(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5884412号
(P5884412)
(45)発行日　平成28年3月15日(2016.3.15)　(24)登録日　平成28年2月19日(2016.2.19)

(51)Int.Cl.　　F I
G09C 1/00 (2006.01)　　G09C 1/00 610A
H03M 7/42 (2006.01)　　H03M 7/42

請求項の数 11　(全 47 頁)

(21)出願番号　特願2011-242830(P2011-242830)
(22)出願日　平成23年11月4日(2011.11.4)
(65)公開番号　特開2013-97332(P2013-97332A)
(43)公開日　平成25年5月20日(2013.5.20)
審査請求日　平成26年7月4日(2014.7.4)

前置審査

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　片岡　正弘
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　古賀　奨
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　大西　照彦
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
最終頁に続く

(54)【発明の名称】変換プログラム、変換装置、変換方法、および変換システム

(57)【特許請求の範囲】
【請求項１】
コンピュータに、
変換対象データの取得に応じ、第１の種類の符号情報群に含まれる第１の種類の符号情報のそれぞれと第２の種類の符号情報群に含まれる第２の種類の符号情報の何れかと関連付けた辞書情報を記憶部に記憶し、
前記記憶部から前記辞書情報を読み出し、前記辞書情報において、各前記第１の種類の符号情報と関連付けられる各前記第２の種類の符号情報を、入力された入力情報を第１のシードとする第１のハッシュ関数のハッシュ値を第２のシードとする第２のハッシュ関数のハッシュ値により変更して前記辞書情報を更新し、
前記変換対象データ内に、ある第１の種類の符号情報が含まれる場合に、前記ある第１の種類の符号情報を、前記更新された前記辞書情報において前記ある第１の種類の符号情報と関連付けて前記記憶部に記憶された第２の種類の符号情報に変換する、
処理を実行させることを特徴とする変換プログラム。
【請求項２】
さらに、
前記コンピュータに、
前記記憶部から前記辞書情報を読み出し、前記変換対象データ内に、前記辞書情報に未登録の第１の種類の符号情報が含まれる場合に、前記辞書情報に未登録の第１の種類の符号情報及び該未登録の第１の種類の符号情報と関連付けられる第２の種類の符号情報を前

記辞書情報に登録し、前記入力情報に応じて、該未登録の第１の種類の符号情報と関連付けられる第２の種類の符号情報を変更して前記辞書情報を更新し、
前記変換対象データ内に、ある第１の種類の符号情報が含まれる場合に、前記ある第１の種類の符号情報を、前記更新された前記辞書情報において前記ある第１の種類の符号情報と関連付けて前記記憶部に記憶された第２の種類の符号情報に変換する、
処理を実行させることを特徴とする請求項１に記載の変換プログラム。
【請求項３】
前記第１の種類の符号情報群に含まれる第１の種類の符号情報よりも、前記第２の種類の符号情報群に含まれる第２の種類の符号情報の方が、データサイズが大きいか小さいかの何れかである、
ことを特徴とする請求項１又は２に記載の変換プログラム。
【請求項４】
前記第１の種類の符号情報群に含まれる第１の種類の符号情報のそれぞれは、文字を示す情報であり、
前記第２の種類の符号情報群に含まれる第２の種類の符号情報のそれぞれは、圧縮符号を示す情報である、
ことを特徴とする請求項３に記載の変換プログラム。
【請求項５】
前記第１の種類の符号情報群に含まれる第１の種類の符号情報のそれぞれは、圧縮符号を示す情報であり、
前記第２の種類の符号情報群に含まれる第２の種類の符号情報のそれぞれは、文字を示す情報である、
ことを特徴とする請求項３に記載の変換プログラム。
【請求項６】
前記コンピュータに、
前記第１の種類の符号情報群に含まれる第１の種類の符号情報のそれぞれと、前記記憶部に記憶する前記辞書情報において関連付けた第２の種類の符号情報を、引数に前記入力情報を用いて所定のアルゴリズムの演算を行なった結果に応じて決定する、
処理を実行させることを特徴とする請求項１～５のいずれか１項に記載の変換プログラム。
【請求項７】
前記所定のアルゴリズムは、前記入力情報が示す値を所定値で除算した場合の余りの値を算出する処理である、
ことを特徴とする請求項６に記載の変換プログラム。
【請求項８】
コンピュータに、
所定の文字列を第１の種類の符号情報群に含め、該第１の種類の符号情報群に含まれる第１の種類の符号情報のそれぞれについて、入力された入力情報に応じて第２の種類の符号情報群に含まれる第２の種類の符号情報の何れかと関連付けて記憶部に記憶し、
前記記憶部において、各前記第１の種類の符号情報と関連付けられる各前記第２の種類の符号情報を、前記入力情報を第１のシードとする第１のハッシュ関数のハッシュ値を第２のシードとする第２のハッシュ関数のハッシュ値により変更し、
変換対象データ内に、前記所定の文字列を含めた前記第１の種類の符号情報群が含む、ある第１の種類の符号情報が含まれる場合に、前記ある第１の種類の符号情報を、前記ある第１の種類の符号情報と関連付けて前記記憶部に記憶された第２の種類の符号情報に変換する、
処理を実行させることを特徴とする変換プログラム。
【請求項９】
コンピュータが、
変換対象データの取得に応じ、第１の種類の符号情報群に含まれる第１の種類の符号情

報のそれぞれと第２の種類の符号情報群に含まれる第２の種類の符号情報の何れかと関連付けた辞書情報を記憶部に記憶し、
前記記憶部から前記辞書情報を読み出し、前記辞書情報において、各前記第１の種類の符号情報と関連付けられる各前記第２の種類の符号情報を、入力された入力情報を第１のシードとする第１のハッシュ関数のハッシュ値を第２のシードとする第２のハッシュ関数のハッシュ値により変更して前記辞書情報を更新し、
前記変換対象データ内に、ある第１の種類の符号情報が含まれる場合に、前記ある第１の種類の符号情報を、前記更新された前記辞書情報において前記ある第１の種類の符号情報と関連付けて前記記憶部に記憶された第２の種類の符号情報に変換する、
処理を実行することを特徴とする変換方法。
【請求項１０】
第１の種類の符号情報群を記憶する記憶部と、
変換対象データの取得に応じ、前記記憶部に記憶された第１の種類の符号情報群に含まれる第１の種類の符号情報のそれぞれと第２の種類の符号情報群に含まれる第２の種類の符号情報の何れかと関連付けた辞書情報を前記記憶部に記憶する記憶制御部と、
前記記憶部から前記辞書情報を読み出し、前記辞書情報において、各前記第１の種類の符号情報と関連付けられる各前記第２の種類の符号情報を、入力された入力情報を第１のシードとする第１のハッシュ関数のハッシュ値を第２のシードとする第２のハッシュ関数のハッシュ値により変更して前記辞書情報を更新する更新部と、
前記変換対象データ内に、ある第１の種類の符号情報が含まれる場合に、前記ある第１の種類の符号情報を、前記更新された前記辞書情報において前記ある第１の種類の符号情報と関連付けて前記記憶部に記憶された第２の種類の符号情報に変換する変換部と、
を含むことを特徴とする変換装置。
【請求項１１】
第１の種類の符号情報群を記憶する第１の記憶部と、
第１の変換対象データの取得に応じ、前記第１の記憶部に記憶された第１の種類の符号情報群に含まれる第１の種類の符号情報のそれぞれと第２の種類の符号情報群に含まれる第２の種類の符号情報の何れかと関連付けた第１の辞書情報を前記第１の記憶部に記憶する第１の記憶制御部と、
前記第１の記憶部から前記第１の辞書情報を読み出し、前記第１の辞書情報において、各前記第１の種類の符号情報と関連付けられる各前記第２の種類の符号情報を、入力された入力情報を第１のシードとする第１のハッシュ関数のハッシュ値を第２のシードとする第２のハッシュ関数のハッシュ値により変更して前記第１の辞書情報を更新する第１の更新部と、
前記第１の変換対象データ内に、ある第１の種類の符号情報が含まれる場合に、前記ある第１の種類の符号情報を、前記更新された前記第１の辞書情報において前記ある第１の種類の符号情報と関連付けて前記第１の記憶部に記憶された第２の種類の符号情報に変換する第１の変換部と、
を含む第１の変換装置と、
前記第２の種類の符号情報群を記憶する第２の記憶部と、
第２の変換対象データの取得に応じ、前記第２の記憶部に記憶された第２の種類の符号情報群に含まれる第２の種類の符号情報のそれぞれと前記第１の種類の符号情報群に含まれる第２の種類の符号情報の何れかと関連付けた第２の辞書情報を前記第２の記憶部に記憶する第２の記憶制御部と、
前記第２の記憶部から前記第２の辞書情報を読み出し、前記第２の辞書情報において、各前記第２の種類の符号情報と関連付けられる各前記第１の種類の符号情報を、前記入力情報を第１のシードとする第１のハッシュ関数のハッシュ値を第２のシードとする第２のハッシュ関数のハッシュ値により変更して前記第２の辞書情報を更新する第２の更新部と、
前記第２の変換対象データ内に、前記第１の変換部で変換された、ある第２の種類の符

号情報が含まれる場合に、前記ある第２の種類の符号情報を、前記更新された前記第２の辞書情報において前記ある第２の種類の符号情報と関連付けて前記第２の記憶部に記憶された第１の種類の符号情報に変換する第２の変換部と、
を含む第２の変換装置と、
を含むことを特徴とする変換システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、変換プログラム、変換装置、変換方法、および変換システムに関する。
【背景技術】
【０００２】
従来、デジタルコンテンツを圧縮し、圧縮したデジタルコンテンツを暗号化し、暗号化したデジタルコンテンツを送信する装置がある。例えば、従来の装置は、圧縮され暗号化されたデジタルコンテンツを、ＰＣ（Personal Computer）や携帯電話などの利用者端末に送信する。なお、デジタルコンテンツの一例としては、動画、音楽、書籍や辞書などが挙げられる。また、利用者端末では、暗号化されたデジタルコンテンツが復号化され、復号化されたデジタルコンテンツが伸張される。そして、利用者端末では、伸張されたデジタルコンテンツの再生が行われる。
【０００３】
また、入力データに含まれるシンボルが辞書に登録されている場合には、シンボルに対応する圧縮符号をスクランブルし、シンボルが辞書に登録されていない場合には、生データをスクランブルし、スクランブルしたシンボルを出力する装置が存在する。
【０００４】
また、アダプティブテンプレートを使用してデータに対して予測符号化を行い、予測符号化された結果を算術符号化する圧縮方式でデータを圧縮する装置が存在する。かかる装置では、アダプティブテンプレートで適用する浮動テンプレートの画素の位置情報を利用して画情報を暗号化する。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００５－９４５１６号公報
【特許文献２】特開２００３－６０６３４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、上記の従来の技術では、圧縮処理を行ったうえにさらに暗号化処理を行う、もしくは、復号化処理を行ったうえにさらに伸張処理を行うため、処理対象データのサイズに応じて処理コストが増大する。
【０００７】
１つの側面では、本発明は、処理対象データのサイズ増大に応じた処理コストの増大を抑制することを目的とする。
【課題を解決するための手段】
【０００８】
本願の開示する変換プログラムは、一つの態様において、コンピュータに、第１種類の符号情報群に含まれる第１種類の符号情報のそれぞれについて、次のような処理を実行させる。すなわち、変換プログラムは、入力された入力情報に応じて第２種類の符号情報群に含まれる第２種類の符号情報の何れかと関連付けて記憶部に記憶する処理を実行させる。そして、変換プログラムは、変換対象データ内にある第１種類の符号情報が含まれる場合に、当該ある第１種類の符号情報を、当該ある第１種類の符号情報と関連付けて記憶部に記憶された第２種類の符号情報に変換する処理を実行させる。

【発明の効果】
【０００９】
１態様によれば、処理対象データのサイズ増大に応じた処理コストの増大を抑制することができる。
【図面の簡単な説明】
【００１０】
【図１】図１は、実施例１に係るシステムの構成の一例を示す図である。
【図２】図２は、コンテンツＤＢの一例を示す図である。
【図３】図３は、トライの木の一例を示す図である。
【図４】図４は、トライの木の第一世代の圧縮符号が変更された場合の一例を示す図である。
【図５】図５は、トライの木の第二世代以降の葉および節点が追加された場合の一例を示す図である。
【図６】図６は、変更部の処理の一例を説明するための図である。
【図７】図７は、実施例１に係るシステムのシーケンス図である。
【図８】図８は、実施例１に係る圧縮処理の手順を示すフローチャートである。
【図９】図９は、実施例１に係る伸張処理の手順を示すフローチャートである。
【図１０】図１０は、実施例２に係るシステムの構成の一例を示す図である。
【図１１】図１１は、実施例２に係るシステムが実行する処理の一例を説明するための図である。
【図１２】図１２は、実施例２に係るシステムが実行する処理の一例を説明するための図である。
【図１３】図１３は、実施例２に係る圧縮処理の手順を示すフローチャートである。
【図１４】図１４は、実施例２に係る伸張処理の手順を示すフローチャートである。
【図１５】図１５は、実施例３に係るシステムの構成の一例を示す図である。
【図１６】図１６は、記憶部に記憶された情報の一例を示す図である。
【図１７】図１７は、実施例３における圧縮符号の変更の一例を説明するための図である。
【図１８】図１８は、実施例３に係る圧縮処理の手順を示すフローチャートである。
【図１９】図１９は、実施例３に係る伸張処理の手順を示すフローチャートである。
【図２０】図２０は、実施例４に係るシステムの構成の一例を示す図である。
【図２１】図２１は、実施例４に係るシステムが実行する処理の一例を説明するための図である。
【図２２】図２２は、実施例４に係る圧縮処理の手順を示すフローチャートである。
【図２３】図２３は、実施例４に係る伸張処理の手順を示すフローチャートである。
【図２４】図２４は、実施例５に係るシステムの構成の一例を示す図である。
【図２５】図２５は、予約語テーブルの一例を示す図である。
【図２６Ａ】図２６Ａは、生成部により生成された文字列の一例を示す図である。
【図２６Ｂ】図２６Ｂは、生成部により生成された文字列の一例を示す図である。
【図２７】図２７は、実施例５に係るシステムの処理を説明するための図である。
【図２８】図２８は、実施例５に係る圧縮処理の手順を示すフローチャートである。
【図２９】図２９は、実施例５に係る伸張処理の手順を示すフローチャートである。
【図３０】図３０は、実施例６に係るシステムの構成の一例を示す図である。
【図３１Ａ】図３１Ａは、ハフマン木で表される辞書の一例を示す図である。
【図３１Ｂ】図３１Ｂは、図３１Ａの例が示す辞書が変更された場合の一例を示す図である。
【図３２】図３２は、実施例６に係る圧縮処理の手順を示すフローチャートである。
【図３３】図３３は、実施例６に係る伸張処理の手順を示すフローチャートである。
【図３４】図３４は、圧縮プログラムを実行するコンピュータを示す図である。
【図３５】図３５は、伸張プログラムを実行するコンピュータを示す図である。

【発明を実施するための形態】
【００１１】
以下に、本願の開示する伸張プログラム、圧縮プログラム、圧縮装置、伸張装置、圧縮方法および伸張方法の各実施例を図面に基づいて詳細に説明する。各実施例は開示の技術を限定するものではない。そして、各実施例は、処理内容を矛盾させない範囲で適宜組み合わせることが可能である。なお、伸張プログラム、圧縮プログラムは、変換プログラムの一例である。また、圧縮装置、伸張装置は、変換装置の一例である。また、圧縮方法、伸張方法は、変換方法の一例である。
【実施例１】
【００１２】
［システム１の構成例］
実施例１に係るシステムについて説明する。図１は、実施例１に係るシステムの構成の一例を示す図である。本実施例に係るシステム１は、サーバ２と、利用者端末３とを有する。サーバ２と、利用者端末３とは、データの送受信が可能なように接続される。図１の例では、サーバ２と、利用者端末３とは、インターネット４を介して接続されている。なお、サーバ２と、利用者端末３とは、無線で接続されてもよい。サーバ２は、辞書や電子書籍などのデジタルコンテンツのファイルのデータを圧縮する。サーバ２は、圧縮されたデジタルコンテンツのファイルのデータを、インターネット４を介して利用者端末３に送信する。利用者端末３は、受信したデジタルコンテンツのファイルのデータを伸張する。利用者端末３は、伸張したデジタルコンテンツのファイルを再生する。
【００１３】
サーバ２は、入力部５と、出力部６と、送受信部７と、記憶部８と、制御部９とを有する。
【００１４】
入力部５は、各種の情報を制御部９に入力する。例えば、入力部５は、ユーザから、デジタルコンテンツを受け付けて、受け付けたデジタルコンテンツを制御部９に入力する。また、入力部５は、ユーザから、後述の圧縮処理を実行する指示を受け付けて、受け付けた指示を制御部９に入力する。また、入力部５は、ユーザから、パスワードを受け付けて、受け付けたパスワードを制御部９に入力する。パスワードの一例としては、数字およびアルファベットが挙げられる。例えば、パスワードとしては、４桁の数字「３２１２」が挙げられる。また、入力部５のデバイスの一例としては、マウスやキーボードなどの操作受付デバイスが挙げられる。
【００１５】
出力部６は、各種の情報を出力する。例えば、出力部６は、サーバ２の稼働状況を表示する。出力部６のデバイスの一例としては、ＬＣＤ（Liquid Crystal Display）やＣＲＴ（Cathode Ray Tube）などの表示デバイスなどが挙げられる。
【００１６】
送受信部７は、サーバ２と利用者端末３との通信を行うための通信インタフェースである。例えば、送受信部７は、利用者端末３からインターネット４を介して、コンテンツデータベース（Data Base）に登録されたデジタルコンテンツのファイルの送信要求を受信すると、受信した送信要求を制御部９へ送信する。なお、以下では、データベースを「ＤＢ」と略記する。また、送受信部７は、制御部９から後述のコンテンツＤＢ８ａに登録されたデジタルコンテンツのファイルを受信すると、受信したデジタルコンテンツのファイルを、インターネット４を介して利用者端末３へ送信する。
【００１７】
記憶部８は、各種情報を記憶する。例えば、記憶部８は、コンテンツＤＢ８ａ、辞書８ｂを記憶する。
【００１８】
コンテンツＤＢ８ａには、圧縮されたデジタルコンテンツのファイルが登録される。例えば、コンテンツＤＢ８ａには、後述の圧縮部９ａにより圧縮されたデジタルコンテンツ

のファイルが登録される。図２は、コンテンツＤＢの一例を示す図である。図２の例では、コンテンツＤＢ８ａに、圧縮されたデジタルコンテンツＡ～Ｋの各ファイルが登録されている場合が示されている。コンテンツＤＢ８ａに登録されたデジタルコンテンツのファイルは、利用者端末３からの指示に応じて、利用者端末３へ送信される。

【００１９】

辞書８ｂは、ＬＺ７８の圧縮方式で用いられる動的辞書である。ＬＺ７８の圧縮方式では、トライの木で表される動的辞書が用いられて、ファイルの圧縮および伸張が行われる。トライの木の葉および節点には、文字の文字コードと参照番号とが格納されている。図３は、トライの木の一例を示す図である。図３の例では、初期化された辞書８ｂが示すトライの木の一例が示されている。図３の例では、初期化された辞書８ｂのトライの木の葉には、１６進数で「００」～「ＦＦ」までの２５６種類の文字のコードと、参照番号とが登録された場合が示されている。ここで、参照番号は、圧縮符号として用いられる。図３の例では、文字「ａ」の文字コードは、１０進数で「９７」である。また、図３の例では、文字「ａ」の圧縮符号は、１６進数で「６１」である。なお、トライの木のルートに接続された一列目の葉および節点は、第一世代とも称される。同様に、トライの木のＮ列目の葉および節点は、第Ｎ世代と称される。第一世代の葉および節点では、文字のコードと圧縮符号とは同一である。

【００２０】

図４は、トライの木の第一世代の圧縮符号が変更された場合の一例を示す図である。図４の例では、図３の例において１６進数で「６１」であった「ａ」の圧縮符号が、１６進数で「５４」に変更された場合が示されている。また、図４の例では、図３の例において１６進数で「６２」であった「ｂ」の圧縮符号が、１６進数で「００」に変更された場合が示されている。図４の例のトライの木の第一世代の圧縮符号は、後述の変更部９ｂによりスクランブルされて、コードと圧縮符号との組合せが変更される。これにより、圧縮されたデータの解読を試みる攻撃者などは、初期化時に辞書８ｂに登録される２５６種類の文字のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、２５６種類の文字の解読が困難となる。

【００２１】

図５は、トライの木の第二世代以降の葉および節点が追加された場合の一例を示す図である。図５の例では、文字列「ｂｉｔ」の参照番号は、１６進数で「１０２」である。図５の例では、文字列「ｂｉｔ」の圧縮符号として参照番号「１０２」を用いることで、文字列「ｂｉｔ」の圧縮を行うことができる。また、図５の例では、圧縮されたファイルのデータ「１０２」を、文字列「ｂｉｔ」に置き換えることで、伸張を行うことができる。

【００２２】

ここで、図５の例では、第一世代の圧縮符号が変更されているため、第二世代以降の葉に登録された圧縮符号が用いられて圧縮されたデータは、攻撃者などによる解読が困難なデータである。具体例を挙げて説明する。例えば、攻撃者などが、圧縮された「ｂｉｔ」の文字列を解読する場合を想定する。この場合、攻撃者などは、初期化時に辞書８ｂに登録される２５６種類の文字のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、「ｂｉｔ」の先頭文字「ｂ」の圧縮符号を特定するのが困難となる。すなわち、攻撃者などは、先頭文字「ｂ」のトライの木での格納位置を特定するのが困難となるため、結果的に「ｂｉｔ」の圧縮符号を特定するのが困難となる。

【００２３】

記憶部８は、例えば、フラッシュメモリなどの半導体メモリ素子、または、ハードディスク、光ディスクなどの記憶装置である。なお、記憶部８は、上記の種類の記憶装置に限定されるものではなく、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）であってもよい。

【００２４】

制御部９は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、これらによって種々の処理を実行する。図１に示すように、制御部９は、

圧縮部９ａと、変更部９ｂとを有する。

【００２５】

圧縮部９ａは、後述の変更部９ｂにより、文字のコードと、圧縮符号との組合せが変更された辞書８ｂを用いて、入力部５から入力されたデジタルコンテンツのファイルのデータを圧縮しつつ、辞書８ｂを更新する。具体例を挙げて説明する。圧縮部９ａは、ＬＺ７８の圧縮方式により、まず、辞書８ｂを初期化して、予め定められた複数の文字のコードと、圧縮符号との組合せを登録する。先の図３の例では、圧縮部９ａは、１６進数で「００」～「ＦＦ」までの２５６種類の文字のコードと、参照番号とを辞書８ｂに登録する。そして、圧縮部９ａは、変更部９ｂにより、文字と圧縮符号との組合せが変更された辞書８ｂを用いて、ＬＺ７８の圧縮方式によって、デジタルコンテンツのファイルのデータを圧縮しつつ、辞書８ｂを更新する。そして、圧縮部９ａは、圧縮したファイルをデジタルコンテンツごとに、コンテンツＤＢ８ａに登録する。また、圧縮部９ａは、利用者端末３からのデジタルコンテンツのファイルの送信要求を受信すると、デジタルコンテンツのファイルをコンテンツＤＢ８ａから取得し、取得したファイルを、送受信部７に送信する。

【００２６】

変更部９ｂは、入力部５から入力されたパスワードに基づいて、文字列と圧縮符号との複数の組合せが登録された辞書８ｂの文字列と圧縮符号との組合せを変更する。具体例を挙げて説明する。まず、変更部９ｂは、パスワードを取得する。そして、変更部９ｂは、パスワードに含まれる数字「０」～「９」のそれぞれを１６進数の「００」～「０９」とし、アルファベット「ａ」～「ｚ」のそれぞれを１６進数の「０Ａ」～「２３」として、各桁の和を算出する。例えば、変更部９ｂは、パスワードとして「３２１２」を取得した場合には、１６進数で「０８」（３＋２＋１＋２）を算出する。続いて、変更部９ｂは、各桁の和を所定値で除算した場合の剰余Ｓを算出する。例えば、各桁の和が「０８」であり、かかる所定値が１０進数で「１６」である場合には、変更部９ｂは、剰余Ｓとして「８」（８÷１６＝０余り８）を算出する。

【００２７】

その後、変更部９ｂは、初期時に辞書８ｂに登録された所定数の文字と圧縮符号との組合せを２Ｓごとにブロック化する。図６は、変更部の処理の一例を説明するための図である。図６の例では、Ｓ＝「８」の場合であり、変更部９ｂは、１６個の文字と圧縮符号との組合せを１６個ごとにブロック化した場合が示されている。図６の例では、１番目のブロック９０は、文字「ＮＵＬ」、「ＳＯＨ」、・・・「ＢＥＬ」、「ＢＳ」、「ＴＡＢ」、・・・「ＳＩ」の１６個の文字のそれぞれのコードと、圧縮符号との組合せを含む。すなわち、図６の例では、１番目のブロック９０は、文字「ＮＵＬ」のコード「０」と圧縮符号「００」との組合せを含む。また、図６の例では、１番目のブロック９０は、文字「ＳＯＨ」のコード「１」と圧縮符号「０１」との組合せを含む。また、図６の例では、１番目のブロック９０は、文字「ＢＥＬ」のコード「７」と圧縮符号「０７」との組合せを含む。また、図６の例では、１番目のブロック９０は、文字「ＢＳ」のコード「８」と圧縮符号「０８」との組合せを含む。また、図６の例では、１番目のブロック９０は、文字「ＴＡＢ」のコード「９」と圧縮符号「０９」との組合せを含む。また、図６の例では、１番目のブロック９０は、文字「ＳＩ」のコード「１５」と圧縮符号「０Ｆ」との組合せを含む。さらに、図６の例では、２番目のブロック９１は、文字「ＤＬＥ」・・・・の１６個の文字のそれぞれのコードと、圧縮符号との組合せを含む。このようにして、変更部９ｂは、１番目のブロックからＮ番目のブロックまでを生成する。なお、Ｎは、処理対象の世代の葉および節点の個数を２Ｓで除した値の小数点以下を切り上げた整数値である。ここで、本実施例では、処理対象の世代は、第一世代である。

【００２８】

続いて、変更部９ｂは、ブロック１～Ｎごとに、次のような処理を行う。すなわち、変更部９ｂは、ブロック内の文字のコードと圧縮符号との複数の組合せのそれぞれについて、圧縮符号に上記の剰余Ｓを加えた値を、上記の所定値で除算した場合の剰余Ｓ´を算出する。そして、変更部９ｂは、ブロック内の文字のコードと圧縮符号との複数の組合せの

それぞれについて、圧縮符号を、剰余Ｓ´に変更する。図６の例では、剰余Ｓが「８」であるため、変更部９ｂは、文字「ＮＵＬ」の圧縮符号を「０８」（（「００」＋「０８」）÷所定値１６＝０余り０８）に変更する。また、図６の例では、変更部９ｂは、文字「ＳＯＨ」の圧縮符号を「０９」（（「０１」＋「０８」）÷所定値１６＝０余り０９）に変更する。また、図６の例では、変更部９ｂは、文字「ＢＥＬ」の圧縮符号を「０Ｆ」（（「０７」＋「０８」）÷所定値１６＝０余り０Ｆ）に変更する。また、図６の例では、変更部９ｂは、文字「ＢＳ」の圧縮符号を「１０」（（「０８」＋「０８」）÷所定値１６＝１余り００）に変更する。また、図６の例では、１番目のブロック９０は、文字「ＴＡＢ」の圧縮符号を「０１」（（「０９」＋「０８」）÷所定値１６＝１余り０１）に変更する。また、図６の例では、変更部９ｂは、文字「ＳＩ」の圧縮符号を「０７」（（「０Ｆ」＋「０８」）÷所定値１６＝１余り０７）に変更する。さらに、図６の例では、変更部９ｂは、文字「ＤＬＥ」の圧縮符号を「１８」に変更する。このようにして、変更部９ｂは、各ブロック単位で、入力部５から入力されたパスワードに基づいて、文字列と圧縮符号との複数の組合せが登録された辞書８ｂの文字列と圧縮符号との組合せを変更する。なお、ブロック１の場合について例示したが、ブロック２以上については、次のようにして、剰余Ｓ´を算出することができる。すなわち、ブロック１と同様に、ブロック内で、文字のコードと圧縮符号との組み合わせが入れ替わるように、ｍ（＞２）ブロックごとに、上述した除算したことにより算出した剰余Ｓ´に、（ｍ－１）×２Ｓの値が加算された値が剰余Ｓ´となる。

【００２９】

このように、本実施例に係るサーバ２では、辞書８ｂの第一世代の葉および節点の圧縮符号がスクランブルされて、コードと圧縮符号との組合せが変更される。これにより、圧縮されたデータの解読を試みる攻撃者などは、初期化時に辞書８ｂに登録される複数の種類の文字のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、これらの複数の種類の文字の解読が困難となる。この結果、これらの複数の種類の文字を先頭文字に含む文字列の解読についても困難となる。

【００３０】

また、本実施例に係るサーバ２では、辞書８ｂの圧縮符号をスクランブルするだけで、複雑な暗号化の処理を行わずに、解読が困難な圧縮データが生成される。したがって、本実施例に係るサーバ２によれば、簡易な圧縮処理により難読化を図ることができる。また、処理対象データのサイズ増大に応じた処理コストの増大を抑制することができる。

【００３１】

また、本実施例に係るサーバ２によれば、辞書８ｂの圧縮符号をスクランブルするだけで、データを圧縮するたびに圧縮されたデータおよび生データにスクランブル処理を行っていないので、簡易に圧縮データの難読化を図ることができる。

【００３２】

利用者端末３は、入力部１０と、出力部１１と、送受信部１２と、記憶部１３と、制御部１４とを有する。

【００３３】

入力部１０は、各種情報を制御部１４に入力する。例えば、入力部１０は、ユーザから後述の伸張処理を実行する指示を受け付けて、受け付けた指示を制御部１４に入力する。また、入力部１０は、ユーザからパスワードを受け付けて、受け付けたパスワードを制御部１４に入力する。入力部１０のデバイスの一例としては、マウスやキーボードなどの操作受付デバイスが挙げられる。

【００３４】

出力部１１は、各種の情報を出力する。例えば、出力部１１は、後述の再生部１４ｃによって、再生されたデジタルコンテンツを表示する。出力部１１のデバイスの一例としては、ＬＣＤ（Liquid Crystal Display）やＣＲＴ（Cathode Ray Tube）などの表示デバイスが挙げられる。

【００３５】

送受信部１２は、利用者端末３とサーバ２との通信を行うための通信インタフェースである。例えば、送受信部１２は、制御部１４から、コンテンツＤＢに登録されたデジタルコンテンツのファイルの送信要求を受信すると、受信した送信要求を、インターネット４を介してサーバ２へ送信する。また、送受信部１２は、サーバ２からコンテンツＤＢ８ａに登録されたデジタルコンテンツのファイルを受信すると、受信したファイルを制御部１４へ送信する。

【００３６】

記憶部１３は、各種情報を記憶する。例えば、記憶部１３は、コンテンツＤＢ１３ａ、辞書１３ｂを記憶する。

【００３７】

コンテンツＤＢ１３ａには、後述の伸張部１４ａにより伸張されたデジタルコンテンツの各ファイルが登録される。

【００３８】

辞書１３ｂは、ＬＺ７８の圧縮方式で用いられる動的辞書である。上述した辞書８ｂと同様に、辞書１３ｂは、後述の伸張部１４ａにより、初期化されると、予め定められた文字のコードと、圧縮符号との複数の組合せが登録される。また、辞書１３ｂが示すトライの木の第一世代の圧縮符号は、辞書８ｂと同様に、後述の変更部１４ｂによりスクランブルされて、コードと圧縮符号との組合せが変更される。これにより、圧縮されたデータの解読を試みる攻撃者などは、初期化時に辞書１３ｂに登録される２５６種類の文字のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、２５６種類の文字の解読が困難となる。

【００３９】

また、辞書１３ｂは、辞書８ｂと同様に、トライの木の第一世代の圧縮符号が変更された後に、伸張部１４ａにより、トライの木の第二世代以降の葉および節点が追加されて、更新される。

【００４０】

記憶部１３は、例えば、フラッシュメモリなどの半導体メモリ素子、または、ハードディスク、光ディスクなどの記憶装置である。なお、記憶部１３は、上記の種類の記憶装置に限定されるものではなく、ＲＡＭ（Random Access Memory)、ＲＯＭ（Read Only Memory)であってもよい。

【００４１】

制御部１４は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、これらによって種々の処理を実行する。図１に示すように、制御部１４は、伸張部１４ａと、変更部１４ｂと、再生部１４ｃとを有する。

【００４２】

伸張部１４ａは、後述の変更部１４ｂにより、文字のコードと、圧縮符号との組合せが変更された辞書１３ｂを用いて、サーバ２から入力されたデジタルコンテンツのファイルのデータを伸張しつつ、辞書１３ｂを更新する。具体例を挙げて説明する。伸張部１４ａは、ＬＺ７８の圧縮方式により、まず、辞書１３ｂを初期化して、予め定められた複数の文字のコードと、圧縮符号との組合せを登録する。ここで、伸張部１４ａは、圧縮部９ａによる辞書８ａの初期化の際に、辞書８ａに登録された文字と圧縮符号との組合せと同一の組合せを辞書１３ｂの初期化時に登録する。そして、伸張部１４ａは、変更部１４ｂにより、文字と圧縮符号との組合せが変更された辞書１３ｂを用いて、ＬＺ７８の圧縮方式によって、デジタルコンテンツのファイルのデータを伸張しつつ、辞書１３ｂを更新する。そして、伸張部１４ａは、伸張したファイルをデジタルコンテンツごとに、コンテンツＤＢ１３ａに登録する。

【００４３】

変更部１４ｂは、入力部１０から入力されたパスワードに基づいて、文字列と圧縮符号との複数の組合せが登録された辞書１３ｂの文字列と圧縮符号との組合せを変更する。具体例を挙げて説明する。まず、変更部１４ｂは、パスワードを取得する。そして、変更部

１４ｂは、変更部９ａと同様に、パスワードに含まれる数字「０」～「９」のそれぞれを１６進数の「００」～「０９」とし、アルファベット「ａ」～「ｚ」のそれぞれを１６進数の「０Ａ」～「２３」として、各桁の和を算出する。

【００４４】

その後、変更部１４ｂは、変更部９ａと同様に、初期時に辞書１３ｂに登録された所定数の文字と圧縮符号との組合せを２Ｓごとにブロック化する。図６の例では、Ｓ＝「８」の場合であり、変更部１４ｂは、１６個の文字と圧縮符号との組合せを１６個ごとにブロック化した場合が示されている。変更部１４ｂは、１番目のブロックからＮ番目のブロックまでを生成する。なお、Ｎは、処理対象の世代の葉および節点の個数を２Ｓで除した値の小数点以下を切り上げた整数値である。ここで、本実施例では、処理対象の世代は、第一世代である。

【００４５】

続いて、変更部１４ｂは、ブロック１～Ｎごとに、次のような処理を行う。すなわち、変更部１４ｂは、変更部９ａと同様に、ブロック内の文字のコードと圧縮符号との複数の組合せのそれぞれについて、圧縮符号に剰余Ｓを加えた値を、上記の所定値で除算した場合の剰余Ｓ´を算出する。そして、ブロック内の文字のコードと圧縮符号との複数の組合せのそれぞれについて、圧縮符号を、剰余Ｓ´に変更する。図６の例では、剰余Ｓが「８」であるため、変更部１４ｂは、文字「ＮＵＬ」の圧縮符号を「０８」（（「００」＋「０８」）÷所定値１６＝０余り０８）に変更する。また、図６の例では、変更部１４ｂは、文字「ＳＯＨ」の圧縮符号を「０９」（（「０１」＋「０８」）÷所定値１６＝０余り０９）に変更する。また、図６の例では、変更部１４ｂは、文字「ＢＥＬ」の圧縮符号を「０Ｆ」（（「０７」＋「０８」）÷所定値１６＝０余り０Ｆ）に変更する。また、図６の例では、変更部１４ｂは、文字「ＢＳ」の圧縮符号を「１０」（（「０８」＋「０８」）÷所定値１６＝１余り００）に変更する。また、図６の例では、１番目のブロック９０は、文字「ＴＡＢ」の圧縮符号を「０１」（（「０９」＋「０８」）÷所定値１６＝１余り０１）に変更する。また、図６の例では、変更部１４ｂは、文字「ＳＩ」の圧縮符号を「０７」（（「０Ｆ」＋「０８」）÷所定値１６＝１余り０７）に変更する。さらに、図６の例では、変更部１４ｂは、文字「ＤＬＥ」の圧縮符号を「１８」に変更する。このようにして、変更部１４ｂは、各ブロック単位で、入力部１０から入力されたパスワードに基づいて、文字列と圧縮符号との複数の組合せが登録された辞書１３ｂの文字列と圧縮符号との組合せを変更する。なお、ブロック１の場合について例示したが、ブロック２以上については、次のようにして、剰余Ｓ´を算出することができる。すなわち、ブロック１と同様に、ブロック内で、文字のコードと圧縮符号との組み合わせが入れ替わるように、ｍ（＞２）ブロックごとに、上述した除算したことにより算出した剰余Ｓ´に、（ｍ－１）×２Ｓの値が加算された値が剰余Ｓ´となる。

【００４６】

ここで、本実施例に係る利用者端末３では、入力されたパスワードが、サーバ２で入力された正規のパスワードと一致しない場合には、上記の所定値が大きくなるほど、算出される剰余Ｓが、サーバ２で算出される剰余Ｓと一致する可能性が低くなる。そのため、本実施例に係る利用者端末３では、入力されたパスワードが正規のパスワードでない場合には、上記の所定値が大きくなるほど、辞書１３ｂの登録内容が辞書８ｂの登録内容と一致する可能性が低くなる。このため、本実施例に係る利用者端末３では、結果として伸張されるデータが正規のものとなる可能性も低くなる。したがって、本実施例に係る利用者端末３によれば、簡易に難読化を図ることができる。

【００４７】

再生部１４ｃは、コンテンツＤＢ１３ａに登録されたデジタルコンテンツを取得し、取得したデジタルコンテンツを出力部１１の表示デバイスに再生する。

【００４８】

制御部１４は、ＡＳＩＣ（Application Specific Integrated Circuit）やＦＰＧＡ（Field Programmable Gate Array）などの集積回路を有する。なお、制御部１４は、

ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）などの電子回路を有してもよい。

【００４９】

［処理の流れ］

次に、本実施例に係るシステム１の処理の流れを説明する。図７は、実施例１に係るシステムのシーケンス図である。

【００５０】

図７に示すように、サーバ２は、後述の圧縮処理を実行する（ステップＳ１０１）。サーバ２は、圧縮されたデジタルコンテンツのファイルをコンテンツＤＢ８ａに登録する（ステップＳ１０２）。

【００５１】

一方、利用者端末３は、ユーザから後述の伸張処理を実行する指示を受け付けると（ステップＳ１０３）、デジタルコンテンツのファイルの送信要求をサーバ２に送信する（ステップＳ１０４）。サーバ２は、デジタルコンテンツのファイルの送信要求を受信すると、コンテンツＤＢ８ａに登録されたデジタルコンテンツのファイルを利用者端末３に送信する（ステップＳ１０５）。

【００５２】

利用者端末３は、デジタルコンテンツのファイルを受信する（ステップＳ１０６）と、後述の伸張処理を実行する（ステップＳ１０７）。利用者端末３は、伸張されたデジタルコンテンツのファイルをコンテンツＤＢ１３ａに登録する（ステップＳ１０８）。利用者端末３は、コンテンツＤＢ１３ａに登録されたデジタルコンテンツを再生する（ステップＳ１０９）。

【００５３】

次に、本実施例に係るサーバ２の処理の流れを説明する。図８は、実施例１に係る圧縮処理の手順を示すフローチャートである。この圧縮処理の実行タイミングとしては様々なタイミングが考えられる。例えば、圧縮処理は、入力部５からデジタルコンテンツが入力された場合に実行されるようにしてもよい。

【００５４】

図８に示すように、圧縮部９ａは、デジタルコンテンツのファイルを取得する（ステップＳ２０１）。圧縮部９ａは、辞書８ｂを初期化する（ステップＳ２０２）。変更部９ｂは、入力部５からパスワードが入力されたか否かを判定する（ステップＳ２０３）。パスワードが入力されていない場合（ステップＳ２０３否定）には、変更部９ｂは、再びステップＳ２０３で、入力部５からパスワードが入力されたか否かを判定する。

【００５５】

一方、パスワードが入力された場合（ステップＳ２０３肯定）には、変更部９ｂは、パスワードの各桁の和を算出し、算出した和を所定値で除算した場合の剰余Ｓを算出する（ステップＳ２０４）。変更部９ｂは、処理対象の世代の葉および節点の個数を２Ｓで除した値の小数点以下を切り上げた整数値Ｎを算出する（ステップＳ２０５）。変更部９ｂは、変数Ｋの値に１を設定する（ステップＳ２０６）。変更部９ｂは、処理対象の世代のＫ番目のブロックの圧縮符号をスクランブルして、文字のコードと圧縮符号との組合せを変更する（ステップＳ２０７）。変更部９ｂは、変数Ｋの値が整数値Ｎ以上となったか否かを判定する（ステップＳ２０８）。変数Ｋの値が整数値Ｎ未満である場合（ステップＳ２０８否定）には、変更部９ｂは、変数Ｋの値を１つインクリメントし（ステップＳ２０９）、ステップＳ２０７へ戻る。

【００５６】

一方、変数Ｋの値が整数値Ｎ以上である場合（ステップＳ２０８肯定）には、圧縮部９ａは、辞書８ｂを用いて、ＬＺ７８の圧縮方式によって、デジタルコンテンツのファイルのデータを圧縮しつつ、辞書８ｂを更新する（ステップＳ２１０）。そして、圧縮部９ａは、処理結果を制御部９の内部メモリに格納し、リターンする。

【００５７】

次に、本実施例に係る利用者端末３の処理の流れを説明する。図９は、実施例１に係る伸張処理の手順を示すフローチャートである。伸張処理においても、図８において説明した圧縮処理と共通の辞書更新アルゴリズムを用いる。

【００５８】

図９に示すように、伸張部１４ａは、デジタルコンテンツの圧縮ファイルをサーバ２から取得する（ステップＳ３０１）。伸張部１４ａは、辞書１３ｂを初期化する（ステップＳ３０２）。変更部１４ｂは、入力部１０からパスワードが入力されたか否かを判定する（ステップＳ３０３）。パスワードが入力されていない場合（ステップＳ３０３否定）には、変更部１４ｂは、再びステップＳ３０３で、入力部１０からパスワードが入力されたか否かを判定する。

【００５９】

一方、パスワードが入力された場合（ステップＳ３０３肯定）には、変更部１４ｂは、パスワードの各桁の和を算出し、算出した和を所定値で除算した場合の剰余Ｓを算出する（ステップＳ３０４）。変更部１４ｂは、処理対象の世代の葉および節点の個数を２Ｓで除した値の小数点以下を切り上げた整数値Ｎを算出する（ステップＳ３０５）。変更部１４ｂは、変数Ｋの値に１を設定する（ステップＳ３０６）。変更部１４ｂは、処理対象の世代のＫ番目のブロックの圧縮符号をスクランブルして、文字のコードと圧縮符号との組合せを変更する（ステップＳ３０７）。変更部１４ｂは、変数Ｋの値が整数値Ｎ以上となったか否かを判定する（ステップＳ３０８）。変数Ｋの値が整数値Ｎ未満である場合（ステップＳ３０８否定）には、変更部１４ｂは、変数Ｋの値を１つインクリメントし（ステップＳ３０９）、ステップＳ３０７へ戻る。

【００６０】

一方、変数Ｋの値が整数値Ｎ以上である場合（ステップＳ３０８肯定）には、伸張部１４ａは、辞書１３ｂを用いて、ＬＺ７８の圧縮方式によって、デジタルコンテンツのファイルのデータを伸張しつつ、辞書１３ｂを更新する（ステップＳ３１０）。そして、伸張部１４ａは、処理結果を制御部１４の内部メモリに格納し、リターンする。

【００６１】

上述してきたように、本実施例に係るサーバ２では、辞書８ｂの第一世代の葉および節点の圧縮符号がスクランブルされて、コードと圧縮符号との組合せが変更される。これにより、圧縮されたデータの解読を試みる攻撃者などは、初期化時に辞書８ｂに登録される複数の種類の文字のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、これらの複数の種類の文字の解読が困難となる。この結果、これらの複数の種類の文字を先頭文字に含む文字列の解読についても困難となる。

【００６２】

また、本実施例に係るサーバ２では、辞書８ｂの圧縮符号をスクランブルするだけで、複雑な暗号化の処理を行わずに、解読が困難な圧縮データが生成される。したがって、本実施例に係るサーバ２によれば、簡易な圧縮処理により難読化を図ることができる。また、処理対象データのサイズ増大に応じた処理コストの増大を抑制することができる。

【００６３】

また、本実施例に係るサーバ２によれば、辞書８ｂの圧縮符号をスクランブルするだけで、データを圧縮するたびに圧縮されたデータおよび生データにスクランブル処理を行っていないので、簡易に圧縮データの難読化を図ることができる。

【００６４】

また、本実施例に係る利用者端末３では、入力されたパスワードが、サーバ２で入力された正規のパスワードと一致しない場合には、上記の所定値が大きくなるほど、算出される剰余Ｓが、サーバ２で算出される剰余Ｓと一致する可能性が低くなる。そのため、本実施例に係る利用者端末３では、入力されたパスワードが正規のパスワードでない場合には、上記の所定値が大きくなるほど、辞書１３ｂの登録内容が辞書８ｂの登録内容と一致する可能性が低くなる。このため、本実施例に係る利用者端末３では、結果として伸張されるデータが正規のものとなる可能性も低くなる。したがって、本実施例に係る利用者端末

３によれば、簡易に難読化を図ることができる。
【実施例２】
【００６５】
さて、上記の実施例１では、第一世代の圧縮符号をスクランブルする場合を例示したが、開示の装置はこれに限定されない。そこで、実施例２では、第二世代以降も圧縮符号をスクランブルする場合について説明する。
【００６６】
［システム２０の構成例］
実施例２に係るシステムについて説明する。図１０は、実施例２に係るシステムの構成の一例を示す図である。本実施例に係るシステム２０は、サーバ２１と、利用者端末２２とを有する。サーバ２１は、実施例１に係る制御部９に代えて制御部２３を有する点が、実施例１と異なる。利用者端末２２は、実施例１に係る制御部１４に代えて制御部２４を有する点が、実施例１と異なる。なお、以下では、上記の実施例１と同様の機能を果たす各部や各機器については図１と同様の符号を付し、その説明は省略する場合がある。サーバ２１は、辞書や電子書籍などのデジタルコンテンツのファイルのデータを圧縮する。サーバ２１は、圧縮されたデジタルコンテンツのファイルのデータを、インターネット４を介して利用者端末２２に送信する。利用者端末２２は、受信したデジタルコンテンツのファイルのデータを伸張する。利用者端末２２は、伸張したデジタルコンテンツのファイルを再生する。
【００６７】
サーバ２１は、入力部５と、出力部６と、送受信部７と、記憶部８と、制御部２３とを有する。
【００６８】
制御部２３は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、これらによって種々の処理を実行する。図１０に示すように、制御部２３は、圧縮部２３ａと、変更部２３ｂとを有する。
【００６９】
圧縮部２３ａは、実施例１に係る圧縮部９ａと同様の処理を行う。すなわち、圧縮部２３ａは、後述の変更部２３ｂにより、文字のコードと圧縮符号との組合せが変更された辞書８ｂを用いて、デジタルコンテンツのファイルのデータを圧縮する。また、圧縮部２３ａは、圧縮された文字列の圧縮前の文字列を含む文字列であって辞書８ｂに未登録の文字列と、圧縮符号との組合せを新たに辞書８ｂに登録する。
【００７０】
変更部２３ｂは、実施例１に係る変更部９ｂと同様の処理を行う。さらに、変更部２３ｂは、パスワードに基づいて、辞書８ｂに新たに登録された文字列と圧縮符号との組合せを新たに変更する。具体例を挙げて説明する。
【００７１】
変更部２３ｂは、辞書８ｂに文字列と圧縮符号との組合せが新たに登録されるたびに、新たに登録された文字列の文字のうち、新規に追加された文字の世代を処理対象の世代として特定する。図１１は、実施例２に係るシステムが実行する処理の一例を説明するための図である。図１１の例では、辞書８ｂに、文字列「ｂｉｔ」のコード「９８１０５１１６」と、圧縮符号「１０２」との組合せが登録されている場合が示されている。図１１の例において、辞書８ｂに、未登録の文字列「ｂｕｔ」のコードと圧縮符号との組合せが圧縮部２３ａにより新たに登録されると、変更部２３ｂは、「ｂｕｔ」の「ｕ」の第二世代と、「ｔ」の第三世代とを処理対象の世代として特定する。
【００７２】
そして、変更部２３ｂは、実施例１に係る変更部９ｂが辞書８ｂに登録された第一世代の文字列と圧縮符号との組合せを変更する方法と同様の方法で、特定した処理対象の世代の文字列と圧縮符号との組合せを変更する。図１２は、実施例２に係るシステムが実行する処理の一例を説明するための図である。図１２の例は、図１１の例において辞書８ｂに

未登録の文字列「ｂｕｔ」のコードと圧縮符号との組合せが、圧縮部２３ａにより辞書８ｂに新たに登録された場合の変更部２３ｂの処理の一例を示す。図１２の例では、変更部２３ｂは、文字列「ｂｕｔ」の第二世代の文字「ｕ」、第三世代の文字「ｔ」のそれぞれの圧縮符号と、文字列「ｂｉｔ」の第二世代の文字「ｉ」、第三世代の文字「ｔ」のそれぞれの圧縮符号とを変更する。すなわち、図１２の例では、変更部２３ｂは、文字列「ｂｕｔ」の第二世代の文字「ｕ」に対応する圧縮符号を「１０１」に変更し、第三世代の文字「ｔ」に対応する圧縮符号を「１０２」に変更する。また、図１２の例では、変更部２３ｂは、文字列「ｂｉｔ」の第二世代の文字「ｉ」に対応する圧縮符号を「１０３」に変更し、第三世代の文字「ｔ」に対応する圧縮符号を「１０４」に変更する。なお、ブロック内で、文字のコードと圧縮符号との組み合わせが入れ替わるように、適宜、そのブロック内の圧縮符号に応じた値が剰余Ｓ´に加算され、加算された結果得られた剰余Ｓ´が文字列と組み合わせられる。

【００７３】

このように、本実施例に係るサーバ２１では、辞書８ｂの第一世代、および、辞書８ｂに新規に追加された文字の世代の葉および節点の圧縮符号がスクランブルされて、コードと圧縮符号との組合せが変更される。これにより、圧縮されたデータの解読を試みる攻撃者などは、初期化時に辞書８ｂに登録される複数の種類の文字のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、これらの複数の種類の文字の解読が困難となる。

【００７４】

また、本実施例に係るサーバ２１では、辞書８ｂの圧縮符号をスクランブルするだけで、複雑な暗号化の処理を行わずに、解読が困難な圧縮データが生成される。したがって、本実施例に係るサーバ２１によれば、簡易な圧縮処理により難読化を図ることができる。また、処理対象データのサイズ増大に応じた処理コストの増大を抑制することができる。

【００７５】

また、本実施例に係るサーバ２１によれば、辞書８ｂの圧縮符号をスクランブルするだけで、データを圧縮するたびに圧縮されたデータおよび生データにスクランブル処理を行っていないので、簡易に圧縮データの難読化を図ることができる。

【００７６】

利用者端末２２は、入力部１０と、出力部１１と、送受信部１２と、記憶部１３と、制御部２４とを有する。

【００７７】

制御部２４は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、これらによって種々の処理を実行する。図１０に示すように、制御部２４は、伸張部２４ａと、変更部２４ｂと、再生部１４ｃとを有する。

【００７８】

伸張部２４ａは、実施例１に係る伸張部１４ａと同様の処理を行う。すなわち、伸張部２４ａは、後述の変更部２４ｂにより、文字のコードと圧縮符号との組合せが変更された辞書１３ｂを用いて、デジタルコンテンツのファイルのデータを伸張する。また、伸張部２４ａは、伸張された文字を含む文字列であって辞書１３ｂに未登録の文字列と、圧縮符号との組合せを新たに辞書１３ｂに登録する。

【００７９】

変更部２４ｂは、実施例１に係る変更部１４ｂと同様の処理を行う。さらに、変更部２４ｂは、パスワードに基づいて、辞書１３ｂに新たに登録された文字列と圧縮符号との組合せを新たに変更する。具体例を挙げて説明する。

【００８０】

変更部２４ｂは、辞書１３ｂに文字列と圧縮符号との組合せが新たに登録されるたびに、新たに登録された文字列の文字のうち、新規に追加された文字の世代を処理対象の世代として特定する。例えば、文字列「ｂｉｔ」のコードと圧縮符号との組合せが辞書１３ｂに登録されている場合に、未登録の文字列「ｂｕｔ」のコードと圧縮符号との組合せが伸

張部２４ａにより新たに登録されると、変更部２４ｂは、次のような処理を行う。すなわち、変更部２４ｂは、「ｂｕｔ」の「ｕ」の第二世代と、「ｔ」の第三世代とを処理対象の世代として特定する。

【００８１】

そして、変更部２４ｂは、実施例１に係る変更部１４ｂが辞書１３ｂに登録された第一世代の文字列と圧縮符号との組合せを変更するのと同様に、特定した処理対象の世代の文字列と圧縮符号との組合せを変更する。例えば、文字列「ｂｉｔ」のコードと圧縮符号との組合せが辞書１３ｂに登録されている場合に、未登録の文字列「ｂｕｔ」のコードと圧縮符号との組合せが伸張部２４ａにより新たに登録されると、変更部２４ｂは、次のような処理を行う。すなわち、変更部２４ｂは、文字列「ｂｕｔ」の第二世代の文字「ｕ」、第三世代の文字「ｔ」のそれぞれの圧縮符号と、文字列「ｂｉｔ」の第二世代の文字「ｉ」、第三世代の文字「ｔ」のそれぞれの圧縮符号とを変更する。なお、ブロック内で、文字のコードと圧縮符号との組み合わせが入れ替わるように、適宜、そのブロック内の圧縮符号に応じた値が剰余Ｓ′に加算され、加算された結果得られた剰余Ｓ′が文字列と組み合わせられる。

【００８２】

このように、本実施例に係る利用者端末２２では、入力されたパスワードが、サーバ２１で入力された正規のパスワードと一致しない場合には、上記の所定値が大きくなるほど、算出される剰余Ｓが、サーバ２１で算出される剰余Ｓと一致する可能性が低くなる。そのため、本実施例に係る利用者端末２２では、入力されたパスワードが正規のパスワードでない場合には、上記の所定値が大きくなるほど、辞書１３ｂの登録内容が辞書８ｂの登録内容と一致する可能性が低くなる。このため、本実施例に係る利用者端末２２では、結果として伸張されるデータが正規のものとなる可能性も低くなる。したがって、本実施例に係る利用者端末２２によれば、簡易に難読化を図ることができる。

【００８３】

制御部２４は、ＡＳＩＣ（Application Specific Integrated Circuit）やＦＰＧＡ（Field Programmable Gate Array）などの集積回路を有する。なお、制御部２４は、ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）などの電子回路を有してもよい。

【００８４】

［処理の流れ］

次に、本実施例に係るサーバ２１の処理の流れを説明する。図１３は、実施例２に係る圧縮処理の手順を示すフローチャートである。この圧縮処理の実行タイミングとしては様々なタイミングが考えられる。例えば、圧縮処理は、入力部５からデジタルコンテンツが入力された場合に実行されるようにしてもよい。なお、本実施例に係るシステム２０の処理の流れは、実施例１に係るシステム１のシーケンス図で示す処理の流れと同様であるので、説明を省略する。

【００８５】

図１３に示すステップＳ４０１～Ｓ４０９は、先の図８に示すステップＳ２０１～Ｓ２０９と同様であるので説明を省略する。図１３に示すように、圧縮部２３ａは、辞書８ｂを用いて、デジタルコンテンツのファイルの未処理のデータを圧縮する（ステップＳ４１０）。圧縮部２３ａは、デジタルコンテンツのファイルのデータが示す文字列のうち、今回圧縮された部分の文字列を先頭部分に含む文字列のコードが、辞書８ｂに未登録であるか否かを判定する（ステップＳ４１１）。未登録である場合（ステップＳ４１１肯定）には、圧縮部２３ａは、圧縮された文字列の圧縮前の文字列を含む文字列であって辞書８ｂに未登録の文字列のコードと、圧縮符号との組合せを新たに辞書８ｂに登録する（ステップＳ４１２）。一方、未登録でない場合（ステップＳ４１１否定）には、圧縮部２３ａは、デジタルコンテンツのファイルのデータのうち、圧縮処理が未処理のデータがあるか否かを判定する（ステップＳ４１６）。圧縮処理が未処理のデータがある場合（ステップＳ４１６肯定）には、ステップＳ４１０へ戻る。圧縮処理が未処理のデータがない場合（ス

テップＳ４１６否定）には、圧縮部２３ａは、処理結果を制御部２３の内部メモリに格納し、リターンする。

【００８６】

変更部２３ｂは、辞書８ｂに新たに登録された文字列の文字のうち新規に追加された文字の世代を処理対象の世代として特定し、特定した処理対象の世代のうち、下記のステップＳ４１４で未選択の処理対象の世代があるか否かを判定する（ステップＳ４１３）。未選択の処理対象の世代がある場合（ステップＳ４１３肯定）には、変更部２３ｂは、未選択の処理対象の世代を１つ選択する（ステップＳ４１４）。変更部２３ｂは、選択した処理対象の世代の葉および節点の個数が複数か否かを判定する（ステップＳ４１５）。複数である場合（ステップＳ４１５肯定）には、ステップＳ４０５へ戻る。

【００８７】

一方、未選択の処理対象の世代がない場合（ステップＳ４１３否定）、複数でない場合（ステップＳ４１５否定）には、ステップＳ４１６へ進む。

【００８８】

次に、本実施例に係る利用者端末２２の処理の流れを説明する。図１４は、実施例２に係る伸張処理の手順を示すフローチャートである。図１４に示すステップＳ５０１～Ｓ５０９は、先の図９に示すステップＳ３０１～Ｓ３０９と同様であるので説明を省略する。図１４に示すように、伸張部２４ａは、辞書１３ｂを用いて、デジタルコンテンツのファイルの未処理のデータを伸張する（ステップＳ５１０）。伸張部２４ａは、今回伸張された文字列を先頭部分に含む文字列のコードが、辞書１３ｂに未登録であるか否かを判定する（ステップＳ５１１）。未登録である場合（ステップＳ５１１肯定）には、伸張部２４ａは、伸張された文字列を含む文字列であって辞書１３ｂに未登録の文字列のコードと、圧縮符号との組合せを新たに辞書１３ｂに登録する（ステップＳ５１２）。一方、未登録でない場合（ステップＳ５１１否定）には、伸張部２４ａは、デジタルコンテンツのファイルのデータのうち、伸張処理が未処理のデータがあるか否かを判定する（ステップＳ５１６）。伸張処理が未処理のデータがある場合（ステップＳ５１６肯定）には、ステップＳ５１０へ戻る。伸張処理が未処理のデータがない場合（ステップＳ５１６否定）には、伸張部２４ａは、処理結果を制御部２４の内部メモリに格納し、リターンする。

【００８９】

変更部２４ｂは、辞書１３ｂに新たに登録された文字列の文字のうち新規に追加された文字の世代を処理対象の世代として特定し、特定した処理対象の世代のうち、下記のステップＳ５１４で未選択の処理対象の世代があるか否かを判定する（ステップＳ５１３）。未選択の処理対象の世代がある場合（ステップＳ５１３肯定）には、変更部２４ｂは、未選択の処理対象の世代を１つ選択する（ステップＳ５１４）。変更部２４ｂは、選択した処理対象の世代の葉および節点の個数が複数か否かを判定する（ステップＳ５１５）。複数である場合（ステップＳ５１５肯定）には、ステップＳ５０５へ戻る。

【００９０】

一方、未選択の処理対象の世代がない場合（ステップＳ５１３否定）、複数でない場合（ステップＳ５１５否定）には、ステップＳ５１６へ進む。

【００９１】

上述してきたように、本実施例に係るサーバ２１では、辞書８ｂの第一世代、および、辞書８ｂに新たに登録された文字列の文字のうち新規に追加された文字の世代の圧縮符号がスクランブルされて、コードと圧縮符号との組合せが変更される。これにより、圧縮されたデータの解読を試みる攻撃者などは、初期化時に辞書８ｂに登録される複数の種類の文字のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、これらの複数の種類の文字の解読が困難となる。

【００９２】

また、本実施例に係るサーバ２１では、辞書８ｂの圧縮符号をスクランブルするだけで、複雑な暗号化の処理を行わずに、解読が困難な圧縮データが生成される。したがって、本実施例に係るサーバ２１によれば、簡易な圧縮処理により難読化を図ることができる。

【００９３】
　また、本実施例に係るサーバ２１によれば、辞書８ｂの圧縮符号をスクランブルするだけで、データを圧縮するたびに圧縮されたデータおよび生データにスクランブル処理を行っていないので、簡易に圧縮データの難読化を図ることができる。
【００９４】
　また、本実施例に係る利用者端末２２では、入力されたパスワードが、サーバ２１で入力された正規のパスワードと一致しない場合には、上記の所定値が大きくなるほど、算出される剰余Ｓが、サーバ２１で算出される剰余Ｓと一致する可能性が低くなる。そのため、本実施例に係る利用者端末２２では、入力されたパスワードが正規のパスワードでない場合には、上記の所定値が大きくなるほど、辞書１３ｂの登録内容が辞書８ｂの登録内容と一致する可能性が低くなる。このため、本実施例に係る利用者端末２２では、結果として伸張されるデータが正規のものとなる可能性も低くなる。したがって、本実施例に係る利用者端末２２によれば、簡易に難読化を図ることができる。
【実施例３】
【００９５】
　さて、上記の実施例１、２では、パスワードが示す値を所定値で除算した場合の余りの値に応じて、辞書８ｂ、１３ｂに登録された文字のコードと圧縮符号との組合せを変更する場合を例示したが、開示の装置はこれに限定されない。そこで、実施例３では、他の方法で、辞書８ｂ、１３ｂに登録された文字と圧縮符号との組合せを変更する場合について説明する。実施例３では、第一のハッシュ関数を用いてパスワードから所定長の第一の値を生成し、第二のハッシュ関数を用いて第一の値から第二の値を生成する。そして、実施例３では、第二の値に応じて、辞書８ｂ、１３ｂに登録された文字と圧縮符号との組合せを変更する。
【００９６】
［システム３０の構成例］
　実施例３に係るシステムについて説明する。図１５は、実施例３に係るシステムの構成の一例を示す図である。本実施例に係るシステム３０は、サーバ３１と、利用者端末３２とを有する。サーバ３１は、実施例１に係る制御部９に代えて制御部３３を有する点が、実施例１と異なる。利用者端末３２は、実施例１に係る制御部１４に代えて制御部３４を有する点が、実施例１と異なる。なお、以下では、上記の実施例１、２と同様の機能を果たす各部や各機器については図１、図１０と同様の符号を付し、その説明は省略する場合がある。サーバ３１は、辞書や電子書籍などのデジタルコンテンツのファイルのデータを圧縮する。サーバ３１は、圧縮されたデジタルコンテンツのファイルのデータを、インターネット４を介して利用者端末３２に送信する。利用者端末３２は、受信したデジタルコンテンツのファイルのデータを伸張する。利用者端末３２は、伸張したデジタルコンテンツのファイルを再生する。
【００９７】
　サーバ３１は、入力部５と、出力部６と、送受信部７と、記憶部８と、制御部３３とを有する。
【００９８】
　制御部３３は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、これらによって種々の処理を実行する。図１５に示すように、制御部３３は、圧縮部３３ａと、変更部３３ｂとを有する。
【００９９】
　圧縮部３３ａは、実施例１に係る圧縮部９ａと同様の処理を行う。すなわち、圧縮部３３ａは、後述の変更部３３ｂにより、文字のコードと圧縮符号との組合せが変更された辞書８ｂを用いて、デジタルコンテンツのファイルのデータを圧縮する。また、圧縮部３３ａは、圧縮された文字列の圧縮前の文字列を含む文字列であって辞書８ｂに未登録の文字列と、圧縮符号との組合せを新たに辞書８ｂに登録する。
【０１００】

変更部３３ｂは、入力部５から入力されたパスワードに基づいて、文字列と圧縮符号との複数の組合せが登録された辞書８ｂの文字列と圧縮符号との組合せを変更する。具体例を挙げて説明する。まず、変更部３３ｂは、パスワードを取得する。そして、変更部３３ｂは、パスワードをシードとして、ＳＨＡ（Secure Hash Algorithm）－２５６などの第一のハッシュ関数を用いて、次の第二のハッシュ関数で用いられる所定長のハッシュ値をシードとして取得する。続いて、変更部３３ｂは、さらに第二のハッシュ関数を用いて、シードからハッシュ値を取得する。このように、第一のハッシュ関数を用いてパスワードからシードを生成するのは、第二のハッシュ関数で用いられるのに十分な所定長のシードを取得するためである。ここで、第二のハッシュ関数の一例としては、疑似乱数を発生させるための関数が挙げられる。以下では、第二のハッシュ関数として、疑似乱数を発生させるための関数を例に挙げて説明する。

【０１０１】

その後、変更部３３ｂは、変更前の圧縮符号として１６進数で「００」の値と、変更後の圧縮符号としてハッシュ値（疑似乱数）とを対応付けて記憶部８に格納する。図１６は、記憶部に記憶された情報の一例を示す図である。図１６の例では、変更部３３ｂは、変更前の圧縮符号として１６進数で「００」の値と、変更後の圧縮符号としてハッシュ値「０３」（１６進数）とを対応付けて記憶部８に格納した場合が示されている。

【０１０２】

次に、変更部３３ｂは、再び、第二のハッシュ関数を用いて、シードからハッシュ値を取得。そして、変更部３３ｂは、得られたハッシュ値が変更後の圧縮符号として記憶部８に登録されているか否かを判定する。得られたハッシュ値が変更後の圧縮符号として記憶部８に登録されている場合には、変更部３３ｂは、次のような処理を行う。すなわち、変更部３３ｂは、否定判定されるまで、得られたハッシュ値を１つインクリメントし、ハッシュ値が変更後の圧縮符号として記憶部８に登録されているか否かを判定することを繰り返し行う。ハッシュ値が変更後の圧縮符号として記憶部８に登録されていない場合には、変更部３３ｂは、変更前の圧縮符号として１６進数で「０１」の値と、変更後の圧縮符号としてハッシュ値とを対応付けて記憶部８に格納する。図１６の例では、変更部３３ｂは、変更前の圧縮符号として１６進数で「０１」の値と、変更後の圧縮符号としてハッシュ値「０７」（１６進数）とを対応付けて記憶部８に格納した場合が示されている。

【０１０３】

変更部３３ｂは、このような処理を、初期化の際に、辞書８ｂに登録された複数の文字の圧縮符号の分だけ繰り返し行う。例えば、初期化の際に辞書８ｂに１６進数で「００」から「ＦＦ」までの２５６種類の文字の圧縮符号が登録された場合には、変更部３３ｂは、「００」から「ＦＦ」までの２５６個の圧縮符号を変更前の圧縮符号として扱う。そして、変更部３３ｂは、それぞれの変更前の圧縮符号に対して、変更後の圧縮符号を生成し、変更前の圧縮符号と、変更後の圧縮符号とを対応付けて記憶部８に格納する。

【０１０４】

そして、変更部３３ｂは、初期化した辞書８ｂに登録された圧縮符号のそれぞれを、対応する変更後の圧縮符号のそれぞれに変更する。例えば、図１６の例では、変更部３３ｂは、圧縮符号が「００」の文字の圧縮符号を「０３」に変更する。また、図１６の例では、変更部３３ｂは、圧縮符号が「０１」の文字の圧縮符号を「０７」に変更する。このようにして、変更部３３ｂは、入力部５から入力されたパスワードに基づいて、文字列と圧縮符号との複数の組合せが登録された辞書８ｂの文字列と圧縮符号との組合せを変更する。上述した実施例１、２では、生成した剰余Ｓの値が１である場合には、文字のコードと圧縮符号との組合せの変更が、隣の組合せ間でしか発生しないことも想定される。しかしながら、本実施例では、パスワードから第二のハッシュ関数に用いられるシードの長さとして十分な所定長のシードを得て、第二のハッシュ関数を用いてシードからハッシュ値を生成している。このため、第二のハッシュ関数により生成されるハッシュ値は、ばらつきが出る。よって、本実施例では、文字のコードと圧縮符号との組合せの変更が、隣の組合せ間でのみ発生する確率が、実施例１、２よりも低くなる。

【０１０５】
図１７は、実施例３における圧縮符号の変更の一例を説明するための図である。図１７の例では、変更部３３ｂは、文字「ＮＵＬ」の圧縮符号を「００」から「９Ｅ」に変更する。また、図１７の例では、変更部３３ｂは、文字「ＳＯＨ」の圧縮符号を「０１」から「Ｃ５」に変更する。また、図１７の例では、変更部３３ｂは、文字「ａ」の圧縮符号を「６１」から「９Ｆ」に変更する。また、図１７の例では、変更部３３ｂは、文字「ｂ」の圧縮符号を「６２」から「３９」に変更する。また、図１７の例では、変更部３３ｂは、文字「ＤＥＬ」の圧縮符号を「ＦＦ」から「００」に変更する。
【０１０６】
このように、本実施例に係るサーバ３１では、辞書８ｂの第一世代の葉および節点の圧縮符号がスクランブルされて、コードと圧縮符号との組合せが変更される。これにより、圧縮されたデータの解読を試みる攻撃者などは、初期化時に辞書８ｂに登録される複数の種類の文字のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、これらの複数の種類の文字の解読が困難となる。この結果、これらの複数の種類の文字を先頭文字に含む文字列の解読についても困難となる。
【０１０７】
また、本実施例に係るサーバ３１では、辞書８ｂの圧縮符号をスクランブルするだけで、複雑な暗号化の処理を行わずに、解読が困難な圧縮データが生成される。したがって、本実施例に係るサーバ２によれば、簡易な圧縮処理により難読化を図ることができる。また、処理対象データのサイズ増大に応じた処理コストの増大を抑制することができる。
【０１０８】
また、本実施例に係るサーバ３１によれば、辞書８ｂの圧縮符号をスクランブルするだけで、データを圧縮するたびに圧縮されたデータおよび生データにスクランブル処理を行っていないので、簡易に圧縮データの難読化を図ることができる。
【０１０９】
利用者端末３２は、入力部１０と、出力部１１と、送受信部１２と、記憶部１３と、制御部３４とを有する。
【０１１０】
制御部３４は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、これらによって種々の処理を実行する。図１５に示すように、制御部２４は、伸張部３４ａと、変更部３４ｂと、再生部１４ｃとを有する。
【０１１１】
伸張部３４ａは、実施例１に係る伸張部１４ａと同様の処理を行う。すなわち、伸張部３４ａは、後述の変更部３４ｂにより、文字のコードと圧縮符号との組合せが変更された辞書１３ｂを用いて、デジタルコンテンツのファイルのデータを伸張する。また、伸張部３４ａは、伸張された文字を含む文字列であって辞書１３ｂに未登録の文字列と、圧縮符号との組合せを新たに辞書１３ｂに登録する。
【０１１２】
変更部３４ｂは、入力部１０から入力されたパスワードに基づいて、文字列と圧縮符号との複数の組合せが登録された辞書１３ｂの文字列と圧縮符号との組合せを変更する。具体例を挙げて説明する。まず、変更部３４ｂは、パスワードを取得する。そして、変更部３４ｂは、パスワードをシードとして、ＳＨＡ－２５６などの第一のハッシュ関数を用いて、次の第二のハッシュ関数で用いられる所定長のハッシュ値をシードとして取得する。続いて、変更部３４ｂは、さらに第二のハッシュ関数を用いて、シードからハッシュ値を取得する。このように、第一のハッシュ関数を用いてパスワードからシードを生成するのは、第二のハッシュ関数で用いられるのに十分な所定長のシードを取得するためである。
【０１１３】
その後、変更部３４ｂは、変更前の圧縮符号として１６進数で「００」の値と、変更後の圧縮符号としてハッシュ値とを対応付けて記憶部１３に格納する。次に、変更部３４ｂは、再び、第二のハッシュ関数を用いて、シードからハッシュ値を取得する。そして、変

更部３４ｂは、得られたハッシュ値が変更後の圧縮符号として記憶部１３に記憶されているか否かを判定する。得られたハッシュ値が変更後の圧縮符号として記憶部１３に記憶されている場合には、変更部３４ｂは、次のような処理を行う。すなわち、変更部３４ｂは、否定判定されるまで、得られたハッシュ値を１つインクリメントし、ハッシュ値が変更後の圧縮符号として記憶部１３に記憶されているか否かを判定することを繰り返し行う。ハッシュ値が変更後の圧縮符号として記憶部１３に記憶されていない場合には、変更部３４ｂは、変更前の圧縮符号として１６進数で「０１」の値と、変更後の圧縮符号としてハッシュ値とを対応付けて記憶部１３に格納する。

【０１１４】

変更部３４ｂは、このような処理を、初期化の際に、辞書１３ｂに登録された複数の文字の圧縮符号の分だけ繰り返し行う。例えば、初期化の際に辞書１３ｂに１６進数で「００」から「ＦＦ」までの２５６種類の文字の圧縮符号が登録された場合には、変更部３４ｂは、「００」から「ＦＦ」までの２５６個の圧縮符号を変更前の圧縮符号として扱う。そして、変更部３４ｂは、それぞれの変更前の圧縮符号に対して、変更後の圧縮符号を生成し、変更前の圧縮符号と、変更後の圧縮符号とを対応付けて記憶部１３に格納する。

【０１１５】

そして、変更部３４ｂは、初期化した辞書１３ｂに登録された圧縮符号のそれぞれを、対応する変更後の圧縮符号のそれぞれに変更する。

【０１１６】

このように、本実施例に係る利用者端末３２では、入力されたパスワードが、サーバ３１で入力された正規のパスワードと一致しない場合には、双方のパスワードから得られるハッシュ値が一致しない限り、伸張されるデータが正規のものとならない。したがって、本実施例に係る利用者端末３２によれば、簡易に難読化を図ることができる。

【０１１７】

制御部３４は、ＡＳＩＣ（Application Specific Integrated Circuit）やＦＰＧＡ（Field Programmable Gate Array）などの集積回路を有する。なお、制御部３４は、ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）などの電子回路を有してもよい。

【０１１８】

［処理の流れ］

次に、本実施例に係るサーバ３１の処理の流れを説明する。図１８は、実施例３に係る圧縮処理の手順を示すフローチャートである。この圧縮処理の実行タイミングとしては様々なタイミングが考えられる。例えば、圧縮処理は、入力部５からデジタルコンテンツが入力された場合に実行されるようにしてもよい。なお、本実施例に係るシステム３０の処理の流れは、実施例１に係るシステム１のシーケンス図で示す処理の流れと同様であるので、説明を省略する。

【０１１９】

図１８に示すステップＳ６０１～Ｓ６０３は、先の図８に示すステップＳ２０１～Ｓ２０３と同様であるので説明を省略する。図１８に示すように、変更部３３ｂは、変数ｉの値に「０」を設定する（ステップＳ６０４）。変更部３３ｂは、パスワードをシードとして、第一のハッシュ関数を用いて、次の第二のハッシュ関数で用いられる所定長のハッシュ値をシードとして取得する（ステップＳ６０５）。変更部３３ｂは、疑似乱数を発生させるための関数を用いて、シードから疑似乱数を発生させる（ステップＳ６０６）。変更部３３ｂは、疑似乱数が、「変更後の圧縮符号」として記憶部８に登録されているか否かを判定する（ステップＳ６０７）。登録されている場合（ステップＳ６０７肯定）には、変更部３３ｂは、擬似乱数の値を１つインクリメントし（ステップＳ６０８）、ステップＳ６０７へ戻る。

【０１２０】

一方、登録されていない場合（ステップＳ６０７否定）には、変更部３３ｂは、処理対象の世代の「変更前の圧縮符号」としての変数ｉと、「変更後の圧縮符号」としての擬似

乱数とを対応付けて記憶部８に登録する（ステップＳ６０９）。なお、本実施例では、処理対象の世代は、第一世代である。変更部３３ｂは、変数ｉの値を１つインクリメントする（ステップＳ６１０）。変更部３３ｂは、変数ｉの値が、処理対象の世代の葉および節点の個数Ｌより大きいか否かを判定する（ステップＳ６１１）。変数ｉの値が、Ｌ以下である場合（ステップＳ６１１否定）には、ステップＳ６０６へ戻る。一方、変数ｉの値がＬより大きい場合（ステップＳ６１１肯定）には、変更部３３ｂは、初期化した辞書８ｂに登録された圧縮符号のそれぞれを、対応する変更後の圧縮符号のそれぞれに変更する（ステップＳ６１２）。圧縮部３３ａは、辞書８ｂを用いて、デジタルコンテンツのファイルのデータを圧縮しつつ、辞書８ｂを更新し（ステップＳ６１３）、処理結果を制御部３３の内部メモリに格納し、リターンする。

【０１２１】

次に、本実施例に係る利用者端末３２の処理の流れを説明する。図１９は、実施例３に係る伸張処理の手順を示すフローチャートである。伸張処理においても、図１８において説明した圧縮処理と共通の辞書更新アルゴリズムを用いる。図１９に示すステップＳ７０１～Ｓ７０３は、先の図９に示すステップＳ３０１～Ｓ３０３と同様であるので説明を省略する。図１９に示すように、変更部３４ｂは、変数ｉの値に「０」を設定する（ステップＳ７０４）。変更部３４ｂは、パスワードをシードとして、第一のハッシュ関数を用いて、次の第二のハッシュ関数で用いられる所定長のハッシュ値をシードとして取得する（ステップＳ７０５）。変更部３４ｂは、疑似乱数を発生させるための関数を用いて、シードから疑似乱数を発生させる（ステップＳ７０６）。変更部３４ｂは、疑似乱数が、「変更後の圧縮符号」として記憶部８に登録されているか否かを判定する（ステップＳ７０７）。登録されている場合（ステップＳ７０７肯定）には、変更部３４ｂは、擬似乱数の値を１つインクリメントし（ステップＳ７０８）、ステップＳ７０７へ戻る。

【０１２２】

一方、登録されていない場合（ステップＳ７０７否定）には、変更部３４ｂは、処理対象の世代の「変更前の圧縮符号」としての変数ｉと、「変更後の圧縮符号」としての擬似乱数とを対応付けて記憶部８に登録する（ステップＳ７０９）。なお、本実施例では、処理対象の世代は、第一世代である。変更部３４ｂは、変数ｉの値を１つインクリメントする（ステップＳ７１０）。変更部３４ｂは、変数ｉの値が、処理対象の世代の葉および節点の個数Ｌより大きいか否かを判定する（ステップＳ７１１）。変数ｉの値が、Ｌ以下である場合（ステップＳ７１１否定）には、ステップＳ７０６へ戻る。一方、変数ｉの値がＬより大きい場合（ステップＳ７１１肯定）には、変更部３４ｂは、初期化した辞書８ｂに登録された圧縮符号のそれぞれを、対応する変更後の圧縮符号のそれぞれに変更する（ステップＳ７１２）。伸張部３４ａは、辞書８ｂを用いて、デジタルコンテンツのファイルのデータを伸張しつつ、辞書８ｂを更新し（ステップＳ７１３）、処理結果を制御部３４の内部メモリに格納し、リターンする。

【０１２３】

上述してきたように、本実施例に係るサーバ３１では、辞書８ｂの第一世代の葉および節点の圧縮符号がスクランブルされて、コードと圧縮符号との組合せが変更される。これにより、圧縮されたデータの解読を試みる攻撃者などは、初期化時に辞書８ｂに登録される複数の種類の文字のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、これらの複数の種類の文字の解読が困難となる。この結果、これらの複数の種類の文字を先頭文字に含む文字列の解読についても困難となる。

【０１２４】

また、本実施例に係るサーバ３１では、辞書８ｂの圧縮符号をスクランブルするだけで、複雑な暗号化の処理を行わずに、解読が困難な圧縮データが生成される。したがって、本実施例に係るサーバ３１によれば、簡易な圧縮処理により難読化を図ることができる。また、処理対象データのサイズ増大に応じた処理コストの増大を抑制することができる。

【０１２５】

また、本実施例に係るサーバ３１によれば、辞書８ｂの圧縮符号をスクランブルするだ

けで、データを圧縮するたびに圧縮されたデータおよび生データにスクランブル処理を行っていないので、簡易に圧縮データの難読化を図ることができる。

【０１２６】

また、本実施例に係る利用者端末３２では、入力されたパスワードが、サーバ３１で入力された正規のパスワードと一致しない場合には、双方のパスワードから得られるハッシュ値が一致しない限り、伸張されるデータが正規のものとならない。したがって、本実施例に係る利用者端末３２によれば、簡易に難読化を図ることができる。

【実施例４】

【０１２７】

さて、上記の実施例３では、実施例１、２とは異なる他の方法で、第一世代の文字と圧縮符号との組合せを変更する場合を例示したが、開示の装置はこれに限定されない。そこで、実施例４では、実施例３の方法と同様の方法で、第二世代以降の文字と圧縮符号との組合せも変更する場合について説明する。

【０１２８】

［システム４０の構成例］

実施例４に係るシステムについて説明する。図２０は、実施例４に係るシステムの構成の一例を示す図である。本実施例に係るシステム４０は、サーバ４１と、利用者端末４２とを有する。サーバ４１は、実施例１に係る制御部９に代えて制御部４３を有する点が、実施例１と異なる。利用者端末４２は、実施例１に係る制御部１４に代えて制御部４４を有する点が、実施例１と異なる。なお、以下では、上記の実施例１～３と同様の機能を果たす各部や各機器については図１、図１０、図１５と同様の符号を付し、その説明は省略する場合がある。サーバ４１は、辞書や電子書籍などのデジタルコンテンツのファイルのデータを圧縮する。サーバ４１は、圧縮されたデジタルコンテンツのファイルのデータを、インターネット４を介して利用者端末４２に送信する。利用者端末４２は、受信したデジタルコンテンツのファイルのデータを伸張する。利用者端末４２は、伸張したデジタルコンテンツのファイルを再生する。

【０１２９】

サーバ４１は、入力部５と、出力部６と、送受信部７と、記憶部８と、制御部４３とを有する。

【０１３０】

制御部４３は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、これらによって種々の処理を実行する。図２０に示すように、制御部４３は、圧縮部４３ａと、変更部４３ｂとを有する。

【０１３１】

圧縮部４３ａは、実施例１に係る圧縮部９ａと同様の処理を行う。すなわち、圧縮部４３ａは、後述の変更部４３ｂにより、文字のコードと圧縮符号との組合せが変更された辞書８ｂを用いて、デジタルコンテンツのファイルのデータを圧縮する。また、圧縮部４３ａは、圧縮された文字列の圧縮前の文字列を含む文字列であって辞書８ｂに未登録の文字列と、圧縮符号との組合せを新たに辞書８ｂに登録する。

【０１３２】

変更部４３ｂは、実施例３に係る変更部３３ｂと同様の処理を行う。さらに、変更部４３ｂは、入力部５から入力されたパスワードに基づいて、辞書８ｂに新たに登録された文字列と圧縮符号との組合せを新たに変更する。具体例を挙げて説明する。

【０１３３】

変更部４３ｂは、辞書８ｂに文字列と圧縮符号との組合せが新たに登録されるたびに、新たに登録された文字列の文字のうち、新規に追加された文字の世代を処理対象の世代として特定する。

【０１３４】

そして、変更部４３ｂは、実施例３に係る変更部３３ｂが辞書８ｂに登録された第一世代の文字列と圧縮符号との組合せを変更する方法と同様の方法で、特定した処理対象の世

代の文字列と圧縮符号との組合せを変更する。すなわち、変更部４３ｂは、特定した処理対象の世代の圧縮符号のそれぞれを「変更前の圧縮符号」とし、「変更前の圧縮符号」ごとに第二のハッシュ関数を用いてシードからハッシュ値を生成する。ここで、変更部４３ｂは、生成されるハッシュ値が、特定した世代に応じた値、例えば、特定した世代が第二世代の場合には、１６進数で「１００」以上となるように、ハッシュ値の範囲を調整する。そして、変更部４３ｂは、「変更前の圧縮符号」のそれぞれと、ハッシュ値のそれぞれとを対応付けて記憶部８に登録する。図２１は、実施例４に係るシステムが実行する処理の一例を説明するための図である。図２１の例は、辞書８ｂに未登録の文字列「ａｂｏｕｔ」のコードと圧縮符号との組合せが、圧縮部４３ａにより辞書８ｂに新たに登録された場合の変更部４３ｂの処理の一例を示す。図２１の例では、変更部４３ｂは、文字列「ａｂｏｕｔ」の第二世代の文字「ｂ」の圧縮符号を「１００」から「１６１」に変更する。また、図２１の例では、変更部４３ｂは、第三世代の文字「ｏ」の圧縮符号を「１０１」から「１ＦＦ」に変更する。また、図２１の例では、変更部４３ｂは、第四世代の文字「ｕ」の圧縮符号を「１０２」から「１００」に変更する。また、図２１の例では、第五世代の文字「ｔ」の圧縮符号を「１０３」から「１Ｂ２」に変更する。

【０１３５】

このように、本実施例に係るサーバ４１では、辞書８ｂの第一世代、および、辞書８ｂに新規に追加された文字の世代の葉および節点の圧縮符号がスクランブルされて、コードと圧縮符号との組合せが変更される。これにより、圧縮されたデータの解読を試みる攻撃者などは、初期化時に辞書８ｂに登録される複数の種類の文字のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、これらの複数の種類の文字の解読が困難となる。

【０１３６】

また、本実施例に係るサーバ４１では、辞書８ｂの圧縮符号をスクランブルするだけで、複雑な暗号化の処理を行わずに、解読が困難な圧縮データが生成される。したがって、本実施例に係るサーバ４１によれば、簡易な圧縮処理により難読化を図ることができる。また、処理対象データのサイズ増大に応じた処理コストの増大を抑制することができる。

【０１３７】

また、本実施例に係るサーバ４１によれば、辞書８ｂの圧縮符号をスクランブルするだけで、データを圧縮するたびに圧縮されたデータおよび生データにスクランブル処理を行っていないので、簡易に圧縮データの難読化を図ることができる。

【０１３８】

利用者端末４２は、入力部１０と、出力部１１と、送受信部１２と、記憶部１３と、制御部４４とを有する。

【０１３９】

制御部４４は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、これらによって種々の処理を実行する。図２０に示すように、制御部４４は、伸張部４４ａと、変更部４４ｂと、再生部１４ｃとを有する。

【０１４０】

伸張部４４ａは、実施例１に係る伸張部１４ａと同様の処理を行う。すなわち、伸張部４４ａは、後述の変更部４４ｂにより、文字のコードと圧縮符号との組合せが変更された辞書１３ｂを用いて、デジタルコンテンツのファイルのデータを伸張する。また、伸張部４４ａは、伸張された文字を含む文字列であって辞書１３ｂに未登録の文字列と、圧縮符号との組合せを新たに辞書１３ｂに登録する。

【０１４１】

変更部４４ｂは、実施例３に係る変更部３４ｂと同様の処理を行う。さらに、変更部４４ｂは、入力部１０から入力されたパスワードに基づいて、辞書１３ｂに新たに登録された文字列と圧縮符号との組合せを新たに変更する。具体例を挙げて説明する。

【０１４２】

変更部４４ｂは、辞書１３ｂに文字列と圧縮符号との組合せが新たに登録されるたびに

、新たに登録された文字列の文字のうち、新規に追加された文字の世代を処理対象の世代として特定する。

【０１４３】

そして、変更部４４ｂは、実施例３に係る変更部３４ｂが辞書１３ｂに登録された第一世代の文字列と圧縮符号との組合せを変更する方法と同様の方法で、特定した処理対象の世代の文字列と圧縮符号との組合せを変更する。すなわち、変更部４４ｂは、特定した処理対象の世代の圧縮符号のそれぞれを「変更前の圧縮符号」とし、「変更前の圧縮符号」ごとに第二のハッシュ関数を用いてシードからハッシュ値を生成する。ここで、変更部４４ｂは、生成されるハッシュ値が、特定した世代に応じた値、例えば、特定した世代が第二世代の場合には、１６進数で「１００」以上となるように、ハッシュ値の範囲を調整する。そして、変更部４４ｂは、「変更前の圧縮符号」のそれぞれと、ハッシュ値のそれぞれとを対応付けて記憶部８に登録する。

【０１４４】

このように、本実施例に係る利用者端末４２では、入力されたパスワードが、サーバ４１で入力された正規のパスワードと一致しない場合には、双方のパスワードから得られるハッシュ値が一致しない限り、伸張されるデータが正規のものとならない。したがって、本実施例に係る利用者端末４２によれば、簡易に難読化を図ることができる。

【０１４５】

制御部４４は、ＡＳＩＣ（Application Specific Integrated Circuit）やＦＰＧＡ（Field Programmable Gate Array）などの集積回路を有する。なお、制御部４４は、ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）などの電子回路を有してもよい。

【０１４６】

［処理の流れ］

次に、本実施例に係るサーバ４１の処理の流れを説明する。図２２は、実施例４に係る圧縮処理の手順を示すフローチャートである。この圧縮処理の実行タイミングとしては様々なタイミングが考えられる。例えば、圧縮処理は、入力部５からデジタルコンテンツが入力された場合に実行されるようにしてもよい。なお、本実施例に係るシステム４０の処理の流れは、実施例１に係るシステム１のシーケンス図で示す処理の流れと同様であるので、説明を省略する。

【０１４７】

図２２に示すステップＳ８０１～Ｓ８１２は、先の図１８に示すステップＳ６０１～Ｓ６１２と同様であるので説明を省略する。図２２に示すように、圧縮部４３ａは、辞書８ｂを用いて、デジタルコンテンツのファイルのデータを圧縮する（ステップＳ８１３）。圧縮部４３ａは、デジタルコンテンツのファイルのデータが示す文字列のうち、今回圧縮された部分の文字列を先頭部分に含む文字列のコードが、辞書８ｂに未登録であるか否かを判定する（ステップＳ８１４）。未登録である場合（ステップＳ８１４肯定）には、圧縮部４３ａは、圧縮された文字列の圧縮前の文字列を含む文字列であって辞書８ｂに未登録の文字列のコードと、圧縮符号との組合せを新たに辞書８ｂに登録する（ステップＳ８１５）。

【０１４８】

一方、未登録でない場合（ステップＳ８１４否定）には、圧縮部４３ａは、デジタルコンテンツのファイルのデータのうち、圧縮処理が未処理のデータがあるか否かを判定する（ステップＳ８２０）。圧縮処理が未処理のデータがある場合（ステップＳ８２０肯定）には、ステップＳ８１３へ戻る。圧縮処理が未処理のデータがない場合（ステップＳ８２０否定）には、圧縮部４３ａは、処理結果を制御部４３の内部メモリに格納し、リターンする。

【０１４９】

変更部４３ｂは、辞書８ｂに新たに登録された文字列の文字のうち新規に追加された文字の世代を処理対象の世代として特定し、特定した処理対象の世代のうち、下記のステッ

プＳ８１７で未選択の処理対象の世代があるか否かを判定する（ステップＳ８１６）。未選択の処理対象の世代がある場合（ステップＳ８１６肯定）には、変更部４３ｂは、未選択の処理対象の世代を１つ選択する（ステップＳ８１７）。変更部４３ｂは、選択した処理対象の世代の葉および節点の個数が複数か否かを判定する（ステップＳ８１８）。複数である場合（ステップＳ８１８肯定）には、変更部４３ｂは、変数ｉの値を０に設定する（ステップＳ８１９）。そして、変更部４３ｂは、再び擬似乱数を発生させ（ステップＳ８０６）、疑似乱数が、「変更後の圧縮符号」として記憶部８に登録されているか否かを判定する（ステップＳ８０７）。登録されていない場合（ステップＳ８０７否定）には、変更部４３ｂは、処理対象の世代の「変更前の圧縮符号」と、「変更後の圧縮符号」としての擬似乱数とを対応付けて記憶部８に登録する（ステップＳ８０９）。

【０１５０】

一方、未選択の処理対象の世代がない場合（ステップＳ８１６否定）、複数でない場合（ステップＳ８１８否定）には、ステップＳ８２０へ進む。

【０１５１】

次に、本実施例に係る利用者端末４２の処理の流れを説明する。図２３は、実施例４に係る伸張処理の手順を示すフローチャートである。図２３に示すステップＳ９０１～Ｓ９１２は、先の図１９に示すステップＳ７０１～Ｓ７１２と同様であるので説明を省略する。図２３に示すように、伸張部４４ａは、辞書１３ｂを用いて、デジタルコンテンツのファイルのデータを伸張する（ステップＳ９１３）。伸張部４４ａは、デジタルコンテンツのファイルのデータが示す文字列のうち、今回圧縮された部分の文字列を先頭部分に含む文字列のコードが、辞書１３ｂに未登録であるか否かを判定する（ステップＳ９１４）。未登録である場合（ステップＳ９１４肯定）には、伸張部４４ａは、圧縮された文字列の圧縮前の文字列を含む文字列であって辞書１３ｂに未登録の文字列のコードと、圧縮符号との組合せを新たに辞書１３ｂに登録する（ステップＳ９１５）。

【０１５２】

一方、未登録でない場合（ステップＳ９１４否定）には、伸張部４４ａは、デジタルコンテンツのファイルのデータのうち、圧縮処理が未処理のデータがあるか否かを判定する（ステップＳ９２０）。圧縮処理が未処理のデータがある場合（ステップＳ９２０肯定）には、ステップＳ９１３へ戻る。圧縮処理が未処理のデータがない場合（ステップＳ９２０否定）には、伸張部４４ａは、処理結果を制御部４４の内部メモリに格納し、リターンする。

【０１５３】

変更部４４ｂは、辞書１３ｂに新たに登録された文字列の文字のうち新規に追加された文字の世代を処理対象の世代として特定し、特定した処理対象の世代のうち、下記のステップＳ９１７で未選択の処理対象の世代があるか否かを判定する（ステップＳ９１６）。未選択の処理対象の世代がある場合（ステップＳ９１６肯定）には、変更部４４ｂは、未選択の処理対象の世代を１つ選択する（ステップＳ９１７）。変更部４４ｂは、選択した処理対象の世代の葉および節点の個数が複数か否かを判定する（ステップＳ９１８）。複数である場合（ステップＳ９１８肯定）には、変更部４４ｂは、変数ｉの値を０に設定する（ステップＳ９１９）。そして、変更部４４ｂは、再び擬似乱数を発生させ（ステップＳ９０６）、疑似乱数が、「変更後の圧縮符号」として記憶部１３に登録されているか否かを判定する（ステップＳ９０７）。登録されていない場合（ステップＳ９０７否定）には、変更部４４ｂは、処理対象の世代の「変更前の圧縮符号」と、「変更後の圧縮符号」としての擬似乱数とを対応付けて記憶部１３に登録する（ステップＳ９０９）。

【０１５４】

一方、未選択の処理対象の世代がない場合（ステップＳ９１６否定）、複数でない場合（ステップＳ９１８否定）には、ステップＳ９２０へ進む。

【０１５５】

上述してきたように、本実施例に係るサーバ４１では、辞書８ｂの第一世代、および、辞書８ｂに新たに登録された文字列の文字のうち新規に追加された文字の世代の圧縮符号

がスクランブルされて、コードと圧縮符号との組合せが変更される。これにより、圧縮されたデータの解読を試みる攻撃者などは、初期化時に辞書８ｂに登録される複数の種類の文字のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、これらの複数の種類の文字の解読が困難となる。

【０１５６】

また、本実施例に係るサーバ４１では、辞書８ｂの圧縮符号をスクランブルするだけで、複雑な暗号化の処理を行わずに、解読が困難な圧縮データが生成される。したがって、本実施例に係るサーバ４１によれば、簡易な圧縮処理により難読化を図ることができる。

【０１５７】

また、本実施例に係るサーバ４１によれば、辞書８ｂの圧縮符号をスクランブルするだけで、データを圧縮するたびに圧縮されたデータおよび生データにスクランブル処理を行っていないので、簡易に圧縮データの難読化を図ることができる。また、処理対象データのサイズ増大に応じた処理コストの増大を抑制することができる。

【０１５８】

また、本実施例に係る利用者端末４２では、入力されたパスワードが、サーバ４１で入力された正規のパスワードと一致しない場合には、双方のパスワードから得られるハッシュ値が一致しない限り、伸張されるデータが正規のものとならない。したがって、本実施例に係る利用者端末４２によれば、簡易に難読化を図ることができる。

【実施例５】

【０１５９】

さて、上記の実施例１～４では、データを圧縮する圧縮方式として、ＬＺ７８の圧縮方式を採用する場合を例示したが、開示の装置はこれに限定されない。そこで、実施例５では、データを圧縮する圧縮方式として、ＬＺ７７の圧縮方式を採用する場合について説明する。

【０１６０】

［システム５０の構成例］

実施例５に係るシステムについて説明する。図２４は、実施例５に係るシステムの構成の一例を示す図である。本実施例に係るシステム５０は、サーバ５１と、利用者端末５２とを有する。サーバ５１は、実施例１に係る記憶部８、制御部９に代えて記憶部５３、制御部５４を有する点が、実施例１と異なる。利用者端末５２は、実施例１に係る記憶部１３、制御部１４に代えて記憶部５５、制御部５６を有する点が、実施例１と異なる。なお、以下では、上記の実施例１～４と同様の機能を果たす各部や各機器については図１、図１０、図１５、図２０と同様の符号を付し、その説明は省略する場合がある。サーバ５１は、辞書や電子書籍などのデジタルコンテンツのファイルのデータを圧縮する。サーバ５１は、圧縮されたデジタルコンテンツのファイルのデータを、インターネット４を介して利用者端末５２に送信する。利用者端末５２は、受信したデジタルコンテンツのファイルのデータを伸張する。利用者端末５２は、伸張したデジタルコンテンツのファイルを再生する。

【０１６１】

サーバ５１は、入力部５と、出力部６と、送受信部７と、記憶部５３と、制御部５４とを有する。

【０１６２】

記憶部５３は、各種情報を記憶する。例えば、記憶部５３は、コンテンツＤＢ８ａ、予約語テーブル５３ａを記憶する。

【０１６３】

予約語テーブル５３ａには、デジタルコンテンツのデータに含まれ、一般的な文字より出現頻度が高いＨＴＭＬ（Hyper Text Markup Language）のタグ、および出現頻度の高い文字などが登録される。予約語テーブル５３ａは、後述の圧縮部５４ｂによりデジタルコンテンツのファイルを圧縮する際に用いられる。図２５は、予約語テーブルの一例を示す図である。図２５の例は、予約語テーブル５３ａに、Ｎ個のタグが登録された場合を

示す。図２５の例は、予約語テーブル５３ａの１番目のレコードにＨＴＭＬの「 」タグが登録された場合を示す。また、図２５の例は、予約語テーブル５３ａの２番目のレコードにＨＴＭＬの「</color>」タグが登録された場合を示す。図２５の例は、予約語テーブル５３ａのＮ番目のレコードにＨＴＭＬの「</title>」タグが登録された場合を示す。

【０１６４】

記憶部５３は、例えば、フラッシュメモリなどの半導体メモリ素子、または、ハードディスク、光ディスクなどの記憶装置である。なお、記憶部５３は、上記の種類の記憶装置に限定されるものではなく、ＲＡＭ（Random Access Memory)、ＲＯＭ（Read Only Memory)であってもよい。

【０１６５】

制御部５４は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、これらによって種々の処理を実行する。図２４に示すように、制御部５４は、生成部５４ａと、圧縮部５４ｂとを有する。

【０１６６】

生成部５４ａは、入力部５から入力されたパスワードに応じた文字列を生成する。例えば、生成部５４ａは、まず、パスワードの各桁の和を算出する。そして、生成部５４ａは、算出した和を予約語テーブル５３ａに登録されたタグの数Ｎで除算した場合の剰余Ｄを算出する。続いて、生成部５４ａは、剰余Ｄの値が示す番号のレコードを起点として、予約語テーブル５３ａの各レコードに登録されたタグを取得し、取得したタグを連結した文字列を生成する。このようにして、生成部５４ａは、予約語テーブル５３ａの登録の順番が変更された予約語を並べた文字列を生成する。

【０１６７】

図２６Ａおよび図２６Ｂは、生成部により生成された文字列の一例を示す図である。図２６Ａの例は、図２５の例において、生成部５４ａにより値が「１」である剰余Ｄが算出された場合に、生成部５４ａが、１番目のレコードを起点として、文字列を生成した場合の一例を示す。すなわち、図２６Ａの例は、生成部５４ａが、予約語テーブル５３ａの１番目、２番目、３番目、・・・、Ｎ番目のレコードの各レコードに登録されたタグを取得し、取得したタグを連結した文字列「 </color>・・・</title>」を生成した場合を示す。また、図２６Ｂの例は、図２５の例において、生成部５４ａにより値が「１」である剰余Ｄが算出された場合に、生成部５４ａが、１番目のレコードを起点として、文字列を生成した場合の一例を示す。すなわち、図２６Ｂの例は、生成部５４ａが、予約語テーブル５３ａの１番目、Ｎ番目、（Ｎ－１）番目、・・・、２番目のレコードの各レコードに登録されたタグを取得し、取得したタグを連結した文字列「 </title>・・・</color>」を生成した場合を示す。

【０１６８】

圧縮部５４ｂは、生成部５４ａにより生成された文字列、および圧縮された文字列の圧縮前の文字列を用いて、文字列を圧縮する。具体例を挙げて説明する。図２７は、実施例５に係るシステムの処理を説明するための図である。図２７の例では、参照部７１および符号化部７２を有するスライド窓７０の先頭に、さらに、文字列を初期化の際に設定するための設定部７３が設けられている。圧縮部５４ｂは、生成部５４ａにより生成された文字列を、設定部７３に設定する。ここで、スライド窓７０がデータ上をスライドしても、設定部７３に設定された文字列は設定されたままとなる。図２７の例では、設定部７３に文字列「 ・・・</color>」が設定された場合が示されている。

【０１６９】

圧縮部５４ｂは、符号化部７２内の先頭のデータを圧縮する場合に、設定部７３および参照部７１内の最長一致系列の位置、および最長一致系列の長さを示すポインタを生成する。ここで、圧縮部５４ｂは、符号化部７２内の先頭のデータと一致する最長のデータを設定部７３および参照部７１内から検索する。また、圧縮部５４ｂは、ポインタに含まれる最長一致系列の位置として、参照部７１の先頭からのアドレスではなく、設定部７３に

設定された文字列の先頭からのアドレスを用いる。

【０１７０】

このように、本実施例に係るサーバ５１によれば、出現頻度の高い文字やタグなどが初期化時に設定部７３に設定されるので、圧縮効率が良くなる。また、本実施例に係るサーバ５１では、ポインタが示す最長一致系列の位置は、設定部７３に設定された文字列の先頭からのアドレスである。そのため、本実施例に係るサーバ５１によれば、圧縮されたデータの解読を試みる攻撃者などが、ポインタが示す最長一致系列の位置を参照部７１の先頭からのアドレスと把握している場合には、攻撃者による圧縮データの解読の困難性を高めることができる。

【０１７１】

また、本実施例に係るサーバ５１では、設定部７３に文字列を設定し、ポインタが示す最長一致系列の位置を設定部７３に設定された文字列の先頭からのアドレスとするという、ＲＳＡなどの暗号化処理と比較すると、簡易な処理で圧縮符号がスクランブルされる。このように、本実施例に係るサーバ５１は、複雑な暗号化の処理を行わずに、解読が困難な圧縮データを生成する。したがって、本実施例に係るサーバ５１によれば、簡易に圧縮データの難読化を図ることができる。また、処理対象データのサイズ増大に応じた処理コストの増大を抑制することができる。

【０１７２】

また、本実施例に係るサーバ５１では、ポインタが示す最長一致系列の位置を設定部７３に設定された文字列の先頭からのアドレスとするだけで、データを圧縮するたびに圧縮されたデータおよび生データにスクランブル処理を行っていない。そのため、本実施例に係るサーバ５１によれば、簡易に圧縮データの難読化を図ることができる。

【０１７３】

利用者端末５２は、入力部１０と、出力部１１と、送受信部１２と、記憶部５５と、制御部５６とを有する。

【０１７４】

記憶部５５は、各種情報を記憶する。例えば、記憶部５５は、コンテンツＤＢ８ａ、予約語テーブル５５ａを記憶する。

【０１７５】

予約語テーブル５５ａは、上述した予約語テーブル５３ａと同様のテーブルであるので、説明を省略する。

【０１７６】

記憶部５５は、例えば、フラッシュメモリなどの半導体メモリ素子、または、ハードディスク、光ディスクなどの記憶装置である。なお、記憶部５５は、上記の種類の記憶装置に限定されるものではなく、ＲＡＭ（Random Access Memory)、ＲＯＭ（Read Only Memory)であってもよい。

【０１７７】

制御部５６は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、これらによって種々の処理を実行する。図２４に示すように、制御部５６は、生成部５６ａと、伸張部５６ｂと、再生部１４ｃとを有する。

【０１７８】

生成部５６ａは、上述した生成部５４ａと同様の処理を行う。すなわち、生成部５６ａは、入力部１０から入力されたパスワードに応じた文字列を生成する。例えば、生成部５６ａは、まず、パスワードの各桁の和を算出する。そして、生成部５６ａは、算出した和を予約語テーブル５５ａに登録されたタグの数Ｎで除算した場合の剰余Ｄを算出する。続いて、生成部５６ａは、剰余Ｄの値が示す番号のレコードを起点として、予約語テーブル５５ａの各レコードに登録されたタグを取得し、取得したタグを連結した文字列を生成する。

【０１７９】

伸張部５６ｂは、生成部５６ａにより生成された文字列、および伸張された文字列を用

いて、圧縮された文字列を伸張する。具体例を挙げて説明する。伸張部５６ｂは、生成部５６ａにより生成された文字列を、設定部７３に設定する。ここで、スライド窓７０がデータ上をスライドしても、設定部７３に設定された文字列は設定されたままとなる。

【０１８０】

伸張部５６ｂは、符号化部７２内のポインタを伸張する場合に、ポインタが示す設定部７３に設定された文字列の先頭からのアドレスが示す文字を特定する。そして、伸張部５６ｂは、特定した文字から、ポインタが示す長さ分の文字列を設定部７３および参照部７１内の文字列から取得し、伸張バッファに格納することで伸張を行う。なお、伸張部５６ｂは、符号化部７２内の伸張対象のデータの先頭ビットが「０」である場合には、生データであり、先頭ビットが「１」である場合には、ポインタであると判定できる。そして、伸張部５６ｂは、符号化部７２内の伸張対象のデータが生データである場合には、生データを伸張バッファに格納する。また、伸張部５６ｂは、符号化部７２内の伸張対象のデータがポインタである場合には、ポインタが示す文字列を設定部７３および参照部７１内の文字列から取得し、伸張バッファに格納する。

【０１８１】

このように、本実施例に係る利用者端末５２では、入力されたパスワードが、サーバ５１で入力された正規のパスワードと一致しない場合には、双方のパスワードから得られる剰余Ｄが一致しない限り、伸張されるデータが正規のものとならない。したがって、本実施例に係る利用者端末５２によれば、簡易に難読化を図ることができる。

【０１８２】

制御部５６は、ＡＳＩＣ（Application Specific Integrated Circuit）やＦＰＧＡ（Field Programmable Gate Array）などの集積回路を有する。なお、制御部５６は、ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）などの電子回路を有してもよい。

【０１８３】

［処理の流れ］

次に、本実施例に係るサーバ５１の処理の流れを説明する。図２８は、実施例５に係る圧縮処理の手順を示すフローチャートである。この圧縮処理の実行タイミングとしては様々なタイミングが考えられる。例えば、圧縮処理は、入力部５からデジタルコンテンツが入力された場合に実行されるようにしてもよい。なお、本実施例に係るシステム５０の処理の流れは、実施例１に係るシステム１のシーケンス図で示す処理の流れと同様であるので、説明を省略する。

【０１８４】

図２８に示すように、圧縮部５４ｂは、デジタルコンテンツのファイルを取得する（ステップＳ１００１）。生成部５４ａは、入力部５からパスワードが入力されたか否かを判定する（ステップＳ１００２）。パスワードが入力されていない場合（ステップＳ１００２否定）には、生成部５４ａは、再びステップＳ１００２で、入力部５からパスワードが入力されたか否かを判定する。

【０１８５】

一方、パスワードが入力された場合（ステップＳ１００２肯定）には、生成部５４ａは、算出した和を、登録されたタグの数Ｎで除算した場合の剰余Ｄを算出し、次のような処理を行う。すなわち、生成部５４ａは、剰余Ｄの値が示す番号のレコードを起点として、予約語テーブル５３ａの各レコードに登録されたタグを取得し、取得したタグを連結した文字列を生成する（ステップＳ１００３）。これにより、予約語テーブル５３ａの登録の順番が変更された予約語を並べた文字列が生成される。圧縮部５４ｂは、生成部５４ａにより生成された文字列を、設定部７３に設定する（ステップＳ１００４）。圧縮部５４ｂは、デジタルコンテンツのファイルのデータを圧縮しつつ、スライド窓７０をスライドさせて参照部７１内のデータを更新することで辞書を更新し（ステップＳ１００５）、処理結果を制御部５４の内部メモリに格納し、リターンする。

【０１８６】

次に、本実施例に係る利用者端末５２の処理の流れを説明する。図２９は、実施例５に係る伸張処理の手順を示すフローチャートである。伸張処理においても、図２８において説明した圧縮処理と共通の辞書更新アルゴリズムを用いる。図２９に示すように、伸張部５６ｂは、デジタルコンテンツの圧縮ファイルを取得する（ステップＳ１１０１）。生成部５６ａは、入力部１０からパスワードが入力されたか否かを判定する（ステップＳ１１０２）。パスワードが入力されていない場合（ステップＳ１１０２否定）には、生成部５６ａは、再びステップＳ１１０２で、入力部１０からパスワードが入力されたか否かを判定する。

【０１８７】

一方、パスワードが入力された場合（ステップＳ１１０２肯定）には、生成部５６ａは、算出した和を、登録されたタグの数Ｎで除算した場合の剰余Ｄを算出し、次のような処理を行う。すなわち、生成部５６ａは、剰余Ｄの値が示す番号のレコードを起点として、予約語テーブル５５ａの各レコードに登録されたタグを取得し、取得したタグを連結した文字列を生成する（ステップＳ１１０３）。これにより、予約語テーブル５５ａの登録の順番が変更された予約語を並べた文字列が生成される。伸張部５６ｂは、生成部５６ａにより生成された文字列を、設定部７３に設定する（ステップＳ１１０４）。伸張部５６ｂは、デジタルコンテンツの圧縮ファイルのデータを伸張しつつ、スライド窓７０をスライドさせて参照部７１内のデータを更新することで辞書を更新し（ステップＳ１１０５）、処理結果を制御部５６の内部メモリに格納し、リターンする。

【０１８８】

上述してきたように、本実施例に係るサーバ５１によれば、出現頻度の高い文字やタグなどが初期化時に設定部７３に設定されるので、圧縮効率が良くなる。また、本実施例に係るサーバ５１では、ポインタが示す最長一致系列の位置は、設定部７３に設定された文字列の先頭からのアドレスである。そのため、本実施例に係るサーバ５１によれば、圧縮されたデータの解読を試みる攻撃者などが、ポインタが示す最長一致系列の位置を参照部７１の先頭からのアドレスと把握している場合には、攻撃者による圧縮データの解読の困難性を高めることができる。

【０１８９】

また、本実施例に係るサーバ５１では、設定部７３に文字列を設定し、ポインタが示す最長一致系列の位置を設定部７３に設定された文字列の先頭からのアドレスとするという、ＲＳＡなどの暗号化処理と比較すると、簡易な処理で圧縮符号がスクランブルされる。このように、本実施例に係るサーバ５１は、複雑な暗号化の処理を行わずに、解読が困難な圧縮データを生成する。したがって、本実施例に係るサーバ５１によれば、簡易に圧縮データの難読化を図ることができる。また、処理対象データのサイズ増大に応じた処理コストの増大を抑制することができる。

【０１９０】

また、本実施例に係るサーバ５１では、ポインタが示す最長一致系列の位置を設定部７３に設定された文字列の先頭からのアドレスとするだけで、データを圧縮するたびに圧縮されたデータおよび生データにスクランブル処理を行っていない。そのため、本実施例に係るサーバ５１によれば、簡易に圧縮データの難読化を図ることができる。

【０１９１】

また、本実施例に係る利用者端末５２では、入力されたパスワードが、サーバ５１で入力された正規のパスワードと一致しない場合には、双方のパスワードから得られる剰余Ｄが一致しない限り、伸張されるデータが正規のものとならない。したがって、本実施例に係る利用者端末５２によれば、簡易に難読化を図ることができる。

【実施例６】

【０１９２】

さて、上記の実施例５では、ＬＺ７７の圧縮方式を採用する場合を例示したが、開示の装置はこれに限定されない。そこで、実施例６では、データを圧縮する圧縮方式として、ハフマン符号を採用する場合について説明する。

【０１９３】
［システム６０の構成例］
実施例６に係るシステムについて説明する。図３０は、実施例６に係るシステムの構成の一例を示す図である。本実施例に係るシステム６０は、サーバ６１と、利用者端末６２とを有する。サーバ６１は、実施例１に係る記憶部８、制御部９に代えて記憶部６３、制御部６４を有する点が、実施例１と異なる。利用者端末６２は、実施例１に係る記憶部１３、制御部１４に代えて記憶部６５、制御部６６を有する点が、実施例１と異なる。なお、以下では、上記の実施例１～５と同様の機能を果たす各部や各機器については図１、図１０、図１５、図２０、図２４と同様の符号を付し、その説明は省略する場合がある。サーバ６１は、辞書や電子書籍などのデジタルコンテンツのファイルのデータを圧縮する。サーバ６１は、圧縮されたデジタルコンテンツのファイルのデータに、暗号化された後述の頻度データ６３ａを付加して、インターネット４を介して利用者端末６２に送信する。利用者端末６２は、受信した頻度データ６３ａを復号化し、受信したデジタルコンテンツのファイルのデータを伸張する。利用者端末６２は、伸張したデジタルコンテンツのファイルを再生する。
【０１９４】
サーバ６１は、入力部５と、出力部６と、送受信部７と、記憶部６３と、制御部６４とを有する。
【０１９５】
記憶部６３は、各種情報を記憶する。例えば、記憶部６３は、コンテンツＤＢ８ａ、頻度データ６３ａ、辞書６３ｂを記憶する。
【０１９６】
頻度データ６３ａは、全文字に対する各文字の出現頻度が登録されたデータである。頻度データ６３ａは、後述の生成部６４ａにより生成され、記憶部６３に格納される。
【０１９７】
辞書６３ｂは、ハフマン木で表される辞書である。辞書６３ｂには、文字のコードと圧縮符号との組合せが後述の圧縮部６４ｂにより登録される。図３１Ａは、ハフマン木で表される辞書の一例を示す図である。図３１Ａの例は、文字「ｅ」のコードと、圧縮符号「００」との組合せが辞書に登録された場合を示す。また、図３１Ａの例は、文字「ｄ」のコードと、圧縮符号「０１」との組合せが辞書に登録された場合を示す。また、図３１Ａの例は、文字「ｃ」のコードと、圧縮符号「１００」との組合せが辞書に登録された場合を示す。また、図３１Ａの例は、文字「ｂ」のコードと、圧縮符号「１１０」との組合せが辞書に登録された場合を示す。また、図３１Ａの例は、文字「ａ」のコードと、圧縮符号「１１１」との組合せが辞書に登録された場合を示す。
【０１９８】
記憶部６３は、例えば、フラッシュメモリなどの半導体メモリ素子、または、ハードディスク、光ディスクなどの記憶装置である。なお、記憶部６３は、上記の種類の記憶装置に限定されるものではなく、ＲＡＭ（Random Access Memory)、ＲＯＭ（Read Only Memory)であってもよい。
【０１９９】
制御部６４は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、これらによって種々の処理を実行する。図３０に示すように、制御部６４は、生成部６４ａと、圧縮部６４ｂと、変更部６４ｃとを有する。
【０２００】
生成部６４ａは、入力部５から入力されたデジタルコンテンツのファイル中に含まれる各文字の個数を計数する。そして、生成部６４ａは、全文字の個数に対する各文字の個数を算出する。続いて、生成部６４ａは、算出した全文字の個数に対する各文字の個数を示す頻度データ６３ａをＲＳＡなどの暗号化アルゴリズムを用いて暗号化し、暗号化した頻度データ６３を記憶部６３に格納する。
【０２０１】

圧縮部６４ｂは、頻度データ６３ａを用いて、ハフマン木で表される辞書６３ｂを生成し、生成した辞書６３ｂを記憶部６３に格納する。そして、圧縮部６４ｂは、後述の変更部６４ｃにより文字列と圧縮符号との組合せが変更された辞書６３ｂを用いて、ハフマン符号により、デジタルコンテンツのファイルを圧縮する。そして、圧縮部６４ｂは、圧縮したデジタルコンテンツのファイルをデジタルコンテンツごとにコンテンツＤＢ８ａに登録する。また、圧縮部６４ｂは、デジタルコンテンツのファイルの送信要求を受信すると、デジタルコンテンツのファイルをコンテンツＤＢ８ａから取得し、記憶部６３から頻度データ６３ａを取得し、取得したファイルに頻度データ６３ａを付加して送受信部７に送信する。

【０２０２】

変更部６４ｃは、辞書６３ｂに登録された複数の圧縮符号について、同一の圧縮符号長の圧縮符号どうしをグループ化する。図３１Ａの例では、変更部６４ｃは、圧縮符号長が同一の文字「ｅ」と「ｄ」を同じグループとする。また、図３１Ａの例では、変更部６４ｃは、圧縮符号長が同一の文字「ｃ」と「ｂ」と「ａ」とを同じグループとする。そして、変更部６４ｃは、入力部５から入力されたパスワードを用いて、実施例１に係る変更部９ｂが実行する所定の範囲内での圧縮符号の変更方法と同様の方法で、剰余Ｓを算出するなどして、同一のグループ内で圧縮符号を変更する。そして、変更部６４ｃは、全グループで、圧縮符号を変更する。図３１Ｂは、図３１Ａの例が示す辞書が変更された場合の一例を示す図である。図３１Ｂの例では、文字「ｅ」の圧縮符号が「００」から「０１」に変更された場合が示されている。また、図３１Ｂの例では、文字「ｄ」の圧縮符号が「０１」から「００」に変更された場合が示されている。また、図３１Ｂの例では、文字「ｃ」の圧縮符号が「１００」から「１１１」に変更された場合が示されている。また、図３１Ｂの例では、文字「ｂ」の圧縮符号が「１１０」から「１００」に変更された場合が示されている。また、図３１Ｂの例では、文字「ａ」の圧縮符号が「１１１」から「１１０」に変更された場合が示されている。このようにして、変更部６４ｃは、辞書６３ｂに登録された文字のコードと、圧縮符号との組合せを変更する。

【０２０３】

上述してきたように、本実施例に係るサーバ６１では、辞書６３ｂの圧縮符号がスクランブルされて、コードと圧縮符号との組合せが変更される。これにより、圧縮されたデータの解読を試みる攻撃者などは、不正行為などによって変更される前のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、複数の種類の文字の解読が困難となる。

【０２０４】

また、本実施例に係るサーバ６１では、辞書６３ｂの圧縮符号をスクランブルするだけで、複雑な暗号化の処理を行わずに、解読が困難な圧縮データが生成される。したがって、本実施例に係るサーバ６１によれば、簡易な圧縮処理により難読化を図ることができる。また、処理対象データのサイズ増大に応じた処理コストの増大を抑制することができる。

【０２０５】

また、本実施例に係るサーバ６１によれば、辞書６３ｂの圧縮符号をスクランブルするだけで、データを圧縮するたびに圧縮されたデータおよび生データにスクランブル処理を行っていないので、簡易に圧縮データの難読化を図ることができる。

【０２０６】

利用者端末６２は、入力部１０と、出力部１１と、送受信部１２と、記憶部６５と、制御部６６とを有する。

【０２０７】

記憶部６５は、各種情報を記憶する。例えば、記憶部６５は、コンテンツＤＢ８ａ、頻度データ６５ａ、辞書６５ｂを記憶する。

【０２０８】

頻度データ６５ａは、後述の生成部６６ａにより、サーバ６１から送信された頻度デー

タ６３ａが復号化されたデータである。頻度データ６５ａは、生成部６６ａにより、記憶部６５に格納される。

【０２０９】

辞書６５ｂは、上述した辞書６３ｂと同様に、ハフマン木で表される辞書である。辞書６５ｂには、文字のコードと圧縮符号との組合せが後述の圧縮部６６ｂにより登録される。

【０２１０】

記憶部６５は、例えば、フラッシュメモリなどの半導体メモリ素子、または、ハードディスク、光ディスクなどの記憶装置である。なお、記憶部６５は、上記の種類の記憶装置に限定されるものではなく、ＲＡＭ（Random Access Memory)、ＲＯＭ（Read Only Memory)であってもよい。

【０２１１】

制御部６６は、各種の処理手順を規定したプログラムや制御データを格納するための内部メモリを有し、これらによって種々の処理を実行する。図３０に示すように、制御部６６は、生成部６６ａと、伸張部６６ｂと、変更部６６ｃと、再生部１４ｃとを有する。

【０２１２】

生成部６６ａは、サーバ６１から送信されたデジタルコンテンツのファイルに付加された頻度データ６３ａを取得する。生成部６６ａは、サーバ２での暗号化に用いられた暗号化アルゴリズムを用いて、取得した頻度データ６３ａを復号化する。そして、生成部６６ａは、復号化した頻度データ６５ａを記憶部６５に格納する。

【０２１３】

伸張部６６ｂは、頻度データ６５ａを用いて、ハフマン木で表される辞書６５ｂを生成し、生成した辞書６５ｂを記憶部６５に格納する。そして、伸張部６６ｂは、後述の変更部６６ｃにより文字列と伸張符号との組合せが変更された辞書６５ｂを用いて、ハフマン符号により、デジタルコンテンツのファイルを伸張する。そして、伸張部６６ｂは、伸張したデジタルコンテンツのファイルをデジタルコンテンツごとにコンテンツＤＢ８ａに登録する。

【０２１４】

変更部６６ｃは、辞書６５ｂに登録された複数の圧縮符号について、同一の圧縮符号長の圧縮符号どうしをグループ化する。そして、変更部６６ｃは、入力部１０から入力されたパスワードを用いて、実施例１に係る変更部９ｂが実行する所定の範囲内での圧縮符号の変更方法と同様の方法で、剰余Ｓを算出するなどして、同一のグループ内で圧縮符号を変更する。そして、変更部６６ｃは、全グループで、圧縮符号を変更することで、辞書６５ｂに登録された文字のコードと、圧縮符号との組合せを変更する。

【０２１５】

このように、本実施例に係る利用者端末６２では、入力されたパスワードが、サーバ６１で入力された正規のパスワードと一致しない場合には、双方のパスワードから得られる剰余Ｓなどが一致しない限り、伸張されるデータが正規のものとならない。したがって、本実施例に係る利用者端末６２によれば、簡易に難読化を図ることができる。

【０２１６】

制御部６６は、ＡＳＩＣ（Application Specific Integrated Circuit）やＦＰＧＡ（Field Programmable Gate Array）などの集積回路を有する。なお、制御部６６は、ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）などの電子回路を有してもよい。

【０２１７】

［処理の流れ］

次に、本実施例に係るサーバ６１の処理の流れを説明する。図３２は、実施例６に係る圧縮処理の手順を示すフローチャートである。この圧縮処理の実行タイミングとしては様々なタイミングが考えられる。例えば、圧縮処理は、入力部５からデジタルコンテンツが入力された場合に実行されるようにしてもよい。なお、本実施例に係るシステム６０の処

理の流れは、実施例１に係るシステム１のシーケンス図で示す処理の流れと同様であるので、説明を省略する。

【０２１８】

図３２に示すように、圧縮部６４ｂは、頻度データ６３ａを用いて、ハフマン木で表される辞書６３ｂを生成し、生成した辞書６３ｂを記憶部６３に格納する（ステップＳ１２０１）。圧縮部６４ｂは、デジタルコンテンツのファイルを取得する（ステップＳ１２０２）。変更部６４ｃは、入力部５からパスワードが入力されたか否かを判定する（ステップＳ１２０３）。パスワードが入力されていない場合（ステップＳ１２０３否定）には、変更部６４ｃは、再びステップＳ１２０３で、入力部５からパスワードが入力されたか否かを判定する。

【０２１９】

一方、パスワードが入力された場合（ステップＳ１２０３肯定）には、変更部６４ｃは、辞書６３ｂに登録された複数の圧縮符号について、同一の圧縮符号長の圧縮符号どうしをグループ化し、全グループのそれぞれで、圧縮符号を変更する（ステップＳ１２０４）。圧縮部６４ｂは、辞書６３ｂを用いて、デジタルコンテンツのファイルのデータを圧縮し（ステップＳ１２０５）、処理結果を制御部６４の内部メモリに格納し、リターンする。

【０２２０】

次に、本実施例に係る利用者端末６２の処理の流れを説明する。図３３は、実施例６に係る伸張処理の手順を示すフローチャートである。図３３に示すように、伸張部６６ｂは、頻度データ６５ａを用いて、ハフマン木で表される辞書６５ｂを生成し、生成した辞書６５ｂを記憶部６５に格納する（ステップＳ１３０１）。伸張部６６ｂは、デジタルコンテンツのファイルを取得する（ステップＳ１３０２）。変更部６６ｃは、入力部１０からパスワードが入力されたか否かを判定する（ステップＳ１３０３）。パスワードが入力されていない場合（ステップＳ１３０３否定）には、変更部６６ｃは、再びステップＳ１３０３で、入力部１０からパスワードが入力されたか否かを判定する。

【０２２１】

一方、パスワードが入力された場合（ステップＳ１３０３肯定）には、変更部６６ｃは、辞書６５ｂに登録された複数の圧縮符号について、同一の圧縮符号長の圧縮符号どうしをグループ化し、全グループのそれぞれで、圧縮符号を変更する（ステップＳ１３０４）。伸張部６６ｂは、辞書６５ｂを用いて、デジタルコンテンツのファイルのデータを伸張し（ステップＳ１３０５）、処理結果を制御部６６の内部メモリに格納し、リターンする。

【０２２２】

上述してきたように、本実施例に係るサーバ６１では、辞書６３ｂの圧縮符号がスクランブルされて、コードと圧縮符号との組合せが変更される。これにより、圧縮されたデータの解読を試みる攻撃者などは、不正行為などによって変更される前のコードと圧縮符号との組合せを把握していたとしても、かかる組合せが変更されるため、複数の種類の文字の解読が困難となる。

【０２２３】

また、本実施例に係るサーバ６１では、辞書６３ｂの圧縮符号をスクランブルするだけで、複雑な暗号化の処理を行わずに、解読が困難な圧縮データが生成される。したがって、本実施例に係るサーバ６１によれば、簡易な圧縮処理により難読化を図ることができる。また、処理対象データのサイズ増大に応じた処理コストの増大を抑制することができる。

【０２２４】

また、本実施例に係るサーバ６１によれば、辞書６３ｂの圧縮符号をスクランブルするだけで、データを圧縮するたびに圧縮されたデータおよび生データにスクランブル処理を行っていないので、簡易に圧縮データの難読化を図ることができる。

【０２２５】

また、本実施例に係る利用者端末６２では、入力されたパスワードが、サーバ６１で入力された正規のパスワードと一致しない場合には、双方のパスワードから得られる剰余Ｓなどが一致しない限り、伸張されるデータが正規のものとならない。したがって、本実施例に係る利用者端末６２によれば、簡易に難読化を図ることができる。

【０２２６】

さて、これまで開示の装置に関する実施例について説明した。上述したように、各実施例におけるサーバと利用者端末とでは、共通の辞書更新アルゴリズムが用いられる。また、本発明は上述した実施例以外にも、種々の異なる形態にて実施されてよいものである。そこで、以下では、本発明に含まれる他の実施例を説明する。

【０２２７】

たとえば、実施例１～６において説明した処理のうち、自動的に行われるものとして説明した処理の全部または一部を手動的に行うこともできる。また、実施例１～６において説明した処理のうち、手動的に行われるものとして説明した処理の全部または一部を公知の方法で自動的に行うこともできる。

【０２２８】

また、各種の負荷や使用状況などに応じて、各実施例において説明した各処理の各ステップでの処理を任意に細かくわけたり、あるいはまとめたりすることができる。また、ステップを省略することもできる。

【０２２９】

また、各種の負荷や使用状況などに応じて、各実施例において説明した各処理の各ステップでの処理の順番を変更できる。例えば、ステップＳ１２０１での処理を行う前に、ステップＳ１２０２での処理を行うこともできる。また、ステップＳ１３０１での処理を行う前に、ステップＳ１３０２での処理を行うこともできる。

【０２３０】

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的状態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。

【実施例７】

【０２３１】

［圧縮プログラム、伸張プログラム］

また、上記の実施例１～６で説明した利用者端末の処理は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーションなどのコンピュータシステムで実行することによって実現することもできる。そこで、以下では、図３４を用いて、上記の実施例で説明したサーバと同様の機能を有する圧縮プログラムを実行するコンピュータの一例を説明する。また、図３５を用いて、上記の実施例で説明した利用者端末と同様の機能を有する伸張プログラムを実行するコンピュータの一例を説明する。

【０２３２】

図３４は、圧縮プログラムを実行するコンピュータを示す図である。図３４に示すように、コンピュータ３００は、ＣＰＵ（Central Processing Unit）３１０、ＲＯＭ（Read Only Memory）３２０、ＨＤＤ（Hard Disk Drive）３３０、ＲＡＭ（Random Access Memory）３４０を有する。また、コンピュータ３００は、入力装置３５０、出力装置３６０、インターネット４に接続された通信インタフェース３７０を有する。これら３１０～３７０の各部は、バス３８０を介して接続される。

【０２３３】

入力装置３５０は、各種の入力デバイスを含み、例えば、キーボードやマウスを含む。入力装置３５０は、各実施例のサーバが有する入力部５に対応する。

【０２３４】

出力装置３６０は、各種の出力デバイスを含み、例えば、液晶ディスプレイを含む。出力装置３６０は、各実施例のサーバが有する出力部６に対応する。

【０２３５】
通信インタフェース３７０は、各実施例のサーバが有する送受信部７に対応する。
【０２３６】
ＲＯＭ３２０には、上記の実施例で示す圧縮部、変更部、生成部と同様の機能を発揮する圧縮プログラム３２０ａが予め記憶される。なお、圧縮プログラム３２０ａについては、適宜分離しても良い。
【０２３７】
そして、ＣＰＵ３１０が、圧縮プログラム３２０ａをＲＯＭ３２０から読み出して実行する。
【０２３８】
そして、ＨＤＤ３３０には、コンテンツＤＢ、辞書、予約語テーブル、頻度データが設けられる。これらのうち、コンテンツＤＢ、辞書、予約語テーブルのそれぞれは、コンテンツＤＢ８ａ、辞書８ｂ，６３ｂ、予約語テーブル５３ａのそれぞれに対応する。また、頻度データは、頻度データ６３ａに対応する。
【０２３９】
そして、ＣＰＵ３１０は、コンテンツＤＢ、辞書、予約語テーブル、頻度データを読み出してＲＡＭ３４０に格納する。さらに、ＣＰＵ３１０は、ＲＡＭ３４０に格納されたコンテンツＤＢ、辞書、予約語テーブル、頻度データを用いて、圧縮プログラムを実行する。なお、ＲＡＭ３４０に格納される各データは、常に全てのデータがＲＡＭ３４０に格納される必要はなく、処理に必要なデータのみがＲＡＭ３４０に格納されれば良い。
【０２４０】
図３５は、伸張プログラムを実行するコンピュータを示す図である。図３５に示すように、コンピュータ４００は、ＣＰＵ４１０、ＲＯＭ４２０、ＨＤＤ４３０、ＲＡＭ４４０を有する。また、コンピュータ４００は、入力装置４５０、出力装置４６０、インターネット４に接続された通信インタフェース４７０を有する。これら４１０～４７０の各部は、バス３８０を介して接続される。
【０２４１】
入力装置４５０は、各種の入力デバイスを含み、例えば、キーボードやマウスを含む。入力装置４５０は、各実施例の利用者端末が有する入力部１０に対応する。
【０２４２】
出力装置４６０は、各種の出力デバイスを含み、例えば、液晶ディスプレイを含む。出力装置４６０は、各実施例の利用者端末が有する出力部１１に対応する。
【０２４３】
通信インタフェース４７０は、各実施例のサーバが有する送受信部１２に対応する。
【０２４４】
ＲＯＭ４２０には、上記の実施例で示す生成部、伸張部、変更部と同様の機能を発揮する伸張プログラム４２０ａが予め記憶される。なお、伸張プログラム４２０ａについては、適宜分離しても良い。
【０２４５】
そして、ＣＰＵ４１０が、伸張プログラム４２０ａをＲＯＭ４２０から読み出して実行する。
【０２４６】
そして、ＨＤＤ４３０には、コンテンツＤＢ、辞書、予約語テーブル、頻度データが設けられる。これらのうち、コンテンツＤＢ、辞書、予約語テーブルのそれぞれは、コンテンツＤＢ１３ａ、辞書１３ｂ，６５ｂ、予約語テーブル５５ａのそれぞれに対応する。また、頻度データは、頻度データ６５ａに対応する。
【０２４７】
そして、ＣＰＵ４１０は、コンテンツＤＢ、辞書、予約語テーブル、頻度データを読み出してＲＡＭ４４０に格納する。さらに、ＣＰＵ４１０は、ＲＡＭ４４０に格納されたコンテンツＤＢ、辞書、予約語テーブル、頻度データを用いて、伸張プログラムを実行する

。なお、ＲＡＭ４４０に格納される各データは、常に全てのデータがＲＡＭ４４０に格納される必要はなく、処理に必要なデータのみがＲＡＭ４４０に格納されれば良い。

【０２４８】

なお、上記した圧縮プログラム、伸張プログラムについては、必ずしも最初からＲＯＭに記憶させておく必要はない。

【０２４９】

例えば、コンピュータに挿入されるフレキシブルディスク（ＦＤ）、ＣＤ－ＲＯＭ、ＤＶＤディスク、光磁気ディスク、ＩＣカードなどの「可搬用の物理媒体」にプログラムを記憶させておく。そして、コンピュータがこれらからプログラムを読み出して実行するようにしてもよい。

【０２５０】

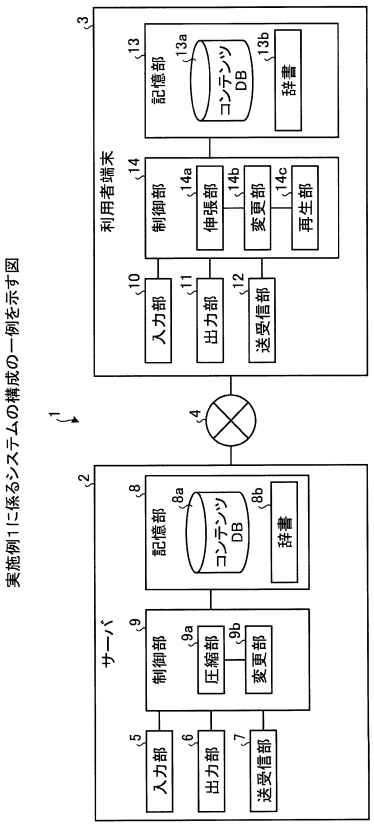
さらには、公衆回線、インターネット、ＬＡＮ、ＷＡＮなどを介してコンピュータに接続される「他のコンピュータ（またはサーバ）」などにプログラムを記憶させておく。そして、コンピュータがこれらからプログラムを読み出して実行するようにしてもよい。

【符号の説明】

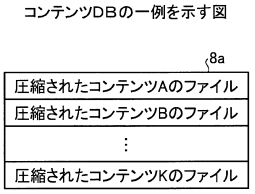
【０２５１】

１	システム
２	サーバ
３	利用者端末
５	入力部
８	記憶部
８ａ	コンテンツＤＢ
８ｂ	辞書
９	制御部
９ａ	圧縮部
９ｂ	変更部
１０	入力部
１３	記憶部
１３ａ	コンテンツＤＢ
１３ｂ	辞書
１４	制御部
１４ａ	伸張部
１４ｂ	変更部

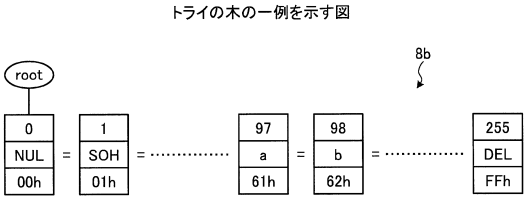
【図１】



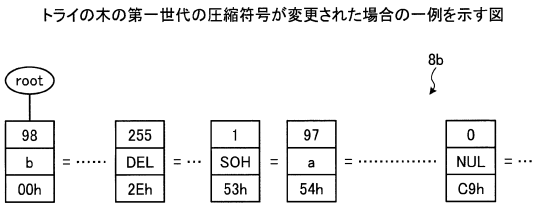
【図２】



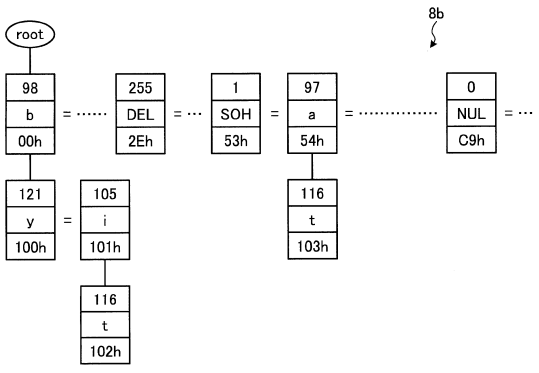
【図３】



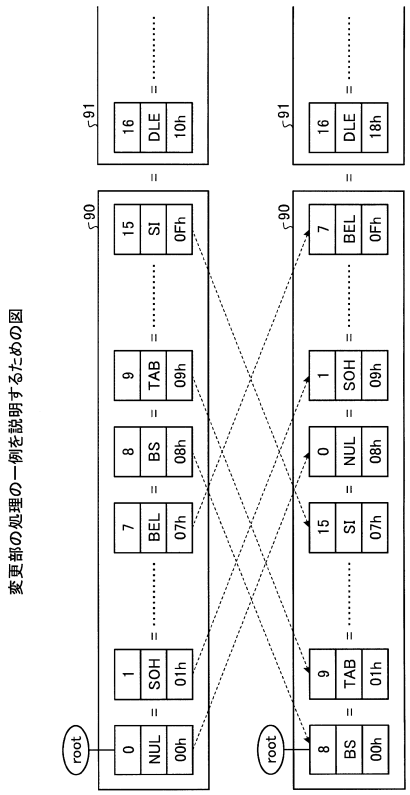
【図４】



【図５】

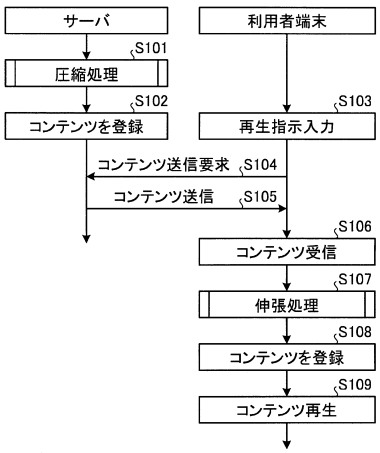


【図６】



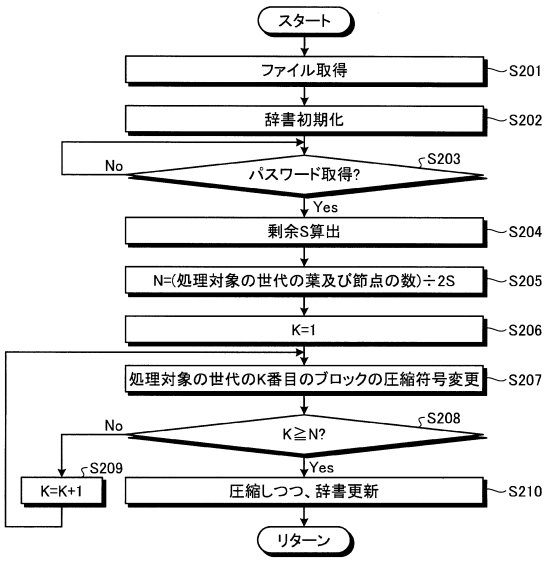
【図７】

実施例1に係るシステムのシーケンス図



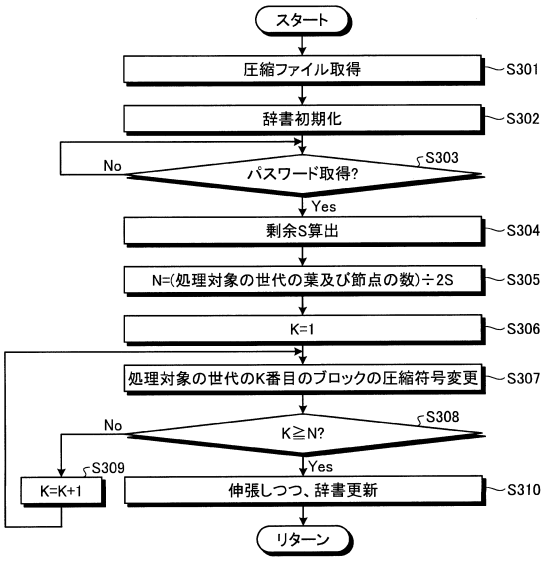
【図８】

実施例1に係る圧縮処理の手順を示すフローチャート



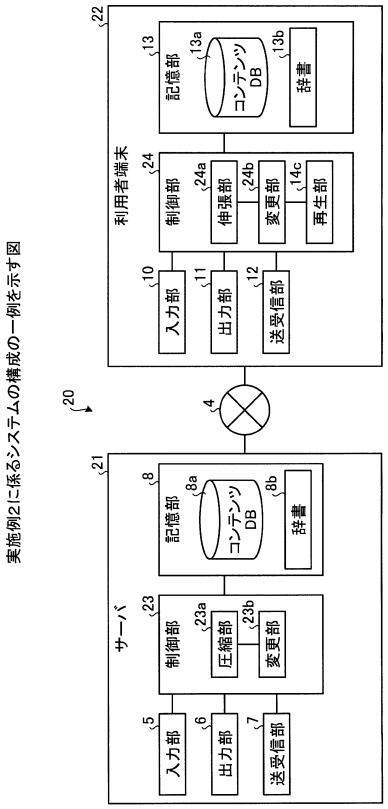
【図９】

実施例1に係る伸張処理の手順を示すフローチャート



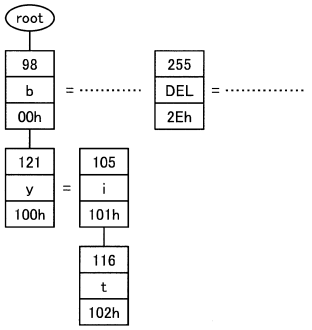
【図１０】

実施例2に係るシステムの構成の一例を示す図



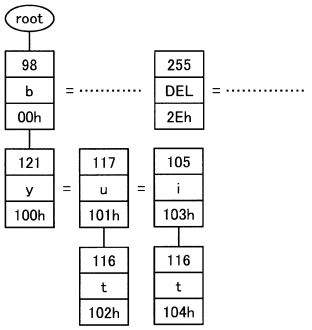
【図１１】

実施例2に係るシステムが実行する処理の一例を説明するための図



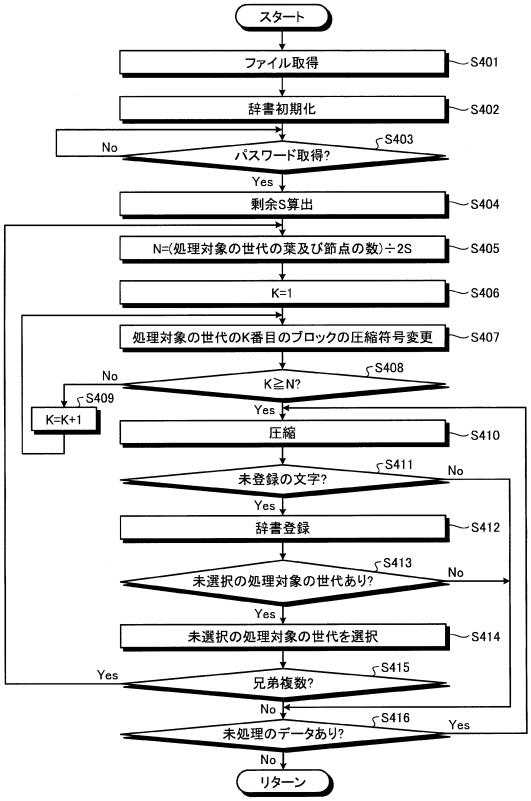
【図１２】

実施例2に係るシステムが実行する処理の一例を説明するための図



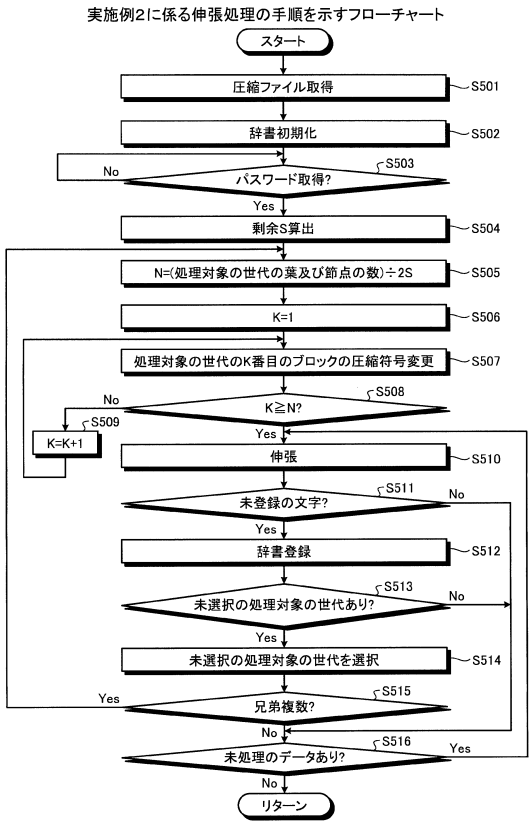
【図１３】

実施例2に係る圧縮処理の手順を示すフローチャート



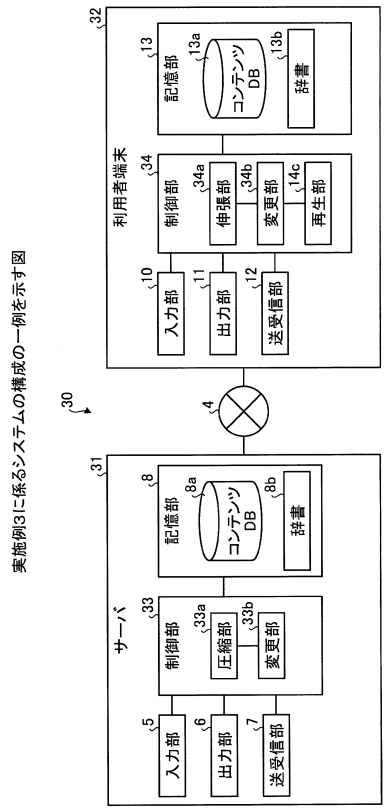
【図１４】

実施例2に係る伸張処理の手順を示すフローチャート



【図１５】

実施例3に係るシステムの構成の一例を示す図



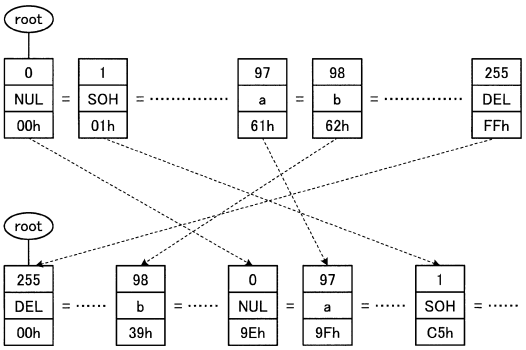
【図１６】

記憶部に記憶された情報の一例を示す図

変更前の圧縮符号	00h	01h	…	98h	…	FFh
変更後の圧縮符号	03h	07h	…	00h	…	16h

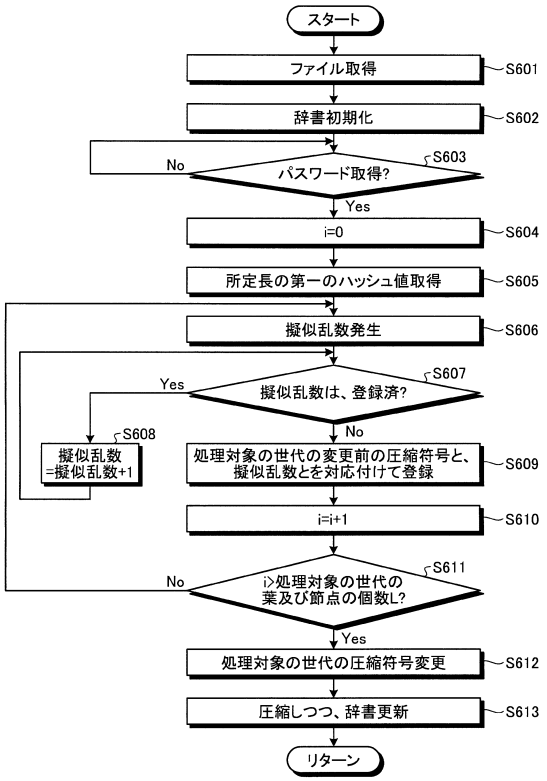
【図１７】

実施例3における圧縮符号の変更の一例を説明するための図



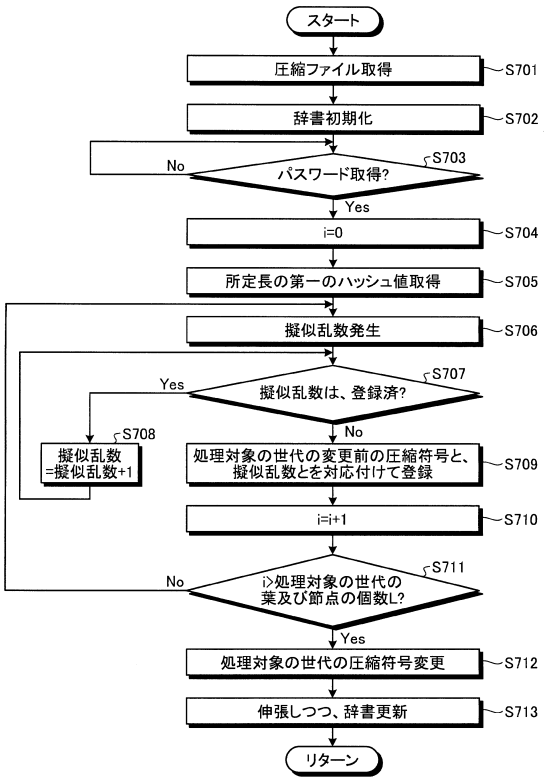
【図１８】

実施例3に係る圧縮処理の手順を示すフローチャート



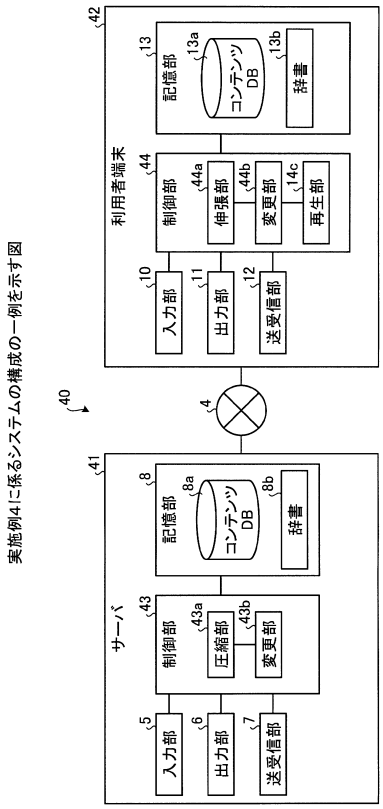
【図１９】

実施例3に係る伸張処理の手順を示すフローチャート

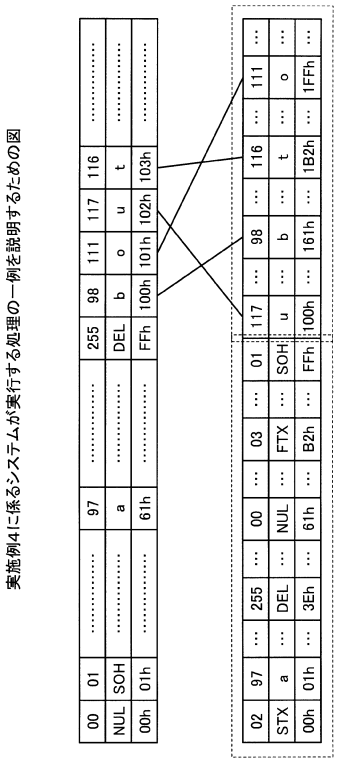


【図２０】

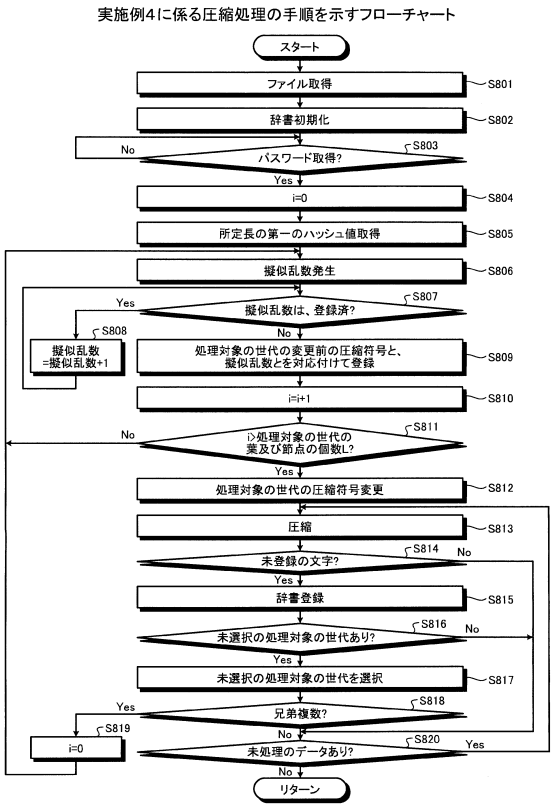
実施例4に係るシステムの構成の一例を示す図



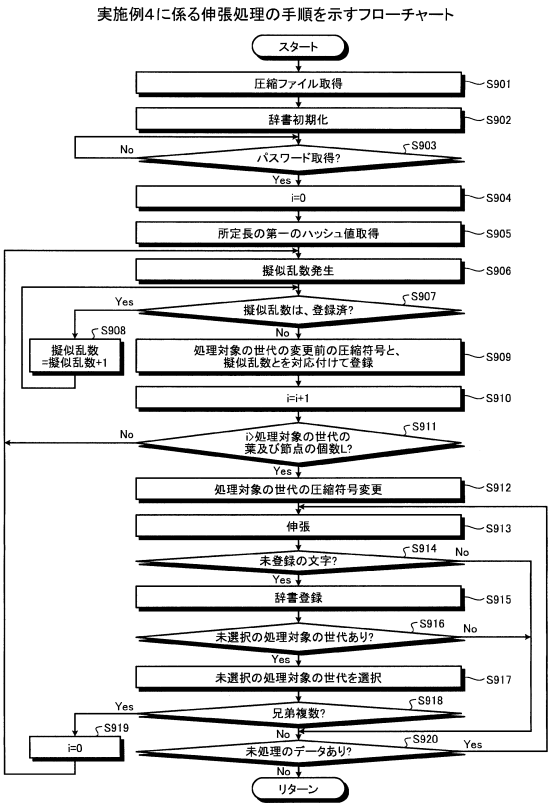
【図２１】



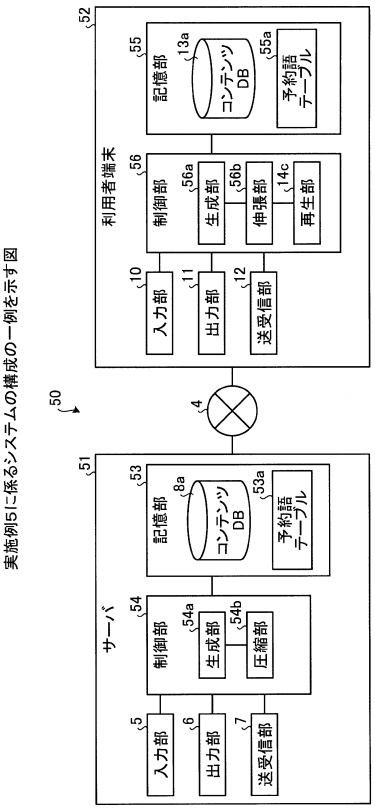
【図２２】



【図２３】



【図２４】



【図２５】

予約語テーブルの一例を示す図

No	
1	
2	</color>
⋮	
N	</title>

【図２６Ａ】

生成部により生成された文字列の一例を示す図

</color>…</title>

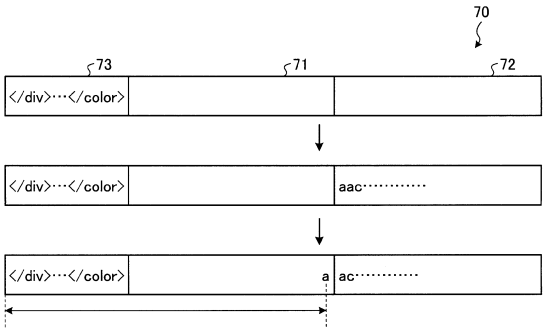
【図２６Ｂ】

生成部により生成された文字列の一例を示す図

</title>…</color>

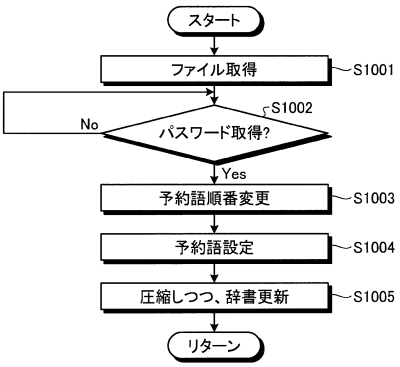
【図２７】

実施例5に係るシステムの処理を説明するための図



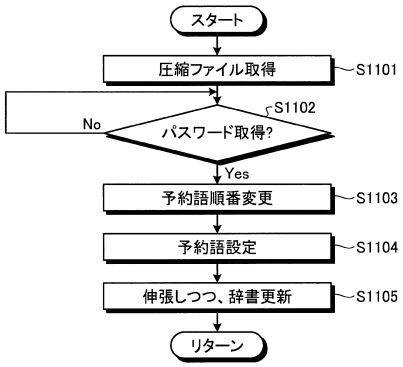
【図２８】

実施例5に係る圧縮処理の手順を示すフローチャート

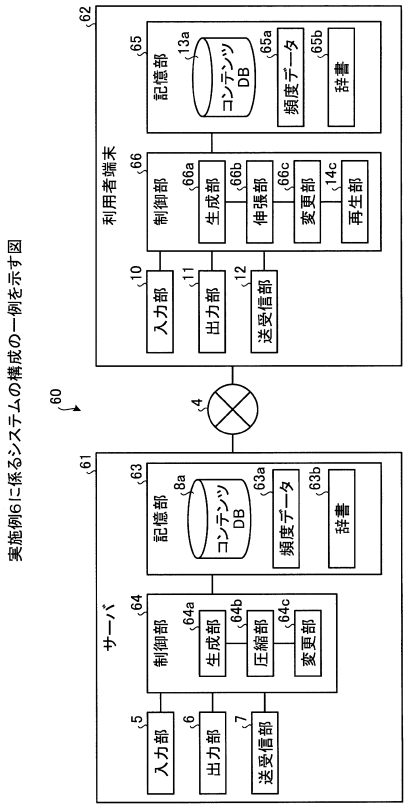


【図２９】

実施例5に係る伸張処理の手順を示すフローチャート



【図３０】



【図３１Ａ】

ハフマン木で表される辞書の一例を示す図

文字	圧縮符号
e	00
d	01
c	100
b	110
a	111

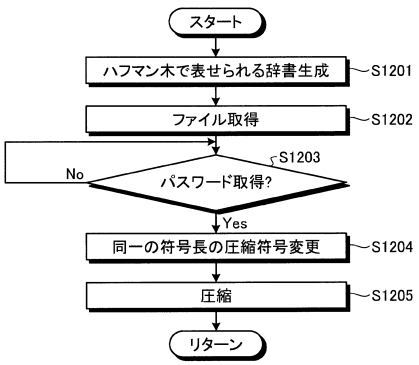
【図３１Ｂ】

図31Ａの例が示す辞書が変更された場合の一例を示す図

文字	圧縮符号
e	01
d	00
c	111
b	100
a	110

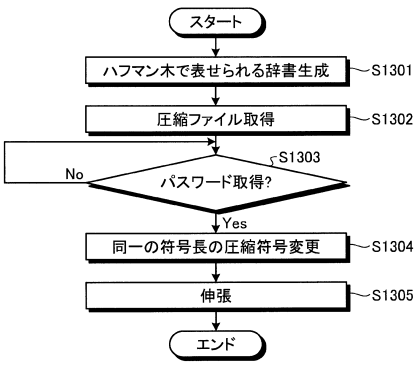
【図３２】

実施例6に係る圧縮処理の手順を示すフローチャート



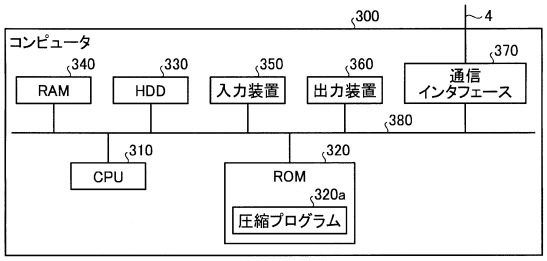
【図３３】

実施例6に係る伸張処理の手順を示すフローチャート



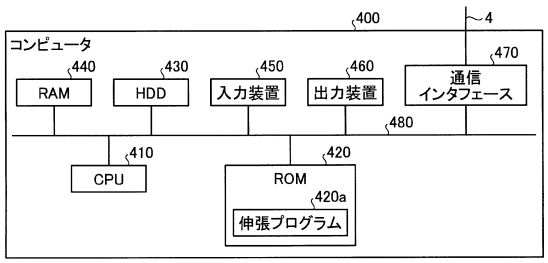
【図３４】

圧縮プログラムを実行するコンピュータを示す図



【図３５】

伸張プログラムを実行するコンピュータを示す図



フロントページの続き

(72)発明者　星　哲郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　青木　重徳

(56)参考文献　特開平０９－００６２３８（ＪＰ，Ａ）
特開２００８－２４２０３４（ＪＰ，Ａ）
特開２０１０－２６３６２３（ＪＰ，Ａ）
米国特許出願公開第２００４／００７６２９９（ＵＳ，Ａ１）
横田　薫、田中　初一，“データ圧縮機能を備えたストリーム暗号システムの提案”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，１９９５年１２月１５日，Ｖｏｌ．９５、Ｎｏ．４２３，ｐ．３９－４４

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｈ０３Ｍ　　７／４２