

(19) 日本国特許庁 (JP)

(12) 特許公報 (B2)

(11) 特許番号

**特許第3672143号**

(P3672143)

(45) 発行日 平成17年7月13日 (2005.7.13)

(24) 登録日 平成17年4月28日 (2005.4.28)

(51) Int. Cl.<sup>7</sup>

F I

H 0 4 N	1/387	H 0 4 N	1/387		
H 0 4 L	9/18	H 0 4 N	1/41		Z
H 0 4 N	1/41	H 0 4 L	9/00	6 5 1	
H 0 4 N	7/24	H 0 4 N	7/13		Z

請求項の数 4

(全 8 頁)

(21) 出願番号 特願平9-22340  
 (22) 出願日 平成9年2月5日 (1997.2.5)  
 (65) 公開番号 特開平10-224342  
 (43) 公開日 平成10年8月21日 (1998.8.21)  
 審査請求日 平成13年5月15日 (2001.5.15)

(73) 特許権者 000004226  
 日本電信電話株式会社  
 東京都千代田区大手町二丁目3番1号  
 (74) 代理人 100066153  
 弁理士 草野 卓  
 (72) 発明者 守谷 健弘  
 東京都新宿区西新宿三丁目19番2号 日  
 本電信電話株式会社内  
 (72) 発明者 岩上 直樹  
 東京都新宿区西新宿三丁目19番2号 日  
 本電信電話株式会社内  
 (72) 発明者 高嶋 洋一  
 東京都新宿区西新宿三丁目19番2号 日  
 本電信電話株式会社内

最終頁に続く

(54) 【発明の名称】 電子すかし作成方法

(57) 【特許請求の範囲】

【請求項 1】

音声や画像の入力ベクトルを、デジタル符号化すると共にそのデジタル符号に電子すかし情報を埋め込む電子すかし作成方法において、

上記入力ベクトルと、上記電子すかし情報と、その電子すかし情報を埋め込むべきビット位置を指定する埋め込み位置指定情報とを入力し、

上記埋め込み位置指定情報により埋め込みが指定されていない部分については符号帳から、上記入力ベクトルとの予め決められた尺度での歪が最小となる量子化ベクトルのインデックスを求めて、そのインデックスを上記デジタル符号として出力し、

上記埋め込み位置指定情報により埋め込みが指定されている部分については、上記符号帳中の上記埋め込み指定されたインデックスのビットを、上記電子すかし情報に固定し、その固定されたインデックス中の量子化ベクトルから入力ベクトルとの予め決められた尺度での歪が最小となるものを選択し、そのインデックスを上記デジタル符号として出力することを特徴とする電子すかし作成方法。

【請求項 2】

ベクトル量子化されたインデックスよりなるデジタル符号列に電子すかし情報を埋め込む電子すかし作成方法において、

上記デジタル符号列と、上記電子すかし情報と、その電子すかし情報を埋め込むべきビット位置を指定する埋め込み位置指定情報とを入力し、

上記埋め込み位置指定情報により埋め込みが指定されていない部分については上記入力

デジタル符号をそのまま出力し、

上記埋め込み位置指定情報により埋め込みが指定されている部分については、上記ベクトル量子化に用いた符号帳の上記埋め込み指定されたインデックスのビットを、上記電子すかし情報に固定し、その固定されたインデックス中の量子化ベクトルから、上記入力インデックスと対応する量子化ベクトルとの予め決められた尺度での歪が最小となるものを選択し、そのインデックスを出力することを特徴とする電子すかし作成方法。

【請求項 3】

上記埋め込み位置指定情報により埋め込みが指定されている部分については、当該入力デジタル符号を、上記ベクトル量子化に用いた符号帳で復号して量子化ベクトルを得、この量子化ベクトルと、上記固定されたインデックス中の量子化ベクトルから、上記歪最小となる量子化ベクトルを選択することを特徴とする請求項 2 記載の電子すかし作成方法

10

【請求項 4】

上記埋め込み位置指定情報により埋め込みが指定されている部分については、上記符号帳の各量子化ベクトルごとに、その他の量子化ベクトルとの歪みが予め求められたテーブルから、上記入力デジタル符号の上記符号帳のインデックスを求め、これと、上記埋め込み指定され、上記すかし情報で固定された上記符号帳中のインデックスとの歪を上記テーブルより求め、その最小のインデックスを求めることを特徴とする請求項 2 記載の電子すかし作成方法。

【発明の詳細な説明】

20

【0001】

【発明の属する技術分野】

この発明は音声や画像をデジタル符号であらわして伝送や蓄積すると同時に、そのビット系列に秘密の情報（電子すかし情報）を埋め込んで不正利用を防ぐ、いわゆる電子すかし作成方法に関する。

【0002】

【従来の技術】

電子すかしは具体的には以下の 2 つの条件を同時に満たす仕組みを提供するものである。

(1) 通常の復号器では音声や画像が再生できるが、秘密の情報（電子すかし情報）はどこに書かれているか見つけることができないし、その秘密の情報を書き換えたり消したりしようとすると、再生された音声や画像に大きな劣化を生じる。

30

【0003】

(2) 一方、検査用の復号器では、別の暗号化された情報を使って秘密の情報（電子すかし情報）がどこに埋め込まれているかを捜して、秘密の情報を読み出すことができる。従来の電子すかし作成方法は画像などの情報圧縮ビット系列のうち、再生した時にほとんど品質が変わらないようなビット位置の中から、電子すかし情報（秘密の情報）を書き込む位置を選択してすかし情報を書き込む方法が知られている。しかし、情報圧縮率が高い場合や、音声や音楽の圧縮ビット系列ではすでに符号化されたビット系列のビットを強制的に書き換えると、大きな歪が生じる場合が多く、品質が変わらないようなビット位置がきわめて限定される。

40

【0004】

【発明が解決しようとする課題】

この発明の目的は電子すかし情報を書きこむ際にもとの音声や画像の量子化歪の増加を最小限に抑えることができる電子すかし作成方法を提供することにある。

【0005】

【課題を解決するための手段】

請求項 1 の発明によれば、入力ベクトルと、電子すかし情報と、その電子すかし情報を埋め込むべきビット位置を指定する埋め込み位置指定情報とを入力し、

上記埋め込み位置指定情報により埋め込みが指定されていない部分については符号帳から、上記入力ベクトルとの予め決められた尺度での歪が最小となる量子化ベクトルのインデ

50

ックスを求めて、そのインデックスを上記デジタル符号として出力し、上記埋め込み位置指定情報により埋め込みが指定されている部分については、上記符号帳中の上記埋め込み指定されたインデックスのビットを、上記電子すかし情報に固定し、その固定されたインデックス中の量子化ベクトルから入力ベクトルとの予め決められた尺度での歪が最小となるものを選択し、そのインデックスを上記デジタル符号として出力する。

#### 【0006】

請求項2の発明によれば、ベクトル量子化されたインデックスよりなるデジタル符号列と、電子すかし情報と、その電子すかし情報を埋め込むべきビット位置を指定する埋め込み位置指定情報とを入力し、

10

上記埋め込み位置指定情報により埋め込みが指定されていない部分については上記入力デジタル符号をそのまま出力し、

上記埋め込み位置指定情報により埋め込みが指定されている部分については、上記ベクトル量子化に用いた符号帳の上記埋め込み指定されたインデックスのビットを、上記電子すかし情報に固定し、その固定されたインデックス中の量子化ベクトルから、上記入力インデックスと対応する量子化ベクトルとの予め決められた尺度での歪が最小となるものを選択し、そのインデックスを出力する。

#### 【0007】

請求項3の発明では請求項2の発明において、上記埋め込み位置指定情報により埋め込みが指定されている部分については、当該入力デジタル符号を、上記ベクトル量子化に用いた符号帳で復号して量子化ベクトルを得、この量子化ベクトルと、上記固定されたインデックス中の量子化ベクトルから、上記歪最小となる量子化ベクトルを選択する。

20

#### 【0008】

請求項4の発明では請求項2の発明において、上記埋め込み位置指定情報により埋め込みが指定されている部分については、上記符号帳の各量子化ベクトルごとに、その他の量子化ベクトルとの歪みが予め求められたテーブルから、上記入力デジタル符号の上記符号帳のインデックスを求め、これと、上記埋め込み指定され、上記すかし情報で固定された上記符号帳中のインデックスとの歪を上記テーブルより求め、その最小のインデックスを求める。

#### 【0009】

以上述べたようにこの発明では一旦符号化されたビット系列に入力ベクトルと無関係に電子すかし情報を埋め込むのではなく、ベクトル量子化の符号帳探索の中で、電子すかし情報を埋め込んだ条件での最適なインデックスを探索することが特徴で、歪の増加を最小限に抑えることができる。

30

#### 【0010】

##### 【発明の実施の形態】

図1Aはこの発明の請求項第1項に対応する実施例を示す構成図である。この例では符号器11の処理の段階で、すかし情報を考慮した量子化ベクトルの探索を行なう。つまり図1Bに示すように入力端子12よりの画像信号、音響信号などの入力ベクトルが入力され、符号帳13から選択され、復号器14で復号された復号ベクトルと、入力ベクトルとの差が加算手段15でとられ、歪計算制御部16で予め決められた尺度での復号ベクトルと入力ベクトルに対する歪が最小となる量子化ベクトルが符号帳13から選択され、その選択された量子化ベクトルを示す符号帳13のインデックスInが符号化出力端子17から出力される。

40

#### 【0011】

この実施例では符号器11に端子18からすかし情報と、端子19から埋込み位置指定情報とが入力される。埋込み位置指定情報により埋込みが指定されていない場合は、入力ベクトルに対する符号化は先に述べたように従来と同様に行うが、埋込み位置指定情報によりすかし情報の埋込みが指定されている場合は、符号帳13のインデックス中の上記埋込み指定位置を、その時のすかし情報で固定して、符号帳13の量子化ベクトルを探索する

50

。つまり図 1 B に示すように選択制御部 2 1 において、埋込み位置指定情報とすかし情報とにより、符号帳 1 3 から検索する量子化ベクトルが制限される。

【 0 0 1 2 】

例えば図 2 A に示すように 5 ビットごとのインデックス  $I_{n1}$ ,  $I_{n2}$ , ... の符号化ビット系列のうち、図 2 B に示す埋込み位置指定情報により指定された位置のビットが図 2 C のすかし情報で固定される。この例ではインデックス  $I_{n1}$  は本来は、5 ビット 3 2 ベクトルの中から歪が最も小さくなる量子化ベクトルを探索するが、埋込み位置指定情報により 3 番目のビットが、すかし情報により 0 に固定される。従って図 2 D に示すように符号帳 1 3 中の 3 番目のビットが 0 であるインデックスに対する量子化ベクトル (計 1 6 個) の中から歪が一番小さいものを選ばれる。

10

【 0 0 1 3 】

この 1 6 個の中から選ばれたものはもともと 3 2 個の中でも最も歪が小さいものであったものと同じかも知れず、そうでなくても、1 6 個中から選択されたものは最適な量子化ベクトルとの差は平均的には非常に小さい。言い換えれば、このすかし情報が埋め込まれた符号化ビット系列を通常の復号器で再生すると、本来の出力との差は僅かである。

【 0 0 1 4 】

またどのビットが固定されて探索されたかは通常の復号器では検出は困難である。何故なら、符号化出力ビットを 1 ビットずつ反転して再生してみても、符号帳 1 3 の構成に依存して再生出力は劣化するが、特にすかし情報のビットでも同じように劣化し、そのビットのみで特徴があるわけではないからである。

20

従来の方法では、入力を考慮せずに、符号化ビットの一部を反転してすかし情報を書き込むので、そのビットを反転することでかえって品質が向上する場合がある。よってこの品質が向上するビットを検出してすかし情報を消去することが可能であるが、この発明の実施例では 1 ビットのみ反転では品質が向上する可能性は非常に少ない。確かにこの図の例では、3 2 種類のすべての組み合わせでインデックスを変更すると品質が向上する場合があるが、その品質向上はごくわずかであるからその向上するインデックスと符号化されたインデックスとを比較しても、すかし情報の位置やその情報を特定することはできない。また入力原音や原画の情報がなければ、客観的に品質が向上したかどうか検査する手段はなく、すかし情報の改ざんは難しい。

【 0 0 1 5 】

以上のすかし情報の改ざんは、通常の復号器の動作、つまり復号化手順、および復号化符号帳や、ビットの位置がすべて公開されていることを前提としているが、つまり全ての量子化ベクトルとそのインデックスとの関係がわかっていることを前提としている。しかし符号帳の一部でも非公開のビットがあると、すかし情報の改ざんは不可能と見なせる。例えば秘密の特定のビットに対する誤り検出符号 (例えばパリティビット) を追加して、そこで誤りが検出されれば復号を中止する処理を通常の復号器に組み合わせることが考えられる。すかし情報の部分のインデックスを少ない劣化で他のインデックスにたまたま置き換えること、つまり改ざんすることができても誤り検出符号で、それが検出され、出力を停止させることが可能であり、改ざんしたものを再生することはできない。

30

【 0 0 1 6 】

以上のようにこの実施例で符号化ビット系列に電子すかし情報を埋込むことができ、その電子すかし情報が埋込まれた符号化ビット系列が出力端子 1 7 に出力される。このすかし情報付符号化ビット系列は伝送又は蓄積された後、通常の復号器 2 4、つまりすかし情報が埋込まれない符号化ビット列に対する復号器 2 4 により復号化され、その出力端子 2 5 からすかし情報の付加にかかわらず、歪の劣化が少ない出力ベクトルが得られる。

40

【 0 0 1 7 】

すかし情報は符号化ビット系列から、すかし情報を取り出すにはすかし情報復号器 2 6 に入力し、符号器 1 1 側より得た埋込み位置指定情報により、すかし情報付符号化ビット系列からすかし情報ビットのみを取り出すことにすかし情報を出力端子 2 7 に得る。埋込み位置指定情報は通常、特別のものしか入手できないように、暗号化され、すかし情報復号器 2

50

6側で埋込み位置指定情報を復号化して、その埋込みビット位置を検出する。

【0018】

図3Aは請求項2の発明に対応する実施例を示すものである。

この例では入力端子31にすかし情報とは無関係に符号化された符号化ビット系列が入力される。つまり通常の符号器11で符号化された符号化ビット系列が伝送され、又は蓄積されたものが読出されて入力端子31よりすかし情報埋込み器32に入力され、原入力ベクトルの情報なしにすかし情報が書き込まれる。この際もとの音声や画像の劣化を小さく抑えるために、符号帳の中のすかし情報ビットが固定されたインデックスに対応する量子化ベクトルの中で、本来の再生ベクトルに最も近いもののインデックスに置き換える。つまりすかし情報埋込み器32においては、その入力端子31に入力された符号化ビット系列が符号化された際に用いた符号帳と同一の符号帳を備え、入力符号化ビット系列を再生し、その再生ベクトルを、図1について説明したように、端子19の埋込み位置指定情報にもとづき、符号帳のインデックスの1つのビットを、端子18のすかし情報で固定した、インデックスから選択した量子化ベクトル中の歪最小のもののインデックスを出力する。

10

【0019】

あるいは決められた歪尺度が、一定の場合は、例えば図3Bに示すように、各インデックス $I_{n1}$ ,  $I_{n2}$ , ...それぞれの量子化ベクトルについて、これと、他の各インデックスの量子化ベクトルとの歪をそれぞれ計算した歪表を用意しておき、また、各埋込み位置指定情報とすかし情報の組合せについて選択可能なインデックスの組を図3Cに示すように選択可能表として作っておき、端子18, 19のすかし情報と埋込み位置指定情報とから、図3Cの選択可能インデックス表を参照して選択可能インデックスの組を検出し、その検出した選択可能インデックスの組中のインデックスと、端子31に入力されたインデックスとの歪が最小のインデックスを図3Bの歪表を参照して探し、そのインデックスを出力端子17へ出力してもよい。あるいは、各入力インデックスについて、すかし情報とその埋込み位置の各場合について、歪最小のインデックスを予め求めておき、これを直ちに出力するようにしてもよい。

20

【0020】

この場合、入力情報を使う図1に示した実施例の場合よりすかし情報を埋込むことによる歪は大きくなるが、大きな劣化にはならず、通常の復号器で復号できる。また通常の復号器で、インデックスを取り替えることで品質が改善される可能性も図1の場合より少し大きくなる。しかし、すかし情報をいれるために毎回符号化する必要がないので処理が簡単になる。

30

【0021】

なお例えば聴覚重み付けベクトル量子化した場合のように歪尺度が、符号化ビット中のほかのパラメータに依存する場合には、そのパラメータを復号して歪尺度を計算し、その尺度で、最も近い量子化ベクトルのインデックスに置き換える必要がある。

【0022】

【発明の効果】

この発明によれば、下記の電子すかしの機能を実現でき、しかもこれによる本来の音声や画像からの劣化は僅かなものに抑えることが可能である。

40

(1) 通常の復号器では音声や画像が再生できるが、秘密の情報(すかし情報)はどこに書かれているかを見つけることが困難であり、その秘密情報を書き換えたり消したりしようとすると、音声や画像に大きな劣化を生じる。

【0023】

(2) 一方、検査用の復号器では、別の暗号化された埋込み位置指定情報を使って情報がどこに埋め込まれているかを捜して、秘密の情報を読み出すことができる。

【図面の簡単な説明】

【図1】Aは請求項1の発明の実施例および請求項5の発明の実施例を示す構成図、Bはその符号器11の具体例を示す機能構成図である。

50

【図2】A, B, Cはそれぞれ符号化ビット系列、埋込み位置指定情報、すかし情報を示す図、Dは符号帳の例を示す図である。

【図3】Aは請求項2の発明の実施例を示すブロック図、Bは歪表を示す図、Cは選択可能インデックス組の表を示す図である。

【図1】

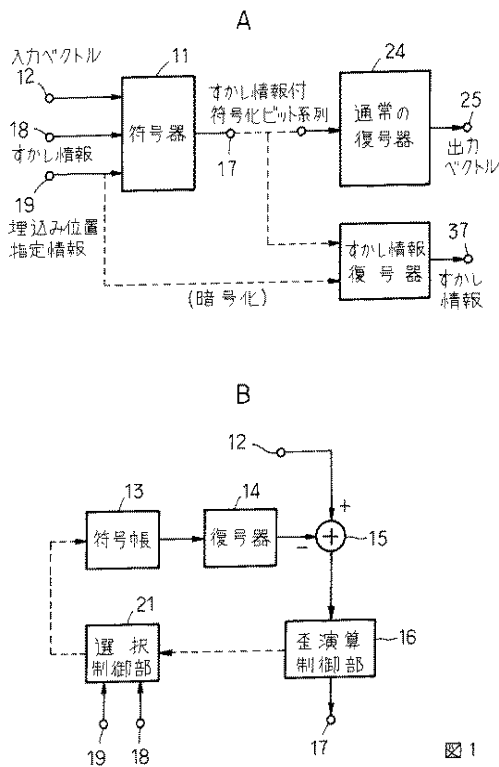


図1

【図2】

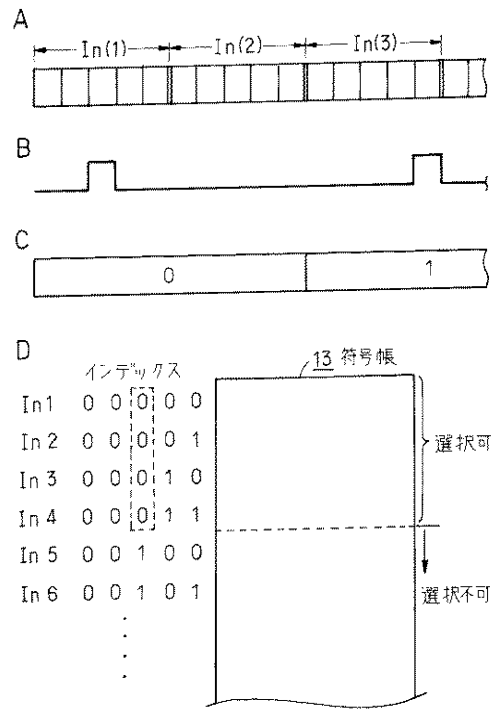
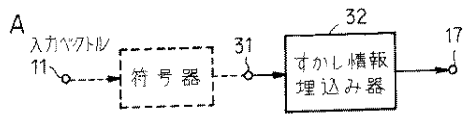


図2

【図 3】



B

歪表

	In1	In2	In3	...
In2	D21	/	/	...
In3	D31	D32	/	...
In4	D41	D42	D43	...
⋮	⋮	⋮		
⋮	⋮	⋮		
⋮	⋮	⋮		
⋮	⋮	⋮		

C

選択可能インデックス表

埋込み位置	溢れ情報 0	溢れ情報 1
1	In, In, ...	In, ...
2	In, In, ...	In, ...
3	In, ...	In, ...
4	In, ...	In, ...
5	In, ...	In, ...

図 3

-----  
フロントページの続き

審査官 白石 圭吾

(56)参考文献 特開平04 - 248771 (JP, A)  
特開平10 - 065912 (JP, A)  
特開昭63 - 146519 (JP, A)

(58)調査した分野(Int.Cl.<sup>7</sup>, DB名)  
H04N 1/387