

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(10) 国際公開番号

WO 2009/144802 A1

PCT

(43) 国際公開日
2009年12月3日(03.12.2009)

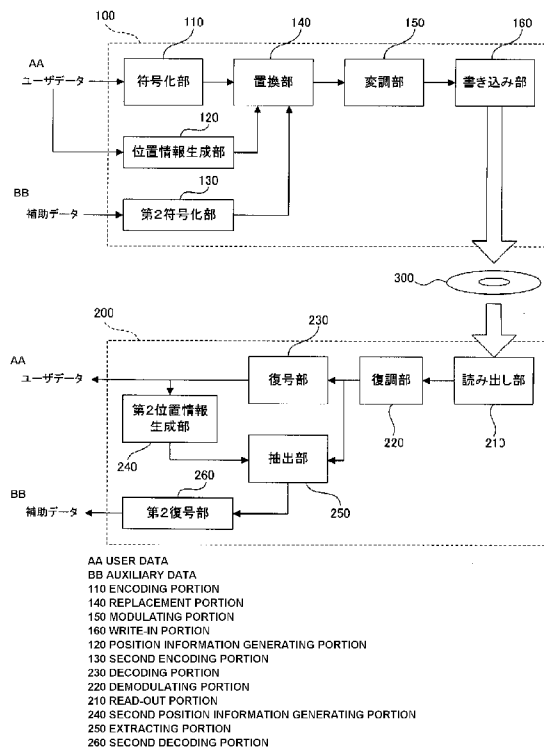
- (51) 国際特許分類:
G11B 20/18 (2006.01) G09C 5/00 (2006.01)
G06F 12/14 (2006.01) G11B 20/10 (2006.01)
- (21) 国際出願番号: PCT/JP2008/059930
- (22) 国際出願日: 2008年5月29日(29.05.2008)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人(米国を除く全ての指定国について): パイオニア株式会社(PIONEER CORPORATION) [JP/JP]; 〒1538654 東京都目黒区目黒1丁目4番1号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 吉田 和幸(YOSHIDA, Kazuyuki) [JP/JP]; 〒3502288 埼玉県鶴ヶ島市富士見6丁目1番2号 パイオニア株式会社 総合研究所内 Saitama (JP).
- (74) 代理人: 江上 達夫, 外(EGAMI, Tatsuo et al.); 〒1040031 東京都中央区京橋一丁目16番10号 オークビル京橋3階 東京セントラル特許事務所内 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB,

[続葉有]

(54) Title: INFORMATION GENERATING EQUIPMENT AND METHOD, INFORMATION REPRODUCTION EQUIPMENT AND METHOD, AND RECORDING MEDIUM

(54) 発明の名称: 情報生成装置及び方法、情報再生装置及び方法、並びに記録媒体

[図1]



(57) Abstract: Information generating equipment (100) replaces part of user data with auxiliary data to generate replaced user data. The information generating equipment comprises an encoding means (110) which adds an error correction code to the user data and generates encoded data, a position information generating means (120) which generates position information that indicates the position of the data in the encoded data to be replaced with the auxiliary data based on the user data, and replacement means (140) which generates the replaced user data by replacing part of the encoded data with the auxiliary data based on the position information. Due to this structure, information which can surely reproduce the auxiliary data can be generated while avoiding various practical inconveniences.

(57) 要約: 情報生成装置(100)は、ユーザデータの一部を、補助データに置換して、置換ユーザデータを生成する。情報生成装置は、ユーザデータに対して誤り訂正符号を付加して、符号化データを生成する符号化手段(110)と、符号化データにおける補助データに置換されるデータの位置を示す位置情報を、ユーザデータに基づいて生成する位置情報生成手段(120)と、符号化データの一部を、位置情報に基づいて補助データに置換して、置換ユーザデータを生成する置換手段(140)とを備える。これにより、実践上の様々な不都合を回避しつつ、補助データを確実に再生可能な情報を生成することができる。



GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, 添付公開書類:

PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, — 国際調査報告 (条約第 21 条(3))
CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

明 細 書

情報生成装置及び方法、情報再生装置及び方法、並びに記録媒体 技術分野

[0001] 本発明は、誤り訂正符号を用いた情報生成装置及び方法、情報再生装置及び方法、並びに記録媒体の技術分野に関する。

背景技術

[0002] この種の情報生成装置として、ユーザデータに関連する補助データを、誤り訂正符号を付加したユーザデータに対して意図的な誤りとして埋め込むものがある。例えば特許文献1では、ユーザデータが不正に複製されたものであるか否かを識別する識別データを意図的な誤りとして埋め込み、誤りの位置を示す情報を暗号化して別途記録するという技術が開示されている。また特許文献2では、誤りを埋め込んだ位置を、誤り訂正前後のデータを互いに比較することで検出するという技術が開示されている。

[0003] 特許文献1:特開平8-212681号公報

特許文献2:特許第3449804号公報

発明の開示

発明が解決しようとする課題

[0004] しかしながら、上述した特許文献1に係る技術では、誤りの位置を示す情報を別途記録することが求められるため、その分ユーザデータを記録できる領域が減少してしまう。また、誤りの位置を示す情報に誤りが生じてしまった場合には、誤りの位置を検出することができなくなってしまうおそれがある。

[0005] また、上述した特許文献2に係る技術では、誤り訂正前後のデータを互いに比較することがもとめられるため、誤りの位置を検出しようとする際の処理量が比較的多くなってしまうおそれがある。

[0006] 以上のように、上述した技術には、実践上の様々な不都合が生じてしまうおそれがあるという技術的問題点がある。

[0007] 本発明は、例えば上述した問題点に鑑みなされたものであり、データ量の増大を防

止しつつ、補助データを確実に再生可能な情報を生成することができる情報生成装置及び方法、情報再生装置及び方法、並びに記録媒体を提供することを課題とする。

課題を解決するための手段

[0008] 本発明の第1の情報生成装置は上記課題を解決するために、ユーザデータの一部を、前記ユーザデータに関連するデータであって、前記ユーザデータとは異なる用途で用いられる補助データに置換して、置換ユーザデータを生成する情報生成装置であって、前記ユーザデータに対して誤り訂正符号を付加して、符号化データを生成する符号化手段と、前記符号化データにおける前記補助データに置換されるデータの位置を示す位置情報を、前記ユーザデータに基づいて生成する位置情報生成手段と、前記符号化データの一部を、前記位置情報に基づいて前記補助データに置換して、前記置換ユーザデータを生成する置換手段とを備える。

[0009] 本発明の第1の情報生成装置によれば、ユーザデータの一部が、補助データに置換されることで、置換ユーザデータが生成される。尚、「ユーザデータ」とは、生成される置換ユーザデータの元となるデータであり、例として電子ファイル、音声データ、画像データ等が挙げられる。また、「補助データ」とは、ユーザデータに関連する補助的なデータであり、ユーザデータとは異なる用途で用いられる。補助データの例として、ユーザデータの属性、ファイル名前及び管理番号等を示すデータや、分割されたユーザデータの分割位置を示すデータ、ユーザデータが不正にコピーされたデータであるか否かを識別するためのデータ等が挙げられる。補助データは、典型的には、ユーザデータと比べると極めて情報量の少ないデータである。

[0010] 生成された置換ユーザデータは、例えば所定の方式で変調された後、ホログラフィックメモリや光ディスク等の記録媒体に記録されたり、インターネット等のネットワークを用いて伝送される。

[0011] 本発明の第1の情報生成装置の動作時には、先ず符号化手段によって、ユーザデータに誤り訂正符号が付加され、符号化データが生成される。続いて、位置情報生成手段によって、符号化データにおける補助データに置換されるデータの位置を示す位置情報が生成される。

- [0012] ここで特に、位置情報は、ユーザデータに基づいて生成される。即ち、位置情報は、ユーザデータを用いた所定の処理により生成される。位置情報は、例えばハッシュ関数により生成されるハッシュ値のように、ユーザデータから一意的に求められる情報であれば、直接的にデータの位置を示すような情報でなくともよい。このような場合は、例えば位置情報が有する値と、置換するデータの位置とを対応させるような法則を予め設定しておくことで、置換されるデータの位置が示される。
- [0013] 位置情報が生成されると、置換手段により、符号化データの一部が位置情報に基づいて補助データに置換され、置換ユーザデータが生成される。補助データは、符号化後に置換されるため、ユーザデータに意図的な誤りとして埋め込まれることとなる。
- [0014] 上述したように生成された置換ユーザデータは、ユーザデータとして再生される際に、誤り訂正符号により誤りを訂正することで復号される。この際、置換された補助データは、ユーザデータにおける誤りとして扱われてしまうため、復号後のユーザデータには残らない。しかしながら、ユーザデータを復号することができれば、ユーザデータから再び位置情報を生成することができる。よって、位置情報に基づいて、容易且つ確実に復号前の置換ユーザデータから補助データを抽出することが可能となる。
- [0015] 本発明では特に、補助データがユーザデータの一部として置換されているため、補助データを別のデータとして扱う場合と比較して、データ全体の大きさを小さくすることができる。また、位置情報についても、ユーザデータから生成できるので、保持しておかなくともよい。よって、データ量の増大を効果的に防止することが可能である。
- [0016] 本発明では更に、上述したように、位置情報を保持しておかなくともよいため、位置情報に誤りが発生することに起因して、補助データを再生できなくなってしまうことを防止できる。即ち、ユーザデータさえ再生できるような状態にあれば、補助データも確実に再生することが可能である。
- [0017] また、単にユーザデータにおける誤りを補助データとして抽出しようとすると、例えば記録媒体における傷や通信時のノイズ等によって発生したノイズとの判別が行えない。このため、置換ユーザデータに誤りが多く発生してしまうような場合には、補助データを抽出することは困難となってしまう。このような場合であっても、本発明に係る置換

ユーザデータによれば、ユーザデータから位置情報を生成することができるため、確実に補助データのみを抽出することが可能である。

[0018] 以上説明したように、本発明の第1の情報生成装置によれば、実践上の様々な不都合を回避しつつ、補助データを確実に再生可能な情報を生成することができる。

[0019] 本発明の第1の情報生成装置の一態様では、前記符号化データは、所定数の連続するデータ毎にブロックとして分割されており、前記置換手段は、前記ブロック毎に、前記符号化データを1つの補助データと置換する。

[0020] この態様によれば、符号化データは、所定数の連続するデータ毎にブロックとして分割されている。尚、ここでの「分割」は、符号化データが複数のデータとして扱われることを意味するものではなく、データ中に区切りが存在しているという意味である。

[0021] 本態様では特に、補助データは、ブロック毎に符号化データの1つと置換される。即ち、符号化データにおける各ブロックにおいて、ブロックを構成するデータのうち、1つのデータが補助データに置換される。これにより、補助データは、置換ユーザデータ内に好適に分散される。よって、補助データの殆ど或いは全てに誤りが発生してしまい、補助データが再生できなくなってしまうことを効果的に防止することができる。

[0022] 尚、補助データが比較的情報量の多いデータである場合には、補助データを、ブロック毎に所定数(即ち、2以上)の符号化データと置換することによっても、上述した効果は相応に得られる。即ち、ブロック毎に2つの補助データを2つの符号化データと置換したり、3つの補助データを3つの符号化データと置換したりしてもよい。

[0023] 本発明の第1の情報生成装置の他の態様では、前記補助データに対して誤り訂正符号を付加する補助符号化手段を更に備え、前記置換手段は、前記符号化データの一部を前記誤り訂正符号が付加された補助データに置換して、置換ユーザデータを生成する。

[0024] この態様によれば、補助符号化手段によって、補助データに対しても誤り訂正符号が付加されている。即ち、補助データも、ユーザデータ同様に符号化されている。尚、ユーザデータ及び補助データの符号化方式は、互いに同じであってもよいし、異なってもよい。

[0025] 補助データが符号化されていることにより、補助データに誤りが生じた場合であって

も、誤り訂正符号によって正しいデータへと復号できる。よって本態様では、補助データをより確実に再生することが可能である。

[0026] 本発明の第1の情報生成装置の他の態様では、前記補助データによって、前記ユーザデータを暗号化することで暗号化されたユーザデータを生成する暗号化手段を更に備え、前記符号化手段は、前記暗号化されたユーザデータに対して誤り訂正符号を付加して、符号化データを生成し、前記位置情報生成手段は、前記位置情報を、前記暗号化されたユーザデータに基づいて生成する。

[0027] この態様によれば、ユーザデータは、符号化手段によって符号化される前に、暗号化手段によって暗号化される。また、ユーザデータの暗号化には補助データが用いられる。即ち、補助データはユーザデータの暗号化を解除する鍵情報と考えることもできる。但し、補助データは、ユーザデータを暗号化するためのデータ以外のデータを含んでいてもよい。

[0028] 補助データは、上述したように、置換ユーザデータの一部と置換されるため、データの増大には繋がらない。また、ユーザデータから生成される位置情報により、確実に抽出できる。従って、より好適にユーザデータを暗号化できる。

[0029] 本態様では、ユーザデータが暗号化されているため、ユーザデータに対するセキュリティを向上させることができる。また、位置情報についても、鍵情報がないと正しく生成することができないため、同様にセキュリティを向上させることができる。

[0030] 本発明の第1の情報生成装置の他の態様では、前記位置情報生成手段は、前記位置情報を、前記ユーザデータに加えて鍵情報に基づいて生成する。

[0031] この態様によれば、位置情報手段は、ユーザデータに加えて鍵情報に基づいて生成される。例えば、位置情報はユーザデータに基づいて仮の位置情報として生成された後、鍵情報に基づいて暗号化されることで生成される。或いは、鍵情報によって暗号化されたユーザデータに基づいて生成されてもよい。また、HMAC (Keyed-Hashing for Message Authentication Code)を用いて、ユーザデータ及び鍵情報から直接的に生成することも可能である。

[0032] 本態様では、位置情報を暗号化された状態で生成するため、位置情報を正しく生成するには鍵情報が求められる。即ち、鍵情報がない場合に、位置情報を正しく

生成することができないようにすることができるため、位置情報に対するセキュリティを向上させることができる。よって、位置情報を用いることで抽出される補助データに対するセキュリティを効果的に高めることが可能である。

[0033] 本発明の第1の情報生成装置の他の態様では、前記位置情報を用いて、前記補助データを変更する補助データ変更手段を更に備える。

[0034] この態様によれば、補助データは、符号化データと置換される前に位置情報を用いて変更される。尚、ここでの「変更」とは、可逆的な変更であり、変更された補助データは、再び位置情報を用いて元の補助データに戻すことが可能である。即ち、ここでの変更は、位置情報を鍵情報とした、補助データの暗号化とも呼ぶことができる。

[0035] 位置情報を用いて補助データを変更することで、補助データに対するセキュリティを向上させることができる。また、位置情報は、ユーザデータに基づいて生成することができるため、ユーザデータと別に保持されなくともよい。従って、情報量が不必要に増大してしまうことを防止できる。

[0036] 本発明の第2の情報生成装置は上記課題を解決するために、ユーザデータの一部を、前記ユーザデータに関連するデータであって、前記ユーザデータとは異なる用途で用いられる補助データに置換して、置換ユーザデータを生成する情報生成装置であって、前記ユーザデータに対して誤り訂正符号を付加して、符号化データを生成する符号化手段と、前記補助データを変更補助データに変更するための変更情報を、前記ユーザデータに基づいて生成する変更情報生成手段と、前記変更情報を用いて、前記補助データを変更補助データに変更する補助データ変更手段と、前記符号化データの一部を、前記変更補助データに置換して、前記置換ユーザデータを生成する置換手段とを備える。

[0037] 本発明の第2の情報生成装置によれば、ユーザデータの一部が、補助データに置換されることで、置換ユーザデータが生成される。尚、「ユーザデータ」とは、生成される置換ユーザデータの元となるデータであり、例として電子ファイル、音声データ、画像データ等が挙げられる。また、「補助データ」とは、ユーザデータに関連する補助的なデータであり、ユーザデータとは異なる用途で用いられる。補助データの例として、ユーザデータの属性、ファイル名前及び管理番号等を示すデータや、分割されたユ

ーザデータの分割位置を示すデータ、ユーザデータが不正にコピーされたデータであるか否かを識別するためのデータ等が挙げられる。補助データは、典型的には、ユーザデータと比べると極めて情報量の少ないデータである。

[0038] 生成された置換ユーザデータは、例えば所定の方式で変調された後、ホログラフィックメモリや光ディスク等の記録媒体に記録されたり、インターネット等のネットワークを用いて伝送される。

[0039] 本発明の第2の情報生成装置の動作時には、先ず符号化手段によって、ユーザデータに誤り訂正符号が付加され、符号化データが生成される。続いて、変更情報生成手段によって、補助データを変更補助データに変更するための変更情報が生成される。尚、ここでの「変更」とは、可逆的な変更であり、変更された補助データは、再び変更情報を用いて元の補助データに戻すことが可能である。

[0040] ここで特に、変更情報は、ユーザデータに基づいて生成される。即ち、変更情報は、ユーザデータを用いた所定の処理により生成される。変更情報は、例えばハッシュ関数により生成されるハッシュ値のように、ユーザデータから一意的に求められる情報であればよい。変更補助データは、例えば変更情報を鍵情報として、補助データが暗号化されることにより生成される。即ち、変更情報を用いて補助データを変更することで、補助データに対するセキュリティを向上させることができる。

[0041] 変更補助データが生成されると、置換手段により、符号化データの一部が変更補助データに置換され、置換ユーザデータが生成される。変更補助データは、符号化後に置換されるため、ユーザデータに意図的な誤りとして埋め込まれることとなる。

[0042] 上述したように生成された置換ユーザデータは、ユーザデータとして再生される際に、誤り訂正符号により誤りを訂正することで復号される。この際、置換された変更補助データは、ユーザデータにおける誤りとして扱われてしまうため、復号後のユーザデータには残らない。しかしながら、例えば置換された変更補助データの位置を示す位置情報を別途記憶しておく、或いは置換する変更補助データの位置を予め設定しておくことで、変更補助データを好適に抽出することが可能である。また、誤り訂正前後のユーザデータ、即ち置換ユーザデータと復号後のユーザデータとを比較することで変更補助データを抽出することができる。

- [0043] 抽出された変更補助データは、変更情報に基づいて元の補助データに再変更することができる。変更情報は、ユーザデータから生成できるので、保持しておかなくともよい。変更情報に誤りが発生することに起因して、補助データを元に戻すことができなくなってしまうことを防止できる。即ち、ユーザデータさえ再生できるような状態であれば、補助データも確実に再生することが可能である。
- [0044] また、変更情報を保持しておかなくともよい分、データ量の増大を防止することが可能である。また、補助データについても、ユーザデータの一部として置換されているため、補助データを別のデータとして扱う場合と比較して、データ全体の大きさを小さくすることができる。
- [0045] 以上説明したように、本発明の第2の情報生成装置によれば、高いセキュリティを実現しつつ、補助データを確実に再生可能な情報を生成することができる。
- [0046] 本発明の第1の記録媒体は上記課題を解決するために、上述した本発明の第1の情報生成装置によって生成された置換ユーザデータが記録されている。
- [0047] 本発明の第1の記録媒体によれば、上述した本発明の第1の情報生成装置によって生成された置換ユーザデータが記録されているため、記録されたデータを再生する際に、確実に誤り位置を検出して、ユーザデータ中の補助データを抽出することができる。また、補助データや位置情報をユーザデータとは別に記録しなくともよいため、ユーザデータを記録する領域を十分に確保することが可能である。
- [0048] 本発明の第2の記録媒体は上記課題を解決するために、上述した本発明の第2の情報生成装置によって生成された置換ユーザデータが記録されている。
- [0049] 本発明の第2の記録媒体によれば、上述した本発明の第2の情報生成装置によって生成された置換ユーザデータが記録されているため、記録されたデータを再生する際に、高いセキュリティを実現しつつ、ユーザデータ中の補助データを確実に抽出することができる。また、補助データや位置情報をユーザデータとは別に記録しなくともよいため、ユーザデータを記録する領域を十分に確保することが可能である。
- [0050] 本発明の第1の情報再生装置は上記課題を解決するために、上述した本発明の第1の情報生成装置によって生成された置換ユーザデータを再生する情報再生装置であって、前記置換ユーザデータを、前記誤り訂正符号を用いて、前記ユーザデー

タに復号する復号手段と、前記位置情報を、前記復号されたユーザデータに基づいて生成する第2位置情報生成手段と、前記第2位置情報生成手段によって生成された前記位置情報に基づいて、前記置換ユーザデータから前記補助データを抽出する抽出手段とを備える。

[0051] 本発明の第1の情報再生装置によれば、上述した本発明の第1の情報生成装置によって生成された置換ユーザデータが再生される。置換ユーザデータは、先ず復号手段において、誤り訂正符号を用いて復号される。これにより、意図的に埋め込まれた誤りである補助データは、置換前のユーザデータに戻される。また、記録の際などに発生した誤りに関しても、同様に訂正される。

[0052] ユーザデータが復号されると、第2位置情報生成手段によって、復号されたユーザデータから位置情報が生成される。尚、第2位置情報生成手段は、上述した本発明の第1の情報生成装置における位置情報生成手段と同様に位置情報を生成する。言い換えれば、情報生成装置における位置情報生成手段と、情報再生手段における第2位置情報生成手段は、同一のものであってもよい。

[0053] 位置情報が生成されると、抽出手段によって、置換ユーザデータから補助データが抽出される。即ち、本発明では、ユーザデータが再生できるような状態であれば、確実に補助データも再生することができる。尚、置換ユーザデータは、復号手段によって復号されるユーザデータとは別に、例えばメモリ等に記憶されており、抽出手段は記憶された置換ユーザデータから補助データを抽出する。

[0054] 以上説明したように、本発明の第1の情報再生装置によれば、置換ユーザデータからユーザデータ及び補助データを確実に再生することができる。

[0055] 本発明の第2の情報再生装置は上記課題を解決するために、上述した本発明の第2の情報生成装置によって生成された置換ユーザデータを再生する情報再生装置であって、前記置換ユーザデータから、前記変更補助データを抽出する抽出手段と、前記置換ユーザデータを、前記誤り訂正符号を用いて、前記ユーザデータに復号する復号手段と、前記変更情報を、前記復号されたユーザデータに基づいて生成する第2変更情報生成手段と、前記第2変更情報生成手段によって生成された前記変更情報に基づいて、前記変更補助データを前記補助データに再変更する再変更手

段とを備える。

- [0056] 本発明の第2の情報再生装置によれば、上述した本発明の第2の情報生成装置によって生成された置換ユーザデータが再生される。置換ユーザデータは、先ず復号手段において、誤り訂正符号を用いて復号される。これにより、意図的に埋め込まれた誤りである変更補助データは、置換前のユーザデータに戻される。
- [0057] ユーザデータが復号されると、抽出手段は、例えば置換されたユーザデータの位置を示す位置情報等を用いて変更補助データを抽出する。位置情報は、ユーザデータとは別に記憶されている情報であってもよいし、ユーザデータを置換する前に予め設定されたものであってもよい。
- [0058] また、復号前の置換ユーザデータと復号後のユーザデータとを互いに比較することで、変更補助データを抽出することもできる。即ち、復号によって、意図的な誤りである変更補助データが訂正されるということを利用して、変更補助データを抽出することができる。尚、置換ユーザデータは、復号手段によって復号されるユーザデータとは別に、例えばメモリ等に記憶されており、抽出手段は記憶された置換ユーザデータと復号されたユーザデータを互いに比較する。
- [0059] また、復号されたユーザデータからは、第2変更情報生成手段によって、変更補助データを補助データに再変更するための変更情報が生成される。尚、第2変更情報生成手段は、上述した本発明の第2の情報生成装置における変更情報生成手段と同様に変更情報を生成する。言い換えれば、情報生成装置における変更情報生成手段と、情報再生手段における第2変更情報生成手段は、同一のものであってもよい。
- [0060] 変更情報が生成されると、再変更手段によって、変更補助データは補助データに再変更される。即ち、本発明では、ユーザデータが再生できるような状態であれば、確実に補助データも再生することができる。変更補助データは、例えば補助データを変更補助データへと変更する際とは逆の演算処理等が行われることによって補助データへと再変更される。
- [0061] 以上説明したように、本発明の第2の情報再生装置によれば、置換ユーザデータからユーザデータ及び補助データを確実に再生することができる。

- [0062] 本発明の第1の情報生成方法は上記課題を解決するために、ユーザデータの一部を、前記ユーザデータに関連するデータであって、前記ユーザデータとは異なる用途で用いられる補助データに置換して、置換ユーザデータを生成する情報生成方法であって、前記ユーザデータに対して誤り訂正符号を付加して、符号化データを生成する符号化工程と、前記符号化データにおける前記補助データに置換されるデータの位置を示す位置情報を、前記ユーザデータに基づいて生成する位置情報生成工程と、前記符号化データの一部を、前記位置情報に基づいて前記補助データに置換して、前記置換ユーザデータを生成する置換工程とを備える。
- [0063] 本発明の第1の情報生成方法によれば、補助データが符号化データの一部と置換され、置換されたデータの位置を示す位置情報がユーザデータに基づいて生成されるので、上述した第1の情報生成装置と同様に、実践上の様々な不都合を回避しつつ、補助データを確実に再生可能な情報を生成することができる。
- [0064] 尚、本発明の第1の情報生成方法においても、上述した第1の情報生成装置と同様の各種態様をとることが可能である。
- [0065] 本発明の第2の情報生成方法は上記課題を解決するために、ユーザデータの一部を、前記ユーザデータに関連するデータであって、前記ユーザデータとは異なる用途で用いられる補助データに置換して、置換ユーザデータを生成する情報生成方法であって、前記ユーザデータに対して誤り訂正符号を付加して、符号化データを生成する符号化工程と、前記補助データを変更補助データに変更するための変更情報を、前記ユーザデータに基づいて生成する変更情報生成工程と、前記変更情報を用いて、前記補助データを変更補助データに変更する補助データ変更工程と、前記符号化データの一部を、前記変更補助データに置換して、前記置換ユーザデータを生成する置換工程とを備える。
- [0066] 本発明の第2の情報生成方法によれば、補助データが、ユーザデータに基づいて生成される変更情報に基づいて変更補助データへと変換されるため、上述した第2の情報生成装置と同様に、高いセキュリティを実現しつつ、補助データを確実に再生可能な情報を生成することができる。
- [0067] 本発明の第1の情報再生方法は上記課題を解決するために、上述した本発明の第

1の情報生成方法によって生成された置換ユーザデータを再生する情報再生方法であって、前記置換ユーザデータを、前記誤り訂正符号を用いて、前記ユーザデータに復号する復号工程と、前記位置情報を、前記復号されたユーザデータに基づいて生成する第2位置情報生成工程と、前記第2位置情報生成工程において生成された前記位置情報に基づいて、前記置換ユーザデータから前記補助データを抽出する抽出工程とを備える。

[0068] 本発明の第1の情報再生方法によれば、ユーザデータに基づいて位置情報が生成されるため、上述した第1の情報再生装置と同様に、置換ユーザデータからユーザデータ及び補助データを確実に再生できる。

[0069] 本発明の第2の情報再生方法は上記課題を解決するために、上述した本発明の第2の情報生成方法によって生成された置換ユーザデータを再生する情報再生方法であって、前記置換ユーザデータから、前記変更補助データを抽出する抽出工程と、前記置換ユーザデータを、前記誤り訂正符号を用いて、前記ユーザデータに復号する復号工程と、前記変更情報を、前記復号されたユーザデータに基づいて生成する第2変更情報生成工程と、前記第2変更情報生成工程において生成された前記変更情報に基づいて、前記変更補助データを前記補助データに再変更する再変更工程とを備える。

[0070] 本発明の第2の情報再生方法によれば、ユーザデータに基づいて変更情報が生成されるため、上述した第2の情報再生装置と同様に、置換ユーザデータからユーザデータ及び補助データを確実に再生できる。

[0071] 本発明の作用及び他の利得は、次に説明する実施するための最良の形態から明らかにされる。

図面の簡単な説明

[0072] [図1]第1実施形態に係る情報生成装置及び情報再生装置の構成を示すブロック図である。

[図2]第1実施形態に係る情報生成装置及び情報再生装置の変形例を示すブロック図である。

[図3]第1実施形態に係る情報生成装置の動作の流れを示すフローチャートである。

[図4]位置情報の生成方法について示す概念図である。

[図5]ユーザデータを補助データに置換する方法について示す概念図(その1)である。

[図6]ユーザデータを補助データに置換する方法について示す概念図(その2)である。

[図7]第1実施形態に係る情報再生装置の動作の流れを示すフローチャートである。

[図8]ユーザデータの復号及び位置情報の生成方法を示す概念図である。

[図9]補助データの抽出及び復号方法を示す概念図である。

[図10]第2実施形態に係る情報生成装置及び情報再生装置の構成を示すブロック図である。

[図11]第3実施形態に係る情報生成装置及び情報再生装置の構成を示すブロック図である。

[図12]位置情報生成部の構成を示すブロック図(その1)である。

[図13]位置情報生成部の構成を示すブロック図(その2)である。

[図14]位置情報生成部の構成を示すブロック図(その3)である。

[図15]第4実施形態に係る情報生成装置における、位置情報の生成及び補助データの置換方法を示す概念図である。

[図16]第4実施形態に係る情報再生装置における、補助データの再生方法を示す概念図である。

[図17]第5実施形態に係る情報生成装置及び情報再生装置の構成を示すブロック図である。

[図18]第5実施形態に係る情報生成装置及び情報再生装置の変形例を示すブロック図である。

[図19]第5実施形態に係る情報生成装置の動作の流れを示すフローチャートである。

[図20]変更情報の生成方法について示す概念図である。

[図21]変更情報を用いた補助データの変更方法について示す概念図である。

[図22]第5実施形態に係る情報再生装置の動作の流れを示すフローチャートである。

。

[図23]ユーザデータの復号及び変更情報の生成方法を示す概念図である。

[図24]補助データの抽出及び再変更、並びに復号方法を示す概念図である。

[図25]符号化部から出力されるデータを示す概念図(その1)である。

[図26]第2符号化部から出力されるデータを示す概念図である。

[図27]補助データの分割について示す概念図(その1)である。

[図28]補助データの分割について示す概念図(その2)である。

[図29]符号化部から出力されるデータを示す概念図(その2)である。

符号の説明

- [0073] 100 情報生成装置
 - 110 符号化部
 - 120 位置情報生成部
 - 121 生成部
 - 122 位置情報暗号化部
 - 123 ユーザデータ暗号化部
 - 124 HMAC処理部
 - 130 第2符号化部
 - 140 置換部
 - 150 変調部
 - 160 書き込み部
 - 170 変更情報生成部
 - 180 変更部
- 200 情報再生装置
 - 210 読み出し部
 - 220 復調部
 - 230 復号部
 - 240 第2位置情報生成部
 - 250 抽出部

260 第2復号部
270 第2変更情報生成部
280 再変更部
300 ホログラフィックメモリ
400 通信ケーブル
510 暗号化部
520 第3復号部

発明を実施するための最良の形態

[0074] 以下では、本発明の実施形態について図を参照しつつ説明する。尚、以下では本発明の情報生成装置及び情報再生装置を用いて、記録媒体であるホログラフィックメモリに対して情報の記録及び再生を行う場合を例にとり説明する。

[0075] <第1実施形態>

先ず、第1実施形態に係る情報生成装置の構成について、図1及び図2を参照して説明する。ここに図1は、第1実施形態に係る情報生成装置及び情報再生装置の構成を示すブロック図であり、図2は、第1実施形態に係る情報生成装置及び情報再生装置の変形例を示すブロック図である。

[0076] 図1において、第1実施形態に係る情報生成装置100は、符号化部110と、位置情報生成部120と、第2符号化部130と、置換部140と、変調部150と、書き込み部160とを備えて構成されている。

[0077] 符号化部110は、本発明の「符号化手段」の一例であり、入力されたユーザデータ（例えば、映像ファイルや音楽ファイル、文書ファイルなどの記録すべきデータ）に対して誤り訂正符号を付加する。

[0078] 位置情報生成部120は、本発明の「位置情報生成手段」の一例であり、入力されたユーザデータから、後述する置換部140において置換するデータの位置を示す位置情報を生成する。位置情報は、ユーザ情報から一意的に求められるような情報である。

[0079] 第2符号化部130は、本発明の「補助符号化手段」の一例であり、入力された補助データに対して誤り訂正符号を付加する。補助データは、ユーザデータに関連する

補助的なデータであり、ユーザデータとは異なる用途で用いられる。補助データの例として、ユーザデータの属性、ファイル名前及び管理番号等を示すデータや、分割されたユーザデータの分割位置を示すデータ、ユーザデータが不正にコピーされたデータであるか否かを識別するためのデータ等が挙げられる。尚、符号化部110及び第2符号化部130を同一の演算回路等から構成するようにしてもよい。

[0080] 置換部140は、本発明の「置換手段」の一例であり、符号化部110において符号化されたユーザデータの一部を、第2符号化部130において符号化された補助データと置換する。この際、置換されるユーザデータの位置は、位置情報生成部120において生成された位置情報に基づいている。

[0081] 変調部150は、置換部140において置換されたユーザデータを記録するのに適切な方式のデータへと変調する。本実施形態のようにホログラフィックメモリ300に対して情報を記録する場合には、例えば2ビットのデータを4つの画素で示す(2, 4)変調や、6ビットのデータを9つの画素で示す(6, 9)変調等が用いられる。

[0082] 書き込み部160は、例えば光源やレンズ等を含んで構成されており、光源から出射されたレーザ光をレンズで集光してホログラフィックメモリ300に照射し、干渉縞としてユーザデータを記憶する。

[0083] 図2において、第1実施形態に係る情報生成装置及び情報再生装置は、上述した情報の記録以外に、例えば通信によって情報をやり取りする場合にも利用することが可能である。このような場合は、変調部150において通信用に変調されたユーザデータが、例えば図に示すような通信ケーブル400を介して電気信号として伝送される。情報生成装置及び情報再生装置は、電気信号の変調や復調に加えて、同期信号を用いた情報位置の特定や管理情報の処理等を行う。

[0084] 続いて、第1実施形態に係る情報生成装置の動作について、図1に加えて、図3から図6を参照して説明する。ここに図3は、第1実施形態に係る情報生成装置の動作の流れを示すフローチャートである。また図4は、位置情報の生成方法について示す概念図であり、図5及び図6は夫々、ユーザデータを補助データに置換する方法について示す概念図である。

[0085] 図1及び図3において、第1実施形態に係る情報生成装置100の動作時には、先

ず符号化部110にユーザデータが入力される。符号化部110は、入力されたユーザデータに対して誤り訂正符号を付加する(ステップS11)。これにより、ユーザデータの一部に誤りが生じた場合であっても、誤り訂正符号を用いて正しいデータを修復することが可能となる。図4に示すように、ユーザデータに対する誤り訂正符号(C1～C4)は、典型的には、ユーザデータ(U1～U8)の最後の部分に付加される。但し、インターリーブ等によって、各データの配置が並び替えられてもよい。

[0086] 他方で、第2符号化部130には補助データが入力される。第2符号化部130は、補助データに対し誤り訂正符号を付加する(ステップS12)。これにより、補助データも、ユーザデータと同様に誤り訂正能力を有することになる。図5に示すように、補助データに対する誤り訂正符号(E1)は、典型的には、補助データ(A1及びA2)の最後の部分に付加される。但し、上述したユーザデータと同様に、インターリーブ等によって、各データの配置が並び替えられてもよい。

[0087] ユーザデータは、上述した符号化部110に加えて、位置情報生成部120にも入力されている。位置情報生成部120は、入力されたユーザデータに基づいて、ユーザデータの一部を補助データに置換する際に置換されるデータの位置を示す位置情報を生成する(ステップS13)。位置情報は、例えばハッシュ関数により生成されるハッシュ値を用いることができ、ハッシュ関数にSHA-1 (Secure Hash Algorithm 1)を用いる場合には、任意長の入力値(即ち、ユーザデータ)に対して、160ビットの出力値(即ち、位置情報)が得られる。尚、位置情報は、ハッシュ値のように、ユーザデータから一意的に求められる情報であれば、直接的にデータの位置を示すような情報でなくともよい。このような場合は、例えば位置情報が有する値と、置換するデータの位置とを対応させるような法則を予め設定しておくことで、置換されるデータの位置が示される。

[0088] 位置情報が生成されると、置換部140は、ユーザデータの一部を補助データへと置換する(ステップS14)。置換部140は、位置情報生成部120によって生成された位置情報に基づいて、ユーザデータを補助データに置換する。尚、ユーザデータは、誤り訂正符号を付加された後に補助データと置換されることとなるため、置換された補助データは意図的な誤りとして扱われる。

- [0089] ここで図4に示すように、位置情報生成部120によって、ユーザデータ(U1～U8)から、7, 2, 5, 6, 8, …といった位置情報が生成されているとする。また図5に示すように、ユーザデータは、4つのデータ毎に第1ブロックから第3ブロックの3つのブロックに分けられており、各ブロック中のデータには0～3のポジション番号が付与されているとする。尚、ここでは後述するように各ブロックに対して補助データを1つずつ置換するため、ユーザデータにおけるブロックの数は、置換する補助データの数(即ち、ここではA1、A2及びE1の3つ)と同じ、或いはそれ以上であることが望ましい。
- [0090] また、補助データの情報量が多く、例えば位置情報として出力されたハッシュ関数の出力値の数より補助データの値の数の方が多い場合には、位置情報を示すための値が不足してしまう。このような場合には、ハッシュ関数の出力を更にハッシュ関数に入力した値(即ち、ハッシュ値のハッシュ値)を生成することで対応することが可能である。
- [0091] 置換部140には、予め位置情報の各値をブロック長(即ち、ここでは“4”)で割った余りが示すポジションのユーザデータと、補助データとを置換するという法則が記憶されている。尚、位置情報は、先頭の値から第1ブロック、第2ブロック、第3ブロックに夫々対応しており、ここでは4つ目以降の値は用いない。但し、4つ目以降の値を用いるようにしてもよい。
- [0092] 図5において、上述した法則により、第1ブロックについては、位置情報の先頭の値である“7”を4で割った余りが“3”となるので、補助データA1が第1ブロックのポジション3のユーザデータU4と置換される。第2ブロックについては、位置情報の2番目の値である“2”を4で割った余りが“2”となるので、補助データA2が第2ブロックのポジション2のユーザデータU7と置換される。第3ブロックについては、位置情報の3番目の値である“5”を4で割った余りが“1”となるので、補助データに付加された誤り訂正符号E1が第3ブロックのポジション1の誤り訂正符号C2と置換される。以上のように置換すれば、比較的容易に、且つユーザデータに対して、均等に補助データを埋め込むことができる。
- [0093] 上述した置換方法はあくまで一例であり、例えばデータが置換されないブロックが存在するようにしてもよい。具体的には、位置情報の各値をブロック長である“4”で割

った余りに応じて補助データを置換するという法則に代えて、余りが0又は3の場合には対応するブロックにおける置換を行わず、余りが2の場合にポジション0及びポジション2の置換を行い、余りが1の場合にポジション1を置換するという法則を用いて置換する。

[0094] 図6において、上述した法則によれば、第1ブロックについては、位置情報の先頭の値である“7”を4で割った余りが“3”となるので置換されない。第2ブロックについては、位置情報の2番目の値である“2”を4で割った余りが“2”となるので、補助データA1及びA2が第2ブロックのポジション0のユーザデータU5及びポジション2のユーザデータU7と夫々置換される。第3ブロックについては、位置情報の3番目の値である“5”を4で割った余りが“1”となるので、補助データに付加された誤り訂正符号E1が第3ブロックのポジション1の誤り訂正符号C2と置換される。

[0095] ブロックにおける補助データが置換される位置を自由に変更することができれば、例えば記録媒体の特定の場所や通信路の特定のタイミングに傷やノイズ等の誤りが生じやすいことが判明している場合に、該当するブロック内にあるシンボルを補助データで置換しないようにする、或いは置換するシンボル数を少なくすることが可能である。これにより、補助データが誤って抽出されてしまう可能性を低減することができる。

[0096] 以上のように、置換方法は位置情報を用いるものであれば特に限定されず、後述する本実施形態に係る情報生成装置の効果を適切に発揮することが可能である。また、複数の置換方法を予め設定しておき、特定のタイミングで法則を切り換えて使用することも可能である。尚、この効果については、後述する本実施形態に係る情報再生装置の説明において詳述する。

[0097] 図1及び図3に戻り、ユーザデータの一部が補助データに置換されると、変調部150は、ユーザデータを記録に適した方式に変調する(ステップS15)。書き込み部160は、変調したユーザデータをホログラフィックメモリ300に記録する(ステップS16)。尚、本実施形態に係る情報生成装置では、置換した補助データの位置を示す位置情報はホログラフィックメモリ300には記録されない。また他の記録媒体にも記録する必要はない。よって、ここで記録されるデータの大きさは、記録すべきユーザデータ

の大きさと同じで済む。

[0098] 次に、第1実施形態に係る情報再生装置の構成について、再び図1及び図2を参照して説明する。

[0099] 図1において、第1実施形態に係る情報再生装置200は、読み出し部210と、復調部220と、復号部230と、第2位置情報生成部240と、抽出部250と、第2復号部260とを備えて構成されている。

[0100] 読み出し部210は、例えば発光部、レンズ及び受光素子を備えて構成されており、ホログラフィックメモリ300にレーザ光を照射して得られる像を、受光素子によって検出し、検出された像からユーザデータを再生する。

[0101] 復調部220は、情報生成装置100における変調部150によって変調したユーザデータを元の状態へと復調する。即ち、変調部150とは逆の処理を行う。

[0102] 復号部230は、本発明の「復号手段」の一例であり、ユーザデータに付加された誤り訂正符号を用いて、ユーザデータに含まれる誤りを訂正する。

[0103] 第2位置情報生成部240は、本発明の「第2位置情報生成手段」の一例であり、復号部230において復号されたユーザデータ(即ち、誤りが訂正されたユーザデータ)から、情報生成装置100における位置情報生成部120と同様に位置情報を生成する。尚、位置情報生成部120を第2位置情報生成部240として用いることもできる。

[0104] 抽出部250は、本発明の「抽出手段」の一例であり、復号前のユーザデータ(即ち、補助データが意図的な誤りとして含まれているユーザデータ)から、第2位置情報生成部240において生成された位置情報を用いて、補助データを抽出する。

[0105] 第2復号部260は、抽出された補助データに付加されている誤り訂正符号を用いて、補助データに含まれる誤りを訂正する。

[0106] 尚、本実施形態に係る情報再生装置を、図2に示すような通信に用いる場合には、通信ケーブル400を介して伝送されたデータが、復調部220に入力される。

[0107] 続いて、第1実施形態に係る情報再生装置の動作について、図1に加えて、図7から図9を参照して説明する。ここに図7は、第1実施形態に係る情報再生装置の動作の流れを示すフローチャートである。また図8は、ユーザデータの復号及び位置情報の生成方法を示す概念図であり、図9は、補助データの抽出及び復号方法を示す概

念図である。

- [0108] 図1及び図7において、本実施形態に係る情報再生装置200の動作時には、先ず読み出し部210が、ホログラフィックメモリ300に記録されたユーザデータを読み出す(ステップS21)。続いて、復調部220が、読み出されたユーザデータを変調前の状態に復調する(ステップS22)。
- [0109] ユーザデータが復調されると、復号部230は、ユーザデータに付加されている誤り訂正符号を用いて、ユーザデータに含まれる誤りを訂正する(ステップS23)。この際、情報生成装置100における置換部140によってユーザデータの一部と置換された補助データは、誤りとして訂正される。即ち、補助データは置換前のユーザデータとされる。復号されたユーザデータは、再生結果として外部に出力されると共に、第2位置情報生成部240に対しても出力される。第2位置情報生成部240は、復号されたユーザデータを用いて位置情報を生成する(ステップS24)。
- [0110] 図8において、読み出し部210によって読み出された際のユーザデータ(D1～D12)には、意図的な誤りである補助データに加えて、ホログラフィックメモリ300における傷や、記録及び再生時のノイズ等によって、いくつかの誤りが含まれている。復号部230は、このような誤りを含んだユーザデータを復号し、置換前のユーザデータ(U1～U8)とする。ユーザデータは、情報生成装置100における位置情報生成部120が用いたユーザデータと同一のデータであるので、第2位置情報生成部240において生成される位置情報は、位置情報生成部120において生成された位置情報と同一のものとなる。このように、ユーザデータが復号できるのであれば、第2位置情報生成部240において再び同一の位置情報を生成することができる。よって、位置情報生成部120において生成した位置情報を、ホログラフィックメモリ300や別の記録媒体等に記録しておく必要がない。
- [0111] 図1及び図7に戻り、第2位置情報生成部240において生成された位置情報は、抽出部250に出力される。また、抽出部250には、復号部230において復号される前のユーザデータも出力されている。抽出部250は、復号前のユーザデータから、位置情報に基づいてデータを抽出する(ステップS25)。
- [0112] 図9において、上述したように、第2位置情報生成部240において生成される位置

情報は、位置情報生成部120において生成された位置情報と同一のもの(7, 2, 5, 6, 8, ...)であるので、置換部140において置換する場合の同様の法則に基づけば、確実に補助データを抽出することができる。具体的には、第1ブロックについては、位置情報の先頭の値である“7”を4で割った余りが“3”となるので、第1ブロックのポジション3からユーザデータD4が抽出される。第2ブロックについては、位置情報の2番目の値である“2”を4で割った余りが“2”となるので、第2ブロックのポジション2からユーザデータD7が抽出される。第3ブロックについては、位置情報の3番目の値である“5”を4で割った余りが“1”となるので、第3ブロックのポジション1からユーザデータD10が抽出される。

[0113] 抽出された補助データ(D4、D7及びD10)は、第2復号部において誤りが訂正され、符号化前の補助データ(A1及びA2)に復号される(ステップS26)。復号された補助データは、再生結果として外部に出力される。

[0114] 以上説明したように、第1実施形態に係る情報生成装置及び情報再生装置によれば、記録すべき情報が増大してしまうことを防止しつつ、確実に補助データを再生することが可能である。例えば補助データが不正ディスクを検出するための識別データとして、ユーザデータと共に記録媒体に記録される場合を考えると、仮に補助データが傷などに起因して再生できなくなれば、不正ディスクの検出ができなくなる。よって、補助データが再生できなくなることで、ユーザデータの再生まで不可能となってしまう或いは不正ディスクかもしれないディスクを再生せざるを得ないおそれがある。第1実施形態に係る情報生成装置及び情報再生装置によれば、このような実践上の不都合を好適に回避することが可能である。

[0115] <第2実施形態>

次に、第2実施形態に係る情報生成装置及び情報再生装置について、図10を参照して説明する。ここに図10は、第2実施形態に係る情報生成装置及び情報再生装置の構成を示すブロック図である。尚、第2実施形態は、上述した第1実施形態と比べて、ユーザデータが暗号化される点が異なり、その他の構成や動作等は概ね同じである。よって、ここでは第1実施形態と異なる部分について詳細に説明し、他の重複する部分については適宜説明を省略する。また図10では、情報生成装置100及

び情報再生装置200の各構成要素が上述した第1実施形態と同一であるため、詳細な図示を省略している。

[0116] 図10において、第2実施形態に係る情報生成装置100には、暗号化部510によって暗号化されたユーザデータが入力される。よって、ユーザデータのセキュリティを向上させることが可能である。

[0117] 暗号化部510におけるユーザデータの暗号化は、鍵情報を用いて行われる。そして、ここで用いられた鍵情報は、情報生成装置100に補助データとして入力される。よって、第2実施形態では、ユーザデータに対して鍵情報が意図的な誤りとして埋め込まれた状態で記録が行われる。従って、鍵情報を記録するためにデータの大きさが増加してしまうことを防止することができる。

[0118] 一方、第2実施形態に係る情報再生装置200は、ホログラフィックメモリ300に記録されたユーザデータを読み出し、暗号化されたユーザデータ及び補助データである鍵情報を再生結果として出力する。

[0119] 暗号化されたユーザデータ及び補助データは、第3復号部520に入力される。第3復号部520は、補助データである鍵情報を用いて暗号化されたユーザデータを復号し、復号されたユーザデータを出力する。

[0120] 以上説明したように、第2実施形態に係る情報生成装置及び情報再生装置によれば、ユーザデータに対するセキュリティが向上しているため、情報をより好適に記録及び再生することが可能である。また、上述した第1実施形態と同様に、データ量の増大を防止しつつ、補助データが確実に再生可能とされているため、実践上極めて有利である。

[0121] <第3実施形態>

次に、第3実施形態に係る情報生成装置及び情報再生装置について、図11から図14を参照して説明する。ここに図11は、第3実施形態に係る情報生成装置及び情報再生装置の構成を示すブロック図であり、図12から図14は夫々、位置情報生成部の構成を示すブロック図である。尚、第3実施形態は、上述した第1実施形態と比べて、位置情報生成部の構成及び動作が異なり、他の構成や動作等は概ね同じである。よって、ここでは第1実施形態と異なる部分について詳細に説明し、他の重複

する部分については適宜説明を省略する。また図11では、上述した第1実施形態に係る情報生成装置及び情報再生装置の各構成要素と同様の構成要素に同一の参照符号を付している。

[0122] 図11において、第3実施形態に係る情報生成装置100には、ユーザデータ及び補助データに加えて、位置情報を暗号化するための鍵情報が入力される。鍵情報は、図に示すように、位置情報生成部120に入力される。

[0123] 図12において、位置情報生成部120は、例えば生成部121と、位置情報暗号化部122とを備えて構成される。生成部121は、入力されたユーザデータに基づいて位置情報を生成し、位置情報暗号化部122に出力する。位置情報暗号化部は、生成された位置情報を鍵情報を用いて暗号化し、暗号化された位置情報として出力する。

[0124] 上述したように構成すれば、鍵情報がないと位置情報を生成することができないため、位置情報のセキュリティを向上させることができる。即ち、補助データが不正に再生されてしまうようなことを効果的に防止することが可能である。

[0125] 図13において、位置情報生成部120は、ユーザデータ暗号化部123と、生成部121とを備えて構成されてもよい。この場合、先ずユーザデータ暗号化部123にユーザデータ及び鍵情報が入力され、ユーザデータが暗号化される。そして、生成部121は、暗号化されたユーザデータを用いて位置情報を生成する。ここでの構成は、上述した第2実施形態と比較的近いものとなる。

[0126] 上述した構成によれば、位置情報は直接暗号化されないが、元となるユーザデータが暗号化されている。このため、暗号化されていないユーザデータを用いて位置情報を生成する場合と比較すると、位置情報のセキュリティを向上させることが可能である。

[0127] 図14において、位置情報生成部120はHMAC処理部124を備えて構成されてもよい。この場合、ユーザデータ及び鍵情報はHMAC処理部124に入力され、HMAC処理部124から出力された位置情報（ハッシュ値）が出力される。

[0128] 上述した構成によれば、HMACを用いることで、図12及び図13で示したように、位置情報を生成する部位及びユーザデータ或いは位置情報を暗号化する部位を別々

に設けなくとも済む。よって、比較的簡単な構成で、位置情報のセキュリティ向上を実現することが可能である。

[0129] 図11に戻り、第3実施形態に係る情報再生装置200には、データを再生する際に鍵情報が入力される。尚、鍵情報は、ホログラフィックメモリ300に記録されていてもよいし、他の記録媒体に記録されていてもよい。

[0130] 鍵情報は、第2位置情報生成部240に入力され、第2位置情報生成部240からは暗号化された位置情報が抽出部250に出力される。尚、第2位置情報生成部240は、図12から図13に示したような構成をとることができる。

[0131] 以上説明したように、第3実施形態に係る情報生成装置及び情報再生装置によれば、位置情報に対するセキュリティが向上させられているため、補助データを確実に保護しつつ記録及び再生を行うことができる。また、上述した第1実施形態と同様に、データ量の増大を防止しつつ、補助データが確実に再生可能とされているため、実践上極めて有利である。

[0132] <第4実施形態>

次に、第4実施形態に係る情報生成装置及び情報再生装置について、図15及び図16を参照して説明する。ここに図15は、第4実施形態に係る情報生成装置における、位置情報の生成及び補助データの置換方法を示す概念図であり、図16は、第4実施形態に係る情報再生装置における、補助データの再生方法を示す概念図である。尚、第4実施形態は、上述した第1実施形態と比べて、補助データを変更させる点が異なり、その他の構成や動作等は概ね同じである。よって、ここでは第1実施形態と異なる部分について詳細に説明し、他の重複する部分については適宜説明を省略する。

[0133] 図15において、第4実施形態に係る情報生成装置100では、補助データが置換部140においてユーザデータの一部と置換される前に、位置情報を用いて変更される。即ち、位置情報は、補助データを置換する位置を示すという役割に加えて、補助データの値を変更するという役割を持っている。

[0134] 例えば、誤り訂正符号が付加された補助データ(A1、A2及びE1)は、位置情報である7, 2, 5, 6, 8, ...と共に演算処理が施されることにより、別の値へと変更される

。尚、ここでの演算処理(即ち、図中で示す“+”)は、XOR演算であるとする。具体的には、補助データA1は、位置情報の先頭の値“7”とXOR演算されることでA1’とされる。補助データA2は、位置情報の2番目の値“2”とXOR演算されることでA2’とされる。補助データに付加された誤り訂正符号E1は、位置情報の3番目の値“5”とXOR演算されることでE1’とされる。

[0135] 位置情報によって変更された補助データ(A1’, A2’及びE1’)は、上述した各実施形態と同様に、置換部140によって、ユーザデータの一部と置換される。

[0136] 図16において、第4実施形態に係る情報再生装置200では、抽出された補助データ(D4, D6及びD10)が位置情報に基づいて変更されたものとなる。よって、ここでは抽出された補助データが、位置情報に基づいて再変更される。例えば、上述したようにXOR演算処理によって補助データを変更した場合には、再び位置情報を用いてXOR演算処理を行うことによって、XOR演算処理の効果が打ち消され、補助データは元の値(A1, A2及びE1)となる。尚、XOR演算処理以外の演算処理であっても、位置情報を用いて可逆的に補助データを変更できるような演算処理であれば、利用することが可能である。

[0137] 以上説明したように、第4実施形態に係る情報生成装置及び情報再生装置によれば、補助データが位置情報によって変更されることにより、補助データのセキュリティが向上させられているため、補助データを確実に保護しつつ記録及び再生を行うことができる。また、上述した第1実施形態と同様に、データ量の増大を防止しつつ、補助データが確実に再生可能とされているため、実践上極めて有利である。

[0138] <第5実施形態>

次に、第5実施形態に係る情報生成装置及び情報再生装置について、図17から図24を参照して説明する。尚、第5実施形態は、上述した第1実施形態と比べて、位置情報に代えて変更情報を用いる点が異なり、その他の構成や動作等は概ね同じである。よって、ここでは第1実施形態と異なる部分について詳細に説明し、他の重複する部分については適宜説明を省略する。

[0139] 先ず、第5実施形態に係る情報生成装置の構成について、図17及び図18を参照して説明する。ここに図17は、第5実施形態に係る情報生成装置及び情報再生装置

の構成を示すブロック図であり、図18は、第5実施形態に係る情報生成装置及び情報再生装置の変形例を示すブロック図である。

[0140] 図17において、第5実施形態に係る情報生成装置100は、符号化部110と、第2符号化部130と、置換部140と、変調部150と、書き込み部160と、変更情報生成部170と、変更部180とを備えて構成されている。

[0141] 符号化部110は、本発明の「符号化手段」の一例であり、入力されたユーザデータ（例えば、映像ファイルや音楽ファイル、文書ファイルなどの記録すべきデータ）に対して誤り訂正符号を付加する。

[0142] 第2符号化部130は、本発明の「補助符号化手段」の一例であり、入力された補助データに対して誤り訂正符号を付加する。補助データは、ユーザデータに関連する補助的なデータであり、ユーザデータとは異なる用途で用いられる。補助データの例として、ユーザデータの属性、ファイル名前及び管理番号等を示すデータや、分割されたユーザデータの分割位置を示すデータ、ユーザデータが不正にコピーされたデータであるか否かを識別するためのデータ等が挙げられる。尚、符号化部110及び第2符号化部130を同一の演算回路等から構成するようにしてもよい。

[0143] 変更情報生成部170は、本発明の「変更情報生成手段」の一例であり、入力されたユーザ情報に基づいて、補助データを変更するための変更情報を生成する。変更情報は、ユーザ情報から一意的に求められるような情報である。

[0144] 変更部180は、本発明の「補助データ変更手段」の一例であり、変更情報生成部170において生成された変更情報を用いて、符号化された補助データを変更する。補助データの変更は、例えば補助データ及び変更情報を用いた演算処理によって行われる。

[0145] 置換部140は、本発明の「置換手段」の一例であり、符号化部110において符号化されたユーザデータの一部を、変更部180において変更された補助データと置換する。

[0146] 変調部150は、置換部140において置換されたユーザデータを記録するのに適切な方式のデータへと変調する。本実施形態のようにホログラフィックメモリ300に対して情報を記録する場合には、例えば2ビットのデータを4つの画素で示す(2, 4)変調

や、6ビットのデータを9つの画素で示す(6, 9)変調等が用いられる。

[0147] 書き込み部160は、例えば光源やレンズ等を含んで構成されており、光源から出射されたレーザ光をレンズで集光してホログラフィックメモリ300に照射し、干渉縞としてユーザデータを記憶する。

[0148] 図18において、第5実施形態に係る情報生成装置及び情報再生装置は、上述した情報の記録以外に、例えば通信によって情報をやり取りする場合にも利用することが可能である。このような場合は、変調部150において通信用に変調されたユーザデータが、例えば図に示すような通信ケーブル400を介して電気信号として伝送される。情報生成装置及び情報再生装置は、電気信号の変調や復調に加えて、同期信号を用いた情報位置の特定や管理情報の処理等を行う。

[0149] 続いて、第5実施形態に係る情報生成装置の動作について、図17に加えて、図19から図21を参照して説明する。ここに図19は、第5実施形態に係る情報生成装置の動作の流れを示すフローチャートである。また図20は、変更情報の生成方法について示す概念図であり、図21は、変更情報を用いた補助データの変更方法について示す概念図である。

[0150] 図17及び図19において、第5実施形態に係る情報生成装置100の動作時には、先ず符号化部110にユーザデータが入力される。符号化部110は、入力されたユーザデータに対して誤り訂正符号を付加する(ステップS31)。これにより、ユーザデータの一部に誤りが生じた場合であっても、誤り訂正符号を用いて正しいデータを修復することが可能となる。図20に示すように、ユーザデータに対する誤り訂正符号(C1～C4)は、典型的には、ユーザデータ(U1～U8)の最後の部分に付加される。但し、インターリーブ等によって、各データの配置が並び替えられてもよい。

[0151] 他方で、第2符号化部130には補助データが入力される。第2符号化部130は、補助データに対し誤り訂正符号を付加する(ステップS32)。これにより、補助データも、ユーザデータと同様に誤り訂正能力を有することになる。図21に示すように、補助データに対する誤り訂正符号(E1)は、典型的には、補助データ(A1及びA2)の最後の部分に付加される。但し、上述したユーザデータと同様に、インターリーブ等によって、各データの配置が並び替えられてもよい。

- [0152] ユーザデータは、上述した符号化部110に加えて、変更情報生成部170にも入力されている。変更情報生成部170は、入力されたユーザデータに基づいて、補助データを変更するための変更情報を生成する(ステップS33)。変更情報は、例えばハッシュ関数により生成されるハッシュ値を用いることができ、ハッシュ関数にSHA-1 (Secure Hash Algorithm 1)を用いる場合には、任意長の入力値(即ち、ユーザデータ)に対して、160ビットの出力値(即ち、変更情報)が得られる。尚、変更情報は、ハッシュ値のように、ユーザデータから一意的に求められる情報である。
- [0153] 変更情報生成部170において生成された変更情報は、変更部180に入力される。また、変更部180には、第2符号化部130において符号化された補助データも入力される。変更部180は、変更情報に基づいて補助データを変更する(ステップS34)。
- [0154] 図20に示すように、変更情報生成部170によって、ユーザデータ(U1~U8)から、7, 2, 5, 6, 8, ...といった変更情報が生成されているとする。この場合、変更部180は、変更情報の各値と補助データとで演算処理を行うことで、補助データを変更する。尚、ここでの演算処理(即ち、図中で示す“+”)は、XOR演算であるとする。具体的には、補助データA1は、変更情報の先頭の値“7”とXOR演算されることでA1’とされる。補助データA2は、変更情報の2番目の値“2”とXOR演算されることでA2’とされる。補助データに付加された誤り訂正符号E1は、変更情報の3番目の値“5”とXOR演算されることでE1’とされる。
- [0155] 上述したように、ここでは1つの補助データに対して1つの変更情報を用いて変更するため、変更情報の値の数は、置換する補助データの数(即ち、ここではA1、A2及びE1の3つ)と同じ、或いはそれ以上であることが望ましい。但し、例えば変更情報としてハッシュ関数を用いており、補助データの値の数の方がハッシュ値より多く、変更情報の値が不足してしまう場合には、ハッシュ関数の出力を更にハッシュ関数に入力した値(即ち、ハッシュ値のハッシュ値)を生成することで対応することが可能である。
- [0156] 位置情報によって変更された補助データ(A1’, A2’及びE1’)は夫々、置換部140に出力される。置換部は、変更された補助データの各々を、ユーザデータの各ブロックにおけるポジション3の位置にあるユーザデータと置換する(ステップS35)。具体

的には、図21に示すように、補助データの先頭の値A1'は、ユーザデータの第1ブロックにおけるポジション3に位置するU4と置換される。補助データの2つ目の値A2'は、ユーザデータの第2ブロックにおけるポジション3に位置するU8と置換される。補助データの誤り訂正符号の値E1'は、ユーザデータの第3ブロックにおけるポジション3に位置するC4と置換される。以上のように置換すれば、比較的容易に、且つユーザデータに対して、均等に補助データを埋め込むことができる。ユーザデータは、誤り訂正符号を付加された後に補助データと置換されることとなるため、置換された補助データは意図的な誤りとして扱われる。

[0157] 尚、ここでは補助データとユーザデータにおけるポジション3に位置するデータとを置換するものとしたが、このような置換法則は設計事項であり、適宜変更することが可能である。即ち、後述する情報再生装置において、補助データがどの位置のユーザデータと置換されたかが分かるようにすればよく、置換に用いる法則は特に限定されない。

[0158] 図17及び図19に戻り、ユーザデータの一部が補助データに置換されると、変調部150は、ユーザデータを記録に適した方式に変調する(ステップS36)。書き込み部160は、変調したユーザデータをホログラフィックメモリ300に記録する(ステップS37)。尚、本実施形態に係る情報生成装置では、補助データを変更するために用いた変更情報はホログラフィックメモリ300には記録されない。また他の記録媒体にも記録する必要はない。よって、ここで記録されるデータの大きさは、記録すべきユーザデータの大きさと同じで済む。

[0159] 次に、第5実施形態に係る情報再生装置の構成について、再び図17及び図19を参照して説明する。

[0160] 図17において、第1実施形態に係る情報再生装置200は、読み出し部210と、復調部220と、復号部230と、抽出部250と、第2復号部260と、第2変更情報生成部270と、再変更部280とを備えて構成されている。

[0161] 読み出し部210は、例えば発光部、レンズ及び受光素子を備えて構成されており、ホログラフィックメモリ300にレーザ光を照射して得られる像を、受光素子によって検出し、検出された像からユーザデータを再生する。

- [0162] 復調部220は、情報生成装置100における変調部150によって変調したユーザデータを元の状態へと復調する。即ち、変調部150とは逆の処理を行う。
- [0163] 復号部230は、本発明の「復号手段」の一例であり、ユーザデータに付加された誤り訂正符号を用いて、ユーザデータに含まれる誤りを訂正する。
- [0164] 抽出部250は、本発明の「抽出手段」の一例であり、復号前のユーザデータ(即ち、補助データが意図的な誤りとして含まれているユーザデータ)から、情報を生成した際の置換法則を用いて補助データを抽出する。
- [0165] 第2復号部260は、抽出された補助データに付加されている誤り訂正符号を用いて、補助データに含まれる誤りを訂正する。
- [0166] 第2変更情報生成部270は、本発明の「第2変更情報生成手段」の一例であり、復号部230において復号されたユーザデータ(即ち、誤りが訂正されたユーザデータ)から、情報生成装置100における変更情報生成部170と同様に変更情報を生成する。尚、変更情報生成部170を第2変更情報生成部270として用いることもできる。
- [0167] 再変更部280は、本発明の「再変更手段」の一例であり、第2変更情報生成部270によって生成された変更情報に基づいて、変更部180によって変更された状態の補助データに各種演算処理を施すことにより、変更前の補助データへと再変更する。
- [0168] 尚、本実施形態に係る情報再生装置を、図18に示すような通信に用いる場合には、通信ケーブル400を介して伝送されたデータが、復調部220に入力される。
- [0169] 続いて、第5実施形態に係る情報再生装置の動作について、図17に加えて、図22から図24を参照して説明する。ここに図22は、第5実施形態に係る情報再生装置の動作の流れを示すフローチャートである。また図23は、ユーザデータの復号及び変更情報の生成方法を示す概念図であり、図24は、補助データの抽出及び再変更、並びに復号方法を示す概念図である。
- [0170] 図17及び図22において、本実施形態に係る情報再生装置200の動作時には、先ず読み出し部210が、ホログラフィックメモリ300に記録されたユーザデータを読み出す(ステップS41)。続いて、復調部220が、読み出されたユーザデータを変調前の状態に復調する(ステップS42)。
- [0171] ユーザデータが復調されると、復号部230は、ユーザデータに付加されている誤り

訂正符号を用いて、ユーザデータに含まれる誤りを訂正する(ステップS43)。この際、情報生成装置100における置換部140によってユーザデータの一部と置換された補助データは、誤りとして訂正される。即ち、補助データは置換前のユーザデータとされる。復号されたユーザデータは、再生結果として外部に出力されると共に、第2変更情報生成部270に対しても出力される。第2変更情報生成部270は、復号されたユーザデータを用いて変更情報を生成する(ステップS44)。

[0172] 図23において、読み出し部210によって読み出された際のユーザデータ(D1～D12)には、意図的な誤りである補助データに加えて、ホログラフィックメモリ300における傷や、記録及び再生時のノイズ等によって、いくつかの誤りが含まれている。復号部230は、このような誤りを含んだユーザデータを復号し、置換前のユーザデータ(U1～U8)とする。ユーザデータは、情報生成装置100における変更情報生成部170が用いたユーザデータと同一のデータであるので、第2変更情報生成部270において生成される変更情報は、変更情報生成部170において生成された変更情報と同一のものとなる。このように、ユーザデータが復号できるのであれば、第2変更情報生成部270において再び同一の変更情報を生成することができる。よって、変更情報生成部120において生成した変更情報を、ホログラフィックメモリ300や別の記録媒体等に記録しておく必要がない。

[0173] 図17及び図22に戻り、抽出部250には、復号部230において復号される前のユーザデータも出力されている。抽出部250は、復号前のユーザデータから補助データを抽出する(ステップS45)。抽出された補助データは、再変更部280に出力される。また再変更部280には、第2変更情報生成部270において生成された変更情報も出力されている。再変更部280は、変更情報に基づいて、抽出された補助データを再変更する(ステップS46)。

[0174] 図24において、抽出部250は、復号前のユーザデータ(D1～D12)における各ブロックのポジション3の位置から夫々データを抽出する。これにより、置換されていた補助データが抽出される。ここで抽出された補助データ(D4, D8及びD12)は、変更部180によって変更された状態であるので、再変更部280は、変更情報に基づいて抽出された補助データを再変更する。例えば、上述したようにXOR演算処理によ

って補助データを変更した場合には、再び位置情報を用いてXOR演算処理を行うことによって、XOR演算処理の効果が打ち消され、補助データは元の値(A1, A2及びE1)となる。尚、XOR演算処理以外の演算処理であっても、位置情報を用いて可逆的に補助データを変更できるような演算処理であれば、利用することが可能である。

[0175] 上述したように、補助データが変更されていることにより、仮に補助データのみが不正に抽出された場合であっても、抽出された補助データは変更された状態にあるため、単独では再生することができない。よって、補助データに対するセキュリティを向上させることが可能である。尚、上述した第2及び第3実施形態に示したように、他の鍵情報を用いた暗号化と組み合わせれば、より高いセキュリティを実現することが可能である。

[0176] 再変更後の補助データは、第2復号部において誤りが訂正され、符号化前の補助データ(A1及びA2)に復号される(ステップS47)。復号された補助データは、再生結果として外部に出力される。

[0177] 以上説明したように、第5実施形態に係る情報生成装置及び情報再生装置によれば、補助データのセキュリティを向上させることができる。また、補助データの変更に用いる変更情報をユーザデータの一部と置換して記録するため、記録すべき情報が増大してしまうことを防止することが可能である。

[0178] <誤り訂正符号決定方法>

最後に、上述した第1から第5実施形態に係る情報生成装置及び情報再生装置において用いられる誤り訂正符号のパラメータ決定方法について、図25から図29を参照して詳細に説明する。ここに図25及び図29は夫々、符号化部から出力されるデータを示す概念図であり、図26は、第2符号化部から出力されるデータを示す概念図である。また図27及び図28は夫々、補助データの分割について示す概念図である。

[0179] 上述した実施形態に係る情報生成装置及び情報再生装置では、補助データを意図的な誤りとして埋め込む分、想定している誤りに対して更に誤りを生じさせることになる。よって、誤り訂正が不可能になることを防止するため、十分な誤り訂正ができるよう、誤り訂正符号のパラメータを慎重に決定することが望ましい。

[0180] 図25において、符号化部110(図1参照)が処理単位とするユーザデータの大きさを k シンボル、出力の大きさを n シンボルとする。即ち、 $n-k$ シンボルの誤り訂正符号がユーザデータに付加されるものとする。この際、 n シンボルのうち最大 e シンボルが誤るものである、即ち符号化部110における誤り訂正能力が e シンボルであるものとする、下記の式(1)、

$$e < (n - k) / 2 \cdots (1)$$

を満たすよう n 及び k を選べばよい。

[0181] ここで e について、記録再生時の雑音など装置に起因するもの及び傷など記録媒体に起因するものの両者に起因する成分(即ち、図中の“傷誤”)を e_1 、ユーザデータの一部を補助データで置き換えることに起因する成分(即ち、図中の“意誤”)を e_2 とおく(即ち、 $e = e_1 + e_2$)。すると、ユーザデータを構成する各ブロックのブロック長 B については、装置や記録媒体に起因する誤りが均一に分布しているという条件下では、 $B = n / e_2$ となる。但し、値が割り切れない場合は切り捨てるものとする。ブロック長 B については、剰余演算を簡単に行うことができるようにするため、2の指数乗にすることが望ましい。これは2の指数乗の剰余演算が単なる下位ビットの抽出になるためである。

[0182] 図26において、第2符号化部130(図1参照)が処理単位とする補助データの大きさを k' シンボル、出力の大きさを n' シンボルとする。 n' シンボルのうち最大 e' シンボルが誤るものである、即ち、第2符号化部130における誤り訂正能力が e' シンボルであるものとする、下記の式(2)、

$$e' < (n' - k') / 2 \cdots (2)$$

を満たすよう n' 及び k' を選べばよい。

[0183] 図27において、第2符号化部130では、例えば入力された補助データを k' シンボルずつに分割して誤り訂正符号を付加する。ここで、補助データ全体の大きさを A シンボルとすると、誤り訂正符号生成及び付加処理の回数である α は、下記の式(3)、

$$A \leq \alpha k' \cdots (3)$$

を満たせばよい。尚、必ずしも A が k' の倍数になるとは限らないので、このような場合には、図に示すように補助データにダミーデータを付加する、或いはゼロパディング

を行うようにすればよい。

- [0184] 図28において、上述した α のうち最小となる値を α' とすると、第2符号化部130の基本処理単位は n' シンボルなので、 k' シンボルに分割された補助データでユーザデータを置換するためには、付加される誤り訂正符号を含めて n' シンボルのユーザデータを置換すればよい。よって、ユーザデータを A シンボル分の補助データで置換するためには、 $\alpha' n'$ シンボルのユーザデータを置換すればよい。 e_2 シンボルを置換したい場合、対応する k シンボル分のユーザデータがあればよいので、上述した $\alpha' n'$ シンボルを置換するためのユーザデータを x シンボルとすると、下記の式(4)

$$e_2:k = \alpha' n':x \cdots (4)$$

という比例関係が成立する。よって、上述した式(4)を x について解けば、下記の式(5)、

$$x = k \alpha' n' / e_2 \cdots (5)$$

という結果が得られる。

- [0185] 図29において、 e_2 シンボルを置換したい場合、符号化部110の出力が n シンボルとなるため、上述した $\alpha' n'$ シンボルを置換するために必要な符号化データを y シンボルとすると、下記の式(6)

$$e_2:n = \alpha' n':y \cdots (6)$$

という比例関係が成立する。よって、上述した式(6)を y について解けば、下記の式(7)、

$$y = n \alpha' n' / e_2 \cdots (7)$$

という結果が得られる。

- [0186] 以上の結果から、これらの条件を満たすようユーザデータや補助データの大きさ、誤り訂正符号のシンボル数やブロック長を設定することで、上述した本実施形態に係る情報生成装置及び情報再生装置における効果を確実に得ることが可能となる。

- [0187] 本発明は、上述した実施形態に限られるものではなく、請求の範囲及び明細書全体から読み取ることができる発明の要旨或いは思想に反しない範囲で適宜変更可能であり、そのような変更を伴う情報生成装置及び方法、情報再生装置及び方法、並びに記録媒体もまた本発明の技術的範囲に含まれるものである。

産業上の利用可能性

[0188] 本発明の情報生成装置及び方法、情報再生装置及び方法、並びに記録媒体は、例えばホログラフィックメモリ等の記録媒体に情報を記録する記録装置又は記憶された情報を再生する再生装置に利用可能である。また、情報をインターネット等によってやり取りする通信装置等においても利用可能である。

請求の範囲

- [1] ユーザデータの一部を、前記ユーザデータに関連するデータであって、前記ユーザデータとは異なる用途で用いられる補助データに置換して、置換ユーザデータを生成する情報生成装置であって、
- 前記ユーザデータに対して誤り訂正符号を付加して、符号化データを生成する符号化手段と、
- 前記符号化データにおける前記補助データに置換されるデータの位置を示す位置情報を、前記ユーザデータに基づいて生成する位置情報生成手段と、
- 前記符号化データの一部を、前記位置情報に基づいて前記補助データに置換して、前記置換ユーザデータを生成する置換手段と
- を備えることを特徴とする情報生成装置。
- [2] 前記符号化データは、所定数の連続するデータ毎にブロックとして分割されており、
- 前記置換手段は、前記ブロック毎に、前記符号化データを1つの補助データと置換する
- ことを特徴とする請求の範囲第1項に記載の情報生成装置。
- [3] 前記補助データに対して誤り訂正符号を付加する補助符号化手段を更に備え、
- 前記置換手段は、前記符号化データの一部を前記誤り訂正符号が付加された補助データに置換して、置換ユーザデータを生成する
- ことを特徴とする請求の範囲第1項に記載の情報生成装置。
- [4] 前記補助データによって、前記ユーザデータを暗号化することで暗号化されたユーザデータを生成する暗号化手段を更に備え、
- 前記符号化手段は、前記暗号化されたユーザデータに対して誤り訂正符号を付加して、符号化データを生成し、
- 前記位置情報生成手段は、前記位置情報を、前記暗号化されたユーザデータに基づいて生成する
- ことを特徴とする請求の範囲第1項に記載の情報生成装置。
- [5] 前記位置情報生成手段は、前記位置情報を、前記ユーザデータに加えて鍵情報

に基づいて生成することを特徴とする請求の範囲第1項に記載の情報生成装置。

- [6] 前記位置情報を用いて、前記補助データを変更する補助データ変更手段を更に備えることを特徴とする請求の範囲第1項に記載の情報生成装置。

- [7] ユーザデータの一部を、前記ユーザデータに関連するデータであって、前記ユーザデータとは異なる用途で用いられる補助データに置換して、置換ユーザデータを生成する情報生成装置であって、

前記ユーザデータに対して誤り訂正符号を付加して、符号化データを生成する符号化手段と、

前記補助データを変更補助データに変更するための変更情報を、前記ユーザデータに基づいて生成する変更情報生成手段と、

前記変更情報を用いて、前記補助データを変更補助データに変更する補助データ変更手段と、

前記符号化データの一部を、前記変更補助データに置換して、前記置換ユーザデータを生成する置換手段と

を備えることを特徴とする情報生成装置。

- [8] 請求の範囲第1項に記載の情報生成装置によって生成された置換ユーザデータが記録されていることを特徴とする記録媒体。

- [9] 請求の範囲第7項に記載の情報生成装置によって生成された置換ユーザデータが記録されていることを特徴とする記録媒体。

- [10] 請求の範囲第1項に記載の情報生成装置によって生成された置換ユーザデータを再生する情報再生装置であって、

前記置換ユーザデータを、前記誤り訂正符号を用いて、前記ユーザデータに復号する復号手段と、

前記位置情報を、前記復号されたユーザデータに基づいて生成する第2位置情報生成手段と、

前記第2位置情報生成手段によって生成された前記位置情報に基づいて、前記置換ユーザデータから前記補助データを抽出する抽出手段と

を備えることを特徴とする情報再生装置。

- [11] 請求の範囲第7項に記載の情報生成装置によって生成された置換ユーザデータを再生する情報再生装置であって、
- 前記置換ユーザデータから、前記変更補助データを抽出する抽出手段と、
- 前記置換ユーザデータを、前記誤り訂正符号を用いて、前記ユーザデータに復号する復号手段と、
- 前記変更情報を、前記復号されたユーザデータに基づいて生成する第2変更情報生成手段と、
- 前記第2変更情報生成手段によって生成された前記変更情報に基づいて、前記変更補助データを前記補助データに再変更する再変更手段と
- を備えることを特徴とする情報再生装置。
- [12] ユーザデータの一部を、前記ユーザデータに関連するデータであって、前記ユーザデータとは異なる用途で用いられる補助データに置換して、置換ユーザデータを生成する情報生成方法であって、
- 前記ユーザデータに対して誤り訂正符号を付加して、符号化データを生成する符号化工程と、
- 前記符号化データにおける前記補助データに置換されるデータの位置を示す位置情報を、前記ユーザデータに基づいて生成する位置情報生成工程と、
- 前記符号化データの一部を、前記位置情報に基づいて前記補助データに置換して、前記置換ユーザデータを生成する置換工程と
- を備えることを特徴とする情報生成方法。
- [13] ユーザデータの一部を、前記ユーザデータに関連するデータであって、前記ユーザデータとは異なる用途で用いられる補助データに置換して、置換ユーザデータを生成する情報生成方法であって、
- 前記ユーザデータに対して誤り訂正符号を付加して、符号化データを生成する符号化工程と、
- 前記補助データを変更補助データに変更するための変更情報を、前記ユーザデータに基づいて生成する変更情報生成工程と、
- 前記変更情報を用いて、前記補助データを変更補助データに変更する補助デー

タ変更工程と、

前記符号化データの一部を、前記変更補助データに置換して、前記置換ユーザデータを生成する置換工程と

を備えることを特徴とする情報生成方法。

- [14] 請求の範囲第12項に記載の情報生成方法によって生成された置換ユーザデータを再生する情報再生方法であって、

前記置換ユーザデータを、前記誤り訂正符号を用いて、前記ユーザデータに復号する復号工程と、

前記位置情報を、前記復号されたユーザデータに基づいて生成する第2位置情報生成工程と、

前記第2位置情報生成工程において生成された前記位置情報に基づいて、前記置換ユーザデータから前記補助データを抽出する抽出工程と

を備えることを特徴とする情報再生方法。

- [15] 請求の範囲第13項に記載の情報生成方法によって生成された置換ユーザデータを再生する情報再生方法であって、

前記置換ユーザデータから、前記変更補助データを抽出する抽出工程と、

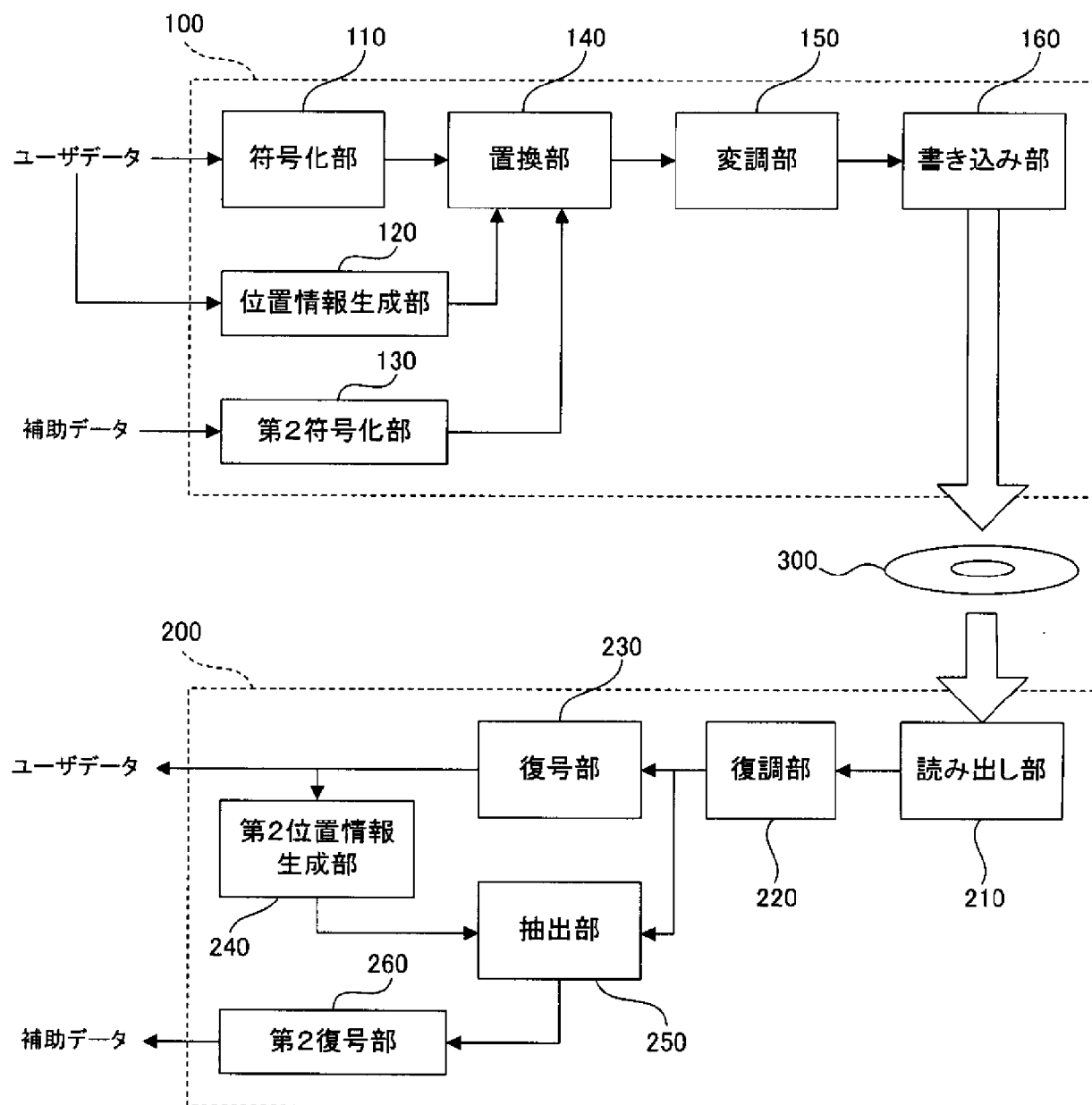
前記置換ユーザデータを、前記誤り訂正符号を用いて、前記ユーザデータに復号する復号工程と、

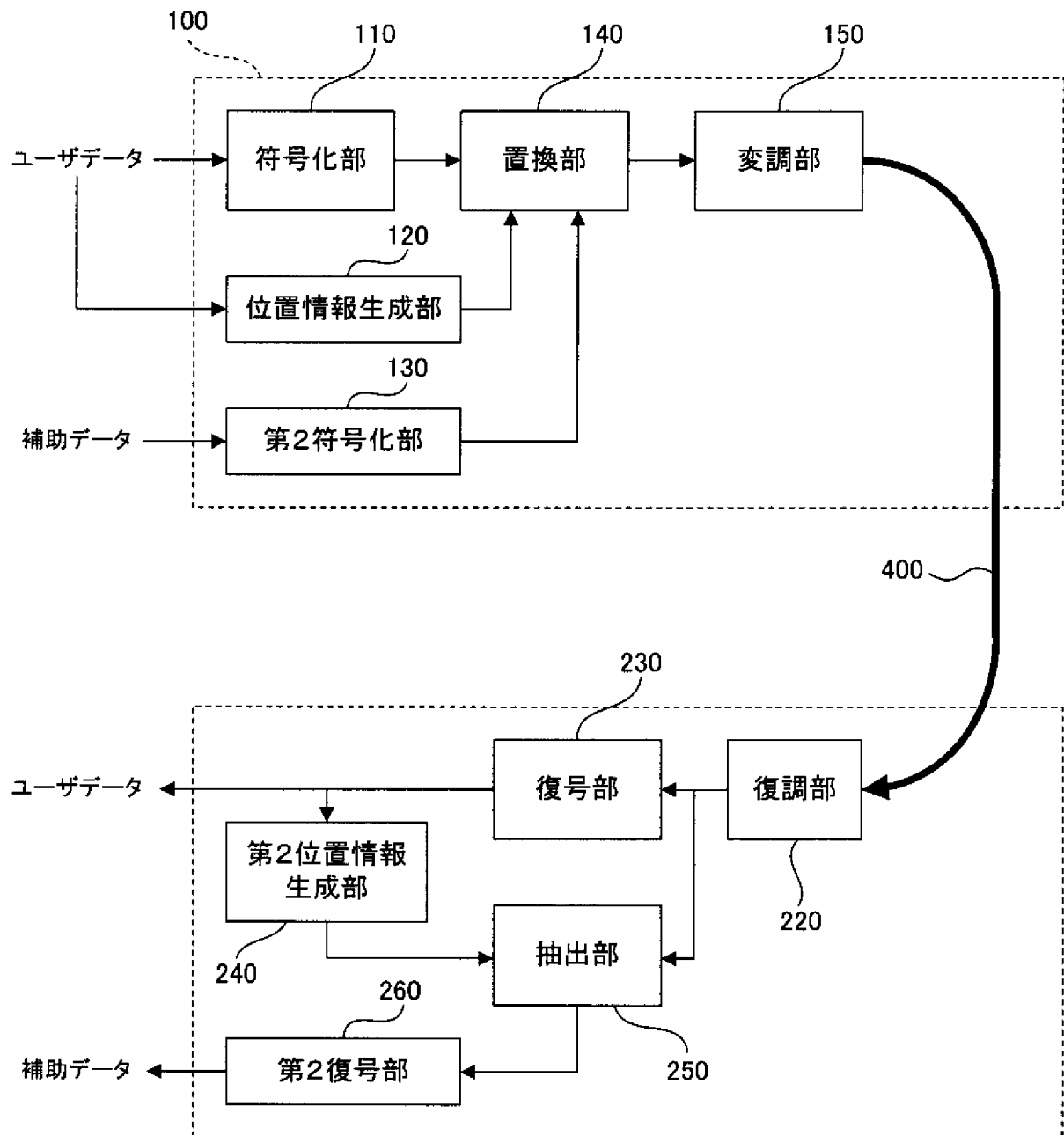
前記変更情報を、前記復号されたユーザデータに基づいて生成する第2変更情報生成工程と、

前記第2変更情報生成工程において生成された前記変更情報に基づいて、前記変更補助データを前記補助データに再変更する再変更工程と

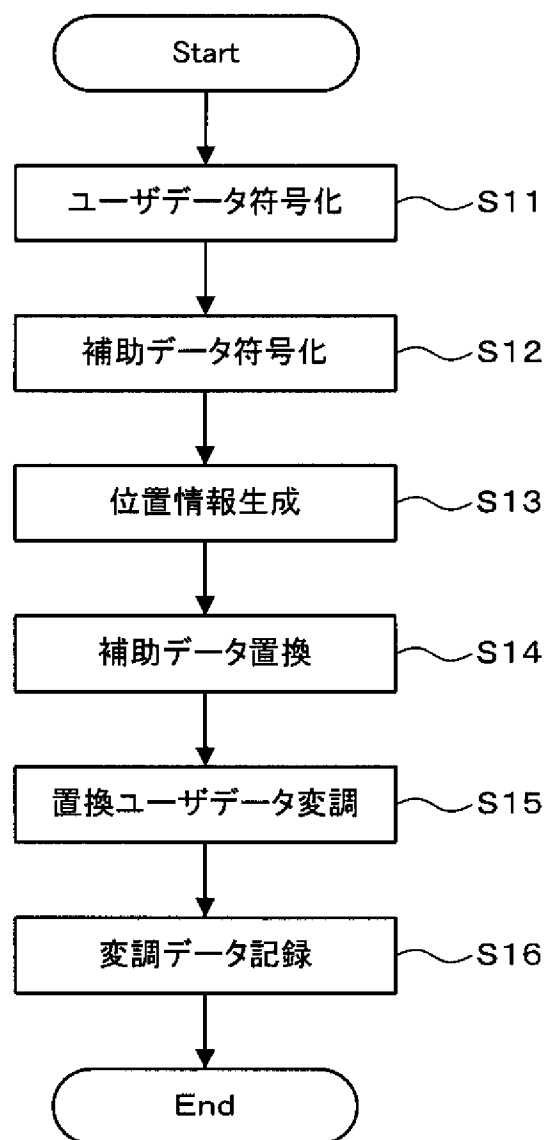
を備えることを特徴とする情報再生方法。

[図1]

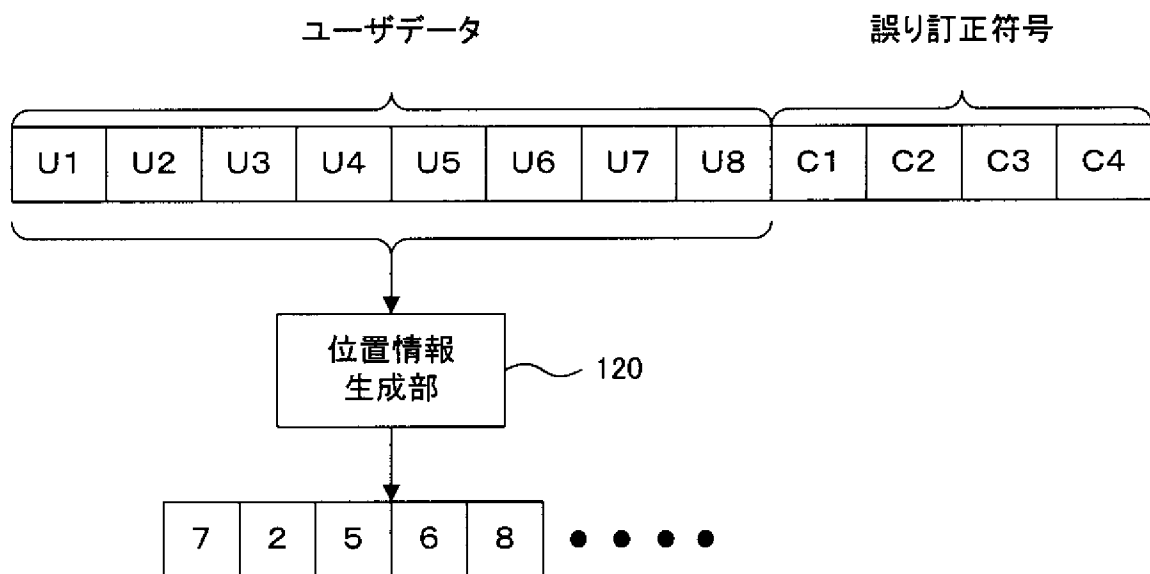




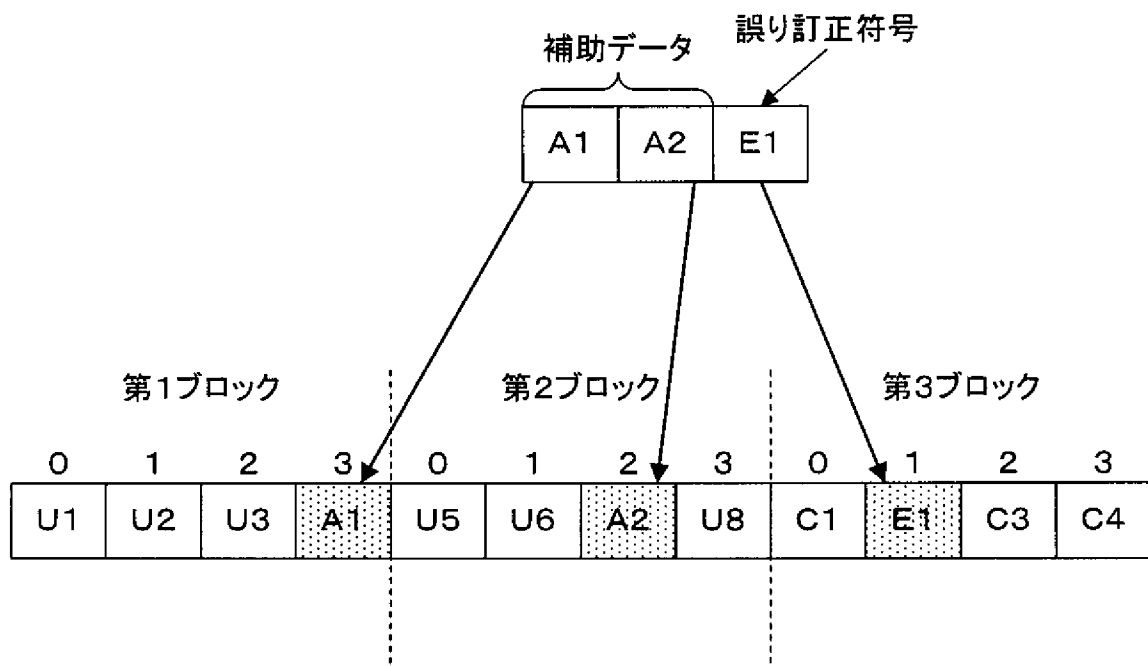
[図3]



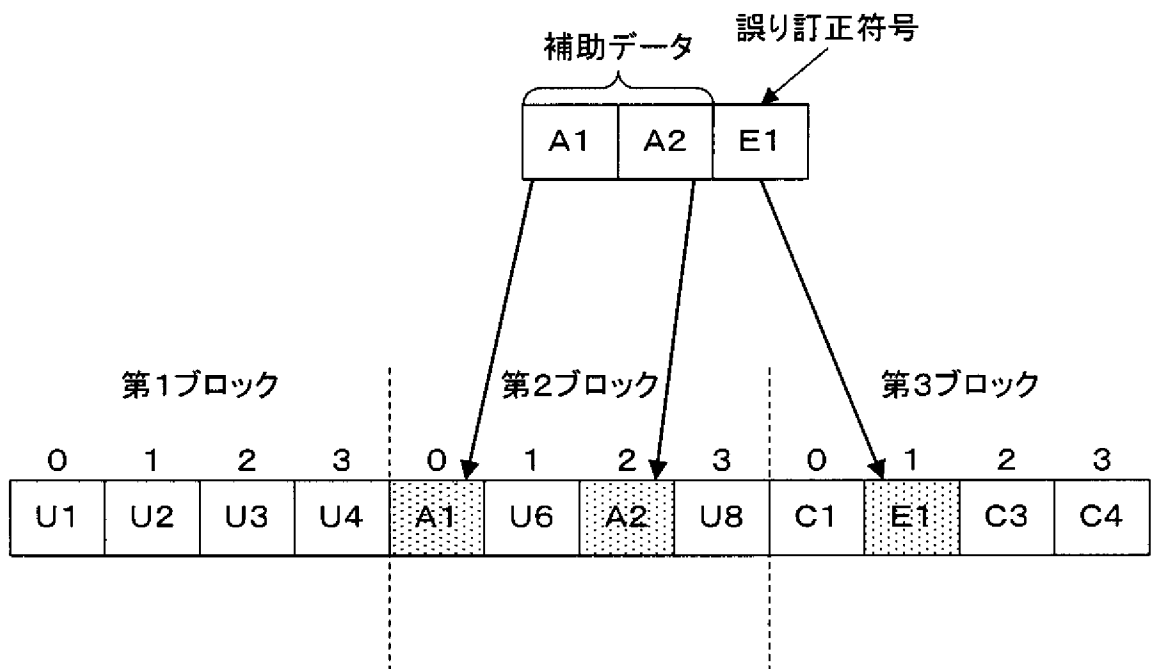
[図4]



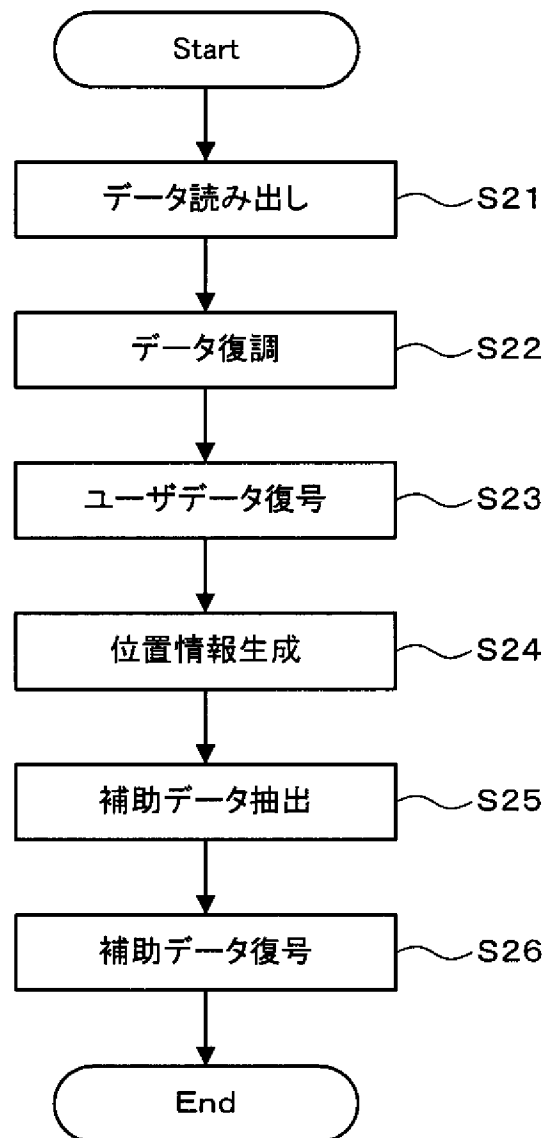
[図5]



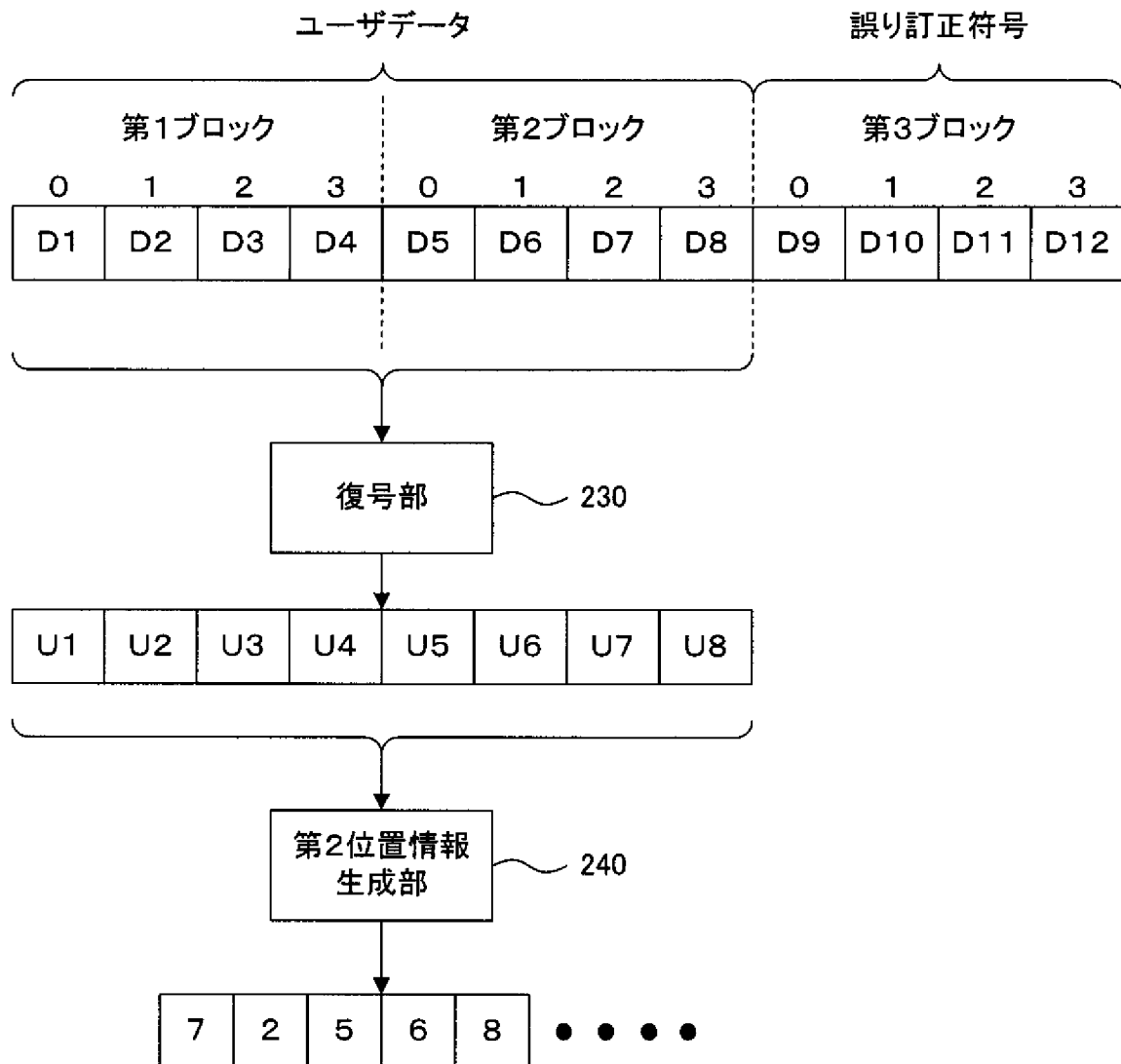
[図6]



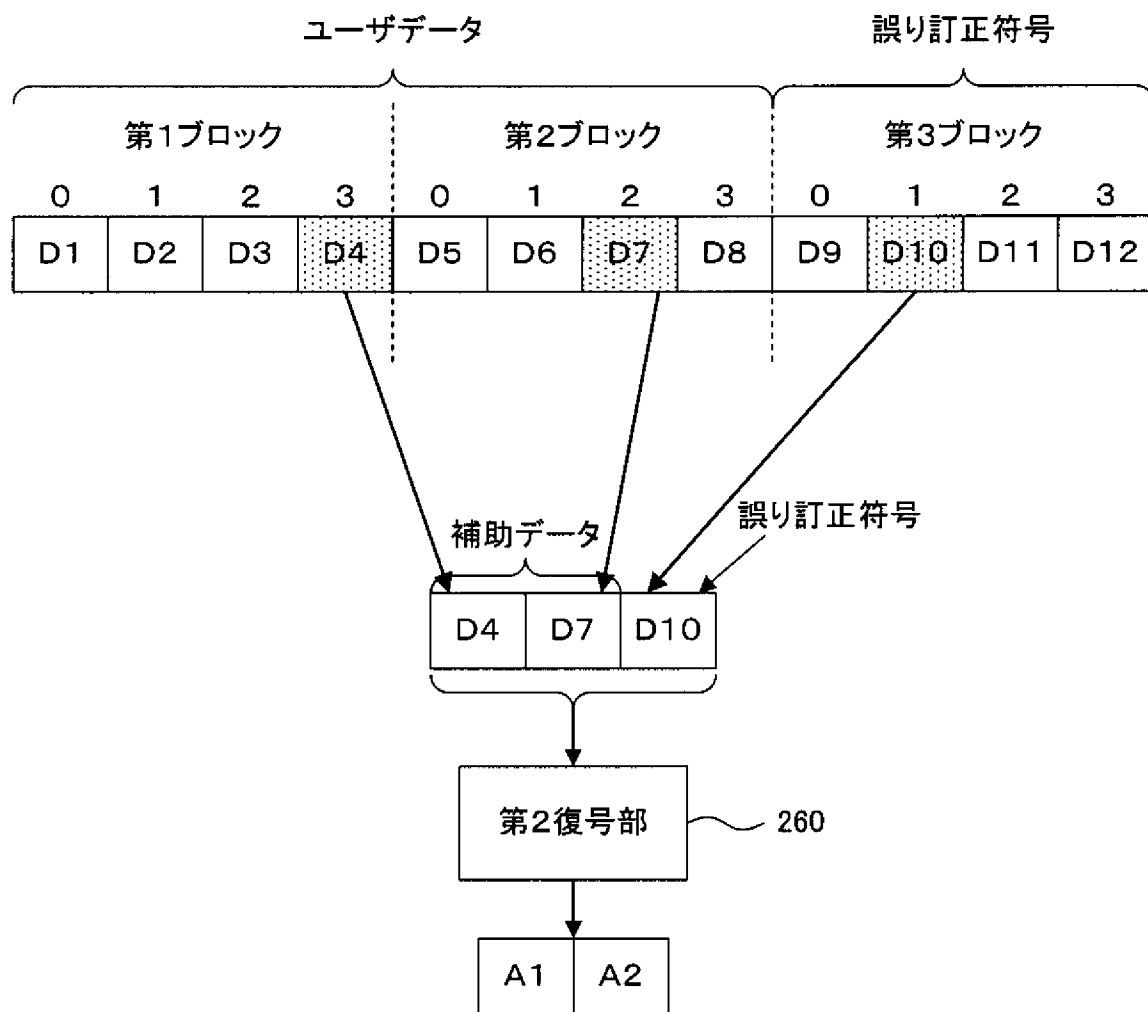
[図7]



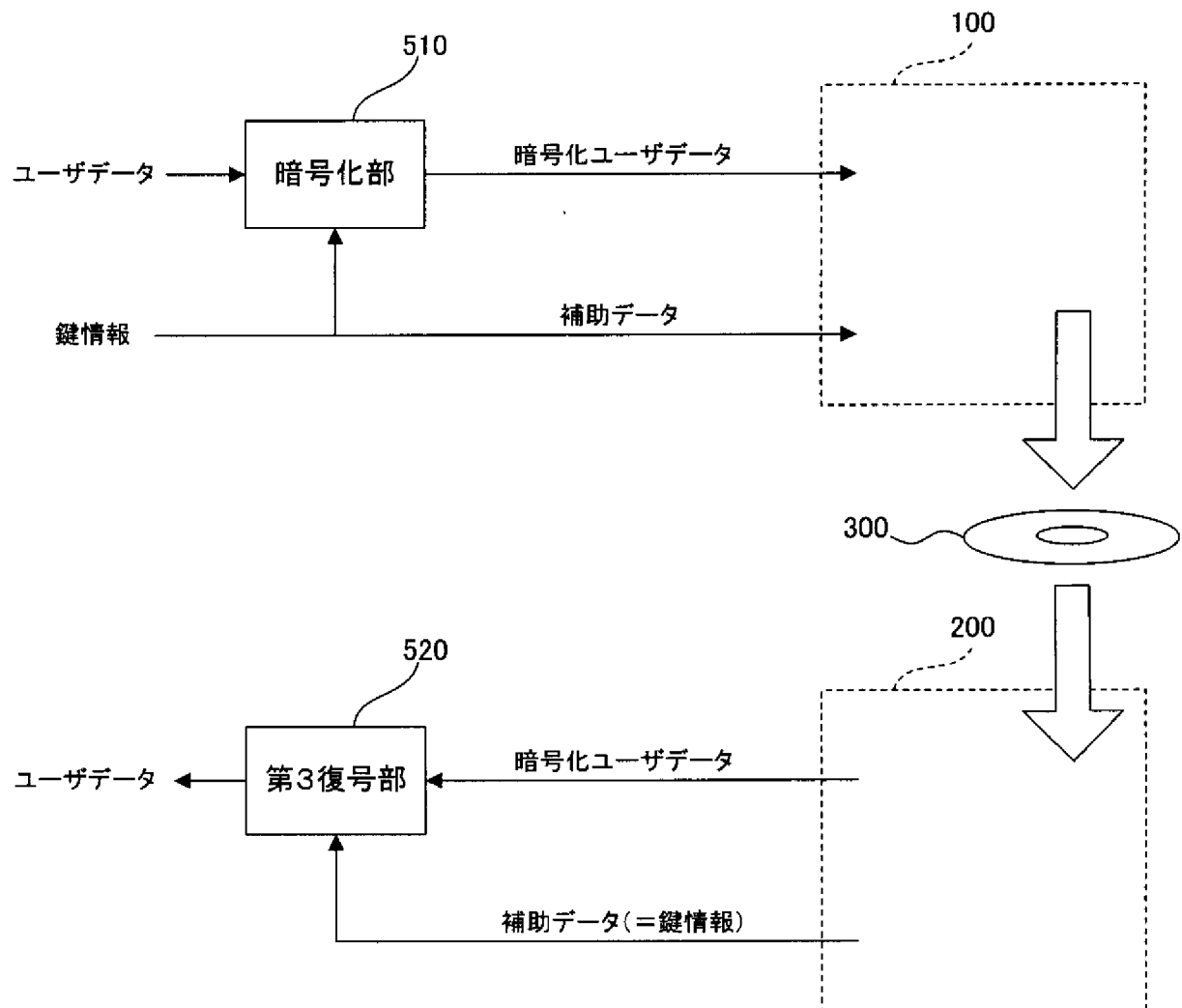
[図8]



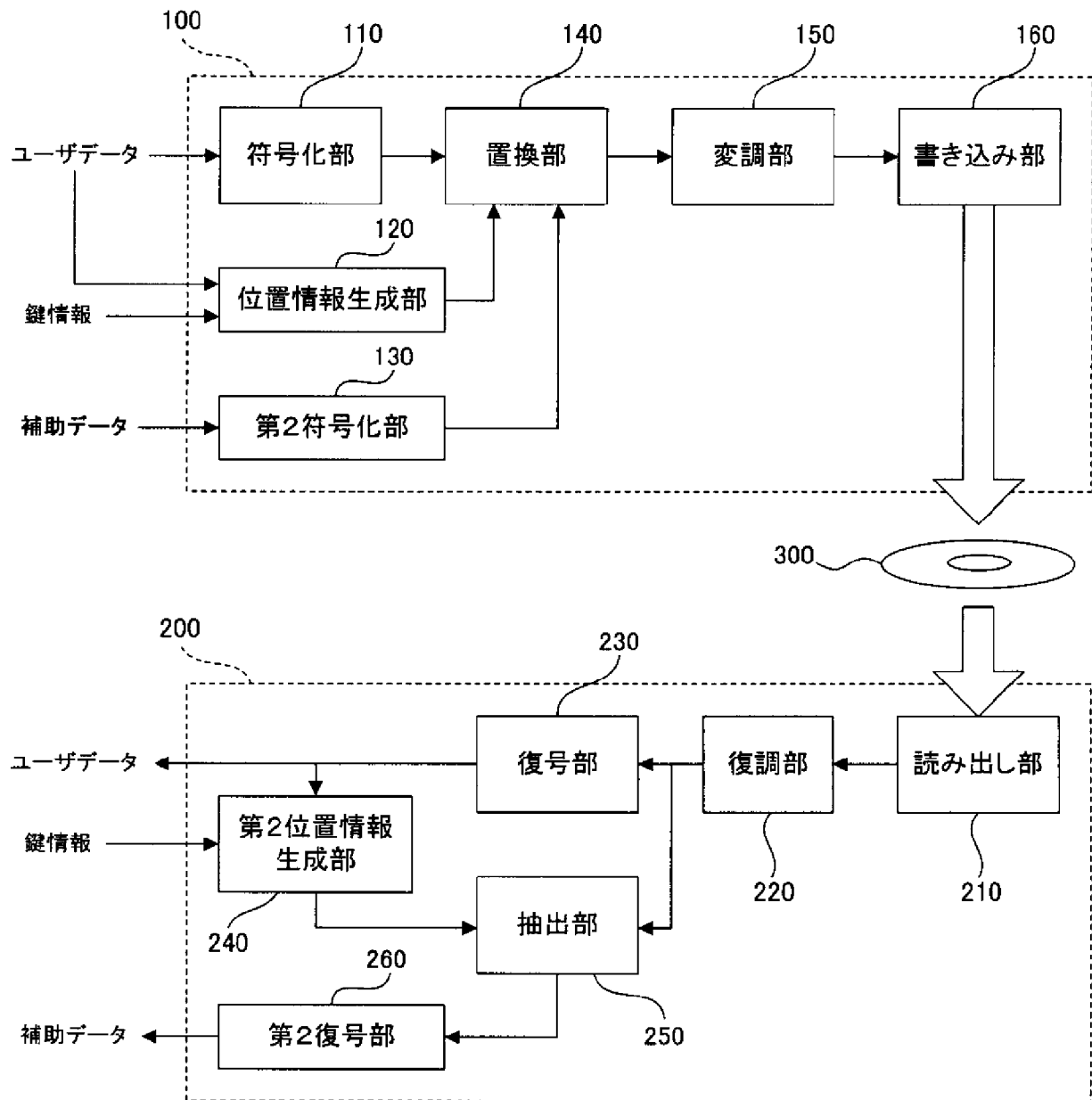
[図9]



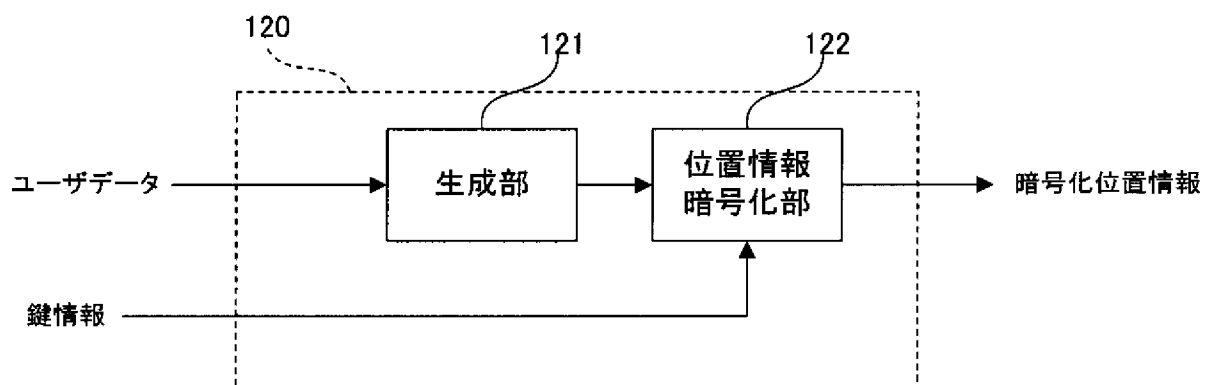
[図10]



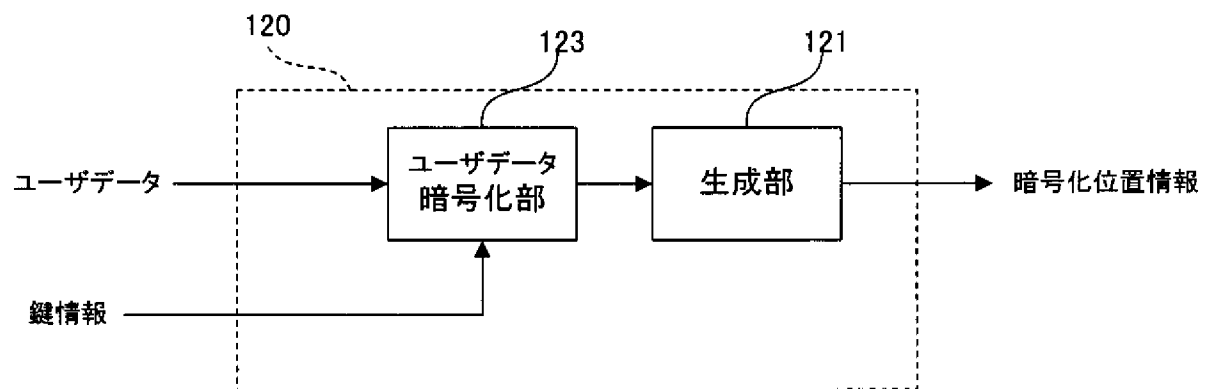
[図11]



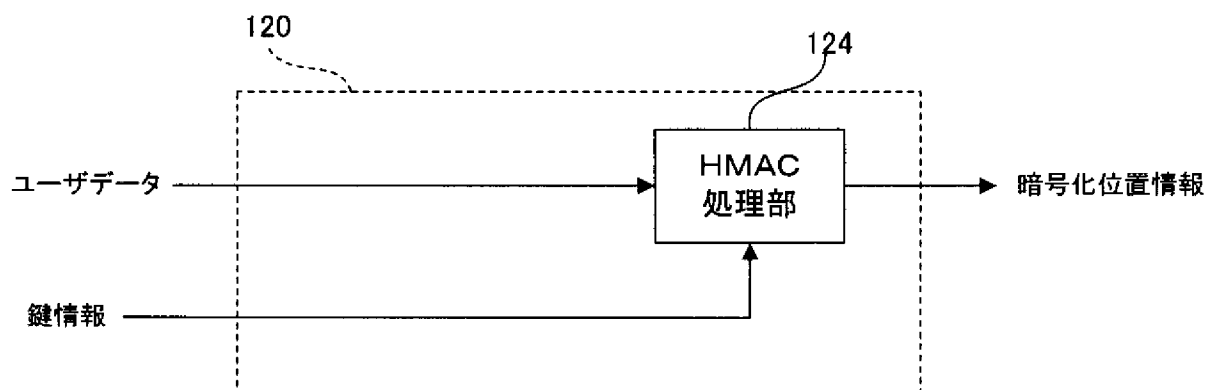
[図12]



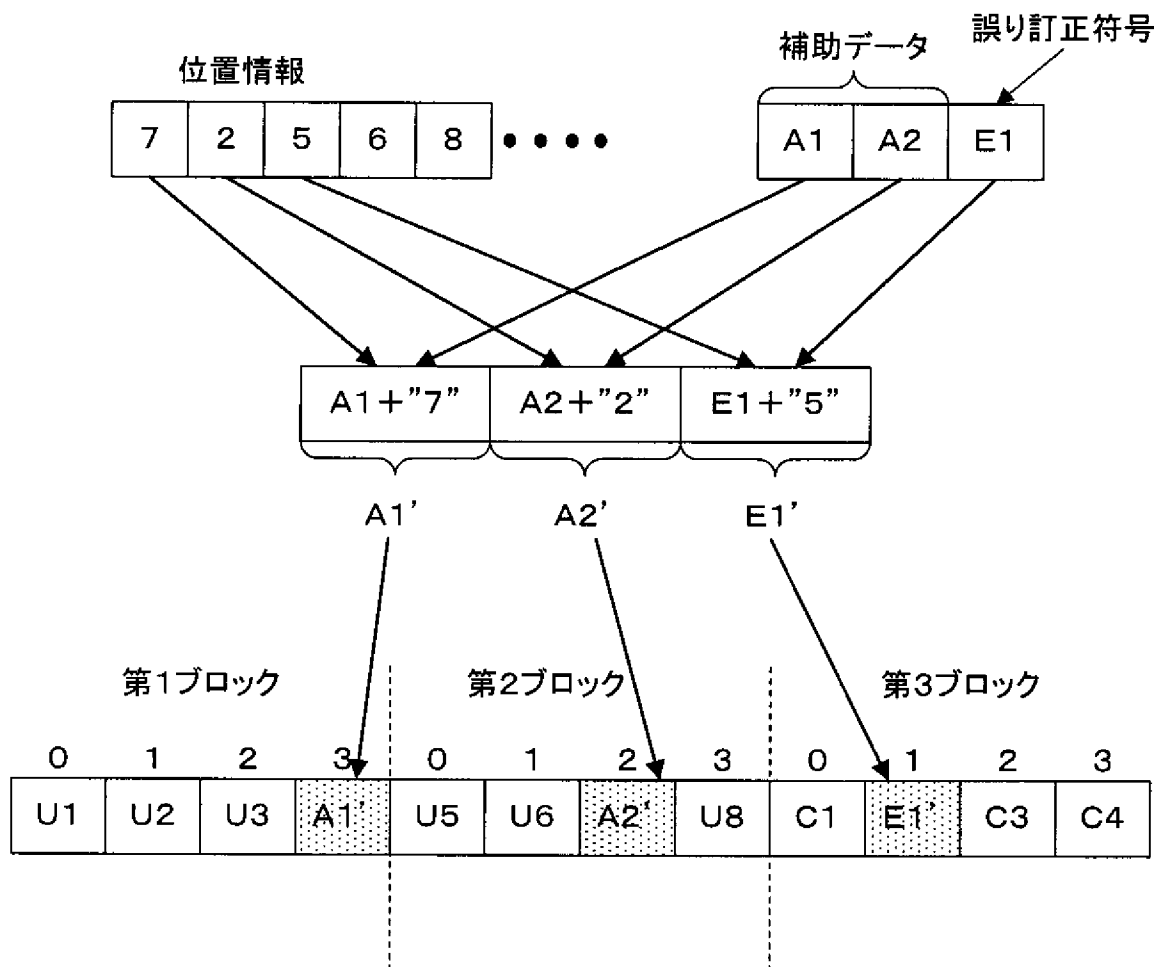
[図13]



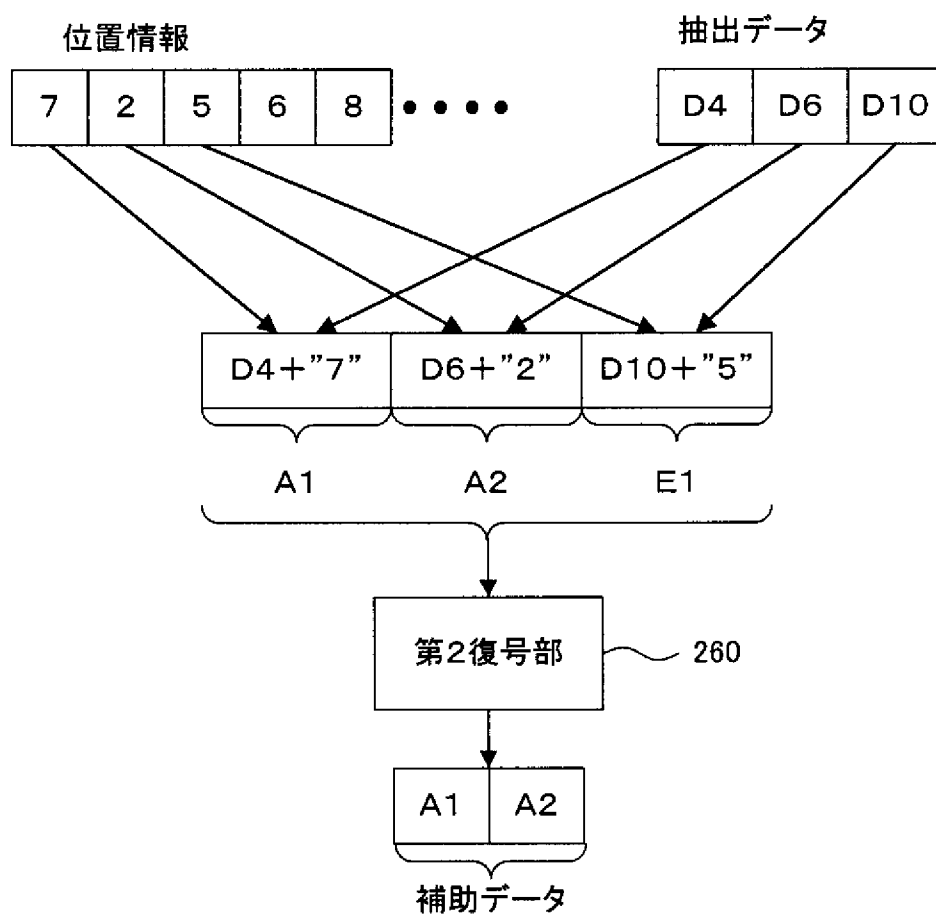
[図14]



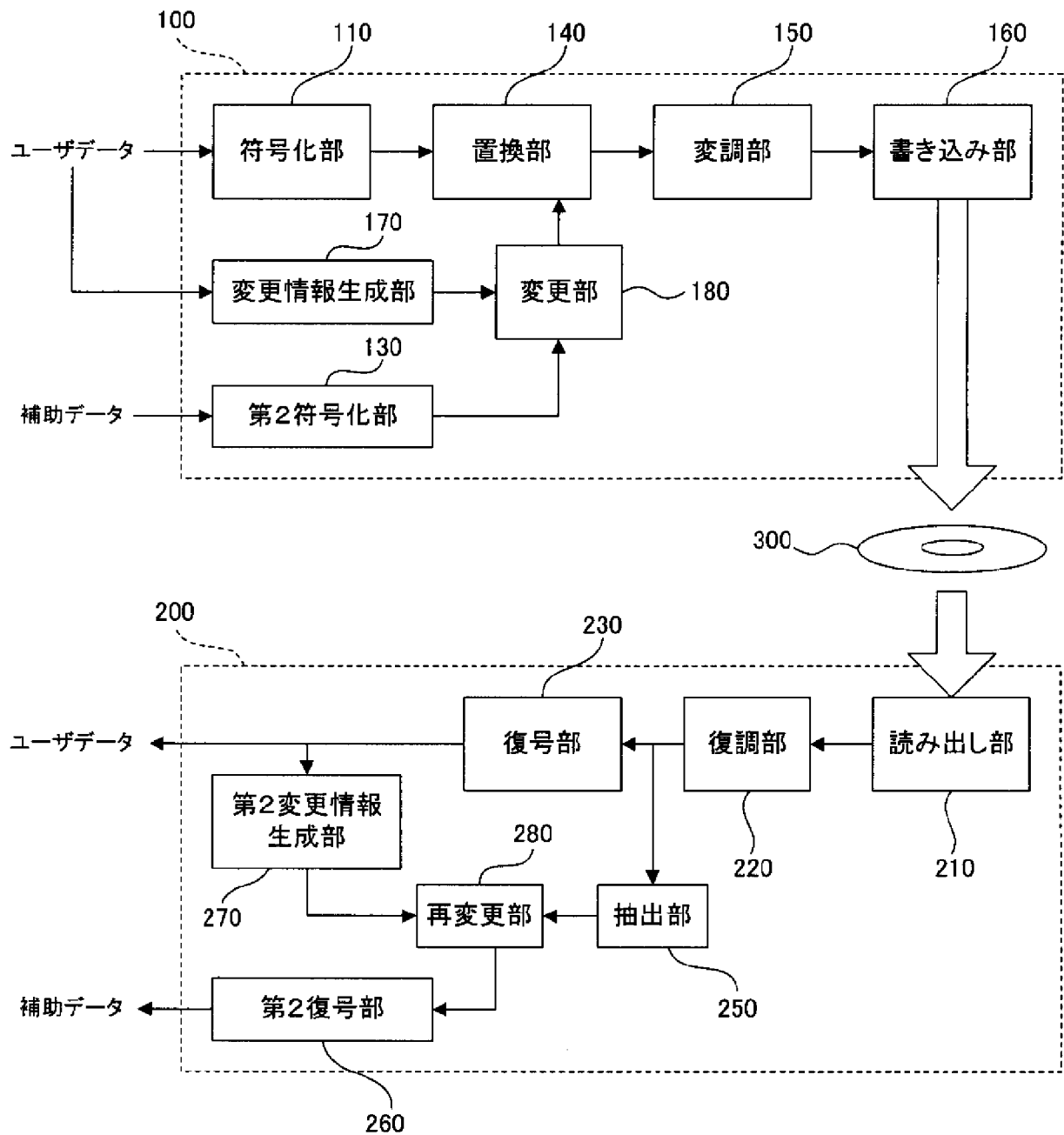
[図15]



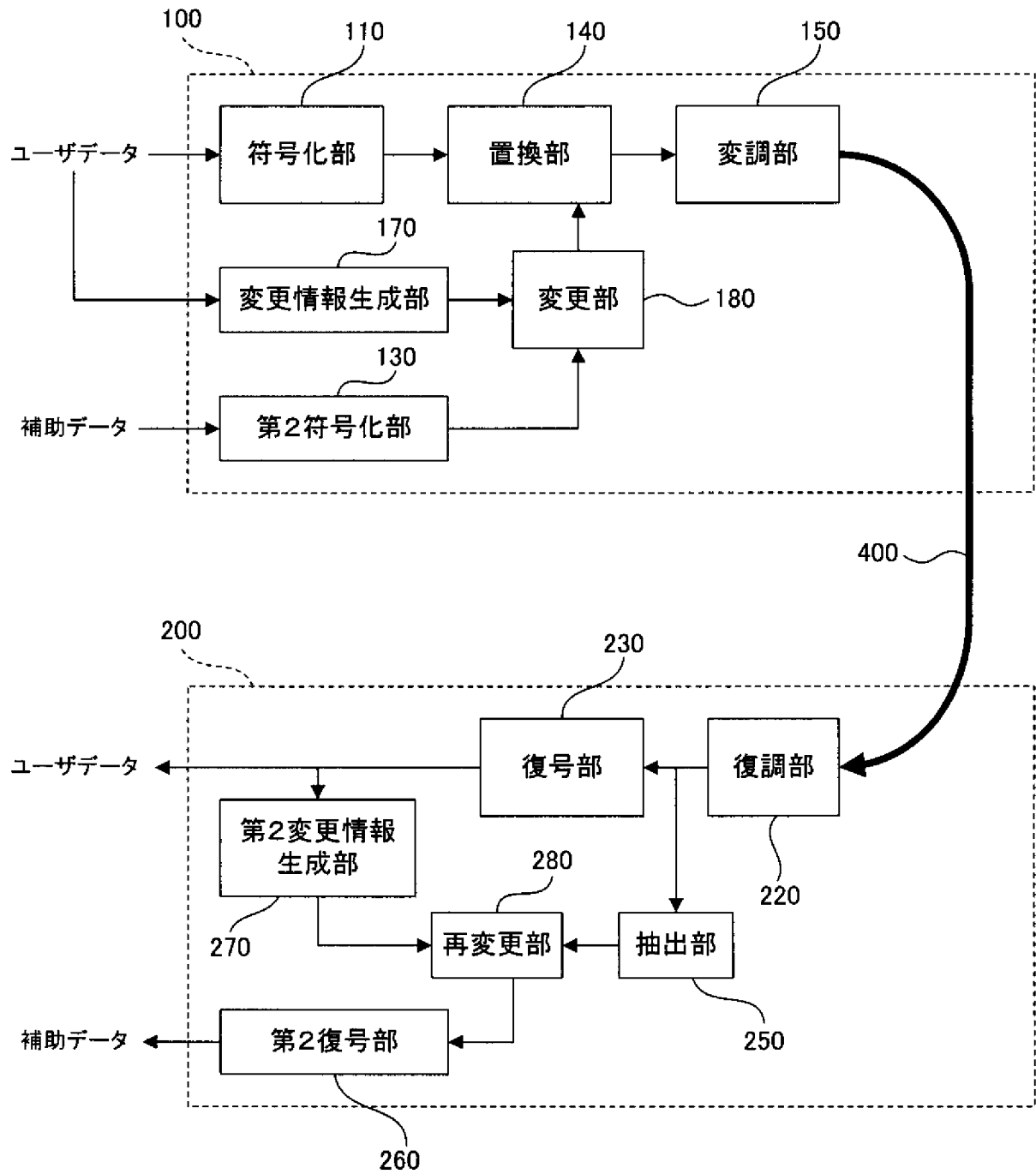
[図16]



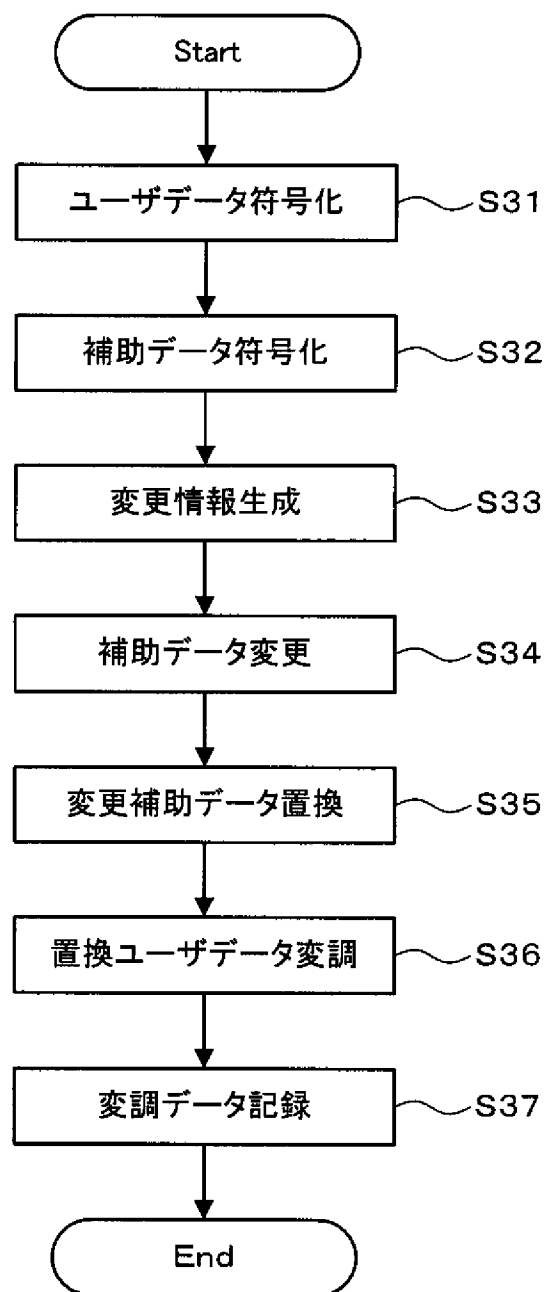
[図17]



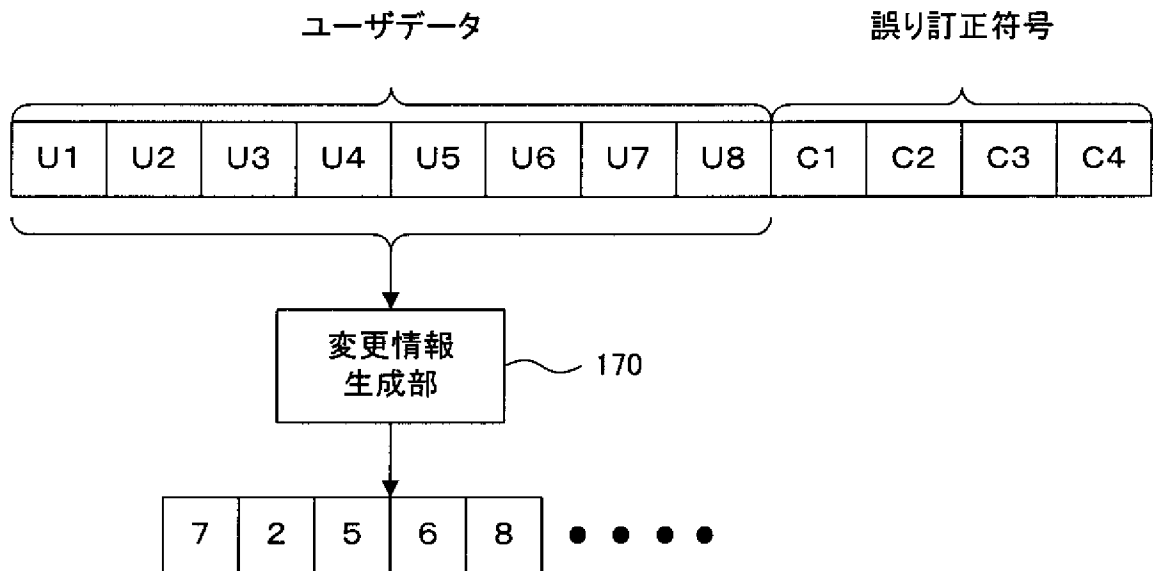
[図18]



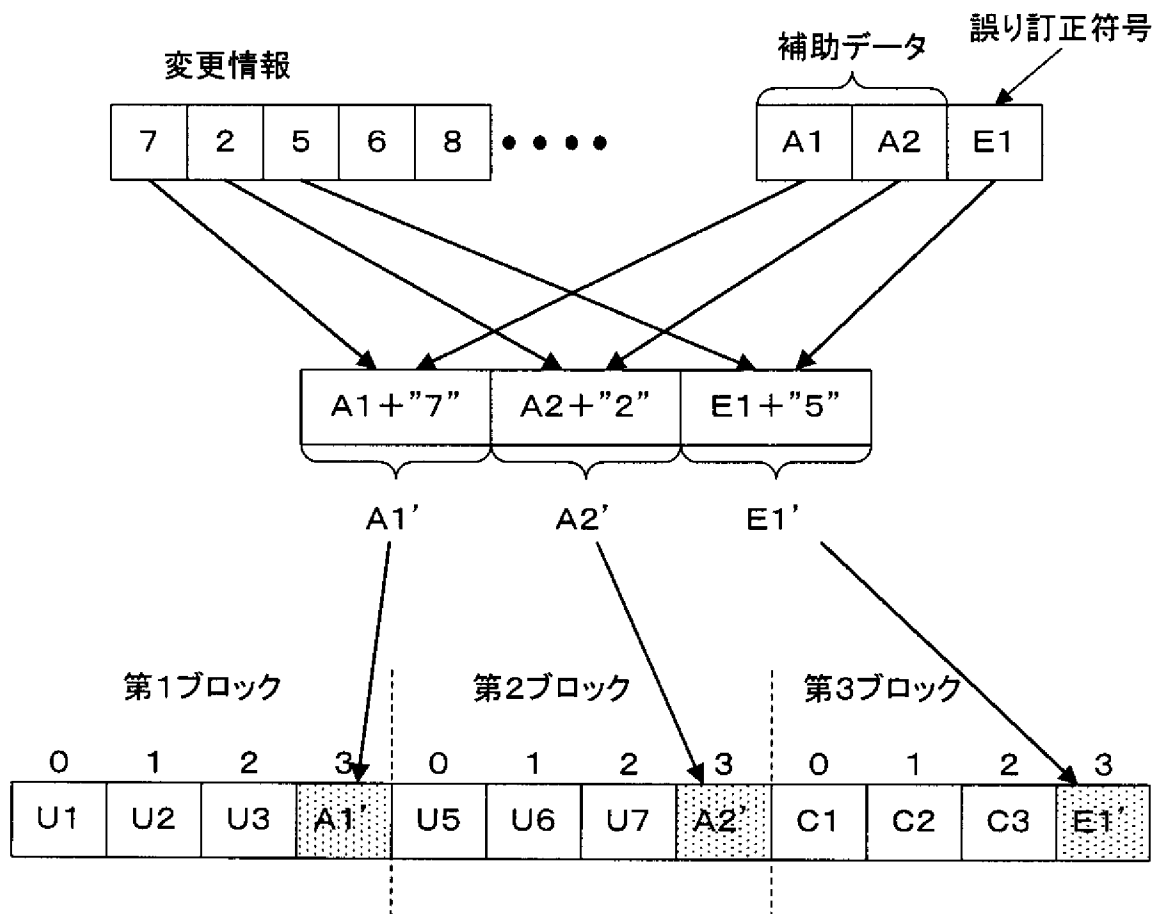
[図19]



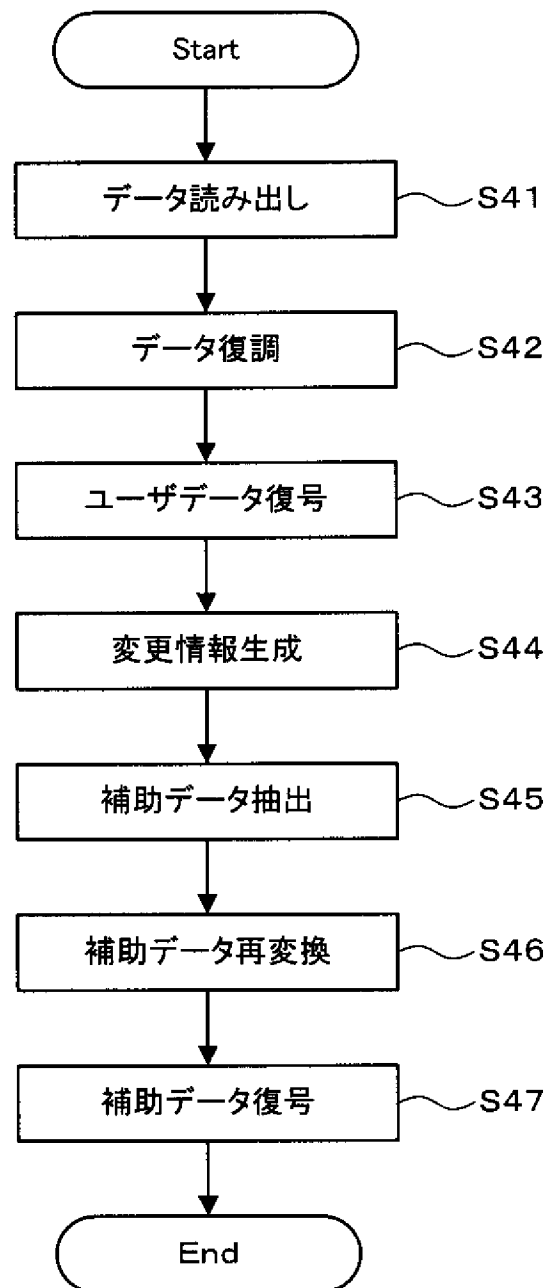
[図20]



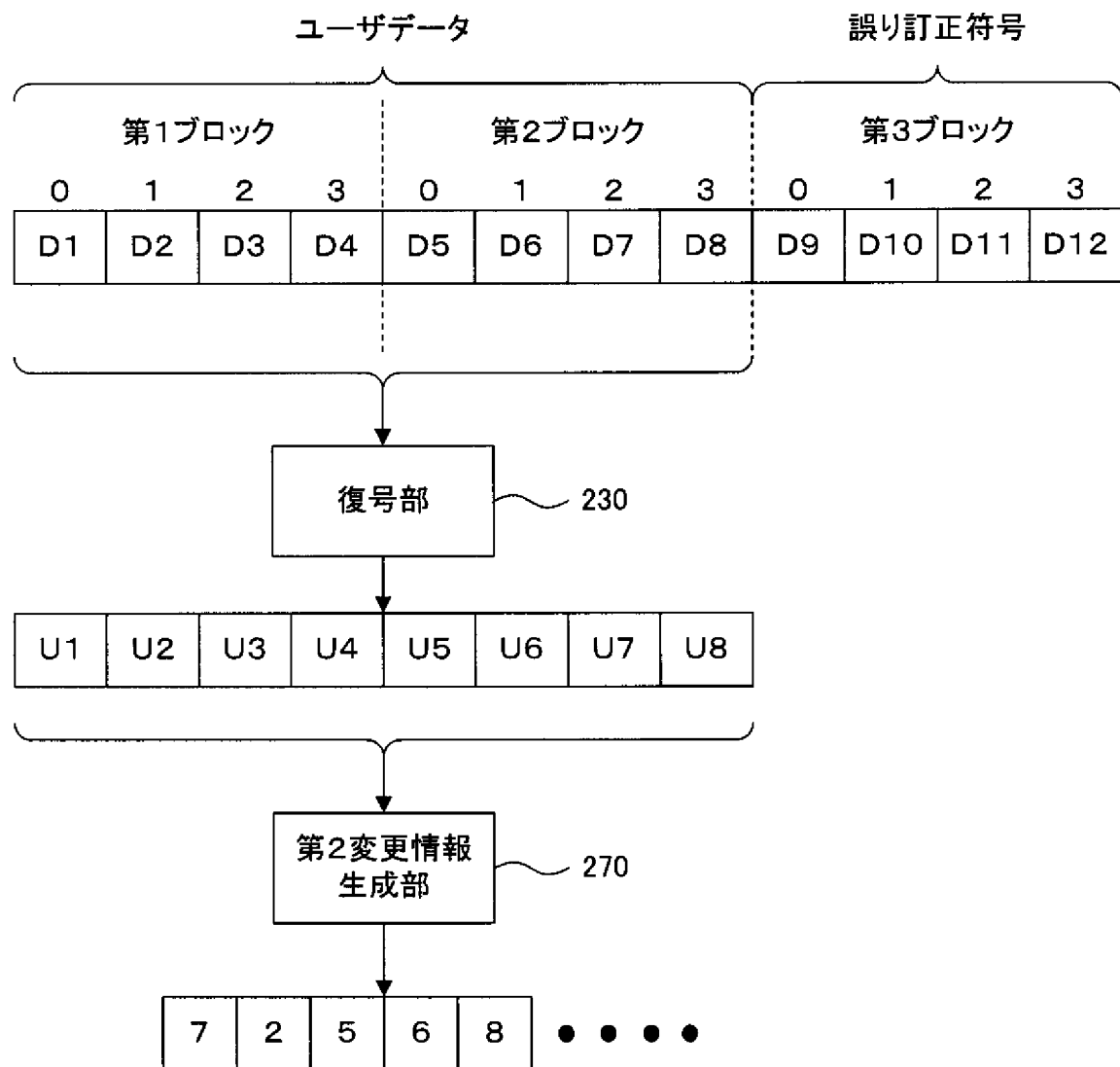
[図21]



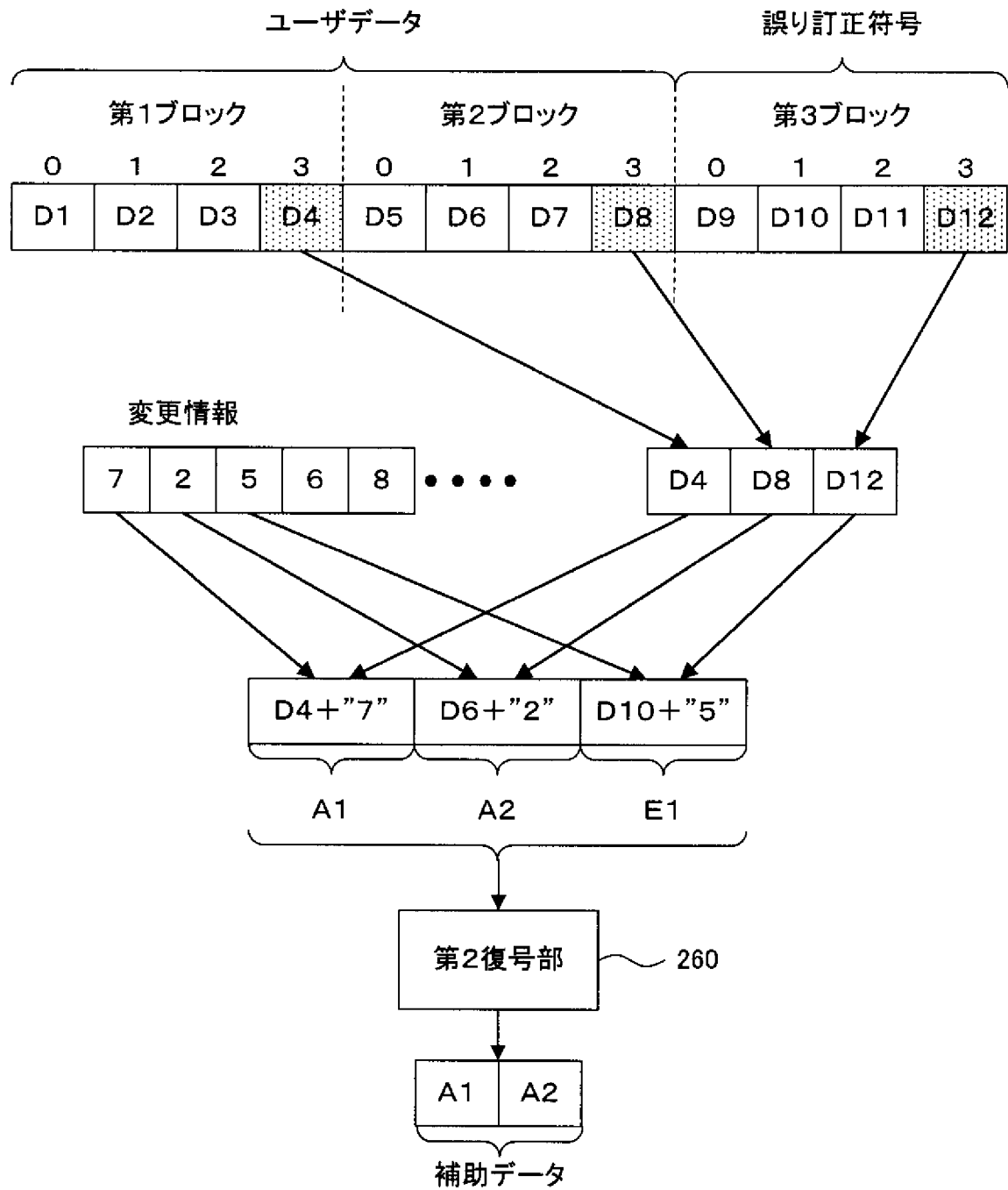
[図22]



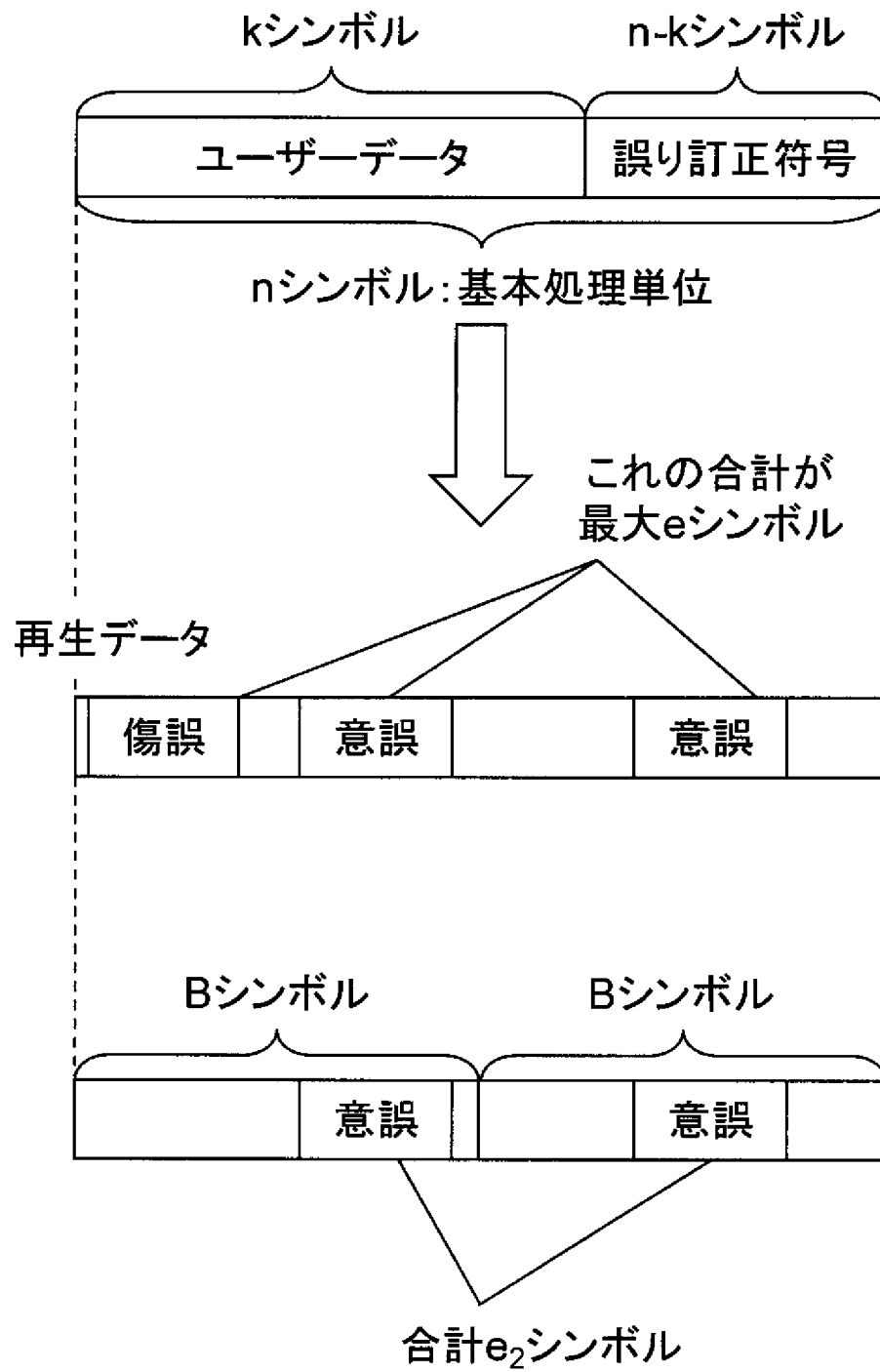
[図23]



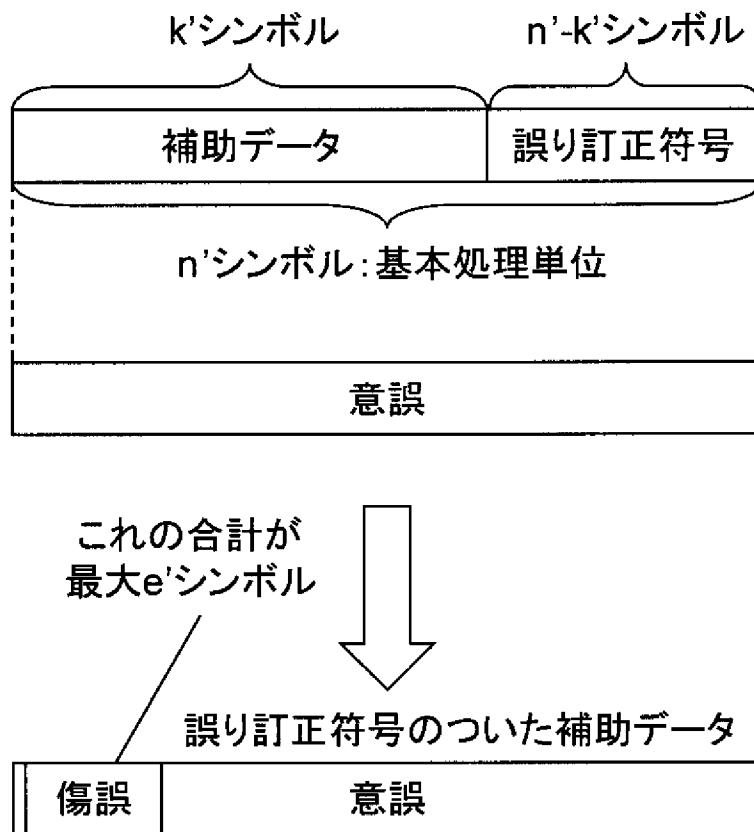
[図24]



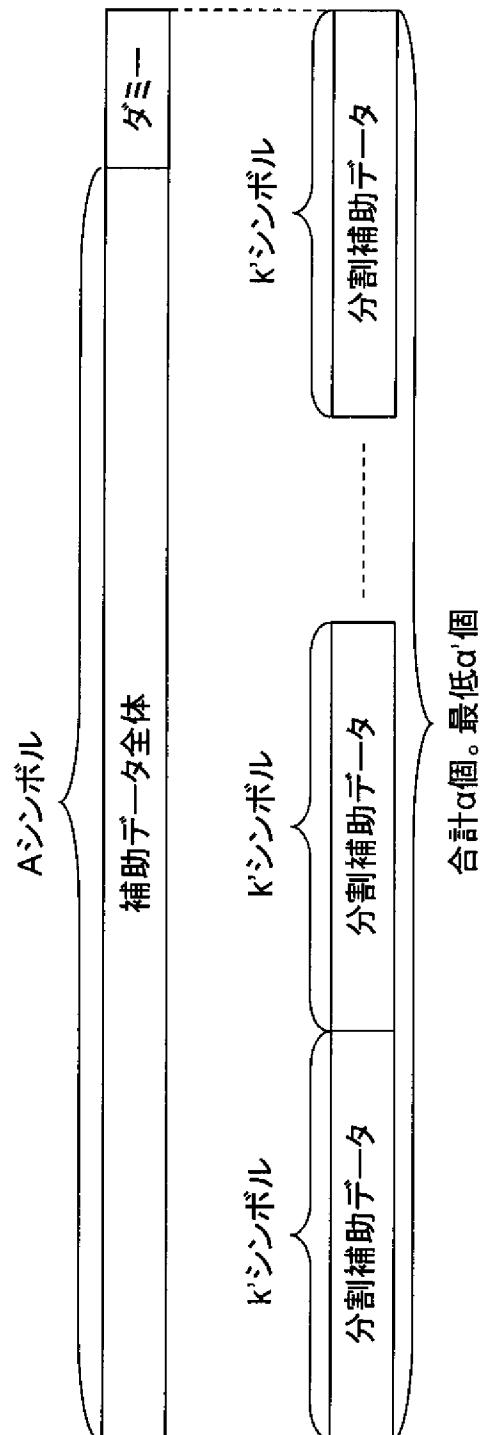
[図25]



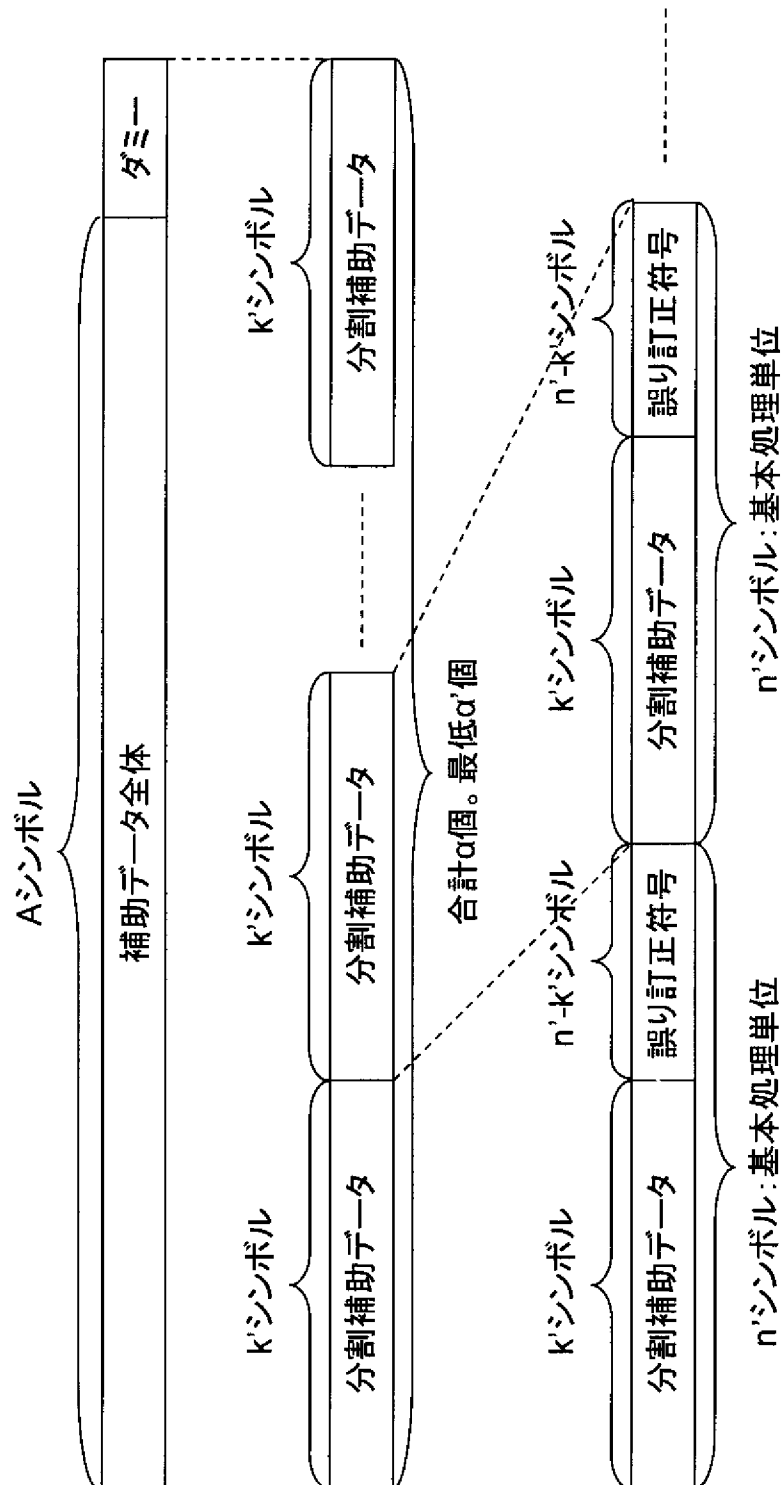
[図26]



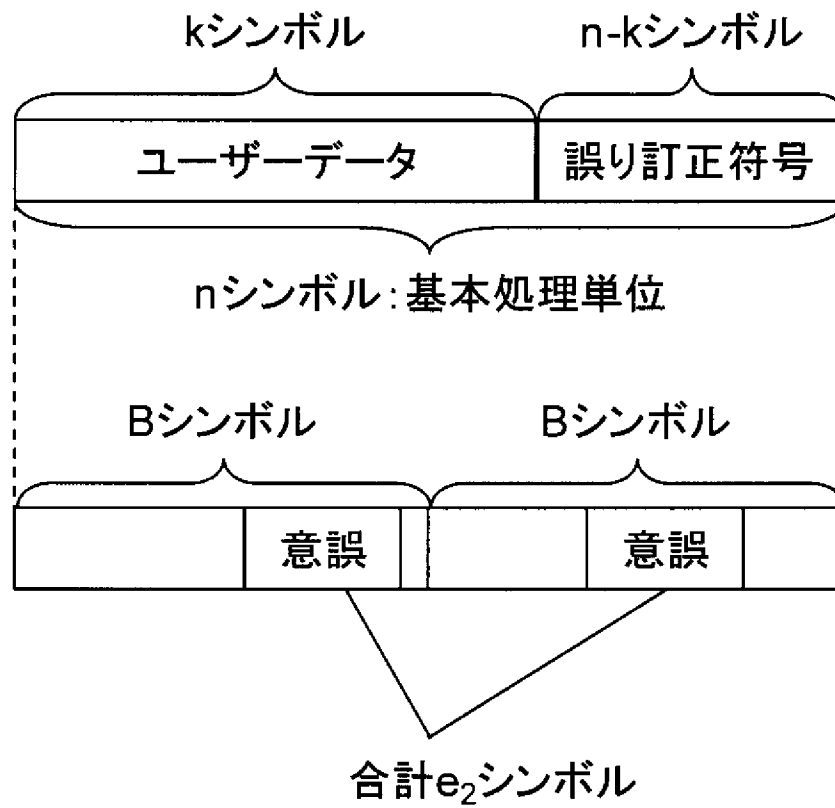
[図27]



[図28]



[図29]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2008/059930

A. CLASSIFICATION OF SUBJECT MATTER

G11B20/18(2006.01)i, G06F12/14(2006.01)i, G09C5/00(2006.01)i, G11B20/10(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G11B20/18, G06F12/14, G09C5/00, G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2008
Kokai Jitsuyo Shinan Koho	1971-2008	Toroku Jitsuyo Shinan Koho	1994-2008

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-198831 A (Toshiba Corp.), 11 July, 2003 (11.07.03), Par. Nos. [0120] to [0131], [0145] to [0161]; Figs. 22, 25, 27 (Family: none)	1-6, 8, 10-12, 14, 15
Y	JP 2000-224411 A (International Business Machines Corp.), 11 August, 2000 (11.08.00), Par. Nos. [0021] to [0024]; Fig. 4 & US 6564322 B1	1-6, 8, 10-12, 14, 15 7, 9, 13
X		
A	JP 11-213554 A (Toshiba Corp.), 06 August, 1999 (06.08.99), Full text; all drawings & US 6556679 B1	1-15

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
08 July, 2008 (08.07.08)

Date of mailing of the international search report
22 July, 2008 (22.07.08)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2008/059930

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-057058 A (Toshiba Corp.), 25 February, 2000 (25.02.00), Full text; all drawings & US 2002/0073037 A1 & EP 0978840 A1	1-15

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G11B20/18(2006.01)i, G06F12/14(2006.01)i, G09C5/00(2006.01)i, G11B20/10(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. G11B20/18, G06F12/14, G09C5/00, G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 8 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 8 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 8 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2003-198831 A（株式会社東芝）2003.07.11, 段落【0120】－【0131】、【0145】－【0161】、 図22、図25、図27（ファミリーなし）	1－6, 8, 10－12, 14, 15
Y	JP 2000-224411 A（インターナショナル・ビジネス・マシーンズ・ コーポレーション）2000.08.11, 段落【0021】－【0024】、図4 & US 6564322 B1	1－6, 8, 10－12, 14, 15
X		7, 9, 13

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

0 8 . 0 7 . 2 0 0 8

国際調査報告の発送日

2 2 . 0 7 . 2 0 0 8

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

堀 洋介

5 Q

3 9 9 6

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 9 1

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 11-213554 A (株式会社東芝) 1999.08.06, 全文、全図 & US 6556679 B1	1 - 1 5
A	JP 2000-057058 A (株式会社東芝) 2000.02.25, 全文、全図 & US 2002/0073037 A1 & EP 0978840 A1	1 - 1 5