(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2017-535123
(P2017-535123A)
(43)公表日　平成29年11月24日(2017.11.24)

(51)Int.Cl.			F I			テーマコード（参考）
H03M	***7/30***	***(2006.01)***	H03M	7/30	Z	5J064
G09C	***1/00***	***(2006.01)***	G09C	1/00	660D	5J104

審査請求 有　予備審査請求 有　（全 67 頁）

(21)出願番号　特願2017-515203 (P2017-515203)
(86)(22)出願日　平成27年9月21日 (2015.9.21)
(85)翻訳文提出日　平成29年5月16日 (2017.5.16)
(86)国際出願番号　PCT/EP2015/025065
(87)国際公開番号　WO2016/041641
(87)国際公開日　平成28年3月24日 (2016.3.24)
(31)優先権主張番号　1416631.8
(32)優先日　平成26年9月19日 (2014.9.19)
(33)優先権主張国　英国 (GB)

(71)出願人　513156386
グルロジック　マイクロシステムズ　オーワイ
Ｇｕｒｕｌｏｇｉｃ　Ｍｉｃｒｏｓｙｓｔｅｍｓ　Ｏｙ
フィンランド共和国　２０１００　トゥルク　リンナンカツ　３４
Ｌｉｎｎａｎｋａｔｕ　３４　２０１００　Ｔｕｒｋｕ　ＦＩＮＬＡＮＤ
(74)代理人　100075409
弁理士　植木　久一
(74)代理人　100129757
弁理士　植木　久彦
(74)代理人　100115082
弁理士　菅河　忠志

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

(57)【要約】
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）を符号化及び暗号化する方法が提供される。入力データ（Ｄ１）は、中間符号化データストリームを生成するために符号化される。中間符号化データストリームは、中間符号化データストリームの１つまたは複数の残りのデータストリームの後続の復号にクリティカルで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。少なくとも１つのクリティカルデータストリームは、１つ以上の暗号化アルゴリズムを使用して暗号化され、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。続いて、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が、少なくとも１つの中間暗号化データストリームと併合されて、符号化され暗号化されたデータ（Ｅ２）が生成される。

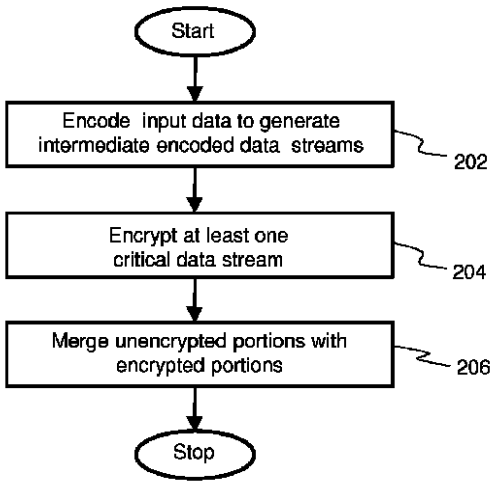


FIG. 2

【特許請求の範囲】
【請求項１】
入力データ（Ｄ１）を符号化し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）であって、以下の処理：
（ａ）データ処理部は、複数の中間符号化データストリームを生成するために入力データ（Ｄ１）を符号化するように動作可能であり、複数の中間符号化データストリームは、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表し、前記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の復号化を行うことと；
（ｂ）前記データ処理部は、少なくとも１つの中間符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ように動作可能であることと；
（ｃ）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）を生成するように動作可能であることと；
を行うように構成される入力データ（Ｄ１）を処理するデータ処理部を備えることを特徴とするエンコーダ（１１０）。
【請求項２】
前記少なくとも１つのクリティカルなデータストリームは、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、前記複数の分割及び／または結合動作のうちの少なくとも１つを示す情報を含む請求項１に記載のエンコーダ（１１０）。前記情報は、複数のデータブロック及び／またはデータパケットの入力データ（Ｄ１）、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つまたは複数の符号化方法、使用される１つまたは複数のエントロピー符号化方法、前記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、及び／または前記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にエントロピー符号化するエントロピー符号化されたデータストリーム、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長さを含む。
【請求項３】
前記データ処理部は、前記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的分析及び／または反復分析を実行して、前記複数のデータブロック及び／またはデータパケットの複数のパラメータを決定するように動作可能である請求項２に記載のエンコーダ（１１０）。前記データ処理部は、複数のデータ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動作可能であり、データ処理部、複数の中間符号化データストリームを生成するための複数のブロック、及び／またはデータパケットを含む。
【請求項４】
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）を処理するように動作可能である請求項１、２、または３に記載のエンコーダ（１１０）。
【請求項５】
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少なくとも１つの圧縮データストリームに圧縮する前に、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圧縮するように動作可能である請求項１、２、３、または４に記載のエンコーダ（１１０）。
【請求項６】
前記データ処理部は、前記少なくとも１つの圧縮データストリームの第１のバイトを計算するように動作可能であり、前記第１バイトは、前記第１バイトが前記第１バイトを圧

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動作可能である請求項５に記載のエンコーダ（１１０）。
【請求項７】
前記データ処理部は、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のバイト及び／またはワードにおける最上位ビット、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、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決定するように動作可能である請求項１から６のいずれかに記載のエンコーダ（１１０）。
【請求項８】
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）を発生する入力データ（Ｄ１）を符号化及び暗号化する方法であって、以下の処理：
（ａ）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データ処理部を動作させることを含み、前記複数の中間符号化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うちの１つ以上の残りのデータストリームのその後の符号化に重要かつ不可欠であり、少なくとも１つの重要な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表すことと；
（ｂ）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つまたは複数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ように前記データ処理部を動作させることと；
（ｃ）前記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）を生成するように前記データ処理部を動作させることと；
を備えることを特徴とする入力データ（Ｄ１）を符号化及び暗号化する方法。
【請求項９】
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、前記入力データ（Ｄ１）を分割及び／または結合するために使用される複数の分割及び／または結合演算を、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符号化するために使用される１つまたは複数の符号化方法、エントロピー符号化に使用される１つまたは複数のエントロピー符号化方法、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複数のエントロピー符号化データブロック及び／または符号化されたデータストリーム、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長さを含む請求項８に記載の方法。
【請求項１０】
（ｄ）前記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、前記複数のデータブロック及び／またはデータパケットを決定することと；
（ｅ）複数のパラメータを使用して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して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１つまたは複数の符号化方法を選択するようにデータ処理部を動作させることと；
を備える請求項９に記載の方法。
【請求項１１】
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８、９、または１０に記載の方法。
【請求項１２】
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前記データ処理部を動作させることを含む請求項８、９、１０、または１１に記載の方法。

【請求項１３】
前記データ処理部を動作させて前記少なくとも１つの圧縮データストリームの第１バイトを計算し、前記第１バイトが前記少なくとも１つの圧縮データストリームの第１バイトを計算し、前記第１バイトが前記少なくとも１つの圧縮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ことを含む、請求項１２に記載の方法。
【請求項１４】
暗号化を定義するために前記データ処理部を動作させることを含み、前記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と、エントロピー符号化方式のバイト及び／またはワードにおける最上位ビット、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暗号化されたデータストリームが含まれる動作、フラグビットを含む請求項８から１３のいずれかに記載の方法。
【請求項１５】
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、
（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つまたは複数の暗号化されたサブ部分及びその１つまたは複数の暗号化されていないサブ部分を決定し、前記１つまたは複数の暗号化されていないサブ部分の符号化された情報は、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み；
（ｉｉ）前記データ処理部は、サイズ及び／または相対位置及び／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つまたは複数の符号化方法を決定するために、１つまたは複数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り；
（ｉｉｉ）前記データ処理部は、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するために、複数の復号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ための、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つまたは複数の符号化方法の逆を適用するように動作可能であり；
（ｉｖ）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、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付けられたサイズ及び／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るように動作可能であることを特徴とするデコーダ（１２０）。
【請求項１６】
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、前記データ処理部が、前記少なくとも１つの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含む請求項１５に記載のデコーダ（１２０）。
【請求項１７】
前記データ処理部は、前記１つまたは複数の暗号化されたサブ部分及び前記１つまたは複数の暗号化されていないサブ部分を、新しいバイトがエントロピー符号化方法のバイト及び／またはワードの最上位ビット、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）、フラグビットに含まれる請求項１５または１６に記載のデコーダ（１２０）。
【請求項１８】
前記データ処理部は、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（Ｅ２）を解読及び復号するように動作可能である請求項１５、１６、または１７に記載のデコーダ（１２０）。
【請求項１９】
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、当該デコーダ（１２０）が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備えており：
（ｉ）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動作させることと、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することと、符号化され暗号化されたデータ（Ｅ２）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／またはデータパケットの符号化された情報を含み；
（ｉｉ）前記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サイズ及び／または相対位置及び／または１つまたは複数の符号化方法を決定するために、前記１つまたは複数の暗号化されたサブ部分を復号するように前記データ処理部を操作することと；
（ｉｉｉ）前記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つまたは複数の符号化方法の逆を適用するようにデータ処理部を動作させることと；
（ｉｖ）前記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付けられたサイズ及び／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）を生成することと；
を備えることを特徴とする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。
【請求項２０】
前記１つ以上の暗号化されたサブ部分が少なくとも１つの圧縮されたデータストリームの形態で提供され、前記方法は、前記データ処理部を動作させて、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含む請求項１９に記載の方法。
【請求項２１】
前記方法は、前記データ処理部を動作させて、前記１つ以上の暗号化されたサブ部分及び前記１つまたは複数の暗号化されていないサブ部分を、エントロピー符号化方法のバイト及び／またはワードの最上位ビット、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暗号化データストリームが含まれる順序の情報、暗号化データストリームの先頭に書き込まれるフラグビットを含む請求項１９または２０に記載の方法。
【請求項２２】
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（Ｅ２）を解読化及び復号化するように動作可能である請求項１９、２０、または２１に記載の方法。
【請求項２３】
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（１１０）を含むコーデック（１３０）であって、符号化され暗号化されたデータ（Ｅ２）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（Ｄ３）を生成する請求項１５に記載の少なくとも１つのデコーダ（１２０）。
【請求項２４】
請求項８または１９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可能な、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】
【０００１】
本発明は、対応する符号化され暗号化されたデータ（Ｅ２）を生成するための入力データ（Ｄ１）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（Ｅ２）を生成するための入力データ（Ｄ１）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（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、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、
（ｉｉ）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エア間の非互換性に基づいて用いられる。

【０００８】

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（ＤＣＴ）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。

【０００９】

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、ＤＣＴ符号化の非ゼロＡＣ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。

【００１０】

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】

【００１１】

本発明は、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。

【００１２】

さらに、本発明は、符号化され暗号化されたデータ（Ｅ２）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（Ｄ３）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。

【００１３】

例えば、第１の態様として、以下の特徴を有する入力データ（Ｄ１）を処理するデータ処理部を有するエンコーダを介して対応する符号化され暗号化されたデータ（Ｅ２）を生成するためにエンコーダを提供する。
（ａ）前記データ処理部は、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り、前記複数の中間符号化データストリームは、前記少なくとも１つのクリティカルデータストリームは、前記複数の中間符号化データストリームのうちの一部のみを表し、前記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の後の符号に対して重要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有し；
（ｂ）前記データ処理部は、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ように動作可能であり；
（ｃ）前記データ処理部は前記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）を生成するように動作可能である。
【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（Ｄ１）を符号化およ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（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(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つまたは複数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。
（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つまたは複数の符号化方法、
（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つまたは複数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、少なくとも１つのクリティカルデータストリームに暗号化されるクリティカル情報として使用することが可能なエントロピーコーティング符号化以前のオリジナルデータの長さ；及び／または
（ｖ）エントロピー符号化に先立って利用される、複数のデータブロック及び／またはデータパケットの長さ。
【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つまたは複数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および／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】
さらに、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。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の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のバイトを計算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の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、および／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、本開示の実施形態は、入力データ（Ｄ１）を処理するデータ処理部を有するエンコーダを介して対応する符号化され暗号化されたデータ（Ｅ２）を生成するために入力データ（Ｄ１）を符号化し暗号化する方法を提供し、（Ｄ１）を含み、前記方法は、
（ａ）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データ処理部を動作させるステップであって、前記複数の中間符号化データストリームは、複数の習慣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であって、複数の中間符号化データストリームの一部のみを表す少なくとも１つのクリティカルデータストリームと、
（ｂ）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つまたは複数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ように前記データ処理部を動作させるステップと、そして
（ｃ）前記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）を生成するように前記データ処理部を動作させるステップを含む。
【００２７】
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。
【００２８】
第４の態様では、本開示の実施形態は、符号化され暗号化されたデータ（Ｅ２）を解読化および復号化して対応する解読化され復号化されたデータ（Ｄ３）を生成し、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有するデコーダを提供し、以下のように特徴付けられる。
（ｉ）前記データ処理部は、符号化され暗号化されたデータ（Ｅ２）を処理して、１つまたは複数の暗号化されたサブ部分およびその１つまたは複数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り、前記符号化され暗号化されたデータ（Ｅ２）は、複数のデータブロックおよび／またはデータパケットの符号化された情報を含み、
（ｉｉ）データ処理部は、サイズおよび／または相対位置および／または複数のデータブロックおよび／またはデータパケットに関連する１つまたは複数の符号化方法を決定するために、１つまたは複数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。
（ｉｉｉ）データ処理部は、複数の復号されたデータブロックおよび／またはデータパケットを生成するために、複数のデータブロックおよび／またはデータパケットの符号化情報を復号するために、複数のデータブロックおよび／またはデータパケットの符号化情報に１つまたは複数の符号化方法の逆を適用するように動作可能であるパケットと、そして
（ｉｖ）データ処理部は、複数のデータブロックおよび／またはデータパケットに関連付けられたサイズおよび／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および／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。

【００２９】
任意に、デコーダのデータ処理部は、符号化および暗号化された１次元データ、符号化および暗号化された多次元データ、符号化および暗号化されたデータテキストデータ、符号化され暗号化されたバイナリデータ、符号化および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、符号化および暗号化された画像データ、符号化およ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データについて、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ることを可能にする。

【００３０】
デ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）を処理して、１つまたは複数の暗号化されたサブ部分およびその１つまたは複数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つまたは複数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および／またはデータパケットの符号化された情報を含む。

【００３１】
デコーダのデータ処理部は、サイズ、相対位置、および／または複数のデータブロックおよび／またはデータパケットに関連する１つまたは複数の符号化方法を決定するために、１つまたは複数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。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および／またはデータパケットに関連する１つまたは複数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。

【００３２】
さらに、任意に、１つまたは複数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。

【００３３】
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のバイトの後に提供される。

【００３４】
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、および／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。

【００３５】

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、および／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および／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および／またはデータパケットの符号化された情報に１つまたは複数の符号化方法の逆を適用して、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、および／または複数のデコードされたデータブロックおよび／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数を複数のエントロピー符号化データブロックおよび／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つまたは複数の符号化方法の逆を適用する前に、符号化され暗号化されたデータ（Ｅ２）を生成する。

【００３６】

その後、デコーダのデータ処理部は、サイズおよび／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および／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。

【００３７】

第５の態様では、本開示の実施形態は、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有するデコーダを介して、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）を符号化および暗号化する方法を提供する。この方法は、以下のように特徴付けられる。

（ｉ）符号化され暗号化されたデータ（Ｅ２）を処理して、１つまたは複数の暗号化されたサブ部分およびその１つまたは複数の暗号化されていないサブ部分を決定するようにデータ処理部を操作するステップであって、符号化され暗号化されたデータ（Ｅ２）は、複数のデータブロックおよび／またはデータパケットの符号化された情報を含み、

（ｉｉ）前記複数のデータブロックおよび／またはデータパケットに関連するサイズおよび／または相対位置および／または１つまたは複数の符号化方法を決定するために、前記１つまたは複数の暗号化されたサブ部分を復号するように前記データ処理部を操作するステップと、

（ｉｉｉ）複数のデータブロックおよび／またはデータパケットの符号化情報を復号し、複数の復号されたデータブロックおよび／またはデータパケットを生成するための、複数のデータブロックおよび／またはデータパケットの符号化情報に１つまたは複数の符号化方法の逆を適用するようにデータ処理部を動作させるステップと、そして、

（ｉｖ）複数のデータブロックおよび／またはデータパケットに関連するサイズおよび／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および／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）を生成するステップを含む。

【００３８】

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。

【００３９】

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

【００４０】

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。

【００４１】

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 Ｃｉｐｈｅｒ６（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。

【００４２】

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番目から１／１０００番目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。

【００４３】

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およ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、ビデオおよ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。

【００４４】

本開示のさらなる態様、利点、特徴および目的は、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および詳細な説明から明らかになるであろう。

【００４５】

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】

【００４６】

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およ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。

【００４７】

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。
【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。
【００４８】
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】
【００４９】
以下の詳細な説明では、本開示の例示的な実施形態およ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。
【００５０】
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。
【００５１】
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。
【００５２】
本開示で説明される部分データ暗号化は、その内容、特性、およ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。
【００５３】
本開示の実施形態は、データの１つまたは複数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およ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。
【００５４】
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。
【００５５】
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、
（ｉｉ）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

）を生成する復号化器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、
（ｉｉｉ）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との組み合わせの組み合わせを含むコーデック１３０に関する。
【００５６】
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。
【００５７】
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。
【００５８】
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。
【００５９】
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。
【００６０】
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）を複数の分割および／または結合するために、データブロックおよび／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。
【００６１】
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および／またはデータパケットに最適な方法で分割および／または結合するために使用することができる。
【００６２】
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。
【００６３】

01 02 03 04 05 06
07 08 09 10 11 12
13 14 15 16 17 18
19 20 21 22 23 24

【００６４】

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。

【００６５】

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

【００６６】

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。

【００６７】

（01 02 03 04）
（05 06 07 08）
（09 10 11 12）
（13 14 15 16）
（17 18 19 20）
（21 22 23 24）

【００６８】

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領域の通常の操作順序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。

【００６９】

（01 02 07 08）
（03 04 09 10）
（05 06 11 12）
（13 14 19 20）
（15 16 21 22）
（17 18 23 24）

【００７０】

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。

【００７１】

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。

【００７２】

入力データ（Ｄ１）が複数のデータブロックおよび／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および／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および／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および／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つまたは複数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。

【００７３】

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および／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つまたは複数の符号化方法を使用するように動作可能である。

【００７４】

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および／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および／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および／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）を生成するときにデータ（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。

【００７５】

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つまたは複数は、以後、「クリティカルデータストリーム」と呼ばれる。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。

【００７６】

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および／またはデータパケットに分割および／または結合するために使用される複数の分割および／または結合動作、

（ｉｉ）複数のデータブロックおよび／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つまたは複数の符号化方法、

（ｉｉｉ）複数のデータブロックおよび／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つまたは複数のエントロピー符号化方法、および／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および／またはデータパケットの長さ、および／または

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

【００７７】

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１／１００番目から１／１０００番目の範囲内にある。

【００７８】

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、および／これらに限定されるものではない。

【００７９】

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。

【００８０】

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つを暗号化する際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。

【００８１】

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。

【００８２】

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。

【００８３】

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に、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。

【００８４】

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および符号化され暗号化されたデータ（Ｅ２）と併合する。

【００８５】

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。

【００８６】

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の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。

【００８７】

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、データストリーム、新しいバイトがデコーダ１２０でのその後の解読およ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。

【００８８】

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、メッソドバイトおよび／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。

【００８９】

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（Ｅ２）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。

【００９０】

暗号化されたデータストリーム、さらに、任意に、１つまたは複数のフラグビットを使用して、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。

【００９１】

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）全体を復号化およ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。

【００９２】

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。

【００９３】

一例として、Ｇｕｒｕｌｏｇｉｃ　Ｍｉｃｒｏｓｙｓｔｅｍｓ　Ｏｙから入手可能なＧｒｕｌｏｇｉｃ　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）のフォーマットおよび内容に応じて、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）のビット数およ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およびエントロピー符号化方法で効率的に符号化およ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。

【００９４】
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、複数の分割および／または組み合わせを示す情報、例えば分割および／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および／またはデータパケットに分割および／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番目から１／２０００番目の範囲にわたる。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および／またはデータパケットのサイズおよび／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および／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および／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および／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。

【００９５】
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および／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および／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番目から１／１０００番目の範囲であり、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。

【００９６】
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および／またはデータパケットに対して生成される。

【００９７】
さらに、任意に、入力データ（Ｄ１）は、例えば入力データ（Ｄ１）の内容およ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および／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および／またはデータパケットに分割され、逆もまた同様である。

【００９８】
分割／結合情報データストリームおよ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および／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および／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、データブロックおよび／またはデータパケットのサイズおよび相対位置、ならびにデータブロックおよび／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。

【００９９】
したがって、スプリット／結合情報データストリームおよ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合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および処理エネルギーの１／１００番目から１／１０００番目のみが消費される。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。

【０１００】

さらに、分割／結合情報データストリームおよび／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、およびデータブロックおよび／またはデータパケットを配置する必要がある。

【０１０１】

しかし、データブロックおよび／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および／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。データブロックおよび／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、データブロックおよび／またはデータパケットが分割および／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、データブロックおよび／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および複数のエントロピー符号化されたデータブロックおよび／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および／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。

【０１０２】

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および／またはデータパケットに対して１つまたは複数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および／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および／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１／１００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。

【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および／またはデータパケットに対して１つまたは複数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および／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つまたは複数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。

【０１０４】

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、暗合されたデータストリームおよ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番目から９９９／１０００番目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（Ｅ２）を解読することができない。

【０１０５】

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（Ｅ２）を解読しようとすることが可能である。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（Ｅ２）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およ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。

【０１０６】

さらに、エンコーダ１１０は、符号化され暗号化されたデータ（Ｅ２）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および／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。データサーバおよび／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（Ｅ２）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。

【０１０７】

さらに、任意に、エンコーダ１１０は、少なくとも１つのキーおよび／またはＩＶをデータサーバおよび／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。

【０１０８】

いくつかの例では、デコーダ１２０は、任意に、データサーバおよび／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（Ｅ２）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、データサーバおよび／またはデータストレージおよび／または別のデータサーバから少なくとも１つのキーおよび／またはデータストレージおよび／または別のデータサーバから少なくとも１つのキーおよび／またはＩＶにアクセスするように動作可能である。

【０１０９】

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（Ｅ２）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）および／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。そのようなハードワイヤ実装は、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。

【０１１０】

さらに他の代表的な例では、デコーダ１２０は、ハードドライブおよ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（Ｅ２）を取り戻せるように任意に実施される。

【０１１１】

さらに、任意に、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（Ｅ２）のその後の解読およ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（Ｔｒａｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）を介して実装される。

【０１１２】

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デ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および／またはビデオ会議情報を含む。

【０１１３】

任意の、デコーダ１２０のデータ処理部は、符号化および暗号化された１次元データ、符号化および暗号化された多次元データ、符号化およ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。

【０１１４】

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つまたは複数の暗号化されたサブ部分およびその１つまたは複数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つまたは複数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および／またはデータパケットの符号化された情報を含む。

【０１１５】

任意に、暗号化されたサブ部分の決定は、前述の第１の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、暗号化およ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。

【０１１６】

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。任意選択的に、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つまたは複数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。

【０１１７】

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つまたは複数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。

【０１１８】

さらに、任意の、１つまたは複数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のバイトから、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。

【０１１９】

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、例えばその最初の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。

【０１２０】

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、および関連する１つまたは複数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。

【０１２１】

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つまたは複数の符号化方法の逆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を適用する前の符号化され暗号化されたデータ（Ｅ２）の非暗号化サブ部分に含まれる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対して１つ以上のエントロピー符号化方法の逆を適用するように動作可能である。

【０１２２】

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。

【０１２３】

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つまたは複数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。

【０１２４】

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。

【０１２５】

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つ又は複数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。

【０１２６】

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。

【０１２７】

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ＳＳＩ／ＴＬＳなどの暗号化された通信接続を必要とせずに、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。

【０１２８】

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。

【０１２９】

「ブルートフォース攻撃」技術に加えて、「バイクリック攻撃」、「関連キー攻撃」、「パッディング・オラクル攻撃」などの他のよく知られている攻撃手法がある。「長さ拡張攻撃」技術などが含まれるが、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。

【０１３０】

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と暗号文バイトをマージする。

５．キー２とＣｉｐｈｅｒｔｅｘｔ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つまたは複数の暗号化されたサブ部分に書き込む。

【０１３１】

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

【０１３２】

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。

【０１３３】

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。

【０１３４】

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つが多くの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目的に特に有益である。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。

【０１３５】

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つまたは複数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。

【０１３６】

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、またはそら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ズのステップの集合として示される。

【０１３７】

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。

【０１３８】

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。

【０１３９】

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。

【０１４０】

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

び任意の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つ又は複数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つ又は複数の符号化方法、１つまたは複数のエントロピー符号化方法、及び／または長さの少なくとも１つを示す情報を含む。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、及び／またはエントロピー符号化に先立つデータブロック及び／またはパケットの長さが適用される。

【０１４１】

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に少なくとも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。

【０１４２】

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。

【０１４３】

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。

【０１４４】

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。

【０１４５】

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。

【０１４６】

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つまたは複数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。

【０１４７】

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。

【０１４８】

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取りまたは受信する。

【０１４９】

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。

【０１５０】

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。

【０１５１】

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。

【０１５２】

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つまたは複数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。

【０１５３】

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。

【０１５４】

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。

【０１５５】

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。

【０１５６】

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つまたは複数のステップが追加され、１つまたは複数のステップが削除されるか、または１つまたは複数のステップが異なるシーケンスで提供される。

【０１５７】

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。

【０１５８】

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）を復号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。

【０１５９】
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。
【０１６０】
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。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。
【０１６１】
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つまたは複数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つまたは複数のエントロピー符号化方法も決定する。
【０１６２】
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。
【０１６３】
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。
【０１６４】
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。
【０１６５】
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つまたは複数の符号化方法の逆数を、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つまたは複数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データ圧縮解除方法を適用する。
【０１６６】
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。
【０１６７】
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つまたは複数のステップが追加され、１つまたは複数のステップが削除されるか、または１つまたは複数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。任意選択的に、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。

【０１６８】
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つまたは複数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。
【０１６９】
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。
【０１７０】
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。
【０１７１】
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。
【０１７２】
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。任意選択で、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。
【０１７３】
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。
【０１７４】
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つまたは複数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。
【０１７５】
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。
【０１７６】
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。
【０１７７】
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。
【０１７８】
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。
【０１７９】
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。

【０１８０】

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。

【０１８１】

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。

【０１８２】

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。

【０１８３】

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。

【０１８４】

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つまたは複数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。

【０１８５】

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。

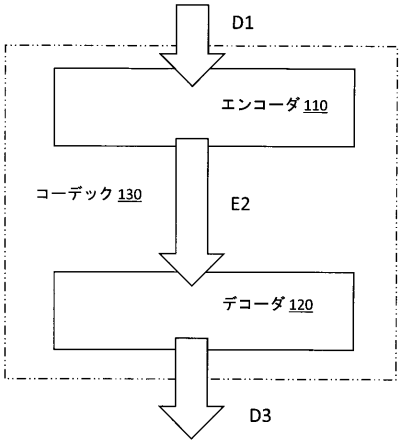
【０１８６】

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。

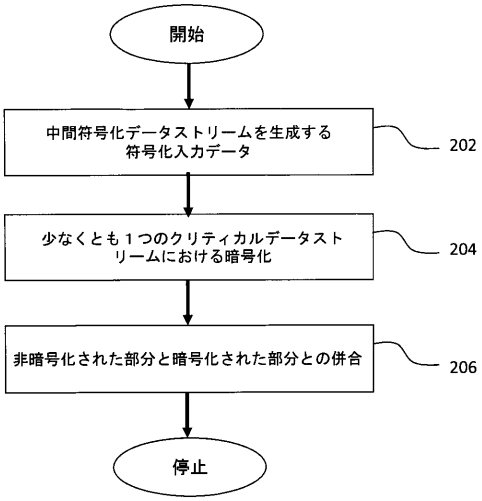
【０１８７】

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「including」、「comprising」、「incorporating」、「consisting of」、「have」、「is」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。

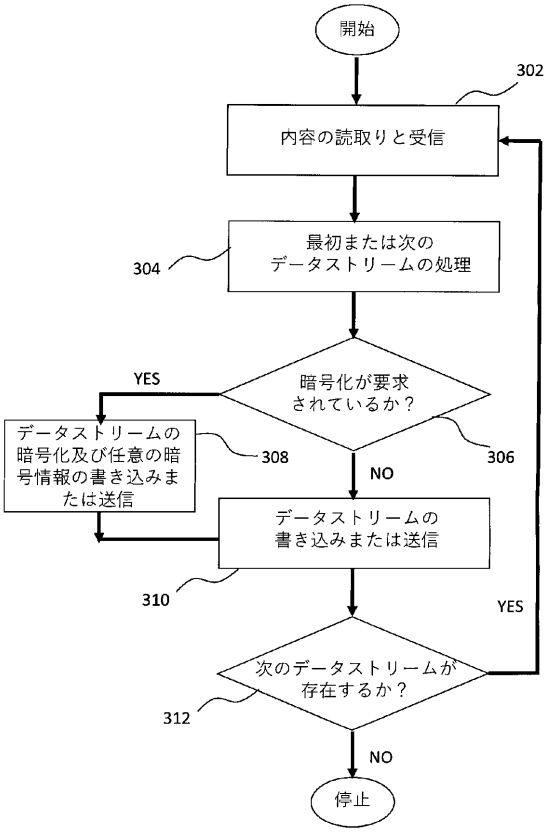
【図１】


D1
エンコーダ 110
コーデック 130
E2
デコーダ 120
D3

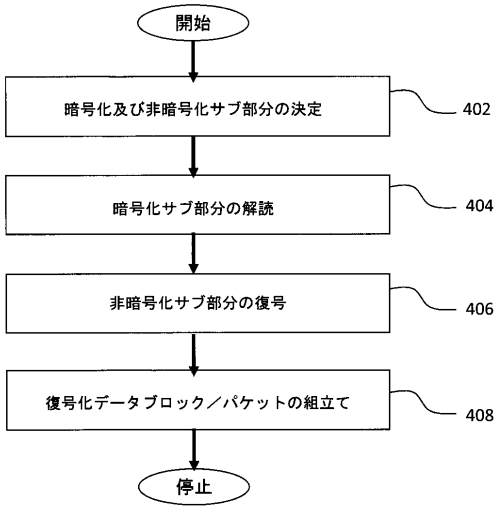
【図２】


開始
中間符号化データストリームを生成する符号化入力データ
202
少なくとも１つのクリティカルデータストリームにおける暗号化
204
非暗号化された部分と暗号化された部分との併合
206
停止

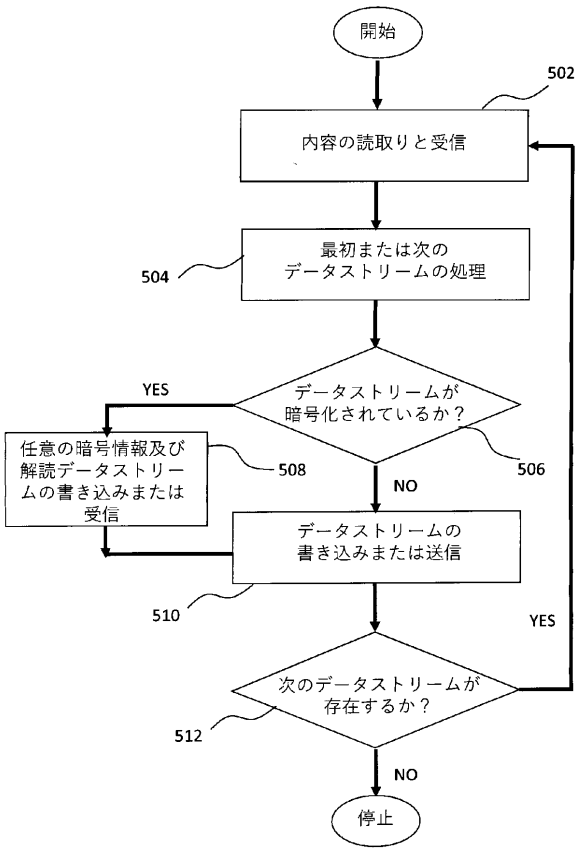
【図３】


開始
302
内容の読取りと受信
304
最初または次のデータストリームの処理
暗号化が要求されているか？
YES
306
データストリームの暗号化及び任意の暗号情報の書き込みまたは送信
308
NO
データストリームの書き込みまたは送信
310
YES
次のデータストリームが存在するか？
312
NO
停止

【図４】


開始
暗号化及び非暗号化サブ部分の決定
402
暗号化サブ部分の解読
404
非暗号化サブ部分の復号
406
復号化データブロック／パケットの組立て
408
停止

【図５】



【手続補正書】
【提出日】平成29年6月21日(2017.6.21)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、対応する符号化され暗号化されたデータ（Ｅ２）を生成するための入力データ（Ｄ１）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（Ｅ２）を生成するための入力データ（Ｄ１）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（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、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、

（ｉｉ）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エア間の非互換性に基づいて用いられる。

【０００８】

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（ＤＣＴ）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。

【０００９】

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、ＤＣＴ符号化の非ゼロＡＣ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。

【００１０】

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】

【００１１】

本発明は、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。

【００１２】

さらに、本発明は、符号化され暗号化されたデータ（Ｅ２）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（Ｄ３）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。

【００１３】

例えば、第１の態様として、入力データ（Ｄ１）を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）を生成するエンコーダを提供する。

（ａ）前記データ処理部は、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うちの一部のみを表し、前記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の後の符号に対して重要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有し；

（ｂ）前記データ処理部は、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ように動作可能であり、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の少なくとも１つの圧縮データストリームの中に前記少なくとも１つのクリティカルデータストリームを圧縮するように動作可能であり；

（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（Ｅ２）への包含に関して、１つ以上の他の圧縮データストリームの中に非クリティカルデータストリームを圧縮するように動作可能であり；そして、

（ｄ）前記データ処理部は前記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）を生成するように動作可能である。

【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（Ｄ１）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（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(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（Ｄ１）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、本開示の実施形態は、入力データ（Ｄ１）を処理するデータ処理部を有するエンコーダを介して対応する符号化され暗号化されたデータ（Ｅ２）を生成するために入力データ（Ｄ１）を符号化し暗号化する方法を提供し、（Ｄ１）を含み、前記方法は：

（ａ）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であって、複数の中間符号化データストリームの一部のみを表す少なくとも１つのクリティカルデータストリームであるところの複数の中間符号化データストリームを生成するように入力データ（Ｄ１）を符号化して動作させることと；

（ｂ）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、そして、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前に少なくとも１つの圧縮データストリームの中に少なくとも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、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ように前記データ処理部を動作させることと；

（ｃ）符号化され暗号化されたデータ（Ｅ２）の包含に関して、１つ以上の圧縮データストリームの中に非クリティカルデータストリームを圧縮するように前記データ処理部を動作させることと；そして

（ｄ）前記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）を生成するように前記データ処理部を動作させることを含む。

【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、本開示の実施形態は、符号化され暗号化されたデータ（Ｅ２）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（Ｄ３）を生成し、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有するデコーダを提供し、以下のように特徴付けられる。
（ｉ）前記データ処理部は、符号化され暗号化されたデータ（Ｅ２）を処理して、１つ以上の暗号化サブ部分及びその１つ以上の非暗号化サブ部分を決定するように動作可能であり、前記符号化され暗号化されたデータ（Ｅ２）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み、
（ｉｉ）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形態で提供される１つ以上の暗号化サブ部分の中にある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サイズ及び／または相対位置及び／または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解読及び解凍するように動作可能である。
（ｉｉｉ）データ処理部は、複数の復号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を復号するために、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るパケットと、そして
（ｉｖ）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付けられたサイズ及び／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。
【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、本開示の実施形態は、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有するデコーダを介して、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）を符号化及び暗号化する方法を提供する。この方法は、以下のように特徴付けられる：
（ｉ）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操作すること、これについては、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が複数のデータブロッ及び／またはデータパケットの符号化情報を含む；
（ｉｉ）１つ以上の暗号化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態で提供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に関連するサイズ及び／または相対位置及び／または１つ以上の符号化方法を決定するために、前記１つ以上の暗号化サブ部分を復号及び解凍するように前記データ処理部を操作することと；
（ｉｉｉ）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し、複数の復号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ための、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データ処理部を動作することと；そして、
（ｉｖ）解読化され復号化されたデータ（Ｄ３）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に関連するサイズ及び／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るようにデータ処理部を動作することを含む。任意に、前記方法は、少なくとも１つの圧縮データストリームから、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ために、前記データ処理部を操作することを含む。
【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（Ｅ２）、フラグピ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（Ｅ２）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 Ｃｉｐｈｅｒ６（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；
（ｉｉ）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；
（ｉｉｉ）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】

01 02 03 04 05 06
07 08 09 10 11 12
13 14 15 16 17 18
19 20 21 22 23 24

【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】

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

【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】

（01 02 03 04）
（05 06 07 08）
（09 10 11 12）
（13 14 15 16）
（17 18 19 20）
（21 22 23 24）

【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領域の通常の操作順序を使用することにより、２Ｄ画像内のビ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】

（01 02 07 08）
（03 04 09 10）
（05 06 11 12）

（13 14 19 20）
（15 16 21 22）
（17 18 23 24）
【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）を生成するときにデータ（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１／１００から１／１０００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つを暗号化する際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に、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（Ｅ２）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Ｇｒｕｌｏｇｉｃ 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／またはデータパケットに分割及び／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合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、暗合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（Ｅ２）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（Ｅ２）を解読しようとすることが可能である。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（Ｅ２）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（Ｅ２）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（Ｅ２）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（Ｅ２）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（Ｅ２）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。そのようなハードワイヤ実装は、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（Ｅ２）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（Ｅ２）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（Ｔｒａｓｐｏｒｔ 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デ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、クリテチ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ＳＳＩ／ＴＬＳなどの暗号化された通信接続を必要とせずに、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、「バイクリック攻撃」、「関連キー攻撃」、「パッディング・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Ｃｉｐｈｅｒｔｅｘｔ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つが多くの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目的に特に有益である。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

ローズ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に少なくとも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。
【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「including」、「comprising」、「incorporating」、「consisting of」、「have」、「is」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。
【手続補正２】
【補正対象書類名】特許請求の範囲

【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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（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（１１０）であって、以下の処理：
（ａ）データ処理部は、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入力データ（Ｄ１）を符号化するように動作可能であり、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前記複数の中間符号化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表し、前記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に続く復号化に重要かつ不可欠であることと；
（ｂ）前記データ処理部は、少なくとも１つの中間符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ように動作可能であり、前記少なくとも１つの中間符号化データストリームには、前記データ処理部が、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暗号化する前に少なくとも1つの圧縮データストリームの中に前記少なくとも1つのクリティカルデータストリームを圧縮するように動作可能であることと；
（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（Ｅ２）の包含に関して、１つ以上の他の圧縮データストリームの中に非クリティカルデータストリームを圧縮するように動作可能であることと；
（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）を生成するように動作可能であることと；
を行うように構成される前記入力データ（Ｄ１）を処理するデータ処理部を備えることを特徴とするエンコーダ（１１０）。
【請求項２】
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、複数の分割及び／または結合動作が複数のデータブロック及び／またはデータパケットの中へ前記入力データ（Ｄ１）を分割及び／または結合するのに用いられ、１つ以上の符号化方法が前記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少なくとも１つの情報を含む請求項１に記載のエンコーダ（１１０）。
【請求項３】
前記データ処理部は、複数のデータ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動作可能であり、前記データ処理部、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の複数のブロック、及び／またはデータパケットを含み、前記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、前記複数のデータブロック及び／またはデータパケットの複数のパラメータを決定するように動作可能である請求項２に記載のエンコーダ（１１０）。
【請求項４】
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）を処理するように動作可能である請求項１に記載のエンコーダ（１１０）。
【請求項５】
前記データ処理部は、第１バイトが少なくとも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表すような少なくとも１つの圧縮データストリームの第１バイトを計算するように動作可能である請求項１に記載のエンコーダ（１１０）。

【請求項６】
前記データ処理部は、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のバイト及び／またはワードにおける最上位ビット、非暗号化され暗号化された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）、フラグビットに含まれる順序のうち少なくとも１つを用いることで暗号化を決定するように動作可能である請求項１に記載のエンコーダ（１１０）。
【請求項７】
エンコーダ（１１０）を経由して、前記対応する符号化され暗号化されたデータ（Ｅ２）を発生する前記入力データ（Ｄ１）を符号化及び暗号化する方法であって、以下の処理：
（ａ）前記入力データ（Ｄ１）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ように前記データ処理部を動作させることを含み、前記複数の中間符号化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うちの１つ以上の残りのデータストリームに続く復号化に重要かつ不可欠であり、少なくとも１つの重要な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表すことと；
（ｂ）前記少なくとも１つの中間暗号化データストリームを生成するため、及び少なくとも１つのクリティカルデータストリームを暗号化する前の少なくとも１つの圧縮データストリームの中に前記少なくとも１つのクリティカルデータストリームを圧縮するために、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ように前記データ処理部を動作させることと；
（ｃ）前記符号化され暗号化されたデータ（Ｅ２）に含まれる１つ以上の圧縮データストリームの中に非クリティカルデータストリームを圧縮するように前記データ処理部を動作させることと；
（ｄ）前記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）を生成するように前記データ処理部を動作させることと；
を備えることを特徴とする前記入力データ（Ｄ１）を符号化及び暗号化する方法。
【請求項８】
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、前記複数のデータブロック及び／またはデータパケット、及び／または前記複数のデータブロック及び／または前記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の中に、前記入力データ（Ｄ１）を分割及び／または結合するために使用される複数の分割及び／または結合演算のうち、少なくとも１つの情報を示すことを含む請求項７に記載の方法。
【請求項９】
（ｅ）前記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、前記複数のデータブロック及び／またはデータパケットを決定することと；
（ｆ）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／またはデータパケット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１つ以上の符号化方法を選択するようにデータ処理部を動作させることと；
を備える請求項８に記載の方法。
【請求項１０】
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７に記載の方法。
【請求項１１】
前記データ処理部を動作させて前記少なくとも１つの圧縮データストリームの第１バイトを計算し、前記第１バイトが前記少なくとも１つの圧縮データストリームの第１バイトを計算し、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ことを含む、請求項７に記載の方法。
【請求項１２】
暗号化を定義するために前記データ処理部を動作させることを含み、前記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と、エントロピー符号化方式のバイト及び／またはワードにおける最上位ビット、前記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暗号化されたデータストリームが含まれる動作、フラグビットを含む請求項７に記載の方法。
【請求項１３】
前記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、
（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／またはデータパケットの符号化された情報を含み；
（ｉｉ）前記データ処理部は、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に提供される、サイズ及び／または相対位置及び／または前記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つ以上の暗号化されたサブ部分を解読し解凍するように動作可能であり；
（ｉｉｉ）前記データ処理部は、前記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するために、複数の復号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ための、前記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；
（ｉｖ）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／またはデータパケットに関連付けられたサイズ及び／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るように動作可能であることを特徴とするデコーダ（１２０）。
【請求項１４】
前記データ処理部が、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動作可能である請求項１３に記載のデコーダ（１２０）。
【請求項１５】
前記データ処理部は、前記１つ以上の暗号化された部分及び前記１つ以上の暗号化されていないサブ部分を、新しいバイトがエントロピー符号化方法のバイト及び／またはワードの最上位ビット、暗号化及び暗号化された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）、フラグビットに含まれる請求項１３に記載のデコーダ（１２０）。
【請求項１６】
前記データ処理部は、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（Ｅ２）を解読及び復号するように動作可能である請求項１３に記載のデコーダ（１２０）。
【請求項１７】
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（Ｅ２）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／またはデータパケットの符号化された情報を含み；
（ｉｉ）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に提供される、サイズ及び／または相対位置及び／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、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；
（ｉｉｉ）前記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するために、前記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；
（ｉｖ）前記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付けられたサイズ及び／または相対位置に基づいて、前記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、前記解読化され復号化されたデータ（Ｄ３）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（Ｅ２）を復号化及び符号化する方法。
【請求項１８】
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方法である請求項１７に記載の方法。
【請求項１９】
前記方法は、前記データ処理部を動作させて、前記１つ以上の暗号化されたサブ部分及び前記１つ以上の暗号化されていない部分を、前記エントロピー符号化方法のバイト及び／またはワードの最上位ビット、前記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暗号化データストリームが含まれる順序の情報、暗号化データストリームの先頭に書き込まれるフラグビットを含む請求項１７に記載の方法。
【請求項２０】
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（Ｅ２）を解読化及び復号化するように動作可能である請求項１７に記載の方法。
【請求項２１】
対応する前記符号化され暗号化されたデータ（Ｅ２）を生成するために前記入力データ（Ｄ１）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（１１０）を含むコーデック（１３０）であって、前記符号化され暗号化されたデータ（Ｅ２）を解読し復号して、前記対応する解読化され復号化されたデータ（Ｄ３）を生成する請求項１３に記載の少なくとも１つのデコーダ（１２０）。
【請求項２２】
請求項７または１７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可能な、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。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/025065

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/06 H04L9/12 H04N21/4385 H04N21/4405
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H03M H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/081333 A1 (GRAB ERIC W [US] ET AL) 29 April 2004 (2004-04-29) abstract paragraphs [0002] - [0019], [0033] - [0057] figures 1-12	1-24
X	WO 2010/150056 A1 (NDS LTD [GB]; FARKASH EYAL [IL]; MURRAY KEVIN A [GB]) 29 December 2010 (2010-12-29) abstract page 1, line 1 - page 24, line 10 figures 1-5	1-24

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 November 2015	11/11/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Mariggis, Athanasios

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/025065

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SHIGUO LIAN ET AL: "Selective Video Encryption Based on Advanced Video Coding", 1 January 2005 (2005-01-01), ADVANCES IN MULITMEDIA INFORMATION PROCESSING - PCM 2005 LECTURE NOTES IN COMPUTER SCIENCE;;LNCS, SPRINGER, BERLIN, DE, PAGE(S) 281 - 290, XP019024055, ISBN: 978-3-540-30040-3 the whole document -----	1-24

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/025065

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004081333 A1	29-04-2004	NONE	
WO 2010150056 A1	29-12-2010	CA 2766308 A1	29-12-2010
		CN 102804766 A	28-11-2012
		EP 2446620 A1	02-05-2012
		US 2012134496 A1	31-05-2012
		WO 2010150056 A1	29-12-2010

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(74)代理人 100125243
弁理士 伊藤 浩彰
(72)発明者 カルッカイネン, トゥオマス
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
(72)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

Ｆターム(参考) 5J064 AA03 BA09 BC02 BC25
5J104 AA18 CA02