【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成27年10月1日(2015.10.1)

【公開番号】特開2013-61650(P2013-61650A)
【公開日】平成25年4月4日(2013.4.4)
【年通号数】公開・登録公報2013-016
【出願番号】特願2012-196888(P2012-196888)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
Ｈ０４Ｌ　9/18　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６６０Ｄ
Ｈ０４Ｌ　9/00　６５１

【手続補正書】
【提出日】平成27年8月14日(2015.8.14)
【手続補正１】
【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】
あるフォーマットを有するビットストリームであって、複数のユニットを含むビットストリームの、フォーマットに準拠した暗号化の方法であって、
当該方法は、暗号化装置において、
第一のタイプである第一のユニットを暗号化して、暗号化されたユニットを取得するステップと、
前記暗号化されたユニットを、前記あるフォーマットに準拠する第二のタイプである第二のユニットに挿入するステップと、
前記第二のユニットを前記ビットストリームに挿入するステップと、
前記第一のタイプの置換えユニットを、前記ビットストリームの前記第一のユニットの位置に挿入するステップと、
を含む方法。
【請求項２】
前記置換えユニットからのデータは、前記第一のタイプの更なるユニットの置換えのために使用可能である、
請求項１記載の方法。
【請求項３】
前記第一のタイプのユニットは、ヘッダ及びボディを有し、
当該方法は、前記第一のユニットからのヘッダデータを、前記第一のタイプのジェネリックユニットのヘッダデータ及びボディデータと結合することで、前記第一のユニットについて前記置換えユニットを取得するステップを更に含む、
請求項１記載の方法。
【請求項４】
前記ビットストリームの前記あるフォーマットは、H.264/MPEG-4　AVC規格に準拠しており、前記第一のユニットは、ビデオデータを含むスライスである、
請求項３記載の方法。
【請求項５】

複数のユニットを含むビットストリームの、フォーマットに準拠した暗号化のための暗号化装置であって、
当該暗号化装置は、
第一のタイプである第一のユニットを暗号化して、暗号化されたユニットを取得する手段と、
前記暗号化されたユニットを、フォーマットに準拠する第二のタイプである第二のユニットに挿入する手段と、
前記第二のユニットを前記ビットストリームに挿入する手段と、
前記第一のタイプの置換えユニットを、前記ビットストリームの前記第一のユニットの位置に挿入する手段と、
を備える暗号化装置。
【請求項６】
あるフォーマットを有する暗号化されたビットストリームであって、複数のユニットを含む暗号化されたビットストリームの、フォーマットに準拠した暗号解読の方法であって、
当該方法は、暗号解読装置において、
前記暗号化されたビットストリームから、暗号化されたユニットを含む第二のタイプの第二のユニットを取得するステップと、
前記暗号化されたユニットを暗号解読して、暗号解読されたデータを取得するステップと、
前記暗号化されたビットストリームにおいて、第一のタイプの置換えユニットを、前記暗号解読されたデータの少なくとも幾つかを含む前記第一のタイプの更なるユニットで置き換えるステップと、
を含む方法。
【請求項７】
前記第二のユニットは、前記暗号化されたビットストリームから前記第二のユニットを除くことで取得される、
請求項６記載の方法。
【請求項８】
前記暗号解読されたデータは、ヘッダデータ及びボディデータを含み、
当該方法は、前記暗号解読されたデータのヘッダデータ及びボディデータの少なくとも幾つかを、前記置換えユニットのヘッダデータと結合することで、前記更なるユニットを生成するステップを更に含む、
請求項６記載の方法。
【請求項９】
前記ビットストリームのフォーマットは、H.264/MPEG-4　AVCに準拠しており、
前記置換えユニットと前記更なるユニットは、ビデオデータを含むスライスである、
請求項６記載の方法。
【請求項１０】
複数のユニットを含む暗号化されたビットストリームの、フォーマットに準拠した暗号解読のための暗号解読装置であって、
当該暗号解読装置は、
前記暗号化されたビットストリームから、暗号化されたユニットを含む第二のタイプの第二のユニットを取得する手段と、
前記暗号化されたユニットを暗号解読して、暗号解読されたデータを取得する手段と、
前記暗号化されたビットストリームにおいて、第一のタイプの置換えユニットを、前記暗号解読されたデータの少なくとも幾つかを含む前記第一のタイプの更なるユニットで置き換える手段と、
を備える暗号解読装置。
【請求項１１】

前記暗号化されたビットストリームから前記第二のユニットを除くことで、前記第二のユニットを取得する手段を更に含む、
請求項１０記載の暗号解読装置。
【請求項１２】
前記暗号解読されたデータは、ヘッダデータ及びボディデータを含み、
前記暗号解読されたデータのヘッダデータ及びボディデータの少なくとも幾つかを、前記置換えユニットのヘッダデータと結合することで、前記更なるユニットを生成する手段を更に備える、
請求項１０記載の暗号解読装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００３
【補正方法】変更
【補正の内容】
【０００３】
特に限定受信テレビジョンシステムにおいて、暗号化によりビデオデータをプロテクトすることが長く知られている。図１は、限定受信制御の慣習的な従来のアプローチを例示する。ビデオ信号CNTは、標準的な圧縮エンコーダを使用してはじめに符号化され（１１０）、次いで、結果として得られるビットストリームCNT’は、（DES, AES又はIDEAのような）対称暗号化規格を使用して暗号化される（１２０）。次いで、暗号化されたビットストリーム［CNT’］は、受信機により受信され、受信機は、暗号化されたビットストリーム［CNT’］を暗号解読して（１３０）符号化されたビットストリームCNT’を取得し、符号化されたビットストリームは、ビデオ信号CNT、すなわち少なくとも理論的には、最初のビデオ信号と同じであるビデオ信号を取得するために復号化される（１４０）。このアプローチで完全階層化（fully layered）と呼ばれ、圧縮及び暗号化は、完全に独立なプロセスである。メディアのビットストリームは、プレインテキストにおける全てのシンボル又はビットが等しい重要性をもつという想定により、古典的なプレインテキストデータとして処理される。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００４
【補正方法】変更
【補正の内容】
【０００４】
このスキームは、コンテンツの伝送が制約されないときに関連するが、（メモリ、パワー又は計算能力のような）リソースが制限される状況において適切ではないと考えられる。多くの研究は、画像及びビデオコンテンツの特定の特性、高い伝送速度及び制限される許容される帯域幅を示し、これらは、係るコンテンツの標準的な暗号化技術が不適切であることを正当化している。これは、暗号化されたビットストリームのサブセットの暗号解読なしに、結果的に得られる部分的に暗号化されたビットストリームが実用にならないという期待により、サブセットに暗号化を適用することによる、「選択的暗号化“selective encryption”」、「部分的暗号化“partial encryption”」、「軟暗号化“soft encryption”」、又は「知覚的暗号化“perceptual encryption”」と名付けられるコンテンツを安全にする新たなスキームを研究することに研究者を導く。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０００６
【補正方法】変更
【補正の内容】
【０００６】

図２は、従来技術に係る選択的な暗号化を例示する。符号化及び復号化は、図１におけるように実行される。選択的な暗号化では、符号化されたビットストリームCNT’は、選択的な暗号化パラメータ２４０に依存して暗号化される（２４０）。これらのパラメータは、上述されたように、たとえばDC係数又は低周波レイヤのみが暗号化される一方、暗号化されたビットストリームCNT’の残りは、暗号化されないまま残される。次いで、部分的に暗号化されたビットストリーム［CNT’］は、選択的な暗号化パラメータ２４０に依存して（部分的に）暗号解読される。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】変更
【補正の内容】
【００２１】

要するに、基本的なJPEG 2000の解決策は、必要とされるヘッダデータが暗号解読の前にアクセス不可能であるので、CABACデータをスクランブルするためにH.264に変更することができないことが理解される。分析することなしにCABACを変更することは、H.264パーサをクラッシュさせる可能性があり、デコーダに失敗させる。主要な代替は、CABACの前にデータを変更するか、又はExp-Golombコードを変更することを提案する。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００２８
【補正方法】変更
【補正の内容】
【００２８】

第三の態様では、本発明は、複数のユニットを含む暗号化されたビットストリームのフォーマットに準拠した暗号解読の方法に向けられる。

【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００２９
【補正方法】変更
【補正の内容】
【００２９】

暗号解読装置は、暗号化されたビットストリームから、暗号化されたユニットを含む第二のユニットであって、第二のタイプからなる第二のユニットを取得し、暗号化されたユニットを暗号解読して、暗号解読されたデータを取得し、暗号化されたビットストリームにおいて、第一のタイプの置換えユニットを、少なくとも幾つかの暗号解読されたデータを含む更なるユニットであって、第一のタイプの更なるユニットで置き換える。

【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００３１
【補正方法】変更
【補正の内容】
【００３１】

第二の好適な実施の形態では、暗号解読されたデータは、ヘッダデータ及びボディデータを含み、暗号解読装置は、暗号解読されたデータのヘッダデータ及びボディデータの少なくとも幾つかを、置換えユニットのヘッダデータと結合することで、更なるユニットを更に生成する。

【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００３３

【補正方法】変更
【補正の内容】
【００３３】
第４の態様では、本発明は、複数のユニットを含む暗号化されたビットストリームのフォーマットに準拠した暗号解読のための暗号解読装置に向けられる。暗号解読装置は、暗号化されたビットストリームから、暗号化されたユニットを含む第二のユニットであって、第二のタイプのからなる第二のユニットを取得する手段、暗号化されたユニットを暗号解読して暗号解読されたデータを取得する手段、暗号化されたビットストリームにおいて、第一のタイプの置換えユニットを、暗号解読されたデータの少なくとも幾つかを含む更なるユニットであって、第一のタイプからなる更なるユニットで置き換える手段を備える。
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００３４
【補正方法】変更
【補正の内容】
【００３４】
第一の好適な実施の形態では、第二のユニットは、暗号化されたビットストリームの一部であり、暗号解読装置は、暗号化されたビットストリームから第二のユニットを除くことで第二のユニットを取得する手段を更に有する。
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００３５
【補正方法】変更
【補正の内容】
【００３５】
第二の好適な実施の形態では、暗号解読されたデータは、ヘッダデータ及びボディデータを含み、暗号解読装置は、暗号解読されたデータのヘッダデータ及びボディデータの少なくとも幾つかを、置換えユニットのヘッダデータと結合することで、更なるユニットを生成する手段を更に有する。
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００３６
【補正方法】変更
【補正の内容】
【００３６】
本発明の好適な特徴は、添付図面を参照しながら、限定するものではない例を通して、以下に記載される。
【図１】本明細書で既に記載された、限定付き受信制御の慣習的な従来のアプローチを例示する図である。
【図２】本明細書で既に記載された、従来技術に係る選択的暗号化を例示する図である。
【図３】例示的な従来技術のH.264ストリームを例示する図である。
【図４】本発明の一般的な発明の着想を例示する図である。
【図５】本発明の好適な実施の形態に係るH.264データの暗号化の方法を例示する図である。
【図６】図５に例示される方法のサブステップの第一の部分を例示する図である。
【図７】本発明の好適な実施の形態に係るプロテクトされたH.264ビデオストリームの暗号解読の方法を例示する図である。
【図８】本発明の好適な実施の形態に係るH.264ビデオストリームの暗号化及び暗号解読の装置を例示する図である。

【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００３８
【補正方法】変更
【補正の内容】
【００３８】
図４は、本発明の一般的な発明の着想を例示する。図において、図３に例示されるH.264ストリームは、限定的ではない例として、NALスライス２　３１０の暗号化により、暗号化されたH.264ストリーム４００を生成するために処理される。少なくともボディ３１４におけるスライスデータ、及び好ましくはスライスヘッダ３１２（又はその一部）は、好ましくは全てのデータの暗号化により暗号化されるが、データの一部を暗号化することも可能である。暗号化は、AES（Advanced Encryption Standard）、Blowfish or Triple DESのような適切な従来の暗号化アルゴリズムを使用して実行される。プロテクトすべきスライスは、好ましくはいわゆるＩ，Ｐ又はＢスライス又はこれらの組み合わせであり、すなわちＩ，Ｐ又はＢフレームに対応するデータを含む。鍵の配信等は、本発明の範囲外であることが理解され、暗号化装置及び暗号解読装置の両者は正しい暗号化又は暗号解読の鍵を有することが想定される。
【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】００４５
【補正方法】変更
【補正の内容】
【００４５】
標準がCABACとCAVLCの混成を許容するとき、Ｐ又はＢ　CABACスライスをＰ又はＢ　CAVLCスライスで、すなわちCAVLCで符号化されたスキップされたマクロブロックで置き換えることも可能である。これを行うため、エントロピーエンコーダをCAVLCに設定する新たなPPS（Picture Parameter Set）が必要とされる。これは、ビデオストリームに、約５バイトを追加する（おそらくスイッチバックのために更なる約５バイト）。幾つかの（連続する）フレーム（それぞれが１以上のスライスから構成される）は、PPSに後続する。CAVLC置換えスライスは、1920×1080高精細（HD）ビデオについて、暗号化されたスライス当たり約３バイト、すなわちオリジナルフレームの0.0001%を要する。スライスヘッダは、スライスデータの適切な復号化のために必要とされる情報を含む。スライスの符号化モードを変えるとき、すなわちCAVLC符号化に切り替えるとき、これらのパラメータの幾つかは、デコーダの適切な動作を可能にするために変更される必要があり、これらのパラメータは、以下を含む。
pic_parameter_set_id（pps_idと呼ばれることがある）：CAVLC符号化のために使用されるピクチャパラメータセットのid。
【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】００４７
【補正方法】変更
【補正の内容】
【００４７】
これらのパラメータは、受信機でCABAC符号化データの適切な復号化のために必要とされるので、これらのパラメータは、暗号化されてSEIに挿入されるＰ又はＢスライスデータに添付される。
【手続補正１６】
【補正対象書類名】明細書
【補正対象項目名】００６７
【補正方法】変更

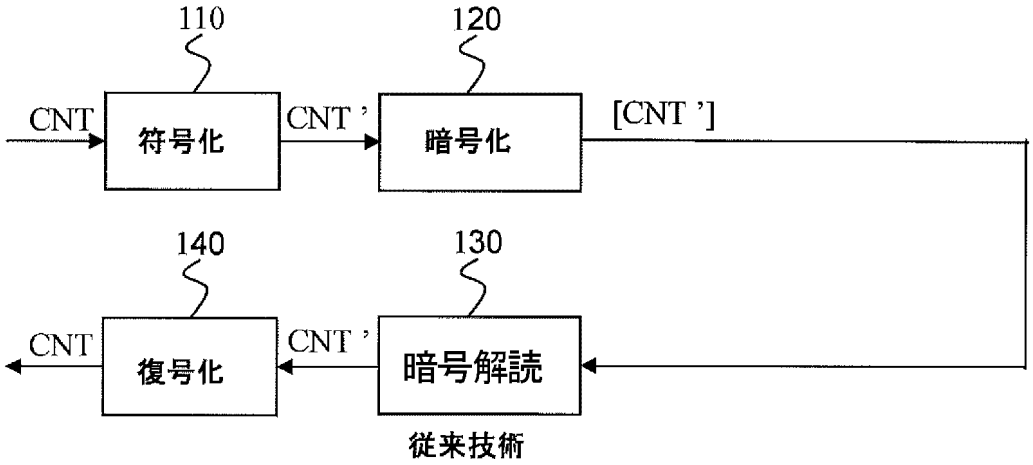
【補正の内容】
【００６７】
図７は、本発明の好適な実施の形態に係るプロテクトされたH.264ビデオストリームの暗号解読の方法を例示する。
【手続補正１７】
【補正対象書類名】明細書
【補正対象項目名】００７０
【補正方法】変更
【補正の内容】
【００７０】
次いで、発見されたSEIは、ステップ７５０で抽出されて暗号解読され、暗号解読されたスライスデータが生成される。そのとき、H.264ストリームからSEIを除くことが有利である。
【手続補正１８】
【補正対象書類名】明細書
【補正対象項目名】００７１
【補正方法】変更
【補正の内容】
【００７１】
ステップ７６０で、対応する置換えスライスが抽出される。次いで、ステップ７７０で、暗号解読されたスライスデータは、置換えデータの位置に配置され、オリジナルの暗号解読されたヘッダデータは、置換えスライスヘッダに回復される。スライスが暗号解読されてストリームに戻されたとき、本方法はステップ７２０に戻り、ストリームが終了したかが確認される。
【手続補正１９】
【補正対象書類名】明細書
【補正対象項目名】００７２
【補正方法】変更
【補正の内容】
【００７２】
図８は、本発明の好適な実施の形態に係る、H.264ビデオストリームの暗号化及び暗号解読のシステム８００を例示する。システム８００は、暗号化装置８１０及び暗号解読装置８４０を備え、それぞれの装置は、少なくとも１つのプロセッサ８１１，８４１，メモリ８１２，８４２，好ましくはユーザインタフェース８１３，８４３及び少なくとも１つの入力／出力ユニット８１４，８４４を備える。暗号化装置８１０は、例えばパーソナルコンピュータ又はワークステーションであり、暗号解読機能を有利にも有している。
【手続補正２０】
【補正対象書類名】明細書
【補正対象項目名】００７３
【補正方法】変更
【補正の内容】
【００７３】
第一のコンピュータ読み取り可能な記録媒体８６０は、暗号化装置８１０のプロセッサ８１１により実行されたとき、H.264ストリームを暗号化する記憶された命令を含む。第一のコンピュータ読み取り可能な記録媒体８７０は、暗号解読装置８４０のプロセッサ８４１により実行されたとき、記載されたように暗号化されたH.264ストリームを暗号解読する記憶された命令を含む。第三のコンピュータ読み取り可能な記憶媒体８８０は、本明細書で記載されたように暗号化される、暗号化されたH.264ストリームを含む。
【手続補正２１】
【補正対象書類名】明細書

【補正対象項目名】００７４
【補正方法】変更
【補正の内容】
【００７４】
当業者であれば、本発明の一般的なスキームは、SVC（Scalable Video Coding）、MVC（Multiview Video Coding）及びHTML-5（HyperText Markup Language 5）のような、他の規格に準拠したデータの、規格に準拠した暗号化及び暗号解読について機能することができることを理解されるであろう。
【手続補正２２】
【補正対象書類名】明細書
【補正対象項目名】００７７
【補正方法】変更
【補正の内容】
【００７７】
・低いオーバヘッド：５ｂ＋４ｂ／プロテクトされたフレーム。
・暗号化すべきフレームＩ，Ｐ及び／又はＢの選択によるチューニング可能な歪みレベル。
・高速な暗号解読。
・スキームは“post compression”であり、圧縮スキームに影響を及ぼさない。
・H.264ファイルフォーマットは、規格に準拠する。スクランブルされたストリームの復号化は、H.264プレーヤを乱さない。
・誤り耐性。スクランブルされているか否かに係らず、デコーダは、同じやり方で誤りを管理し、誤りは同じやり方で伝搬される。
【手続補正２３】
【補正対象書類名】明細書
【補正対象項目名】００７９
【補正方法】変更
【補正の内容】
【００７９】
請求項で現れる参照符号は、例示するものであって、請求項の範囲に限定的な影響を有するものではない。
上記の実施形態に加えて、以下の付記を開示する。
（付記１）
あるフォーマットを有するビットストリームであって、複数のユニットを含むビットストリームの、フォーマットに準拠した暗号化の方法であって、
当該方法は、暗号化装置において、
第一のタイプからなる第一のユニットを暗号化して、暗号化されたユニットを取得するステップと、
前記暗号化されたユニットを、前記あるフォーマットに準拠する第二のタイプからなる第二のユニットに挿入するステップと、
前記第二のユニットを前記ビットストリームに挿入するステップと、
前記第一のタイプの置換えユニットを、前記ビットストリームの前記第一のユニットの位置に挿入するステップと、
を含む方法。
（付記２）
前記置換えユニットからのデータは、前記第一のタイプの更なるユニットの置換えのために使用可能である、
付記１記載の方法。
（付記３）
前記第一のタイプのユニットは、ヘッダ及びボディを有し、

当該方法は、前記第一のユニットからのヘッダデータを、前記第一のタイプのジェネリックユニットのヘッダデータ及びボディデータと結合することで、前記第一のユニットについて前記置換えユニットを取得するステップを更に含む、
付記１記載の方法。
（付記４）
前記ビットストリームの前記あるフォーマットは、H.264/MPEG-4　AVC規格に準拠しており、前記第一のユニットは、ビデオデータを含むスライスである、
付記３記載の方法。
（付記５）
複数のユニットを含むビットストリームの、フォーマットに準拠した暗号化のための暗号化装置であって、
当該装置は、
第一のタイプからなる第一のユニットを暗号化して、暗号化されたユニットを取得する手段と、
前記暗号化されたユニットを、フォーマットに準拠する第二のタイプである第二のユニットに挿入する手段と、
前記第二のユニットを前記ビットストリームに挿入する手段と、
前記第一のタイプの置換えユニットを、前記ビットストリームの前記第一のユニットの位置に挿入する手段と、
を備える装置。
（付記６）
あるフォーマットを有する暗号化されたビットストリームであって、複数のユニットを含む暗号化されたビットストリームの、フォーマットに準拠した復号の方法であって、
当該方法は、復号装置において、
前記暗号化されたビットストリームから、第二のタイプからなる第二のユニットであって、暗号化されたユニットを含む第二のユニットを取得するステップと、
前記暗号化されたユニットを復号して、復号されたデータを取得するステップと、
前記暗号化されたビットストリームにおいて、第一のタイプからなる置換えユニットを、前記第一のタイプからなる更なるユニットであって、前記復号されたデータの少なくとも幾つかを含む更なるユニットで置き換えるステップと、
を含む方法。
（付記７）
前記第二のユニットは、前記暗号化されたビットストリームから前記第二のユニットを除くことで取得される、
付記６記載の方法。
（付記８）
前記復号されたデータは、ヘッダデータ及びボディデータを含み、
当該方法は、前記復号されたデータのヘッダデータ及びボディデータの少なくとも幾つかを、前記置換えユニットのヘッダデータと結合することで、前記更なるユニットを生成するステップを更に含む、
付記６記載の方法。
（付記９）
前記ビットストリームのフォーマットは、H.264/MPEG-4　AVCに準拠しており、
前記置換えユニットと前記更なるユニットは、ビデオデータを含むスライスである、
付記６記載の方法。
（付記１０）
複数のユニットを含む暗号化されたビットストリームの、フォーマットに準拠した復号のための復号装置であって、
当該装置は、
前記暗号化されたビットストリームから、第二のタイプからなる第二のユニットであっ

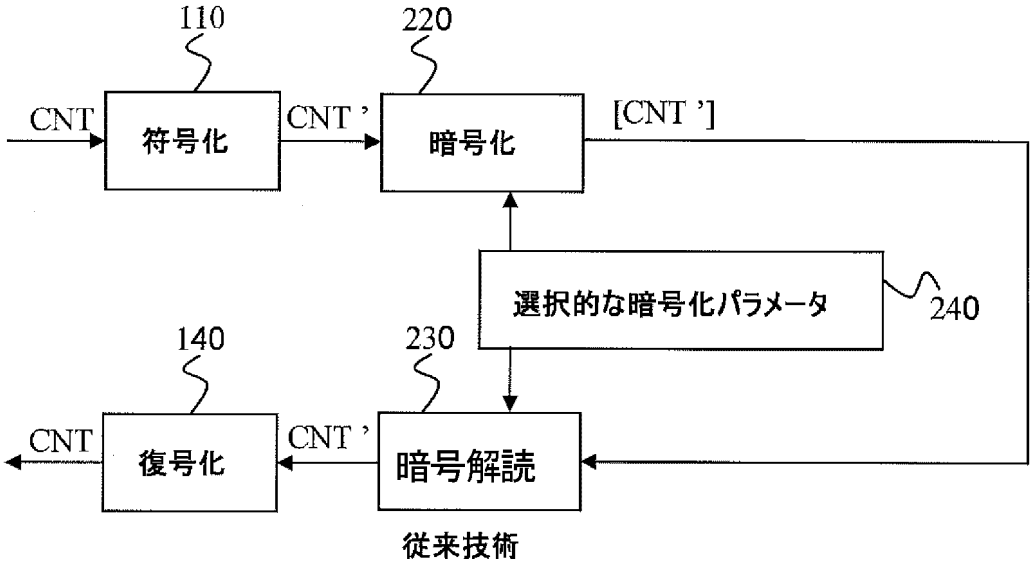
て、暗号化されたユニットを含む第二のユニットを取得する手段と、
前記暗号化されたユニットを復号して、復号されたデータを取得する手段と、
前記暗号化されたビットストリームにおいて、第一のタイプからなる置換えユニットを、前記第一のタイプからなる更なるユニットであって、前記復号されたデータの少なくとも幾つかを含む更なるユニットで置き換える手段と、
を備える装置。
（付記１１）
前記暗号化されたビットストリームから前記第二のユニットを除くことで、前記第二のユニットを取得する手段を更に含む、
付記１０記載の装置。
（付記１２）
前記復号されたデータは、ヘッダデータ及びボディデータを含み、
前記復号されたデータのヘッダデータ及びボディデータの少なくとも幾つかを、前記置換えユニットのヘッダデータと結合することで、前記更なるユニットを生成する手段を更に備える、
付記１０記載の復号装置。
【手続補正２４】
【補正対象書類名】明細書
【補正対象項目名】００８０
【補正方法】変更
【補正の内容】
【００８０】
８００：システム
８１０：暗号化装置
８１１，８４１：プロセッサ
８１２，８４２：メモリ
８１３，８４３：ユーザインタフェース
８１４，８４４：入出力装置
８４０：暗号解読装置
８６０：第一のコンピュータ読み取り可能な記録媒体
８７０：第二のコンピュータ読み取り可能な記録媒体
８８０：第三のコンピュータ読み取り可能な記録媒体
【手続補正２５】
【補正対象書類名】図面
【補正対象項目名】図１
【補正方法】変更
【補正の内容】

【図１】



従来技術

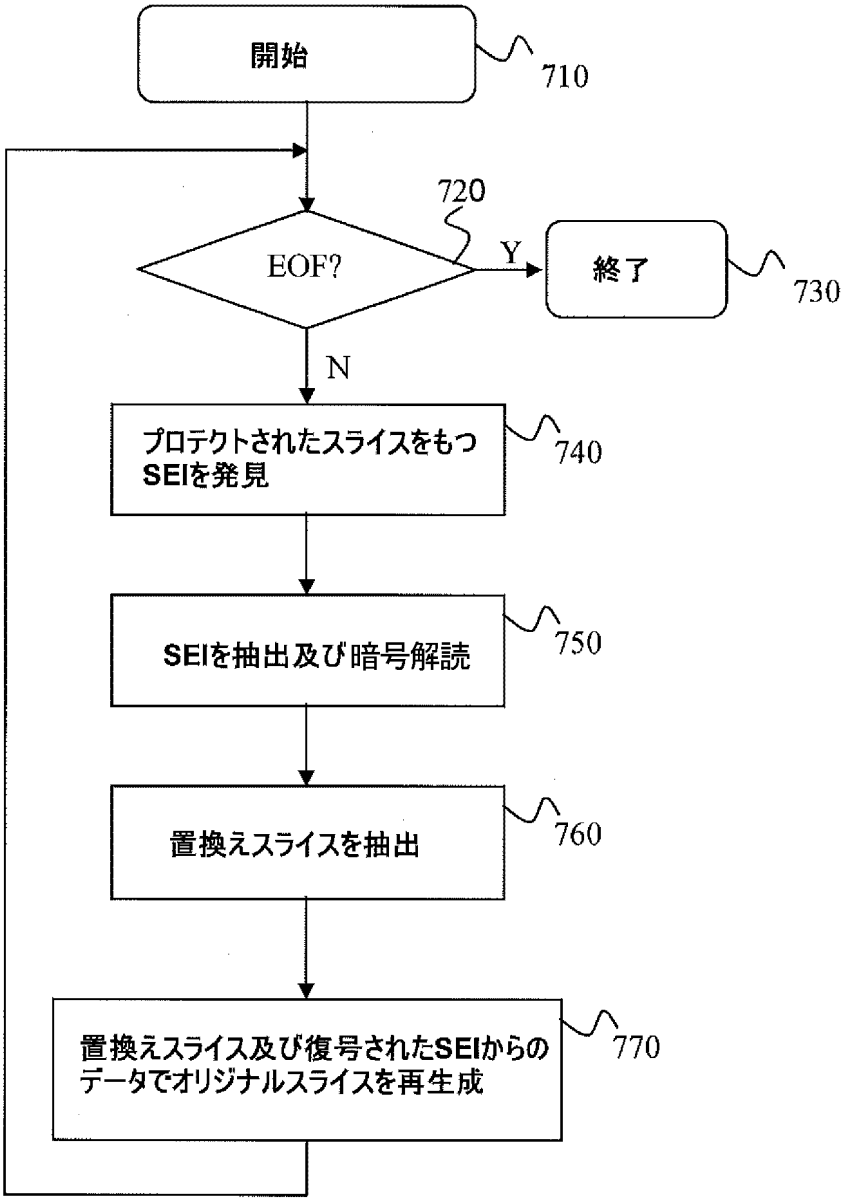
【手続補正２６】
【補正対象書類名】図面
【補正対象項目名】図２
【補正方法】変更
【補正の内容】
【図２】



従来技術

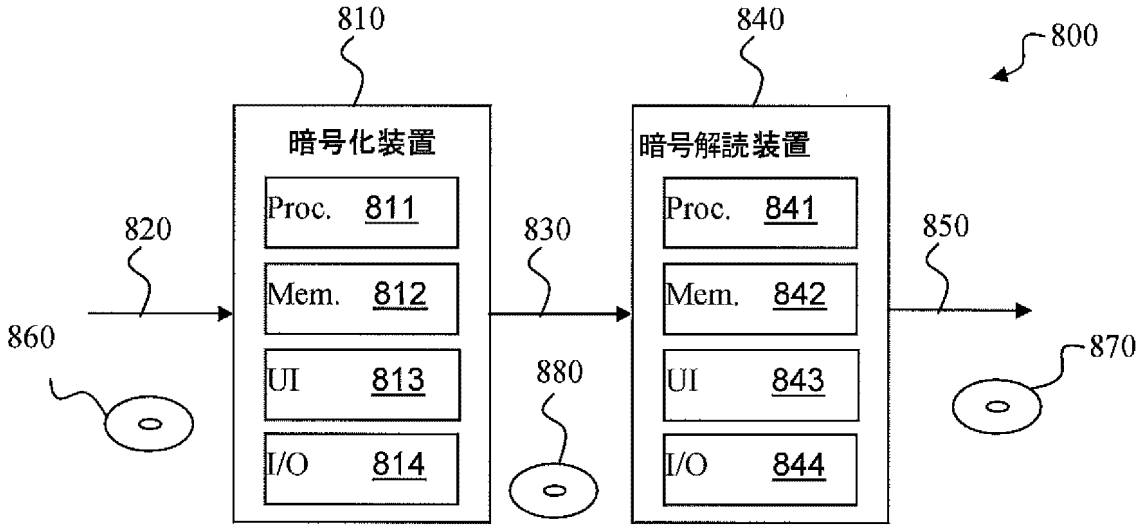
【手続補正２７】
【補正対象書類名】図面
【補正対象項目名】図７
【補正方法】変更
【補正の内容】

【図７】



【手続補正２８】
【補正対象書類名】図面
【補正対象項目名】図８
【補正方法】変更
【補正の内容】

【図８】


810
840
800
暗号化装置
暗号解読装置
Proc. 811
Mem. 812
UI 813
I/O 814
Proc. 841
Mem. 842
UI 843
I/O 844
820
830
850
860
880
870