(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-303776
(P2005-303776A)
(43)公開日　平成17年10月27日(2005.10.27)

| (51)Int.Cl.[7] | F I | | テーマコード（参考） |
|---|---|---|---|
| H04L 9/08 | H04L | 9/00　601A | 5J104 |

審査請求 未請求　請求項の数 6　OL　（全 19 頁）

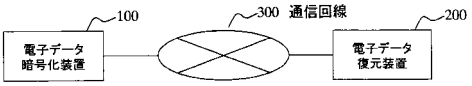
(21)出願番号　特願2004-118706 (P2004-118706)
(22)出願日　平成16年4月14日 (2004.4.14)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100073760
弁理士　鈴木　誠
(72)発明者　廣田　啓一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　遠藤　雅和
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　山室　雅司
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】電子データ暗号化装置、電子データ復元装置及びプログラム

(57)【要約】
【課題】画像データや音楽データなどの任意の種類の電子データを復元鍵データとして、利便性と安全性の高い電子データの暗号化を可能とする。
【解決手段】秘匿の対象とする電子データの入力を受け付ける手段１２０、分散暗号化した電子データを復元する際の鍵情報となる電子データの入力を受け付ける手段１３０、入力された秘匿データおよび復元鍵データを一定長以下の長さのブロックに分割する手段１４０、秘匿対象の電子データに対して、分散生成される暗号化データの内の１つが、前記復元鍵データとなるように、分散データを生成するための分散関数中の変数値を決定して分散関数を生成する手段１５０、秘匿対象の電子データに対して、前記分散関数により暗号化データを一つあるいは複数分散生成する手段１６０、暗号化データを単独あるいは複数あるいは組み合わせた上で一つあるいは複数出力する手段１７０を備える。
【選択図】図１




本発明の実施例におけるシステム構成例

【特許請求の範囲】
【請求項１】
秘匿の対象とする電子データを分散暗号化する電子データ暗号化装置であって、
秘匿の対象とする電子データの入力を一つあるいは複数受け付ける秘匿データ入力手段と、
分散暗号化した電子データを復元する際の鍵情報となる電子データの入力を一つあるいは複数受け付ける復元鍵データ入力手段と、
入力された秘匿データおよび復元鍵データを一定長以下の長さのブロックに分割する電子データ分割手段と、
秘匿対象の電子データに対して、分散生成される暗号化データの内の１つが、前記受け付けた復元鍵データとなるように、分散データを生成するための分散関数中の変数値を決定して分散関数を生成する分散関数生成手段と、
秘匿対象の電子データに対して、前記生成した分散関数により暗号化データを一つあるいは複数分散生成する分散データ生成手段と、
前記生成した暗号化データを単独あるいは複数あるいは組み合わせた上で一つあるいは複数出力する暗号化データ出力手段と、
を備える事を特徴とする電子データ暗号化装置。
【請求項２】
請求項１記載の電子データ暗号化装置であって、
分散情報を生成するための分散関数の個別性を決定付ける引数の入力を受け付ける引数設定手段を更に備え、分散関数生成手段は、秘匿対象の電子データに対して、分散生成される暗号化データの内の１つが、前記受け付けた復元鍵データとなるように、前記入力された引数を元に分散情報を生成するための分散関数中の変数値を決定して分散関数を生成する事を特徴とする電子データ暗号化装置。
【請求項３】
請求項１もしくは２に記載の電子データ暗号化装置により分散暗号化された秘匿対象の電子データを復元する電子データ復元装置であって、
復元の対象とする暗号化データの入力を一つあるいは複数受け付ける暗号化データ入力手段と、
分散暗号化した電子データを復元する際の鍵情報となる電子データの入力を一つあるいは複数受け付ける復元鍵データ入力手段と、
入力された秘匿データおよび復元鍵データを一定長以下の長さのブロックに分割する電子データ分割手段と、
暗号化データと復元鍵データを元に、所定の復元関数により秘匿対象の電子データを復元する秘匿データ復元手段と、
前記復元した秘匿対象の電子データを一つあるいは複数出力する秘匿データ出力手段と、を備える事を特徴とする電子データ復元装置。
【請求項４】
請求項３記載の電子データ復元装置であって、
分散情報を生成するための分散関数の個別性を決定付ける引数の入力を受け付ける引数設定手段を更に備え、秘匿データ復元手段は、暗号化データと復元鍵データと引数を元に、所定の復元関数により秘匿対象の電子データを復元する事を特徴とする電子データ復元装置。
【請求項５】
請求項１もしくは２に記載の電子データ暗号化装置における処理機能をコンピュータで実行させるためのプログラム。
【請求項６】
請求項３もしくは４に記載の電子データ復元装置における処理機能をコンピュータで実行させるためのプログラム。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、パスワードや鍵情報といった秘密情報や、テキスト、画像、音楽などの電子化されたデータを対象として分散暗号化し、幾つか以上の分散生成された電子データ片から元の電子データを復元可能とする秘密分散法を用いた分散暗号化技術に関する。
【背景技術】
【０００２】
従来、秘匿の対象とする電子データを暗号化する技術としては、例えばパスワードや暗証番号による暗号化、共通鍵や公開鍵・秘密鍵などの鍵暗号方式を用いた暗号化、などが一般に知られている。
【０００３】
前者は、所定のあるいは入力されたパスワードや暗証番号を使って、元の秘密データに対して和、積、論理的排他和などの演算処理を行う事で電子データの暗号化を実現するもので、復号化するためには暗号化時に用いられたパスワードや暗証番号を使って逆演算を行う必要があり、したがってパスワードや暗証番号を知らない場合は元の秘密データを復元する事ができず、電子データの秘匿が実現できる（例えば、特許文献１参照）。
【０００４】
後者は、共通鍵や公開鍵・秘密鍵と呼ばれる鍵情報を使って、元の秘密データに対して剰余演算などの演算処理を行う事で電子データの暗号化を実現するもので、復号化するためには同様に共通鍵や公開鍵・秘密鍵を使って演算処理を行う必要があり、共通鍵や公開鍵・秘密鍵を持たない限り元の秘密データを復元する事ができず、電子データの秘匿が実現できる（例えば、特許文献２参照）。
【０００５】
一方、秘匿の対象とする電子データを分散暗号化する技術として秘密分散法がある。秘密分散法は、分散関数と呼ばれる関数情報を使って元の秘密データから複数の異なる情報を生成する事で電子データの暗号化を実現するもので、復号化するためには生成した分散情報の全てあるいは一定数以上の情報を集めた上で行列演算などによる復元処理を行う必要があり、したがって必要な数に足りない分散情報からは元の秘密データを復元する事ができず、電子データの秘匿が実現できる（例えば、特許文献３参照）。
【０００６】
【特許文献１】特開平５－５３９９０号公報
【特許文献２】特開平５－１３００９９号公報
【特許文献３】特開平２００３－３４８０６５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
前述した鍵情報あるいはパスワードによる暗号化技術においては、鍵情報やパスワード等の暗号化のための情報を記憶する必要があり、人間の記憶可能な容量や期間の問題が存在する。特に、共通鍵や公開鍵・秘密鍵と呼ばれる鍵情報を使った暗号化技術においては、そもそも鍵情報は人間に記憶可能な大きさのものではない。これらの鍵情報やパスワード等の暗号化のための情報を何らかの記録装置に記録させた場合、該記録された情報が不正に入手される事によって秘匿した電子データが復元されるという問題が発生する。また、利用者にとってある程度記憶し易い、意味のあるような鍵情報やパスワードを設定した場合、該暗号化のための情報を推測される事によって秘匿した電子データが復元されるという問題が発生する。さらには、個々の鍵情報やパスワードに対して、総当りで可能性を試す事によって秘匿した電子データを復元する事も可能である。
【０００８】
また、前述した秘密分散法を使った暗号化においては、必要数より１個少ない分散情報の集合を保存し、残りの１個の分散情報を別個に保有する事で、該分散情報を秘密データを復元するための鍵情報あるいはパスワードと見なす事ができる。その場合、個々の分散

情報が十分に大きければ、総当りで正しい分散情報を得る可能性を試す事によって秘匿した電子データを復元する事は困難となる。しかしながら、秘密分散法により生成される分散情報はそもそも全くのランダムデータとなる事を目的としており、鍵情報あるいはパスワードによる暗号化技術と同様に、利用者が記憶できるようなものではない。

【０００９】

上記のように従来の電子データ暗号化技術は、記憶あるいは理解可能な復元の鍵となる情報を設定すると推測や総当りなどの手段により復元されてしまう恐れがあるという問題と、復元の鍵となる情報を利用者が記憶あるいは理解するのが困難であるという問題の、二つの相反する課題を有している。

【００１０】

本発明は、上記の課題に鑑みてなされたもので、電子データの暗号化において、画像データや音楽データといった利用者にとって記憶あるいは理解し易く、かつ推測や総当りなどの手法が困難であるような特定の固定データによって電子データを暗号化・復号化する事で、利便性と安全性の高い電子データの暗号化を可能とする電子データ暗号化装置、電子データ復元装置及びプログラムを実現することを目的とする。

【課題を解決するための手段】

【００１１】

本発明は、（ｋ，ｎ）閾値秘密分散法、（ｄ，ｋ，ｎ）閾値秘密分散法、あるいは、本出願人の既出願に係る特願２００３－３６６５３８号に記載の復元制御型秘密情報分散法などのいわゆる閾値秘密分散法を用いる。

【００１２】

（ｋ，ｎ）閾値秘密分散法は、分散情報を配布する数である２以上の整数の分散数ｎと、秘密情報Ｓの復元に必要な分散情報の最低数である２以上ｎ以下の整数の閾値ｋから、秘密情報Ｓを定数項とする（ｋ－１）次の多項式ｆ（ｘ）を、

$$f(x)=S+r_1x+\cdots r_{k-1}x^{k-1} \mod p \quad \cdots(1)$$

として作成し（ｒ１，…，ｒｋ－１：乱数、ｐ：素数）、元の秘密情報Ｓを所有あるいは預託により分配する秘密情報分配者は、分散情報を保管する各分散情報保持者ｉ（ｉ＝１，２，…，ｎ）に対して、分散情報Ｗｉ＝ｆ（ｉ）を分配するものである。

【００１３】

この（ｋ，ｎ）閾値秘密分散法は、ｎ個の分散情報の内、任意のｋ個の分散情報がそろえば、ｆ（ｘ）に関する連立方程式を解く事により元の秘密情報Ｓを復元できるが、任意の（ｋ－１）個までの分散情報がそろってもｆ（ｘ）に関する連立方程式を解く事はできないため、元の秘密情報Ｓは復元できないという特徴がある。したがって、（ｎ－ｋ）個までの分散情報が紛失や破壊により損なわれても元の秘密情報Ｓが復元可能であり、（ｋ－１）個までの分散情報が漏洩や盗難により得られても元の秘密情報Ｓは復元できないという、秘密情報を安全に保管する方法が実現できる。

【００１４】

（ｄ，ｋ，ｎ）閾値秘密分散法は、上記（ｋ，ｎ）閾値秘密分散法を拡張したもので、分散情報を配布する数である２以上の整数の分散数ｎと、秘密情報Ｓの完全な復元に必要な分散情報の最低数である２以上ｎ以下の整数の閾値ｋと、閾値ｋに対して秘密情報Ｓの部分的な復元を許容する分散情報の不足数を決定する２以上ｋ以下の整数の分割数ｄから、秘密情報Ｓを$S_0$，$S_1$，…，$S_{d-1}$に分割し、これらの分割した秘密情報（分割情報）を定数項とする（ｋ－１）次の多項式ｆ（ｘ）を、

$$f(x)=S_0+S_1x+\cdots S_{d-1}x^{d-1}r_1x^d+\cdots r_{k-d}x^{k-1} \mod P \quad \cdots(2)$$

として作成し（$r_1$，…，$r_{k-d}$：乱数、ｐ：素数）、元の秘密情報Ｓを所有あるいは預託により分配する秘密情報分配者は、分散情報を保管する各分散情報保持者ｉ（１＝１，２，…，ｎ）に対して、分散情報$W_i=f(i)$を分配するものである。

【００１５】

この（ｄ，ｋ，ｎ）閾値秘密分散法は、上記の（ｋ，ｎ）閾値秘密分散法と同様に、ｎ

個の分散情報の内、任意のｋ個の分散情報がそろえば、ｆ（ｘ）に関する連立方程式を解く事により元の秘密情報Ｓを復元できるが、任意の（ｋ－ｄ）個までの分散情報がそろってもｆ（ｘ）に関する連立方程式を解く事はできないため、元の秘密情報Ｓは復元できないという特徴がある。ただし、任意の（ｋ－ｄ＋１）個から（ｋ－１）個までの分散情報がそろった場合には、ｆ（ｘ）に関する連立方程式から分割情報$S_0$，$S_1$，…，$S_{d-1}$に関する関係式が求められるため、分割情報$S_0$，$S_1$，…，$S_{d-1}$として可能な値を得る事ができ、元の秘密情報Ｓを部分的に復元する事ができる。

【００１６】

なお、（ｋ，ｎ）閾値秘密分散法および（ｄ，ｋ，ｎ）閾値秘密分散法については、詳しくは、それぞれ「Ａ．Ｓｈａｍｉｒ，“Ｈｏｗ ｔｏ Ｓｈａｒｅ ａ Ｓｅｃｒｅｔ”，Ｃｏｍｍｕｎ．ｏｆ ＡＣＭ，Ｖｏｌ．２２，Ｎｏ．１１，ｐｐ．６１２－６１３，１９７９」および「Ｇ．Ｒ．Ｂｌａｋｌｅｙ，Ｃ．Ｍｅａｄｏｗｓ，“Ｓｅｃｕｒｉｔｙ ｏｆ ｒａｍｐ ｓｃｈｅｍｅｓ”，Ｐｒｏｃ．ｏｆ Ｃｒｙｐｔｏ’８４，Ｌｅｃｕｒｅ Ｎｏｔｅｓ ｏｎ Ｃｏｍｐｕｔ．Ｓｃｉ．，１９６，ｐｐ．２４２－２６８，１９８４」に述べられている。

【００１７】

復元制御型秘密情報分散法は、この（ｋ，ｎ）閾値秘密分散法および（ｄ，ｋ，ｎ）閾値秘密分散法を更に拡張した方法で、ｎ個の分散情報の内、任意のｋ個の分散情報がそろえば、ｆ（ｘ）に関する連立方程式を解く事により元の秘密情報Ｓを復元できるが、任意の（ｋ－ｄ）個までの分散情報がそろってもｆ（ｘ）に関する連立方程式を解く事はできないため、元の秘密情報Ｓは復元できないという特徴をもつ。ただし、情報を分散させる分散関数を特定の形式に規定する事により、任意の（ｋ－ｄ＋１）個から（ｋ－１）個までの分散情報が特定の組み合わせによりそろった場合にはｆ（ｘ）に関する連立方程式から特定の分割情報$S_0$，$S_1$，…，$S_{d-1}$を求める事ができ、元の秘密情報Ｓを部分的に復元する事ができる情報分散方法である。

【００１８】

この復元制御型秘密情報分散法は、基本的には、秘密情報Ｓについて、秘密情報Ｓの完全な復元に必要な分散情報の最低数である２以上の整数の閾値ｋ、閾値ｋに対して秘密情報Ｓの部分的な復元を許容する分散情報の不足数を決定する２以上ｋ以下の整数の分割数ｄと、秘密情報Ｓのｄ個の分割情報（分配情報）$S_0$，$S_1$，…，$S_{d-1}$などの秘密情報Ｓを分散するための条件を入力し、

最大の分割情報$S_t$（$0 \leqq t \leqq d-1$）よりも大きな素数ｐと、素数ｐよりも小さく０でない（ｋ－ｄ個）の乱数$r_i$（$1 \leqq 1 \leqq k-d$）と、（ｋ（ｋ－１）／２）個の乱数$a_j$（$1 \leqq j \leqq k(k-1)/2$）を生成して、

$$f(x)=S_0+S_1(x-a_1)+\cdots+S_{d-1}(x-a_{(d-1)(d-2)/2+1})(x-a_{(d-1)(d-2)/2+2})\cdots(x-a_{(d-1)(d-2)/2+d-1})+r_1(x-a_{d(d-1)/2+1})(x-a_{d(d-1)/2+2})\cdots(x-a_{d(d-1)/2+d})+\cdots+r_{k-d}(x-a_{(k-1)(k-2)/2+1})(x-a_{(k-1)(k-2)/2+2})\cdots(x-a_{(k-1)(k-2)/2+k-1}) \mod P \quad \cdots(3)$$

の式で表現される秘密情報Ｓの分散情報ｆ（ｘ）を生成するものである。

【００１９】

上記式（３）の分散関数ｆ（ｘ）は、例えばｋ＝３、ｄ＝２とした場合、

$$f(x)=S0+S1(x-a1)+r(X-a2)(x-a3) \mod P \quad \cdots(4)$$

で表現され、任意の２個の分散情報ＷｘとＷｘ＋ｂ（ｘ＞０、ｂ＞０）についての連立方程式は以下のような行列式で表現できる。

【００２０】

【数１】

$$\begin{bmatrix} 1 & x-a_1 & (x-a_2)(x-a_3) \\ 1 & x+b-a_1 & (x+b-a_2)(x+b-a_3) \end{bmatrix} \begin{bmatrix} S_0 \\ S_1 \\ r \end{bmatrix} = \begin{bmatrix} W_x \\ W_{x+b} \end{bmatrix} \quad \cdots (5)$$

上記行列式の左項を掃き出し法により変形すると、

【００２１】

【数２】

$$\begin{bmatrix} 1 & 0 & -x^2+(2a_1-b)x+a_1b-a_1a_2-a_1a_3+a_2a_3 \\ 0 & 1 & 2x+b-a_2-a_3 \end{bmatrix} \quad \cdots (6)$$

となり、$a_1$，$a_2$，$a_3$の値によっては$-x^2+(2a_1-b)+a_1b-a_1a_2-a_1a_3+a_2a_3=0$，もしくは$2x+b-a_2-a_3=0$を満たすｘとｂがある場合に、連立方程式から分割情報（部分情報）の$S_0$のみ、もしくは$S_1$のみを求めることができる。

【００２２】

本発明は、秘匿の対象とする電子データを分散暗号化する電子データ暗号化装置であって、秘匿の対象とする電子デー夕の入力を一つあるいは複数受け付ける秘匿データ入力手段と、分散暗号化した電子データを復元する際の鍵情報となる電子データの入力を一つあるいは複数受け付ける復元鍵データ入力手段と、入力された秘匿データおよび復元鍵データを一定長以下の長さのブロックに分割する電子データ分割手段と、上記復元制御型秘密情報分散法などを利用し、秘匿対象の電子データに対して、分散生成される暗号化データの内の１つが、前記受け付けた復元鍵データとなるように、分散データを生成するための分散関数中の変数値を決定して分散関数を生成する分散関数生成手段と、秘匿対象の電子データに対して、前記生成した分散関数により暗号化データを一つあるいは複数分散生成する分散データ生成手段と、前記生成した暗号化データを単独あるいは複数あるいは組み合わせた上で一つあるいは複数出力する暗号化データ出力手段とを備える事を特徴とする。

【００２３】

また、本発明の電子データ暗号化装置は、分散情報を生成するための分散関数の個別性を決定付ける引数の入力を受け付ける引数設定手段を更に備え、分散関数生成手段は、秘匿対象の電子データに対して、分散生成される暗号化データの内の１つが、前記受け付けた復元鍵データとなるように、前記入力された引数を元に分散情報を生成するための分散関数中の変数値を決定して分散関数を生成することを特徴とする。

【００２４】

また、本発明は、電子データ暗号化装置により分散暗号化された秘匿対象の電子データを復元する電子データ復元装置であって、復元の対象とする暗号化データの入力を一つあるいは複数受け付ける暗号化データ入力手段と、分散暗号化した電子データを復元する際の鍵情報となる電子データの入力を一つあるいは複数受け付ける復元鍵データ入力手段と、入力された秘匿データおよび復元鍵データを一定長以下の長さのブロックに分割する電子データ分割手段と、暗号化データと復元鍵データを元に、所定の復元関数により秘匿対象の電子データを復元する秘匿データ復元手段と、前記復元した秘匿対象の電子データを一つあるいは複数出力する秘匿データ出力手段と、を備える事を特徴とする。

【００２５】

また、本発明の電子データ復元装置は、分散情報を生成するための分散関数の個別性を

決定付ける引数の入力を受け付ける引数設定手段を更に備え、秘匿データ復元手段は、暗号化データと復元鍵データと引数を元に、所定の復元関数により秘匿対象の電子データを復元することを特徴とする。

【発明の効果】

【００２６】

本発明によれば、電子データ暗号化装置において、秘匿の対象とする電子データＳに対して、画像データや音楽データなどの任意の種類の電子データを復元鍵データとして、秘匿データＳを分散暗号化した後の分散データの少なくとも一つが固定の復元鍵データとなるように分散関数を決定する事で、該分散関数により分散暗号化した分散データに対して、電子データ復元装置において固定の復元鍵データを用いて元の秘匿データＳを復元する事が可能となる。これにより、電子データの暗号化において、画像データや音楽データといった利用者にとって記憶あるいは理解し易く、かつ推測や総当りなどが困難であるような特定の固定データによって電子データを暗号化・復号化することができ、利便性と安全性の高い電子データの暗号化を可能とする電子データ暗号化装置電子データ復元装置を実現できる。

【発明を実施するための最良の形態】

【００２７】

図１に、本発明における電子データ暗号化装置１００、電子データ復元装置２００による実施の形態のシステム構成例を示す。電子データ暗号化装置１００は、入力された秘匿対象とする電子データを、同じく入力された復元の鍵情報とする電子データに基づいて分散暗号化して暗号化データを生成し出力する。電子データ復元装置２００は、入力された暗号化データに対して、同じく入力された復元の鍵情報である電子データに基づいて秘匿対象の電子データを復元して出力する。電子データ暗号化装置１００と電子データ復元装置２００は、相互に接続されていても良いし、接続されていなくとも良い。また、図１のようにインターネットなどの通信回線３００を通じてネットワーク的に接続されていても良い。

【実施例】

【００２８】

以下、電子データ暗号化装置１００、電子データ復元装置２００の構成例及び動作例について詳述する。なお、動作例では特願２００３－３６６５３８に記載の復元制御型秘密情報分散法を用いるとする。

【００２９】

［電子データ暗号化］

図２に本発明の実施例における電子データ暗号化装置１００の機能構成図を示す。電子データ暗号化装置１００は、暗号化制御部１１０、秘匿データ入力部１２０、復元鍵データ入力部１３０、電子データ分割部１４０、分散関数生成部１５０、分散データ生成部１６０、暗号化データ出力部１７０、情報記憶部１８０から構成される。電子データ暗号化装置１００は暗号化制御部１１０の制御にしたがって動作する。

【００３０】

秘匿データ入力部１２０は、秘匿の対象とする電子データの入力を受け付ける。受け付けた電子データは、例えば情報記憶部１８０や内部メモリなどに一時的に記録するのが望ましい。本実施例では、秘匿対象の電子データとして６桁の文字列テキスト「秘密情報の例」が入力されたものとする。入力された文字列テキストは、例えばシフトＪＩＳコードにより符号化され、情報記憶部１８０などに格納される。ここでは、「秘密情報の例」が２４桁の１６進文字列「94E996A78FEE95F182CC97El」と符号化され、情報記憶部１８０などに格納されるとする。以下、入力された電子データを秘匿データＳとして記す。

【００３１】

なお、本発明は秘匿データ入力部１２０において入力を受け付ける電子データの種類や内容およびその数を特に規定するものではない。数値情報、文字列など符号化する事で分散関数による演算が可能であればどのような情報でも良く、また文字列テキストだけでな

く画像データや音楽データなどの任意の電子データ、あるいは予め暗号化された暗号化データを対象としても良い。さらに、入力された秘匿データを秘匿データ入力部１２０においてさらに暗号化する事で安全性を高める事も考えられる。また、本実施例は情報の入力の方法および形式を規定するものではない。キーボード入力やファイル入力の他に、インターネットなどの接続回線を介して他の装置から入力するようにしても構わない。

【００３２】

次に、復元鍵データ入力部１３０は、復元の鍵とする電子データの入力を受け付ける。受け付けた電子データは例えば情報記憶部１８０や内部メモリなどに一時的に記録するのが望ましい。本実施例では、復元鍵の電子データとして、図３に示すような、一列目が赤青青白、二列目が青赤白青、三列目が青白赤青、四列目が白青青赤である、単純な４×４ピクセルの画像が入力されたものとする。入力された復元鍵としての画像データは符号化されて、例えば情報記憶部１８０などに格納される。図３では各色に対応したデータが赤は「FF0000」、青は「0000FF」、白は「FFFFFF」であるため、９６桁の16進文字列

「FF00000000FF0000FFFFFFFF0000FFFF0000FFFFFF0000FF0000FFFFFFFFFF00000000FFFFFFFF0000FF0000FFFF0000」

と符号化され、情報記憶部１８０などに格納される。以下、入力された復元鍵データをＷＦと記す。

【００３３】

なお、本発明は復元鍵データ入力部１３０において入力を受け付ける電子データの種類や内容およびその数を特に規定するものではない。数値情報、文字列など符号化する事で分散関数による演算が可能であればどのような情報でも良く、ビットマップ画像などの画像データだけでなく音楽データや文字列テキスト、プログラムなどの任意の電子データを対象として良い。なお、これらの電子データにおけるヘッダと呼ばれる固定フォーマットのデータ部分は除去して、チャンクと呼ばれる残りのデータ部分のみを復元鍵データとして使用するようにしても良いし、本実施例のように入力された電子データ全てを復元鍵データとして使用しても良い。また、本実施例は復元鍵データの入力の方法および形式を規定するものではない。キーボード入力やファイル入力の他に、インターネットなどの接続回線を介して他の装置から入力するようにしても構わない。さらには、復元の鍵とする電子データを常に固定のものとして電子データ暗号化装置１００の内部に作り込むあるいは外部ファイルを読み込むようにして、復元鍵データ入力部１３０では入力を受け付けずに固定の復元鍵データを用いる、あるいは複数の復元鍵データの候補を提示して復元の鍵とする電子データを選択させるようにしても構わない。

【００３４】

次に、電子データ分割部１４０は、情報記憶部１８０または内部メモリなどに記録された秘匿データＳおよび復元鍵データＷＦを読み出し、一定長の電子データに分割してブロック化した上で、再度情報記憶部１８０または内部メモリなどに記録する。

【００３５】

本実施例では分割後のブロック化した電子データの長さを３バイトとする。秘匿データＳをブロック化した電子データは、分散暗号化の際に分散関数の一部として使用する素数である固定文字列Ｐよりも小さくなければならない。本実施例では固定文字列Ｐを３バイトの１６進文字列「FFFFFD」とする。したがって、３バイト単位で分割した後の電子データが固定文字列Ｐ以上の値をとる、「FFFFFD」、「FFFFFE」、「FFFFFF」がブロックとして存在する場合が考えられる。そのような場合には、例えば分割する際に冗長なブロックに置換するなどの方法がある。本実施例ではＰ＝FFFFFDであるため、ブロック化した電子データがＰより１少ないFFFFFCの場合には、「FFFFFC」、「FFFFFC」というように冗長なブロックを追加し、「FFFFFD」の場合には「FFFFFC」、「000001」のように、「FFFFFE」の場合には「FFFFFC」、「000002」のように、「FFFFFF」の場合には「FFFFFC」、「000003」のように冗長なブロックを追加して置換する事で、復元時の秘匿データが完全に元の秘匿データと同一になるようにブロック化する事ができる。なお、復元の鍵とする復元鍵データについては厳密性を持たせずに、「FFFFFD」、「FFFFFE」、「FFFFFF」を全て「FF

FFFC」に置換するようにしても良い。また、このようなブロック化した電子データの補完あるいは置換を行わずに、固定文字列Ｐをブロック化する電子データの長さよりも大きくする方法も考えられるが、その場合は分散データ生成部１６０において分散生成される暗号化データの大きさが元の秘匿データよりも大きくなる事になる。

【００３６】

本実施例における秘匿データは２４桁の１６進文字列「94E996A78FEE95F182CC97El」であり、３バイト単位にブロック化すると「94E996」，「A78FEE」，「95F182」，「CC97El」の４ブロックとなる。以下、秘匿データをブロック化した個々の電子データをＳｉ（１≦ｉ≦４）と記す。また、本実施例における復元鍵データに対しては簡単化のために固定文字列Ｐ＝FFFFFD以上のブロック化した電子データは全て「FFFFFC」に置換するものとすると、９６桁の１６進文字列

「FF00000000FF0000FFFFFFFF0000FFFF0000FFFFFF0000FF0000FFFFFFFFFF00000000FFFFFFFF0000FF0000FFFF0000」

であり、これを３バイト単位でブロック化して置換を行うと「FF0000」，「0000FF」，「0000FF」，「FFFFFC」，「0000FF」，「FF0000」，「FFFFFC」，「0000FF」，「0000FF」，「FFFFFC」，「FF0000」，「0000FF」，「FFFFFC」，「0000FF」，「0000FF」，「FF0000」の１６ブロックとなる。以下、復元鍵データをブロック化した個々の電子データをＷＦｊ（１≦ｊ≦１６）と記述する。

【００３７】

なお、本実施例は電子データ分割部１４０における電子データをブロック化するための分割方法を特に規定するものではない。本実施例では３バイト単位で単純に分割したが、後から正しく元の電子データに復元できれば良く、例えば２バイト単位で分割した上にエラー訂正符号やハッシュ値などを付与して３バイトとしてデータの復元誤りや改ざん検出機能を持たせたりするなどの分割方法が考えられる。さらに、復元鍵データの単一性を保証するために、例えば復元鍵データの全体のハッシュ値を算出した上で、個々のブロックに足し合わせるような方法も考えられる。これにより、個々のブロックが類似した復元鍵データを用いる場合でも、厳密に復元鍵データの区別をつけて暗号化できるようになる。

【００３８】

次に、分散関数生成部１５０は、分割した個々の秘匿データＳｉおよび復元鍵データＷＦｊを元に、秘匿データを分散暗号化するための分散関数と呼ばれる特殊な関数ｆ（ｘ）において必要な変数を決定し、分散関数ｆ（ｘ）を生成する。まず、本実施例における分散関数ｆ（ｘ）の基本形を、先の式（４）を用いて次の式（５）で表現するものとする。

【００３９】

$$f(x) = S + RA(x - a1) + RB(x - a2)(x - a3) \pmod{P} \quad \cdots (7)$$

この式（７）におけるＳは秘匿の対象とする電子データ、ｘは電子データを分散暗号化して分散データＷＸを生成するための情報番号ａｌ，ａ２，ａ３は分散関数ｆ（ｘ）を個別化するために必要な変数引数、ＲＡ、ＲＢは乱数文字列、Ｐは素数である固定文字列を表わす。

【００４０】

本実施例においては、前述したように固定文字列Ｐとして素数である３バイトの１６進文字列Ｐ＝FFFFFDを用いる。なお、素数である固定文字列Ｐのサイズおよび値に関しては、本実施例で特に規定するものではない。分散暗号化する電子データの想定されるブロック単位やまた総当り攻撃に対するセキュリティ強度などの観点から任意に決定して良く、また個別の電子データ暗号化装置によって異なるようにしても良い。

【００４１】

また、本実施例では個別化のための変数引数ａｌ，ａ２，ａ３として、それぞれａｌ＝７，ａ２＝１，ａ３＝５を用いるものとする。したがって、本実施例における分散関数ｆ（ｘ）の具体的な式は次のようになる。

【００４２】

ｆ（ｘ）＝Ｓ＋ＲＡ（ｘ－７）＋ＲＢ（ｘ－１）（ｘ－５）　（ｍｏｄ　Ｐ）…（８）

この式（８）の分散関数ｆ（ｘ）は、ｘに２を代入して算出したｆ（２）をＷ２、ｘに３を代入して算出したｆ（３）をＷ３、ｘに４を代入して算出したｆ（４）をＷ４とした時に、Ｗ３とＷ４からＳが、Ｗ２とＷ４からＲＡが、Ｗ２とＷ３とＷ４または任意の３つのＷｘからＳ、ＲＡ、ＲＢがそれぞれ復元可能となるような秘密情報Ｓの分散関数である。また、Ｗ２、Ｗ３、Ｗ４を始めとする個々の分散データＷｘからは元となる秘密情報Ｓおよび乱数ＲＡ、ＲＢが全く分からないため、秘密情報Ｓの安全な秘匿が実現できる。このような特殊な分散関数ｆ（ｘ）は、先に出願した特願２００３－３６６５３８に記載の復元制御聖秘密情報分散法により求める事ができ、本実施例に記載の式に制限されない。分散関数ｆ（ｘ）の次数と変数引数の数を増やしたり、また秘密情報Ｓを例えば前半分と後半分のように分割して複数の秘密情報Ｓｌと Ｓ２とした上でＳの代わりにＳｌ、ＲＡの代わりにＳ２を用いたり、分散関数ｆ（ｘ）における秘密情報Ｓの位置と乱数ＲＡ、ＲＢの位置を入れ替えたりといった様々な分散関数ｆ（ｘ）を考える事ができる。また、分散関数ｆ（ｘ）として従来の秘密分散法で用いられる分散関数を用いるようにしても良い。

【００４３】

なお、変数引数ａｌ，ａ２，ａ３により個別化された分散関数ｆ（ｘ）および固定文字列Ｐについては、電子データ暗号化装置１００だけでなく、電子データ復元装置２００においても共通に使用する必要がある。これらの情報を各装置間で共有する手段については本発明で規定するものではないが、例えばこれらの情報を記憶したＩＣ力一ドなどの記録媒体を共通に使用したり、また各装置に固有の秘密鍵情報などによって分散暗号化したこれらの情報を送信したりなどの手段が考えられる。また、これらの情報を常に固定の情報として、各装置内の固定メモリなどに作り込んでしまっても構わない。

【００４４】

電子データ暗号化装置や後述の電子データ復元装置がこれらの変数引数ａｌ，ａ２，ａ３の入力を受け付け、設定する手段（引数設定手段）を持つ事により、分散関数ｆ（ｘ）の動作の個別化を実現することが可能である。

【００４５】

以下に、分散関数生成部１５０の動作について詳細を説明する。分散関数生成部１５０は、ブロック化した個々の秘匿データＳｉに対して、前記ブロック化した復元鍵データＷＦｊを用いて、乱数文字列ＲＡｉおよびＲＢｉを算出する。乱数ＲＡｉおよびＲＢｉは固定文字列Ｐより小さく秘匿データＳｉと同程度のサイズの乱数文字列である事が望ましい。ここで、式（８）に示した本実施例における分散関数ｆ（ｘ）がｘ＝３を代入したＷ３とｘ＝４を代入したＷ４から元の秘匿データＳを復元可能とするものである事から、ｘ＝４を代入したＷ４が復元鍵データと一致するように乱数ＲＡおよびＲＢを決定する事により、復元鍵データＷＦ＝Ｗ４により秘匿データＳが復元可能となるようにＷ３を暗号化データとして分散生成する事ができる。式（８）の本実施例における分散関数ｆ（ｘ）を、復元鍵データをＷＦとして、ＲＢに着目して変形すると以下のようになる。

【００４６】

【数３】

$$RB = \frac{WF - S - RA(x - a1)}{(x - a2)(x - a3)} \pmod{P} \qquad \cdots (9)$$

本実施例においては、ａｌ＝７，ａ２＝１，ａ３＝５であり、かつＷＦ＝Ｗ４である事からｘ＝４である。したがって個々のブロック化した秘匿データＳｉに対して、乱数ＲＡｉ、ＲＢｉおよび復元鍵データＷＦｊの関係を式にすると以下のようになる。

【００４７】

【数４】

$$RBi = \frac{WFj - Si + 3RAi}{-3} \pmod{P} \qquad \cdots (10)$$

乱数ＲＡｉは秘匿データの各ブロックＳｉ毎に全くの乱数として生成し、よってブロック毎に異なるものとする。乱数ＲＢｉは式（１０）にしたがって、ＲＡｉを生成した後にＳｉ、ＷＦｊ、ＲＡｉを代入して算出する。例えば１ブロック目としてＳｌ＝94E996、ＷＦｌ＝FF0000であり、乱数ＲＡｉとしてＲＡｌ＝1A2B3Cを得たとすると、式（１０）よりＲＢｌ＝C277F3となる。以下、秘匿データの各ブロックＳｌに対して、順次ＲＡうおよびＲＢｌを算出して情報記憶部１８０または内部メモリなどに記録する。本実施例においては、乱数によりＲＡ２＝2A3B4C、ＲＡ３＝3B4C5D、ＲＡ４＝4C5D6Eと得たとして、式（１０）により、ＲＢ２＝61F357、ＲＢ３＝A05821、ＲＢ４＝4C2986が得られる。

【００４８】

図４に電子データ暗号化装置１００での処理例をまとめて示す。図４の４列目が、上記実施例における乱数ＲＢｉの計算例である。

【００４９】

なお、本実施例ではＳｌに対してＷＦｌを対応付けて算出を行ったが、Ｓ１に対してＷＦｌｌのようにｉとｊの対応関係を変えて算出を行うようにしても良い。また、各ブロックＳｉ毎にＲＡｉを乱数として生成したが、ＲＡｉとして固定の値を使っても良く、また後で生成する暗号化データＷＯ＝ｆ（３）がうまくランダム性を持つようにＲＡｉを生成しても良い。本発明は、これらの各変数の決定方法を特に規定するものではなく、生成される分散関数ｆ（ｘ）がある固定のｘの値の下で復元鍵データＷＦを算出するように各変数が決定されれば良い。

【００５０】

次に、分散データ生成部１６０は、分散関数生成部１５０において生成した秘匿データＳｉ、および乱数文字列ＲＡｉ、ＲＢｉからなる分散関数ｆ（ｘ）を使って、ｘ＝３を代入した暗号化データＷＯｉ＝ｆ（３）を算出する。本実施例においては、例えば１ブロック目としてＳｌ＝94E996、ＲＡｌ＝1A2B3C、ＲＢｌ＝C277F3であり、式（８）の分散関数ｆ（ｘ）に情報番号ｘとして３を代入して暗号化データＷＯｉを算出すると、以下のようにＷＯｉ＝225CDlが得られる。

【００５１】

ＷＯ＝ｆ（３）＝94E996＋1A2B3C×(3-7)＋C277F3×(3-1)×(3-5)
＝225CDl（mod FFFFFD）

ちなみに、式（８）の分散関数ｆ（ｘ）にｘ＝４を代入して分散データＷ４ｉを算出すると、

Ｗ４＝ｆ（４）＝94E996＋1A2Ｂ3C×(4-7)＋C277F3×(4-1)×(4-5)
＝FF0000（mod FFFFFD）

のようにＷ４ｉ＝FF0000が得られ、ＷＦｌと一致する。すなわち、式（８）の分散関数ｆ（ｘ）は固定値ｘ＝４の下で復元鍵データＷＦを算出するような分散関数ｆ（ｘ）である。また、本分散関数ｆ（ｘ）は前述したようにＷ３＝ｆ（３）とＷ４＝ｆ（４）から秘匿データＳを復元可能とするような復元制御型秘密分散法の分散関数である。したがって、本分散関数ｆ（ｘ）により生成した暗号化データＷＯ＝Ｗ３＝ｆ（３）は、固定の復元鍵データＷＦ＝Ｗ４＝ｆ（４）から秘匿データＳを復元できるような暗号化データとなる。

【００５２】

以下、分散データ生成部１６０では、同様にして秘匿データＳｉの各ブロックに対してＷＯｉを算出し、情報記憶部１８０または内部メモリなどにＷＯｉを記録する。本実施例においては、Ｗ０２＝72D158、Ｗ０３＝235B7D、ＷＯ４＝667807が計算により得られる。図４の５列目が、本実施例における分散データ生成部１６０の計算例を示す。図４の最下

列は分散データＷ４ｉの計算例を示したものである。

【００５３】

なお、個々のブロックに対して暗号化データＷＯｉを算出した後は、情報の漏洩を紡ぐために、秘匿データＳｉ、復元鍵データＷＦｊ、乱数ＲＡｉ、ＲＢｉなどの各値を情報記憶部１８０や内部メモリなどから破棄する事が望ましい。

【００５４】

なお、本実施例では秘匿データＳｉが４ブロック、復元鍵データＷＦｊが１６ブロックであり、復元鍵データＷＦよりも秘匿データＳの方が短かったが、秘匿データＳの方が長くても構わない。その場合は復元鍵データＷＦを分割したブロックＷＦｊを繰り返し使用する事で、暗号化データＷＯｉを作成する事ができる。また、本実施例では暗号化データＷＯｉの長さは秘匿データＳｉと同様に４ブロックとしたが、秘匿データＳの長さが暗号化データＷＯからは分からないようにダミーのデータを追加するようにしても良い。例えば、ｉ＝５からｉ＝８までの４ブロックについて、Ｓｉ＝000000という空データを追加して乱数ＲＡｉ、ＲＢｉを算出し、ＷＯｉを計算する事で、生成する暗号化データの長さを秘匿データの長さと異なるようにできる。さらに、復元後の秘匿データの正当性を検証するために、一定の特徴を持つダミーの検証用データを追加するようにしても良い。これにより復元後の秘匿データが正しいものかどうかを電子データ復元装置が検証できるようになる。

【００５５】

次に、暗号化データ出力部１７０は、情報記憶部１８０または内部メモリなどに記録された暗号化データＷＯｉをまとめ、暗号化データＷＯとして出力する。本実施例においては、図４の５列目の暗号データＷＯ１～ＷＯ４をまとめて、出力される暗号化データは「225CD172D158235B7D667807」となる。暗号化データを出力した後は、暗号化データの漏洩を防ぐために情報記憶部１８０や内部メモリなどから出力した暗号化データを破棄する事が望ましい。

【００５６】

なお、本実施例は、暗号化データ出力部１７０における暗号化データの出力の方法やフロトコル、フォーマットを特に規定するものではない。本実施例では単なる１６進文字列の状態で出力するものとしたが、例えばビットマップ画像のようなヘッダ部分を付与した特定のフォーマットを持つデータとして出力しても良い。これにより暗号化データは通常のビットマップ画像と同様に参照する事ができるようになる。

【００５７】

また、暗号化データを画面や記録媒体などに直接出力したり、ファイル出力したりする他に、ネットワーク出力として、例えば電子データ復元装置２００に通信回線３００を介して送信するようにしても良い。出力する際に暗号化データをさらに暗号化したり、出力先の電子データ復元装置２００との問で認証を行うなどして、通信回線３００における盗聴に対する安全性を高める事も考えられる。

【００５８】

［電子データ復元］

図５に本発明の実施例における電子データ復元装置２００の機能構成図を示す。電子データ復元装置２００は、復元制御部２１０、暗号化データ入力部２２０、復元鍵データ入力部２３０、電子データ分割部２４０、秘匿データ復元部２５０、復元データ出力部２６０、情報記憶部２７０から構成される。電子データ復元装置２００は復元制御部２１０の制御にしたがって動作する。

【００５９】

暗号化データ入力部２２０は、復元の対象とする暗号化データの入力を受け付ける。受け付けた暗号化データは例えば情報記憶部２７０や内部メモリなどに一時的に記録するのが望ましい。本実施例では暗号化データとして、前述の電子データ復元装置１００により秘匿データとして入力された文字列テキスト「秘密情報の例」から生成された暗号化データＷＯ＝225CD172D158235B7D667807が入力されたものとする。以下、入力された暗号化デ

ータをＷＩと記す。

【００６０】

なお、本発明は暗号化データ入力部２２０において入力を受け付ける暗号化データの種類や内容およびその数を特に規定するものではない。数値情報、文字列など符号化する事で分散関数による演算が可能であればどのような情報でも良く、また文字列テキストだけでなく画像データや音楽データなどの任意の電子データ、あるいは予めさらに暗号化された暗号化データを対象として良い。その場合に、入力された暗号化データを暗号化データ入力部２２０において復号化する事で入力の安全性を高める事も考えられる。また、本実施例は情報の入力の方法および形式を規定するものではない。キーボード入力やファイル入力の他に、インターネットなどの接続回線を介して他の装置から入力するようにしても構わない。

【００６１】

次に、復元鍵データ入力部２３０は、復元の鍵とする電子データの入力を受け付ける。受け付けた電子データは例えば情報記憶部２７０や内部メモリなどに一時的に記録するのが望ましい。復元鍵データは前述の電子データ暗号化装置１００で入力された復元鍵データと同じものであり、本実施例では、図３に示すような、一列目が赤青青白、二列目が青赤白青、三列目が青白赤青、四列目が白青青赤である、単純な４×４ピクセルの画像が入力されたものとする。入力された画像データは、符号化されて情報記憶部２７０などに格納される。本実施例では、各色に対応したデータが赤は「FF0000」、青は「0000FF」、白は「FFFFFF」であるため、９６桁の16進文字列

「FF00000000FF0000FFFFFFFF0000FFFF0000FFFFFF0000FF0000FFFFFFFFFF00000000FFFFFFFF0000FF0000FFFF0000」

となる。以下、入力された復元鍵データをＷＦと記す。

【００６２】

なお、本発明は復元鍵データ入力部２３０において入力を受け付ける電子データの種類や内容およびその数を特に規定するものではない。数値情報、文字列など符号化する事で分散関数による演算が可能であればどのような情報でも良く、ビットマップ画像などの画像データだけでなく音楽データや文字列テキスト、プログラムなどの任意の電子データを対象として良い。なお、これらの電子データにおけるヘッダと呼ばれる固定フォーマットのデータ部分は除去して、チャンクと呼ばれる残りのデータ部分のみを復元鍵データとして使用するようにしても良いし、本実施例のように入力された電子データ全てを復元鍵データとして使用しても良い。ただし、電子データ暗号化装置１００と復元鍵として使用する個所を合わせる必要がある。また、本実施例は復元鍵データの入力の方法および形式を規定するものではない。キーボード入力やファイル入力の他に、インターネットなどの接続回線を介して他の装置から入力するようにしても構わない。さらには、復元の鍵とする電子データを常に固定のものとして電子データ復元装置２００の内部に作り込むあるいは外部ファイルを読み込むようにして、復元鍵データ入力部２３０では入力を受け付けずに固定の電子データを用いる、あるいは複数の電子データの候補を提示して復元の鍵とする電子データを選択させるようにしても構わない。

【００６３】

電子データ分割部２４０は、情報記憶部２７０または内部メモリなどに記録された暗号化データＷＩおよび復元鍵データＷＦを読み出し、一定長の電子データに分割してブロック化した上で、再度情報記憶部２７０または内部メモリなどに記録する。本実施例では素数である固定文字列Ｐが３バイトの１６進文字列FFFFFDである事から、分割後のブロック化した電子データの長さを３バイトと固定する。なお、電子データを３バイト単位で分割した場合、暗号化データは常に固定文字列Ｐより小さい値をとるが、復元鍵データは固定文字列Ｐ以上の値として「FFFFFD」、「FFFFFE」、「FFFFFF」をとる場合が考えられる。そのような場合には、電子データ暗号化装置と同様に冗長なブロックを追加あるいは置換するなどして、情報の損失を補う事ができる。

【００６４】

本実施例における暗号化データは「225CD172D158235B7D667807」であり、３バイト単位にブロック化すると「225CD1」，「72D158」，「235B7D」，「667807」の４ブロックとなる。以下、暗号化データをブロック化した個々の電子データをＷＩｉ（１≦ｉ≦４）と記述する。また、本実施例における復元鍵データは、電子データ暗号化装置１００と同様に簡単化のために固定文字列Ｐ＝FFFFFD以上のブロック化した電子データは全てFFFFFCに置換するものとして、「FF0000」，「0000FF」，「0000FF」，「FFFFFC」，「0000FF」，「FF0000」，「FFFFFC」，「0000FF」，「0000FF」，「FFFFFC」，「FF0000」，「0000FF」，「FFFFFC」，「0000FF」，「0000FF」，「FF0000」の１６ブロックとなる。以下、復元鍵データをブロック化した個々の電子データをＷＦｊ（１≦ｊ≦１６）と記述する。

【００６５】

なお、本実施例は電子データ分割部２４０における電子データをブロック化するための分割方法を特に規定するものではない。本実施例では３バイト単位で単純に分割したが、例えば２バイト単位で分割した上にエラー訂正符号やハッシュ値などを付与して３バイトとしてデータの復元誤りや改ざん検出機能を持たせたりするなどの分割方法が考えられる。さらに、復元鍵データの単一性を保証するために、例えば復元鍵データの全体のハッシュ値を算出した上で、個々のブロックに足し合わせるような方法も考えられる。これにより、個々のブロックが類似した復元鍵データに対して厳密に区別をつけて復元できるようになる。

【００６６】

次に、秘匿データ復元部２５０において、暗号化データＷＩと復元鍵データＷＦから、秘匿データＳを復元する。秘匿データ復元部２５０は、分割した暗号化データＷＩｉおよび復元鍵データＷＦｊの各ブロック毎に演算を行う事で秘匿データのブロックＳｉを算出する。先の式（８）と同じく、本実施例における分散関数ｆ（ｘ）が

ｆ（ｘ）＝Ｓ＋ＲＡ（ｘ－７）＋ＲＢ（ｘ－1）（ｘ－5）（mod　Ｐ）　…（11）

である事から、２個の分散情報に関する連立方程式は次のような行列式で表現できる。

【００６７】

【数５】

$$\begin{bmatrix} 1 & x-7 & (x-1)(x-5) \\ 1 & y-7 & (y-1)(y-5) \end{bmatrix} \begin{bmatrix} S \\ RA \\ RB \end{bmatrix} = \begin{bmatrix} Wx \\ Wy \end{bmatrix} \quad \cdots (12)$$

式（１１）の分散関数ｆ（ｘ）は、前述したように暗号化データＷＯ＝ｆ（３）と復元鍵データＷＦ＝ｆ（４）から秘匿データＳを復元可能とするような復元制御型秘密分散法の分散関数であるため、上記行列式において、Ｗｘは暗号化データＷＩとしてｘ＝３を代入し、Ｗｙは復元鍵データＷＦとしてｘ＝４を代入して、次のように、行列式を掃き出し法などにより解いてＳを求める事で、秘匿データＳを復元する事ができる。

【００６８】

【数６】

$$\begin{bmatrix}1 & -4 & -4\\ 1 & -3 & -3\end{bmatrix}\begin{bmatrix}S\\ RA\\ RB\end{bmatrix}=\begin{bmatrix}WI\\ WF\end{bmatrix} \Rightarrow \begin{bmatrix}1 & -4 & -4\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}S\\ RA\\ RB\end{bmatrix}=\begin{bmatrix}WI\\ WF-WI\end{bmatrix}$$

$$\Rightarrow \begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}S\\ RA\\ RB\end{bmatrix}=\begin{bmatrix}WI+4(WF-WI)\\ WF-WI\end{bmatrix}=\begin{bmatrix}4WF-3WI\\ WF-WI\end{bmatrix} \quad \cdots (13)$$

上記の演算の結果、Ｓｌは行列式からＳｉ＝４ＷＦｊ－３ＷＩｉにより求める事ができる。本実施例においては、秘匿データの１ブロック目のＳ１は、ＷＩｌ＝225CDl、ＷＦｌ＝FF0000より、Ｓｌ＝94E996を得る。秘匿データ復元部２５０は、Ｓｌを情報記憶部２７０あるいは内部メモリなどに記録する。以下、入力された暗号化データの各ブロックＷＩｉについても同様の計算を行い、ＷＩ２＝72D158、ＷＩ３＝235B7D、ＷＩ４＝667807に対して、それぞれＳ２＝A78FEE、Ｓ３＝95F182、Ｓ４＝CC97Elを計算結果として得る。本実施例における秘匿データ復元部２５０の計算例を図６に示す。

【００６９】

なお、本実施例においては個別のブロック毎にＳｌの式を求めるように記述しているが、Ｓｌを求める式は全てのブロックに対して同一である事から、全てのブロックに対する処理を始める前に計算式を求めた上で、順次個々のＷＩｉおよびＷＦｊを代入してＳｉを求めるようにしても良い。

【００７０】

次に、復元データ出力部２６０は、情報記憶部２７０または内部メモリなどに記録された秘匿データＳｉをまとめ、復元された秘匿データＳとして出力する。本実施例においては、図６の３行目の秘匿データＳ１～Ｓ４をまとめて、出力される秘匿データは「94E996A78FEE95F182CC97El」となる。秘匿データを出力した後は、秘匿データの漏洩を防ぐために情報記憶部２７０や内部メモリなどから出力した秘匿データを破棄する事が望ましい。

【００７１】

電子データ暗号化装置１００において、秘匿データのブロック化時に冗長化処理を行っている場合には、復元データ出力部２６０において縮退処理を行う必要がある。本実施例では固定文字列Ｐが「FFFFFD」であるため、算出したブロックがＰより１少ない「FFFFFC」の場合には、次のブロックの値により縮退処理を行って出力する。例えば「FFFFFC」、「FFFFFC」と続いた場合は「FFFFFC」を、「FFFFFC」、「000001」の場合には「FFFFFD」を、「FFFFFC」、「000002」の場合には「FFFFFE」を、「FFFFFC」、「000003」の場合には「FFFFFF」を出力するようにすれば、復元時の秘匿データは完全に元の秘匿データと同一になる。

【００７２】

また、電子データ暗号化装置１００において、秘匿データＳに対してグミーのデータが追加されている場合には、ダミーのデータを除去して出力する事が望ましい。また、一定の特徴を持つダミーの検証用データが追加されている場合には、復元後の秘匿データＳが検証用データを含まない場合には復元後の秘匿データの正当性が検証できないものとして復元処理を中止、あるいはエラーメッセージを表示するなどして、復元処理の正当性を検証するようにもできる。

【００７３】

なお、本実施例は、復元データ出力部２６０における秘匿データの出力の方法やフロトコル、フォーマットを特に規定するものではない。本実施例では単なる１６進文字列の状態で出力するものとしたが、例えばシフトＪＩＳコードにより逆符号化した文字列を出力

するようにしても良い。本実施例における秘匿データＳの出力文字列は「秘密情報の例」となり、これは電子データ暗号化装置１００において秘匿の対象とされた秘匿データＳと同値である。また、暗号化データを画面や記録媒体などに直接出力したり、ファイル出力したりする他に、ネットワークを介して他の装置に出力するなどの方法が考えられる。

【００７４】

以上のように、本実施例においては、電子データ暗号化装置１００において入力された１つの秘匿データと１つの復元鍵データを元にして１つの暗号化データを生成し、電子データ復元装置２００において入力された１つの暗号化データと１つの復元鍵データを元にして１つの秘匿データを復元したが、本発明は処理の対象とする各電子データの個数や組み合わせをただ１つに限るものではない。例えば１つの秘匿データと２つの復元鍵データを元にして１つの暗号化データを生成し、該暗号化データと２つの復元鍵データから元の秘匿データを復元するようにしたり、２つの秘匿データと２つの復元鍵データを元にして１つの暗号化データを生成し、該暗号化データとどちらか一方の復元鍵データからどちらか一方の秘匿データを復元するようにしたりする事も可能である。

【００７５】

なお、図１及び図５で示した装置における各部の一部もしくは全部の処理機能をコンピュータのプログラムで構成し、そのプログラムをコンピュータを用いて実行して本発明を実現することができること、あるいは、その処理手順をコンピュータのプログラムで構成し、そのプログラムをコンピュータに実行させることができることは言うまでもない。また、コンピュータでその処理機能を実現するためのプログラム、あるいは、コンピュータにその処理手順を実行させるためのプログラムを、そのコンピュータが読み取り可能な記録媒体、例えば、ＦＤ、ＭＯ、ＲＯＭ、メモリカード、ＣＤ、ＤＶＤ、リムーバブルディスクなどに記録して、保存したり、提供したりすることができるとともに、インターネット等のネットワークを通してそのプログラムを配布したりすることが可能である。

【図面の簡単な説明】

【００７６】

【図１】本発明の一実施の形態としてのシステム構成例を示す図である。

【図２】本発明の電子データ暗号化装置の一実施例の機能構成図である。

【図３】復元鍵データとその１６進表現の一例を示す図である。

【図４】本発明の電子データ暗号化装置における暗号化データの計算例である。

【図５】本発明の電子データ復元装置の一実施例の機能構成図である。

【図６】本発明の電子データ復元装置における秘匿データの計算例である。

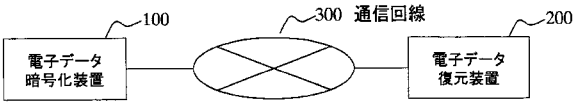
【符号の説明】

【００７７】

１００　電子データ暗号化装置
１１０　暗号化制御部
１２０　秘匿データ入力部
１３０　復元鍵データ入力部
１４０　電子データ分割部
１５０　分散関数生成部
１６０　分散データ生成部
１７０　暗号化データ出力部
１８０　情報記憶部
２００　電子データ復元装置
２１０　復元制御部
２２０　復元化データ入力部
２３０　復元鍵データ入力部
２４０　電子データ分割部
２５０　秘匿データ復元部
２６０　復元データ出力部

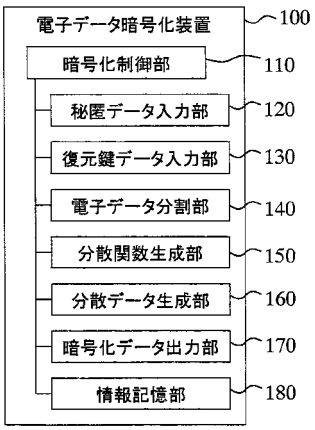
２７０　情報記憶部
３００　通信回線

【図１】



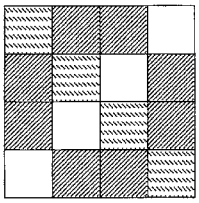

本発明の実施例におけるシステム構成例

【図２】




電子データ暗号化装置の機能構成図

【図３】



凡例 ▨ : 赤
▨ : 青
□ : 白

| | | | |
|---|---|---|---|
| FF0000 | 0000FF | 0000FF | FFFFFF |
| 0000FF | FF0000 | FFFFFF | 0000FF |
| 0000FF | FFFFFF | FF0000 | 0000FF |
| FFFFFF | 0000FF | 0000FF | FF0000 |

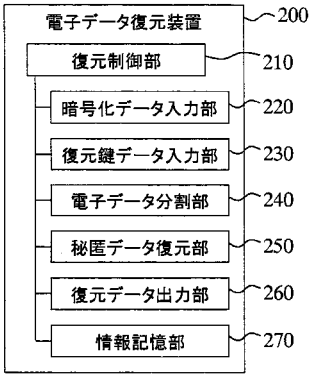
復元鍵データとその 16 進表現の例

【図４】

| 項目 | 計算式 | i＝1 | i＝2 | i＝3 | i＝4 |
|---|---|---|---|---|---|
| 秘匿データ Ｓｉ | ―――― | 94E996 | A78FEE | 95F182 | CC97E1 |
| 復元鍵データ ＷＦｊ | ―――― | FF0000 | 0000FF | 0000FF | FFFFFC |
| 乱数文字列 ＲＡｉ | ―――― | 1A2B3C | 2B3C4D | 3C4D5E | 4D5E6F |
| 乱数文字列 ＲＢｉ | $RBi=\frac{WFj-Si+3RAi}{-3} \pmod P$ | C277F3 | 61F357 | A05821 | 4C2986 |
| 暗号化データ ＷＯｉ | f(3)=Si-4RAi-4RBi (mod P) | 225CD1 | 72D158 | 235B7D | 667807 |
| 分散情報 Ｗ４ｉ | f(4)=Si-3RAi-3RBi (mod P) | FF0000 | 0000FF | 0000FF | FFFFCC |

暗号化データの計算例

【図５】




電子データ復元装置の機能構成図

【図６】

| 計算項目 | 計算式 | i＝1 | i＝2 | i＝3 | i＝4 |
|---|---|---|---|---|---|
| 暗号化データ ＷＩｉ | ―――― | 225CD1 | 72D158 | 235B7D | 667807 |
| 復元鍵データ ＷＦｊ | ―――― | FF0000 | 0000FF | 0000FF | FFFFFC |
| 秘匿データ Ｓｉ | Si=4WFj-3Si (mod P) | 94E996 | A78FEE | 95F182 | CC97E1 |

秘匿データの計算例

フロントページの続き

(72)発明者　北原　亮
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　山本　隆二
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　萬本　正信
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考) 5J104 AA16　EA04　EA15　EA18　JA03　NA02　NA37　PA14