

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4765065号
(P4765065)

(45) 発行日 平成23年9月7日(2011.9.7)

(24) 登録日 平成23年6月24日(2011.6.24)

(51) Int.Cl.		F I	
HO4K	1/02	(2006.01)	HO4K 1/02
HO3M	13/19	(2006.01)	HO3M 13/19
HO3M	13/25	(2006.01)	HO3M 13/25

請求項の数 20 (全 21 頁)

(21) 出願番号	特願2005-140579 (P2005-140579)	(73) 特許権者	304021277
(22) 出願日	平成17年5月13日(2005.5.13)		国立大学法人 名古屋工業大学
(65) 公開番号	特開2005-354674 (P2005-354674A)		愛知県名古屋市昭和区御器所町字木市29番
(43) 公開日	平成17年12月22日(2005.12.22)	(74) 代理人	100110744
審査請求日	平成20年4月28日(2008.4.28)		弁理士 藤川 敬知
(31) 優先権主張番号	特願2004-145381 (P2004-145381)	(72) 発明者	岡本 英二
(32) 優先日	平成16年5月14日(2004.5.14)		愛知県名古屋市昭和区御器所町(番地なし) 名古屋工業大学内
(33) 優先権主張国	日本国(JP)	(72) 発明者	岩波 保則
			愛知県名古屋市昭和区御器所町(番地なし) 名古屋工業大学内
		審査官	西田 聡子

最終頁に続く

(54) 【発明の名称】 カオス符号化変調復調方法

(57) 【特許請求の範囲】

【請求項1】

送信側と受信側との間で符号化変調により情報の伝送を行う符号化変調復調方法であって、

前記送信側は、

伝送情報ビット列をカオス生成器に入力して符号化信号系列を生成し、符号化変調方式のカオス伝送信号系列として前記受信側へ伝送するカオス伝送信号系列生成ステップを備え、

前記受信側は、

推定送信系列を生成する推定送信系列生成ステップと、

前記推定送信系列を入力として前記送信側の前記カオス伝送信号系列生成ステップと同一の処理により推定伝送信号系列を生成する推定伝送信号系列生成ステップと、

前記送信側より受信した受信信号系列と前記推定伝送信号系列との誤差を計算し、その最小誤差を与える推定送信系列を前記受信信号系列の復号結果として出力する復号ステップと

を備え、

前記送信側における前記カオス伝送信号系列生成ステップは、

前記伝送情報ビット列と帰還されたカオス系列とを入力として所定の入力側演算を施すことにより入力信号系列を生成する入力側演算ステップと、

前記入力信号系列を入力として前記カオス生成器によりカオス系列を生成するカオス

10

20

系列生成ステップと、

前記カオス系列を入力として所定の出力側演算を施すことにより前記カオス伝送信号系列を生成する出力側演算ステップと

を備え、

前記受信側における前記推定伝送信号系列生成ステップは、

前記推定送信系列と帰還された推定カオス系列とを入力として前記送信側と同一の入力側演算を施すことにより推定入力信号系列を生成する入力側演算ステップと、

前記推定入力信号系列を入力として前記送信側と同一のカオス生成器により推定カオス系列を生成する推定カオス系列生成ステップと、

前記推定カオス系列を入力として前記送信側と同一の出力側演算を施すことにより推定伝送信号系列を生成する出力側演算ステップと

を備えたことを特徴とするカオス符号化変調復調方法。

【請求項 2】

前記所定の入力側演算 f は、数式 $f(k, s_1(k-1)) = s_1(k-1)$ で表される（但し、 s_1 はカオス生成器への入力信号系列を表し、 $k = 0, 1, \dots$ である。）ことを特徴とする請求項 1 に記載のカオス符号化変調復調方法。

【請求項 3】

前記所定の出力側演算 h は、以下の数式で表されることを特徴とする請求項 2 に記載のカオス符号化変調復調方法。

【数 1】

$$h(k, b(n), s_1(k)) = \begin{cases} s_2(k) & : b(n) = 0 \\ s_2(k) + 3 \exp j(\text{rad}[s_2(k)] + \pi) & : b(n) = 1 \end{cases}$$

但し、 b はデジタルの伝送情報ビット列 $\{0, 1\}$ を表し、 $n, k = 0, 1, \dots$ である。

【請求項 4】

前記 $s_2(k)$ は、以下の数式で表されることを特徴とする請求項 3 に記載のカオス符号化変調復調方法。

【数 2】

$$s_2(k) = \frac{\text{Re}[s_1(k)] + \text{Im}[s_1(k)]}{75} + j \frac{\text{Re}[-s_1(k)] + \text{Im}[s_1(k)]}{20}$$

【請求項 5】

前記カオス生成器は、円環状カオスの生成方程式を用いて、初期値を $x_0 = \text{Re}[s_1(k)]$ 、 $y_0 = \text{Im}[s_1(k)]$ とし、以下の数式で表わされるものとしたことを特徴とする請求項 2 乃至 4 のいずれかに記載のカオス符号化変調復調方法。

【数 3】

$$\begin{cases} x_{i+1} = y_i - 1.73x_i + \frac{5(-1+x_i^2)}{1+x_i^2} + \tan^{-1}(x_i + y_i) \\ y_{i+1} = -0.98x_i \end{cases}$$

$$s_1(k) = x_{20} + j y_{20}$$

【請求項 6】

前記所定の出力側演算 h は、以下の数式で表されることを特徴とする請求項 2 に記載のカオス符号化変調復調方法。

10

20

30

40

【数 4】

$$h(k, b(n), s_1(k)) = \begin{cases} \exp j(\text{rad}[s_2(k)]) & : b(n) = 0 \\ \exp j(\text{rad}[s_2(k)] + \pi) & : b(n) = 1 \end{cases}$$

但し、 b はデジタルの伝送情報ビット列 $\{0, 1\}$ を表し、 $n, k = 0, 1, \dots$ である。

【請求項 7】

前記所定の出力側演算 h は、以下の数式で表されることを特徴とする請求項 2 に記載のカオス符号化変調復調方法。

10

【数 5】

$$h(k, b(n), s_1(k)) = \begin{cases} (1 + 0.5p)s_2(k) & : b(n) = 0 \\ (1 + 0.5p)\{s_2(k) + 3\exp j(\text{rad}[s_2(k)] + \pi)\} & : b(n) = 1 \end{cases}$$

$$p = \{k - nr_c + b(n)\} \bmod 2$$

但し、 b はデジタルの伝送情報ビット列 $\{0, 1\}$ を表し、 $n, k = 0, 1, \dots$ である。

【請求項 8】

前記出力側演算は、前記カオス系列から振幅、位相とも疑似雑音的に変化するカオス伝送信号系列を生成することを特徴とする請求項 1 乃至 7 のいずれかに記載のカオス符号化変調復調方法。

20

【請求項 9】

前記出力側演算は、前記カオス系列から振幅又は位相のいずれか一方のみが変化するカオス伝送信号系列を生成することを特徴とする請求項 1 乃至 7 のいずれかに記載のカオス符号化変調復調方法。

【請求項 10】

前記受信側における前記復号ステップは、所定の長さ $v \geq 1$ 以上の各系列に対して、復号拘束長を 1 増加させる毎に前記推定伝送信号系列を $1/2$ ずつ廃棄して前記誤差計算を行うことを特徴とする請求項 1 乃至 9 のいずれかに記載のカオス符号化変調復調方法。

30

【請求項 11】

送信側と受信側との間で符号化変調により情報の伝送を行う符号化変調復調方法であって、

前記送信側は、

伝送情報ビット列をカオス生成器に入力して符号化信号系列を生成し、符号化変調方式のカオス伝送信号系列として前記受信側へ伝送するカオス伝送信号系列生成ステップを備え、

前記受信側は、

推定送信系列を生成する推定送信系列生成ステップと、

前記推定送信系列を入力として前記送信側の前記カオス伝送信号系列生成ステップと同一の処理により推定伝送信号系列を生成する推定伝送信号系列生成ステップと、

40

前記送信側より受信した受信信号系列と前記推定伝送信号系列との誤差を計算し、その最小誤差を与える推定送信系列を前記受信信号系列の復号結果として出力する復号ステップと

を備え、

前記受信側における前記復号ステップは、所定の長さ $v \geq 1$ 以上の各系列に対して、復号拘束長を 1 増加させる毎に前記推定伝送信号系列を $1/2$ ずつ廃棄して前記誤差計算を行うことを特徴とするカオス符号化変調復調方法。

【請求項 12】

前記受信側における前記復号ステップは、復号拘束長を可变的に設定することを特徴と

50

する請求項 1 乃至 1 1 のいずれかに記載のカオス符号化変調復調方法。

【請求項 1 3】

前記受信側における前記復号ステップは、復号ビットの確からしさの尺度に基づいて前記復号拘束長を可变的に設定することを特徴とする請求項 1 2 に記載のカオス符号化変調復調方法。

【請求項 1 4】

前記受信側における前記復号ステップは、前記推定送信系列における復号ビットを 0 とした場合の前記受信信号系列との最小誤差 d_0 と、前記復号ビットを 1 とした場合の最小誤差 d_1 とを比較し、前記最小誤差 d_1 の方が小さい場合は前記復号ビットを 1 と復号し、前記最小誤差 d_0 の方が小さい場合は前記復号ビットを 0 と復号することを特徴とする請求項 1 乃至 1 3 のいずれかに記載のカオス符号化変調復調方法。

10

【請求項 1 5】

前記受信側における前記復号ステップは、前記最小誤差 d_0 と前記最小誤差 d_1 との差の絶対値を 0 以上の閾値と比較し、前記差の絶対値が前記閾値以上の場合は復号を行い、前記閾値未満の場合は復号拘束長を増加させて前記最小誤差 d_0 、 d_1 を再計算することを特徴とする請求項 1 4 に記載のカオス符号化変調復調方法。

【請求項 1 6】

前記送信側における前記カオス伝送信号系列生成ステップは、複数のカオス生成器を用いて、前記伝送情報ビットの値によって異なるカオス生成器によりカオス伝送信号系列を生成することを特徴とする請求項 1 乃至 1 5 のいずれかに記載のカオス符号化変調復調方法。

20

【請求項 1 7】

前記送信側における前記カオス伝送信号系列生成ステップは、縦続又は並列或いはこれらの組み合わせにより接続された複数のカオス生成器を用いて前記カオス伝送信号系列を生成することを特徴とする請求項 1 乃至 1 6 のいずれかに記載のカオス符号化変調復調方法。

【請求項 1 8】

前記送信側における前記カオス伝送信号系列生成ステップは、前記カオス伝送信号系列をパケット化すると共に前記カオス生成器によるカオス系列の生成を一旦終了して前記カオス生成器を初期化するパケット化ステップを含むことを特徴とする請求項 1 乃至 1 7 のいずれかにカオス符号化変調復調方法。

30

【請求項 1 9】

前記パケット化ステップは、前記各パケットを終端させる際にテールビットを挿入することを特徴とする請求項 1 8 に記載のカオス符号化変調復調方法。

【請求項 2 0】

前記カオス伝送信号系列生成ステップの前又は後に実行され且つ雑音的に変化する変調信号を許容する他方式の符号化ステップを更に備えたことを特徴とする請求項 1 乃至 1 9 のいずれかに記載のカオス符号化変調復調方法。

【発明の詳細な説明】

【技術分野】

40

【0 0 0 1】

本発明は、送信側と受信側との間で符号化変調により情報の伝送を行う符号化変調復調方法に関するものであり、特に、デジタル通信において通信路における雑音により受信信号が劣化した場合においても高品質な伝送を行うことができ、且つ他者からは容易に復号を行うことができないカオス符号化変調復調方法に関するものである。

【背景技術】

【0 0 0 2】

移動無線通信や無線 LAN などの分野では近年のマルチメディア通信の普及により、ますますの高速化、高効率化の需要が高まっている。しかし、移動通信などではマルチパスにより符号間干渉が発生し、伝搬路環境が頻繁に変化するため、劣悪な環境における高品質

50

質通信の確立が必要である。一方、近年では無線通信端末を用いた電子商取引のシステムなども徐々に普及してきており、通信におけるセキュリティーの確保、秘匿性の高い通信の実現が非常に重要なものになっている。

【 0 0 0 3 】

ところで、従来より通信路符号化技術の分野において、より劣悪な環境において高品質な通信を実現するために、変調方式や符号化技術の改良が行われている。その中でもターボ符号はシャノン限界に迫る高品質伝送を実現する手法である。これは符号の並列接続接続にインターリーバを介し、さらに繰り返し復号を行うことで誤り訂正能力を飛躍的に向上させたものである。また、暗号化技術の分野においても、従来から優れた特性を示す方法が多数提案されている（特許文献1参照。）。さらに、本発明者によりカオス方程式を用いたブロック符号化変調方式が提案されている（非特許文献1参照。）。 10

【 0 0 0 4 】

【特許文献1】特開2001-326631号公報

【非特許文献1】岡本英二，”カオス方程式を用いた符号化変調方式の一検討，”信学技法，RCS2001-307，pp.159-164，Mar.2002

【発明の開示】

【発明が解決しようとする課題】

【 0 0 0 5 】

しかしながら、上述したターボ符号では比較的大きいサイズのインターリーバと繰り返し演算が必要なため、逐次的に復号結果を取り出すことができないという問題がある。一方、従来の暗号化技術は符号化とは別の概念で用いられており、高品質な伝送を行うための符号化技術と、秘匿性を高めるための暗号化技術とは別々に処理されていたため、計算規模が増大していたという問題がある。 20

【 0 0 0 6 】

解決しようとする課題は、低受信信号品質でも比較的良好な伝送誤り率特性が得られ、かつ逐次復号が可能であり、さらに通信信号系列が雑音に近く、他者が通信内容を容易に解読できない秘匿性に優れたカオス符号化変調方式を提供することである。

【課題を解決するための手段】

【 0 0 0 7 】

以下、上記課題を解決するのに適した各手段につき、必要に応じて作用効果を付記しつつ説明する。 30

【 0 0 0 8 】

1. 送信側と受信側との間で符号化変調により情報の伝送を行う符号化変調復調方法であって、

前記送信側は、

伝送情報ビット列をカオス生成器に入力して符号化信号系列を生成し、符号化変調方式のカオス伝送信号系列として前記受信側へ伝送するカオス伝送信号系列生成ステップを備え、

前記受信側は、

推定送信系列を生成する推定送信系列生成ステップと、 40

前記推定送信系列を入力として前記送信側の前記カオス伝送信号系列生成ステップと同一の処理により推定伝送信号系列を生成する推定伝送信号系列生成ステップと、

前記送信側より受信した受信信号系列と前記推定伝送信号系列との誤差を計算し、その最小誤差を与える推定送信系列を前記受信信号系列の復号結果として出力する復号ステップと

を備え、

前記送信側における前記カオス伝送信号系列生成ステップは、

前記伝送情報ビット列と帰還されたカオス系列とを入力として所定の入力側演算を施すことにより入力信号系列を生成する入力側演算ステップと、

前記入力信号系列を入力として前記カオス生成器によりカオス系列を生成するカオス 50

系列生成ステップと、

前記カオス系列を入力として所定の出力側演算を施すことにより前記カオス伝送信号系列を生成する出力側演算ステップと

を備え、

前記受信側における前記推定伝送信号系列生成ステップは、

前記推定送信系列と帰還された推定カオス系列とを入力として前記送信側と同一の入力側演算を施すことにより推定入力信号系列を生成する入力側演算ステップと、

前記推定入力信号系列を入力として前記送信側と同一のカオス生成器により推定カオス系列を生成する推定カオス系列生成ステップと、

前記推定カオス系列を入力として前記送信側と同一の出力側演算を施すことにより推定伝送信号系列を生成する出力側演算ステップと

を備えたことを特徴とするカオス符号化変調復調方法。

手段 1 によれば、送信側において、カオス伝送信号系列生成ステップが伝送情報ビット列をカオス生成器に入力して符号化信号系列を生成し、符号化変調方式のカオス伝送信号系列として受信側へ伝送すると、受信側において、推定送信系列生成ステップが推定送信系列を生成し、推定伝送信号系列生成ステップが推定送信系列を入力として送信側のカオス伝送信号系列生成ステップと同一の処理により推定伝送信号系列を生成し、復号ステップが送信側より受信した受信信号系列と推定伝送信号系列との誤差を計算し、その最小誤差を与える推定送信系列を受信信号系列の復号結果として出力する。従って、カオス系列を用いたアナログ符号化、つまり信号波形による符号化を行うことにより、良好な伝送特性と伝送の秘匿性とを両立することができる。すなわち、低受信信号品質でも比較的良好的な伝送誤り率特性が得られ、かつ逐次復号が可能である。さらに通信信号系列がカオスによってランダムに変動するため雑音に近く、他者が通信内容を容易に解読できない秘匿性に優れた情報の伝送を行うことができる。つまり、カオス系列を用いることにより伝送信号が疑似雑音的に変化するため信号自体では伝送情報が明確ではなく、かつ送信側及び受信側で用いるカオス伝送信号系列生成ステップにおけるパラメータを全て把握しなければ、カオス系列の無相関性から他者が復号を行うことがほぼ不可能であることから伝送の秘匿性が実現されている。尚、カオス生成器の種類は何を用いてもよく、複数の系統を混在させてもよい。符号化過程の演算の自由度も高く、符号化率の設定も自由である。

特に、送信側において、入力側演算ステップが伝送情報ビット列と帰還されたカオス系列とを入力として所定の入力側演算を施すことにより入力信号系列を生成し、カオス系列生成ステップが入力信号系列を入力としてカオス生成器によりカオス系列を生成し、出力側演算ステップが、カオス系列を入力として所定の出力側演算を施すことによりカオス伝送信号系列を生成する。一方、受信側において、推定送信系列生成ステップが推定送信系列を生成し、入力側演算ステップは推定送信系列と帰還された推定カオス系列とを入力として送信側と同一の入力側演算を施すことにより推定入力信号系列を生成し、推定カオス系列生成ステップは推定入力信号系列を入力として送信側と同一のカオス生成器により推定カオス系列を生成し、出力側演算ステップは推定カオス系列を入力として送信側と同一の出力側演算を施すことにより推定伝送信号系列を生成し、復号ステップは送信側より受信した受信信号系列と推定伝送信号系列との誤差を計算し、その最小誤差を与える推定送信系列を受信信号系列の復号結果として出力する。尚、入力側演算としては、カオス生成器の収束範囲内の演算であればどのような演算を用いてもよく、出力側演算としては、例えば、最大振幅等を制限する演算を用いてもよい。

【 0 0 0 9 】

2 . 前記所定の入力側演算 f は、数式 $f(k, s_1(k-1)) = s_1(k-1)$ で表される (但し、 s_1 はカオス生成器への入力信号系列を表し、 $k = 0, 1, \dots$ である。) ことを特徴とする手段 1 に記載のカオス符号化変調復調方法。

手段 2 によれば、送信側において、入力側演算ステップが伝送情報ビット列と帰還されたカオス系列とを入力としてカオス生成器の収束範囲内の演算である入力側演算 f を施すことにより入力信号系列を生成し、カオス系列生成ステップが入力信号系列を入力として

10

20

30

40

50

カオス生成器によりカオス系列を生成し、出力側演算ステップが、カオス系列を入力として所定の出力側演算を施すことによりカオス伝送信号系列を生成する。一方、受信側において、推定送信系列生成ステップが推定送信系列を生成し、入力側演算ステップは推定送信系列と帰還された推定カオス系列とを入力として送信側と同一の入力側演算 f を施すことにより推定入力信号系列を生成し、推定カオス系列生成ステップは推定入力信号系列を入力として送信側と同一のカオス生成器により推定カオス系列を生成し、出力側演算ステップは推定カオス系列を入力として送信側と同一の出力側演算を施すことにより推定伝送信号系列を生成し、復号ステップは送信側より受信した受信信号系列と推定伝送信号系列との誤差を計算し、その最小誤差を与える推定送信系列を受信信号系列の復号結果として出力する。

10

【 0 0 1 0 】

3 . 前記所定の出力側演算 h は、以下の数式で表されることを特徴とする手段 2 に記載のカオス符号化変調復調方法。

【 数 1 】

$$h(k, b(n), s_1(k)) = \begin{cases} s_2(k) & : b(n) = 0 \\ s_2(k) + 3 \exp j(\text{rad}[s_2(k)] + \pi) & : b(n) = 1 \end{cases}$$

但し、 b はデジタルの伝送情報ビット列 $\{ 0, 1 \}$ を表し、 $n, k = 0, 1, \dots$ である。

手段 3 によれば、送信側において、入力側演算ステップが伝送情報ビット列と帰還されたカオス系列とを入力としてカオス生成器の収束範囲内の演算である入力側演算 f を施すことにより入力信号系列を生成し、カオス系列生成ステップが入力信号系列を入力としてカオス生成器によりカオス系列を生成し、出力側演算ステップが、カオス系列を入力として出力側演算 h を施すことによりカオス伝送信号系列を生成する。一方、受信側において、推定送信系列生成ステップが推定送信系列を生成し、入力側演算ステップは推定送信系列と帰還された推定カオス系列とを入力として送信側と同一の入力側演算 f を施すことにより推定入力信号系列を生成し、推定カオス系列生成ステップは推定入力信号系列を入力として送信側と同一のカオス生成器により推定カオス系列を生成し、出力側演算ステップは推定カオス系列を入力として送信側と同一の出力側演算 h を施すことにより推定伝送信号系列を生成し、復号ステップは送信側より受信した受信信号系列と推定伝送信号系列との誤差を計算し、その最小誤差を与える推定送信系列を受信信号系列の復号結果として出力する。尚、出力信号は $b(n)$ の違いにより 3 以上のユークリッド距離を有する。

20

30

【 0 0 1 1 】

4 . 前記 $s_2(k)$ は、以下の数式で表されることを特徴とする手段 3 に記載のカオス符号化変調復調方法。

【 数 2 】

$$s_2(k) = \frac{\text{Re}[s_1(k)] + \text{Im}[s_1(k)]}{75} + j \frac{\text{Re}[-s_1(k)] + \text{Im}[s_1(k)]}{20}$$

手段 4 において、 $s_2(k)$ は、円環状カオスの生成式により導かれる。

40

【 0 0 1 2 】

5 . 前記カオス生成器は、円環状カオスの生成方程式を用いて、初期値を $x_0 = \text{Re}[s_1(k)]$, $y_0 = \text{Im}[s_1(k)]$ とし、以下の数式で表わされるものとしたことを特徴とする手段 2 乃至 4 のいずれかに記載のカオス符号化変調復調方法。

【数3】

$$\begin{cases} x_{l+1} = y_l - 1.73x_l + \frac{5(-1+x_l^2)}{1+x_l^2} + \tan^{-1}(x_l + y_l) \\ y_{l+1} = -0.98x_l \end{cases}$$

$$s_1(k) = x_{20} + j y_{20}$$

手段5によれば、上記 $s_1(k)$ の式より、 x_{l+1} と y_{l+1} の式が1出力ごとに20回繰り返されることになる。なお、出力される伝送信号は振幅と位相が変化するカオス変調信号 (chaos shift keying: CSK) となる。

10

【0013】

6. 前記所定の出力側演算 h は、以下の数式で表されることを特徴とする手段2に記載のカオス符号化変調復調方法。

【数4】

$$h(k, b(n), s_1(k)) = \begin{cases} \exp j(\text{rad}[s_2(k)]) & : b(n) = 0 \\ \exp j(\text{rad}[s_2(k)] + \pi) & : b(n) = 1 \end{cases}$$

但し、 b はデジタルの伝送情報ビット列 $\{0, 1\}$ を表し、 $n, k = 0, 1, \dots$ である。

20

手段6によれば、送信側において、入力側演算ステップが伝送情報ビット列と帰還されたカオス系列とを入力としてカオス生成器の収束範囲内の演算である入力側演算 f を施すことにより入力信号系列を生成し、カオス系列生成ステップが入力信号系列を入力としてカオス生成器によりカオス系列を生成し、出力側演算ステップが、カオス系列を入力として出力側演算 h を施すことによりカオス伝送信号系列を生成する。一方、受信側において、推定送信系列生成ステップが推定送信系列を生成し、入力側演算ステップは推定送信系列と帰還された推定カオス系列とを入力として送信側と同一の入力側演算 f を施すことにより推定入力信号系列を生成し、推定カオス系列生成ステップは推定入力信号系列を入力として送信側と同一のカオス生成器により推定カオス系列を生成し、出力側演算ステップは推定カオス系列を入力として送信側と同一の出力側演算 h を施すことにより推定伝送信号系列を生成し、復号ステップは送信側より受信した受信信号系列と推定伝送信号系列との誤差を計算し、その最小誤差を与える推定送信系列を受信信号系列の復号結果として出力する。尚、変調信号は振幅1で位相のみ変動するカオス位相変調信号 (chaos phase shift keying: CPSK) となる。

30

【0014】

7. 前記所定の出力側演算 h は、以下の数式で表されることを特徴とする手段2に記載のカオス符号化変調復調方法。

【数5】

$$h(k, b(n), s_1(k)) = \begin{cases} (1+0.5p)s_2(k) & : b(n) = 0 \\ (1+0.5p)\{s_2(k) + 3\exp j(\text{rad}[s_2(k)] + \pi)\} & : b(n) = 1 \end{cases}$$

$$p = \{k - nr_c + b(n)\} \bmod 2$$

40

但し、 b はデジタルの伝送情報ビット列 $\{0, 1\}$ を表し、 $n, k = 0, 1, \dots$ である。

手段7によれば、送信側において、入力側演算ステップが伝送情報ビット列と帰還されたカオス系列とを入力としてカオス生成器の収束範囲内の演算である入力側演算 f を施すことにより入力信号系列を生成し、カオス系列生成ステップが入力信号系列を入力としてカオス生成器によりカオス系列を生成し、出力側演算ステップが、カオス系列を入力とし

50

て出力側演算 h を施すことによりカオス伝送信号系列を生成する。一方、受信側において、推定送信系列生成ステップが推定送信系列を生成し、入力側演算ステップは推定送信系列と帰還された推定カオス系列とを入力として送信側と同一の入力側演算 f を施すことにより推定入力信号系列を生成し、推定カオス系列生成ステップは推定入力信号系列を入力として送信側と同一のカオス生成器により推定カオス系列を生成し、出力側演算ステップは推定カオス系列を入力として送信側と同一の出力側演算 h を施すことにより推定伝送信号系列を生成し、復号ステップは送信側より受信した受信信号系列と推定伝送信号系列との誤差を計算し、その最小誤差を与える推定送信系列を受信信号系列の復号結果として出力する。尚、畳込み符号のパリティにより伝送信号の振幅を変動させ、過去の $b(n)$ の違いによってもユークリッド距離が伸びる。

10

【 0 0 1 5 】

8 . 前記出力側演算は、前記カオス系列から振幅、位相とも疑似雑音的に変化するカオス伝送信号系列を生成することを特徴とする手段 1 乃至 7 のいずれかに記載のカオス符号化変調復調方法。

手段 8 によれば、出力側演算は、カオス系列から振幅、位相とも疑似雑音的に変化するカオス伝送信号系列を生成するので、極めて秘匿性の高い情報の伝送を行うことができる。

【 0 0 1 6 】

9 . 前記出力側演算は、前記カオス系列から振幅又は位相のいずれか一方のみが変化するカオス伝送信号系列を生成することを特徴とする手段 1 乃至 7 のいずれかに記載のカオス符号化変調復調方法。

20

手段 9 によれば、出力側演算は、カオス系列から振幅又は位相のいずれか一方のみが変化するカオス伝送信号系列を生成するので、安価なデバイスを用いてカオス伝送信号系列を生成することができる。

【 0 0 1 7 】

1 0 . 前記受信側における前記復号ステップは、所定の長さ $v-1$ 以上の各系列に対して、復号拘束長を 1 増加させる毎に前記推定伝送信号系列を $1/2$ ずつ廃棄して前記誤差計算を行うことを特徴とする手段 1 乃至 9 のいずれかに記載のカオス符号化変調復調方法。

手段 1 0 によれば、所定の長さ $v-1$ 未満の系列に対しては全探索を行って誤差計算を行い、 $v-1$ 以上の各系列に対しては復号拘束長を 1 増加させる毎に推定伝送信号系列を $1/2$ ずつ廃棄して誤差計算を行うので、計算系列数を常に 2^{v-1} 個に保つことができ、計算量の発散を防止しつつ復号拘束長を増加させて復号誤り率を低減することができる。

30

【 0 0 1 8 】

1 1 . 送信側と受信側との間で符号化変調により情報の伝送を行う符号化変調復調方法であって、

前記送信側は、

伝送情報ビット列をカオス生成器に入力して符号化信号系列を生成し、符号化変調方式のカオス伝送信号系列として前記受信側へ伝送するカオス伝送信号系列生成ステップを備え、

前記受信側は、

推定送信系列を生成する推定送信系列生成ステップと、
前記推定送信系列を入力として前記送信側の前記カオス伝送信号系列生成ステップと同一の処理により推定伝送信号系列を生成する推定伝送信号系列生成ステップと、
前記送信側より受信した受信信号系列と前記推定伝送信号系列との誤差を計算し、その最小誤差を与える推定送信系列を前記受信信号系列の復号結果として出力する復号ステップと

40

を備え、

前記受信側における前記復号ステップは、所定の長さ $v-1$ 以上の各系列に対して、復号拘束長を 1 増加させる毎に前記推定伝送信号系列を $1/2$ ずつ廃棄して前記誤差計算を行うことを特徴とするカオス符号化変調復調方法。

50

手段 1 1 によれば、送信側において、カオス伝送信号系列生成ステップが伝送情報ビット列をカオス生成器に入力して符号化信号系列を生成し、符号化変調方式のカオス伝送信号系列として受信側へ伝送すると、受信側において、推定送信系列生成ステップが推定送信系列を生成し、推定伝送信号系列生成ステップが推定送信系列を入力として送信側のカオス伝送信号系列生成ステップと同一の処理により推定伝送信号系列を生成し、復号ステップが送信側より受信した受信信号系列と推定伝送信号系列との誤差を計算し、その最小誤差を与える推定送信系列を受信信号系列の復号結果として出力する。従って、カオス系列を用いたアナログ符号化、つまり信号波形による符号化を行うことにより、良好な伝送特性と伝送の秘匿性とを両立することができる。すなわち、低受信信号品質でも比較的良好的な伝送誤り率特性が得られ、かつ逐次復号が可能である。さらに通信信号系列がカオスによってランダムに変動するため雑音に近く、他者が通信内容を容易に解読できない秘匿性に優れた情報の伝送を行うことができる。つまり、カオス系列を用いることにより伝送信号が疑似雑音的に変化するため信号自体では伝送情報が明確ではなく、かつ送信側及び受信側で用いるカオス伝送信号系列生成ステップにおけるパラメータを全て把握しなければ、カオス系列の無相関性から他者が復号を行うことがほぼ不可能であることから伝送の秘匿性が実現されている。尚、カオス生成器の種類は何を用いてもよく、複数の系統を混在させてもよい。符号化過程の演算の自由度も高く、符号化率の設定も自由である。

10

特に、所定の長さ $v-1$ 未満の系列に対しては全探索を行って誤差計算を行い、 $v-1$ 以上の各系列に対しては復号拘束長を 1 増加させる毎に推定伝送信号系列を $1/2$ ずつ廃棄して誤差計算を行うので、計算系列数を常に 2^{v-1} 個に保つことができ、計算量の発散を防止しつつ復号拘束長を増加させて復号誤り率を低減することができる。

20

【 0 0 1 9 】

1 2 . 前記受信側における前記復号ステップは、復号拘束長を可變的に設定することを特徴とする手段 1 乃至 1 1 のいずれかに記載のカオス符号化変調復調方法。

手段 1 2 によれば、受信側における復号ステップが、復号拘束長を可變的に設定するので、復号拘束長の長さによって計算量とビット誤り率とのトレードオフを得て、受信側のみで復号ビット誤り率を所望に制御することができる。尚、復号拘束長とは、復号結果を得るために用いる信号系列の長さであり、本発明では、復号ステップにおいて誤差計算の対象となる受信信号系列又は推定伝送信号系列の長さを意味する。

1 3 . 前記受信側における前記復号ステップは、復号ビットの確からしさの尺度に基づいて前記復号拘束長を可變的に設定することを特徴とする手段 1 2 に記載のカオス符号化変調復調方法。

30

手段 1 3 によれば、受信側における復号ステップが、復号ビットの確からしさの尺度に基づいて復号拘束長を可變的に設定するので、復号ビットの確からしさが高いときは復号拘束長を短く設定して計算量を低減し、復号ビットの確からしさが低いときは復号拘束長を長く設定して探索範囲を広げて確からしさを向上させることができる。

1 4 . 前記受信側における前記復号ステップは、前記推定送信系列における復号ビットを 0 とした場合の前記受信信号系列との最小誤差 d_0 と、前記復号ビットを 1 とした場合の最小誤差 d_1 とを比較し、前記最小誤差 d_1 の方が小さい場合は前記復号ビットを 1 と復号し、前記最小誤差 d_0 の方が小さい場合は前記復号ビットを 0 と復号することを特徴とする手段 1 乃至 1 3 のいずれかに記載のカオス符号化変調復調方法。

40

手段 1 4 によれば、最小誤差 d_0 よりも最小誤差 d_1 の方が小さい場合は、0 よりも 1 の方がより確からしい値であるため、復号ビットが 1 と復号され、最小誤差 d_1 よりも最小誤差 d_0 の方が小さい場合は、1 よりも 0 の方がより確からしい値であるため、復号ビットが 0 と復号される。尚、最小誤差 d_0 と最小誤差 d_1 とが等しい場合、0 と 1 とで確からしさの優劣がつかないため、復号ビットを任意の値 (0 又は 1) に復号するようにしてもよい。

【 0 0 2 0 】

1 5 . 前記受信側における前記復号ステップは、前記最小誤差 d_0 と前記最小誤差 d_1 との差の絶対値を 0 以上の閾値と比較し、前記差の絶対値が前記閾値以上の場合は復号を

50

行い、前記閾値未満の場合は復号拘束長を増加させて前記最小誤差 d_0 、 d_1 を再計算することを特徴とする手段 1 4 に記載のカオス符号化変調復調方法。

手段 1 5 において、最小誤差 d_0 と最小誤差 d_1 との差の絶対値が閾値以上の場合、受信信号系列と推定伝送信号系列との最小誤差 d_0 、 d_1 の差が十分に大きく、確からしい復号結果を得ることができる。よって、この場合は、復号拘束長を増加させることなく復号を行うことにより、計算量の増大を抑えることができる。一方、最小誤差 d_0 と最小誤差 d_1 との差の絶対値が閾値未満の場合は、最小誤差 d_0 、 d_1 の差が小さく、確からしい復号結果を得ることができない。よって、この場合は、復号拘束長を増加させて d_0 、 d_1 を再計算し、最小誤差 d_0 と最小誤差 d_1 との差の絶対値が閾値以上となるまで復号拘束長の増加と誤差計算とを繰り返すことによって、より確からしい復号結果を得ることができる。

10

1 6 . 前記送信側における前記カオス伝送信号系列生成ステップは、複数のカオス生成器を用いて、前記伝送情報ビットの値によって異なるカオス生成器によりカオス伝送信号系列を生成することを特徴とする手段 1 乃至 1 5 のいずれかに記載のカオス符号化変調復調方法。

手段 1 6 によれば、伝送情報ビットの値が 0 か 1 によって、異なるカオス生成器によりカオス伝送信号系列を生成するので、同一の 0、1 の系列を与えない限り同一のカオス伝送信号系列を得ることができない（換言すれば、復号拘束長が無量大である）ため、良好な伝送誤り率特性を得ることができる。

1 7 . 前記送信側における前記カオス伝送信号系列生成ステップは、縦続又は並列或いはこれらの組み合わせにより接続された複数のカオス生成器を用いて前記カオス伝送信号系列を生成することを特徴とする手段 1 乃至 1 6 のいずれかに記載のカオス符号化変調復調方法。

20

手段 1 7 によれば、カオス伝送信号系列生成ステップが、縦続又は並列或いはこれらの組み合わせにより接続された複数のカオス生成器を用いてカオス伝送信号系列を生成するので、信号系列のランダム性をより増大させて、情報伝送の秘匿性を向上させることができる。

【 0 0 2 1 】

1 8 . 前記送信側における前記カオス伝送信号系列生成ステップは、

前記カオス伝送信号系列をパケット化すると共に前記カオス生成器によるカオス系列の生成を一旦終了して前記カオス生成器を初期化するパケット化ステップを含むことを特徴とする手段 1 乃至 1 7 のいずれかにカオス符号化変調復調方法。

30

手段 1 8 によれば、カオス伝送信号系列生成ステップは、パケット化ステップにおいてカオス伝送信号系列をパケット化すると共にカオス生成器によるカオス系列の生成を一旦終了してカオス生成器を初期化するので、一部のビットに復号誤りが生じた場合でも、当該ビット以降の系列に誤りが伝搬することを抑制することができる。

1 9 . 前記パケット化ステップは、前記各パケットを終端させる際にテールビットを挿入することを特徴とする手段 1 8 に記載のカオス符号化変調復調方法。

手段 1 9 によれば、パケット化ステップが、各パケットを終端させる際にテールビットを挿入するので、パケット終端付近でのビット誤りを抑制することができる。

40

2 0 . 前記カオス伝送信号系列生成ステップの前又は後に実行され且つ雑音的に変化する変調信号を許容する他方式の符号化ステップを更に備えたことを特徴とする手段 1 乃至 1 9 のいずれかに記載のカオス符号化変調復調方法。

手段 2 0 によれば、カオス伝送信号系列生成ステップと他方式の符号化ステップとを組み合わせることで、復号ステップにおける計算量をより一層低減することができる。例えば、他方式の符号化ステップとしては、雑音的に変化する変調信号を許容する他の符号化（ターボ符号など）、MIMO (Multiple-input multiple-output) 伝送手法、多重伝送手法等を用いることができる。

【 発明の 効果 】

【 0 0 2 2 】

50

本発明によれば、カオス系列を用いたアナログ符号化、つまり信号波形による符号化を行うことにより、良好な伝送特性と伝送の秘匿性とを両立することができる。すなわち、低受信信号品質でも比較的良好な伝送誤り率特性が得られ、かつ逐次復号が可能である。さらに通信信号系列がカオスによってランダムに変動するため雑音に近く、他者が通信内容を容易に解読できない秘匿性に優れた情報の伝送を行うことができる。

【発明を実施するための最良の形態】

【0023】

以下、本発明のカオス符号化変調復調方法を具体化した実施の形態について、図面を参照しつつ詳細に説明する。まず、本実施形態の構成を説明し、続いて伝送特性について、シミュレーション結果を用いて説明する。

10

【0024】

図1に、送信側に設けられるカオス符号化器の構成を示す。カオス符号化器は、伝送情報ビット列をカオス生成器に入力して符号化信号系列を生成し、符号化変調方式のカオス伝送信号系列として受信側へ伝送する（カオス伝送信号系列生成ステップ）。

【0025】

以下、カオス符号化器において実行されるカオス伝送信号系列生成ステップの具体的な内容を説明する。まず、デジタルの伝送情報ビット列 $b(n) \in \{0, 1\}$ 、 $(n = 0, 1, \dots)$ が、1ビットずつ演算部 f に入力され、カオス生成器への入力信号系列 s_i が生成される（入力側演算ステップ）。このとき、

$$s_i(k) = f(k, b(n), s_i(k-1)), \quad (k = 0, 1, \dots) \quad (1)$$

20

で表される。 $s_i(k-1)$ は、後述する帰還をかけるカオス信号である。 f は、後段のカオス生成部の収束範囲内の演算であればどのようなものでもよい。

【0026】

次に、この $s_i(k)$ を入力として、カオス生成器によりカオスの特性をもつベクトル $s_1(k)$ が生成される（カオス系列生成ステップ）。これは出力信号となると同時に、次の $s_i(k+1)$ の入力ともなり、カオス系列生成を継続させる。なお、初期値 $s_1(-1)$ は事前に与えておく。

【0027】

そして、 $s_1(k)$ は、出力側演算 h により、

$$s(k) = h(b(n), s_1(k)) \quad (2)$$

30

として最大振幅などが制限されて、出力信号 $s(k)$ が得られる（出力側演算ステップ）。これは、カオス変調信号（本発明のカオス伝送信号系列）となる。

【0028】

なお、図2に示すカオス符号化器の変形例のように、複数のカオス生成器（カオス生成器1、カオス生成器2）を設け、演算 f において入力ビットもしくは入力系列によりカオス生成器を変更するように構成することも可能である。或いは、 $s(k)$ を他のカオス生成器の入力として用い、カオス生成器を多段縦続接続したり、並列接続して他のカオス系列信号と多重させてもよい。

【0029】

図1に示すように、本実施形態では、カオス系列を帰還し伝送ビットによって演算を施すことで、伝送ビット列ごとに各々対応した伝送信号が発生されるが、カオスの特性によりこれらは伝送ビットが異なればまったく異なる信号系列となる。つまり、(1)、(2)式において発生する伝送信号 $s(k)$ は、必ず $b(0), \dots, b(n-1)$ の値にも依存して変化することになる。したがって、本実施形態を符号化変調方式としてみたとき、符号の拘束長は任意に伸ばすことが可能であるといえる。

40

【0030】

図3に、受信側に設けられるカオス復号器の構成を示す。図中のカオス生成器、演算部 f, h などのカオス系列生成部分は送信側と同一のものを用いる。まず、カオス復号器内の図3左端に示すブロックにおいて、以下の数式で表わす推定送信系列を生成する（推定送信系列生成ステップ）。

50

【数 6】

$$\hat{b}(n)$$

【0031】

次に、この推定送信系列（上記数式）を入力として送信側のカオス伝送信号系列生成ステップと同一の処理により、以下の数式で表わす推定伝送信号系列を生成する（推定伝送信号系列生成ステップ）。

【数 7】

$$\hat{r}(k)$$

10

【0032】

すなわち、推定伝送信号系列生成ステップは、推定送信系列と帰還された推定カオス系列とを入力として送信側と同一の入力側演算 f を施すことにより推定入力信号系列を生成する入力側演算ステップと、推定入力信号系列を入力として送信側と同一のカオス生成器により推定カオス系列を生成する推定カオス系列生成ステップと、推定カオス系列を入力として送信側と同一の出力側演算 h を施すことにより推定伝送信号系列を生成する出力側演算ステップとを含んでいる。

【0033】

次に、送信側より受信された受信信号系列 $r(k)$ と推定伝送信号系列（上記数式）との誤差 E_r を算出する。誤差 E_r は、以下のように表わされる。

20

【数 8】

$$E_r = \text{err}[r(k), \hat{r}(k)] \quad (3)$$

【0034】

そして、最小誤差 $\min |E_r|$ を与える上述した推定送信系列を復号結果とする（復号ステップ）。ここで、 $\text{err}()$ は何らかの距離を導出する関数、例えば、以下の数式に示す 2 乗ユークリッド距離である。

【数 9】

$$|r(k) - \hat{r}(k)|^2$$

30

【0035】

復号は各 n 毎に単独に行うこともできるが、1 ビット ($l > 0$) を 1 フレームとして、以下に示すように、一括して復号することも可能である。

【数 10】

$$\hat{\mathbf{b}} = \{\hat{b}(n), \hat{b}(n+1), \dots, \hat{b}(n+l-1)\}$$

40

【数 11】

$$\mathbf{r} = \{r(n), r(n+1), \dots, r(n+l-1)\}$$

【数 12】

$$\hat{\mathbf{r}} = \{\hat{r}(n), \hat{r}(n+1), \dots, \hat{r}(n+l-1)\}$$

【0036】

この場合、推定送信系列 [数 10] の全系列を生成し、比較する必要がある。誤差の関

50

数として2乗ユークリッド距離を用いる場合、 E_r は、以下のように表わされる。

【数13】

$$E_r = \sum_l |r(k+l) - \hat{r}(k+l)|^2 \quad (4)$$

【0037】

(4)式において、 l は復号拘束長に相当するものである。また、閾値を用いることによりフレーム長(復号拘束長)を適応的に可変としてもよい。以下に復号拘束長を可变的に設定する方法について説明する。

10

【0038】

復号ビット(先頭ビット)が0であるときの推定送信系列を次式に、復号ビットが1であるときの推定送信系列を次々式にそれぞれ表わす。

【数14】

$$\hat{\mathbf{b}}_0 = \{0, \hat{b}(n+1), \dots, \hat{b}(n+l-1)\}$$

【数15】

$$\hat{\mathbf{b}}_1 = \{1, \hat{b}(n+1), \dots, \hat{b}(n+l-1)\}$$

20

【0039】

また、それぞれの最小誤差 $\min |E_r|$ を d_0 、 d_1 と表わし、(5)式に示すパラメータを導入する。

$$d[b(n)] = d_0 - d_1 \quad (5)$$

【0040】

そして、 $d[b(n)] > 0$ のとき $b(n) = 1$ 、 $d[b(n)] < 0$ のとき $b(n) = 0$ ($d[b(n)] = 0$ のときは任意)のように復号する。すなわち、最小誤差 d_0 よりも最小誤差 d_1 の方が小さい場合は、0よりも1の方がより確からしい値であるため、復号ビットが1と復号され、最小誤差 d_1 よりも最小誤差 d_0 の方が小さい場合は、1よりも0の方がより確からしい値であるため、復号ビットが0と復号される。また、最小誤差 d_0 と最小誤差 d_1 とが等しい場合、0と1とで確からしさの優劣がつかないため、復号ビットを任意の値(0又は1)に復号する。

30

【0041】

図4にこの復号手法の概念を示す。図4下の0, 1の並びにおいて、四角で囲んだ左端のビットが復号ビットであり、それ以外は復号結果を得るために必要とされるビットであって、全体で l ビットの長さとなっている。この $d[b(n)]$ に対してある閾値 s_h (0)を用いて、 $|d[b(n)]| \geq s_h$ なら復号、そうでなければ l として d_0 、 d_1 の再計算を行うというアルゴリズムを実行する。つまり、最小誤差 d_0 と最小誤差 d_1 との差の絶対値が閾値以上の場合、受信信号系列と推定伝送信号系列との最小誤差 d_0 、 d_1 の差が十分に大きく、確からしい復号結果を得ることができる。よって、この場合は、復号拘束長を増加させることなく復号を行うことにより、計算量の増大を抑えることができる。一方、最小誤差 d_0 と最小誤差 d_1 との差の絶対値が閾値未満の場合は、最小誤差 d_0 、 d_1 の差が小さく、確からしい復号結果を得ることができない。よって、この場合は、復号拘束長を増加させて d_0 、 d_1 を再計算し、最小誤差 d_0 と最小誤差 d_1 との差の絶対値が閾値以上となるまで復号拘束長の増加と誤差計算とを繰り返すことによって、より確からしい復号結果を得ることができる。

40

【0042】

以上により、閾値 s_h の設定によって復号計算量とビット誤り率(BER)とのトレードオフをある程度制御することが可能となる。すなわち、閾値 s_h を大きくすると l が大

50

きくなるまで計算を繰り返す場合が多くなり、あまり s_h が大きすぎると $|d[b(n)]|$ s_h なる l が増大して計算量が発散してしまうかもしれないが、信号系列 $s(k)$ における伝送符号自体の拘束長は信号系列長と同じ長さであるため、復号の拘束長である l が延びるほど復号ビット誤りが起こる確率が減ることになる。

【0043】

したがって、本実施形態は、同一の受信信号系列においても、拘束長 l もしくは s_h の値の設定により受信側のみでビット誤り率と計算複雑度とのトレードオフを実現することができる。しかし、復号拘束長 l のときの次式に示す推定送信系列の系列数は 2^l となるため、 l の増加に伴いすぐに計算量は発散してしまう。

【数16】

$$\hat{\mathbf{b}} = \{\hat{b}_0, \hat{b}_1\}$$

10

【0044】

そこで、(4)式の計算時に図5に示すように、 2^{v-1} までの系列は全探索を行い、それ以降は毎回 $b(n) = \{0, 1\}$ のそれぞれの領域において E_r の大きい系列を $1/2$ ずつ廃棄し、計算系列数を常に 2^{v-1} 個に保つことを考える。これにより、計算量の発散を防ぎつつ l を増加させることが可能となる。 $v-1$ が小さい場合は正しい復号系列を誤って廃棄する確率が上がるため l を伸ばしても効果が少ないが、 $v-1$ と l とを大きくすることで受信側のみで復号誤り率を下げる事が可能となる。また、一旦、推定送信系列[数式1]を誤って復号すると、以降の復号器内のカオス系列が送信側と合致しなくなり、復号誤りが以降のビットに伝播して正常な復号が行えなくなる。この誤り伝播を防ぐために、カオス伝送信号系列のパケット化を行うようにしてもよい。

20

【0045】

例えば、送信器側で、図6に示すようなパケット化を行い、パケットの終端にテールビットを挿入し、パケット終端でカオス生成器を初期化する(パケット化ステップ)。カオス生成器の初期化とは、カオス生成器を初期値 $s_1(-1)$ に戻すことである。受信側でも同様にパケット終端で初期化を行うことで、パケット内に誤りが生じても後段のパケットへの誤り伝播を防ぐことができる。

【0046】

原理的には、テールビットを挿入せずカオス生成器の状態をパケットの終端で初期化するだけでもよいが、その場合パケット終端付近のデータは復号拘束長を伸ばすことができないため誤り確率が上昇する。

30

【0047】

これまでの検討では、入力 $b(n)$ は1ビットであったが、図7に示すように数ビットの $b(n)$ として演算 f に入力することも可能である。この一度に入力する $b(n)$ のビット数を n_d とし、 $b(n)$ に対して出力される $s(k)$ の数を r_c 個とした場合、 $r_c/n_d > 1$ であれば冗長度を付加する符号化を施すことになる。このとき、図6のパケット構成を含めると全体の伝送効率は、次式によって表わされる。

【数17】

$$\frac{n_d \cdot k_d}{(k_d + k_t) \cdot r_c} \text{ bit/symbol}$$

40

【実施例1】

【0048】

図8に示すような、入力ビットにより後段の出力側演算 h のみを操作する符号化器を用いて伝送信号を発生させる符号の伝送を考える。受信器においても同じ構成のカオス生成器、 f , h , 初期値 $s_1(-1)$ を持つものとする。

【0049】

50

図9のような等価低域系、ガウス雑音通信路の等価低域系伝送システムにおけるシミュレーションを行い、伝送特性を調べた。なお、以降では受信側での同期は完全に取れていることを仮定する。伝送システムのパラメータは表1のとおりであり、符号化器におけるパラメータは、入力側演算 f を、

$$f(k, s_1(k-1)) = s_1(k-1) \quad (6)$$

とし、出力側演算 h を以下のようにした。

【数18】

$$h(k, b(n), s_1(k)) = \begin{cases} s_2(k) & : b(n) = 0 \\ s_2(k) + 3 \exp j(\text{rad}[s_2(k)] + \pi) & : b(n) = 1 \end{cases} \quad (7)$$

10

【表1】

n_d	1
r_c	10
k_d	20000
k_t	4
v_l	8 - 13
l_{max}	$20v_l - 100$
sh	$12r_c \times$ (平均信号電力)

20

【0050】

ここで、 $s_2(k)$ は、以下のとおりである。

【数19】

$$s_2(k) = \frac{\text{Re}[s_1(k)] + \text{Im}[s_1(k)]}{75} + j \frac{\text{Re}[-s_1(k)] + \text{Im}[s_1(k)]}{20} \quad (8)$$

30

【0051】

カオス生成器には、円環状カオスの生成方程式を用いて、初期値を $x_0 = \text{Re}[s_1(k)]$, $y_0 = \text{Im}[s_1(k)]$ とし、以下の(9)式、(10)式で表わされるものとした。

【数20】

$$\begin{cases} x_{i+1} = y_i - 1.73x_i + \frac{5(-1+x_i^2)}{1+x_i^2} + \tan^{-1}(x_i + y_i) \\ y_{i+1} = -0.98x_i \end{cases} \quad (9)$$

40

$$s_1(k) = x_{20} + j y_{20} \quad (10)$$

【0052】

(7)式より、出力信号は $b(n)$ の違いにより3以上のユークリッド距離を有することになる。(8)式は、(9)式のカオス生成式より導かれる式であり、(10)式より(9)式は1出力ごとに20回繰り返されることになる。また、初期値 $s_1(-1)$ は乱数によって発生させた。なお、出力される伝送信号は振幅と位相が変化するカオス変調信号(chaos shift keying: CSK)となる。また、出力側演算 h を(11)式のようにすると、変調信号は振幅1で位相のみ変動するカオス位相変調信号(c 50

chaos phase shift keying : CPSK)となる。

【数 2 1】

$$h(k, b(n), s_1(k)) = \begin{cases} \exp j(\text{rad}[s_2(k)]) & : b(n) = 0 \\ \exp j(\text{rad}[s_2(k)] + \pi) & : b(n) = 1 \end{cases} \quad (11)$$

【0053】

ここで、CSKにより構成された伝送信号系列をベースバンドにおけるIQ平面で示すと図10のようになる。この点列はカオス系列の特徴として、初期値 $s_1(-1)$ 、伝送情報ビット列、カオス方程式の種類などによって互いに異なる無相関な遷移を示すため、第三者はこれら全てのパラメータが一致し、フレーム同期、シンボル同期を獲得し、その時点以前の $b(n)$ を正しく把握している場合以外には元のデータ系列 $b(n)$ を復号することは困難である。したがって、本手法は秘匿性の高さを併せ持つ方式であるといえる。なお、表1から全体の伝送効率は、ほぼ 0.1 bit/symbol となる。

10

【0054】

図11に復号器の構成を示す。図中のカオス生成部分は図8の符号化器のものと同じである。誤差の計算には(4)式の2乗ユークリッド距離を用い、(5)式のパラメータに対し閾値 s_h を設定して拘束長を可変とし、1ビットずつ復号する復号法を適用した。ここで、表1に示すように、 $v_1 = 8 \sim 13$ 、最大の拘束長を l_{max} とした。

【0055】

すなわち、復号においては、まず、 $v_1 = 8$ とし、(4)、(5)式により復号計算を行う。拘束長が l_{max} に達するまでに(5)式の $d[b(n)]$ が s_h を越えた場合は判定を行い、次のビットへと進む。 s_h を越えずに l_{max} に達した場合は、 $v_1 = v_1 + 1$ として同様に計算を繰り返す。最終的に $v_1 = 13$ 、拘束長が l_{max} となっても s_h を越えない場合は、その時点までの $|d[b(n)]|$ が最大となる $b(n)$ の値により判定を行う。

20

【0056】

シミュレーションでは E_b/N_0 が $2 \sim 10 \text{ dB}$ 、5フレーム(10^5 ビット)伝送時の平均復号拘束長と平均の v_1 (平均復号状態指数)を評価した。計算結果を図12に示す。なお、この設定ではいずれの場合も復号誤りは発生しなかった。図のように E_b/N_0 が大きくなるにつれて、平均復号拘束長が短くなり、平均 v_1 も低減していることがわかる。 E_b/N_0 の向上にともない v_1 が8を若干下回っているが、これはテールビット付近で実効的に復号複雑度が $v_1 = 1$ 相当まで下がるためである。

30

【0057】

以上のように、カオス方程式に基づく符号化変調を行い、閾値を用いて復号拘束長を適応的に可変とすることにより、 10^5 ビットの伝送において $E_b/N_0 = 2 \text{ dB}$ で無誤り伝送が実現された。 v_1 、 l_{max} の値を増加させることにより計算量とトレードオフの関係でこの特性はさらに改善されることが予想できる。さらに、伝送系列は第三者からは容易に復号できないという特徴を持つ。用いるカオス系列や符号化率、フレーム長、テールビット長、復号拘束長によりさまざま伝送特性が実現できると考えられる。

40

【実施例2】

【0058】

次に、図13に示すように、カオス符号化器の前段にトレリス符号化器を接続させて、 $b(n)$ をトレリス符号のパリティとした場合の特性を評価した。この例に示すように本装置はその他の伝送手法と組み合わせて用いることが可能である。

【0059】

用いたトレリス符号は、再帰的組織畳込み符号RSC[15/7]であり、 $b(n)$ はトレリス符号語のパリティビットとし無符号化情報ビットは伝送しない。そのため、トレリス符号化器による伝送効率の低下はなく、全体の伝送効率は実施例1と同じである。符号化器におけるパラメータは、実施例1の(7)式部分が以下の(12)式に示すと

50

おりとなり、畳込み符号のパリティにより伝送信号の振幅を変動させ、過去の $b(n)$ の違いによってもユークリッド距離が伸びるように設定した。それ以外は、実施例 1 と同じである。

【数 2 2】

$$h(k, b(n), s_1(k)) = \begin{cases} (1+0.5p)s_2(k) & : b(n)=0 \\ (1+0.5p)\{s_2(k)+3\exp j(\text{rad}[s_2(k)]+\pi)\} & : b(n)=1 \end{cases} \quad (12)$$

$$p = \{k - nr_c + b(n)\} \bmod 2$$

【0060】

復号側は、 $v_1 = 8 \sim 13$ の (4), (5) 式の計算が畳込み符号のトレリス線図も内包しているため、実施例 1 と同様に行う。

【0061】

実施例 1 のシミュレーション条件と同様に E_b/N_0 が $2 \sim 10$ dB、5 フレーム (10^5 ビット) 伝送時の平均復号拘束長と平均の v_1 (平均復号状態指数) を計算した。結果を図 14 に示す。本例においてもいずれの場合も復号誤りは発生しなかった。図 12 と同様に E_b/N_0 が大きくなるにつれて平均復号拘束長が短くなり、平均 v_1 も低減しており、しかも無符号化時に比べどちらもさらに低減していることが分かる。すなわち、外部の符号化器と組み合わせることで、復号計算量が低減されるということが示されている。以上のように、カオス符号化変調を用いて外部の伝送システムと組み合わせることで、

【図面の簡単な説明】

【0062】

【図 1】カオス符号化器の構成を示すブロック図である。

【図 2】カオス生成器を 2 系統用いた符号化器の変形例を示すブロック図である。

【図 3】カオス復号器の構成を示すブロック図である。

【図 4】フレームを用いた復号の概念図である。

【図 5】探索系列数の削減手法について概要を説明した図である。

【図 6】データビットとテールビットとからなるパケットの構成例を示す図である。

【図 7】入力ビット数及び演算 f の例を示す図である。

【図 8】実施例 1 で使用した符号化器の構成を示すブロック図である。

【図 9】シミュレーションに用いるカオス符号を用いた伝送システムのブロック図である。

【図 10】CSK の伝送信号系列の例を示したものである。

【図 11】実施例 2 で使用した復号器の構成を示すブロック図である。

【図 12】カオス符号化変調復調方法の伝送時における復号の平均復号拘束長と平均復号状態指数とを示すグラフである。

【図 13】畳込み符号を接続したカオス符号化器の構成を示すブロック図である。

【図 14】畳込み符号を接続した場合の伝送時における復号の平均復号拘束長と平均復号状態指数とを示すグラフである。

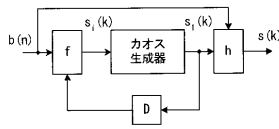
10

20

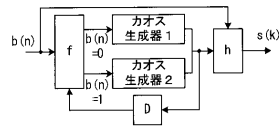
30

40

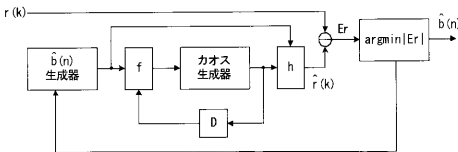
【図 1】



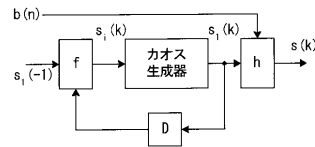
【図 2】



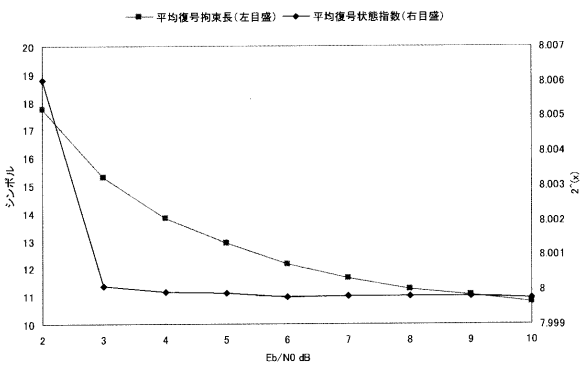
【図 3】



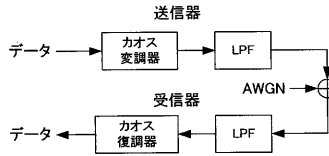
【図 8】



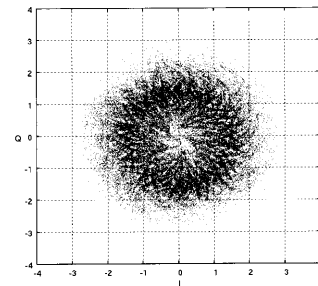
【図 1 2】



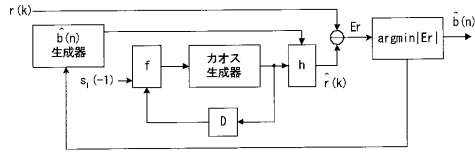
【図 9】



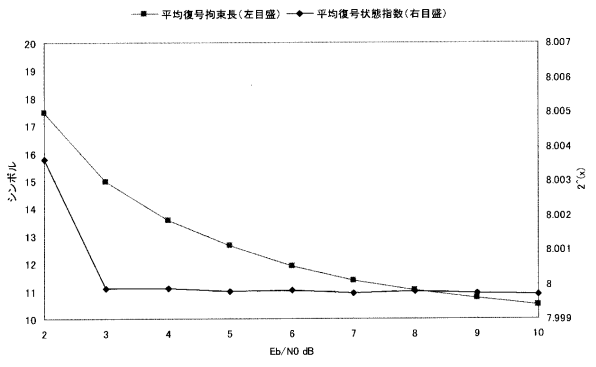
【図 1 0】



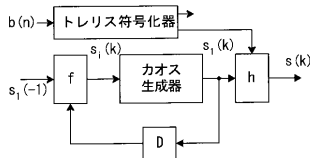
【図 1 1】



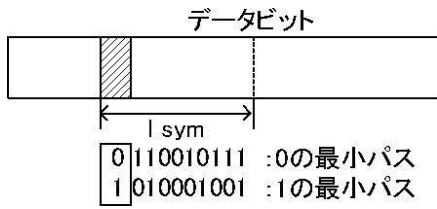
【図 1 4】



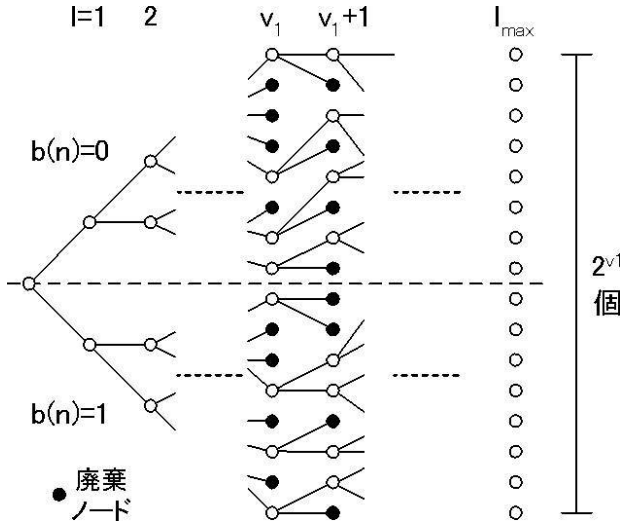
【図 1 3】



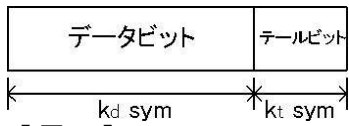
【図4】



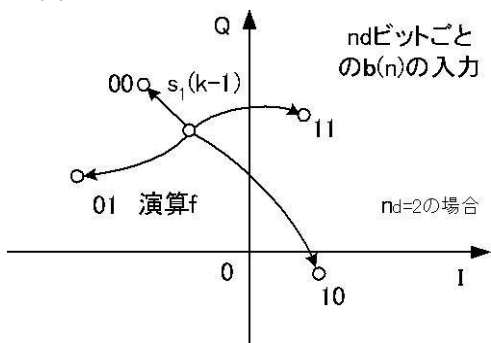
【図5】



【図6】



【図7】



フロントページの続き

(56)参考文献 特開平 2 - 2 7 3 8 9 (J P , A)

特開平 4 - 2 3 0 5 8 4 (J P , A)

岡本英二, カオス方程式を用いた符号化変調方式の一検討, 電子情報通信学会技術研究報告. RCS, 無線通信システム, 社団法人電子情報通信学会, 2 0 0 2 年 2 月 2 8 日, 101(683), 第159-164頁

(58)調査した分野(Int.Cl., DB名)

H 0 4 K 1 / 0 2

H 0 3 M 1 3 / 1 9

H 0 3 M 1 3 / 2 5

C i N i i