(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2005-354674
(P2005-354674A)
(43)公開日　平成17年12月22日(2005.12.22)

(51)Int.Cl.[7]	F I	テーマコード（参考）
H04K 1/02	H04K 1/02	5J065
H03M 13/19	H03M 13/19	5J104
H03M 13/25	H03M 13/25	

審査請求 未請求　請求項の数 14　ＯＬ　（全 17 頁）

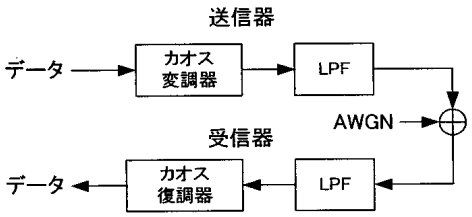
(21)出願番号　特願2005-140579 (P2005-140579)
(22)出願日　平成17年5月13日 (2005.5.13)
(31)優先権主張番号　特願2004-145381 (P2004-145381)
(32)優先日　平成16年5月14日 (2004.5.14)
(33)優先権主張国　日本国 (JP)

(71)出願人　304021277
国立大学法人　名古屋工業大学
愛知県名古屋市昭和区御器所町（番地なし）
(74)代理人　100110744
弁理士　藤川　敬知
(72)発明者　岡本　英二
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
(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

Ｆターム(参考)　5J065 AA01 AB01 AC02 AD10 AE06 AF02 AH02 AH22
5J104 AA01 AA32 FA08 JA20 NA02 NA19

(54)【発明の名称】カオス符号化変調復調方法

(57)【要約】
【課題】　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。
【解決手段】　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、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、推定送信系列を入力として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、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復号ステップとを備える。
【選択図】　図９



【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】
前記受信側における前記復号ステップは、復号拘束長を可変的に設定す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変的に設定す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。
【請求項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３のいずれかに記載のカオス符号化変調復調方法。
【請求項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４に記載のカオス符号化変調復調方法。
【請求項６】
前記受信側における前記復号ステップは、所定の長さｖ１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５のいずれかに記載のカオス符号化変調復調方法。
【請求項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、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、縦続又は並列或いはこれらの組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９】
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８のいずれかにカオス符号化変調復調方法。
【請求項１０】
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９に記載のカオス符号化変調復調方法。
【請求項１１】
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請求項１乃至１０のいずれかに記載のカオス符号化変調復調方法。
【請求項１２】
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１１に記載のカオス符号化変調復調方法。
【請求項１３】
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１１に記載のカオス符号化変調復調方法。
【請求項１４】
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１３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】
【０００１】
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】
【０００２】
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。
【０００３】

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。これは符号の並列連接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。）。

【０００４】

【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】

【０００５】

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。

【０００６】

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】

【０００７】

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。

【０００８】

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。

【０００９】

２．前記受信側における前記復号ステップは、復号拘束長を可変的に設定す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、受信側における復号ステップが、復号拘束長を可変的に設定するので、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。

【００１０】

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変的に設定す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。

手段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変的に設定するので、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。

【００１１】

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３のいずれかに記載のカオス符号化変調復調方法。

手段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。

【００１２】

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手段４に記載のカオス符号化変調復調方法。

手段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は、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が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。

【００１３】

６．前記受信側における前記復号ステップは、所定の長さｖｌ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５のいずれかに記載のカオス符号化変調復調方法。

手段６によれば、所定の長さｖｌ未満の系列に対しては全探査を行って誤差計算を行い、ｖｌ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_l}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。

【００１４】

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、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６のいずれかに記載のカオス符号化変調復調方法。

手段７によれば、伝送情報ビットの値が０か１かによって、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、復号拘束長が無限大である）ため、良好な伝送誤り率特性を得ることができる。

【００１５】

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、縦続又は並列或いはこれらの組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、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。

【００１６】

９．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８のいずれかにカオス符号化変調復調方法。

手段９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。

【００１７】

１０．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９に記載のカオス符号化変調復調方法。

手段１０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。

【００１８】

１１．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手段１乃至１０のいずれかに記載のカオス符号化変調復調方法。

手段１１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。

【００１９】

１２．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１１に記載のカオス符号化変調復調方法。

手段１２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。

【００２０】

１３．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１１に記載のカオス符号化変調復調方法。

手段１３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。

【００２１】

１４．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１３のいずれかに記載のカオス符号化変調復調方法。

手段１４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により、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】

【００２２】

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。

【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、ディジタルの伝送情報ビット列ｂ（ｎ）∈｛０，１｝，（ｎ＝０，１，…）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、

$s_i(k)=f(k, b(n), s_1(k-1))$，（ｋ＝０，１，…）（１）

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、

$s(k)=h(b(n), s_1(k))$　（２）

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），．．，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。

【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１］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）。

【数１】

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

【００３１】

次に、この推定送信系列［数式１］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２］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２】

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

【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［数式２］との誤差Ｅｒを算出する。誤差Ｅｒは、以下のように表わされる。

【数３】

$$\mathrm{Er} = \mathrm{err}\left[r(k), \hat{r}(k)\right] \quad (3)$$

【００３４】

そして、最小誤差ｍｉｎ｜Ｅｒ｜を与える推定送信系列［数式１］を復号結果とする（復号ステップ）。ここで、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４】

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

【００３５】

復号は各ｎ毎に単独に行うこともできるが、ｌ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５】

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

【数６】

$$\mathbf{r} = \left\{r(n), r(n+1), \cdots, r(n+l-1)\right\}$$

【数７】

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

【００３６】

この場合、推定送信系列［数式５］の全系列を生成し、比較する必要がある。誤差の関数として２乗ユークリッド距離を用いる場合、Ｅｒは、以下のように表わされる。

【数８】

$$\mathrm{Er} = \sum_{l} \left|r(k+l) - \hat{r}(k+l)\right|^2 \quad (4)$$

【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変的に設定する方法について説明する。

【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［数式９］に、復号ビットが１であるときの推定送信系列を［数式１０］にそれぞれ表わす。

【数９】

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

【数１０】

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

【００３９】

また、それぞれの最小誤差ｍｉｎ｜Ｅｒ｜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$_1$　　（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。

【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ｓｈ（≧　０）を用いて、｜ｄ［ｂ（ｎ）］｜≧ｓｈなら復号、そうでなければｌ　→　ｌ＋１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は、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が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。

【００４２】

以上により、閾値ｓｈ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ｓｈを大きくするとｌが大きくなるまで計算を繰り返す場合が多くなり、あまりｓｈが大きすぎると｜ｄ［ｂ（ｎ）］｜≧　ｓｈ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ｓｈ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のときの以下の［数式１１］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１１】

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

【００４４】

そこで、（４）式の計算時に図５に示すように、2^{v-l}までの系列は全探査を行い、それ以降は毎回ｂ（ｎ）＝｛０，１｝のそれぞれの領域においてＥｒの大きい系列を１／２ずつ廃棄し、計算系列数を常に2^{v-l}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。ｖ１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、ｖ１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ことが可能となる。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。

【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。

【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、以下の数式１２によって表わされる。

【数１２】

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

【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】

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）　（６）

とし、出力側演算ｈを以下のようにした。

【数１３】

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

【表１】

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

【００５０】

ここで、ｓ２（ｋ）は、以下のとおりである。

【数１４】

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

【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＝Ｒｅ［s_i（ｋ）］，y_0＝Ｉｍ［s_i（ｋ）］とし、以下の（９）式，（１０）式で表わされるものとした。

【数１５】

$$\begin{cases}x_{l+1}=y_l-1.73x_l+\dfrac{5\left(-1+x_l^2\right)}{1+x_l^2}+\tan^{-1}\left(x_l+y_l\right)\\ y_{l+1}=-0.98x_l\end{cases} \quad (9)$$

s_1（ｋ）＝x_{20}＋ｊy_{20}　　（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（ｃｈａｏｓ　ｐｈａｓｅ　ｓｈｉｆｔ　ｋｅｙｉｎｇ：ＣＰＳＫ）となる。

【数１６】

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

【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。

【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ｓｈ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_l＝８～１３、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_l＝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ｓｈを越えた場合は判定を行い、次のビットへと進む。ｓｈを越えずにl_{max}に達した場合は、$v_l \rightarrow v_l$＋１として同様に計算を繰り返す。最終的にv_l＝１３、拘束長がl_{max}となってもｓｈ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。

【００５６】

シミュレーションではＥｂ／Ｎ０が２～１０ｄＢ、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_l（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Ｅｂ／Ｎ０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_lも低減していることがわかる。Ｅｂ／Ｎ０の向上にともないv_l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_l＝１相当まで下がるためである。

【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Ｅｂ／Ｎ０＝２ｄＢで無誤り伝送が実現された。v_l，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。

【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連接させて、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［１　５／７］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。

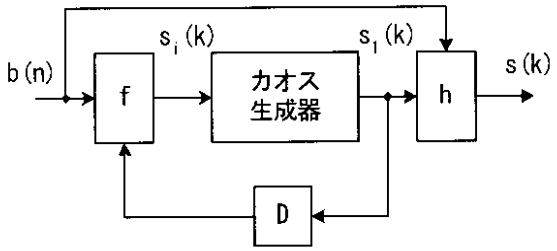
【数１７】

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

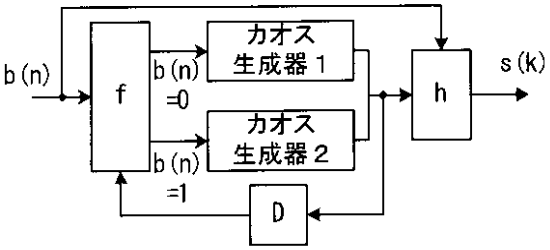
$$p = \left\{k - nr_c + b(n)\right\} \bmod 2$$

【００６０】
復号側は、v_l＝８～１３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Ｅｂ／Ｎ０が２～１０ｄＢ、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_l（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Ｅｂ／Ｎ０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_l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、さまざま伝送形態が実現できると考えられる。
【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】探査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】畳込み符号を連接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】畳込み符号を連接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。

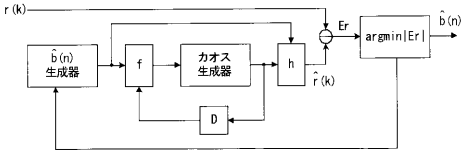
【図１】



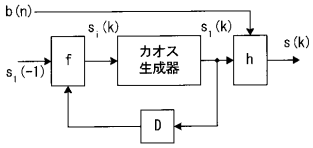
【図２】



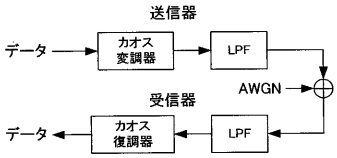
【図３】



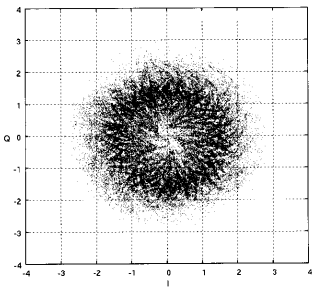
【図８】



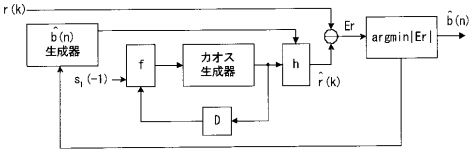
【図９】



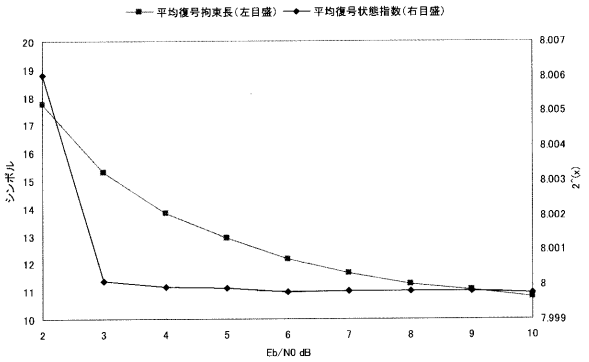
【図１０】



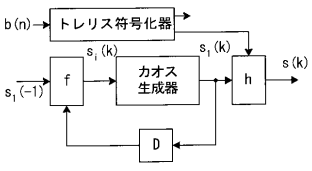
【図１１】



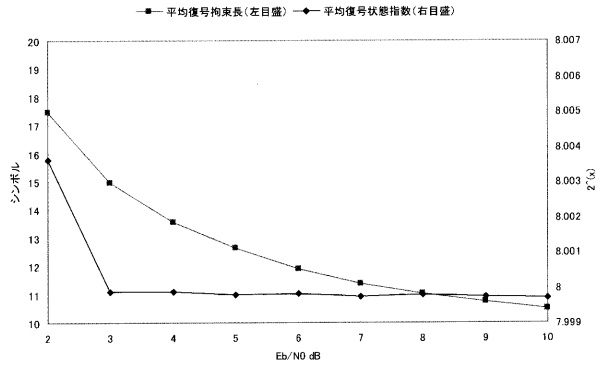
【図１２】



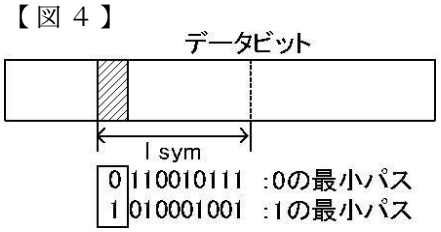
【図１３】



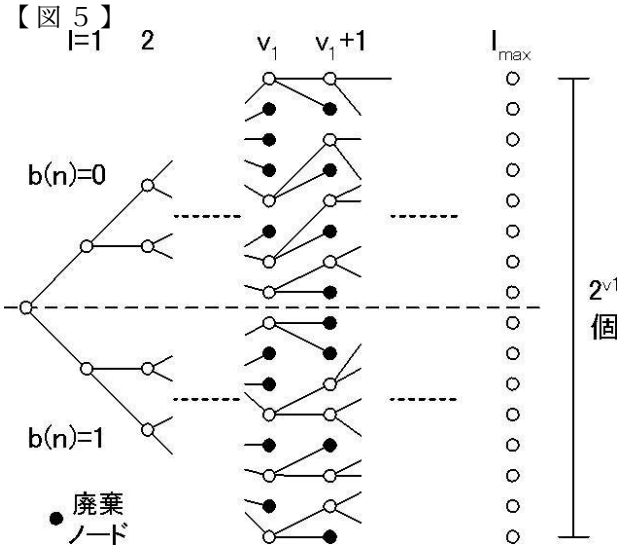
【図１４】


平均復号拘束長（左目盛）
平均復号状態指数（右目盛）
シンボル
Eb/N0 dB

【図４】


データビット
l sym
0 110010111 :0の最小パス
1 010001001 :1の最小パス

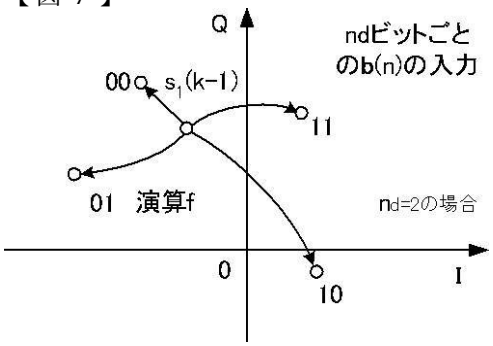
【図５】


l=1 2
v1
v1+1
lmax
b(n)=0
b(n)=1
2v1個
廃棄ノード

【図６】


データビット
テールビット
kd sym
kt sym

【図７】


Q
ndビットごと
のb(n)の入力
00
s1(k-1)
11
01
演算f
nd=2の場合
0
I
10