジン 204 の少なくとも一部を pure C++ コードで実装した。試験は、512 メガ・バイトのメモリを有する PENTIUM (登録商標) III の 667 メガヘルツの DELL (登録商標) PC 上で例示的な暗号化エンジン 204 を使用して実行した。(PENTIUM (登録商標) III は、カリフォルニア州サンタクララの INTEL (登録商標) コーポレーションの商標である。)(テキサス州、オースティン市、DELL (登録商標) コンピュータ・コーポレーション)。

【0070】

図 7 は、例示的なスケーラブル暗号化の前と後のスケーラブル・マルチメディア・ストリームの視覚的レンダリング 700 を示している。オリジナルのビデオ・イメージ 702、702' のフレームは、例示的な暗号化エンジン 204 による処理の前のマルチメディア・コンテンツ 102 を示している。選択的に暗号化されたビデオ・イメージ 704、704' は、例示的な選択的暗号化の後の、ただし、暗号化解除前の暗号化されたマルチメディア・コンテンツ 210 を示している。選択的に暗号化されたビデオ・イメージ 704、704' は、いくつかの認識可能なビデオ・オブジェクト 706 を含むが、実際の鑑賞目的に対しては、明瞭で理解可能な楽しめる鑑賞を求めるには、あまりにもスクランブルがかかっている。完全に暗号化されたビデオ・イメージ 708、708' は、例示的な完全暗号化後の、ただし、暗号化解除前の暗号化されたマルチメディア・コンテンツ 210 を示している。完全に暗号化されたビデオ・イメージ 708、708' は、視野全体に散らばったランダムな形状およびパターンとして現れ、実際の鑑賞目的では役に立たない。この場合も、暗号化されたマルチメディア・コンテンツ 210 は、例示的なスケーラ

ブル完全暗号化で暗号化されているか、例示的なスケーラブル選択的暗号化で暗号化されているかに関わらず、前述したとおり、MPEG-4 FGSの完全な機能、およびFGSTスケーラビリティの特徴を保持する。

【0071】

結論

以上、スケーラブル・マルチメディアの完全にスケーラブルな暗号化のための例示的な暗号化エンジン、および関連する方法を説明した。前述した本発明は、ハードウェアで、ソフトウェアで、またはハードウェアとソフトウェア両方で実装することができる。ある実装では、例示的な暗号化エンジン、および関連する方法は、コンピュータによって実行される、プログラム・モジュールなどのコンピュータ実行可能命令の一般的な文脈において説明することができる。一般に、プログラム・モジュールには、特定のタスクを実行する、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造等が含まれる。また、本発明は、通信ネットワークを介してリンクされた遠隔の処理デバイスによってタスクがワイヤレス通信を介して実行される分散通信環境において実施することも可能である。ワイヤレス・ネットワークでは、プログラム・モジュールは、メモリ記憶装置を含むローカルの通信デバイス記憶メディアと遠隔の通信デバイス記憶メディアの両方の中に配置されることが可能である。

10

【図面の簡単な説明】

【0072】

【図1】基本層だけを暗号化する例示的なスケーラブル暗号化を示すブロック図である。

20

【図2】基本層と拡張層とともに暗号化する例示的なスケーラブル暗号化システムを示すブロック図である。

【図3】例示的なスケーラブル暗号化エンジンを示すブロック図である。

【図4】図3の例示的なスケーラブル暗号化エンジンの例示的なビデオ・オブジェクト・プレーン・マネージャを示すブロック図である。

【図5】例示的なスケーラブル暗号化方法を示す流れ図である。

【図6】別の例示的なスケーラブル暗号化方法を示す流れ図である。

【図7】例示的なスケーラブル完全暗号化および例示的なスケーラブル選択的暗号化を示す1組のビデオ・イメージである。

30

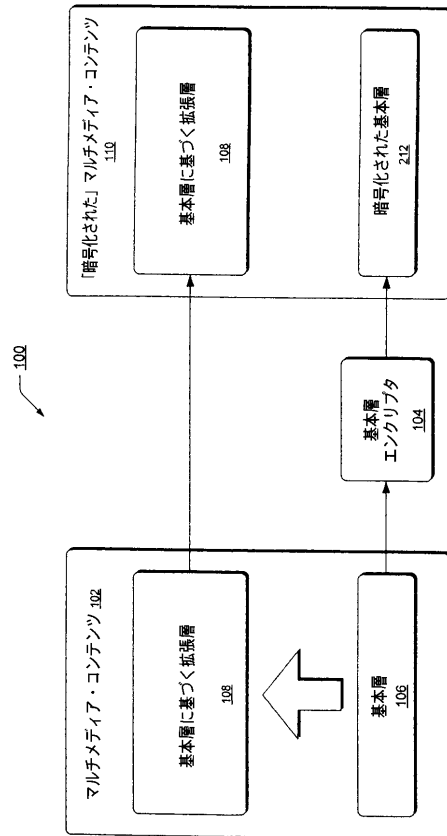
【符号の説明】

【0073】

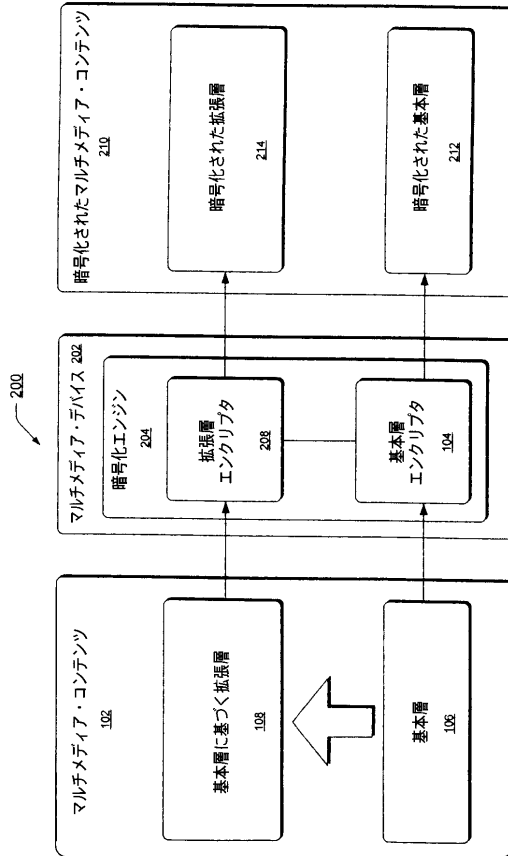
- 102 マルチメディア・コンテンツ
- 104 基本層エンクリプタ
- 106 基本層
- 108 拡張層
- 200 暗号化解除システム
- 202 マルチメディア・デバイス
- 204 暗号化エンジン
- 208 拡張層エンクリプタ
- 210 暗号化されたマルチメディア・コンテンツ
- 212 暗号化された基本層
- 214 暗号化された拡張層

40

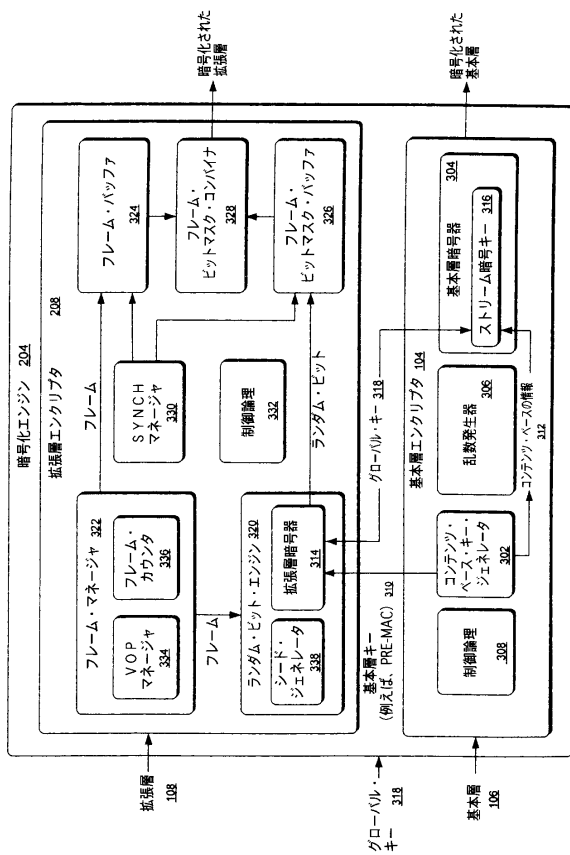
【図 1】



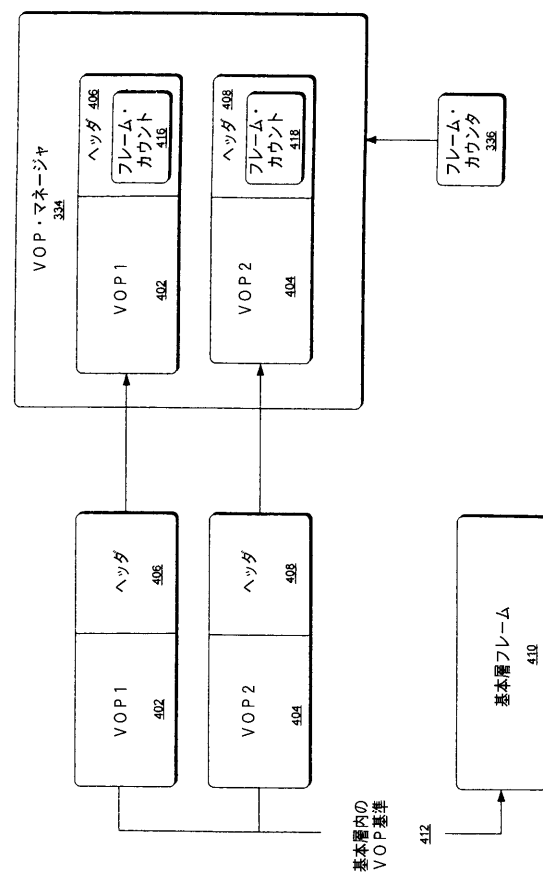
【図 2】



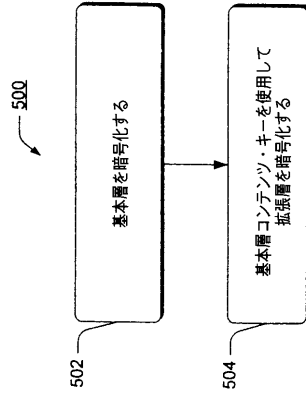
【図 3】



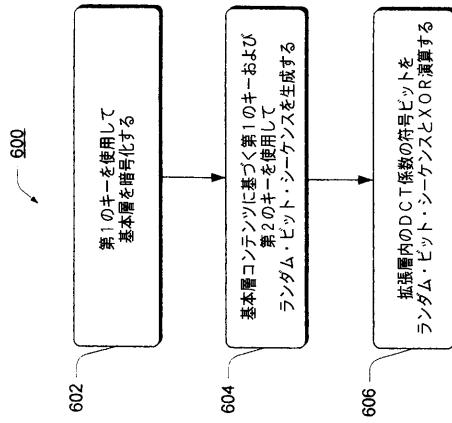
【図 4】



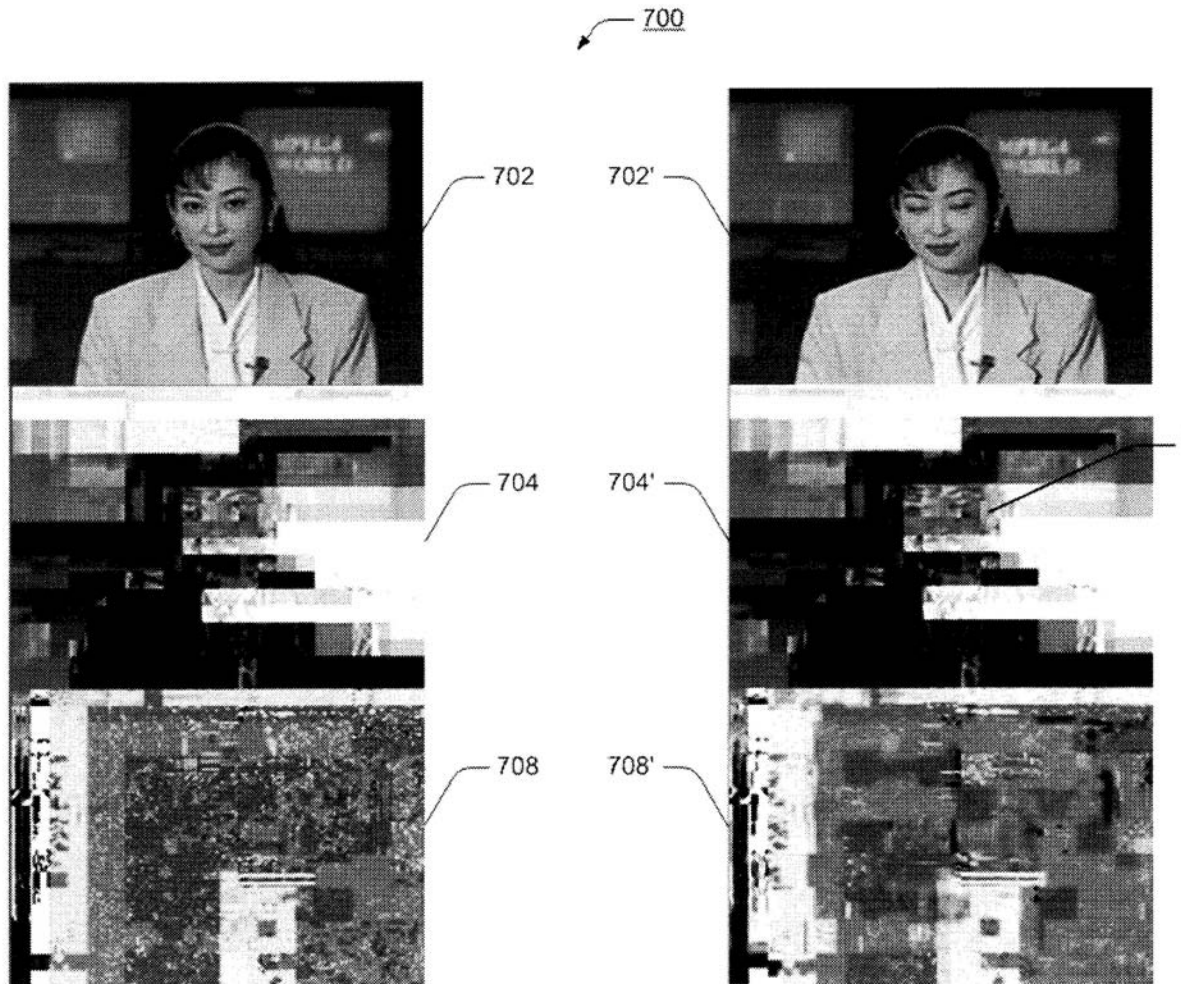
【図 5】



【図 6】



【図 7】



フロントページの続き

- (72)発明者 ユアン チュン
中華人民共和国 100084 ペキン シンファ ユニバーシティ コンピュータ デパートメ
ント (番地なし)
- (72)発明者 ワン イドン
中華人民共和国 100080 ペキン ペキン ユニバーシティ 46 ナンバー2117
- (72)発明者 リ シペン
アメリカ合衆国 92618 カリフォルニア州 アービン オーク グレン 628

審査官 川崎 優

- (56)参考文献 米国特許出願公開第2003/0021296 (US, A1)

(58)調査した分野(Int.Cl., DB名)

H04N 7/16-173、7/24, 26-50
H04L 9/00-36
G06F 21/22-24