

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6608436号
(P6608436)

(45) 発行日 令和1年11月20日(2019.11.20)

(24) 登録日 令和1年11月1日(2019.11.1)

(51) Int.Cl.		F I			
H03M	7/30	(2006.01)	H03M	7/30	Z
G09C	1/00	(2006.01)	G09C	1/00	660D

請求項の数 18 (全 34 頁)

(21) 出願番号	特願2017-515203 (P2017-515203)	(73) 特許権者	513156386
(86) (22) 出願日	平成27年9月21日 (2015. 9. 21)		グルロジック マイクロシステムズ オーワイ
(65) 公表番号	特表2017-535123 (P2017-535123A)		Gurulogic Microsystems Oy
(43) 公表日	平成29年11月24日 (2017. 11. 24)		フィンランド共和国 20100 トゥルク リンナンカツ 34
(86) 国際出願番号	PCT/EP2015/025065		Linnankatu 34 20100
(87) 国際公開番号	W02016/041641		Turku FINLAND
(87) 国際公開日	平成28年3月24日 (2016. 3. 24)	(74) 代理人	110002837
審査請求日	平成29年6月21日 (2017. 6. 21)		特許業務法人アスフィ国際特許事務所
(31) 優先権主張番号	1416631.8	(72) 発明者	カルツカイネン, トゥオマス
(32) 優先日	平成26年9月19日 (2014. 9. 19)		フィンランド共和国, 20320, トゥルク, ラウタランカツ 2 ビー17
(33) 優先権主張国・地域又は機関	英国 (GB)		
早期審査対象出願			
前置審査			最終頁に続く

(54) 【発明の名称】 エンコーダ、デコーダ、及び部分的データ暗号化を用いる方法

【特許請求の範囲】

【請求項 1】

対応する符号化され暗号化されたデータ (E 2) を生成するために入力データ (D 1) を符号化し暗号化するエンコーダ (110) であって、該エンコーダ (110) は前記入力データ (D 1) を処理するためのデータ処理部を含む：

(a) 前記データ処理部は、入力データ (D 1) を符号化して複数の中間符号化データストリームを生成するように構成されており、

前記複数の中間符号化データストリームは、少なくとも1つのクリティカルデータストリームと該クリティカルデータストリームとは異なる1つ以上の非クリティカルデータストリームを含んでおり、前記クリティカルデータストリームは、前記非クリティカルデータストリームを後に復号化するために用いられるものであり、

前記少なくとも1つのクリティカルデータストリームは、前記複数の中間符号化データストリームの一部のみを構成するものであり、

(b) 前記データ処理部は、1つ以上の暗号化アルゴリズムを使用して前記少なくとも1つのクリティカルデータストリームを暗号化することにより少なくとも1つの中間暗号化データストリームを生成するように構成されており、

前記データ処理部は、前記少なくとも1つのクリティカルデータストリームを暗号化する前に、前記少なくとも1つのクリティカルデータストリームを少なくとも1つの圧縮データストリームに圧縮するように構成されており、

(c) 前記データ処理部は、前記符号化され暗号化されたデータ (E 2) に含まれるよ

うにするために前記非クリティカルデータストリームを1つ以上の圧縮データストリームに圧縮するように構成されており、

(d) 前記データ処理部は、前記複数の中間符号化データストリームのうち暗号化されていない部分を前記少なくとも1つの中間暗号化データストリームと併合して前記符号化され暗号化されたデータ(E2)を生成するように構成されており、

(e) 前記少なくとも1つのクリティカルデータストリームが下記(i)～(v)の少なくとも一つを示す情報を含んでいるエンコーダ(110)。

(i) 前記入力データ(D1)を複数のデータブロック及びデータパケットの少なくとも一方に分割及び結合の少なくとも一方をするように構成されている複数の分割及び結合の少なくとも一方の動作。

(ii) 複数のデータブロック及びデータパケットの少なくとも一方の情報を符号化するのに用いられる1つ以上の符号化方法。

(iii) 複数のデータブロック及びデータパケットの少なくとも一方を複数のエントロピー符号化されたデータブロック及びデータパケットの少なくとも一方にエントロピー符号化するのに用いられる1つ以上のエントロピー符号化方法。

(iv) エントロピー符号化されたデータストリームのうち複数のエントロピー符号化されたデータブロック及びデータパケットの少なくとも一方の長さ。

(v) エントロピー符号化前の複数のデータブロック及びデータパケットの少なくとも一方の長さ。

【請求項2】

前記データ処理部は、前記複数のデータブロック及びデータパケットの少なくとも一方に対して統計的分析及び反復分析の少なくとも一方を実行して、それぞれのデータブロック及びデータパケットの少なくとも一方内の統計的変動を示す複数のパラメータを決定するように構成されており、

前記データ処理部は、前記複数のパラメータを使用して、前記複数の中間符号化データストリームを生成するために前記複数のデータブロック及びデータパケットの少なくとも一方の情報を符号化するために使用される前記1つ以上の符号化方法を選択するように構成されている請求項1に記載のエンコーダ(110)。

【請求項3】

前記データ処理部は、1次元データ、多次元データ、テキストデータ、バイナリデータ、センサデータ、オーディオデータ、画像データ、ビデオデータ、符号化データの少なくとも1つの形態で提供される前記入力データ(D1)を処理するように構成されている請求項1に記載のエンコーダ(110)。

【請求項4】

前記少なくとも一つの圧縮データストリームの第1バイトが前記少なくとも1つのクリティカルデータストリームを圧縮するのに用いられるエントロピー符号化方法を記述するように、前記データ処理部が前記第一バイトを計算するよう構成されている請求項1に記載のエンコーダ(110)。

【請求項5】

前記データ処理部が、暗号化されたデータストリームの先頭に書き込まれる新しいバイト、エントロピー符号化方法のバイト及びワードのうち少なくとも一方における最上位ビット、非暗号化データストリームと暗号化データストリームが前記符号化され暗号化されたデータ(E2)に含まれる順序、フラグビット、のうち少なくとも一つを用いることで暗号化を定義するように構成されている請求項1に記載のエンコーダ(110)。

【請求項6】

エンコーダ(110)によって、対応する符号化され暗号化されたデータ(E2)を生成する、入力データ(D1)を符号化及び暗号化する方法であって、前記エンコーダ(110)は前記入力データ(D1)を処理するためのデータ処理部を含むものであり、該方法は前記データ処理部による以下のステップを含む：

(a) 前記入力データ(D1)を符号化して複数の中間符号化データストリームを生成

するステップ、

但し、前記複数の中間符号化データストリームは、少なくとも1つのクリティカルデータストリームと該クリティカルデータストリームとは異なる1つ以上の非クリティカルデータストリームを含んでおり、前記クリティカルデータストリームは、前記非クリティカルデータストリームを後に復号化するために用いられるものであり、

前記少なくとも1つのクリティカルデータストリームは、前記複数の中間符号化データストリームの一部のみを構成するものである。

(b) 1つ以上の暗号化アルゴリズムを使用して前記少なくとも1つのクリティカルデータストリームを暗号化することにより少なくとも1つの中間暗号化データストリームを生成するステップ、

但し、前記データ処理部は、前記少なくとも1つのクリティカルデータストリームを暗号化する前に、前記少なくとも1つのクリティカルデータストリームを少なくとも1つの圧縮データストリームに圧縮するように構成されている。

(c) 前記符号化され暗号化されたデータ(E2)に含めるために前記非クリティカルデータストリームを1つ以上の圧縮データストリームに圧縮するステップ、

(d) 前記複数の中間符号化データストリームのうち暗号化されていない部分を前記少なくとも1つの中間暗号化データストリームと併合して前記符号化され暗号化されたデータ(E2)を生成するステップ。

(e) さらに該方法は、前記少なくとも1つのクリティカルデータストリームが下記(i)～(v)の少なくとも一つを示す情報を含んでいる。

(i) 前記入力データ(D1)を複数のデータブロック及びデータパケットの少なくとも一方に分割及び結合の少なくとも一方をするように構成されている複数の分割及び結合の少なくとも一方の動作。

(ii) 複数のデータブロック及びデータパケットの少なくとも一方の情報を符号化するのに用いられる1つ以上の符号化手法。

(iii) 複数のデータブロック及びデータパケットの少なくとも一方を複数のエントロピー符号化されたデータブロック及びデータパケットの少なくとも一方にエントロピー符号化するのに用いられる1つ以上のエントロピー符号化方法。

(iv) エントロピー符号化されたデータストリームのうち複数のエントロピー符号化されたデータブロック及びデータパケットの少なくとも一方の長さ。

(v) エントロピー符号化前の複数のデータブロック及びデータパケットの少なくとも一方の長さ。

【請求項7】

前記複数のデータブロック及びデータパケットの少なくとも一方に対して統計的分析及び反復分析の少なくとも一方を実行して、それぞれのデータブロック及びデータパケットの少なくとも一方内の統計的変動を示す複数のパラメータを決定するように前記データ処理部を動作させることと；

複数のパラメータを使用して前記複数のデータブロック及びデータパケットの少なくとも一方の情報を符号化して前記複数の中間符号化データストリームを生成するために使用される前記1つ以上の符号化方法を選択するように前記データ処理部を動作させることと；を備える請求項6に記載の方法。

【請求項8】

前記データ処理部を動作させて、1次元データ、多次元データ、テキストデータ、バイナリデータ、センサデータ、オーディオデータ、画像データ、ビデオデータ、符号化されたデータのうち少なくとも1つの形態で提供される前記入力データ(D1)を処理することを含む請求項6に記載の方法。

【請求項9】

前記データ処理部を動作させて、前記少なくとも一つの圧縮データストリームの第1バイトを、前記第1バイトが前記少なくとも1つのクリティカルデータストリームを圧縮するために使用されるエントロピー符号化方法を記述するように計算することを含む請求項

6 に記載の方法。

【請求項 10】

前記データ処理部を動作させて、暗号化データストリームの先頭に書き込まれる新しいバイト、エントロピー符号化方法のバイト及びワードの少なくとも一方における最上位ビット、非暗号化データストリームと暗号化データストリームが前記符号化され暗号化されたデータ (E 2) に含まれる順序、フラグビット、のうち少なくとも 1 つを用いることで暗号化を定義することを含む請求項 6 に記載の方法。

【請求項 11】

符号化され暗号化されたデータ (E 2) を解読及び復号して対応する解読化され復号化されたデータ (D 3) を生成するデコーダ (120) であって、該デコーダ (120) は前記符号化され暗号化されたデータ (E 2) を処理するためのデータ処理部を含む：

(i) 前記データ処理部は、前記符号化され暗号化されたデータ (E 2) を処理して、暗号化データストリームの先頭に書き込まれる新しいバイト、エントロピー符号化方法のバイト及びワードの少なくとも一方における最上位ビット、非暗号化データストリームと暗号化データストリームが前記符号化され暗号化されたデータ (E 2) に含まれる順序、フラグビット、のうち少なくとも 1 つを用いることでそのうち 1 つ以上の暗号化されたサブ部分及び 1 つ以上の暗号化されていないサブ部分を決定し、前記符号化され暗号化されたデータ (E 2) の前記 1 つ以上の暗号化されていないサブ部分は、複数のデータブロック及びデータパケットの少なくとも一方の符号化された情報を含み；

(i i) 前記データ処理部は、(a) サイズ、(b) 相対位置、及び (c) 前記複数のデータブロック及びデータパケットの少なくとも一方に関連する 1 つ以上の符号化方法、のうち少なくとも 1 つを決定するために、前記 1 つ以上の暗号化されたサブ部分を解読し解凍するように構成されており、前記 1 つ以上の暗号化されたサブ部分が少なくとも 1 つの圧縮データストリームの形式で提供されるものであり；

(i i i) 前記データ処理部は、前記複数のデータブロック及びデータパケットの少なくとも一方の符号化された情報を復号して複数の復号化されたデータブロック及びデータパケットの少なくとも一方を生成するために、前記複数のデータブロック及びデータパケットの少なくとも一方の符号化情報に前記 1 つ以上の符号化方法の逆変換を適用するように構成されており；

(i v) 前記データ処理部は、前記解読化され復号化されたデータ (D 3) を生成するために、前記複数のデータブロック及びデータパケットの少なくとも一方に関連付けられた前記サイズ及び相対位置の少なくとも一方に基づいて、前記複数の復号化データブロック及びデータパケットの少なくとも一方を組み立てるように構成されている。

【請求項 12】

前記データ処理部が、前記少なくとも 1 つの圧縮データストリームの第 1 バイトから、前記少なくとも 1 つの圧縮データストリームと関連するエントロピー符号化方法を決定するように構成されている請求項 11 に記載のデコーダ (120) 。

【請求項 13】

前記データ処理部が、符号化され暗号化された一次元データ、符号化され暗号化された多次元データ、符号化され暗号化されたテキストデータ、符号化され暗号化されたバイナリデータ、符号化され暗号化されたセンサデータ、符号化され暗号化されたオーディオデータ、符号化され暗号化された画像データ、符号化され暗号化されたビデオデータのうち、少なくとも 1 つの形態で提供される前記符号化され暗号化されたデータ (E 2) を解読及び復号するように構成されている請求項 11 に記載のデコーダ (120) 。

【請求項 14】

デコーダ (120) によって、対応する解読化され復号化されたデータ (D 3) を生成する、符号化され暗号化されたデータ (E 2) を解読及び復号する方法であって、前記デコーダ (120) が前記符号化され暗号化されたデータ (E 2) を処理するデータ処理部を備えており、該方法は前記データ処理部による以下のステップを含む：

(i) 前記符号化され暗号化されたデータ (E 2) を処理して、暗号化データストリー

ムの先頭に書き込まれる新しいバイト、エントロピー符号化方法のバイト及びワードのうち少なくとも一方における最上位ビット、非暗号化データストリームと暗号化データストリームが前記符号化され暗号化されたデータ（E 2）に含まれる順序、フラグビット、のうち少なくとも1つを用いることでそのうち1つ以上の暗号化されたサブ部分及び1つ以上の暗号化されていないサブ部分を決定するステップ；

但し、前記符号化され暗号化されたデータ（E 2）の前記1つ以上の暗号化されていないサブ部分は複数のデータブロック及びデータパケットの少なくとも一方の符号化された情報を含む。

（i i）（a）サイズ、（b）相対位置、及び（c）前記複数のデータブロック及びデータパケットの少なくとも一方に関連する1つ以上の符号化方法、のうち少なくとも1つを決定するために、前記1つ以上の暗号化されたサブ部分を解読し解凍するステップ；

但し前記1つ以上の暗号化されたサブ部分は少なくとも1つの圧縮データストリームの形式で提供される。

（i i i）前記複数のデータブロック及びデータパケットの少なくとも一方の符号化された情報を復号化して複数の復号化されたデータブロック及びデータパケットの少なくとも一方を生成するために、前記複数のデータブロック及びデータパケットの少なくとも一方の符号化情報に前記1つ以上の符号化方法の逆変換を適用するステップ；及び

（i v）前記解読化され復号化されたデータ（D 3）を生成するために、前記複数のデータブロック及びデータパケットの少なくとも一方に関連付けられた前記サイズ及び相対位置の少なくとも一方に基づいて、前記複数の復号化データブロック及びデータパケットの少なくとも一方を組み立てるステップ。

【請求項 1 5】

前記少なくとも1つの圧縮されたデータストリームの第1バイトから、前記少なくとも1つの圧縮されたデータストリームに関連するエントロピー符号化方法を決定するために、前記データ処理部を動作することを含む請求項 1 4 に記載の方法。

【請求項 1 6】

前記データ処理部を動作させて、符号化され暗号化された一次元データ、符号化され暗号化された多次元データ、符号化され暗号化されたテキストデータ、符号化され暗号化されたバイナリデータ、符号化され暗号化されたセンサデータ、符号化され暗号化されたオーディオデータ、符号化され暗号化された画像データ、符号化され暗号化されたビデオデータのうち、少なくとも1つの形態で提供される前記符号化され暗号化されたデータ（E 2）を解読及び復号化することを含む請求項 1 4 に記載の方法。

【請求項 1 7】

対応する符号化され暗号化されたデータ（E 2）を生成するために入力データ（D 1）を符号化及び暗号化するための請求項 1 に記載の少なくとも1つのエンコーダ（1 1 0）と、前記符号化され暗号化されたデータ（E 2）を解読し復号して、対応する解読化され復号化されたデータ（D 3）を生成する請求項 1 1 に記載の少なくとも1つのデコーダ（1 2 0）とを含むコーデック（1 3 0）。

【請求項 1 8】

請求項 6 または 1 4 に記載の方法を実行するためのプロセスハードウェアを含むコンピュータ化された装置によって実行されるように構成されている、コンピュータ可読命令を記憶した非一時的なコンピュータ可読記憶媒体を備えるコンピュータプログラム製品。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明は、対応する符号化され暗号化されたデータ（E 2）を生成するための入力データ（D 1）を符号化し暗号化するエンコーダに関し、対応する符号化され暗号化されたデータ（E 2）を生成するための入力データ（D 1）の符号化及び暗号化する方法に関する。また、本発明は、対応する解読化され復号化されたデータ（D 3）を生成するための符号化され暗号化されたデータ（E 2）を解読、及び復号するデコーダに関し、対応する解

読化され復号化されたデータ（D3）を生成するための符号化され暗号化されたデータ（E2）を解読化、及び復号化する方法に関する。また、本発明は、上述の方法を実行するための処理ハードウェアを含むコンピュータ化された装置によって実行可能なコンピュータ読取り命令を記憶した非一時的コンピュータ読取り保存媒体を有するコンピュータプログラム製品に関する。さらに、本発明は、少なくとも1つの前述のエンコーダ及びデコーダを含むコーデックに関する。

【背景技術】

【0002】

一般に、「暗号化」という用語は、許可された当事者のみがメッセージあるいは情報を読むことができるようにメッセージあるいは情報を符号化するプロセスを指す。暗号化を扱う科学分野を暗号学と呼ぶ。情報は歴史を通じて暗号化され、各暗号化アルゴリズムには、それぞれに関連する弱点があることはよく知られている。暗号学に属する暗号解析は、暗号化アルゴリズムの弱点を見つけるために用いられる。

【0003】

暗号化アルゴリズムは、対称アルゴリズム（すなわち、対称キーアルゴリズム）及び非対称アルゴリズム（すなわち、非対称キーアルゴリズム）に分類することができる。対称アルゴリズムと非対称アルゴリズムは、暗号化キーを用いて処理する方法が互いに異なる。対称暗号化アルゴリズムは、共通のキーを使用して送信側でデータを暗号化し、暗号化されたデータを対応する受信側で復号化する。一方、非対称暗号化アルゴリズムは2つの異なるキーを使用し、そのうちの1つはデータを暗号化するために使用される公開キーであり、もう一つは暗号化されたデータを復号化するために使用される秘密のキーである。公開キーのみが当事者間で公開される。

【0004】

さらに、一方向のメッセージダイジェスト関数、すなわち暗号化技術ではないデータ暗号化技術であるハッシュ関数がある。その理由は、それらのデータが回復することが困難、または不可能であるためである。ただし、一方向のメッセージダイジェスト関数は、データとパスワードの信頼性を検証するために使用され、暗号化アルゴリズム用の暗号化キーを生成するためにも用いられる。

【0005】

データ暗号化は、かなりのコンピューティングリソースを必要とする技術的に要求の厳しい操作であることはよく知られている。したがって、コンピューティングリソースを節約し、計算時間を短縮するために、非対称暗号アルゴリズムと対称暗号アルゴリズムのハイブリッドの組合せがよく用いられる。この組合せは、不正な第三者解読を現在のコンピューティングリソースでリアルタイムに実行することができないように、十分に強力な保護を提供する。このようなアプローチは、SSL（Secure Sockets Layer）／TLS（Transport Layer Security）やSSH（Secure Shell）などの様々な異なるデータ転送プロトコルや例えば、Pretty Good Privacy（PGP）のような電子メールのメッセージの署名と暗号化などのアプリケーションで一般的に使用されている。

【0006】

暗号学、すなわち暗号と解読の科学的究明である暗号は、暗号解読の手法を用いて暗号アルゴリズムの弱点を発見しようと試みており、絶えず発展している科学分野であることが確立されている。このため、情報を最大限保護できることが不可欠であるが、対応して暗号化を実装するために使用されるコンピューティングリソースの使用に関して妥協する必要がある。さらに、利用可能なコンピューティングリソースは、特にバッテリー電力を節約するために最大限に活用するモバイルデバイスにおいて通常限られている。

【0007】

さらに、電子メールアプリケーションは、通常以下のものの暗号化を可能にする。
(i) 電子メールメッセージのみで、電子メールメッセージの電子メール添付ファイルではなく、あるいは、

(i i) 電子メールメッセージの電子メール添付ファイルのみで、電子メールメッセージではない。

つまり、電子メールの添付ファイルを含む電子メールメッセージ全体が暗号化されない。しかしながら、そのような種類の操作は、暗号化を実行するために利用可能な適度な処理能力の結果ではなく、使用シナリオまたはクライアントソフトウェア間の非互換性に基づいて用いられる。

【 0 0 0 8 】

ここ数年では、インターネット上のデータ転送量が年々大きく増加していることが主な理由で、画像及びビデオ情報の部分的な暗号化に関してかなりの研究が行われてきた。従来、「部分画像暗号化」技術は、離散コサイン変換 (D C T) 及びウェーブレットに基づく画像及びビデオコーデックで一般に使用されている。しかしながら、この技術は速度に関しては非効率的であり、達成可能な保護の程度に関しては弱い。

【 0 0 0 9 】

1つの従来技術では、与えられた画像の画素値が暗号化される。別の従来技術では、所与の画像ブロック内の画素の順序が暗号化によってスクランブルされる。さらに別の従来技術では、D C T符号化の非ゼロA C係数が暗号化される。更に別の従来技術では、画像の詳細、すなわち明るさ、色のコントラストなどが暗号化され、画像中のパターンの形状及び輪郭は暗号化されずに人間の目で見ることが出来る。

【 0 0 1 0 】

しかしながら、現在の従来技術では、本質的に部分データストリームを生成しない画像を符号化するためのこのような方法を使用するため、前述の従来技術は効率的に動作しない。その結果、上記の従来技術では、暗号化の速度と強さとを妥協することなく効率的な部分画像を暗号化することができなかった。

【 発明の概要 】

【 0 0 1 1 】

本発明は、対応する符号化され暗号化されたデータ (E 2) を生成するために入力データ (D 1) を符号化及び暗号化するための改良されたエンコーダを提供することを目的とする。

【 0 0 1 2 】

さらに、本発明は、符号化され暗号化されたデータ (E 2) を解読化及び復号化して、対応する解読化され復号化されたデータ (D 3) を生成するための改良されたデコーダを提供することを目的とする。

【 0 0 1 3 】

例えば、第1の態様として、対応する符号化され暗号化されたデータ (E 2) を生成するために入力データ (D 1) を符号化し暗号化するエンコーダ (1 1 0) であって、前記エンコーダは前記入力データ (D 1) を処理するためのデータ処理部を含む：

(a) 前記データ処理部は、入力データ (D 1) を符号化して複数の中間符号化データストリームを生成するように構成されており、

前記複数の中間符号化データストリームは、少なくとも1つのクリティカルデータストリームと該クリティカルデータストリームとは異なる1つ以上の非クリティカルデータストリームを含んでおり、前記クリティカルデータストリームは、前記非クリティカルデータストリームを後に復号化するために用いられるものであり、

前記少なくとも1つのクリティカルデータストリームは、前記複数の中間符号化データストリームの一部のみを構成するものであり、

(b) 前記データ処理部は、1つ以上の暗号化アルゴリズムを使用して前記少なくとも1つのクリティカルデータストリームを暗号化することにより少なくとも1つの中間暗号化データストリームを生成するように構成されており、

前記データ処理部は、前記少なくとも1つのクリティカルデータストリームを暗号化する前に、前記少なくとも1つのクリティカルデータストリームを少なくとも1つの圧縮データストリームに圧縮するように構成されており、

(c) 前記データ処理部は、前記符号化され暗号化されたデータ (E 2) に含まれるようにするために前記非クリティカルデータストリームを1つ以上の圧縮データストリームに圧縮するように構成されており、

(d) 前記データ処理部は、前記複数の中間符号化データストリームのうち暗号化されていない部分を前記少なくとも1つの中間暗号化データストリームと併合して前記符号化され暗号化されたデータ (E 2) を生成するように構成されている。

【0014】

任意に、エンコーダのデータ処理部は1次元データ、多次元データ、テキストデータ、バイナリデータ、センサデータ、オーディオデータ、画像データ、ビデオデータ、符号化データなどの少なくとも1つの形態で提供される入力データ (D 1) を符号化及び暗号化することを可能にするが、これらに限定されるものではない。

【0015】

エンコーダのデータ処理部は、入力データ (D 1) を符号化して複数の中間符号化データストリームを生成することを可能にする。また、この目的のためにエンコーダのデータ処理部は、入力データ D 1 を複数のデータブロック及び/またはデータパケットに分割及び/または結合するために複数の分割及び/または結合演算を使用することを可能にする。

【0016】

任意に、エンコーダのデータ処理部は複数のデータブロック及び/またはデータパケットの統計分析及び/または反復分析を実行して、それぞれのデータブロック及び/またはデータパケット内の統計的変動を示す複数のパラメータを決定することを可能にする。そして、エンコーダのデータ処理部は、複数のデータブロック及び/またはデータパケットの情報を複数の中間符号化データストリームに符号化するための1つのまたは複数の符号化方法を選択する複数のパラメータを用いることを可能にする。

【0017】

その後、エンコーダのデータ処理部は、複数のデータブロック及び/またはデータパケットの情報を複数の中間符号化データストリームに符号化するための1つ又は複数の符号化方法を使用するように動作可能である。

【0018】

任意に、エンコーダのデータ処理部は、複数の中間符号化データストリームに含められる複数のデータブロック及び/またはデータパケットを複数のエントロピー符号化データブロック及び/またはデータパケットに圧縮するための1つ以上のエントロピー符号化方法を使用するように動作可能である。そのようなエントロピー符号化は、1つ以上のデータブロック及び/またはデータパケットが前述の符号化方法を使用して符号化された後に任意に実行される。

【0019】

複数の中間符号化データストリームは、複数の中間符号化データストリームの1つ以上の残りのデータストリームを後で復号するために重要で、かつ不可欠な少なくとも1つのクリティカルデータストリームを含む。任意に、少なくとも1つのクリティカルデータストリームは、以下のうちの少なくとも1つを示す情報を含む。：入力データ (D 1) を複数のデータブロック及び/またはデータパケットを符号化する情報に使用される複数のデータブロック及び/またはデータパケット及び/または1つ以上の符号化方法に分割及び/または結合するために使用される複数の分割及び/または結合動作。

【0020】

したがって、少なくとも1つのクリティカルデータストリームは、複数の中間符号化データストリームの一部のみを表す。

【0021】

さらに、エンコーダのデータ処理部は、少なくとも1つの中間暗号化データストリームを生成するために1つ以上の暗号化アルゴリズムを使用して少なくとも1つのクリティカルデータストリームを暗号化するように動作可能である。

【0022】

続いて、エンコーダのデータ処理部は、符号化され暗号化されたデータ（E2）を生成するために、複数の中間符号化データストリームの暗号化されていない部分、すなわち複数のデータブロック及び／またはデータパケットの符号化情報を少なくとも1つの中間暗号化データストリームと併合するように動作可能である。

【0023】

任意に、エンコーダのデータ処理部は、少なくとも1つのクリティカルデータストリームを暗号化する前に、少なくとも1つのクリティカルデータストリームを少なくとも1つの圧縮データストリームに圧縮するように動作可能である。

【0024】

任意に、少なくとも1つの圧縮データストリームの長さを示す情報は、少なくとも1つの圧縮データストリームの先頭に、例えば、前述の第1バイトの後に提供される。

【0025】

さらに、任意に、エンコーダのデータ処理部は、暗号化されたデータストリームの先頭に書き込まれる新しいバイト、エントロピー符号化方法で最上位ビット（Most Significant Bit：MSB）のバイト及び／又はワード、符号化され暗号化されたデータ（E2）に含まれる符号化され暗号化されたデータストリームの順序、及び／またはフラグビットの少なくとも1つを用いて暗号化を定義するように動作可能である。

【0026】

第2の態様では、エンコーダ（110）を経由して、対応する符号化され暗号化されたデータ（E2）を生成する、入力データ（D1）を符号化及び暗号化する方法であって、前記エンコーダ（110）は前記入力データ（D1）を処理するためのデータ処理部を含むものであり、該方法は前記データ処理部による以下のステップを含む：

（a）前記入力データ（D1）を符号化して複数の中間符号化データストリームを生成するステップ、

但し、前記複数の中間符号化データストリームは、少なくとも1つのクリティカルデータストリームと該クリティカルデータストリームとは異なる1つ以上の非クリティカルデータストリームを含んでおり、前記クリティカルデータストリームは、前記非クリティカルデータストリームを後に復号化するために用いられるものであり、

前記少なくとも1つのクリティカルデータストリームは、前記複数の中間符号化データストリームの一部のみを構成するものである。

（b）1つ以上の暗号化アルゴリズムを使用して前記少なくとも1つのクリティカルデータストリームを暗号化することにより少なくとも1つの中間暗号化データストリームを生成するステップ、

但し、前記データ処理部は、前記少なくとも1つのクリティカルデータストリームを暗号化する前に、前記少なくとも1つのクリティカルデータストリームを少なくとも1つの圧縮データストリームに圧縮するように構成されている。

（c）前記符号化され暗号化されたデータ（E2）に含めるために前記非クリティカルデータストリームを1つ以上の圧縮データストリームに圧縮するステップ、

（d）前記複数の中間符号化データストリームのうち暗号化されていない部分を前記少なくとも1つの中間暗号化データストリームと併合して前記符号化され暗号化されたデータ（E2）を生成するステップ。

【0027】

任意に、少なくとも1つのクリティカルデータストリームは、複数のデータブロック及び／またはデータパケットを符号化する情報に用いられる複数のデータブロック及び／またはデータパケット及び／または1つ以上の符号化方法の中に入力データ（D1）を分割及び／または結合するのに用いられる少なくとも1つの複数の分割及び／または結合動作を示す情報を含む。

【0028】

さらに任意に、以下の方法を含む：

(e) 各データブロック及び／またはデータパケットの範囲内で統計変化を示す複数のパラメータを決定するために、統計分析及び／または複数のデータブロック及び／またはデータパケットの反復分析を実行する前記データ処理部を動作することと；そして

(f) 複数の中間符号化データストリームを生成するために、複数のデータブロック及び／またはデータパケットの情報を符号化するのに用いられる1つ以上の符号化方法を選択する複数のパラメータを用いる前記データ処理部を動作することを含む。

【0029】

任意に、前記方法は、1次元データ、多次元データ、テキストデータ、バイナリデータ、オーディオデータ、画像データ、ビデオデータ、符号化データのうち少なくとも1つの形態で提供される入力データ(D1)を実行するデータ処理部を動作することを含む。

【0030】

任意に、前記方法は、少なくとも1つのクリティカルデータストリームを圧縮するのに用いられるエントロピー符号化方法を記録する第1バイトのような少なくとも1つの圧縮データストリームの第1バイトを計算するデータ処理部を動作することを含む。

【0031】

任意に、前記方法は、暗号化データストリームの開始時に書き込みされる新しいバイト、エントロピー符号化方法のバイト及び／または世界、非暗号化及び暗号化データストリームが符号化され暗号化されたデータ(E2)、フラグビットに含まれる配列のうち少なくとも1つを用いることにより暗号化を規定するデータ処理部を動作することを含む。

【0032】

第3の態様では、本開示の実施形態は、コンピュータ可読命令が格納された非一時的(すなわち非過渡的)コンピュータ可読記憶媒体を含むコンピュータプログラム製品を提供し、前記コンピュータ可読命令は、上記の方法を実行するための処理ハードウェアを含む。

【0033】

第4の態様では、符号化され暗号化されたデータ(E2)を対応する解読化され復号化されたデータ(D3)を生成するデコーダ(120)であって、該デコーダ(120)は符号化され暗号化されたデータ(E2)を処理するためのデータ処理部を含む；

(i) 前記データ処理部は、前記符号化され暗号化されたデータ(E2)を処理して、1つ以上の暗号化されたサブ部分及びその1つ以上の暗号化されていないサブ部分を決定し、前記1つ以上の暗号化されていない部分の符号化された情報は、複数のデータブロック及びデータパケットの少なくとも一方の符号化された情報を含み；

(i i) 前記データ処理部は、サイズ、相対位置、及び前記複数のデータブロック及びデータパケットの少なくとも一方に関連する1つ以上の符号化方法、のうち少なくとも1つを決定するために、1つ以上の暗号化されたサブ部分を解読し解凍するように構成されており、前記1つ以上の暗号化されたサブ部分が少なくとも1つの圧縮データストリームの形式で提供されるものであり；

(i i i) 前記データ処理部は、前記複数のデータブロック及びデータパケットの少なくとも一方の符号化された情報を復号するために、複数の復号されたデータブロック及びデータパケットの少なくとも一方を生成するための、前記複数のデータブロック及びデータパケットの少なくとも一方の符号化情報に1つ以上の符号化方法の逆変換を適用するように構成されており；

(i v) 前記データ処理部は、解読化され復号化されたデータ(D3)を生成するために、前記複数のデータブロック及びデータパケットの少なくとも一方に関連付けられたサイズ及び相対位置に基づいて、複数の復号化データブロック及びデータパケットを組み立てるように構成されている。

【0034】

任意に、デコーダのデータ処理部は、符号化及び暗号化された1次元データ、符号化及び暗号化された多次元データ、符号化及び暗号化されたデータテキストデータ、符号化及び暗号化されたバイナリデータ、符号化及び暗号化されたセンサデータ、符号化及び暗号

化されたオーディオデータ、符号化及び暗号化された画像データ、符号化及び暗号化されたビデオデータ、またはこれに限定されない少なくとも1つの形態で提供される符号化され暗号化されたデータ（E2）を解読化し復号化するように動作可能である。

【0035】

デコーダのデータ処理部は、1つ以上の暗号化サブ部分及び1つ以上の非暗号化サブ部分等を決定するために、符号化され暗号化されたデータ（E2）を処理するように動作可能である。符号化され暗号化されたデータ（E2）の1つ以上の非暗号化サブ部分は、複数のデータブロック及び／またはデータパケットの符号化された情報を含む。

【0036】

デコーダのデータ処理部は、サイズ、相対位置、及び／または複数のデータブロック及び／またはデータパケットに関連する1つ以上の符号化方法を決定するために、1つ以上の暗号化サブ部分を復号するように動作可能である。任意に、デコーダのデータ処理部はまた、複数のデータブロック及び／またはデータパケットに関連する1つ以上のエントロピー符号化方法を決定するように動作可能である。

【0037】

さらに、任意に、1つ以上の暗号化サブ部分が、少なくとも1つの圧縮されたデータストリームの形式で提供される。そのような場合、デコーダのデータ処理部は、少なくとも1つの圧縮データストリームの第1バイトから、少なくとも1つの圧縮データストリームに関連付けられたエントロピー符号化方法を決定するように選択的に動作可能である。

【0038】

任意に、少なくとも1つの圧縮データストリームの長さを示す情報は、少なくとも1つの圧縮データストリームの先頭に、例えば、前述の第1バイトの後に提供される。

【0039】

さらに、任意に、エンコーダのデータ処理部は、暗号化されたデータストリームの先頭に書き込まれる新しいバイト、エントロピー符号化方法で最上位ビット（MSB）のバイト及び／又はワード、符号化され暗号化されたデータ（E2）に含まれる符号化され暗号化されたデータストリームの順序、及び／またはフラグビットの少なくとも1つを用いて暗号化を定義するように動作可能である。

【0040】

次に、デコーダのデータ処理部は、エントロピー符号化方法の逆変換を適用して、少なくとも1つの圧縮ストリームを解凍して、サイズ、相対位置、及び／または1つ以上の符号化方法を決定するように、複数のデータブロック及び／またはデータパケットを有する。次いで、デコーダのデータ処理部は、複数のデータブロック及び／またはデータパケットの符号化された情報に1つ以上の符号化方法の逆変換を適用して、複数のデータブロックの符号化された情報を復号するように、及び／または複数のデコードされたデータブロック及び／またはデータパケットを生成する。選択的に、デコーダのデータ処理部はまた、1つ以上のエントロピー符号化方法の逆変換を複数のエントロピー符号化データブロック及び／または1つ以上の非暗号化サブ部分に含まれるデータパケットに適用するように動作可能である。1つ以上の符号化方法の逆変換を適用する前に、符号化され暗号化されたデータ（E2）を生成する。

【0041】

その後、デコーダのデータ処理部は、サイズ及び／または位置に基づいて複数の復号化データブロック及び／またはデータパケットを組み立てて、解読化され復号化されたデータ（D3）を生成するように動作可能である。

【0042】

第5の態様では、デコーダ（120）を介して、対応する解読化され復号化されたデータ（D3）を生成するために、符号化され暗号化されたデータ（E2）を復号化及び符号化する方法であって、前記デコーダ（120）が前記符号化され暗号化されたデータ（E2）を処理するデータ処理部を備えており：

（i）前記符号化され暗号化されたデータ（E2）を処理する前記データ処理部を動作さ

せることと、前記暗号化されたサブ部分及びその1つ以上の暗号化されていないサブ部分を決定することと、前記符号化され暗号化されたデータ（E 2）の暗号化されていないサブ部分は、複数のデータブロック及びデータパケットの少なくとも一方の符号化された情報を含み；

（i i） サイズ、 相対位置、及び 複数のデータブロック及びデータパケットに関連する1つ以上の符号化方法、のうち少なくとも1つを決定するために、前記1つ以上の暗号化されたサブ部分を解読し解凍するように前記データ処理部を動作させることと；但し1つ以上の暗号化されたサブ部分は少なくとも1つの圧縮データストリームの形式で提供される。

（i i i） 前記複数のデータブロック及びデータパケットの少なくとも一方の符号化情報を復号するために、前記複数のデータブロック及びデータパケットの符号化情報に前記1つ以上の符号化方法の逆変換を適用するように前記データ処理部を動作させることと；

（i v） 前記複数のデータブロック及びデータパケットに関連付けられたサイズ及び相対位置の少なくとも一方に基づいて、前記複数の復号データブロック及びデータパケットの少なくとも一方を組み立てて、前記解読化され復号化されたデータ（D 3）を生成することと；

を備えることを特徴とする前記符号化され暗号化されたデータ（E 2）を復号化及び符号化する方法。

【0043】

任意に、前記方法は、暗号化データストリーム、エントロピー符号化方法及び／または符号化され暗号化されたデータ（E 2）、フラグビットの中に含まれた非暗号化及び暗号化されたデータストリームの配列の言語、知識における最も重要なビットを開始する際に書き込まれる新しいバイトの少なくとも1つを用いる1つ以上の暗号化サブ部分及び1つ以上の非暗号化サブ部分を決定するために、前記データ処理部を操作することを含む。

【0044】

任意に、前記方法は、少なくとも1つの符号化され暗号化された1次元データ、符号化され暗号化された多次元データ、符号化され暗号化されたテキストデータ、符号化され暗号化されたバイナリデータ、符号化され暗号化されたセンサデータ、符号化され暗号化されたオーディオデータ、符号化され暗号化された画像データ、符号化され暗号化されたビデオデータのうち少なくとも1つの形態で提供される符号化され暗号化されたデータ（E 2）を解読し復号するために、前記データ処理部を操作することを含む。

【0045】

第6の態様では、本開示の実施形態は、コンピュータ可読命令が格納された非一時的（すなわち非過渡的）コンピュータ可読記憶媒体を含むコンピュータプログラム製品を提供する。コンピュータ可読命令は、上述した方法を実行するための処理ハードウェアを含むコンピュータ化された装置である。

【0046】

第7の態様では、本開示の実施形態は、前述のエンコーダ及び前記デコーダを含むコーデックを提供する。

【0047】

本開示の実施形態による前述の方法は、どの暗号化アルゴリズムが使用されるかにかかわらず、任意の適切な符号化構成で実施することができる。その際、前述の方法は暗号化アルゴリズムの動作を変更しない。すなわち、暗号化アルゴリズムによって提供される保護が損われないことを意味する。

【0048】

前述の方法は、非常に高速で効率的な暗号化アルゴリズムを使用することを可能にする。これに関して、前述の方法は、暗号化アルゴリズム自体の内部動作を妨害することなく、効率的な方法で暗号化アルゴリズムと共に使用することができる。前述の方法での実装に適した暗号化アルゴリズムの例には、AES、RSA、Twofish、Blowfish、データ暗号化標準（DES）、トリプルDES（3-DES）、Serpent、

国際データ暗号化アルゴリズム (IDEA)、MARS、Rivest Cipher 6 (RC6)、Camellia、CAST-128、Skipjack、XTEA (Extended Tiny Encryption Algorithm) これらの例の名前には登録商標が含まれている。

【0049】

本開示の実施形態に従う前述の方法は、既知の従来技術の方法と比較して、データを保護する非常に高速かつかなり効率的な方法を提供する。特に、符号化されたデータの1つまたはそれ以上の必須部分のみが暗号化される。例えば、画像またはビデオが、Gurulogic Microsystems Oyから入手可能なGurulogic Multi-Variate Codec (GMVC (登録商標)) コード化ソリューションでコード化され、コード化された全体の1/100から1/1000部分のみデータは暗号化で保護されているが、データセキュリティを損うリスクはない。したがって、このような方法での暗号化の使用は、リアルタイムビデオの転送レートに大きな影響を及ぼさず、いかなる重要な方法でもコンピューティングリソースの消費を増加させるものではないと結論付けることができる。

【0050】

さらに、暗号化プロセスのさらなる利点は、例えばVPN (Virtual Private Network) トンネリング、Secure Shell (SSH)、またはSSL/TLSプロトコルのように、符号化され暗号化されたデータ (E2) が保護された、安全なネットワーク接続によりネットワークを超えて移送されることを必要としない。したがって、前述の方法は、例えばパブリックインターネットのネットワークまたはウェブサービス及びクラウドサービスにおいてテキスト、バイナリ、オーディオ、画像、ビデオ及び他のタイプのデータを送信するための有利なモデルを提供する。

【0051】

本開示のさらなる態様、利点、特徴及び目的は、添付の特許請求の範囲と関連して解釈される例示的な実施形態の図面及び詳細な説明から明らかになるであろう。

【0052】

本開示の特徴は、添付の特許請求の範囲によって規定される本開示の範囲から逸脱することなく、様々な組み合わせで組み合わせることが可能であることが理解されるであろう。

【図面の簡単な説明】

【0053】

上記の概要、ならびに例示的な実施形態の以下の詳細な説明は、添付の図面と併せて読めばよりよく理解される。本開示を例示する目的で、本開示の例示的な構造が図面に示されている。しかし、本開示は、本明細書に開示される特定の方法及び装置に限定されない。さらに、当業者は図面が一定の縮尺ではないことを理解するであろう。可能な限り、同じ要素が同じ番号で示されている。

【0054】

本開示の実施形態は、以下の図を参照して、例としてのみ説明される。

【図1】 図1は、対応する符号化され暗号化されたデータ (E2) を生成するために入力データ (D1) を符号化し暗号化するエンコーダと、解読化され暗号化されたデータ (D3) を生成するためのデコーダであって、本開示の実施形態によるコーデックを集合的に形成するエンコーダとデコーダを示す。

【図2】 図2は、本開示の一実施形態による、入力データ (D1) を符号化して暗号化して対応する符号化され暗号化されたデータ (E2) を生成する第1の方法のステップを示すフローチャートの概略図である。

【図3】 図3は、本開示の一実施形態による、暗号化プロセスのステップの概略図である。

【図4】 図4は、本開示の一実施形態による、解読化され復号化されたデータ (D3) を生成するための符号化され暗号化されたデータ (E2) を解読化し復号化する第2の方法

のステップを示すフローチャートの概略図である。そして、

【図5】 図5は、本開示の一実施形態による解読プロセスのステップの概略図である。

【0055】

添付の図において、下線番号は、下線番号が位置する項目または下線番号が隣接する項目を表すために使用される。下線が引かれていない数字は、下線が引かれていない数字と項目を結ぶ線で識別される項目に関連している。

【発明を実施するための形態】

【0056】

以下の詳細な説明では、本開示の例示的な実施形態及びそれらが実施され得る方法が解明される。本開示を実施するいくつかの態様が記載されているが、当業者であれば、本開示を実施または実施するための他の実施形態も可能であることを認識するであろう。

【0057】

概要として、本開示の実施形態は、部分データ暗号化のための暗号化方法、それに対応する復号化方法に準ずるものに関する。前述の方法は、非常に速い暗号化プロセスが達成されることを可能にし、不正アクセスに対する非常に強力な保護を提供する。

【0058】

前述の方法は、既に圧縮された、または他の方法で符号化された1次元または多次元のテキスト、バイナリ、オーディオ、画像、ビデオまたは他のタイプのデータに対して既知の暗号化アルゴリズムを有益に使用する。しかしながら、本方法は、未知の暗号化アルゴリズム、例えば、将来的に考案される暗号化アルゴリズムを任意に使用する。その方法の機能は、様々な暗号化アルゴリズムに適合させることができる。

【0059】

本開示で説明される部分データ暗号化は、その内容、特性、及び構成に基づいてデータを符号化する様々な圧縮アルゴリズムと共に非常に効率的に機能する。このような圧縮アルゴリズムは、出力として2つ以上のデータストリームを生成し、そのうちの少なくとも1つは、データの内容に関して本質的に重要である。

【0060】

本開示の実施形態は、データの1つ以上の最も重要な部分のみを暗号化することによって、データを暗号化する費用効率の高い方法を提供することを目的とする。これにより、データ処理部によって消費される計算資源及び処理エネルギーが節約され、暗号化から望まれる保護の程度を弱めることなく、暗号化に必要な時間が短縮される。このようなエネルギー消費の節約は、小型の充電式電池を使用することを可能にするスマートフォンなどのポータブルコンピューティング機器、または電池の充電が必要とされるまでの延長された動作時期に非常に有益である。

【0061】

本開示を通じて、暗号化されていない情報は「平文」と呼ばれ、それに対応して暗号化された情報は「暗号文」と呼ばれる。

【0062】

図1を参照すると、本開示の実施形態は、

(i) 入力データ(D1)を符号化して暗号化して対応する符号化され暗号化されたデータ(E2)を生成するエンコーダ110と、入力データ(D1)を符号化して暗号化して符号化され暗号化されたデータ(E2)を生成する方法と；

(i i) 符号化され暗号化されたデータ(E2)を解読化され復号化されたデータ(D3)を生成するデコーダ120と、符号化され暗号化されたデータ(E2)を復号化及び対応する解読化され復号化されたデータ(D3)と；

(i i i) 少なくとも1つのエンコーダと、少なくとも1つのデコーダ、例えば、エンコーダ110とデコーダ120との組み合わせを含むコーデック130に関する。

【0063】

任意に、対応する解読化され復号化されたデータ(D3)は、無損失モードの動作と同様に、入力データ(D1)と全く同じである。あるいは、任意に、対応する解読化され復

号化されたデータ（D3）は、損失のある動作モードの場合のように、入力データ（D1）とほぼ同じである。さらに、任意に、データをトランスコードする際に使用される変換などによって、対応する解読化され復号化されたデータ（D3）は入力データ（D1）とは異なるが、入力データ（D1）に存在する実施的に同様の情報を保持する。（D3）の再フォーマットが必要である場合、例えば、異なるタイプの通信プラットフォーム、ソフトウェア（例えば、通信プラットフォーム）に適合するために、対応する解読化され復号化されたデータ（D3）が入力データ層、通信装置などを含む。

【0064】

エンコーダ110は、入力データ（D1）を処理して対応する符号化され暗号化されたデータ（E2）を生成するデータ処理部を含む。任意に、エンコーダ110でデータ処理部は、以下で詳細に説明するプログラム命令を実行するように動作可能な少なくとも1つのRISC（Reduced Instruction Set Computing）プロセッサを使用することによって実施される。

【0065】

任意に、エンコーダ110のデータ処理部は、1次元データ、多次元データ、テキストデータ、バイナリデータ、センサデータの少なくとも1つの形態で提供される入力データ（D1）を符号化し、暗号化するように動作可能である。オーディオデータ、画像データ、ビデオデータ、符号化データなどが含まれるが、これに限定されるものではない。任意に、入力データ（D1）は、ストリームまたはファイルとして受信される。

【0066】

エンコーダ110のデータ処理部は、入力データ（D1）を符号化して複数の中間符号化データストリームを生成するように動作可能である。

【0067】

任意に、入力データ（D1）を符号化するために、エンコーダ110のデータ処理部は、入力データ（D1）を複数の分割及び/または結合するために、データブロック及び/またはデータパケットを含む。第1の例では、入力データ（D1）は1次元であり、走査線を使用して分割することができる。第2の例では、入力データ（D1）は多次元であり、データブロックの次元数に応じてデータブロックに分割することができる。

【0068】

これに関して、エンコーダ110は、他の公知のエンコーダで有益に使用可能である。英国特許GB2503295Bに記載されているようなブロックエンコーダと併せて使用することができる。ブロックエンコーダは、入力データ（D1）を複数のデータブロック及び/またはデータパケットに最適な方法で分割及び/または結合するために使用することができる。

【0069】

入力データ（D1）が1次元である第1の例では、入来ストリーム、すなわちバイト例をより短いストリームに分割することによって、入力データ（D1）からデータブロックが抽出される。例えば、規則的な走査の後に得られた6×4画像内のピクセルのインデックス、すなわち、最初に左から右に、次に上から下に走査すると、次のように表すことができる。

【0070】

【0071】

これらのインデックスは、エンコードのために1次元形式で配信されるとき、次のように表すことができるライン結合バイト文字列を生成する。

【0072】

【0073】

バイト列は、例えば、4バイトのより短いバイト列に分割することができ、以下のように表すことができる。

【0074】

()
()
()
()
()
()

【0075】

第2の例では、説明のために、入力データ(D1)は2次元(2D)画像である。この例では、2D画像は任意で2×2のより小さい領域に分割され、2D画像の2×2領域の通常の手順を使用することにより、2D画像内のピクセルのインデックスを4バイトのバイト列として再構成することができる。これらのバイト文字列は、次のように表すことができる。

【0076】

()
()
()
()
()
()

【0077】

さらに、いくつかの例では、入力データ(D1)は、例えば3Dビデオコンテンツの場合のように、3次元(3D)とすることができる。他の例では、入力データ(D1)には、例えばビデオ中の時間など、より多くの次元が存在し得る。

【0078】

同様に、入力データ(D1)が音声データの場合も、同様の分割処理を行うことができる。一例では、オーディオデータは、任意に、複数のマイクロフォンからのオーディオ信号を含む。このような場合、オーディオデータは、個々のオーディオ信号が分離され、その後さらにデータパケットに分割されることができる。

【0079】

入力データ(D1)が複数のデータブロック及び／またはデータパケットに分割されると、エンコーダ110のデータ処理部は、複数のデータブロックの統計解析及び／または反復分析を実行するように任意に動作可能であり、それらのそれぞれのデータブロック及び／またはデータパケット内の統計的変動を示す複数のパラメータを決定する。次いで、エンコーダ110のデータ処理部は、複数のデータブロック及び／またはデータパケットの情報を符号化するために使用される1つ以上の符号化方法を選択するために、複数のパラメータを使用するように任意に動作可能である。

【0080】

その後、エンコーダ110のデータ処理部は、複数のデータブロック及び／またはデータパケットの情報を複数の中間符号化データストリームの少なくとも1つに符号化するための1つ以上の符号化方法を使用するように動作可能である。

【0081】

任意に、エンコーダ110のデータ処理部は、複数のデータブロック及び／またはデータパケットを、複数のエントロピー符号化データブロック及び／またはデータパケットに圧縮して複数の中間符号化データストリームのうちの少なくとも1つを符号化する。そのようなエントロピー符号化は、複数のデータブロック及び／またはデータパケットが前述の符号化方法を使用して符号化された後に任意に実行される。このような圧縮に関しては

、符号化され暗号化されたデータ（E2）を生成するときデータ（D1）を圧縮することは前述のエントロピー符号化方法の目的であり、このようなデータ圧縮を達成する方法はしばしば成功するが、常にではない。いずれの場合も、本開示の実施形態で適用される所与のエントロピー符号化方法は、しばしばエントロピー符号化されるデータの長さを有する中間符号化データストリームに含まれる必要があり、時にはエントロピーエンコーディングが実行される前のデータの長さを有する。

【0082】

複数の中間符号化データストリームのうちの1つ以上が、複数の中間符号化データストリームの1つ以上の残りのデータストリームを正しく復号するために重要であり、不可欠であることが理解されるであろう。クリティカルかつ本質的である複数の中間符号化データストリームのうちの1つ以上は、以後、「クリティカルデータストリーム」と呼ばれる。

【0083】

複数の中間符号化データストリームのうちの1つ以上の残りのデータストリームは、以後、「非クリティカルデータストリーム」と呼ばれる。

【0084】

任意に、複数の中間符号化データストリームのクリティカルデータストリームは、以下のうちの少なくとも1つを示す情報を含む。

(i) 入力データ(D1)を複数のデータブロック及び/またはデータパケットに分割及び/または結合するために使用される複数の分割及び/または結合動作、

(ii) 複数のデータブロック及び/またはデータパケットの情報を符号化するために使用される1つ以上の符号化方法、

(iii) 複数のデータブロック及び/またはデータパケットをエントロピー符号化するために使用される1つ以上のエントロピー符号化方法、及び/または

(iv) エントロピー符号化データストリーム内の複数のエントロピー符号化データブロック及び/またはデータパケットの長さ、及び/または

(v) エントロピーエンコーディングが適用される前の複数のデータブロック及び/またはデータパケットの長さ。

【0085】

したがって、クリティカルデータストリームは、複数の中間符号化データストリームの一部のみを表す。クリティカルデータストリームは、典型的には、中間符号化データストリーム全体の1/1000から1/10000部分の範囲内にある。

【0086】

任意に、非クリティカルデータストリームは、データベース基準値、離散コサイン変換(DCT)パラメータの値、DC係数の値、スライド値、ライン値、スケール値、マルチレベル値、及び/これらに限定されるものではない。

【0087】

さらに、前述したように、クリティカルデータストリームは、複数の中間符号化データストリームの不可欠な部分であり、複数の中間符号化データストリームの重要ではないデータストリームを正しく復号することが不可能である。したがって、複数の中間符号化データストリームを不正アクセスから保護するために、以下でより詳細に説明するように、クリティカルデータストリームの少なくとも1つを有益に暗号化する。

【0088】

さらに、任意に、エンコーダ110のデータ処理部は、クリティカルデータストリームの少なくとも1つを暗号化するために使用するための少なくとも1つのキーを生成または受信するように動作可能である。

【0089】

任意に、1つの実施形態では、エンコーダ110のデータ処理部は、動作中に少なくとも1つのキーを供給される。

【0090】

あるいは、別の実施形態では、エンコーダ110のデータ処理部は、適切なキー生成アルゴリズムを使用して少なくとも1つのキーを生成するためにキーストレッチを適用するように任意に動作可能である。任意に、キーの伸張は、関連するパスワードに一方方向ダイジェストアルゴリズム（すなわち、ハッシュアルゴリズム）を複数回繰り返して反復することを含む。

【0091】

さらに、任意に、エンコーダ110のデータ処理部は、少なくとも1つの中間暗号化データストリームを生成するために、少なくとも1つのキーを使用してクリティカルデータストリームの少なくとも1つを暗号化する。任意に、エンコーダ110のデータ処理部は、クリティカルデータストリームの少なくとも1つを暗号化するとき、少なくとも1つの初期ベクトル（「Init Vector」；IV）を少なくとも1つのキーと共に適用するように動作可能である。

【0092】

続いて、エンコーダ110のデータ処理部は、暗号化されていない非クリティカルデータストリームを含む複数の中間エンコードデータストリームの暗号化されていない部分を少なくとも1つの中間暗号化データストリーム及び符号化され暗号化されたデータ（E2）と併合する。

【0093】

さらに、任意に、エンコーダ110のデータ処理部は、クリティカルデータストリームの少なくとも1つを、暗号化に先立って少なくとも1つの圧縮データストリームに圧縮するように動作可能である。同様に、任意に、エンコーダ110のデータ処理部は、非クリティカルデータストリームを符号化され暗号化されたデータ（E2）に含めるために1つ以上の他の圧縮データストリームに圧縮するように動作可能である。

【0094】

任意に、エンコーダ110のデータ処理部は、第1バイトがクリティカルデータストリームの少なくとも1つを圧縮するために使用されるエントロピー符号化方法を記述するように、少なくとも1つの圧縮データストリームの第1バイトを計算するように動作可能である。同様に、任意に、エンコーダ110のデータ処理部は、これらの第1バイトが非クリティカルデータストリームを圧縮するために使用されるエントロピー符号化方法を記述するように、1つ以上の他の圧縮データストリームの第1バイトを計算するように動作可能である。

【0095】

任意に、クリティカルデータストリームの少なくとも1つ、すなわち少なくとも1つの圧縮データストリームが暗号化されて暗号化データストリームを生成するとき、1つのエントロピー符号化方法として暗号化を定義する新しいバイトが、暗号化データストリームの開始時に読み取られる。新しいバイトがデコーダ120でのその後の解読及び復号中に読み取られるとき、デコーダ120は、データストリームが暗号化されていることに気付く。したがって、デコーダ120は、暗号化されたデータストリームを少なくとも1つの圧縮データストリームに解読し、少なくとも1つの圧縮データストリームの第1バイトから実際のエントロピー符号化方法を読み取る。これは、少なくとも1つの圧縮されたデータストリームの圧縮解除を可能にする。

【0096】

代替として、暗号化を定義する新しいバイトを配信する代わりに、使用される暗号化に関する情報を、新しいバイトは、例えば、メソッドバイト及び／またはワードのエントロピー符号化において、最上位ビット（Most Significant Bit：MSB）を用いることによって、採用されたエントロピー符号化方法に関する情報と結合される。

【0097】

さらに、任意に、エンコーダ110は、符号化され暗号化されたデータ（E2）に暗号化されていないデータストリームが含まれる順序と、符号化され暗号化されたデータ（E

2) のうちの少なくとも1つに関する情報とをデコーダ120に通信するように動作可能である。

【0098】

さらに、任意に、1つ以上のフラグビットは、どのデータストリームが符号化情報(すなわち、非クリティカルデータストリーム)を含み、どのデータストリームが符号化情報を含まない(すなわちクリティカルデータストリーム)かを示すために用いられる。

【0099】

任意に、少なくとも1つの圧縮データストリームの長さを示す情報は、第1バイトの後に提供される。これにより、デコーダ120は、少なくとも1つの圧縮データストリームの長さを読み出し、おそらくそのコンテンツをその自身のバッファにコピーし、ジャンプして次のデータストリームを読み出すことができる。任意に、長さを示す情報は暗号化されずに残される。あるいは、任意に、暗号化されたデータストリームの新しい長さが新しいバイトの後に書き込まれる。さらに、任意に、第1バイトは、符号化され暗号化されたデータ(E2)全体を復号化及び符号化することなしに、エンコーダ110で暗号化され、続いてデコーダ120で復号化される。

【0100】

別の実施形態では、クリティカルデータストリームの少なくとも1つを最初に暗号化し、次に圧縮することができる。しかしながら、クリティカルデータストリームのうちの少なくとも1つがかなりの冗長データを含むことが多いので、暗号化に先立ってクリティカルデータストリームの少なくとも1つの圧縮を実行することが有利であることが理解されよう。したがって、エンコーダ110のデータ処理部は、クリティカルデータストリームの少なくとも1つを圧縮するのに適したエントロピー符号化方法を使用するように動作可能である。そのような場合、符号化され暗号化されたデータ(E2)のエントロピー及びデータサイズは、クリティカルデータストリームのうちの少なくとも1つが圧縮前に暗号化された場合よりも小さい。理論的に可能であるように符号化され暗号化されたデータ(E2)を解読するために多くの選択肢があることを数学的に意味する符号化され暗号化されたデータ(E2)において最大データエントロピーを生成する傾向がある。

【0101】

一例として、Gurulogic Microsystems Oyから入手可能なGurulogic Multi-Variate Codec(GMVC(登録商標))コード化ソリューションは、本開示の実施形態と組み合わせて有益に使用される。GMVC(登録商標)コーディングソリューションは、元の入力の情報全体、つまり、効率的にエントロピー符号化された方法において、入力データ(D1)を含むいくつかの異なるデータストリームを生成しながら、異なるタイプのデータを効率的にエンコードすることができる。例えば、上述の独自のGMVC(登録商標)コーディングソリューションでは、画像データまたはビデオデータの符号化は、入力データ(D1)のフォーマット及び内容に応じて、異なるデータストリームを生成するために互いに異なる符号化方法を使用する。したがって、入力データ(D1)のビット数及びエントロピーを考慮して、異なる種類のデータが、正確にそれらの種類のデータに最適な異なる符号化及びエントロピー符号化方法で効率的に符号化及び圧縮されることが有利である。圧縮により、データのサイズが小さくなる。これは、より少量のデータを暗号化する必要があることを意味し、したがって、暗号化プロセスがより高速になる。

【0102】

さらに、画像データまたはビデオデータを符号化するとき、GMVC(登録商標)符号化ソリューションは、複数の分割及び/または組み合わせを示す情報、例えば分割及び/または結合を含むエンコーダに典型的なデータストリームを生成する入力データ(D1)を複数のデータブロック及び/またはデータバケットに分割及び/または結合するために採用される。このデータストリームは、以下、「分割/結合情報データストリーム」と呼ばれる。分割/結合情報データストリームは、典型的には、データサイズに関して中間符号化データストリーム全体の1/200から1/2000部分の範囲にわたる。分割/結

合情報データストリームは、複数のデータブロック及び／またはデータパケットのサイズ及び／または相対位置を定義するため、中間符号化データストリームの最も重要な部分の1つである。いくつかの実施形態では、非クリティカルデータストリームの復号は、複数のデータブロック及び／またはデータパケットのサイズが分かった後にのみ行うことができることが多い。異なるサイズのデータブロック及び／またはデータパケットの符号化された情報が異なるデータストリームに別々に供給される他の実施形態では、非クリティカルデータストリームの復号は、これらのデータブロック及び／またはデータパケットの相対位置が知られているときのみ可能である。

【0103】

さらに、GMVC（登録商標）コーディングソリューションは、複数のデータブロック及び／またはデータパケットに対して1つ又は複数のエンコード方法を実行するので、エンコードに使用される1つ又は複数のエンコード方法を示す情報を含むデータストリームを生成する複数のデータブロック及び／またはデータパケットの情報を含む。以下、このデータストリームを「符号化方式データストリーム」と呼ぶ。符号化方法データストリームは、一般に、サイズに関して中間符号化データストリーム全体の1／100から1／1000部分の範囲であり、中間符号化データストリームの最も重要な部分の1つである。

【0104】

任意に、異なる符号化方法のデータストリームが、異なるサイズのデータブロック及び／またはデータパケットに対して生成される。

【0105】

さらに、任意に、入力データ（D1）は、例えば入力データ（D1）の内容及び所望の符号化品質に基づいて、異なるサイズのデータブロック及び／またはデータパケットに分割される。典型的には、より良好な符号化品質のために、入力データ（D1）は、より小さいサイズのデータブロック及び／またはデータパケットに分割され、逆変換もまた同様である。

【0106】

分割／結合情報データストリーム及び符号化方法データストリームとは別に、GMVC（登録商標）符号化ソリューションは、例えば、画像データあるいはビデオデータ内のデータブロック及び／またはデータパケットの少なくとも部分的な再発に関連する他のデータストリームを生成する。他のデータストリームは、通常、複数のデータブロック及び／またはデータパケット内のデータ要素のデータ値を含む。しかし、これらの他のデータストリームは、データブロック及び／またはデータパケットのサイズ及び相対位置、ならびにデータブロック及び／またはデータパケットの情報を符号化するために使用される符号化方法に関する情報を提供しない。

【0107】

したがって、スプリット／結合情報データストリーム及び符号化方法データストリームは、エンコーダ110によって実行される符号化処理に不可欠かつ重要であり、暗号化プロセスを介して一緒にまたは個別に保護される。結果として、すべてのデータストリームが暗号化される既知の従来技術の解決法と比較として、コンピューティングリソース及び処理エネルギーの1／100から1／1000部分のみが消費される。したがって、利用可能な専用暗号化回路があるかどうかにかかわらず、暗号化プロセスは非常に高速である。

【0108】

さらに、分割／結合情報データストリーム及び／または符号化方法データストリームが暗号化されている場合、不正な盗聴をする第三者は、他のデータストリームをどのように使用すべきか、及びデータブロック及び／またはデータパケットを配置する必要がある。

【0109】

しかし、データブロック及び／またはデータパケットが同じサイズであり、したがって、複数の符号化方法がデータブロック及び／またはデータパケットを符号化する際に使用されない状況が生じる可能性がある。データブロック及び／またはデータパケットは既に

所定の最小／最大サイズを有しているので、データブロック及び／またはデータパケットが分割及び／または結合されないこともあり、暗号化される情報を結合する。この種の状況では、悪意のある第三者が、データブロック及び／またはデータパケットをどのようにどこに配置するかを解読する可能性がある。したがって、本開示の実施形態では、代替的な選択肢が任意に採用される。暗号化されるべき任意のストリームは、複数のエントロピー符号化方法及び複数のエントロピー符号化されたデータブロック及び／またはデータパケットの長さに関連し、長さは複数のデータブロック及び／またはデータパケットの長さとは異なるエントロピー符号化したものが適用される。

【0110】

実際に、GMVC（登録商標）コーディングソリューションが複数のデータブロック及び／またはデータパケットに対して1つ以上のエントロピーを示す情報を含む別のデータストリームを生成する複数のデータブロック及び／またはデータパケットを複数のエントロピー符号化データブロック及び／またはデータパケットにエントロピー符号化するために使用される符号化方法、このデータストリームは、以下、「エントロピー符号化方法データストリーム」と呼ばれる。このエントロピー符号化方法のデータストリームは、典型的には、サイズに関して中間符号化されたデータストリーム全体の1／1000未満の部分を含み、したがって、本開示の実施形態に従った前述の方法において効率的に使用され得る。

【0111】

さらに、GMVC（登録商標）コーディングソリューションは、複数のデータブロック及び／またはデータパケットに対して1つ以上のエントロピー符号化方法を実行するので、GMVC（登録商標）コーディングソリューションは、複数のデータブロックの長さを示す情報エントロピー符号化されたデータストリーム内のエントロピー符号化されたデータブロック及び／またはデータパケットを含む。このデータストリームは、以下、「エントロピー符号化データ長ストリーム」と呼ばれる。エントロピー符号化データの長さは通常、元のデータの長さとは異なるため、第三者が暗号化されていないデータを再構築しようとすることは不可能である。さらに、長さ情報のサイズは、実際のデータと比較して、典型的には非常に小さいので、データ全体を暗号化するのではなく、使用された1つ以上のエントロピー符号化方法を示す情報とともに、長さ情報のみを暗号化することが有益である。

【0112】

多くの場合、エントロピー符号化に先行するデータの長さは既に知られているが、時にはそれが暗号化される中間符号化データストリームに情報を含めることによってデコーダに供給される必要があることを理解されるべきである他のデータやその内容とは無関係に復号を実行することができる。さらに、エントロピー符号化されたデータの長さは、元のデータの長さ（すなわち、前のエントロピー符号化）とエントロピー符号化されたデータとの間の差として表現／伝達されても、しばしば有益ではない。代わりに、単純化し、データ量を低く抑えるために、その情報を実際の長さ情報として配信することがしばしば有益である。ここでは、画像データ（D1）が前述のGMVC（登録商標）符号化ソリューションで符号化され、中間符号化データストリーム全体から分割／結合情報データストリームと符号化／復号化データストリームのみが符号化され、メソッドデータストリームは、RSAで作成された非常に強力な暗号化キーで符号化され暗号化されたデータ（E2）が生成される。RSAは、よく知られている公開暗号化アルゴリズムである。さらに、この例では、符号化され暗号化されたデータ（E2）へのアクセスを有する不正な盗聴をする第三者が、暗号化されたデータストリーム及び他のデータストリームを符号化され暗号化されたデータ（E2）の解読を試みると仮定する。さらに、画像データ（D1）がGMVC（登録商標）コーディングソリューションでエンコードされているため、不正な盗聴をする第三者が画像データ（D1）のフォーマットを知っていると仮定する。結果として、不正な盗聴をする第三者は、符号化され暗号化されたデータ（E2）の99／100から999／1000部分までの範囲の他のすべてのデータストリームを解凍することができ

る。しかし、不正な盗聴をする第三者は、暗号化されたデータストリームを解読することができず、したがって、符号化され暗号化されたデータ（E 2）を解読することができない。

【0113】

理論的には、悪意のある第三者が、すべての可能な符号化方法の選択肢に対してすべての可能な分割／結合の選択肢を試みるように符号化され暗号化されたデータ（E 2）を解読しようとするのが可能である。しかし、そのような場合、暗号化を破り、符号化され暗号化されたデータ（E 2）を解読しようとする際に必要とされるコンピューティングリソースの量及び時間が相当になり、暗号解読者に新しい挑戦を提示する。

【0114】

さらに、エンコーダ110は、符号化され暗号化されたデータ（E 2）をデータベース（図1には図示せず）に格納するためのデータサーバ及び／またはデータストレージ（図1には図示せず）に通信するように動作可能である。データサーバ及び／またはデータストレージは、符号化され暗号化されたデータ（E 2）を続いて復号化するために、エンコーダ110と有益な互換性を有するデコーダ120にアクセス可能に構成される。

【0115】

さらに、任意に、エンコーダ110は、少なくとも1つのキー及び／またはIVをデータサーバ及び／またはデータベースに収納するためのデータ記憶装置に通信するように動作可能である。

【0116】

いくつかの例では、デコーダ120は、任意に、データサーバ及び／またはデータストレージから符号化され暗号化されたデータ（E 2）にアクセスするように動作可能である。さらに、任意に、デコーダ120は、データサーバ及び／またはデータストレージ及び／または別のデータサーバから少なくとも1つのキー及び／またはデータストレージ及び／または別のデータサーバから少なくとも1つのキー及び／またはIVにアクセスするように動作可能である。

【0117】

別の例では、エンコーダ110は、通信ネットワークまたは直接接続を介して、符号化され暗号化されたデータ（E 2）をデコーダ120に流すように任意に動作可能である。さらに、ハードウェアベースまたはソフトウェアベースのエンコーダを備えたデバイスは、ハードウェアベースまたはソフトウェアベースのデコーダを備えた別のデバイスと直接通信することもできることに留意されたい。本開示の実施形態は、例えば、特定用途向け集積回路（ASIC）及び／またはビアを介して、フィールドプログラマブルゲートアレイ（FPGA）を使用するように、コンピューティング命令を実行するように動作可能なコンピューティングハードウェアを利用するものとして説明されている。そのようなハードウェア実装は、例えば電離放射線被曝の影響を受けやすい装置、例えば衛星などの宇宙機関に非常に強固な暗号化を実装する場合にも有用である。

【0118】

さらに他の代表的な例では、デコーダ120は、ハードドライブ及びソリッドステートドライブ（SSD）などの非一時的（すなわち非過渡的）コンピュータ可読記憶媒体から符号化され暗号化されたデータ（E 2）を取り戻せるように任意に実施される。

【0119】

さらに、エンコーダ110のデータ処理部は、符号化され暗号化されたデータ（E 2）のその後の解読及び復号に使用するために、エンコーダ110からデコーダ120への少なくとも1つのキーの配信を行うように構成することができる。任意に、少なくとも1つのキーは、エンコーダ110からデコーダ120に、それぞれの着用者の間で手動で配信される。あるいは、任意に、少なくとも1つのキーは、例えば、Pretty Good Privacy（PGP）、GNU Privacy Guard（GnuPG）、または他の任意の適切な方法を使用して暗号化された電子メールを介して、またはそれに類するものである。さらに代替的に、任意の、少なくとも1つのキーは、暗号化された通信

接続を介してエンコーダ110からデコーダ120に供給される。任意に、暗号化された通信接続は、SSL (Secure Sockets Layer) / TLS (Transport Layer Security) を介して実装される。

【0120】

デコーダ120は、符号化され暗号化されたデータ(E2)を処理して、対応する解読化され復号化されたデータ(D3)を生成するためのデータ処理部を有する。任意に、デコーダ120のデータ処理部は、後で詳細に説明するようにプログラム命令を実行するように動作可能な少なくとも1つのRISCプロセッサを使用することによって実施される。そのようなRISCプロセッサは、比較的簡単な連結演算を非常に高速で実行することができ、例えばリアルタイムストリーム形式で提供されるデータを復号するのに適している。ストリーミング形式で提供されるこのようなデータは、例えば、ビデオ情報、遠隔監視ビデオ情報及び/またはビデオ会議情報を含む。

【0121】

任意に、デコーダ120のデータ処理部は、符号化及び暗号化された1次元データ、符号化及び暗号化された多次元データ、符号化及び暗号化された多次元データ、エンコードされ暗号化されたテキストデータ、エンコードされ暗号化されたバイナリデータ、エンコードされ暗号化されたセンサデータ、エンコードされ暗号化されたオーディオデータ、エンコードされ暗号化された画像データのうち少なくとも1つの形態で提供される符号化され暗号化されたデータ(E2)を解読化し復号化するように動作可能である。

【0122】

デコーダ120のデータ処理部は、符号化され暗号化されたデータ(E2)を処理して、1つ以上または複数の暗号化されたサブ部分及びその1つ以上の暗号化されていないサブ部分を決定するように動作可能である。符号化され暗号化されたデータ(E2)の1つ以上の暗号化されていないサブ部分は、クリティカルではないデータストリーム、すなわち複数のデータブロック及び/またはデータパケットの符号化された情報を含む。

【0123】

任意に、暗号化されたサブ部分の決定は、前述の第1バイトに基づいて行われる。あるいは、随意的に、決定は、暗号化に関する情報及び採用されたエントロピー符号化方法を含むエントロピー符号化方法のバイト及び/またはワードにおける前述のMSBに基づいて行うことができる。さらに代替的には、暗号化及び暗号化されたデータストリームが符号化され暗号化されたデータ(E2)に含まれる順序の知識に基づいて決定が行われる。さらに、代替的には、随意的に、決定は、どのデータストリームが符号化された情報を含む、どのデータストリームが符号化された情報を含まないかを示す前述のフラグビットに基づいて行われる。

【0124】

任意に、デコーダ120のデータ処理部には、解読化され復号化されたデータ(D3)を生成するために使用される少なくとも1つのキーが供給される。任意に、少なくとも1つのキーを使用して、デコーダ120のデータ処理部は、1つ以上の暗号化されたサブ部分を復号して、サイズ、相対位置、及び/または1つ以上の符号化方法を決定するように動作可能である。複数のデータブロック及び/またはデータパケットを受信する。任意に、デコーダ120のデータ処理部はまた、複数のデータブロック及び/またはデータパケットに関連する1つ以上のエントロピー符号化方法を決定するように動作可能である。

【0125】

任意に、デコーダ120のデータ処理部は、少なくとも1つのキーと組み合わせて少なくとも1つの初期化ベクトル(「Init Vector」、IV)を使用して1つ以上の暗号化されたサブ部分を復号するように動作可能である。前述のように、少なくとも1つの初期化ベクトルは、動作中にデコーダ120に供給される。

【0126】

さらに、任意に、1つ以上の暗号化されたサブ部分が、少なくとも1つの圧縮されたデータストリームの形式で提供される。そのような場合、デコーダ120のデータ処理部は

、少なくとも1つの圧縮データストリームの第1バイトから、少なくとも1つの圧縮データストリームに関連するエントロピー符号化方法を決定するために任意に動作可能である。

【0127】

さらに、任意に、少なくとも1つの圧縮されたデータストリームの長さを示す情報が、少なくとも1つの圧縮されたデータストリームの先頭に、例えばその第1バイトの後に提供される。その結果、デコーダ120のデータ処理には、少なくとも1つの圧縮されたデータストリームの開始のみを解読することによって復号化されるデータの量に関する情報が解読されることなく提供される。これは、並列処理、すなわちデータストリームの並列復号の目的に特に有益である。

【0128】

デコーダ120のデータ処理部は、次に、エントロピー符号化方法の逆変換を適用して、少なくとも1つの圧縮ストリームを解凍して、前述のサイズ、前述の相対位置、及び関連する1つ以上の符号化方法を決定するように、複数のデータブロック及び/またはデータパケットを受信する。

【0129】

次いで、デコーダ120のデータ処理部は、複数のデータブロック及び/またはデータパケットの符号化情報を復号化するために、複数のデータブロック及び/またはデータパケットの符号化情報に1つ以上の符号化方法の逆変換を適用するように動作可能であり、複数の復号データブロック及び/またはデータパケットを生成することができる。任意に、デコーダ120のデータ処理部は、1つ以上の符号化方法の逆変換を適用する前に、1つ以上のエントロピー符号化データブロック及び/または1つ以上の非暗号化サブ部分に含まれるデータパケットに1つ以上のエントロピー符号化方法の逆変換を適用するように動作可能である。

【0130】

その後、デコーダ120のデータ処理部は、サイズ及び/または相対位置に基づいて複数の復号化データブロック及び/またはデータパケットを組み立てて、解読化され復号化されたデータ(D3)を生成するように動作可能である。

【0131】

前述のサイズ、前述の相対位置及び/または複数のデータブロック及び/またはデータパケットに関連する1つ以上の符号化方法を示す情報は、暗号化されたサブ部分に含まれている方法であると理解されるであろう。したがって、複数のデータブロック及び/またはデータパケットの符号化された情報を復号して解読化され復号化されたデータ(D3)を生成することは、符号化され暗号化されたデータ(E2)の暗号化された部分を正しく復号する必要がある。

【0132】

図1の実施形態は単なる一例であり、本明細書の特許請求の範囲を不当に限定するものではない。コーデック130の特定の指定は一例として提供され、コーデック130をエンコーダ及びデコーダの特定の数、タイプ、または配置に限定するものとして解釈されるべきではないことを理解されたい。当業者であれば、本開示の実施形態の多くの変形形態、代替形態及び変更形態を認識するであろう。

【0133】

任意に、コーデック130は、単一の装置内に実装される。あるいは、任意に、コーデック130は、複数のデバイス間で効果的に実装される。任意に、コーデック130は、例えば1つ以上の特定用途向け集積回路(ASIC)の使用を介してカスタム設計デジタルハードウェアとして実装される。あるいは、またはさらに、コーデック130は、ハードウェアを計算する際に実行可能なコンピュータソフトウェア命令で実施される。

【0134】

コーデック130は、データコーデック、オーディオコーデック、イメージコーデック及び/またはビデオコーデックのうちの少なくとも1つとして実装されるが、これに限定

されない。

【0135】

さらに、コーデック130は、データ転送に必要なネットワーク帯域幅を大幅に節約し、データ転送のためのSSL/TLSなどの暗号化された通信接続を必要とせず、送信者と受信者との間の安全な通信を提供するように実装することができる。一例では、コーデック130は、データ転送のためにウェブブラウザ及びワールドワイドウェブ（www）サーバで使用されるハイパーテキスト転送プロトコル（HTTP）などの要求・応答型通信に基づくシステムに実装することができる。

【0136】

将来的には、「ブルートフォース攻撃」技術を使用することで、今日暗号化されたデータを分解して解読することは可能であるが、将来の暗号化アルゴリズムは現在の暗号化アルゴリズムよりも強力な暗号化キーを生成し、データの暗号化を確実なものとする。

【0137】

「ブルートフォース攻撃」技術に加えて、「バיקリック攻撃」、「関連キー攻撃」、「パディング・オラクル攻撃」、「長さ拡張攻撃」技術など他のよく知られている攻撃手法があるが、これらの技術は、エンコーダ110によって実行される暗号化を破壊することに本質的に失敗する。

【0138】

説明の目的のために、エンコーダ110で実行されるような暗号化プロセスの技術的な例が次に提供される。この例では、以下のステップに従って拡張された暗号化キーを有するCBC（Cipher Block Chaining）モードの対称Advanced Encryption Standard（AES）暗号化アルゴリズムを使用することによって、暗号化されていない平文データストリームを暗号化するための1つの効果的なモデルが示される。

1. 2つの暗号キー、すなわちキー1及びキー2を取得または生成する。
2. AES CBCの暗合擬似ランダム初期化ベクトル（IV）バイトの生成。
3. AES CBC関数を用いて、平文バイト（すなわち、クリティカルデータストリームの少なくとも1つ）を暗号文バイト（すなわち、すくなくとも1つの中間暗号化データストリーム）に暗号化する。
4. IVと暗号文バイトを結合する。
5. キー2とCipher textでHMAC関数を使用してメッセージ認識コード（MAC）バイトを作成する。そして、
6. MACストリーム及びテキストバイトをデータストリーム、すなわち、符号化され暗号化されたデータ（E2）の1つ以上の暗号化されたサブ部分に書き込む。

【0139】

さらに、前述のアルゴリズムのための擬似コードは、以下のように提示される。

```
Key1=KeyStretch(GetKey())
Key2=KeyStretch(GetKey())
IV=Random()
CipherText=IV+AES(Key1,IV,Plaintext)
MAC=HMAC(Key2,CipherText)
DATA=MAC+CipherText
```

【0140】

上記の例では、2つの強化されたキーが「キーストレッチ」技術を使用して作成されている。「キーストレッチ」技術は、通常、一方向ダイジェストアルゴリズム、すなわちハッシュアルゴリズムを介して何千もの時間を暗号化するためのパスワードを保護するための十分な順列が作成される。

【0141】

その後、対応するランダム初期化ベクトル（IV）バイトがCBCモード用に生成される。これらのIVバイトは、次に、スクランブルされ、プレーンテキストバイトの1つ以

上の第1バイト、すなわち暗号化されるクリティカルデータストリームの少なくとも1つに混合される。クリティカルデータストリームの少なくとも1つは、CBCモードの対称AES暗号化アルゴリズムを使用して、複数の拡張キー及びIVバイトで暗号化される。

【0142】

IVバイトを使用することは、例えばクリティカルデータストリームの少なくとも1つが多く冗長データを含む場合に得られる暗号化の保護の程度を向上させるために特に有益である。結果として、侵入者は、一連の情報が最初から最後まで破壊される前に、少なくとも1つの重要なデータストリームを解読することができない。

【0143】

最後に、メッセージ認識コード(MAC)バイトが暗号文バイト、すなわち少なくとも1つの中間暗号化データストリームに挿入される。これにより、クリティカルデータストリームの少なくとも1つにおそらく発生する冗長平文によって引き起こされる可能性のある同一の暗号文が防止され、例えば、「ハディングオラクル攻撃」技術を介して暗号化が破られることも防止される。これはまた、符号化され暗号化されたデータ(E2)の1つ以上の暗号化された部分の完全性が損われないことを保証する。

【0144】

図2を参照すると、本開示の一実施形態による、入力データ(D1)の符号化及び暗号化して対応する符号化され暗号化されたデータ(E2)を生成する第1の方法のステップを示すフローチャートが提供される。この方法は、例えば上述したように、ハードウェア、ソフトウェア、またはそれらの組み合わせで実施され得る一連のステップを表す論理フローのステップの集合として示される。

【0145】

説明の目的のために、第1の方法を、図1に示すエンコーダ110を参照して以下に説明する。

【0146】

ステップ202において、エンコーダ110のデータ処理部は、入力データ(D1)を符号化して、複数の中間符号化データストリームを生成する。

【0147】

任意に、ステップ202は、エンコーダ110のデータ処理部が複数の分割及び/または結合演算を使用して入力データ(D1)を複数のデータブロック及び/またはデータに分割及び結合するサブステップを含む。複数のデータブロック及び/またはデータパケットの情報を複数の中間符号化データストリームの少なくとも1つに符号化するための1つ又は複数の符号化方法を使用する。

【0148】

任意に、ステップ202は、エンコーダ110のデータ処理部が、複数のデータブロック及び/またはデータパケットを複数のエントロピー符号化データブロックに圧縮するための1つ又は複数のエントロピー符号化方法を使用するサブステップと、またはそれらの方法のインプリメンテーションを示す情報が、エントロピー符号化されたデータの長さ及び任意にオリジナルの長さと共に、複数の中間符号化データストリームの少なくとも1つに含まれるデータ；それらの方法、またはそれらの方法の実施を示す情報、ならびに長さ情報は、有益には、それら自体の中間データストリームに含まれる。そのようなエントロピー符号化は、1つ以上のデータブロック及び/またはデータパケットが前述の符号化方法を使用して符号化された後に任意に実行される。任意に、このフェーズにおいて、生成された中間符号化データストリームは、それらが暗号化される前にさらに圧縮され得る。次に、ステップ204で、エンコーダ110のデータ処理部は、少なくとも1つの中間暗号化データストリームを生成するために、1つ以上の暗号化アルゴリズムを使用して、複数の中間符号化データストリームの少なくとも1つのクリティカルデータストリームを暗号化する。任意に、少なくとも1つのクリティカルデータストリームは、複数の分割及び/または結合動作、1つ以上の符号化方法、1つ以上のエントロピー符号化方法、及び/または複数のエントロピー符号化データブロック及び/またはデータパケット、及び/ま

たはエントロピー符号化が適用される前のデータブロック及び／またはパケットの長さのうち少なくとも1つを示す情報を含む。

【0149】

任意に、ステップ204において、エンコーダ110のデータ処理部は、少なくとも1つのクリティカルデータストリームを暗号化するとき少なくとも1つのキーと共に少なくとも1つの初期化ベクトル（「Init Vector」：IV）を適用する。

【0150】

ステップ204の暗号化処理については、図3を参照して説明した。

【0151】

続いて、ステップ206において、エンコーダ110のデータ処理部は、複数の中間符号化データストリームの暗号化されていない部分、すなわち、複数のデータブロック及び／またはデータパケットの符号化された情報は少なくとも符号化され暗号化されたデータ（E2）を生成する。

【0152】

ステップ202～206は例示的なものに過ぎず、本明細書の特許請求の範囲から逸脱することなく、1つ以上のステップが追加され、1つ以上のステップが削除されるか、または1つ以上のステップが異なるシーケンスで提供される。例えば、必要に応じて、本方法は、エンコーダ110のデータ処理部が、少なくとも1つのクリティカルデータストリームを暗号化に先立って少なくとも1つの圧縮データストリームに圧縮する追加のステップを含む。任意に、追加のステップにおいて、エンコーダ110のデータ処理部は、少なくとも1つの重要なデータストリームを圧縮するために使用されるエントロピー符号化方法を第1バイトが記述するように、少なくとも1つの圧縮データストリームの第1バイトを計算する。

【0153】

さらに、ステップ204は、任意に、対称AES暗号化アルゴリズムのCBCモードを使用して実行される。ステップ204は、ランダムに生成されたIVを使用して任意に実行され、少なくとも1つのキーと併合される。ステップ204は、IVが少なくとも1つのクリティカルデータストリームを暗号化するために使用されるか否かに関わらず、CBCモードが使用されるかどうかに関わらず、他の暗号化アルゴリズムを使用して実行され得ることが理解される。

【0154】

あるいは、任意に、入力データ（D1）は既に符号化されている。そのような場合、この方法は、少なくとも1つの重要なデータストリームが識別され、次に暗号化される代替ステップで開始する。そのような識別は、入力データ（D1）をストリームごとに処理し、その中の1つ以上の重要なデータストリームを識別することによって任意に実行される。このプロセスは、入力データ（D1）の各データストリームが、使用される符号化方法の情報ならびにそのデータストリームの長さを含むとき、迅速かつ効率的である。

【0155】

図3は、本開示の一実施形態による、暗号化プロセスのステップの概略図である。

【0156】

ステップ302において、エンコーダ110のデータ処理部は、複数の中間符号化データストリームの内容を読み取りまたは受信する。

【0157】

ステップ304において、エンコーダ110のデータ処理部は、複数の中間符号化データストリームの第1または次のデータストリームを処理する。

【0158】

ステップ306において、エンコーダ110のデータ処理部は、ステップ304で処理された第1または次のデータストリームが暗号化される必要があるか否かを判定する。

【0159】

ステップ306で、第1または次のデータストリームが暗号化される必要があると判定

された場合、ステップ308が実行される。そうでない場合には、第1または次のデータストリームが暗号化される必要がないと判定された場合、ステップ310が実行される。

【0160】

ステップ308において、エンコーダ110のデータ処理部は、第1または次のデータストリームを暗号化する。ステップ308にしたがって、エンコーダ110のデータ処理部は、任意に、暗号化情報、すなわちステップ308で使用される1つ以上¹の暗号化アルゴリズムを示す情報を書き込みまたは送信する。

【0161】

その後、ステップ310において、エンコーダ110のデータ処理部は、暗号化されたデータストリームを暗号化されたデータストリームに書き込みまたは送信して、符号化され暗号化されたデータ(E2)に含める。

【0162】

第1または次のデータストリームが暗号化されていないとき、エンコーダ110のデータ処理部は、ステップ310で、第1または次のデータストリームをそのまま、または送信する。

【0163】

次に、ステップ312において、エンコーダ110のデータ処理部は、入力データ(D1)に次のデータストリームが存在するか否かを判定する。次のデータストリームが存在すると判定された場合、ステップ302で暗号化プロセスが再開する。一方、入力データ(D1)に次のデータストリームが存在しないと判定された場合、暗号化処理は停止する。

【0164】

ステップ302～312は例示的なものに過ぎず、本明細書の特許請求の範囲から逸脱することなく、1つ以上¹のステップが追加され、1つ以上¹のステップが削除されるか、または1つ以上¹のステップが異なるシーケンスで提供される。

【0165】

本開示の実施形態は、実行可能な処理ハードウェアを含むコンピュータ化された装置によって実行可能な、コンピュータ可読命令が記憶された非一時的(すなわち非過渡的)コンピュータ可読記憶媒体を含むコンピュータプログラム製品を提供する。図2に関連して説明した第1の方法は、図2及び図3を参照する。コンピュータ可読命令は、例えば、「App Store」からコンピュータ化されたデバイスに、ソフトウェアアプリケーションストアから任意にダウンロード可能である。

【0166】

図4は、本開示の一実施形態による、符号化され暗号化されたデータ(E2)を解読及び復号して対応する解読化され復号化されたデータ(D3)を生成する第2の方法のステップを示すフローチャートの概略図である。この方法は、ハードウェア、ソフトウェア、またはそれらの組み合わせで実施することができる一連のステップを表す論理フロー図のステップの集合として示されている。

【0167】

説明の目的のために、第2の方法を、図1に示すデコーダ120を参照して次に説明する。

【0168】

ステップ402において、デコーダ120のデータ処理部は、符号化され暗号化されたデータ(E2)を処理して、1つ以上¹の暗号化されたサブ部分及びその1つ以上の暗号化されていないサブ部分を決定する。符号化され暗号化されたデータ(E2)の1つ以上の暗号化されていない部分は、重要ではないデータストリーム、すなわち複数のデータブロック及び/またはデータパケットの符号化された情報を含む。

【0169】

ステップ404において、デコーダ120のデータ処理部は、符号化され暗号化されたデータ(E2)の1つ以上¹の暗号化された部分を復号して、サイズ、相対位置、及び/ま

たは複数のデータブロック及び／またはデータパケットを含む。任意に、ステップ404において、デコーダ120のデータ処理部は、複数のデータブロック及び／またはデータパケットに関連する1つ以上のエントロピー符号化方法も決定する。

【0170】

任意に、ステップ404において、デコーダ120のデータ処理部は、少なくとも1つのキーと組み合わせて少なくとも1つの初期化ベクトル（「Init Vector」、IV）を使用して、1つ以上の暗号化されたサブ部分を復号する。

【0171】

任意に、少なくとも1つのキー及び／または少なくとも1つの初期化ベクトルは、動作中にデコーダ120に供給される。

【0172】

ステップ404の解読プロセスは、図5と共に説明されている。

【0173】

次に、ステップ406において、デコーダ120のデータ処理部は、ステップ404で決定された1つ以上の符号化方法の逆変換を、複数のデータブロック及び／またはデータパケットの情報を受信し、複数の復号データブロック及び／またはデータパケットを生成する。必要に応じて、ステップ406において、デコーダ120のデータ処理部は、加えられたエントロピー符号化方法の情報ならびにエントロピー符号化データブロック及び／またはパケットに関する長さ情報も抽出し、1つ以上の符号化され暗号化されたデータ（E2）の1つ以上の暗号化されていないサブ部分に含まれる複数のエントロピー符号化されたデータブロック及び／またはデータパケットにエントロピー符号化方法を適用する。中間符号化データストリームがさらに暗号化される前に圧縮されている場合、デコーダ120は、1つ以上の対応する逆変換データ圧縮解除方法を適用する。

【0174】

続いて、ステップ408において、デコーダ120のデータ処理部は、ステップ404で決定されたサイズ及び／または相対位置に基づいて、複数の復号データブロック及び／またはデータパケットを組み立てて、解読化され復号化されたデータ（D3）を生成する。

【0175】

ステップ402～408は例示的なものに過ぎず、本明細書の特許請求の範囲から逸脱することなく、1つ以上のステップが追加され、1つ以上のステップが削除されるか、または1つ以上のステップが異なるシーケンスで提供される。例えば、任意に、この方法は、デコーダ120のデータ処理部が、1つ以上の暗号化された部分の少なくとも1つの圧縮されたデータストリームの第1バイトからエントロピー符号化方法を決定する追加のステップを含む。少なくとも1つの圧縮されたデータストリームに関連する。任意に、追加のステップにおいて、デコーダ120のデータ処理部は、エントロピー符号化方法の逆変換を適用して、少なくとも1つの圧縮ストリームを解凍して、サイズ、相対位置、及び複数のデータブロック及び／またはデータパケットを受信する。

【0176】

さらに、ステップ404は、対称AES暗号化アルゴリズムのCBCモードを使用して任意に実行される。ステップ404は、ランダムに生成されたIVを使用して任意に実行され、少なくとも1つのキーと併合される。ステップ404は、IVが1つ以上の暗号化された副部分を解読するために使用されるかどうかに関わらず、かつCBCモードが使用されるかどうかに関わらず、他の解読アルゴリズムを使用して実行され得ることが理解される。

【0177】

図5は、本開示の一実施形態による解読プロセスのステップの概略図である。

【0178】

ステップ502において、デコーダ120のデータ処理部は、符号化され暗号化されたデータ（E2）の内容を読み取るか、または受け取る。

【0179】

ステップ504において、デコーダ120のデータ処理部は、符号化され暗号化されたデータ(E2)に含まれる第1または次のデータストリームを処理する。

【0180】

ステップ506において、デコーダ120のデータ処理部は、第1のまたは次のデータストリームが暗号化されているか否かを判定する。任意に、ステップ506において、上記の第1バイト、エントロピー符号化方法のバイト及び/またはワードにおける上記の最上位ビット(MSB)、暗号化されていない及び暗号化されたデータストリームの順序、及び/または前述のフラグビットを含む。

【0181】

ステップ506において、第1または次のデータストリームが暗号化されていると判定された場合、ステップ508が実行される。そうでない場合、第1または次のデータストリームが暗号化されていないと判定された場合、ステップ510が実行される。

【0182】

ステップ508において、デコーダ120のデータ処理部は、第1のまたは次のデータストリームを解読する。ステップ508によれば、デコーダ120のデータ処理部は、暗号化情報、すなわち、第1または次のデータストリームに関連する1つ以上の暗号化アルゴリズムを示す情報を随意に読み取るか、または受け取る。

【0183】

その後、ステップ510において、デコーダ120のデータ処理部は、解読されたデータストリームを書き込みまたは送信する。

【0184】

第1または次のデータストリームが暗号化されていない場合、デコーダ120のデータ処理部は、ステップ510において、第1または次のデータストリームをそのまま、または送信する。

【0185】

次に、ステップ512において、デコーダ120のデータ処理部は、符号化され暗号化されたデータ(E2)に次のデータストリームが存在するか否かを判定する。次のデータストリームが存在すると判定された場合、復号化プロセスはステップ502で再開する。そうでない場合には、符号化され暗号化されたデータ(E2)に次のデータストリームが存在しないと判定された場合、復号化プロセスは停止する。

【0186】

ステップ502～512は例示的なものに過ぎず、本明細書の特許請求の範囲から逸脱することなく、1つ以上のステップが追加され、1つ以上のステップが削除されるか、または1つ以上のステップが異なるシーケンスで提供される。

【0187】

本開示の実施形態は、図4及び図5に関連して説明された第2の方法を実行する処理ハードウェアを含むコンピュータ化された装置によって実行可能な、コンピュータ可読命令が記憶された非一時的(すなわち非過渡的)コンピュータ可読記憶媒体を含むコンピュータプログラム製品を提供する。コンピュータ可読命令は、例えば、「App store」からコンピュータ化されたデバイスに、ソフトウェアアプリケーションストアから任意にダウンロード可能である。

【0188】

前述の暗号化方法及び暗号化プロセスは、エンコーダまたは他の対応するプリプロセッサへの実装に適している。同様に、前述の解読方法及び解読プロセスは、デコーダまたは他の対応するプリプロセッサへの実装に適している。前述の方法は、ソフトウェア及び/またはハードワイヤードロジック、例えばASICの使用を介して実施することができる。多くのシステムは、純粋なソフトウェアアプローチよりも少ない電力を使用しながら、暗号化を効率的に実施する現代的なAESのような、暗号化用の専用マイクロチップを有することはよく知られている。上述の方法は、例えば監視組織に対して、第三者の攻撃に

対して対応する強度を有する暗号化を使用する従来技術の手法と比較して、相当な電力及びエネルギーの節約を達成することを可能にする。

【0189】

本開示の実施形態による暗号化方法がソフトウェア実装として実行される場合、そのソフトウェアプロセスを保護されたメモリ空間の全部または部分的に実行することが有益である。そのような予防措置は、マルウェアが暗号化される情報または暗号化プロセスで使用される暗号化キーを読み取る可能性を防ぐのを助ける。これに対応して、そのような場合には、暗号解読は保護されたメモリ空間においても有利に実行される。現行の多くのデバイスが暗号化のための専用マイクロチップを含む場合、または前述のAESのように暗号化に利用可能な別個の命令セットがある場合であっても、本開示による暗号化ソリューションは、暗号化されたデータは完全に保護されたメモリ空間または部分的に保護されたメモリ空間で処理される。後者の場合、暗号化されるプレーンテキストデータは、例えば、使用されている暗号化キーが保護されたメモリ空間で処理される場合、保護されたメモリ空間の外で処理することができる。最も有益なことに、プレーンテキスト情報は、保護されていないメモリにのみ暗号化された形式で存在する。しかしながら、これが不可能な場合は、暗号化の後に保護されていないメモリにそのような状態にならないようにすることが有効である。暗号化されたデータのこの部分は、例えば本開示の実施形態にしたがって、保護されたメモリ内にのみ常に格納されることが有利である。メモリ保護は、現代的なタイプのオペレーティングシステムなど、ほとんどのオペレーティングシステムで実装できるような保護であるが、テクニックとアクセスメカニズムは潜在的に変化する可能性がある。

【0190】

本開示の実施形態に従う方法は、どの暗号化アルゴリズムが使用されるかに関係なく、任意の適切な符号化解決法で実施することができる。その際、前述の方法は暗号化アルゴリズムの動作を変更しない。すなわち、暗号化アルゴリズムによって提供される保護が損われないことを意味する。

【0191】

前述の方法は、非常に高速で効率的な暗号化アルゴリズムを使用することを可能にする。これに関して、前述の方法は、暗号化アルゴリズム自体の内部動作を妨害することなく、効率的に暗号化アルゴリズムを使用する。前述の方法で実装に適した暗号化アルゴリズムの例には、AES、RSA、Twofish、Blowfish、データ暗号化標準（DES）、トリプルDES（3-DES）、Serpent、国際データ暗号化アルゴリズム（IDEA）、MARS、Rivest Cipher 6（RC6）、Camellia、CAST-128、Skipjack、extended Tiny Encryption Algorithm（XTEA）これらの例の名前には登録商標が含まれている。

【0192】

本開示の実施形態に従う前述の方法は、既知の従来技術の方法と比較して、データを保護する非常に高速かつかなり効率的な方法を提供する。特に、符号化されたデータの1つ以上の重要かつ重要な部分だけが暗号化される。例えば、画像またはビデオがプログレッシブGMVC（登録商標）符号化ソリューションで符号化されるとき、符号化されたデータの1/100番目から1/1000番目のみが、より早期に解明されるように、暗号化によって保護される。したがって、このような方法での暗号化の使用は、リアルタイムビデオの転送レートに大きな影響を及ぼさず、いかなる重要な方法でもコンピューティングリソースの消費を増加させるものではないと結論付けることができる。

【0193】

さらに、暗号化プロセスのさらなる利点は、符号化され暗号化されたデータ（E2）が、例えばVPN（Virtual Private Network）トンネリング、Secure Shell（SSH）、またはSSL/TLSプロトコルのように、保護された安全なネットワーク接続で移されることを必要としない。したがって、前述の方法は

、例えば、パブリックインターネットネットワークまたはウェブサービス及びクラウドサービスにおいてテキスト、バイナリ、オーディオ、画像、ビデオ及び他のタイプのデータを送信するための有利なモデルを提供する。

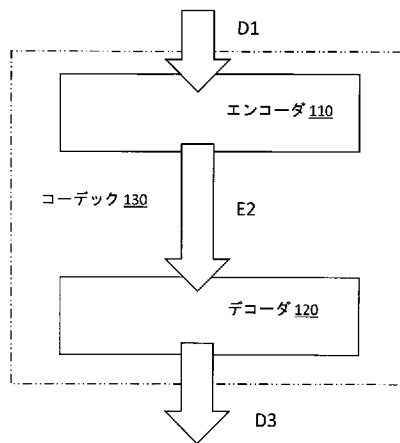
【0194】

本開示の実施形態は、スマートフォン、パーソナルコンピュータ（PC）、オーディオビジュアル装置、カメラ、通信ネットワーク、データ記憶装置、監視システムなどの広範なシステム及び装置で使用することが可能である。地震探知装置、「ブラックボックス」フライトレコーダ、サンプリング技術を使用するデジタル楽器などが含まれるが、これらに限定されない。

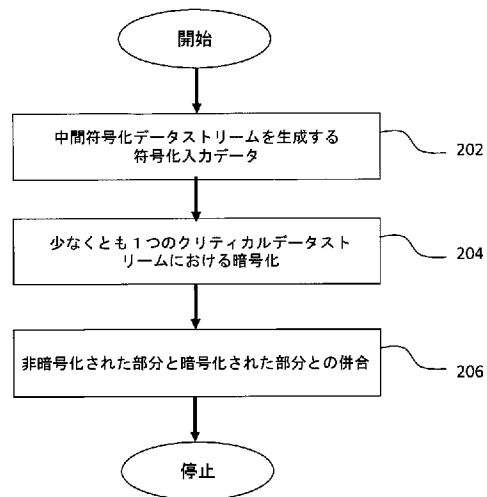
【0195】

上述した本発明の実施形態に対する変更は、添付の請求項によって限定される本発明の範囲から逸脱することなく可能である。本発明を説明しクレームするために使用される「 」、「 」、「 」、「 」、「 」、「 」等の表現は、非排他的に解釈されることを意図しており、明示的に記載されていない構成要素または要素も存在する。単数形への言及はまた、複数形に関連すると解釈されるべきである。添付の特許請求の範囲の括弧内に含まれる数字は、特許請求の範囲の理解を助けることを意図しており、これらの特許請求の範囲によって請求される主題を制限するものと解釈されるべきではない。

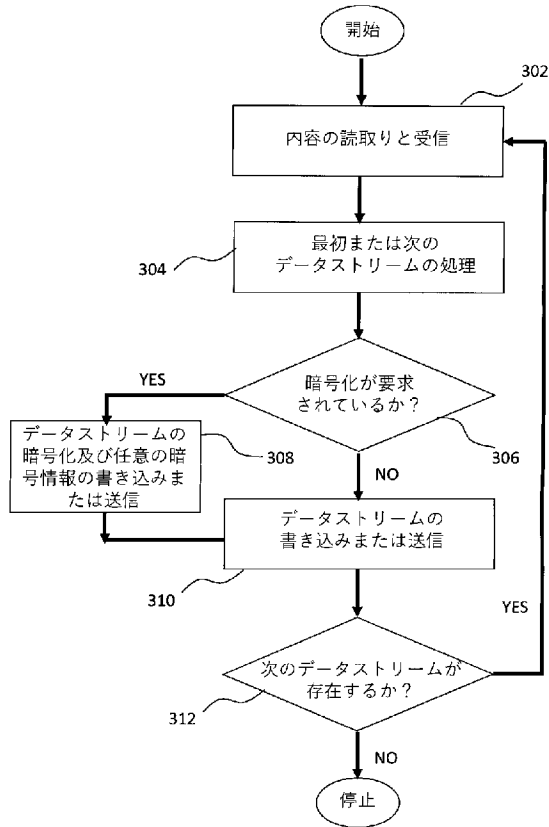
【図1】



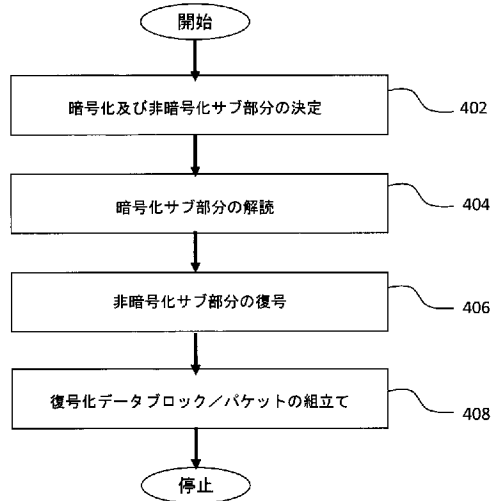
【図2】



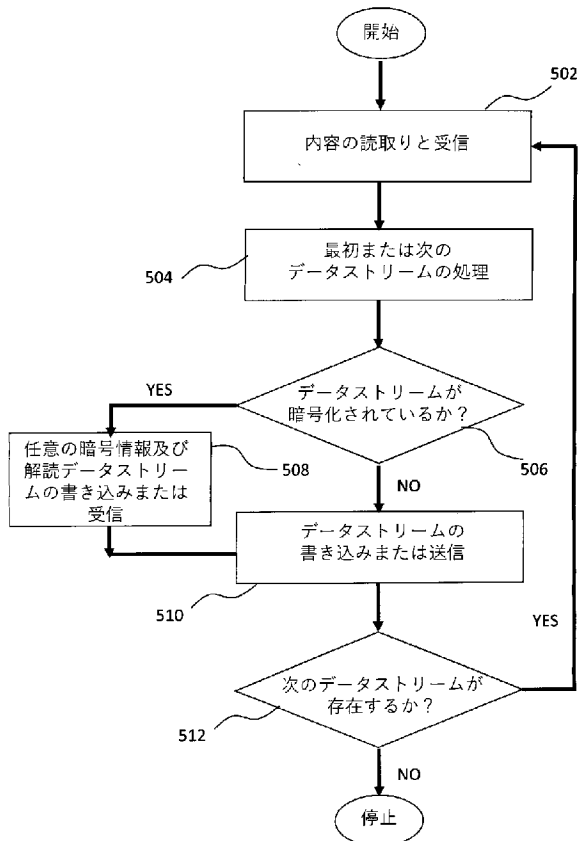
【図3】



【図4】



【図5】



フロントページの続き

発明者 カレヴォ, オッシ
フィンランド共和国, 37800, アカー, ケトゥンハンタ 1

審査官 金沢 史明

参考文献 特開2004-198760 (JP, A)
特表2014-520282 (JP, A)
米国特許出願公開第2004/0081333 (US, A1)
国際公開第2010/150056 (WO, A1)
特開平08-056356 (JP, A)
特開2008-118406 (JP, A)

調査した分野 , DB名
H04L 9/00- 9/38
H04N 21/00-21/858
H03M 7/30
G09C 1/00