(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-208992
(P2006-208992A)
(43)公開日　平成18年8月10日(2006.8.10)

(51)Int.Cl.			F I			テーマコード（参考）
G09C	1/00	(2006.01)	G09C	1/00	610Z	5C059
H04N	7/26	(2006.01)	H04N	7/13	Z	5C164
H04N	7/167	(2006.01)	H04N	7/167	Z	5J104

審査請求 未請求　請求項の数 5　OL　（全 25 頁）

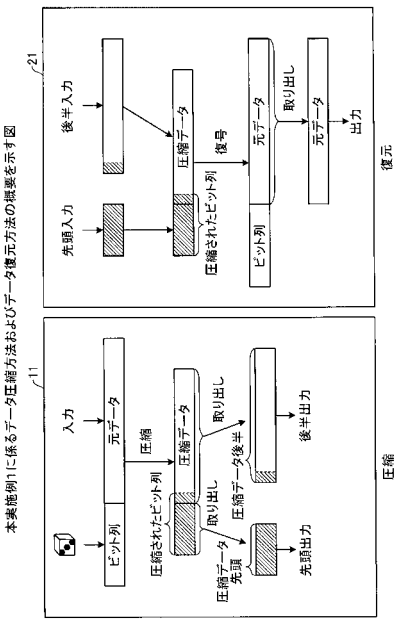
(21)出願番号　特願2005-23825(P2005-23825)
(22)出願日　平成17年1月31日(2005.1.31)

(71)出願人　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　100089118
弁理士　酒井　宏明
(72)発明者　井谷　宣子
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

Fターム(参考)　5C059 RB01 RC35 UA02
5C164 MA02P PA04 PA10
5J104 AA01 AA03 AA16 EA04 EA15
EA16 JA03 NA02 NA08 NA37

(54)【発明の名称】データ圧縮方法、データ復元方法、データ圧縮装置、データ復元装置、データ圧縮プログラムおよびデータ復元プログラム

(57)【要約】
【課題】圧縮データ自体に秘匿性をもたせてデータ量削減とデータ秘匿とを両立させること。
【解決手段】圧縮処理側では、元データに任意のビット列を付加して圧縮処理をおこない、先頭部分と後半部分とに分離して別ルートで復元処理側に渡すこととし、復元処理側では、別ルートで渡された先頭部分と後半部分とから圧縮データを再現して復号処理をおこない元データを復元する。また、圧縮処理側で、後半部分をさらに複数の部分データに分割し、分割された最初の部分データ以外の部分データと先頭部分とを結合して出力する。さらに、圧縮処理側で先頭部分を削除して後半部分のみを復元処理側に渡し、復元処理側では、圧縮処理側と共通の手法を用いることにより削除された先頭部分を再現する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
被圧縮データ列から秘匿性を有する圧縮データ列を生成するデータ圧縮方法であって、
所定長のビット列を前記被圧縮データ列の先頭に付加するビット列付加工程と、
前記ビット列付加工程により前記ビット列が付加された前記被圧縮データ列を圧縮する圧縮工程と、
前記圧縮工程により生成された圧縮データ列の先頭位置から該データ圧縮工程により圧縮された前記ビット列の所定位置までの先頭部分を、該圧縮データ列から分割する分割工程と
を含んだことを特徴とするデータ圧縮方法。
【請求項２】
前記圧縮データ列から前記先頭部分を除いた後半部分を１または複数のブロックとし、少なくとも、該先頭部分と最初のブロックとを別々に出力する出力工程をさらに含んだことを特徴とする請求項１に記載のデータ圧縮方法。
【請求項３】
前記圧縮データ列から前記先頭部分を除いた後半部分を出力する後半部分出力工程をさらに含んだことを特徴とする請求項１に記載のデータ圧縮方法。
【請求項４】
請求項２で出力されたデータから前記被圧縮データ列を復元するデータ復元方法であって、
前記先頭部分および１または複数の前記ブロックから前記圧縮データ列を再現する圧縮データ再現工程と、
前記圧縮データ再現工程により再現された前記圧縮データ列を復号する復号工程と、
前記復号工程により復号されたデータ列から前記ビット列を除去して前記被圧縮データ列を出力する出力工程と
を含んだことを特徴とするデータ復元方法。
【請求項５】
請求項３で出力されたデータを用いて前記被圧縮データ列を復元するデータ復元方法であって、
前記ビット列を前記圧縮工程により圧縮するビット列圧縮工程と、
前記ビット列圧縮工程により圧縮されたビット列から前記先頭部分を分割するビット列分割工程と、
前記後半部分出力工程により出力された前記後半部分を入力する入力工程と、
前記ビット列分割工程により分割された前記先頭部分を、前記入力工程により入力された前記後半部分の先頭に付加することにより前記圧縮データ列を再現する圧縮データ再現工程と、
前記圧縮データ再現工程により再現された前記圧縮データ列を復号する復号工程と、
前記復号工程により復号されたデータ列から前記ビット列を除去して前記被圧縮データ列を出力する出力工程と
を含んだことを特徴とするデータ復元方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、被圧縮データ列から秘匿性を有する圧縮データ列を生成するデータ圧縮方法、データ復元方法、データ圧縮装置、データ復元装置、データ圧縮プログラムおよびデータ復元プログラムに関し、特に、圧縮データ自体に秘匿性をもたせてセキュリティ強度を高めることにより、データ量削減とデータ秘匿とを両立させることができるデータ圧縮方法、データ復元方法、データ圧縮装置、データ復元装置、データ圧縮プログラムおよびデータ復元プログラムに関するものである。
【背景技術】

【０００２】
近年、インターネットや携帯端末の普及にともない、各装置内に格納されるデータや、各装置間で通信されるデータのデータ量削減およびセキュリティ（データ秘匿）に対する関心が高まっている。データ量削減に関する技術としては種々の圧縮技術が広く知られており、かかる圧縮技術を用いることによりデータ量削減のニーズを満たすことができる。
【０００３】
一方、データ秘匿に関する技術としては、データにパスワード機能を付加したり、データを暗号化したりする技術が広く知られており、これらの技術と、かかる圧縮技術とをあわせて用いることにより、データ量削減とデータ秘匿との両立を図ることが可能となる。
【０００４】
データ量削減とデータ秘匿との両立を図ったものとしては、たとえば、圧縮データにパスワード情報を添付するパスワード機能付きデータ圧縮方法がある。このパスワード機能付きデータ圧縮方法では、圧縮済のデータにパスワードを付加することによりパスワード情報を含んだ圧縮データを生成する。そして、復元側であらたに入力されたパスワードと、圧縮側で入力されたパスワードとが一致した場合にのみ圧縮データの復元をおこなうこととしている。
【０００５】
また、特許文献１には、圧縮後の画像データにダミーデータを挿入することにより、画像データの秘匿をおこなうファクシミリ装置についての技術が開示されており、データ量削減とデータ秘匿との両立が図られている。
【０００６】
【特許文献１】特開２００１－１１９５８８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながら、上記したパスワード機能付きデータ圧縮方法では、圧縮データそのものにはデータを秘匿するための加工をおこなっていないので、パスワード情報を含んだ圧縮データからパスワード情報を除去するだけで、圧縮データを復元できてしまうという問題があった。すなわち、かかるデータ圧縮方法においては、圧縮データのセキュリティ強度が低いという問題があった。
【０００８】
また、上記した特許文献１の技術においても、圧縮データ（圧縮後の画像データ）そのものにはデータを秘匿するための加工はなされておらず、挿入されたダミーデータを除去するだけで、圧縮データを復元できてしまうという、同様の問題がある。
【０００９】
これらのことから、圧縮データ自体に秘匿性をもたせることによりデータ量削減とデータ秘匿とを両立させることができる圧縮方法およびその復元方法をいかにして実現するかが大きな課題となっている。
【００１０】
この発明は、上述した従来技術による問題点を解消するためになされたものであり、圧縮データ自体に秘匿性をもたせてセキュリティ強度を高めることにより、データ量削減とデータ秘匿とを両立させることができるデータ圧縮方法、データ復元方法、データ圧縮装置、データ復元装置、データ圧縮プログラムおよびデータ復元プログラムを提供することを目的とする。
【課題を解決するための手段】
【００１１】
上述した課題を解決し、目的を達成するため、本発明は、被圧縮データ列から秘匿性を有する圧縮データ列を生成するデータ圧縮方法であって、所定長のビット列を前記被圧縮データ列の先頭に付加するビット列付加工程と、前記ビット列付加工程により前記ビット列が付加された前記被圧縮データ列を圧縮する圧縮工程と、前記圧縮工程により生成され

た圧縮データ列の先頭位置から該データ圧縮工程により圧縮された前記ビット列の所定位置までの先頭部分を、該圧縮データ列から分割する分割工程とを含んだことを特徴とする。

【発明の効果】

【００１２】

本発明によれば、所定長のビット列を被圧縮データ列の先頭に付加し、ビット列が付加された被圧縮データ列を圧縮し、生成された圧縮データ列の先頭位置から、圧縮されたビット列の所定位置までの先頭部分を、かかる圧縮データ列から分割するよう構成したので、圧縮データ自体に秘匿性をもたせてセキュリティ強度を高めることにより、データ量削減とデータ秘匿とを両立させることができるという効果を奏する。

【発明を実施するための最良の形態】

【００１３】

以下に添付図面を参照して、この発明に係るデータ圧縮方法、データ復元方法、データ圧縮装置、データ復元装置、データ圧縮プログラムおよびデータ復元プログラムの好適な実施例１～３を詳細に説明する。なお、これらの実施例によりこの発明が限定されるものではない。

【実施例１】

【００１４】

まず、本実施例１のデータ圧縮方法およびデータ復元方法の概要について図１を用いて説明する。図１は、本実施例１に係るデータ圧縮方法およびデータ復元方法の概要を示す図である。なお、同図に示す１１が本実施例１に係るデータ圧縮方法であり、同図に示す２１が本実施例１に係るデータ復元方法である。

【００１５】

図１の１１に示したように、このデータ圧縮方法では、圧縮対象となる元データの先頭に乱数発生関数などで発生させたビット列を付加し、かかるビット列が付加された元データを所定の圧縮手法を用いて圧縮する。そして、この圧縮データを先頭部分と後半部分とに分離して異なる出力先に出力する。

【００１６】

本実施例１は、かかる圧縮手法として、スプレイ符号（Ｓｐｌａｙ　ｔｒｅｅ　ｃｏｄｉｎｇ）による圧縮手法を用い、さらに、圧縮データの分離位置を工夫することにより、分離された先頭部分および後半部分にデータ秘匿性をもたせている点に特徴がある。

【００１７】

従来のパスワード機能付きデータ圧縮方法（図１５の５１）およびデータ復元方法（図１５の５２）では、図１５の５１に示すように、元データを圧縮して圧縮データを生成し、生成した圧縮データの先頭部分に、ハッシュ関数によりハッシュ値に変換されたパスワードを付加することとしていた。

【００１８】

また、復元側では、図１５の５２に示すように、復元側であらたに入力されたパスワードを、圧縮側と同様にハッシュ関数によりハッシュ値に変換し、このハッシュ値と、圧縮データとともに渡されたハッシュ値とを照合して、一致する場合にのみ復元処理をおこなうこととしていた。

【００１９】

しかしながら、このパスワード機能付きデータ圧縮方法では、圧縮データそのものにはデータを秘匿するための加工をおこなっていないので、圧縮データに付加されたハッシュ値を除去するだけで圧縮データを復元できてしまうという問題があった。本発明に係るデータ圧縮方法およびデータ復元方法では、圧縮データそのものにデータを秘匿するための加工をおこなうことにより、上記した問題点を解決している。

【００２０】

ここで、上記したスプレイ符号を用いた圧縮手法について図１６を用いて説明しておく。図１６は、スプレイ符号の概要を示す図である。スプレイ符号は、２分木を用いた符合

であり、出現した文字の符号長が半分になるように木を折り曲げていくことにより、文字の符号長が文字の出現頻度に応じて随時変更されていく。

【００２１】

まず、スプレイ符号木（以下、単に符号木と言う）の各部の名称について説明する。図１６の６１は、Ａ～Ｈの８文字からなる場合の符号木について示している。木の頂点にある「○」は「根」と呼ばれ、それ以外の「○」は「節」と呼ばれる。そして、Ａ～Ｈの文字が記された「○」は、「葉」と呼ばれる。

【００２２】

また、「根」、「節」および「葉」を結ぶ直線は「経路」と呼ばれ、各経路に記されている「０」または「１」の数字は「符号」と呼ばれる。たとえば、文字「Ａ」をあらわす符号は「００」であり、文字「Ｆ」をあらわす符号は「１１００」である。

【００２３】

６１に示した状態の符号木において、あらたに文字「Ｆ」を読み込んで圧縮処理をおこなう場合の符号木折り曲げの手順を、図１６の６２および６３を用いて説明する。６２に示したように、あらたに読み込んだ文字「Ｆ」を「葉」から「根」へたどりながら２つずつ「節」の組をつくる。そして、それぞれの組で「Ｆ」から「根」までの経路を１つ減らすように、「節」の組の子供（「節」または「葉」）を交換する。

【００２４】

図１６の６２では、「節６」の子供である「Ｆ」と、「節５」の子供である「Ｈ」とを交換し、つづいて、「節２」の子供である「節５」配下の木を、「根」（節０）のもう１つの子供である「節１」配下の木と交換する。

【００２５】

このようにして折り曲げられた符号木を図１６の６３に示す。６２に示した折り曲げ前の文字「Ｆ」の符号は「１１００」であったが、６３に示した折り曲げ後の文字「Ｆ」の符号は「０１」となり、符号長が４ビットから２ビットに短縮されている。

【００２６】

かかる折り曲げ処理は木全体に影響を及ぼすので、被圧縮データを木に反映するごとにまったく異なる構造の２分木が生成される。このため、このスプレイ符号による圧縮手法によりデータの圧縮をおこなうと、圧縮されたデータの途中から被圧縮データを復元することはできない。

【００２７】

すなわち、被圧縮データを復元するためには、圧縮されたデータの先頭から復元処理をおこなう必要がある。したがって、スプレイ符号により圧縮された圧縮データを任意の位置で２つに分割した場合には、後半の圧縮データから元データの情報を取得することはできない。

【００２８】

図１の説明にもどり、スプレイ符号を用いた圧縮手法により圧縮されたデータの分割について説明する。本実施例１に係るデータ圧縮方法では、上述した手順で生成された圧縮データを、「圧縮データ先頭部分」と、「圧縮データ後半部分」の２つに分離して取り出す。ここで、圧縮データを分離する際には、圧縮されたビット列を区切るような位置で分離することとする。そして、このようにして分離された「圧縮データ先頭部分」および「圧縮データ後半部分」は、それぞれ異なる出力先に出力される。

【００２９】

かかる「圧縮データ先頭部分」は、スプレイ符号による圧縮データの先頭位置付近のデータに相当するため、悪意の第三者により解読されうるが、「圧縮データ先頭部分」は、乱数発生関数などで発生させた意味をもたないビット列の一部分のみからなるので、解読されたとしても、この「圧縮データ先頭部分」から元データに関する情報を取得することは不可能である。

【００３０】

また、上述したように、スプレイ符号による圧縮手法により生成された圧縮データは、

圧縮データの途中からは復元することができないことから、「圧縮データ後半部分」を解読することは不可能である。したがって、「圧縮データ後半部分」が悪意の第三者の手に渡ったとしても、「圧縮データ後半部分」が解読されることはない。

【００３１】

このように、「圧縮データ先頭部分」から取得できる情報量は０であり、「圧縮データ後半部分」から取得できる情報量も０であるため、これらの部分データの片方が悪意の第三者の手に渡ったとしても、元データの秘匿性を確保することができる。

【００３２】

次に、本実施例１に係るデータ復元方法の概要について説明する。図１の２１に示したように、圧縮データを復元する場合には、別ルートで取得した先頭部分と、後半部分とを入力し、後半部分の先頭に先頭部分を付加することにより、圧縮データを再現する。そして、圧縮処理で用いたスプレイ符号により、再現した圧縮データを復号し、復号した圧縮データから、元データを取り出して出力することにより、元データを復元する。

【００３３】

このように、本実施例１に係るデータ圧縮方法およびデータ復元方法は、圧縮処理側では、元データに任意のビット列を付加して圧縮処理をおこない、先頭部分と後半部分とに分離して別ルートで復元処理側に渡すこととし、復元処理側では、別ルートで渡された先頭部分と後半部分とから圧縮データを再現して復号処理をおこない、元データを復元することとした。分離された先頭部分および後半部分からは、それぞれ単独では元データの情報を取得することができないので、圧縮データ自体に秘匿性をもたせたことと等価となる。

【００３４】

したがって、本実施例１に係るデータ圧縮方法およびデータ復元方法によれば、圧縮データ自体に秘匿性をもたせてセキュリティ強度を高めることにより、データ量削減とデータ秘匿とを両立させることができる。

【００３５】

次に、本実施例１に係るデータ圧縮方法およびデータ復元方法を実行するデータ圧縮装置およびデータ復元装置について図２を用いて説明する。図２は、本実施例１に係るデータ圧縮装置およびデータ復元装置の構成を示す機能ブロック図である。

【００３６】

まず、本実施例１に係るデータ圧縮装置について説明する。同図に示すように、データ圧縮装置１０は、元データ入力部１０ａと、ビット列生成部１０ｂと、ビット列付加部１０ｃと、圧縮部１０ｄと、部分取得部１０ｅと、部分データ出力部１０ｆとを備えている。

【００３７】

元データ入力部１０ａは、圧縮対象データ（元データ）を入力する処理部である。この元データ入力部１０ａは、圧縮対象データ（元データ）を受け取ると、受け取った圧縮対象データをビット列付加部１０ｃに渡す処理をおこなう。なお、かかる圧縮対象データ（元データ）の種類や大きさには制限はない。

【００３８】

ビット列生成部１０ｂは、乱数発生関数などで任意のビット列を生成し、生成したビット列をビット列付加部１０ｃに渡す処理をおこなう処理部である。このビット列生成部１０ｂが生成するビット列は、それ自体が意味を持たないビット列である。なお、生成するビット列のビット長は、後述するデータ復元装置２０のビット列除去部２０ｄにおいて用いられるビット長と共通である。

【００３９】

ビット列付加部１０ｃは、ビット列生成部１０ｂから受け取ったビット列を、元データ入力部１０ａから受け取った元データの先頭に付加し、かかるビット列を付加した元データを圧縮部１０ｄに渡す処理部である。

【００４０】

圧縮部１０ｄは、ビット列付加部１０ｃから受け取ったビット列が付加された元データを、スプレイ符号による圧縮手法により圧縮し、部分取得部１０ｅに渡す処理をおこなう処理部である。

【００４１】

部分取得部１０ｅは、圧縮部１０ｄから受け取った圧縮データを、先頭部分と、後半部分とに分離し、分離した各データ列を部分データ出力部１０ｆに渡す処理部である。具体的には、この部分取得部１０ｅは、先頭部分を分離する際に、ビット列生成部１０ｂが生成した任意のビット列が圧縮部１０ｄにより圧縮された後のビット長と同じか、それよりも短くなるように先頭部分を分離する。

【００４２】

このような分離処理をおこなうと、先頭部分には元データが全く含まれておらず、先頭部分は乱数発生関数などにより生成された意味をもたないビット列の一部分のみからなるので、先頭部分が悪意の第三者の手に渡った場合であっても、元データの情報の漏洩を防止することができる。

【００４３】

部分データ出力部１０ｆは、部分取得部１０ｅから渡された先頭部分および後半部分をそれぞれ異なる出力先に出力する処理部である。たとえば、この部分データ出力部１０ｆは、先頭部分を、通信ネットワークを介して復元側に送信するとともに、後半部分をＣＤ－Ｒ（CD Recordable）などの可搬記憶媒体に出力する。このようにすることで、圧縮データを安全に復元側に渡すことができる。

【００４４】

なお、圧縮データを安全に復元側に渡すためには、先頭部分および後半部分のいずれもが悪意の第三者に渡らないようにすればよいので、先頭部分を、通信ネットワークを介してサーバ装置に送信し、後半部分を復元側のコンピュータに送信することとしてもよい。さらに、前半部分を、通信ネットワークを介して第一のサーバ装置に送信し、後半部分を第二のサーバ装置に送信することとしてもよく、上記した前半部分および後半部分の出力先を入れ替えたり、組み合わせたりすることとしてもよい。

【００４５】

また、先頭部分をＵＳＢ（Universal Serial Bus）メモリに出力し、後半部分をＨＤＤ（Hard Disk Drive）に記憶することとすることもできる。このようにすることで、コンピュータ上のデータを安全に管理することができる。

【００４６】

なお、コンピュータ上のデータを安全に管理するためには、先頭部分および後半部分のいずれもが悪意の第三者に渡らないようにすればよいので、先頭部分を、通信ネットワークを介してサーバ装置に送信しておくこととしてもよく、ＣＤ－Ｒなどの可搬記憶媒体に出力することとしてもよい。

【００４７】

次に、本実施例１に係るデータ復元装置の構成について説明する。同図に示すように、データ復元装置２０は、部分データ入力部２０ａと、圧縮データ再現部２０ｂと、復号部２０ｃと、ビット列除去部２０ｄと、元データ出力部２０ｅとを備えている。

【００４８】

部分データ入力部２０ａは、データ圧縮装置１０により分離したうえで出力された先頭部分と、後半部分とを入力する処理部である。この部分データ入力部２０ａは、先頭部分および後半部分を受け取ると、これらのデータ列を圧縮データ再現部２０ｂに渡す処理をおこなう。

【００４９】

圧縮データ再現部２０ｂは、部分データ入力部２０ａから受け取った先頭部分および後半部分から圧縮後のデータ（圧縮データ）を再現し、復号部２０ｃに渡す処理をおこなう処理部である。具体的には、この圧縮データ再現部２０ｂは、後半部分の先頭に先頭部分を付加することにより圧縮データを再現する。

【００５０】
復号部２０ｃは、データ圧縮装置１０の圧縮処理において用いたスプレイ符号による圧縮手法に対応する復号手法により、圧縮データ再現部２０ｂから渡された圧縮データを復号し、復号後のデータをビット列除去部２０ｄに渡す処理をおこなう処理部である。
【００５１】
ビット列除去部２０ｄは、復号部２０ｃから受け取った復号後のデータから先頭に付加されたビット列を除去して元データを取り出し、取り出した元データを元データ出力部２０ｅに渡す処理をおこなう処理部である。なお、このビット列除去部２０ｄがビット列を除去する際に用いるビット長は、ビット列生成部１０ｂが生成したビット列のビット長と共通である。
【００５２】
元データ出力部２０ｅは、ビット列除去部２０ｄから受け取った元データをＨＤＤやＲＡＭ（Random Access Memory）などの出力用デバイスに出力する処理部である。
【００５３】
次に、本実施例１に係るデータ圧縮処理の処理手順について図３を用いて説明する。図３は、本実施例１に係るデータ圧縮処理の処理手順を示すフローチャートである。同図に示すように、データ圧縮装置１０の元データ入力部１０ａにより元データを入力すると（ステップＳ１０１）、ビット列付加部１０ｃは、ビット列生成部１０ｂにより生成されたビット列を元データの先頭に付加する（ステップＳ１０２）。
【００５４】
つづいて、圧縮部１０ｄは、ビット列が付加された元データを圧縮し（ステップＳ１０３）、圧縮データを部分取得部１０ｅに渡す。そして、部分取得部１０ｅは、圧縮データを所定位置で分離することにより、先頭部分および後半部分を取り出す（ステップＳ１０４）。
【００５５】
先頭部分および後半部分を受け取った部分データ出力部１０ｆは、先頭部分の出力をおこない（ステップＳ１０５）、後半部分の出力をおこなって（ステップＳ１０６）処理を終了する。
【００５６】
次に、本実施例１に係るデータ復元処理の処理手順について図４を用いて説明する。図４は、本実施例１に係るデータ復元処理の処理手順を示すフローチャートである。同図に示すように、データ復元装置２０の部分データ入力部２０ａは、データ圧縮装置１０から出力された先頭部分を入力し（ステップＳ２０１）、つづいて、後半部分を入力する（ステップＳ２０２）。
【００５７】
そして、圧縮データ再現部２０ｂは、部分データ入力部２０ａにより入力された後半部分の先頭に、同じく入力された先頭部分を付加して（ステップＳ２０３）圧縮データを再現する。つづいて、復号部２０ｃは、圧縮データ再現部２０ｂにより再現された圧縮データを復号し（ステップＳ２０４）、ビット列除去部２０ｄは、復号部２０ｃにより再現された圧縮データから、元データを取り出す（ステップＳ２０５）。
【００５８】
つづいて、元データ出力部２０ｅは、ビット列除去部２０ｄにより取り出された元データをＨＤＤやＲＡＭなどに出力して（ステップＳ２０６）処理を終了する。
【００５９】
上述してきたように、本実施例１に係るデータ圧縮方法およびデータ復元方法によれば、圧縮データ自体に秘匿性をもたせることができるので、データ量削減とデータ秘匿とを両立させることができる。
【００６０】
ところで、上述した実施例１では、圧縮側では、ビット列データを付加した元データを圧縮し、圧縮されたデータを先頭部分および後半部分の２個のデータ列に分離して出力す

ることとした。しかしながら、本発明に係るデータ圧縮方法およびデータ復元方法は、かかる後半部分をさらに分離して出力することもできる。

【００６１】

そこで、以下に示す実施例２では、かかる後半部分をさらに２個のデータ列に分離する場合について図５～図７を用いて説明することとする。

【実施例２】

【００６２】

まず、本実施例２のデータ圧縮方法およびデータ復元方法の概要について図５を用いて説明する。図５は、本実施例２に係るデータ圧縮方法およびデータ復元方法の概要を示す図である。なお、同図に示す１２が本実施例２に係るデータ圧縮方法であり、同図に示す２２が本実施例２に係るデータ復元方法である。

【００６３】

図５の１２に示したように、圧縮対象となる元データの先頭に乱数発生関数などで発生させたビット列を付加し、かかるビット列が付加された元データをスプレイ符号による圧縮手法を用いて圧縮する点については、上述した実施例１と同様である。

【００６４】

このようにして生成された圧縮データを、圧縮データの先頭部分１２ａと、圧縮データ後半部分の２つに分離する点についても、上述した実施例１と同様であるが、本実施例２に係るデータ圧縮方法では、かかる後半部分を同図に示す１２ｂと１２ｃとにさらに分離して取り出すこととしている。

【００６５】

そして、３つに分離された圧縮データ（１２ａ、１２ｂおよび１２ｃ）のうち、１２ｂを前半部分として出力するとともに、１２ｃの先頭に１２ａを付加したデータ列を後半部分として出力する。

【００６６】

このようにして出力された「圧縮データ前半部分」から取得できる情報量は０である。なぜならば、スプレイ符号による圧縮データは、途中から復元することができないからである。また、「圧縮データ後半部分」から取得できる情報量も０である。なぜならば、後半部分の先頭に付加された１２ａは意味をもたないビット列の一部分のみからなり、１２ｃは、圧縮データの途中以降のデータ列であるからである。したがって、これらの部分データ（圧縮データ前半部分および圧縮データ後半部分）の片方が悪意の第三者の手に渡ったとしても、元データの秘匿性を確保することができる。

【００６７】

なお、本実施例２においては、圧縮データから先頭部分１２ａを除いた後半部分を、１２ｂと１２ｃとの２つのデータ列に分離する場合について説明したが、３つ以上のデータ列に分離することとしてもよい。この場合、先頭部分１２ａの直後に位置するデータ列と、先頭部分１２ａとを別々に出力することとする。

【００６８】

たとえば、圧縮データから先頭部分１２ａを除いた後半部分を、１２ｂ、１２ｃおよび１２ｄの３つに分離した場合には、１２ａと１２ｃとを結合したデータ列と、１２ｂと、１２ｄとをそれぞれ出力するか、１２ａと１２ｄとを結合したデータ列と、１２ｂと、１２ｃとをそれぞれ出力する。

【００６９】

上述した実施例１では、圧縮データを先頭部分および後半部分の２つに分離することとしていたので、先頭部分は、元データの先頭に付加されるビット列の長さによりサイズが限定され、先頭部分を鍵のように扱う使い方に限定されていた。

【００７０】

しかしながら、本実施例２によれば、長さが限定される先頭部分１２ａを、１２ｃと組み合わせて出力することとしたので、前半部分（１２ｂ）と後半部分（１２ａおよび１２ｃ）の長さを等分にするなど、分割するサイズを自由に設定することが可能となる。した

がって、前半部分と後半部分とを、それぞれ異なるサーバ装置に送信するなど、実施例１の場合よりも広範な使い方することができる。

【００７１】

次に、本実施例２に係るデータ復元方法の概要について説明する。図５の２２に示したように、圧縮データを復元する場合には、別ルートで取得した前半部分（１２ｂ）と、後半部分（１２ａおよび１２ｃ）とを入力し、後半部分を１２ａと１２ｃとに分離する。そして、１２ａ、１２ｂおよび１２ｃの順序に並び替えることにより圧縮データを再現し、圧縮処理で用いたスプレイ符号により、再現した圧縮データを復号して復号した圧縮データから、元データを取り出して出力することにより、元データを復元する。

【００７２】

次に、本実施例２に係るデータ圧縮処理の処理手順について図６を用いて説明する。図６は、本実施例２に係るデータ圧縮処理の処理手順を示すフローチャートである。同図に示すように、データ圧縮装置１０の元データ入力部１０ａにより元データを入力すると（ステップＳ３０１）、ビット列付加部１０ｃは、ビット列生成部１０ｂにより生成されたビット列を元データの先頭に付加する（ステップＳ３０２）。

【００７３】

つづいて、圧縮部１０ｄは、ビット列が付加された元データを圧縮し（ステップＳ３０３）、圧縮データを部分取得部１０ｅに渡す。そして、部分取得部１０ｅは、圧縮データを所定位置で分離することにより、先頭部分および後半部分を取り出し（ステップＳ３０４）、さらに後半部分を部分Ａと部分Ｂとの２つに分割し(ステップＳ３０５)、先頭部分、部分Ａおよび部分Ｂを部分データ出力部１０ｆに渡す。

【００７４】

先頭部分、部分Ａおよび部分Ｂを受け取った部分データ出力部１０ｆは、部分Ａを前半部分として出力するとともに（ステップＳ３０６）、部分Ｂの先頭に先頭部分を付加したうえで（ステップＳ３０７）、先頭部分が付加された部分Ｂを後半部分として出力して（ステップＳ３０８）処理を終了する。

【００７５】

次に、本実施例２に係るデータ復元処理の処理手順について図７を用いて説明する。図７は、本実施例２に係るデータ復元処理の処理手順を示すフローチャートである。同図に示すように、データ復元装置２０の部分データ入力部２０ａは、データ圧縮装置１０から出力された前半部分を入力し（ステップＳ４０１）、つづいて、後半部分を入力する（ステップＳ４０２）。

【００７６】

そして、圧縮データ再現部２０ｂは、部分データ入力部２０ａにより入力されたデータを、後半部分に含まれる先頭部分、前半部分（部分Ａ）および後半部分に含まれる部分Ｂの順序に並び替えることにより、圧縮データを再現する(ステップＳ４０３)。

【００７７】

つづいて、復号部２０ｃは、圧縮データ再現部２０ｂにより再現された圧縮データを復号し（ステップＳ４０４）、ビット列除去部２０ｄは、復号部２０ｃにより再現された圧縮データから、元データを取り出す（ステップＳ４０５）。そして、元データ出力部２０ｅは、ビット列除去部２０ｄにより取り出された元データをＨＤＤやＲＡＭなどに出力して（ステップＳ４０６）処理を終了する。

【００７８】

上述してきたように、本実施例２に係るデータ圧縮方法およびデータ復元方法によれば、分割するサイズを自由に設定することができるので、前半部分と後半部分とを、それぞれ異なるサーバ装置に送信するなど、広範な使い方をすることができる。

【００７９】

ところで、上述した実施例１および実施例２では、元データに付加されたビット列を圧縮側から復元側に渡す場合について説明したが、かかるビット列を圧縮側から復元側に渡さずに、圧縮側で生成されたビット列と同じビット列を、復元側で生成することもできる

。
【００８０】
そこで、以下に示す実施例３では、ビット列を圧縮側から復元側に渡すことなく、復元側でかかるビット列を生成する場合について図８～図１４を用いて説明することとする。
【実施例３】
【００８１】
まず、本実施例３のデータ圧縮方法およびデータ復元方法の概要について図８を用いて説明する。図８は、本実施例３に係るデータ圧縮方法およびデータ復元方法の概要を示す図である。なお、同図に示す１３が本実施例３に係るデータ圧縮方法であり、同図に示す２３が本実施例３に係るデータ復元方法である。
【００８２】
図８の１３に示したように、このデータ圧縮方法では、圧縮対象となる元データの先頭に乱数発生関数などで発生させたビット列１３ａを付加し、このビット列１３ａが付加された元データを所定の圧縮手法を用いて圧縮する。ここで、かかる圧縮手法として、上述したスプレイ符号（Ｓｐｌａｙ　ｔｒｅｅ　ｃｏｄｉｎｇ）を用いる。
【００８３】
このようにして生成された圧縮データを、圧縮データ先頭部分と、圧縮データ後半部分の２つに分離して取り出す。圧縮データを分離する際には、圧縮されたビット列１３ａを区切るような位置で分離することとする。そして、分離された先頭部分を削除し、分離された後半部分のみをネットワークや可搬記憶媒体に出力する。
【００８４】
スプレイ符号による圧縮データの途中から復元することができないことから、この「圧縮データ後半部分」を解読することは不可能である。したがって、「圧縮データ後半部分」が悪意の第三者の手に渡ったとしても、元データを含む「圧縮データ後半部分」が解読されることはない。
【００８５】
次に、本実施例３に係るデータ復元方法の概要について説明する。図８の２３に示したように、圧縮データを復元する場合には、上述した実施例１と同様に後半部分を入力する。一方、復元側は圧縮側からビット列１３ａを含むデータを受け取っていないので、このビット列１３ａを生成し、圧縮側と同様の手法により、圧縮側で削除された先頭部分を再現する。
【００８６】
具体的には、圧縮側でビット列１３ａを生成する際に用いた乱数発生関数と同一の乱数発生関数により、圧縮側で生成したものと同一のビット列１３ａを生成する。つづいて、圧縮側でデータ列を圧縮した際に用いたスプレイ符号によりビット列１３ａを圧縮し、圧縮側で先頭部分を分離した位置と同一の位置において、ビット列１３ａを図８に示した２３ａおよび２３ｂに分離する。
【００８７】
そして、この２３ａを、入力された後半部分の先頭に付加することにより、圧縮データを再現する。つづいて、圧縮処理で用いたスプレイ符号により、再現した圧縮データを復号し、復号した圧縮データから、元データを取り出して出力することにより、元データを復元する。
【００８８】
このように、本実施例３に係るデータ圧縮方法およびデータ復元方法は、圧縮処理側では、元データに任意のビット列を付加して圧縮処理をおこない、先頭部分と後半部分とに分離して後半部分のみを復元処理側に渡すこととし、復元処理側では、渡された後半部分と、復元側で生成したビット列とを用いて圧縮データを再現して復号処理をおこない、元データを復元することとした。圧縮側から復元側に渡される後半部分からは、元データの情報を取得することができないので、圧縮データ自体に秘匿性をもたせたことになる。
【００８９】

したがって、本実施例３に係るデータ圧縮方法およびデータ復元方法によれば、先頭部分を圧縮側から復元側に渡さないので、先頭部分と後半部分との双方ともを悪意の第三者に取得されることがない。したがって、より安全にデータの受渡しをおこなうことができる。

【００９０】

次に、本実施例３に係るデータ圧縮方法およびデータ復元方法を実行するデータ圧縮装置およびデータ復元装置について図９を用いて説明する。図９は、本実施例３に係るデータ圧縮装置およびデータ復元装置の構成を示す機能ブロック図である。なお、実施例１と同様の処理をおこなう構成部分については、簡単な説明のみにとどめることとする。

【００９１】

まず、本実施例３に係るデータ圧縮装置について説明する。同図に示すように、データ圧縮装置３０は、元データ入力部３０ａと、ビット列生成部３０ｂと、ビット列付加部３０ｃと、圧縮部３０ｄと、部分取得部３０ｅと、後半データ出力部３０ｆとを備えている。

【００９２】

元データ入力部３０ａ～部分取得部３０ｅは、実施例１における元データ入力部１０ａ～部分取得部１０ｅと同一であるので、説明を省略する。後半データ出力部３０ｆは、部分取得部３０ｅから渡された先頭部分を削除するとともに、後半部分を、通信ネットワークを介して復元側に送信したり、可搬記憶媒体に出力したりする処理部である。

【００９３】

このように、後半データ出力部３０ｆは、圧縮データの後半部分のみを出力するので、この後半部分が悪意の第三者に渡ったとしても、後半部分のみを用いて元データが復元されることはない。

【００９４】

次に、本実施例３に係るデータ復元装置の構成について説明する。同図に示すように、データ復元装置４０は、後半データ入力部４０ａと、ビット列生成部４０ｂと、圧縮部４０ｃと、部分取得部４０ｄと、圧縮データ再現部４０ｅと、復号部４０ｆと、ビット列除去部４０ｇと、元データ出力部４０ｈとを備えている。

【００９５】

後半データ入力部４０ａは、データ圧縮装置３０により出力された後半部分を入力する処理部である。この後半データ入力部４０ａは、かかる後半部分を受け取ると、受け取った後半部分を圧縮データ再現部４０ｂに渡す処理をおこなう。

【００９６】

ビット列生成部４０ｂは、圧縮装置３０のビット列生成部３０ｂと同様の処理をおこなうことにより、ビット列生成部３０ｂが生成したビット列と同一のビット列を生成し、生成したビット列を圧縮部４０ｃに渡す処理をおこなう処理部である。

【００９７】

圧縮部４０ｃは、圧縮装置３０の圧縮部３０ｄと同様の処理をおこなうことにより、ビット列生成部４０ｂが生成したビット列を圧縮し、圧縮されたビット列を部分取得部４０ｄに渡す処理を行なう処理部である。

【００９８】

部分取得部４０ｄは、圧縮装置３０の部分取得部３０ｅと同様の処理をおこなうことにより、圧縮部４０ｃから受け取った圧縮されたビット列から、圧縮装置３０の部分取得部３０ｅが取得した先頭部分と同じビット長の先頭部を取得し、圧縮データ再現部４０ｅに渡す処理をおこなう処理部である。

【００９９】

圧縮データ再現部４０ｅは、後半データ入力部４０ａから受け取った後半データと、部分取得部４０ｄから受け取った先頭データとから圧縮データを再現する処理部である。具体的には、この圧縮データ再現部４０ｅは、かかる後半データの先頭に、かかる先頭データを付加することにより圧縮データを再現する。

【０１００】
なお、復号部４０ｆ、ビット列除去部４０ｇおよび元データ出力部４０ｈがおこなう処理は、実施例１で示した復号部２０ｃ、ビット列除去部２０ｄおよび元データ出力部２０ｅがおこなう処理と同様であるので説明を省略する。
【０１０１】
次に、本実施例３に係るデータ圧縮処理の処理手順について図１０を用いて説明する。図１０は、本実施例３に係るデータ圧縮処理の処理手順を示すフローチャートである。同図に示すように、データ圧縮装置３０の元データ入力部３０ａにより元データを入力すると（ステップＳ５０１）、ビット列付加部３０ｃは、ビット列生成部３０ｂにより生成されたビット列を元データの先頭に付加する（ステップＳ５０２）。
【０１０２】
つづいて、圧縮部３０ｄは、ビット列が付加された元データを圧縮し（ステップＳ５０３）、圧縮データを部分取得部３０ｅに渡す。そして、部分取得部３０ｅは、圧縮データを所定位置で分離することにより、先頭部分および後半部分を取り出す（ステップＳ５０４）。先頭部分および後半部分を受け取った後半データ出力部３０ｆは、かかる先頭部分を削除するとともに、後半部分の出力をおこなって（ステップＳ５０５）処理を終了する。
【０１０３】
次に、本実施例３に係るデータ復元処理の処理手順について図１１を用いて説明する。図１１は、本実施例３に係るデータ復元処理の処理手順を示すフローチャートである。同図に示すように、データ復元装置４０のビット列生成部４０ｂは、任意のビット列を生成し（ステップＳ６０１）、生成したビット列を圧縮部４０ｃに渡す。そして、圧縮部４０ｃは、渡されたビット列を圧縮し（ステップＳ６０２）、部分取得部４０ｄは、圧縮されたビット列の先頭部分を取り出して（ステップＳ６０３）圧縮データ再現部４０ｅに渡す。
【０１０４】
つづいて、データ復元装置４０の後半データ入力部４０ａは、データ圧縮装置３０から出力された先頭部分を入力し（ステップＳ６０４）、圧縮データ再現部４０ｅに渡す。そして、圧縮データ再現部４０ｅは、後半データ入力部４０ａから渡された後半部分の先頭に、部分取得部４０ｄから渡された先頭部分を付加することにより圧縮データを再現する（ステップＳ６０５）。
【０１０５】
そして、復号部４０ｆは、圧縮データ再現部４０ｅにより再現された圧縮データを復号し（ステップＳ６０６）、ビット列除去部４０ｇは、復号部４０ｆにより再現された圧縮データから、元データを取り出す（ステップＳ６０７）。つづいて、元データ出力部２０ｈは、ビット列除去部４０ｇにより取り出された元データをＨＤＤやＲＡＭなどに出力して（ステップＳ６０８）処理を終了する。
【０１０６】
上述してきたように、本実施例３に係るデータ圧縮方法およびデータ復元方法によれば、分離した圧縮データの後半部分のみを圧縮側から復元側に渡すこととしたので、分離した圧縮データすべてが悪意の第三者の手に渡ることを防止することにより、安全なデータの受渡しをおこなうことができる。
【０１０７】
ところで、上述した実施例３では、圧縮側と復元側とで、同一の乱数発生関数を用いて共通のビット列を生成することとしたが、かかるビット列を生成する手法にはいくつかのバリエーションが存在する。以降では、かかるビット列生成のバリエーションを用いたデータ圧縮方法およびデータ復元方法の例を、図１２～図１４を用いて説明することとする。
【０１０８】
最初に、実施例３の変形例１について図１２を用いて説明する。図１２は、本実施例３

に係るデータ圧縮方法およびデータ復元方法の変形例１の概要を示す図である。なお、同図に示す１４が本変形例１に係るデータ圧縮方法であり、同図に示す２４が本変形例１に係るデータ復元方法である。

【０１０９】

図１２の１４に示したように、本変形例１に係るデータ圧縮方法では、元データの先頭に付加するビット列をシードおよび鍵から生成する。この場合、かかるシードおよび鍵からハッシュ関数（一方向性関数）を用いてビット列を生成する。そして、かかるビット列が付加された元データを圧縮し、この圧縮データを、圧縮データ先頭部分と、圧縮データ後半部分の２つに分離して取り出す。そして、分離された先頭部分を削除するとともに、後半部分の先頭にビット列生成において用いたシードを付加して出力する。

【０１１０】

次に、本変形例１に係るデータ復元方法の概要について説明する。図１２の２４に示したように、圧縮データを復元する場合には、図８に示した２３と同様に後半部分を入力する。なお、この後半部分は、先頭にシードが付加されたデータ列である。復元側は、圧縮側からビット列を含むデータを受け取っていないので、このビット列を生成し、圧縮側において削除された先頭部分を再現することになる。

【０１１１】

かかるビット列を生成する際に、本変形例１に係るデータ復元方法では、圧縮側と共有している（圧縮側と同一の）鍵と、後半部分の先頭に付加されて渡されたシードとから、圧縮側と同様の手法によりビット列を生成する。なお、以降の処理については、図８に示した２３の処理と同様であるため、説明を省略する。

【０１１２】

次に、実施例３の変形例２について図１３を用いて説明する。図１３は、本実施例３に係るデータ圧縮方法およびデータ復元方法の変形例２の概要を示す図である。なお、同図に示す１５が本変形例２に係るデータ圧縮方法であり、同図に示す２５が本変形例２に係るデータ復元方法である。

【０１１３】

図１３の１５に示したように、本変形例２に係るデータ圧縮方法では、元データの先頭に付加するビット列をカウンタ値および鍵から生成する。この場合、かかるカウンタ値を生成するカウンタは、圧縮側と復元側とで共通のものを用い、所定の規則でカウンタ値が変化していくようにする。このようにして生成されたカウンタ値および鍵からハッシュ関数（一方向性関数）を用いてビット列を生成する。

【０１１４】

そして、かかるビット列が付加された元データを圧縮し、この圧縮データを、圧縮データ先頭部分と、圧縮データ後半部分の２つに分離して取り出す。そして、分離された先頭部分を削除するとともに、後半部分のみを出力する。

【０１１５】

次に、本変形例２に係るデータ復元方法の概要について説明する。図１３の２５に示したように、圧縮データを復元する場合には、図８に示した２３と同様に後半部分を入力する。復元側は、圧縮側からビット列を含むデータを受け取っていないので、このビット列を生成し、圧縮側において削除された先頭部分を再現することになる。

【０１１６】

かかるビット列を生成する際に、本変形例２に係るデータ復元方法では、圧縮側と共有している（圧縮側と同一の）鍵と、圧縮側と同期している（圧縮側と同一の規則でカウンタ値を生成する）カウンタが生成したカウンタ値とから、圧縮側と同様の手法によりビット列を生成する。なお、以降の処理については、図８に示した２３の処理と同様であるため、説明を省略する。

【０１１７】

最後に、実施例３の変形例３について図１４を用いて説明する。図１４は、本実施例３に係るデータ圧縮方法およびデータ復元方法の変形例３の概要を示す図である。なお、同

図に示す１６が本変形例３に係るデータ圧縮方法であり、同図に示す２６が本変形例３に係るデータ復元方法である。

【０１１８】

図１４の１６に示したように、本変形例３に係るデータ圧縮方法では、元データの先頭に付加するビット列をビット列群から選択する。この場合、選択されたビット列を特定する選択番号を一時的に記憶しておく。

【０１１９】

そして、かかるビット列が付加された元データを圧縮し、この圧縮データを、圧縮データ先頭部分と、圧縮データ後半部分の２つに分離して取り出す。そして、分離された先頭部分を削除するとともに、後半部分の先頭に、ビット列生成において一時的に記憶しておいた選択番号を付加して出力する。

【０１２０】

なお、本変形例３においては、ビット列群から選択されたビット列を特定するための認識情報として選択番号を用いた場合について説明したが、ビット列が格納されたアドレスなどのように、選択されたビット列を特定できる情報であればよい。

【０１２１】

次に、本変形例３に係るデータ復元方法の概要について説明する。図１４の２６に示したように、圧縮データを復元する場合には、図８に示した２３と同様に後半部分を入力する。なお、この後半部分は、先頭に選択番号が付加されたデータ列である。

【０１２２】

復元側は、圧縮側からビット列を含むデータを受け取っていないので、このビット列を生成し、圧縮側において削除された先頭部分を再現することになる。かかるビット列を生成する際に、本変形例３に係るデータ復元方法では、圧縮側と共有している（圧縮側と同一の）ビット列群と、後半部分の先頭に付加されて渡された選択番号とから、圧縮側と同様の手法によりビット列を選択する。なお、以降の処理については、図８に示した２３の処理と同様であるため、説明を省略する。

【０１２３】

ところで、上記の実施例で説明した各種の処理は、あらかじめ用意されたプログラムをコンピュータで実行することによって実現することができる。そこで、以下では、図１７を用いて、上記の実施例と同様の機能を有するデータ圧縮プログラムおよびデータ復元プログラムを実行するコンピュータの一例を説明する。

【０１２４】

図１７は、データ圧縮プログラムおよびデータ復元プログラムを実行するコンピュータを示す図である。なお、図１７においては、データ圧縮プログラムおよびデータ復元プログラムを同一のコンピュータ上で動作させる場合について示しているが、データ圧縮プログラムおよびデータ復元プログラムのいずれか一方のみを各コンピュータ上で動作させることとしてもよい。

【０１２５】

同図に示すようにデータ圧縮・復元装置としてのコンピュータ１００は、入力装置１０１、モニタ１０２、可搬媒体制御Ｉ／Ｆ部１０３、ネットワークＩ／Ｆ部１０４、ＨＤＤ（Hard Disk Drive）１０５およびＣＰＵ（Central Processing Unit）１０６をバス１０７で接続して構成される。ここで、入力装置１０１はキーボードなどの入力用デバイスであり、モニタ１０２はディスプレイなどの表示用デバイスである。

【０１２６】

また、可搬媒体制御Ｉ／Ｆ部１０３は、ＣＤ－Ｒ装置などの可搬媒体装置制御用デバイスである。そして、ネットワークＩ／Ｆ部１０４は、ＬＡＮ（Local Area Network）ボードなどの通信用デバイスであり、ＬＡＮなどのネットワークを介して他のコンピュータ１００や図示しないサーバ装置と通信をおこなう。

【０１２７】

ＨＤＤ１０５には、データ圧縮プログラム１０５ａおよびデータ復元プログラム１０５

ｂがあらかじめ記憶されており、ＣＰＵ１０６が、ＨＤＤ１０５のデータ圧縮プログラム１０５ａおよびデータ復元プログラム１０５ｂを読み出して実行することで、図１７に示すように、データ圧縮プログラム１０５ａはデータ圧縮プロセス１０６ａとして、データ復元プログラム１０５ｂはデータ復元プログラム１０６ｂとして、それぞれ機能するようになる。

【０１２８】

ところで、上記したデータ圧縮プログラム１０５ａおよびデータ復元プログラム１０５ｂについては、必ずしもあらかじめＨＤＤ１０５に記憶させておく必要はなく、たとえば、コンピュータ１００が読み出し可能なフレキシブルディスク（ＦＤ）、ＣＤ－ＲＯＭ、光磁気ディスクなどの可搬記憶媒体、または、公衆回線、インターネット、ＬＡＮ、ＷＡＮ（Wide Area Network）などを介してコンピュータ１００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き、コンピュータ１００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。

【０１２９】

（付記１）被圧縮データ列から秘匿性を有する圧縮データ列を生成するデータ圧縮方法であって、

所定長のビット列を前記被圧縮データ列の先頭に付加するビット列付加工程と、

前記ビット列付加工程により前記ビット列が付加された前記被圧縮データ列を圧縮する圧縮工程と、

前記圧縮工程により生成された圧縮データ列の先頭位置から該データ圧縮工程により圧縮された前記ビット列の所定位置までの先頭部分を、該圧縮データ列から分割する分割工程と

を含んだことを特徴とするデータ圧縮方法。

【０１３０】

（付記２）前記圧縮データ列から前記先頭部分を除いた後半部分を１または複数のブロックとし、少なくとも、該先頭部分と最初のブロックとを別々に出力する出力工程をさらに含んだことを特徴とする付記１に記載のデータ圧縮方法。

【０１３１】

（付記３）前記出力工程は、前記先頭部分を出力する前半データ出力工程と、前記圧縮データ列から前記先頭部分を除いた後半部分を出力する後半データ出力工程とをさらに含んだことを特徴とする付記２に記載のデータ圧縮方法。

【０１３２】

（付記４）前記出力工程は、前記後半部分を２つのブロックに分割する後半部分分割工程と、最初の該ブロックを出力する前半データ出力工程と、最後の該ブロックの先頭に前記先頭部分を付加して出力する後半データ出力工程とをさらに含んだことを特徴とする付記２に記載のデータ圧縮方法。

【０１３３】

（付記５）前記前半データ出力工程と前記後半データ出力工程とは、それぞれ異なる出力先にデータ出力をおこなうことを特徴とする付記３または４に記載のデータ圧縮方法。

【０１３４】

（付記６）前記圧縮データ列から前記先頭部分を除いた後半部分を出力する後半部分出力工程をさらに含んだことを特徴とする付記１に記載のデータ圧縮方法。

【０１３５】

（付記７）鍵を生成する鍵生成工程と、

任意のシードを生成するシード生成工程と、

前記鍵生成工程により生成された前記鍵と、前記シード生成工程により生成された前記シードとから、ハッシュ関数を用いて前記ビット列を生成するビット列生成工程とをさらに含み、

前記後半部分出力工程は、該シードを前記後半部分に付加したデータを出力することを特徴とする付記６に記載のデータ圧縮方法。

【０１３６】
（付記８）鍵を生成する鍵生成工程と、
カウンタ値生成ごとに、所定の規則に基づいて異なるカウンタ値を生成するカウンタ値生成工程と、
前記鍵生成工程により生成された前記鍵と、前記カウンタ値生成工程により生成された前記カウンタ値とから、ハッシュ関数を用いて前記ビット列を生成するビット列生成工程と
をさらに含んだことを特徴とする付記６に記載のデータ圧縮方法。
【０１３７】
（付記９）ビット列群を記憶装置に保持させるビット列群保持工程と、
前記ビット列群保持工程から１つの前記ビット列を選択するビット列選択工程とをさらに含み、
前記後半部分出力工程は、前記ビット列選択工程により選択された前記ビット列の選択情報を前記後半部分に付加したデータを出力することを特徴とする付記６に記載のデータ圧縮方法。
【０１３８】
（付記１０）付記２で出力されたデータから前記被圧縮データ列を復元するデータ復元方法であって、
前記先頭部分および１または複数の前記ブロックから前記圧縮データ列を再現する圧縮データ再現工程と、
前記圧縮データ再現工程により再現された前記圧縮データ列を復号する復号工程と、
前記復号工程により復号されたデータ列から前記ビット列を除去して前記被圧縮データ列を出力する出力工程と
を含んだことを特徴とするデータ復元方法。
【０１３９】
（付記１１）付記６で出力されたデータを用いて前記被圧縮データ列を復元するデータ復元方法であって、
前記ビット列を前記圧縮工程により圧縮するビット列圧縮工程と、
前記ビット列圧縮工程により圧縮されたビット列から前記先頭部分を分割するビット列分割工程と、
前記後半部分出力工程により出力された前記後半部分を入力する入力工程と、
前記ビット列分割工程により分割された前記先頭部分を、前記入力工程により入力された前記後半部分の先頭に付加することにより前記圧縮データ列を再現する圧縮データ再現工程と、
前記圧縮データ再現工程により再現された前記圧縮データ列を復号する復号工程と、
前記復号工程により復号されたデータ列から前記ビット列を除去して前記被圧縮データ列を出力する出力工程と
を含んだことを特徴とするデータ復元方法。
【０１４０】
（付記１２）付記７で出力されたデータを用いて前記被圧縮データ列を復元するデータ復元方法であって、
鍵を生成する鍵生成工程と、
前記鍵生成工程により生成された前記鍵と、前記後半部分出力工程により出力されたデータから分離した前記シードとから、前記ハッシュ関数を用いて前記ビット列を生成するビット列生成工程と、
前記ビット列生成工程により生成された前記ビット列を前記圧縮工程により圧縮するビット列圧縮工程と、
前記ビット列圧縮工程により圧縮されたビット列から前記先頭部分を分割するビット列分割工程と、
前記後半部分出力工程により出力されたデータから前記シードを分離して得られる前記

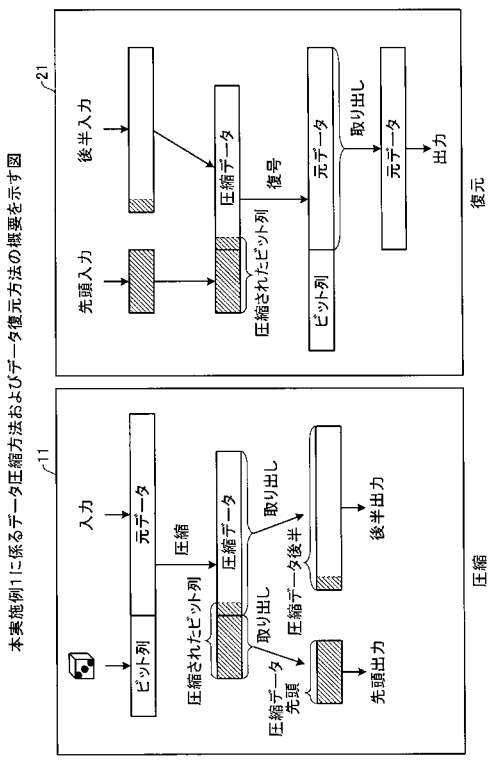
後半部分を入力する入力工程と、
前記ビット列分割工程により分割された前記先頭部分を、前記入力工程により入力された前記後半部分の先頭に付加することにより前記圧縮データ列を再現する圧縮データ再現工程と、
前記圧縮データ再現工程により再現された前記圧縮データ列を復号する復号工程と、
前記復号工程により復号されたデータ列から前記ビット列を除去して前記被圧縮データ列を出力する出力工程と
を含んだことを特徴とするデータ復元方法。
【０１４１】
（付記１３）付記８で出力されたデータを用いて前記被圧縮データ列を復元するデータ復元方法であって、
鍵を生成する鍵生成工程と、
カウンタ値生成ごとに、所定の規則に基づいて異なるカウンタ値を生成するカウンタ値生成工程と、
前記鍵生成工程により生成された前記鍵と、前記カウンタ値生成工程により生成された前記カウンタ値とから、ハッシュ関数を用いて前記ビット列を生成するビット列生成工程と、
前記ビット列生成工程により生成された前記ビット列を前記圧縮工程により圧縮するビット列圧縮工程と、
前記ビット列圧縮工程により圧縮されたビット列から前記先頭部分を分割するビット列分割工程と、
前記後半部分出力工程により出力された前記後半部分を入力する入力工程と、
前記ビット列分割工程により分割された前記先頭部分を、前記入力工程により入力された前記後半部分の先頭に付加することにより前記圧縮データ列を再現する圧縮データ再現工程と、
前記圧縮データ再現工程により再現された前記圧縮データ列を復号する復号工程と、
前記復号工程により復号されたデータ列から前記ビット列を除去して前記被圧縮データ列を出力する出力工程と
を含んだことを特徴とするデータ復元方法。
【０１４２】
（付記１４）付記９で出力されたデータを用いて前記被圧縮データ列を復元するデータ復元方法であって、
ビット列群を記憶装置に保持させるビット列群保持工程と、
前記ビット列群保持工程から、前記後半部分出力工程により出力されたデータから分離した前記選択情報を用いて前記ビット列を選択するビット列選択工程と、
前記ビット列選択工程により選択された前記ビット列を前記圧縮工程により圧縮するビット列圧縮工程と、
前記ビット列圧縮工程により圧縮されたビット列から前記先頭部分を分割するビット列分割工程と、
前記後半部分出力工程により出力されたデータから前記選択情報を分離して得られる前記後半部分を入力する入力工程と、
前記ビット列分割工程により分割された前記先頭部分を、前記入力工程により入力された前記後半部分の先頭に付加することにより前記圧縮データ列を再現する圧縮データ再現工程と、
前記圧縮データ再現工程により再現された前記圧縮データ列を復号する復号工程と、
前記復号工程により復号されたデータ列から前記ビット列を除去して前記被圧縮データ列を出力する出力工程と
を含んだことを特徴とするデータ復元方法。
【０１４３】
（付記１５）被圧縮データ列から秘匿性を有する圧縮データ列を生成するデータ圧縮装置

であって、
所定長のビット列を前記被圧縮データ列の先頭に付加するビット列付加手段と、
前記ビット列付加手段により前記ビット列が付加された前記被圧縮データ列を圧縮する圧縮手段と、
前記圧縮手段により生成された圧縮データ列の先頭位置から該データ圧縮手段により圧縮された前記ビット列の所定位置までの先頭部分を、該圧縮データ列から分割する分割手段と
を備えたことを特徴とするデータ圧縮装置。
【０１４４】
（付記１６）前記圧縮データ列から前記先頭部分を除いた後半部分を１または複数のブロックとし、少なくとも、該先頭部分と最初のブロックとを別々に出力する出力手段をさらに備えたことを特徴とする付記１５に記載のデータ圧縮装置。
【０１４５】
（付記１７）前記圧縮データ列から前記先頭部分を除いた後半部分を出力する後半部分出力手段をさらに含んだことを特徴とする付記１５に記載のデータ圧縮装置。
【０１４６】
（付記１８）被圧縮データ列から秘匿性を有する圧縮データ列を生成するデータ圧縮プログラムであって、
所定長のビット列を前記被圧縮データ列の先頭に付加するビット列付加手順と、
前記ビット列付加手順により前記ビット列が付加された前記被圧縮データ列を圧縮する圧縮手順と、
前記圧縮手順により生成された圧縮データ列の先頭位置から該データ圧縮手段により圧縮された前記ビット列の所定位置までの先頭部分を、該圧縮データ列から分割する分割手順と
をコンピュータに実行させることを特徴とするデータ圧縮プログラム。
【０１４７】
（付記１９）前記圧縮データ列から前記先頭部分を除いた後半部分を１または複数のブロックとし、少なくとも、該先頭部分と最初のブロックとを別々に出力する出力手順をさらにコンピュータに実行させることを特徴とする付記１８に記載のデータ圧縮プログラム。
【０１４８】
（付記２０）前記圧縮データ列から前記先頭部分を除いた後半部分を出力する後半部分出力手順をさらにコンピュータに実行させることを特徴とする付記１８に記載のデータ圧縮プログラム。
【産業上の利用可能性】
【０１４９】
以上のように、本発明に係るデータ圧縮方法、データ復元方法、データ圧縮装置、データ復元装置、データ圧縮プログラムおよびデータ復元プログラムは、文書データや画像データなどの各種データの圧縮処理および復元処理に有用であり、特に、データに秘匿性をもたせることが必要なデータの圧縮処理および復元処理に適している。
【図面の簡単な説明】
【０１５０】
【図１】本実施例１に係るデータ圧縮方法およびデータ復元方法の概要を示す図である。
【図２】本実施例１に係るデータ圧縮装置およびデータ復元装置の構成を示す機能ブロック図である。
【図３】本実施例１に係るデータ圧縮処理の処理手順を示すフローチャートである。
【図４】本実施例１に係るデータ復元処理の処理手順を示すフローチャートである。
【図５】本実施例２に係るデータ圧縮方法およびデータ復元方法の概要を示す図である。
【図６】本実施例２に係るデータ圧縮処理の処理手順を示すフローチャートである。
【図７】本実施例２に係るデータ復元処理の処理手順を示すフローチャートである。
【図８】本実施例３に係るデータ圧縮方法およびデータ復元方法の概要を示す図である。

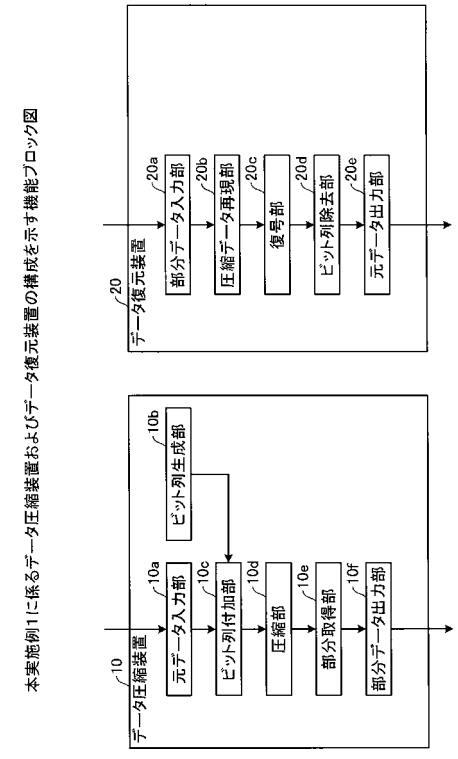
【図９】本実施例３に係るデータ圧縮装置およびデータ復元装置の構成を示す機能ブロック図である。
【図１０】本実施例３に係るデータ圧縮処理の処理手順を示すフローチャートである。
【図１１】本実施例３に係るデータ復元処理の処理手順を示すフローチャートである。
【図１２】本実施例３に係るデータ圧縮方法およびデータ復元方法の変形例１の概要を示す図である。
【図１３】本実施例３に係るデータ圧縮方法およびデータ復元方法の変形例２の概要を示す図である。
【図１４】本実施例３に係るデータ圧縮方法およびデータ復元方法の変形例３の概要を示す図である。
【図１５】従来のデータ圧縮方法およびデータ復元方法の概要を示す図である。
【図１６】スプレイ符号の概要を示す図である。
【図１７】データ圧縮プログラムおよびデータ復元プログラムを実行するコンピュータを示す図である。
【符号の説明】
【０１５１】
１０　圧縮装置
１０ａ　元データ入力部
１０ｂ　ビット列生成部
１０ｃ　ビット列付加部
１０ｄ　圧縮部
１０ｅ　部分取得部
１０ｆ　部分データ出力部
１１～１６　圧縮処理
２０　復元装置
２０ａ　部分データ入力部
２０ｂ　圧縮データ再現部
２０ｃ　復号部
２０ｄ　ビット列除去部
２０ｅ　元データ出力部
２１～２６　復元処理
３０　圧縮装置
３０ａ　元データ入力部
３０ｂ　ビット列生成部
３０ｃ　ビット列付加部
３０ｄ　圧縮部
３０ｅ　部分取得部
３０ｆ　後半データ出力部
４０　復元装置
４０ａ　後半データ入力部
４０ｂ　ビット列生成部
４０ｃ　圧縮部
４０ｄ　部分取得部
４０ｅ　圧縮データ再現部
４０ｆ　復号部
４０ｇ　ビット列除去部
４０ｈ　元データ出力部
５１　従来の圧縮処理
５２　従来の復元処理
６１～６３　スプレイ符号木

１００　データ圧縮・復元装置（コンピュータ）
１０１　入力装置
１０２　モニタ
１０３　可搬媒体制御Ｉ／Ｆ部
１０４　ネットワークＩ／Ｆ部
１０５　ＨＤＤ
１０５ａ　データ圧縮プログラム
１０５ｂ　データ復元プログラム
１０６　ＣＰＵ
１０６ａ　データ圧縮プロセス
１０６ｂ　データ復元プロセス
１０７　バス

【図１】

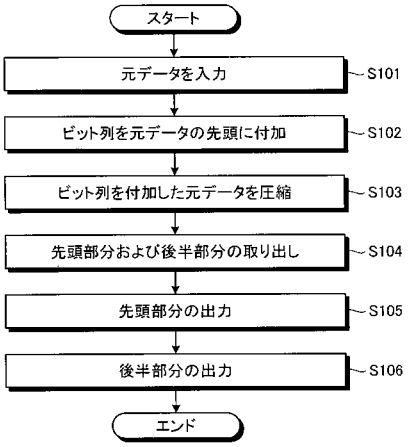


【図２】



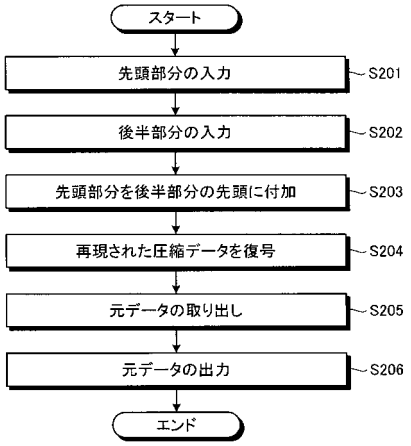
【図３】

本実施例1に係るデータ圧縮処理の処理手順を示すフローチャート

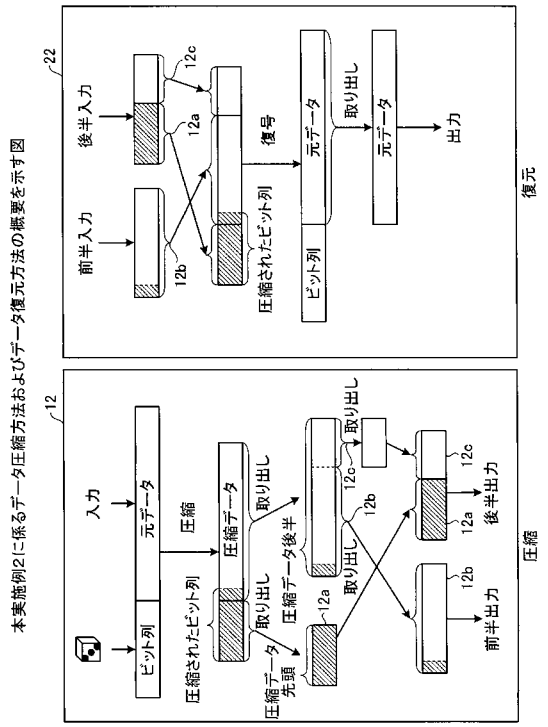


【図４】

本実施例1に係るデータ復元処理の処理手順を示すフローチャート

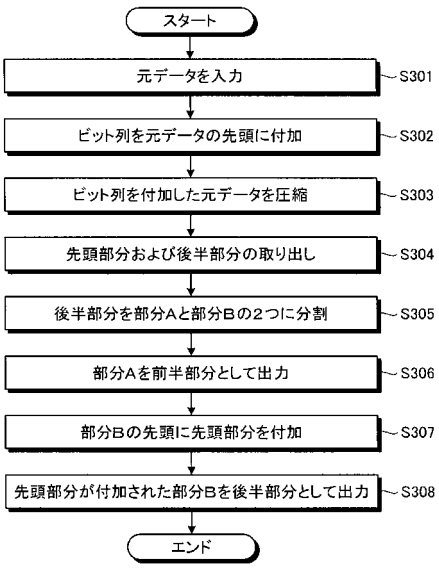


【図５】



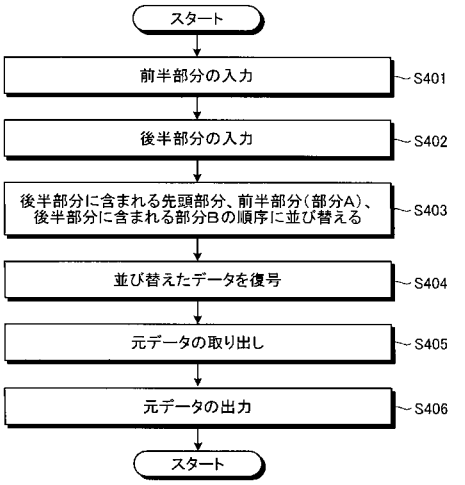
【図６】

本実施例2に係るデータ圧縮処理の処理手順を示すフローチャート



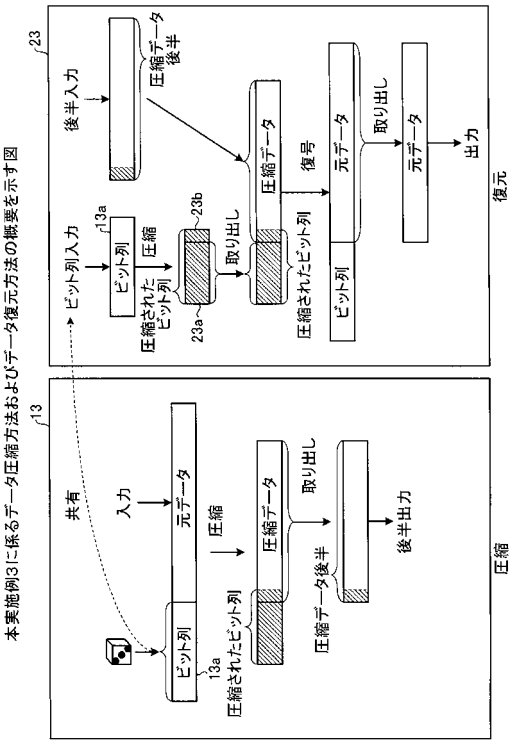
【図７】

本実施例2に係るデータ復元処理の処理手順を示すフローチャート



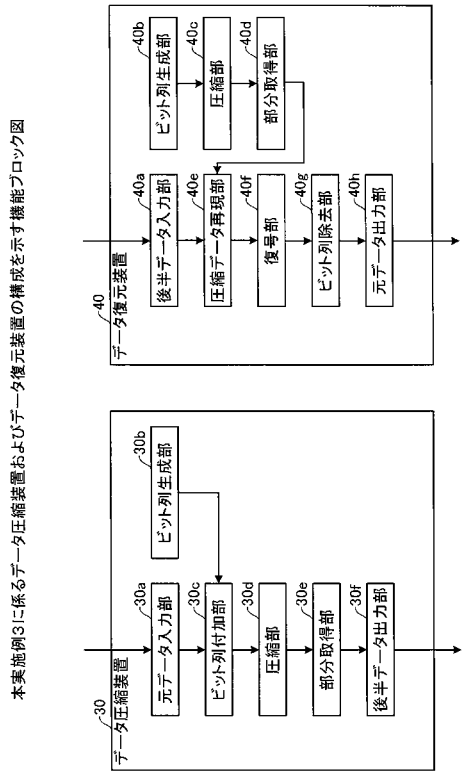
【図８】

本実施例3に係るデータ圧縮方法およびデータ復元方法の概要を示す図



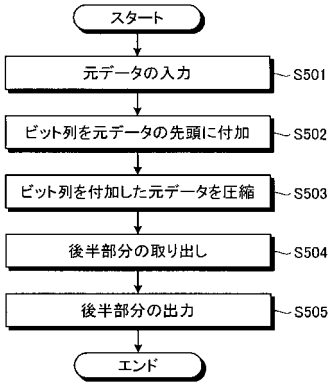
【図９】

本実施例3に係るデータ圧縮装置およびデータ復元装置の構成を示す機能ブロック図



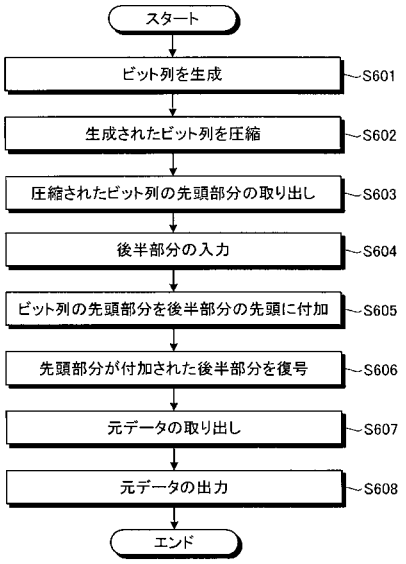
【図１０】

本実施例3に係るデータ圧縮処理の処理手順を示すフローチャート

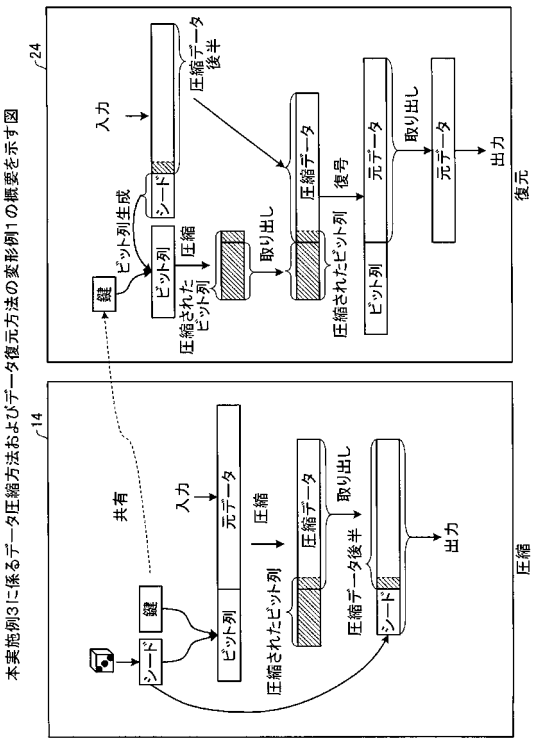


【図１１】

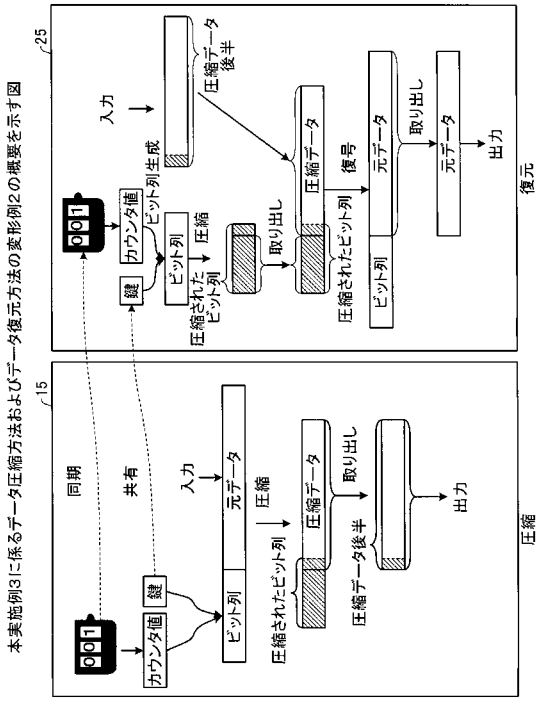
本実施例3に係るデータ復元処理の処理手順を示すフローチャート



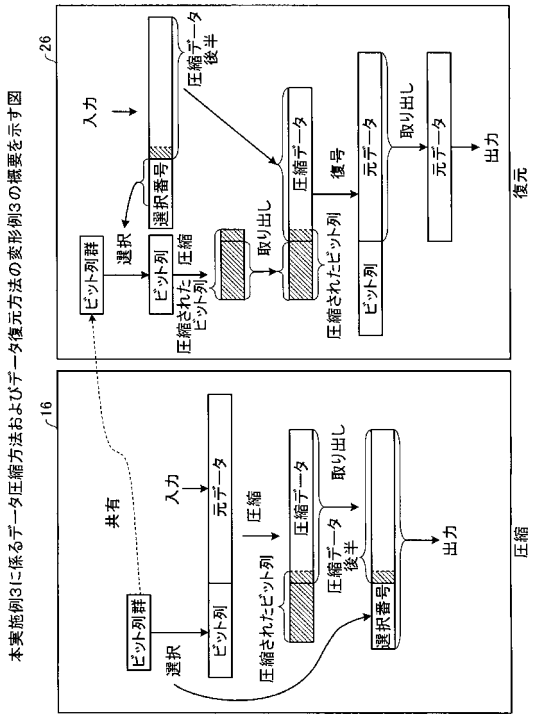
【図１２】



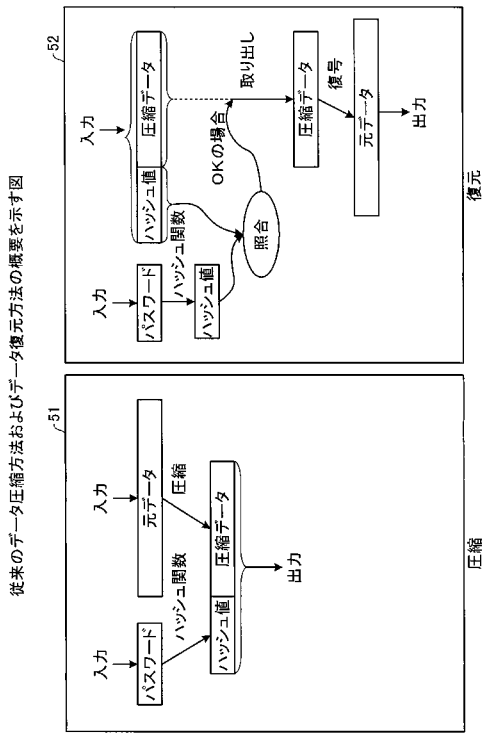
【図１３】



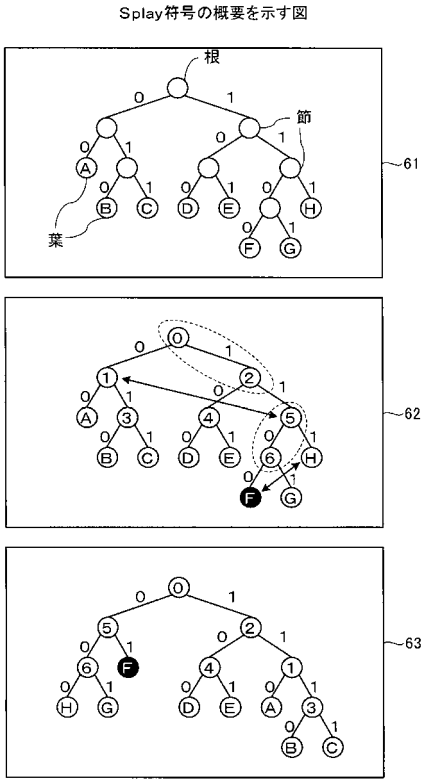
【図１４】



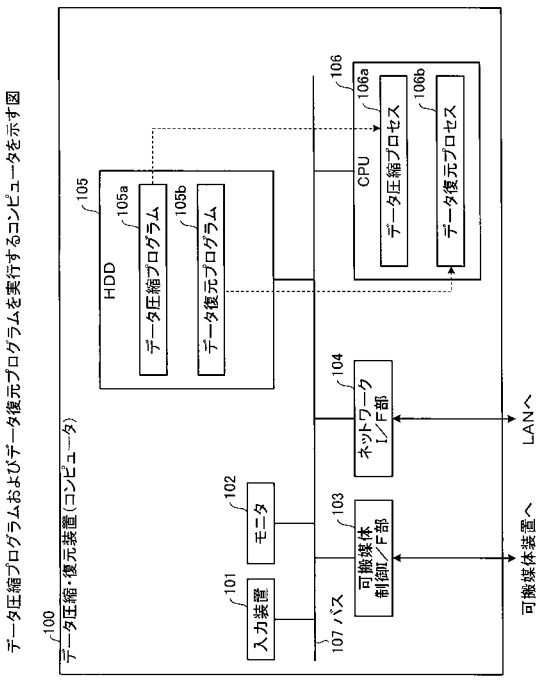
【図１５】


従来のデータ圧縮方法およびデータ復元方法の概要を示す図
圧縮
51
入力
パスワード
入力
元データ
圧縮
ハッシュ関数
ハッシュ値
圧縮データ
出力
復元
52
入力
パスワード
ハッシュ関数
ハッシュ値
入力
圧縮データ
ハッシュ値
照合
OKの場合
取り出し
圧縮データ
復号
元データ
出力

【図１６】


Splay符号の概要を示す図
根
節
葉
61
62
63

【図１７】


データ圧縮プログラムおよびデータ復元プログラムを実行するコンピュータを示す図
データ圧縮・復元装置(コンピュータ)
100
HDD
105
データ圧縮プログラム
105a
データ復元プログラム
105b
CPU
106
データ圧縮プロセス
106a
データ復元プロセス
106b
入力装置
101
モニタ
102
可搬媒体制御I/F部
103
ネットワークI/F部
104
107 バス
LANへ
可搬媒体装置へ