(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-35850
(P2019-35850A)
(43)公開日　平成31年3月7日(2019.3.7)

(51)Int.Cl.			F I		テーマコード（参考）
G09C	5/00	(2006.01)	G09C	5/00	5C076
G09C	1/02	(2006.01)	G09C	1/02	5J104
H04N	1/387	(2006.01)	H04N	1/387	

審査請求 未請求　請求項の数 15　ＯＬ　（全 17 頁）

(21)出願番号　特願2017-156805 (P2017-156805)
(22)出願日　平成29年8月15日 (2017.8.15)

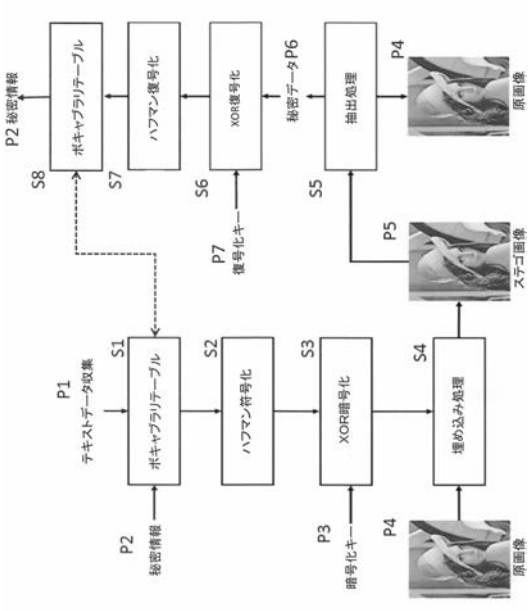
（特許庁注：以下のものは登録商標）
１．ＭＡＴＬＡＢ

(71)出願人　506301140
公立大学法人会津大学
福島県会津若松市一箕町大字鶴賀字上居合
９０番地
(74)代理人　100094525
弁理士　土井　健二
(74)代理人　100094514
弁理士　林　恒徳
(72)発明者　趙　強福
福島県会津若松市一箕町大字鶴賀字上居合
９０番地　公立大学法人会津大学内
(72)発明者　劉　家維
福島県会津若松市一箕町大字鶴賀字上居合
９０番地　公立大学法人会津大学内

Ｆターム(参考)　5C076 AA14　BA06　BA07
5J104 AA01　JA03　NA02　NA20　NA37

(54)【発明の名称】秘密データの隠蔽方法、これを実施するプログラム、及び秘密データ通信システム

(57)【要約】　（修正有）
【課題】データサイズを削減するとともによりセキュリティを高める秘密データの隠蔽方法を提供する。
【解決手段】送信側から受信側に送信される秘密データの隠蔽方法は、送信側と受信側に共通のボキャブラリテーブルを有し、送信側で、秘密データを、前記ボキャブラリテーブルを参照して圧縮コード列に変換するステップと、前記変換された圧縮コード列をカバー画像に埋め込み、ステゴ画像を形成するステップと、前記形成されたステゴ画像を受信側に送信するステップとを有する。また、受信側で、前記ステゴ画像を受信するステップと、受信したステゴ画像から埋め込まれた圧縮コード列を分離してカバー画像を復元するステップと、前記分離した圧縮コード列から前記ボキャブラリテーブルを参照して前記秘密データを復号するステップを有する。
【選択図】図２



【特許請求の範囲】
【請求項１】
送信側から受信側に送信される秘密データの隠蔽方法であって、
送信側と受信側に共通のリストテーブルを有し、
送信側で、
秘密データを、前記リストテーブルを参照して圧縮コード列に変換するステップと、
前記変換された圧縮コード列をカバー画像に埋め込み、ステゴ画像を形成するステップと、
前記形成されたステゴ画像を受信側に送信するステップと、
受信側で、
前記ステゴ画像を受信するステップと、
受信したステゴ画像から埋め込まれた圧縮コード列を分離してカバー画像を復元するステップと、
更に、前記分離した圧縮コード列から前記リストテーブルを参照して前記秘密データを復号するステップ有する、
ことを特徴とする秘密データの隠蔽方法。
【請求項２】
請求項１において、
さらに、送信側で、
前記圧縮コード列に対し、ロスレス符号化を行うステップと、
前記ロスレス符号化の結果に対して、ポータブル暗号化を行うステップを有し、
前記ポータブル暗号化されたデータを前記カバー画像に埋め込ませる、
ことを特徴とする秘密データの隠蔽方法。
【請求項３】
請求項２において、
前記ロスレス符号化はハフマン符号化、及び前記ポータブル暗号化はＸＯＲ暗号化である、
ことを特徴とする秘密データの隠蔽方法。
【請求項４】
請求項１乃至３の何れか１項において、
前記リストテーブルは、秘密データがテキストデータであるとき、単語及び短文をリストの項番に対応付けられたボキャブラリテーブルであって、前記圧縮コード列に変換するステップは、前記秘密データの単語を対応するリストの項番に変換して出力する、
ことを特徴とする秘密データの隠蔽方法。
【請求項５】
請求項１乃至３の何れか１項において、
前記リストテーブルは、秘密データが画像、音声などの非テキストデータであるとき、ベクトル量子化（VQ：Vector Quantization）された前記非テキストデータがリストの項番に対応付けられたコードブック（codebook）であって、前記圧縮コード列に変換するステップは、前記秘密データのベクトル量子化に対応するリストの項番に変換して出力する、
ことを特徴とする秘密データの隠蔽方法。
【請求項６】
送信側から受信側に送信される秘密データの隠蔽を実行するプログラムであって、
送信側の処理装置に、
秘密データを、リストテーブルを参照して圧縮コード列に変換するステップと、
前記変換された圧縮コード列をカバー画像に埋め込み、ステゴ画像を形成するステップと、
前記形成されたステゴ画像を受信側に送信するステップを実行させ、
受信側の処理装置に、

前記ステゴ画像を受信するステップと、
受信したステゴ画像から埋め込まれた圧縮コード列を分離してカバー画像を復元するステップと、
更に、前記分離した圧縮コード列から前記リストテーブルを参照して前記秘密データを復号するステップを実行させる
ことを特徴とする秘密データの隠蔽を実施するプログラム。
【請求項７】
請求項６において、
さらに、送信の処理装置に、
前記圧縮コード列に対し、ロスレス符号化を行うステップと、
前記ロスレス符号化の結果に対して、ポータブル暗号化を行うステップを実行させ、
前記ポータブル暗号化されたデータを前記カバー画像に埋め込ませる、
ことを特徴とする秘密データの隠蔽を実施するプログラム。
【請求項８】
請求項７において、
前記ロスレス符号化としてハフマン符号化、前記ポータブル暗号化としてＸＯＲ暗号化を行わせる、
ことを特徴とする秘密データの隠蔽を実施するプログラム。
【請求項９】
請求項６乃至８の何れか１項において、
前記リストテーブルは、秘密データがテキストデータであるとき、単語及び短文をリストの項番に対応付けられたボキャブラリテーブルであって、前記圧縮コード列に変換するステップは、前記秘密データの単語を対応するリストの項番に変換して出力する、
ことを特徴とする秘密データの隠蔽を実施するプログラム。
【請求項１０】
請求項６乃至８の何れか１項において、
前記リストテーブルは、秘密データが画像、音声などの非テキストデータであるとき、ベクトル量子化（VQ：Vector Quantization）された前記非テキストデータがリストの項番に対応付けられたコードブック（codebook）であって、前記圧縮コード列に変換するステップは、前記秘密データのベクトル量子化に対応するリストの項番に変換して出力する、
ことを特徴とする秘密データの隠蔽を実施するプログラム。
【請求項１１】
送信側から受信側に秘密データを送信する秘密データ通信システムであって、
送信側と受信側に共通のリストテーブルを有し、
送信側に処理装置を有し、
前記送信側の処理装置により、
前記秘密データを、前記リストテーブルを参照して圧縮コード列に変換するステップと、
前記変換された圧縮コード列をカバー画像に埋め込み、ステゴ画像を形成するステップと、
前記形成されたステゴ画像を受信側に送信するステップを実行し、更に
受信側に処理装置を有し、
前記受信側の処理装置により、
前記ステゴ画像を受信するステップと、
受信したステゴ画像から埋め込まれた圧縮コード列を分離してカバー画像を復元するステップと、
更に、前記分離した圧縮コード列から前記リストテーブルを参照して前記秘密データを復号するステップを実行する、
ことを特徴とする秘密データ通信システム。

【請求項１２】
請求項１１において、
さらに、送信側の処理装置で、
前記圧縮コード列に対し、ロスレス符号化を行うステップと、
前記ロスレス符号化の結果に対して、ポータブル暗号化を行うステップを有し、
前記ポータブル暗号化されたデータを前記カバー画像に埋め込むステップを実行する、
ことを特徴とする秘密データ通信システム。
【請求項１３】
請求項１２において、
前記ロスレス符号化としてハフマン符号化、前記ポータブル暗号化としてＸＯＲ暗号化を行う、
ことを特徴とする秘密データ通信システム。
【請求項１４】
請求項１１乃至１３の何れか１項において、
前記リストテーブルは、秘密データがテキストデータであるとき、単語及び短文をリストの項番に対応付けられたボキャブラリテーブルであって、前記圧縮コード列に変換するステップは、前記秘密データの単語を対応するリストの項番に変換して出力する、
ことを特徴とする秘密データ通信システム。
【請求項１５】
請求項１１乃至１３の何れか１項において、
前記リストテーブルは、秘密データが画像、音声などの非テキストデータであるとき、ベクトル量子化（VQ：Vector Quantization）された前記非テキストデータがリストの項番に対応付けられたコードブック（codebook）であって、前記圧縮コード列に変換するステップは、前記秘密データのベクトル量子化に対応するリストの項番に変換して出力する、
ことを特徴とする秘密データ通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、秘密データの隠蔽方法、これを実施するプログラム、及び秘密データの通信システムに関する。
【背景技術】
【０００２】
近年、インターネットを通しての秘密処理の急速な進展により、違法な第三者の攻撃から秘密データを守るために、効率の良い情報の隠蔽方法が求められている。
【０００３】
そして、個人的あるいは、重要情報でマルチメディアに埋め込まれるデータ情報の送信におけるセキュリティを確保するための種々の情報隠蔽技術が多くの研究者により発明されている。
【０００４】
情報隠蔽、即ちステガノグラフィ技術は、画像、ビデオ、テキスト、あるいは他の種類のマルチメディアデータをカバーデータ（キャリア）として用い、キャリアに秘密データを埋め込むものである。多くの場合、人は、マルチメディアデータに埋め込まれている個人的あるいは、重要情報の存在に気づくことはない。それ故に、ある意味では情報隠蔽により、暗号化よりもより良く情報の保護を行うことが可能である。
【０００５】
情報隠蔽技術は、キャリア（例えば、画像）の復元を必要とするか否かにより大まかに２つのタイプ、即ち、可逆か非可逆かに分類できる。可逆隠蔽情報にあっては、当該可逆隠蔽情報から埋め込まれている秘密データを抽出する際、元のキャリアを復元することができる。これにより医療、軍事といった、あるいは他の敏感なデータの保護に役立てるこ

とが可能である。
【０００６】
可逆情報隠蔽は、過去１０年において、広く研究され、４つの主なタイプにクラス分けできる。すなわち、差拡張法（difference expansion:ＤＥ）、ヒストグラムシフト法（histogram shifting：ＨＳ）、デュアルイメージ法(dual images)、及びピクセル値順序付け法（pixel value ordering：ＰＶＯ）である。
【０００７】
差拡張法（ＤＥ）は、二つの隣接ピクセルをグループとして用い、秘密データを埋め込む前に、幾度か差を拡張するものである。2003年に、Tian，他が、古典的な差拡張法を提案している（非特許文献１）。この方法は、２つのピクセルの差を計算し、その差の値を２倍に拡張し、秘密データの１ビットを埋め込むものである。
【０００８】
ヒストグラムシフト法（ＨＳ）は、予測エラー周波数の統計を用い、予測エラーヒストグラムを生成し、高周波領域に秘密データを埋め込むものである。2006年に、Ni，他が、ヒストグラムシフトを提案している（非特許文献２）。2009年に、Tsai，他が、直線予測を用いてエラー値を生成して、正及び負のヒストグラムを構成し、秘密データを高周波領域に埋め込んでいる（非特許文献３）。
【０００９】
デュアルイメージ法(dual images) は、秘密データを埋め込む前に、オリジナルの画像から同じサイズの２つのステゴ（stego）画像を複写するものである。この方法は、近年、より一般になっている。なぜならば、埋め込む情報を大きくすることができるという意味がある。2015年に、Lu，他が最下位ビット（least significant bit）に基づく、デュアルイメージ法を提案している（非特許文献４）。この方法は、最下位ビット法を用いて二つのステゴ画像に対するピクセル値を生成し、それぞれ二つのピクセルの平均値を計算し、ステゴピクセルが復元されたか否かを判定する。Lu,他は、同じ年に、中央折り返し法（center folding strategy）に基づくデュアルイメージ法を提案している（非特許文献５）。この方法は、秘密データのサイズを効果的に削減し、低歪を得ることができ、従って、復元される画像の品質を良くすることができる。
【００１０】
上記に述べた３つの方法以外に、ピクセル値順序付け法（ＰＶＯ）が、データの可逆秘匿にしばしば用いられる。ＰＶＯ法は、画像をいくつかのサイズのブロックに分割し、それぞれのブロックにおける全ピクセル値を昇順に分類し、最大または最小値に、秘密データを埋め込む。Li,他が、2013年に古典的ＰＶＯ法を提案している。
【００１１】
この方法では、それぞれ分割されたブロックにおいて全てのピクセル値をソートして予測エラーを求め、“maximum minus second maximum” か、“minimum minus second minimum”を用いて秘密データを埋め込む（非特許文献６）。QuとKimは、Liの方法を改良し、2015年にpixel based pixel value ordering(ＰＰＶＯ)を提案している（非特許文献７）。
【００１２】
上記をまとめると、大半の研究者は、いかに埋め込み法を改良して高画像品質を得るかに焦点を当てているが、少数の学者は、ステゴ画像の品質に影響を与える重要な要因である秘密データのサイズを検討してきた。
【先行技術文献】
【特許文献】
【００１３】
【特許文献１】特許第５９３９５７２号公報
【特許文献２】特開２０１３－１６７８６５号
【非特許文献】
【００１４】

【非特許文献１】J. Tian, “Reversible Data Hiding Using a Difference Expansion, ”IEEE Transactions on Circuits and Systems for Video Technology, Vol.13, No. 8, pp.890-896, Aug.2003.
【非特許文献２】Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, “Reversible Data Hiding, ”IEEE Transactions on Circuits and Systems for Video Technology, Vol.16, No. 3, pp.354-362, Mar.2006.
【非特許文献３】P. Tsai, Y.C. Hu, and H.L. Yeh, “Reversible Image Hiding Scheme Using Predictive Coding and Histogram Shifting,”Signal Processing, Vol.89, pp. 1129-1143, Jun.2009.
【非特許文献４】T.C. Lu, C.Y. Tseng, and J.H. Wu, “Dual Imaging-based Reversible Hiding Technique Using LSB Matching,” Signal Processing, Vol.108, pp.77-89, Mar.2015.
【非特許文献５】T.C. Lu, J.H. Wu, and C.C. Huang, “Dual-Image-Based Reversible Data Hiding Method Using Center Folding Strategy,”Signal Processing, Vol.115, pp.195-213, Oct.2015.
【非特許文献６】X.L. Li, J. Li, B. Li, and B. Yang, “High-Fidelity Reversible Data Hiding Scheme Based on Pixel-Value-Ordering and Prediction Error-Expansion, ”Signal Processing, Vol.93, Issue 1, pp.198-205, Jan.2013.
【非特許文献７】X.Qu, H.J.Kim, “Pixel-Based Pixel Value Ordering Predictor for High-Fidelity Reversible Data Hiding,”Signal Processing, Vol.111, pp. 249-260, Jun.2015.

【発明の概要】
【発明が解決しようとする課題】
【００１５】
ここで、上記秘匿データの送信においては、そのデータサイズと通信における秘匿性が重要である。したがって、本発明の目的は、上記の背景技術に鑑みて、データサイズを削減するとともによりセキュリティを高める秘密データの隠蔽方法、これを実施するプログラム、及び秘密データ通信システムを提供することにある。
【課題を解決するための手段】
【００１６】
上記課題を達成する本発明は、第１の側面として、送信側から受信側に送信される秘密データの隠蔽方法であって、送信側と受信側に共通のリストテーブルを有し、送信側で、秘密データを、前記リストテーブルを参照して圧縮コード列に変換するステップと、前記変換された圧縮コード列をカバー画像に埋め込み、ステゴ画像を形成するステップと、前記形成されたステゴ画像を受信側に送信するステップと、受信側で、前記ステゴ画像を受信するステップと、受信したステゴ画像から埋め込まれた圧縮コード列を分離してカバー画像を復元するステップと、更に、前記分離した圧縮コード列から前記リストテーブルを参照して前記秘密データを復号するステップ有することを特徴とする。
【００１７】
上記課題を達成する本発明は、第２の側面として、送信側から受信側に送信される秘密データの隠蔽を実行するプログラムであって、送信側の処理装置に、秘密データを、リストテーブルを参照して圧縮コード列に変換するステップと、前記変換された圧縮コード列をカバー画像に埋め込み、ステゴ画像を形成するステップと、前記形成されたステゴ画像を受信側に送信するステップを実行させ、受信側の処理装置に、前記ステゴ画像を受信するステップと、受信したステゴ画像から埋め込まれた圧縮コード列を分離してカバー画像を復元するステップと、更に前記分離した圧縮コード列から前記リストテーブルを参照して前記秘密データを復号するステップを実行させることを特徴とする。
【００１８】
上記課題を達成する本発明は、第３の側面として、送信側から受信側に秘密データを送信する秘密データ通信システムであって、送信側と受信側に共通のリストテーブルを有し

、送信側に処理装置を有し、前記送信側の処理装置により、前記秘密データを、前記リストテーブルを参照して圧縮コード列に変換するステップと、前記変換された圧縮コード列をカバー画像に埋め込み、ステゴ画像を形成するステップと、前記形成されたステゴ画像を受信側に送信するステップを実行し、更に受信側に処理装置を有し、前記受信側の処理装置により、前記ステゴ画像を受信するステップと、受信したステゴ画像から埋め込まれた圧縮コード列を分離してカバー画像を復元するステップと、更に、前記分離した圧縮コード列から前記リストテーブルを参照して前記秘密データを復号するステップを実行することを特徴とする。

【００１９】

上記課題を達成する本発明は、前記第１、第２及び第３の側面において、第１の態様として、送信側で、前記圧縮コード列に対し、ロスレス符号化を行い、前記ロスレス符号化の結果に対して、ポータブル暗号化を行い、前記ポータブル暗号化されたデータを前記カバー画像に埋め込むことを特徴とする。

【００２０】

上記課題を達成する本発明は、前記第１、第２及び第３の側面において、第２の態様として、前記ロスレス符号化としてハフマン符号化、前記ポータブル暗号化としてＸＯＲ暗号化を行うことを特徴とする。

【００２１】

上記課題を達成する本発明は、前記第１、第２及び第３の側面において、第３の態様として、前記リストテーブルは、秘密データがテキストデータであるとき、単語及び短文をリストの項番に対応付けられたボキャブラリテーブルであって、前記圧縮コード列に変換するステップは、前記秘密データの単語を対応するリストの項番に変換して出力することを特徴とする。

【００２２】

上記課題を達成する本発明は、前記第１、第２及び第３の側面において、第４の態様として、前記リストテーブルは、秘密データが画像、音声などの非テキストデータであるとき、ベクトル量子化（VQ：Vector Quantization）された前記非テキストデータがリストの項番に対応付けられたコードブック（codebook）であって、前記圧縮コード列に変換するステップは、前記秘密データのベクトル量子化に対応するリストの項番に変換して出力することを特徴とする。

【図面の簡単な説明】

【００２３】

【図１】本発明に従う秘密データの隠蔽方法を用いる秘密データ通信システムの概念構成図である。

【図２】本発明に従う秘密データの隠蔽方法の手順を示す処理フローである。

【図３】ボキャブラリテーブル（単語テーブル）の一例を理解容易に簡略して示す図である。

【図４】入力データを、単語テーブルを参照してインデックスに変換した結果を示す図である。

【図５】ボキャブラリテーブルにより変換されたインデックス列における、インデックス(シンボル)の発生回数をまとめたテーブルである。

【図６】図５のテーブルに基づいて構成されたハフマンツリーを示す図である。

【図７】シンボルの発生回数に基づき割り当てられたハフマンコードテーブルの例である。

【図８】ＸＯＲ暗号化を説明する図である。

【図９】ＰＰＶＯ法の処理過程を示す図である。

【図１０】８つのグレイスケール画像を示す図である。

【図１１】ハフマン符号化圧縮に用いるデータ量と生データ量を比較する表である。

【図１２】容量が10,000ビットに等しい時、同じ埋め込み容量で、本発明とＰＰＶＯの画像品質を比較した表である。

【図１３】容量が20,000ビットに等しい時、同じ埋め込み容量で、本発明とＰＰＶＯの画像品質を比較した表である。
【発明を実施するための形態】
【００２４】
本発明の基本概念は、送信側と受信側で、同じリストテーブル、例えばボキャブラリテーブル（Vocabulary Table）を共有する。そして、元の秘密のテキストデータにおける単語（word）あるいは短文を前記ボキャブラリテーブル（以下、単語テーブルと表記）にリストされた単語（あるいは短文）のアドレス又はインデックスを用いて表す。これにより、第三者は、同じ単語順の同じ単語テーブルを有しない限り、ステゴ（stego）画像からデータを抽出したとしても、元の秘密データを復元することができない。
【００２５】
ここで、本発明の適用は、上記秘匿すべきデータがテキストデータである場合の他、画像、音声などの非テキストデータであってもよい。非テキストデータを隠蔽するときは、ベクトル量子化（VQ：Vector Quantization）を利用して、リストテーブルとしてボキャブラリテーブル（Vocabulary Table）に相当するコードブック（codebook）を求めればよい。したがって、本発明の説明において、秘匿すべきデータがテキストデータあるいは非テキストデータを含むものとして「秘密データ」と表記する。
【００２６】
この本発明の方法により、秘密データのデータサイズを小さく出来るとともに、よりセキュリティを高めることができる。
【００２７】
秘密データを表すビットの総数を削減するために、更に、ロスレス符号化（lossless coding）を追加することができる。ロスレス符号化の一例として、ハフマン符号化(Huffman Coding)が知られている。すなわち、頻繁に出現する単語のインデックスを短い二値の文字列（コード）に割り当てる。このコードを定義するために、各枝葉が単語のコードを規定する様に二値ツリーを生成する。かかるロスレス符号化であるハフマン符号化アルゴリズムを用いて、効率的に画像歪みを低減することができる。
【００２８】
さらに、本発明は、セキュリティを改良するために、ポータブル暗号化（Portable Encryption），例えば、ＸＯＲ暗号化を用いて秘密データを暗号化することもできる。
【００２９】
これにより、攻撃者がステガノ解析によりステゴ（stego）画像を検出しても、埋め込まれている秘密データを容易に特定することができない。
【００３０】
以下に、本発明の上記基本概念を実現する実施例を添付の図面に従い説明する。しかし、本発明は、これら実施例に限定されるものではなく、本発明の保護の範囲は、特許請求の範囲と同一又は類似の範囲にも及ぶ。
【００３１】
図１は、本発明に従う秘密データの隠蔽方法を実施するための秘密データ通信システムの概念構成図である。
【００３２】
実施例として端末１からサーバ２に秘密データを送信する通信システムを想定する。キャリア（カバーデータ）としての原画像に秘密データを埋め込ませてステゴ画像を生成して秘密データとして送信する。これにより原画像と秘密データをともに攻撃者から保護して送信することができる。
【００３３】
端末１とサーバ２は、情報処理装置として基本的に同じ機能構成で示される。さらに、端末１とサーバ２は、インターネット等のネットワーク３を介して接続される。したがって、遠隔地間であっても、相互に接続が可能である。
【００３４】

端末１は、バス１５に接続される構成要素として、演算処理を行う演算処理素子であるＣＰＵ１０、本発明の秘密データの隠蔽方法を実行するためのプログラム、及び送信側と受信側で同じリストテーブルを格納する固定記憶素子であるＲＯＭ１１、演算処理途中にデータを保存する一時記憶素子であるＲＡＭ１３、更に入力素子１２及び通信機能を有する出力素子１４等を有して構成される。

【００３５】

一方、サーバ２は、端末１と同様構成であって、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２３、更に入力素子２２及び出力素子２４等が、バス２５に接続されて構成されている。

【００３６】

図２は、本発明に従う秘密データの隠蔽方法の手順を示す処理フローである。

【００３７】

ステップＳ１－Ｓ４は、送信側（端末１）で実行され、ＲＯＭ１１に格納されるプログラムをＣＰＵ１０により実行して実現される処理であり、ステップＳ５－Ｓ８は、受信側（サーバ２）で実行され、ＲＯＭ２１に格納されるプログラムをＣＰＵ２０により実行して実現される処理である。

【００３８】

ここで、本発明の特徴として送信データのサイズを小さくするとともに、秘密データを保護するための特徴として第１に、端末１とサーバ２間で、実施例として秘密データが、テキストデータであるとき、リストテーブルとして同じボキャブラリテーブル（単語テーブル）をＲＯＭ１１，２１に保持している。秘密データが、非テキストデータであるときは、リストテーブルとしてコードブックを保持する。

【００３９】

以下は、実施例として、秘密データがテキストデータであるときを想定して説明する。

【００４０】

単語テーブルは、通信対象の秘密のテキストデータに現れる文字（単語、及び短文を含む）をインデックスリスト化したテーブルである。

【００４１】

通信対象の秘密データのテキスト種類に対応して、事前にテキストデータ（Ｐ１）を取集し、単語テーブルを作成して端末１とサーバ２のそれぞれのＲＯＭ１１，２１に登録しておく。

【００４２】

図３は、上記作成される単語テーブルの一例を理解容易に簡略して示す図である。

【００４３】

ボキャブラリ（単語）“And”,“This”,“an”,“another”,“difficult”,“example”,“is”, “of”,“stenography”に対して単語テーブルの順番をインデックスとして対応付けている。このインデックスの順番は、送信側と受信側で対応して定義され、後にデータ変換に対するキー（key）として使用される。

【００４４】

次いで、入力データとして秘密データ（Ｐ２）を入力素子１２により入力し、ＣＰＵ１０により、ＲＯＭ１１に登録してある単語テーブルを参照して、入力データ（Ｐ２）をインデックスのリストに変換する（ステップＳ１）。

【００４５】

図４は、入力データを、単語テーブルを参照してインデックスに変換した結果を示す図である。入力データ（Ｐ２）が、“This is an example of stenography. This example is difficult example.”という文章であるとき、この文章を構成するそれぞれの単語を単語テーブルのインデックスに変換することができる。すなわち、変換されたインデックス列は、“２７３６８９２６７５６”である。

【００４６】

このように変換されたインデックス列は、１１文字で構成されて上記の入力データ（Ｐ２）を表すことができるので、送信データのビット数サイズを小さくすることが可能であ

る。すなわち、１文字が８ビットで表示されるので、１１文字を８８ビットで表示できる。

【００４７】

同時に、受信側で同じ単語テーブルを用いなければ元の入力データに戻すことができない。したがって、データの通信途中における秘密保持を担保することができる。

【００４８】

次に、本発明では、秘密データ（Ｐ２）をキャリアとしての秘密画像である原画像（Ｐ４）に埋め込むことを考え、更に送信データのサイズを小さくする技術を付加することが可能である。

【００４９】

そのために、ロスレス符号化（lossless coding）の一例であるハフマン符号化(Huffman Coding)を用いる。図５は、上記ボキャブラリテーブル（単語テーブル）により変換されたインデックス列における、インデックス(シンボル)の発生回数をまとめたテーブルである。これを参照すると、最も発生回数の大きいシンボルは単語“example”に対応する“６”である。図５のテーブルに基づいて、ハフマンツリー（Huffman Tree）を構成してハフマン符号化を行って、更にデータを短縮することが可能である(ステップＳ２)。

【００５０】

図６は、かかる図５のテーブルに基づいて構成されたハフマンツリーを示す図である。このハフマンツリーにおいて、左分岐に“０”,右分岐に“１”を割り当てる。

【００５１】

シンボルの発生回数の大きい順に、ハフマンツリーによりコードを割り当てると図７に示すようなハフマンコードテーブルが得られる。左欄にシンボル、中欄に発生回数、そして右欄にハフマンツリーに基づくハフマンコードを対応して示している。

【００５２】

したがって、このハフマンコードテーブルにより先の秘密データ“This is an example of stenography. This example is difficult example.” は、次のようにハフマンコードで表される。

【００５３】

秘密データ＝001 000 101 01 111 110 001 01 000 100 01

ここで、更に秘密強化のためにポータブル暗号化（Portable Encryption），例えば、ＸＯＲ暗号化を用いて秘密データを暗号化することができる(ステップＳ３)。

【００５４】

図８は、ＸＯＲ暗号化を説明する図であり、暗号化キー（Ｐ３）として、例えば、バイナリ暗号化キー＝“ＡＢＣ”＝100000110000101000011を用いる。このバイナリ暗号化キー（Ｐ３）を用いて、ハフマンコードをＸＯＲ暗号化により暗号化して、より秘密性を高めることができる。

【００５５】

図８において、ステップＳ２で演算したハフマンコードとバイナリ暗号化キー（Ｐ３）の先頭ビットを合わせて、ＸＯＲを求める。次いで、バイナリ暗号化キーを１桁右方向にシフトして、前記ＸＯＲ演算結果とのＸＯＲを演算する。同様に、バイナリ暗号化キーをその最終桁位置が、ハフマンコードの最終桁位置と一致するまで順次シフトしながら繰り返しＸＯＲを求める。

【００５６】

図８において、最終のＸＯＲ演算結果は、“1101111101110011100001110100 00”という秘密コードになる。

【００５７】

次に、この最終のＸＯＲ演算結果である秘密コードをキャリアである原画像（Ｐ４）に埋め込みステゴ画像を生成して両者を秘匿する(ステップＳ４)。

【００５８】

ここで、実施例として、キャリアへの秘密コードの埋め込みをＰＰＶＯ法（Pixel base

d Pixel Value Ordering）を用いて行う。

【００５９】

ＰＰＶＯ法は、Qu,他により２０１５年に提案された。この方法は、スライディング窓を用い、原画像の全てのピクセルを埋め込みに用い、秘密コードの埋め込みの間、ただ一つのピクセルが、スライディング窓において変化され、より高度の埋め込み容量を得ることが可能である。

【００６０】

この方法は、参照ピクセルを用いて埋め込ケースを決定する。参照ピクセルが、最大もしくは最小ピクセルと等しい場合、ブロックに秘密データを埋め込むことができることを意味している。

【００６１】

秘密データを埋め込む前に、ピクセルを順方向にソートして順序付けられた系列（$x_{\pi(1)}$，$x_{\pi(2)}$，…，$x_{\pi(n-1)}$）を得る（スライディング窓にｎピクセルあると想定）。次いで、参照ピクセルを以下のケースに従い修正する。

【００６２】

ケース１：$x_{\pi(1)} \neq x_{\pi(n-1)}$である場合、参照ピクセル$x_t$が修正される。そして、秘密コードb∈{0,1}が埋め込まれ、式（１）のように計算される。

【００６３】

【数１】

$$x'_t = \begin{cases} x_t - 1, & if\ x_t < x_{\pi(1)} \\ x_t - b, & if\ x_t = x_{\pi(1)} \\ x_t + 1, & if\ x_t > x_{\pi(n-1)} \\ x_t + b, & if\ x_t = x_{\pi(n-1)} \\ skip, if\ x_t > x_{\pi(1)} \| x_t < x_{\pi(n-1)} \end{cases} \qquad (1)$$

【００６４】

ケース２：$x_{\pi(1)} = x_{\pi(n-1)}$である場合、系列のピクセルが全て等しいことを意味し、等しい値をＶＣ値と呼び、参照ピクセルは、（２）式のように修正される。

【００６５】

【数２】

$$x'_t = \begin{cases} x_t + b, & if\ x_t = VC = 254 \\ x_t - b, & if\ x_t = VC < 254 \\ x_t - 1, & if\ x_t < VC \\ skip, & if\ x_t > VC \end{cases} \qquad (2)$$

【００６６】

先に背景技術において説明したＰＶＯ法は、ピクセルをスムース領域にするブロック仕様に秘密コードを埋め込むので、秘密コードの埋め込みに対して効率的に用いられない。これに対してＰＰＶＯ法は、非重畳ブロックの代わりにスライディング窓を用いてブロック制約を回避する。このことは、容量と画像品質を著しく改善する。

【００６７】

本発明の実施例説明に戻ると、ｈ×ｗピクセルの原画像Ｘ（Ｐ４）に埋め込み処理を行う。まず、スライディング窓に対してブロックサイズｎ×ｎを設定する。各ブロックに対して、それぞれ上部の左隅のピクセルを参照ピクセル値とし、ピクセルを順方向にソートして参照ピクセルを除く順序列を得る。上記式（１）または（２）に従い、ブロックに秘密コードを埋め込むことが可能か否かを決定する。

【００６８】

例えば、ＰＰＶＯ法の処理過程を示す図９において、２×３の原画像Ｘ＝｛45，35，30，45，39，40｝と秘密コードＳ＝１０を想定する。

【００６９】
最初のピクセル値“４５”が参照ピクセルであり、他のピクセルがソートされる。ついで秘密コードを埋め込むブロックを決定するために式（１）を用いると、参照ピクセルは“４６”に修正される。

【００７０】
スライディング窓の第２のブロック｛35，30，39，40｝において、第１のピクセル値“３５”が参照ピクセルとなり、他のピクセルがソートされる。ついで、参照ピクセル値が最大と最小値の間にあるので、参照ブロックは修正されないので、式（１）を用いてブロックの決定がスキップされる。

【００７１】
図２に戻り、原画像（Ｐ４）が、埋め込み処理（Ｓ４）により秘密コードが埋め込まれたステゴ画像（Ｐ５）が得られる。

【００７２】
このステゴ画像（Ｐ５）が秘密データとしてサーバ２に送られ、秘密データ抽出処理（ステップＳ５）が行われる。この秘密データ抽出処理（ステップＳ５）において、原画像（Ｐ４）と秘密コード（Ｐ６）に分離される。

【００７３】
すなわち、秘密データ抽出処理（ステップＳ５）において、参照ピクセルを除いて、スライディング窓におけるピクセル値がソートされる。そして秘密コード（Ｐ６）を抽出し、原画像（Ｐ４）のピクセル値を復元することができる。これは、次の式（３）、または（４）を用いて計算できる。

【００７４】
【数３】

$$x_t=\begin{cases} x_t'+1 & if\ x_t'<x_{\pi(1)}' \\ x_t',b=0, & if\ x_t'=x_{\pi(1)}' \\ x_t'+1,b=1, & if\ x_t'=x_{\pi(1)}'-1 \\ x_t'-1 & if\ x_t'>x_{\pi(n-1)}' \\ x_t',b=0, & if\ x_t'=x_{\pi(n-1)}' \\ x_t'-1,b=1, & if\ x_t'=x_{\pi(n-1)}'+1 \\ skip, if\ x_t'>x_{\pi(1)}' \| x_t'<x_{\pi(n-1)}' \end{cases} \qquad (3)$$

【００７５】
【数４】

$$x_t=\begin{cases} x_t',b=0, & if\ x_t'=VC=254 \\ x_t',b=1, & if\ x_t'=VC=253 \\ x_t',b=0, & if\ x_t'=VC<254 \\ x_t'+1,b=1, & if\ x_t'=VC<253 \\ x_t'+1, & if\ x_t'<VC \\ skip, & if\ x_t'>VC \end{cases} \qquad (4)$$

【００７６】
秘密コード（Ｐ６）を抽出した後、上記ステップＳ１-Ｓ３に対応する次の３ステップにより逆処理が行われて秘密データ（Ｐ２）を復元する。

【００７７】
（１）ＸＯＲ復号化（ステップＳ６）
ＸＯＲ復号化により二値復号化を用いてハフマン符号化された状態の秘密データを復号

化する。
【００７８】
例えば、秘密コードＰ６＝“11011001010”が抽出され、復号化キーＰ７＝“1000001”ガ入力され、この復号化キーＰ７を用いてＸＯＲ復号化（ステップＳ６）が行われ、秘密コードＰ６を復号し、“00100010101”を得る。
【００７９】
（２）ハフマン復号化（ステップＳ７）
ハフマン符号化では、シンボルの全てが一度だけ符号化される。それゆえ、それぞれのシンボルに対して、ユニークな符号ワードがあることを意味する。したがって、ハフマンツリーに従い、圧縮前のシンボルに変換する。
【００８０】
上記ＸＯＲ復号化（ステップＳ６）により得られた“00100010101”をハフマン復号化すると、001，000，101，01が得られる。
【００８１】
（３）単語テーブルによる復元（Ｓ８）
単語テーブルに従って、インデックス番号により元の秘密データ（Ｐ２）を復元することができる。
【００８２】
最終的に単語テーブルを用いると、ハフマン復号化して得られる２値コード列001，000，101，01から元の秘密データ＝“This is an example”が復元できる。
【００８３】
上記に述べた本発明の適用例として、原画像が患者の医療画像であり、秘密データが患者の医療測定数値等であると想定すると、本発明の適用により、医療画像と患者固有の医療数値データが、送信可能にデータ量が圧縮されるとともに、両者を秘匿した秘密データとして送信することが可能である。
【００８４】
したがって、本発明の適用により患者の個人情報を秘匿しながら遠隔地医療を行うようなシステムへの適用も可能である。
【００８５】
ここで、上記本発明の効果の実験による実証結果について以下に説明する。
【００８６】
本発明者は、Matlab R2015bを用いて本発明方法を構築し、実験のため８つのグレイスケール画像を用いた。８つのグレイスケール画像は、図１０に示すようであり、Waterloo Greyscale Set2 (http://links.uwaterloo.ca/Repository.html)から得られる画像であり、５１２×５１２標準８ビットのグレイスケール画像である。
【００８７】
図１１は、ハフマン符号化圧縮に用いるデータ量と生データ量を比較する表である。
【００８８】
生データは、ASCIIの15,920文字を有する。それぞれの文字を８ビット２値に変換すると127,360ビットとなる。ハフマン符号化圧縮の段階では、69,044ビット（データ圧縮率1.844，スペース削減率45.78%）であるが、ポータブル暗号化までを行う本発明を用いると、23,781ビット（データ圧縮率5.355，スペース削減率81.32%）まで圧縮することができる。
【００８９】
図１１におけるデータ圧縮率及びスペース削減率は、式（５），（６）の関係式により計算して求めている。
【００９０】
データ圧縮率＝生データ量／圧縮データ量　　（５）
スペース削減率＝（生データ量－圧縮データ量）／生データ量　　（６）
【００９１】

本発明に従う前処理により78.6％のデータスペース削減が可能である。

【００９２】

つぎに、ピーク信号対ノイズ比（ＰＳＮＲ）を用いて原画像とステゴ画像の差を評価する。

【００９３】

ＰＳＮＲは、次式（７）により表される。

【００９４】

【数５】

$$PSNR = 10 \times log_{10}\left[\frac{255^2}{\frac{1}{h\times w}\times\sum_{i=1}^{h}\sum_{j=1}^{w}(x'_{i,j}-x_{i,j})^2}\right] \qquad (7)$$

【００９５】

ここで、ｈ×ｗは、全体画像のサイズであり、$x'_{i,j}$と$x_{i,j}$は、ステゴ画像と原画像のピクセルである。二つの画像間の差が小さいほど、ステゴ画像は、知覚不能であり、ＰＳＮＲが大きくなる。反対に、差が大きいほど画像品質が悪く、ＰＳＮＲが小さくなる。

【００９６】

ＰＳＮＲ値に関しては、多くの場合、ＰＰＶＯはより大きいＰＳＮＲになる。ＰＰＶＯの優れた点は、大きなサイズで明確に示される。非常にスムースな画像、例えばWashsat（図１０参照）では、ＰＳＮＲは、６０ｄＢ以上が得られる。

【００９７】

10,000 と20,000ビットを埋め込み、本発明とＰＰＶＯとを比較した。その結果はそれぞれ図１２と図１３の表に示される。

【００９８】

図１２は、容量が10,000ビットに等しい時、同じ埋め込み容量で、本発明とＰＰＶＯの画像品質(dB値)を比較した表である。図１３は、容量が20,000ビットに等しい時、同じ埋め込み容量で、本発明とＰＰＶＯの画像品質を比較した表である。

【００９９】

図１２、図１３において、図１０に示す画像ごとに本発明とＰＰＶＯとを比較している。ペイロードが10,000ビットであるとき、本発明では、実容量は53,550ビットの埋め込み（隠ぺい）が可能であり、ＰＰＶＯより約43,550ビット多く、ＰＳＮＲも平均的に約0.4ｄＢ以上になる。

【０１００】

ペイロードが20,000ビットであるとき、同様に本発明では、実容量は107,100ビットの埋め込みが可能であり、ＰＰＶＯより約87,100ビット多く、ＰＳＮＲも平均的に約0.5ｄＢ以上になる。

【０１０１】

上記したように、本発明により、可逆ステガノグラフィの新しい方法が提供される。

【０１０２】

データの共用とハフマン符号化によりデータサイズを削減し、これにより埋め込み処理における歪を現象することができる。埋め込みと抽出にはＰＰＶＯ法を用いる。

【０１０３】

実験により埋め込み容量を大幅に削減できることを示している。さらに、本発明により秘密データのセキュリティを高めることができる。

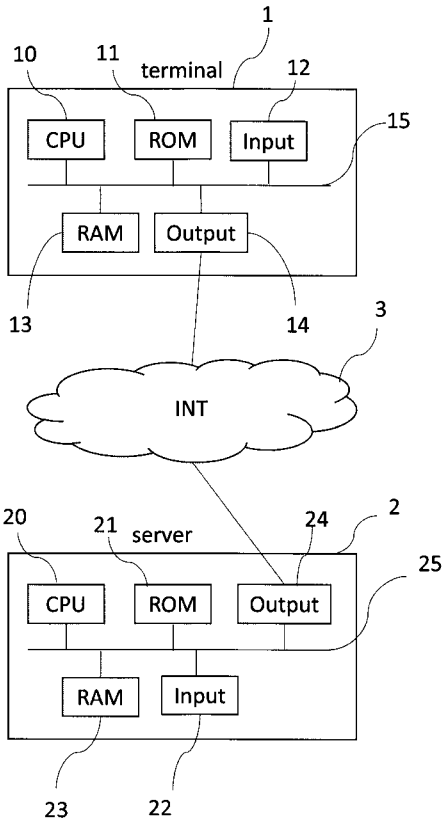
【符号の説明】

【０１０４】

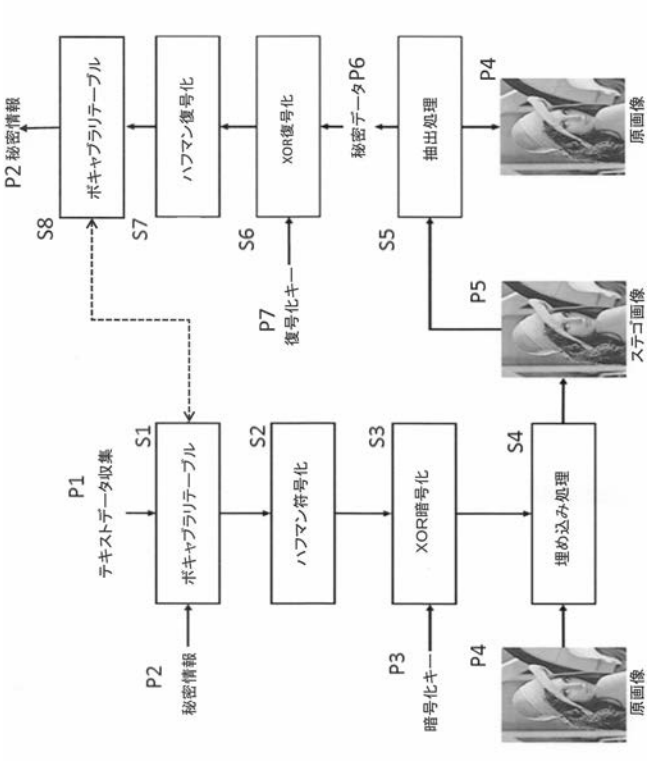
１　端末
２　サーバ
３　ネットワーク

１０，２０　ＣＰＵ
１１，２１　ＲＯＭ
１２，２２　入力素子
１３，２３　ＲＡＭ
１４，２４　出力素子
１５，２５　バス

【図１】



【図２】



【図３】

Vocabulary	Index
And	1
This	2
an	3
another	4
difficult	5
example	6
is	7
of	8
steganography.	9

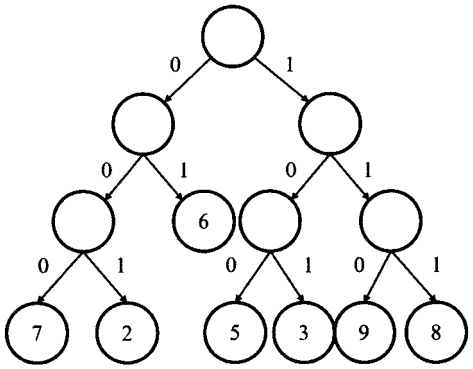
【図４】

This	is	an	example	of	steganography.
2	7	3	6	8	9
This	example	is	difficult	example	
2	6	7	5	6	

【図５】

Symbol	Occurrences
2	2
7	2
3	1
6	3
8	1
9	1
5	1

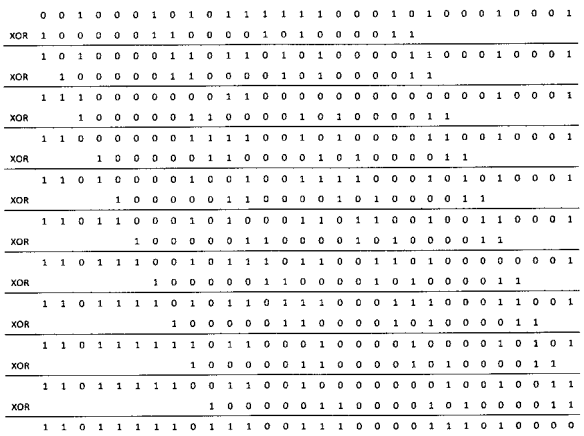
【図６】



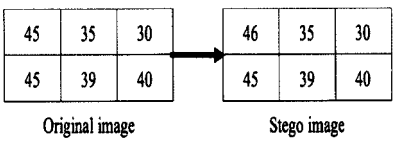
【図７】

Symbol	Occurrences	Huffman code
6	3	01
7	2	000
2	2	001
9	1	110
8	1	111
5	1	100
3	1	101

【図８】



【図９】



【図１０】

【図１１】

生データ	ハフマン符号化	本発明方法
127,360 bits	69,044 bits	23,781 bits
データ圧縮率 Data compression ratio	1.844	5.355
スペース削減率 Rate of space saving	45.78%	81.32%

【図１２】

画像 Image	PPVO 10,000 bits	本発明 10,000 bits (Real capacity: 53,550 bits)
Lena	58.73	58.99
Mandrill	55.34	55.84
Pepper	57.12	57.35
Barbara	57.01	57.12
Boat	60.91	61.11
Goldhill	59.25	59.37
Washsat	63.97	64.29
Zelda	57.44	57.79

【図１３】

Image	PPVO 20,000 bits	Proposed method 20,000 bits (Real capacity: 107,100 bits)
Lena	54.9	55.02
Mandrill	55.35	55.85
Pepper	54.56	55.25
Barbara	54.65	55.02
Boat	56.86	57.04
Goldhill	55.12	55.57
Washsat	60.92	61.26
Zelda	54.56	54.81