２００５年度知的財産翻訳検定問題【電気・電子工学】

※解答作成前に必ず下記の注意事項に目を通してください。

【解答にあたっての注意事項】
下に掲載した課題文中の二つの指定箇所（＊＊＊START＊＊＊から＊＊＊END＊＊＊まで）を翻訳しなさい。なお、二つの翻訳の順序は指定箇所の順序通りとするが、それぞれ米国特許明細書に使用することを前提とした翻訳とすること。

＊＊＊START＊＊＊
【特許請求の範囲】
１．入力データに対して冗長性を付加して誤り訂正符号化を行う誤り訂正符号化手段と、該誤り訂正符号化手段の出力データを一定のビット数ごとにあらかじめ指定された規則に従い並べ換えて出力するインターリーブ手段と、該インターリーブ手段の出力データの内容を秘匿するために該インターリーブ手段の出力データを暗号化する暗号化手段とを備えた暗号記録手段と、
　任意の記録媒体より再生される上記暗号記録手段の出力データを入力データとし、該入力データに対する暗号化を解除する復号化手段と、該復号化手段の出力データの上記インターリーブ手段によるデータの並べ換えを元の順序に復元するために、上記復号化手段の出力データを一定のビット数ごとにあらかじめ指定された規則に従い並べ換えて出力するデインターリーブ手段と、該デインターリーブ手段の出力データを入力データとし、上記誤り訂正符号化手段により付加された冗長性をもとに上記入力データ中の誤ったデータを訂正する誤り訂正復号手段とを備えた暗号再生手段とを備えたことを特徴とする暗号通信装置。
２．上記暗号記録手段の各手段及び上記暗号再生手段の各手段は、それぞれ鍵情報発生手段により動作のための情報が与えられることを特徴とする特許請求の範囲第１項記載の暗号通信装置。
＊＊＊END＊＊＊

【産業上の利用分野】
　この発明は、暗号化されたデータを記録再生する暗号通信装置に関するものである。

【従来の技術】
　第４図に示す従来の暗号通信装置について説明する。図において、３は暗号化手段、５は暗号化されたデータの復号化手段である。
　次に動作について説明する。
　暗号化手段３は入力データに対してそのアルゴリズムと鍵によって定まる暗号化を行い、任意の記録媒体に記録する。
　復号化手段５は上記暗号化手段３によって記録されたデータを任意の記録媒体より再生し、再生されたデータに対してそのアルゴリズムと鍵によって定まる復号化を行い、上記暗号化手段３への入力データを復元する。

【発明が解決しようとする問題点】

従来の暗号通信装置は以上のように構成されているので、暗号化されたデータを記録媒体より再生する際のデータの誤りが、復号後のデータに伝搬する。特に強度が高い暗号を使用した場合には、上記復号後のデータの劣化が著しくなるという問題があった。

この発明は上記のような問題点を解消するためになされたもので、強度が高い暗号方式においても、再生時におけるデータの誤りが復号化時の手続きによって伝搬するのを軽減でき、暗号化を施した記録再生系を高品質に保持することの出来る暗号通信装置を得ることを目的とする。

【問題点を解決するための手段】

この発明に係わる暗号通信装置は、暗号記録手段において、誤り訂正符号化、インターリーブを行ったデータに対して暗号化を行い、暗号再生手段において、任意の記録媒体から再生され、復号化されたデータに対し、デインターリーブ及び誤り訂正復号化をかけるようにしたものである。

【作用】

この発明においては、記録再生時の誤りを含んだ暗号化データに対し複合化を行った際に発生する連続的な誤りが、デインターリーブ手段によるデータの並べ換えにより拡散され、このデータが誤り訂正されるので、強度の高い暗号方式においても、再生時におけるデータの誤りが復号化時の手段によって伝搬するのを軽減でき、暗号化を施した記録再生系を高品質に保持することが出来る。

【実施例】

以下、この発明の実施例を図について説明する。

第１図（ａ）及び（ｂ）はこの発明の一実施例による暗号通信装置を示し、（ａ）は暗号記録手段、（ｂ）は暗号再生手段を示す。図において、１は入力データに対し誤り訂正復号手段による誤り訂正を行う目的で冗長性を付加する誤り訂正符号化手段、２は誤り訂正符号化手段１の出力データを一定のビット数ごとにあらかじめ指定された規則に従い並べ換えて出力するインターリーブ手段、３はインターリーブ手段２の出力データを暗号化する暗号化手段であり、これらの手段１，２，３により暗号記録手段を構成している。５は任意の記録媒体より再生された上記暗号記録手段の出力データを入力データとし、該入力データに対する上記暗号化手段３による暗号化を解除する復号化手段、６は上記インターリーブ手段２によるデータの並べ換えを元の順序に復元する目的で上記復号化手段５の出力データを一定のビット数ごとにあらかじめ指定された規則に従い並べ換えて出力するデインターリーブ手段、７はデインターリーブ手段６の出力データを入力データとし、上記誤り訂正符号化手段１により付加された冗長性をもとに、該入力データ中の上記任意の記録媒体よりデータ再生する際に発生した誤ったデータを訂正する誤り訂正復号手段であり、これらの手段５，６，７により暗号再生手段を構成している。

次に動作について説明する。

まず、暗号記録手段においては、入力データは、誤り訂正符号化手段１により誤り訂正符号化が掛けられ、次にインターリーブ手段２により一定のビット数ごとにあらかじめ指定された規則に従い並べ換えられる。そしてその出力データは暗号化手段３により暗号化される。

＊＊＊START＊＊＊

暗号再生手段においては、上記暗号記録手段からの出力データが復号化手段５により復号される。そ

して該復号化手段５の出力データ中の上記任意の記録媒体において起こったデータの誤りによる連続的な誤りは、デインターリーブ手段６により擬似的なランダム誤りに変換される。第３図（ａ），（ｂ），（ｃ）はこの様子を示したものである。ここで仮に、暗号化手段３及び復号化手段５がブロック暗号であるとすると、復号化手段５の入力データに、記録媒体より再生される過程で誤りが発生した場合、第３図（ａ）の１３におけるＢｉブロックに示すように、入力中に誤りの発生したブロックは連続的に誤りが発生する。デインターリーブ手段６を、第３図（ｂ）の１４に示す行列によるメモリ構成において、書き込み側は行中の列方向に順次書き込みを行い順次行を進め、読み出し側は列中の行方向に読み出しを行い順次列を進めていく方式のものとすると、上記誤りの発生したブロックＢｉはデインターリーブ手段６のメモリ中の第ｉ行に書き込まれ、読み出し側では上記誤りの発生したブロックＢｉのデータは各列の各々ｉ番目のビットに分散して現われる。（第３図（ｃ）におけるＰｊ１５中のＰｊ,ｉ１６）。このように、復号化手段５の出力データ中の連続的な誤りの存在するブロックは、デインターリーブ手段６により分散され、デインターリーブ手段６の出力では誤ったデータはランダム誤りに近い状態となることとなる。

＊＊＊END＊＊＊

そして、デインターリーブ手段６の出力データは誤り訂正復号手段７により誤り訂正復号化が施される。こうして、暗号再生手段は暗号記録手段の入力データを復元する。

このように本実施例では、復号化時のデータの連続的な誤りをデインターリーブ手段により擬似的なランダム誤りに変換して、これを誤り訂正するようにしたので、強度の高い暗号方式においても、再生時におけるデータの誤りが復号化時の手続きのよって伝搬するのを軽減でき、暗号化を施した記録再生系を高品質に保持することができる。

なお、上記実施例では、入力データの暗号化の情報は暗号化手段３及び復号化手段５のアルゴリズム及び鍵のみとしたが、誤り訂正符号化手段１，誤り訂正復号手段７及びインターリーブ手段２，デインターリーブ手段６の情報も秘匿のために利用できる。

第２図はこの発明の他の実施例による暗号通信装置を示す。本実施例は、暗号記録手段において、本暗号記録手段の鍵情報を発生するための鍵情報発生手段１１ａにより、誤り訂正符号化手段１，インターリーブ手段２及び暗号化手段３の動作のための情報を発生させ、暗号再生手段において、鍵情報発生手段１１ｂの情報をもとに、復号化手段５，デインターリーブ手段６及び誤り訂正復号手段７の動作の情報を発生させるようにしたものである。

このような本実施例においても、上記実施例と同様に、復号化時のデータの誤りの伝搬を軽減でき、記録再生系を高品質に保持することができる。

【発明の効果】

以上のように、この発明の暗号通信装置によれば、暗号化されたデータに誤りが発生した時の復号後データの連続的な誤りをデインターリーブ手段によりランダム化し、そして誤り訂正を行うようにしたので、強度の高い暗号方式においても、再生時におけるデータの誤りが復号化時の手続きによって伝搬するのを軽減でき、暗号を施した記録再生系を高品質に保持することができる効果がある。

【図面の簡単な説明】

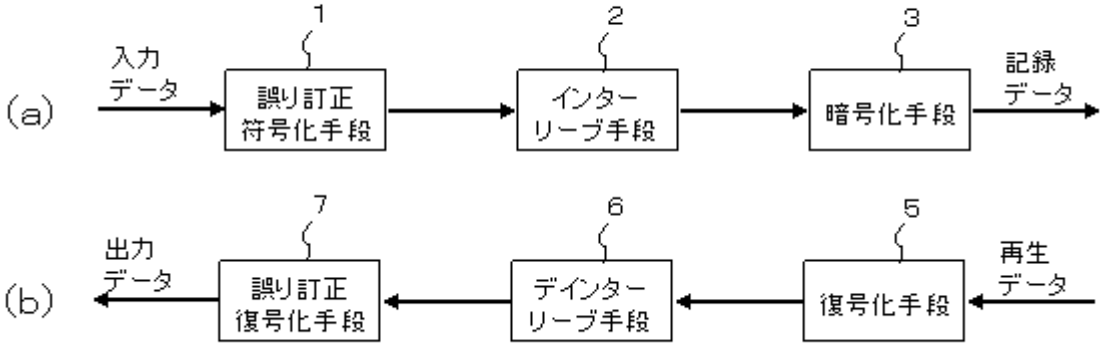
第１図（ａ）、（ｂ）はこの発明の一実施例による暗号通信装置を示すブロック図、第２（ａ）、（ｂ）はこの発明の他の実施例による暗号通信装置を示すブロック図、第３図（ａ）、（ｂ），（ｃ）は本発明に

おけるデインターリーブ手段の動作の説明図、第４図は従来の暗号通信装置を示すブロック図である。

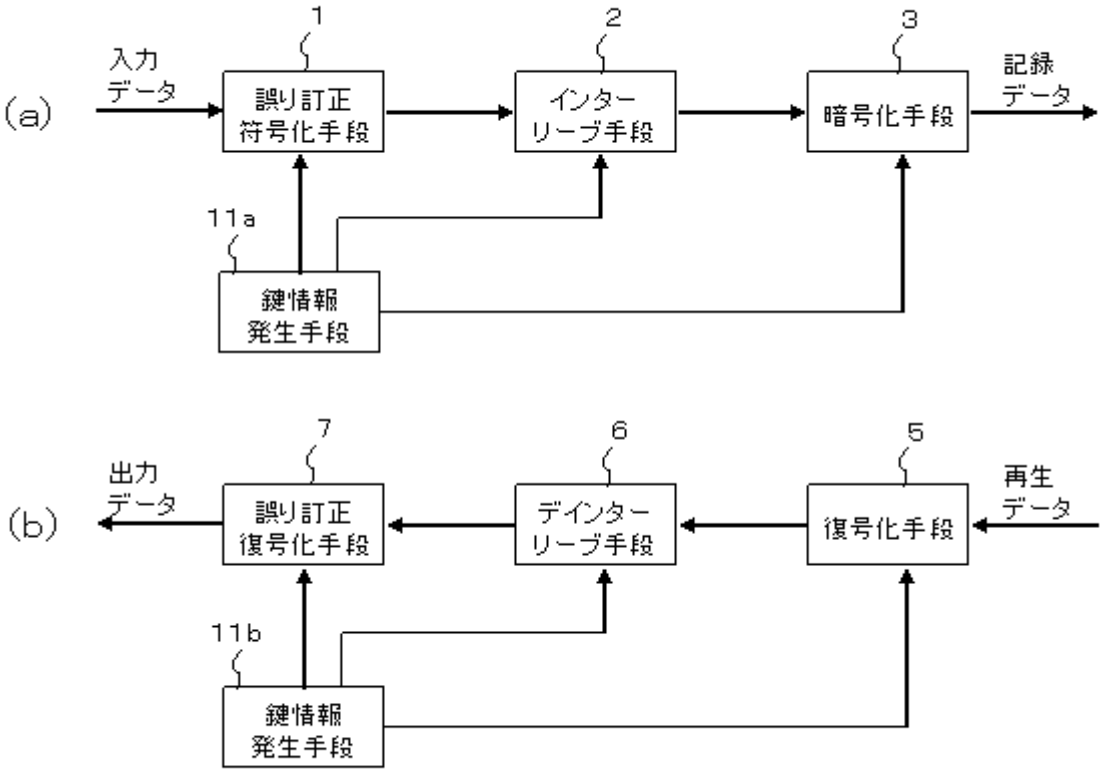
図において、１は誤り訂正符号化手段、２はインターリーブ手段、３は暗号化手段、５は復号化手段、６はデインターリーブ手段、７は誤り訂正復号手段、１１ａ、１１ｂは鍵情報発生手段、１３は復号化手段５の出力データ、１４はデインターリーブ手段６の行列、１５はデインターリーブ手段６の出力データである。

なお図中同一符号は同一または相当部分を示す。

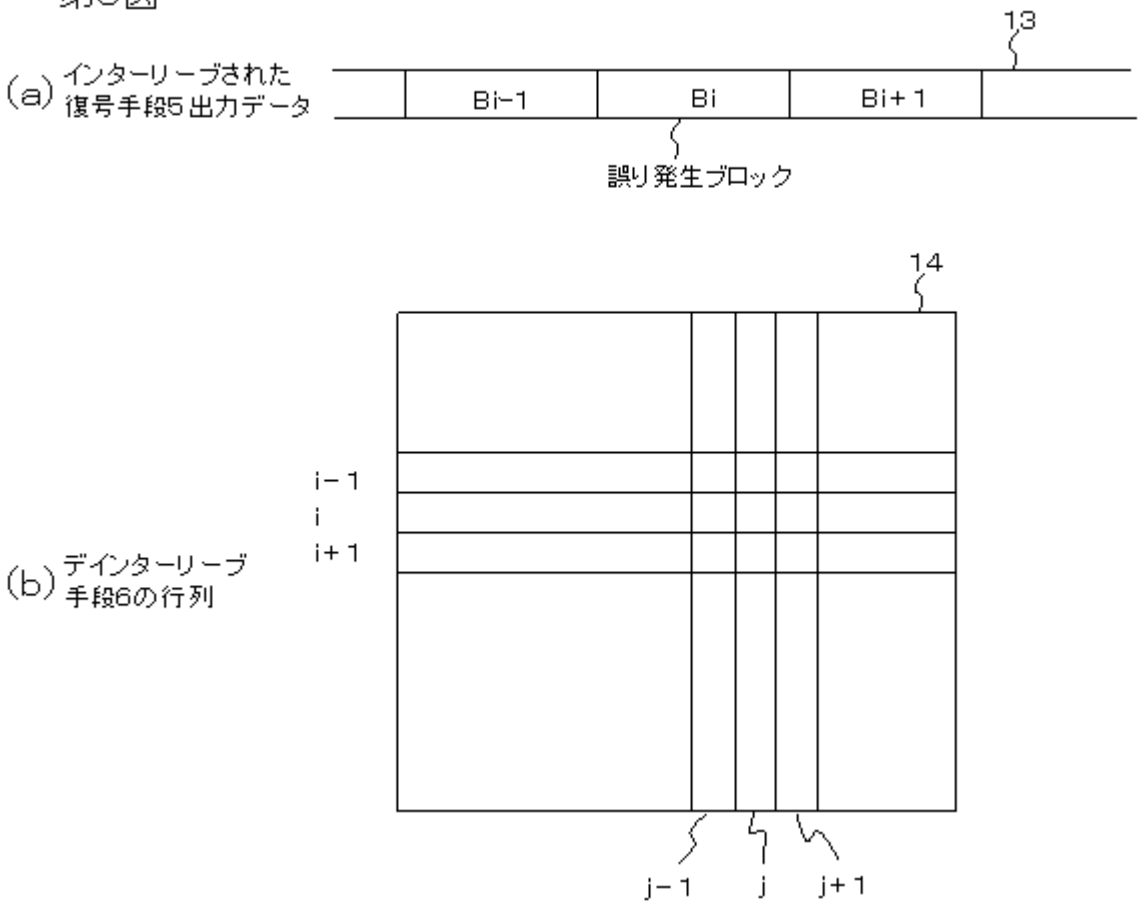
第1図



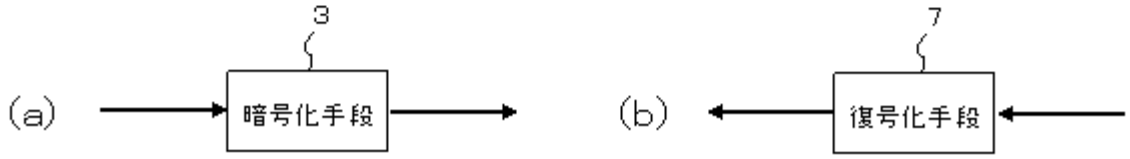
第2図



第3図


(a) インターリーブされた
復号手段5出力データ
13
Bi-1
Bi
Bi+1
誤り発生ブロック
14
i-1
i
i+1
(b) デインターリーブ
手段6の行列
j-1
j
j+1
15
(c) デインターリーブ
手段6出力データ
Pj-1
Pj
Pj+1
16
Pj, i-1
Pj, i
Pj, i+1
誤り発生データ

第4図


(a)
3
暗号化手段
(b)
7
復号化手段