(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4719880号
(P4719880)

(45)発行日　平成23年7月6日(2011.7.6)　(24)登録日　平成23年4月15日(2011.4.15)

(51)Int.Cl.			F I		
H04K	1/02	(2006.01)	H04K	1/02	
G10L	19/00	(2006.01)	G10L	19/00	240
H04N	7/30	(2006.01)	H04N	7/133	Z
G06T	9/00	(2006.01)	G06T	9/00	
H04N	1/41	(2006.01)	H04N	1/41	B

請求項の数 1　(全 13 頁)　最終頁に続く

(21)出願番号　特願2005-319320 (P2005-319320)
(22)出願日　平成17年11月2日 (2005.11.2)
(65)公開番号　特開2007-129409 (P2007-129409A)
(43)公開日　平成19年5月24日 (2007.5.24)
審査請求日　平成20年7月22日 (2008.7.22)

(73)特許権者　304020177
国立大学法人山口大学
山口県山口市吉田１６７７－１
(72)発明者　松藤　信哉
山口県宇部市常盤台２丁目１６－１　山口大学工学部内
(72)発明者　田中　幹也
山口県宇部市常盤台２丁目１６－１　山口大学工学部内
(72)発明者　棚田　嘉博
山口県宇部市常盤台２丁目１６－１　山口大学工学部内
(72)発明者　松元　隆博
山口県宇部市常盤台２丁目１６－１　山口大学工学部内

最終頁に続く

(54)【発明の名称】アナログ符号化システム

(57)【特許請求の範囲】
【請求項１】
離散多値に係る１次元又は２次元のアナログデータ（１２）が入力される入力部（１）と、
初期値が入力されることで乱数を発生する乱数発生関数を備える乱数発生部（７）と、
前記乱数発生部（７）において発生された乱数を用いて複数の多次元直交系列を発生させる複数分割多次元直交系列発生部（６）と、
前記アナログデータ（１２）が所定長さのブロックに分割して入力され、それぞれのブロックの前記アナログデータ（１２）の符号化処理を行う複数のブロック符号化処理部とを有し、
前記ブロック符号化処理部は、
前記アナログデータ（１２）の次元数よりも大きな次元数の多次元アナログデータ（１３）に写像変換する写像変換部（５）と、
前記複数分割多次元直交系列発生部（６）から前記多次元直交系列を読み出して、前記写像変換部（５）によって写像変換された前記多次元アナログデータ（１３）を、多次元直交変換して暗号化した変換データを生成する分割多次元直交変換部（８）と、
前記分割多次元直交変換部（８）の出力データに、前段のブロック符号化処理部における前記分割多次元直交変換部（８）の出力データを重みを付けて加算し、加算結果の多次元データをより少ない次元のデータに写像して変換する次元変換部とを備えたものであるアナログ符号化システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は離散多値のアナログ情報の保護を考慮したアナログ符号化システムに関する。
【背景技術】
【０００２】
近年、ユビキタスネットワーク社会を迎えつつあり、情報伝送や保存においては、音声や画像などのアナログ的情報（離散多値情報）が容易にやり取りできるようになった反面、それらを他人に盗み見られないような情報保護を目的とした通信が要求されている。そのために、雑音などに対する耐性が強く、しかも信頼性が高く、かつ、効率良く伝送できるようなデータ圧縮可能な符号化方式やシステムが益々必要となっている。このような状況下において、近年様々な符号化方式やシステムに関する発明が開示されている。
【０００３】
例えば、情報秘匿システムの一つである単位ブロック毎に変換を行なうブロック型の符号変換方式において、次数の小さいラテン方陣Ｌを複数並べて段を構成し、この段を複数設け、前段の各ラテン方陣Ｌから後段の少なくとも二つのラテン方陣Ｌに変換したデータを入力させて、入力データＡの各ビットが出力データＢの全てのビットに影響を与えるようにして秘匿性を高めた符号化方式の開示がある（例えば、特許文献１参照）。この符号化方式によれば、秘匿性の高い符号変換を簡単にかつ正確に得ることができる。
【０００４】
また、画像データに低域フィルタ及び高域フィルタを用いてフィルタリングしてフィルタ係数を生成し、当該生成したフィルタ係数を量子化して量子化係数を生成し、その量子化係数を所定の符号化方式で符号化処理して算術符号データを生成した後、当該算術符号データの少なくとも一部にスクランブル処理を施すと共に、算術符号データに基づいて符号化処理に関する所定の符号化情報を生成し、当該生成した符号化情報を格納して生成したヘッダデータにスクランブル処理を施した算術符号データを付加してパケットデータを生成する符号化装置が開示されている（例えば、特許文献２参照）。このような符号化装置によれば、算術符号データにスクランブル処理を施す分、量子化係数を符号化したときのデータ量の増加を防止することができ、画像データの圧縮率の低下を防止できる。
【０００５】
更に、コンテンツのストリームを記録再生するストリーム記録再生装置が開示されているが、そのストリーム記録再生装置において、アナログ放送波等によって伝送されて入力されたアナログ映像音声信号からディジタルストリームを生成する符号化手段が開示されている（例えば、特許文献３参照）。このようなアナログからデジタルに変換することによって、圧縮化あるいは多重化が可能となっている。
【特許文献１】特開２０００－１９９５７号公報
【特許文献２】特開２００２－１３５５９４号公報
【特許文献３】特開２００３－１６３８８９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、上述の従来例に開示された発明においては、いずれもアナログ情報（離散多値情報）を対象とし、情報保護と信頼性向上を念頭に入れた符号化方式では、アナログ情報をデジタル情報に直し、それをスクランブル技術、暗号化技術、誤り訂正符号化技術などを組み合わせた符号化方式が一般的である。また、データ圧縮を行う場合は高い周波数成分をカットするような離散コサイン変換やウエーブレット変換を組み込んだシステムとなる。
【０００７】
また、アナログ情報は、ある一部が雑音、妨害、加工などによって大きく変形することよりも、全体的に少しずつ異なっているほうが、その品質は保障される。しかし、上記の

ようにデジタルに一度直して符号化する方式は、最上位ビットと最下位ビットにおける情報量のばらつきも生じるので、品質を保障し、かつ効率のよいアナログ符号化法とは言えない可能性があるという課題があった。

【０００８】

本発明はかかる従来の事情に対処してなされたものであり、複数分割多次元直交系列を使用した分割多次元直交変換を実行することにより、簡単な構成で容易に取り扱うことができ、しかも高い品質を担保可能で秘匿性が高いアナログ符号化システムを提供することを目的とする。

【課題を解決するための手段】

【０００９】

上記目的を達成するために、本発明のアナログ符号化システムは、離散多値に係る１次元又は２次元のアナログデータが入力される入力部と、初期値が入力されることで乱数を発生する乱数発生関数を備える乱数発生部と、前記乱数発生部において発生された乱数を用いて複数の多次元直交系列を発生させる複数分割多次元直交系列発生部と、前記アナログデータが所定長さのブロックに分割して入力され、それぞれのブロックの前記アナログデータの符号化処理を行う複数のブロック符号化処理部とを有し、前記ブロック符号化処理部は、前記アナログデータの次元数よりも大きな次元数の多次元アナログデータに写像変換する写像変換部と、前記複数分割多次元直交系列発生部から前記多次元直交系列を読み出して、前記写像変換部によって写像変換された前記多次元アナログデータを、多次元直交変換して暗号化した変換データを生成する分割多次元直交変換部と、前記分割多次元直交変換部の出力データに、前段のブロック符号化処理部における前記分割多次元直交変換部の出力データを重みを付けて加算し、加算結果の多次元データをより少ない次元のデータに写像して変換する次元変換部とを備えたものである。これは、言わば縦続型のアナログ符号化方式である。

【００１０】

こうして、複数分割多次元直交系列を分割多次元直交変換を施すことによれば、アナログデータの一部に雑音や妨害要素あるいは加工要素が含まれたとしても、それらは変換後のデータに均一に分散され、しかも逆変換される場合にも、分割多次元直交逆変換することにより均一に分散されたままとなるため、例えば音声データのような一次元データや画像データのような二次元データの場合には、雑音などが分散されて復元されるので耳や目にはその雑音などが感知できない程度にまで低減することができる。すなわち、局所的に雑音などが現れるよりも一定の品質が担保される。

【００１１】

また、本発明のアナログ符号化システムは、離散多値に係る１次元又は２次元のアナログデータが入力される入力部と、初期値が入力されることで乱数を発生する乱数発生関数を備える乱数発生部と、前記乱数発生部において発生された乱数を用いて複数の多次元直交系列を発生させる複数分割多次元直交系列発生部と、前記アナログデータが所定長さのブロックに分割して入力され、それぞれのブロックの前記アナログデータの符号化処理を行う複数のブロック符号化処理部とを有し、前記ブロック符号化処理部は、前記アナログデータの次元数よりも大きな次元数の多次元アナログデータに写像変換する写像変換部と、前記複数分割多次元直交系列発生部から前記多次元直交系列を読み出して、前記写像変換部によって写像変換された前記多次元アナログデータに所定の秘密データを重みを付けて加算し、加算結果の多次元データを多次元直交変換して暗号化した変換データを生成する分割多次元直交変換部と、前記分割多次元直交変換部の出力データをより少ない次元のデータに写像して変換する次元変換部とを備えたものである。これは、言わば並列型のアナログ符号化方式である。

【００１２】

このような、並列型のアナログ符号化方式においても、前述の縦続型のアナログ符号化方式と同様の利点が得られる。なお、複数分割多次元直交系列を分割多次元直交変換後にデータの圧縮を施すようにしてもよい。アナログ符号化システムにおいては、分割多次元

直交変換後に、圧縮データを生成することができるので多量のデータの処理、保存を行なうことが便利であり、しかも前述のとおり品質の劣化は復元データの全体に亘るため、全体的には一定の品質を担保することができる。

【００１３】

本発明のアナログ符号化方式においては、符号化し暗号化したデータを送信データに変換して送信し、受信側では受信データを逆に変換して元のアナログデータに復元することができる。

【００１４】

こうして、この発明のアナログ符号化システムにおいて、暗号化データを送信する場合には、乱数発生関数に初期値を与えて乱数を発生させ、それを用いて容易に複数分割多次元直交系列を生成させ、更に、それを用いてアナログデータに分割多次元直交変換を施し、これを逆変換する際に、先の乱数発生関数の初期値を鍵としてアナログデータに復元することができる。従って、受信者側では予め送信者側と同一の乱数発生関数を備えておき、乱数発生関数の初期値さえ入手すれば、容易に乱数の発生の再現を実行することができる。このような乱数発生関数とその初期値を利用することで、鍵の送受信を容易にすることができるとともに、受信側の逆変換によるアナログデータの復元も容易となる。

【００１５】

また、本発明のアナログ符号化方式においては、アナログデータをブロックに分割して前述の縦続型および並列型の構成により複数のブロックを同時に処理することができる。

【００１６】

こうして、安全性をできるだけ維持したまま、高速化できるよう多値データを分割し、他の多値情報を鍵としてこれらを合成することができ、品質の劣化は復元データの全体に亘るため、全体的には一定の品質を担保することができる。

【発明の効果】

【００１７】

本発明のアナログ符号化システムにおいては、複数分割多次元直交系列を分割多次元直交変換を施すことによれば、アナログデータの一部に雑音や妨害要素あるいは加工要素が含まれたとしても、それらは変換後のデータに均一に分散され、しかも逆変換される場合にも、分割多次元直交逆変換することにより均一に分散されたままとなるため、例えば音声データのような一次元データや画像データのような二次元データの場合には、雑音などが分散されて復元されるので耳や目にはその雑音などが感知できない程度にまで低減することができる。すなわち、局所的に雑音などが現れるよりも一定の品質が担保される。

【００１８】

また、特に複数分割多次元直交系列を分割多次元直交変換後にデータの圧縮を施すアナログ符号化システムにおいては、分割多次元直交変換後に、圧縮データを生成することができるので多量のデータの送信を行なうことが可能であり、しかも前述のとおり品質の劣化は復元データの全体に亘るため、全体的には一定の品質を担保することができる。

【００１９】

また、信頼性向上のためには、暗号化した部分は誤り補正できるので、基本的には制御ビット部に対してのみ符号化を行うので、従来法に比べて、符号化効率の観点からも優れているものと期待できる。更に、本実施の形態においては、多次元直交系列は無数に存在するのでそれを鍵とすることで、多次元的に情報を複雑に変換できるので秘話性の高い暗号的符号化が可能である。

【発明を実施するための最良の形態】

【００２０】

先に、本発明者等は、周期自己相関関数がシフト零以外の位相シフトでは零を取るような多次元直交系列の一般解を与え、更に、その直交性を活用した多次元直交変換のアナログ符号化システムを提案している（特願２００４－１４９６０８号）。これは、アナログ的情報を一度多次元情報に直し、それと多次元直交系列との畳み込みを行う変換である。この変換は、変換データの振幅分布はガウス分布に近づくので、性質の良いスクランブル

が可能である、逆変換（相関検出）より大きな処理利得を得るので、雑音に対して高い耐性を持つ、変換情報の一部に大きな雑音が加わったとしても、それを復号すると大きな雑音は全体に広がるので誤り補正が可能などの特長を有する。更に、多次元直交系列は無限に存在し、それを知らないと情報復元が容易でないことから、暗号化が可能である。

【００２１】

図１は、本発明者等が提案した、テキストや音楽などの１次元データを３次元直交系列を用いて直交変換する場合を示すアナログ符号化システムの概念図である。図１ではデータのみに着目する。図１において、１次元データ３２を多次元直交変換前に何らかの方法により写像し、３次元データ３３とし、その後、多次元直交変換を行う。一般には、これらを１次元データに直したりして、加工しやすいデータに符号化し、それを記録したり通信する。また、復号では、逆の操作を行い、容易に情報を取り出すことができる。具体的には、多次元直交逆変換を行い逆変換データ３５を得て、さらに写像変換によって１次元データ３６を得るものである。

【００２２】

図２は図１に示すアナログ符号化システムにおける、離散多値情報を入力として多次元直交変換するような方式の一例を示す。Ｂｊは多値情報列、Ｃｊは暗号化された情報列、Ｅｋは鍵ｋからなる多次元直交変換、ＩＶは乱数発生関数初期値を示す。

【００２３】

ここで、多次元直交変換は次のような２つの性質を有する。第一に、変換後はどのようなデータでもその出力値はガウス分布に近づくので性質の良いスクランブルが可能であるという性質、第二には、局所的な雑音が入ったとしても逆変換後はその雑音は全体に散らばるので誤差の少ない誤り補正が可能な符号化が実現できるという性質である。

【００２４】

本発明は、この提案したアナログ符号化システムの多次元直交変換の特長を最大限活用することにより、より保全性高く、誤り補正でき、効率良いアナログ暗号化方式の実現を目的とした暗号化システムに関するものである。この暗号化方式は、乱数の初期値を鍵とすることより、複数分割多次元直交系列を自動生成し、それを用いた分割多次元直交変換に基づく方式である。

【００２５】

以下に本発明の実施の形態に係るアナログ符号化システムについて図３乃至図８を参照しながら説明する。図３は本発明の特徴とする、１次元データを多次元直交変換前に複数のブロック化されたデータとする概念図であり、図４は本発明の離散多値情報を入力として多次元直交変換する暗号化方式例、図５は縦続型アナログ暗号化方式で多次元直交変換する暗号化方式例、図６は並列型アナログ暗号化方式で多次元直交変換する暗号化方式例、図７は本発明の第１の実施形態図、図８は本発明の第２の実施形態図である。

【００２６】

図３には、本発明の特徴とするアナログデータを複数に分割する概念図を示し、アナログデータ３２の１次元データを複数ブロックに分割し、複数分割データＢｊ，Ｂｊ＋１・・Ｂｊ＋ｎを生成して、多次元直交変換前に何らかの方法により写像し、複数ブロックに分割された３次元データ３３とする。

【００２７】

ここで、離散多値情報を入力として多次元直交変換する方式は、図４で示すようにストリーム暗号の技術を適用した幾つかのモードが考えられる。基本的には、離散多値情報はブロック化され、前までの多値情報ブッロクが次のブロックに加算され、それを入力として多次元直交変換するような暗号化方式である。これにより、暗号の複雑さは更に高くなり、また、雑音に対する耐性を高めることができると考えられる。ただし、Ｂｊはｊ番目の多値情報ブロック、Ｃｊはｊ番目の暗号ブロック、Ｅｋは鍵ｋからなる多次元直交変換、Ｗは適当な重み、ＩＶは乱数発生関数初期値を示す。このように、本発明の方式は、アナログ的情報を直接暗号化し、それを２値デジタル情報に符号化する。

【００２８】

次に、図５に縦続型アナログ符号化方式で多次元直交変換する符号化方式例を示す。多値情報ｘを｛x_1，x_2，・・・，x_S｝とＳ分割し、分割したブロックごとに符号化の処理を行う。まず、それらを写像M_jにより写像変換してｎ次元情報Ｘ＝｛X_1，X_2，・・・，X_S｝にする。ここで、X_jはx_jを写像変換によりｎ次元化した情報である。

【００２９】

これらは、

$$Y=\{Y_1, Y_2, \cdots, Y_S\}$$
$$Y_j=Ta_j^n(X_j)+w_jY_{j-1}\}$$

と符号化（暗号化）される。ここで、$Ta_j^n(X_j)$はｎ次元ブロックデータX_jをｎ次元直交変換した結果を表している。また、一般には、変換データＹ＝｛Y_1，Y_2，・・・，Y_S｝は、写像m_jによってより低次元のデータｙ＝｛y_1，y_2，・・・，y_S｝に変換される。

【００３０】

ただし、w_jは重み、a_jは適当なｎ次元直交系列であり、各々、ブロックごとに異なっても構わない。また、x_0は他人には秘密のデータであり、もう一つの共通鍵の役目をする。なお、多値情報ｘと変換データｙは、音声では１次元データ、画像では２次元データとして考えることができる。

【００３１】

次に、図６に並列型アナログ符号化方式で多次元直交変換する符号化方式例を示す。多値情報ｘを｛x_1，x_2，・・・，x_S｝とＳ分割し、分割したブロックごとに符号化の処理を行う。まず、それらを写像M_jにより写像変換してｎ次元情報Ｘ＝｛X_1，X_2，・・・，X_S｝にする。ここで、X_jはx_jを写像変換によりｎ次元化した情報である。

【００３２】

これらは、

$$Y=\{Y_1, Y_2, \cdots, Y_S\}$$
$$Y_j=Ta_j^n(X_j)$$
$$X_j=M_j(x_j)+w_jM_0(x_0)$$

と符号化（暗号化）される。ここで、$Ta_j^n(X_j)$はｎ次元ブロックデータX_jをｎ次元直交変換した結果を表しており、$M_j(x_j)$はブロックデータx_jを写像変換した結果を表している。また、一般には、変換データＹ＝｛Y_1，Y_2，・・・，Y_S｝は、写像m_jによってより低次元のデータｙ＝｛y_1，y_2，・・・，y_S｝に変換される。

【００３３】

ただし、w_jは重み、a_jは適当なｎ次元直交系列であり、各々、ブロックごとに異なっても構わない。また、x_0は他人には秘密のデータであり、もう一つの共通鍵の役目をする。なお、多値情報ｘと変換データｙは、音声では１次元データ、画像では２次元データとして考えることができる。

【００３４】

また図７は、本発明の第１の実施の形態に係るアナログ符号化システムの構成図である。アナログ符号化システムは、大きく入力部１、演算部２、出力部３及びデータベース４から構成されている。入力部１は、データベース４に格納されている各種データが入力されたり、演算部２に対してデータを入力する際に使用されるユーザーとのインターフェースである。

【００３５】

データベース４には、秘匿性の高いアナログ情報である生アナログデータ１２が格納されている。この生アナログデータ１２の例としては、一次元データとしては音声データ、二次元データとしては画像データがある。また、動画像は静止画像が時間的に連続するものであるため三次元データとして認識される場合がある。この生アナログデータ１２は、予めデータベース４に格納されてもよいが、入力部１から演算時に演算部２の第１写像変換部５に入力されてもよい。

【００３６】

生アナログデータ１２は演算部２に含まれる第１写像変換部５によって写像変換され、ｎ次元アナログデータ１３となる。例えば、一次元の音声データや２次元の画像データを３次元のアナログデータに写像変換されたものである。ｎ次元のｎは、秘匿性を考慮すれば生アナログデータ１２の次元よりも高い次数を表現するものであり、生アナログデータ１２が一次元の音声データであれば、ｎは２次以上となり、生アナログデータ１２が二次元の画像データであればｎは３次以上となる。但し、一般的には１以上の任意の数を意味するものである。図７では、ｎ次元アナログデータ１３もデータベース４に格納されているが、格納されずに第１写像変換部５に留めておいてもよい。

【００３７】

データベース４には、乱数発生関数データ１５が格納されており、同じく格納されている乱数発生関数初期値１４を用いることによって、乱数を発生させることができる。具体的には、演算部２の乱数発生部７によって乱数発生関数初期値１４と乱数発生関数データ１５が読み出され、乱数発生関数初期値１４によって乱数を発生させる。但し、乱数発生関数データ１５は予めデータベース４に格納することなく乱数発生部７の内部に格納しておいてもよい。また、乱数発生関数初期値１４もデータベース４に予め格納されるのではなく、入力部１を介して乱数発生部７に入力されるようにしておいてもよい。

【００３８】

発生した乱数は演算部２の複数分割多次元直交系列発生部６によって乱数発生部７から読み出され、図３のように、複数分割多次元直交系列データ１６が一義的に生成される。生成された複数分割多次元直交系列データ１６はデータベース４に格納されるようにしておくとよい。また、この複数分割多次元直交系列データ１６は、分割多次元直交変換部８によってデータベース４から読み出され個々に多次元直交変換されてデータ１７に変換される。この変換データ１７もデータベース４に格納される。さらに、演算部２の圧縮部９は、情報格納装置４から変換データ１７を読みだして圧縮し、圧縮データ１８を生成し、データベース４に格納する。圧縮部９は、多量のデータを送信などする際に設けられるものであるが、多量で重いデータを取り扱う必要がない場合には、必ずしも設けなくともよい。

【００３９】

変換データ１７あるいは圧縮データ１８は、演算部２の分割多次元直交逆変換部１０によって逆変換される。この逆変換の内容については後述するが、逆変換の際には、先に分割多次元直交変換部８で用いられた複数分割多次元直交系列データ１６が必要となる。そこで、この複数分割多次元直交系列データ１６を生成する際に、先の乱数発生関数初期値１４を用いて乱数の発生を再現して分割多次元直交変換時の複数分割多次元直交系列を再生成する。

【００４０】

分割多次元直交逆変換部１０によって逆変換されて得られたｎ次元アナログデータは、さらに第２写像変換部１１によって生アナログデータに変換される。この演算部２における演算結果をはじめとして、入力部１から入力されるデータやデータベース４に格納されているデータは、出力部３によって他の装置やシステムに対して出力されたり、あるいは出力部３自身に表示される。

【００４１】

なお、データベース４には、演算部２の内部で演算されたデータがそれぞれ格納されるが、演算部２の各要素において演算した後にデータベース４に格納されることなく、下流側の要素に送信されるようにしておいてもよいし、下流側にデータ送信を行なうと同時に並行してデータベース４に格納するようにしてもよい。

【００４２】

次に、本発明の第２の実施の形態に係るアナログ符号化システムについて図８を参照しながら説明する。図８において、図７と同一部分については同一の符号を付し、その構成の説明は省略する。

【００４３】

本実施の形態においては、送信側演算部１９において、変換データ１７あるいは圧縮データ１８を生成し、それを受信側演算部２０へ送信して復元するものである。従って、多次元直交変換部８によって生成された変換データ１７あるいは圧縮部９によって生成された圧縮データ１８は送信部２１によって、受信側演算部２０の受信部２２へ送信される。

【００４４】

受信部２２は、受信した変換データ１７あるいは圧縮データ１８を分割多次元直交逆変換部１０によって復元するが、その際に用いられる複数分割多次元直交系列データ１６が必要となる。複数分割多次元直交系列データ１６は、受信側演算部２０の乱数発生部２４によって発生される乱数を用いて、複数分割多次元直交系列発生部２３によって生成される。乱数の発生には、乱数発生関数データ２６が用いられるが、その乱数発生関数の初期値を鍵とするため、この初期値を送信部２１から受信部２２へ伝送する必要がある。あるいは、乱数発生関数とその初期値を鍵として伝送してもよい。

【００４５】

受信部２２によって受信された乱数発生関数の初期値は鍵とされ、乱数発生部２４に送信され、さらに乱数発生部２４は、第１データベース２５から乱数発生関数データ２６を読み出して乱数を発生させる。このときに発生される乱数は、送信側演算部１９によって発生された乱数と値、順序において同じものとなる。

【００４６】

乱数発生部２４で発生された乱数を用いて複数分割多次元直交系列発生部２３では、送信側演算部１９と同様に複数分割多次元直交系列を生成する。さらに、第２データベース２７に格納された圧縮データ２８あるいは変換データ２９を読み出して受信側演算部２０の分割多次元直交逆変換部１０では逆変換を実施する。この逆変換によって、ｎ次元アナログデータ３０が得られ、このｎ次元アナログデータ３０は第２データベース２７に格納される。

【００４７】

更に、第２写像変換部１１は、第２データベース２７をデータベース４から読み出して写像変換を行い、送信側演算部１９によって写像変換された生アナログデータ３１を生成し、第２データベース２７に格納する。なお、第２データベース２７には、受信部２２で受信された圧縮データ２８及び変換データ２９が格納されているが、必ずしも格納せずとも、受信部２２で受信されたそれぞれを分割多次元直交逆変換部１０が受信して逆変換を実行してもよい。また、分割多次元直交逆変換部１０によって生成される多次元直交系列については、第２データベース２７に格納されていないが、生成した後に第２データベース２７に格納するようにしてもよい。

【００４８】

一般には、アナログ的情報は、最初に２値デジタル情報に変換され、それを、ストリーム暗号化方式などを使用して暗号化する。基本的には暗号化されたデジタル情報は、ブロック化されて、その先頭に制御ビットが付加される。ここで、雑音に対する信頼性を向上させるには、そのブロック化された全てのビットに対して符号化する必要がある。

【００４９】

これに対して、本実施の形態においては、アナログ的情報を直接暗号化し、それを２値デジタル情報に符号化するものであり、アナログ的情報の複数分割多次元直交系列を分割多次元直交変換を実施して伝送し、それを復元することによれば、雑音を全体に散らばらせることが可能であるため、局所的な劣化は認められず、全体的に影響が希釈化されるため、全体的には、一定の品質を担保することができる。

【００５０】

また、信頼性向上のためには、暗号化した部分は誤り補正できるので、基本的には制御ビット部に対してのみ符号化を行うので、従来法に比べて、符号化効率の観点からも優れているものと期待できる。

【００５１】

更に、本実施の形態においては、多次元直交系列は無数に存在するのでそれを鍵とする

ことで、多次元的に情報を複雑に変換できるので秘話性の高い暗号的符号化が可能であるとなる。

【００５２】

以上説明したとおり、本実施の形態に係るアナログ符号化システムにおいて、暗号化データを送信する場合には、乱数発生関数に初期値を与えて乱数を発生させ、それを用いて容易に複数分割多次元直交系列を生成させ、更に、それを用いてアナログデータに分割多次元直交変換を施し、これを逆変換する際に、先の乱数発生関数の初期値を鍵としてアナログデータに復元することができる。従って、受信者側では予め送信者側と同一の乱数発生関数を備えておき、乱数発生関数の初期値さえ入手すれば、容易に乱数の発生の再現を実行することができる。このような乱数発生関数とその初期値を利用することで、鍵の送受信を容易にすることができるとともに、受信側の逆変換によるアナログデータの復元も容易となる。

【００５３】

また、分割多次元直交変換は、アナログデータの一部に雑音や妨害要素あるいは加工要素が含まれたとしても、それらは変換後のデータに均一に分散される性質を備えており、しかも逆変換される場合にも均一に分散されたままとなるため、雑音などが感知できない程度にまで低減させることができ、一定の品質が維持することができる。

【００５４】

更に、圧縮部を備えることによれば、複数分割多次元直交系列を分割多次元直交変換後に、圧縮データを生成することができるので多量のデータの送信を行なうことが可能であり、しかも前述のとおり品質の劣化は復元データの全体に亘るため、全体的には一定の品質を担保することができる。

【産業上の利用可能性】

【００５５】

本発明に係るアナログ符号化システムは、秘匿性の高いネットワーク構築や、音声、画像、情報信号などを伝送する際の暗号化システムとして金融システム、情報通信システム、行政システム、移動体通信システム、放送システム、セキュリティシステム、防衛システムなど汎用性の高いニーズが見込めるものである。

【図面の簡単な説明】

【００５６】

【図１】既提案のアナログ符号化システムの概念図である。

【図２】既提案の離散多値情報を入力として多次元直交変換する方式の一例である。

【図３】本発明の１次元データを多次元直交変換前に複数のブロック化する概念図である。

【図４】本発明の離散多値情報を入力として多次元直交変換する暗号化方式例である。

【図５】本発明の縦続型アナログ暗号化方式で多次元直交変換する暗号化方式例である。

【図６】本発明の並列型アナログ暗号化方式で多次元直交変換する暗号化方式例である。

【図７】本発明の第１の実施の形態に係るアナログ符号化システムの構成図である。

【図８】本発明の第２の実施の形態に係るアナログ符号化システムの構成図である。

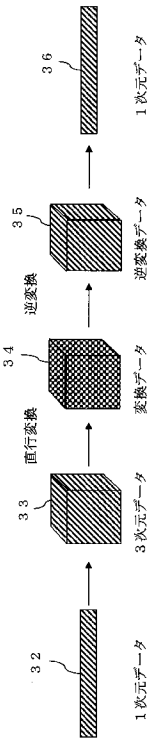
【符号の説明】

【００５７】

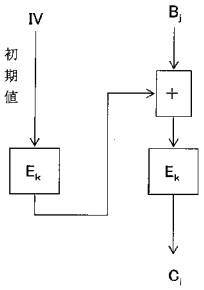
１　入力部
２　演算部
３　出力部
４　データベース
５　第１写像変換部
６　多次元直交系列発生部
７　乱数発生部
８　多次元直交変換部
９　圧縮部

１０　多次元直交逆変換部
１１　第２写像変換部
１２　生アナログデータ
１３　ｎ次元アナログデータ
１４　乱数発生関数初期値
１５　乱数発生関数データ
１６　多次元直交系列データ
１７　変換データ
１８　圧縮データ
１９　送信側演算部
２０　受信側演算部
２１　送信部
２２　受信部
２３　多次元直交系列発生部
２４　乱数発生部
２５　第１データベース
２６　乱数発生関数データ
２７　第２データベース
２８　圧縮データ
２９　変換データ
３０　ｎ次元アナログデータ
３１　生アナログデータ
３２　１次元データ
３３　３次元データ
３４　変換データ
３５　逆変換データ
３６　１次元データ

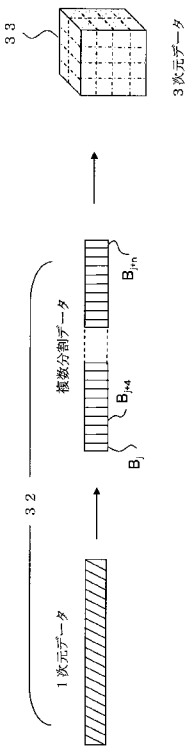
【図１】


３２
１次元データ
３３
３次元データ
直行変換
３４
変換データ
逆変換
３５
逆変換データ
３６
１次元データ

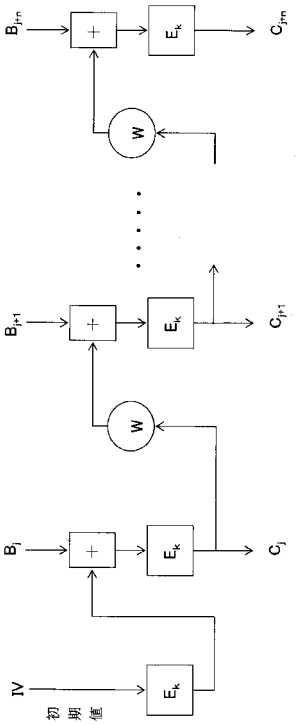
【図２】


IV
初期値
B_j
E_k
E_k
C_j

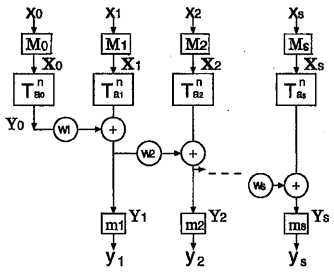
【図３】


３３
３次元データ
３２
１次元データ
複数分割データ
B_j
B_{j+4}
B_{j+m}

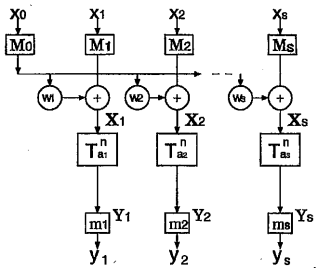
【図４】


IV
初期値
E_k
B_j
C_j
W
B_{j+1}
C_{j+1}
B_{j+m}
C_{j+m}

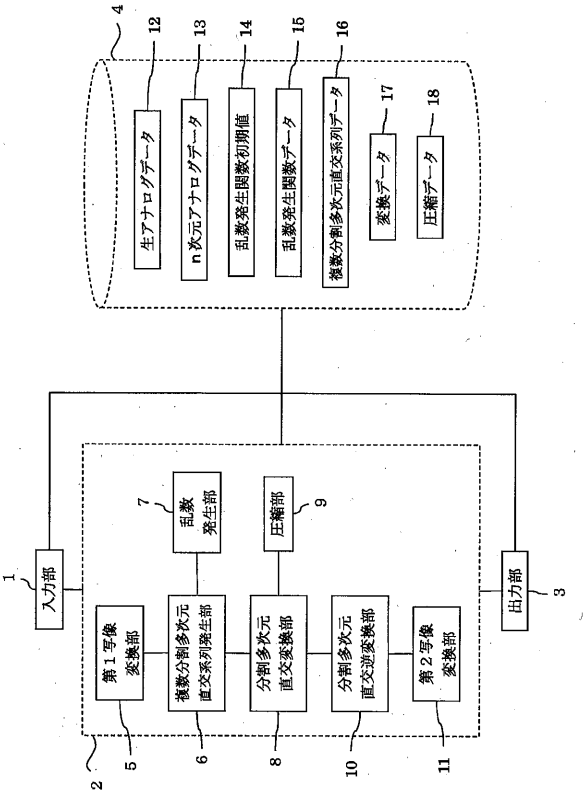
【図５】



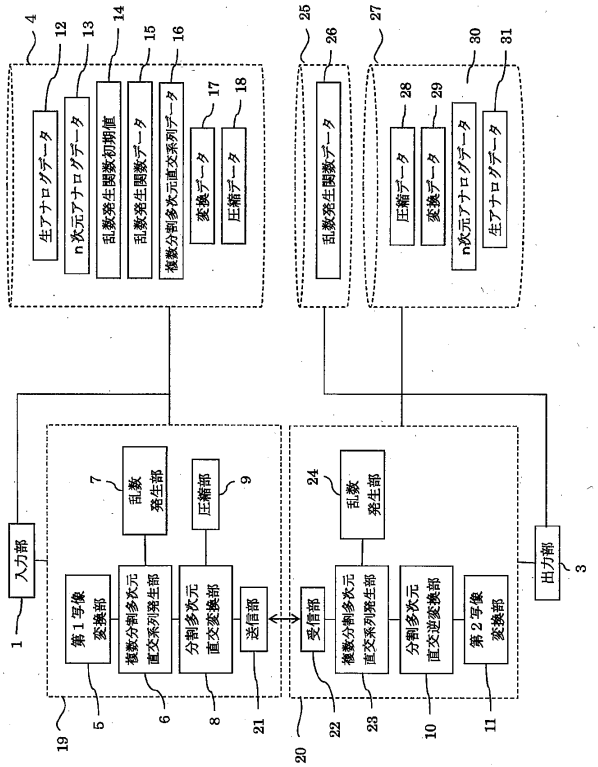
【図６】



【図７】


生アナログデータ
n次元アナログデータ
乱数発生関数初期値
乱数発生関数データ
複数分割多次元直交系列データ
変換データ
圧縮データ
入力部
第１写像変換部
複数分割多次元直交系列発生部
乱数発生部
分割多次元直交変換部
圧縮部
分割多次元直交逆変換部
第２写像変換部
出力部

【図８】


生アナログデータ
n次元アナログデータ
乱数発生関数初期値
乱数発生関数データ
複数分割多次元直交系列データ
変換データ
圧縮データ
乱数発生関数データ
圧縮データ
変換データ
n次元アナログデータ
生アナログデータ
入力部
第１写像変換部
複数分割多次元直交系列発生部
乱数発生部
分割多次元直交変換部
圧縮部
送信部
受信部
乱数発生部
複数分割多次元直交系列発生部
分割多次元直交逆変換部
第２写像変換部
出力部

フロントページの続き

(51)Int.Cl.			F I		
H04N	***7/167***	***(2011.01)***	H04N	7/167	Z
H03M	***7/30***	***(2006.01)***	H03M	7/30	A

審査官　松平　英

(56)参考文献　特開２００５－３３３３８６（ＪＰ，Ａ）
特開平１１－０８８８５７（ＪＰ，Ａ）
特開平１０－１５５１５１（ＪＰ，Ａ）
特開平１１－１１２９８５（ＪＰ，Ａ）
特開２００２－０９４７８０（ＪＰ，Ａ）
特開２００２－２０９１１２（ＪＰ，Ａ）
特開平０４－３６２８８６（ＪＰ，Ａ）
特開平１０－２３４０１２（ＪＰ，Ａ）
特開２００３－００９１８６（ＪＰ，Ａ）
特開２００３－２５８６９５（ＪＰ，Ａ）
松藤　信哉　Shinya　MATSUFUJI，雑音への耐性を考慮したアナログ暗号化方式の提案　Analog Cipher System to Consider Tolerance to Noise，電子情報通信学会技術研究報告　Ｖｏｌ．１０５　Ｎｏ．１７７　IEICE Technical Report，日本，社団法人電子情報通信学会　The Institute of Electronics,Information and Communication Engineers，２００５年　7月　8日，第105巻　第177号，ｐ．７～１０
松藤　信哉他，多次元直交系列の構成，電子情報通信学会技術研究報告，社団法人電子情報通信学会，２００２年１０月１４日，Ｖｏｌ．１０２　Ｎｏ．３９１，ｐ．２３～２６
藤本　亜希他，多次元直交系列を用いた直交変換の性質，電子情報通信学会技術研究報告，社団法人電子情報通信学会，２００３年１０月２４日，Ｖｏｌ．１０３　Ｎｏ．４００，ｐ．６１～６４

(58)調査した分野(Int.Cl.，ＤＢ名)

Ｈ０４Ｋ　　１／００
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／００
Ｈ０３Ｍ　　３／００
Ｈ０３Ｍ　　７／００
Ｈ０４Ｎ　　１／４１
Ｈ０４Ｎ　　７／１６７
Ｈ０４Ｎ　　７／３０