(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5221357号
(P5221357)
(45)発行日　平成25年6月26日(2013.6.26)　(24)登録日　平成25年3月15日(2013.3.15)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
H04L 9/00 601E

請求項の数 16　(全 11 頁)

(21)出願番号　特願2008-536076(P2008-536076)
(86)(22)出願日　平成18年10月12日(2006.10.12)
(65)公表番号　特表2009-513049(P2009-513049A)
(43)公表日　平成21年3月26日(2009.3.26)
(86)国際出願番号　PCT/FR2006/002303
(87)国際公開番号　WO2007/045746
(87)国際公開日　平成19年4月26日(2007.4.26)
審査請求日　平成21年9月10日(2009.9.10)
(31)優先権主張番号　0510787
(32)優先日　平成17年10月21日(2005.10.21)
(33)優先権主張国　フランス(FR)

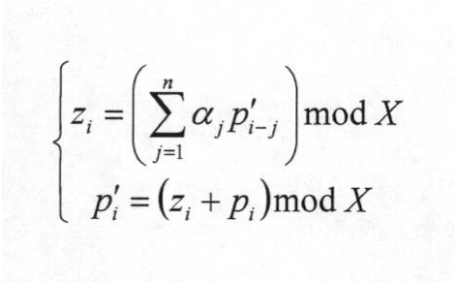
(73)特許権者　500174661
サントル・ナショナル・ドゥ・ラ・レシェルシュ・サイエンティフィーク－セ・エン・エール・エス－
フランス・Ｆ－７５７９４・パリ・セデックス・１６・リュ・ミシェル－アンジュ・３
(73)特許権者　307028839
ユニヴェルシテ・ドゥ・モンペリエ・ドゥ
フランス・Ｆ－３４０９５・モンペリエ・セデックス・５・プラス・ウージェーヌ・バタイヨン・（番地なし）・スィヤンス・ゼ・テクニック・デュ・ラングドック
(74)代理人　100064908
弁理士　志賀　正武

最終頁に続く

(54)【発明の名称】セキュアなデータ転送のための方法

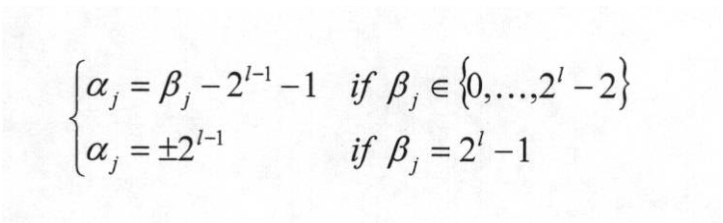
(57)【特許請求の範囲】
【請求項１】
（ａ）プロセッサにより、グローバル暗号化鍵を初期決定する段階と、
（ｂ）プロセッサにより、断片化可能ファイルを前記グローバル暗号化鍵の関数として暗号化して、第１の暗号化されたファイルを形成する段階と、
（ｃ）プロセッサにより、グローバル暗号化鍵を非対称暗号化アルゴリズムによって暗号化して、暗号化されたグローバル暗号化鍵を得る段階と、
（ｄ）プロセッサにより、暗号化されたグローバル暗号化鍵を表す値を前記暗号化されたファイルのフラグメントの間に挿入して、第２の暗号化されたファイルを形成する段階と、
（ｅ）転送手段により、前記第２の暗号化されたファイルを転送する段階と
を有する、複数のフラグメントに断片化可能なファイルのセキュアな転送方法であって、
前記（ｂ）段階は、連続したフラグメントに対して、
（ｂ１）プロセッサにより、各カレントフラグメントへ、以前に暗号化されたフラグメントのグループに関する組合せに基づいて決定されたダイナミック暗号化鍵を割り当てる段階と、
（ｂ２）プロセッサにより、カレントフラグメントの値へ、その初期値及び前記ダイナミック暗号化鍵によって決まる値を割り当てる段階と
を有することを特徴とする方法。

【請求項２】
前記（ｄ）段階において、断片化可能ファイルの署名を表す値が、さらに挿入されることを特徴とする請求項１に記載の方法。
【請求項３】
前記（ｂ１）段階において、線形結合が、以前に暗号化されたフラグメントの値に適用されることを特徴とする請求項１又は請求項２に記載の方法。
【請求項４】
線形結合が次式で表されることを特徴とする請求項３に記載の方法。
【数１】



$$\begin{cases} z_i = \left(\sum_{j=1}^{n} \alpha_j p'_{i-j} \right) \bmod X \\ p'_i = (z_i + p_i) \bmod X \end{cases}$$

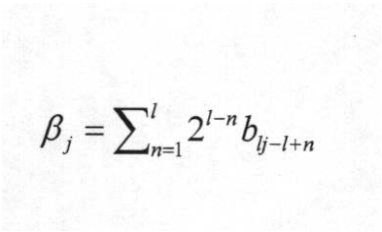
ここで、
ｚ$_{i}$は、値ｐ$_{i}$のカレントフラグメントに割り当てられたダイナミック暗号化鍵の値であり、
α$_{j}$は、カレントフラグメントに適用された線形結合を実行するための係数一式であり、
ｐ’$_{i-j}$は、ｎ個の以前に暗号化されたフラグメントの値一式であり、
ｐ’$_{i}$は、暗号化されたカレントフラグメントの値であり、
ｍｏｄ　Ｘは、前記フラグメントのサンプリングに固有の合同式に対応する。
このとき、
ｊは、１からｎの間の値をとり、
ｉ－ｊは、ｉ－ｎからｉ－１の間の値をとる。
【請求項５】
前記線形結合が、グローバル暗号化鍵の関数として表される係数（α$_{j}$）に関係することを特徴とする請求項４に記載の方法。
【請求項６】
前記線形結合が、その合計の絶対値が最小である係数に関係することを特徴とする請求項３から請求項５のうちのいずれか１項に記載の方法。
【請求項７】
グローバル暗号化鍵が、連続した第１数の値を有し、
線形結合が、以前に暗号化されたフラグメントの第２数に関係し、
第１数は、第２数の倍数であることを特徴とする請求項３から請求項６のうちのいずれか１項に記載の方法。
【請求項８】
係数α$_{j}$が次式で表されることを特徴とする請求項６と組み合わされた請求項７に記載の方法。
【数２】



$$\begin{cases} \alpha_j = \beta_j - 2^{l-1} - 1 & if\ \beta_j \in \{0,\ldots,2^l - 2\} \\ \alpha_j = \pm 2^{l-1} & if\ \beta_j = 2^l - 1 \end{cases}$$

このとき、β$_{j}$を以下のようにおく。

【数３】



ここで、ｂ ｌ ｊ － ｌ ＋ ｎは、グローバル暗号化鍵の１個の連続した値である。

【請求項９】

第１数が、第２数の２倍（ｎ＝ｋ／２）であることを特徴とする請求項７又は請求項８に記載の方法。

【請求項１０】

グローバル暗号化鍵の前記連続した値が、暗号化されたフラグメントの同じ大きさの各ブロックへ挿入されることを特徴とする請求項１から請求項９のうちのいずれか１項に記載の方法。

【請求項１１】

前記ファイルが、サンプルから成り、

各フラグメントが、サンプル又はサンプルのブロックであることを特徴とする請求項１から請求項１０のうちのいずれか１項に記載の方法。

【請求項１２】

サンプルが、画素又はボクセル画素若しくはテンポラル画素であることを特徴とする請求項１１に記載の方法。

【請求項１３】

（ａ’）受信手段により、暗号化されたファイルを受信する段階と、

（ｂ’）プロセッサにより、暗号化されたグローバル暗号化鍵を表す値を前記暗号化されたファイルのフラグメントの間から抽出する段階と、

（ｃ’）プロセッサにより、暗号化されたグローバル暗号化鍵を公開鍵を用いて復号して、復号されたグローバル暗号化鍵を得る段階と、

（ｄ’）プロセッサにより、暗号化された断片化可能ファイルを前記復号されたグローバル暗号化鍵の関数として復号する段階と

を有する、複数のフラグメントに断片化可能な暗号化されたファイルのセキュアな受信方法であって、

前記段階（ｂ’）において、各カレントフラグメントに固有のダイナミック暗号化鍵が、以前に暗号化されたフラグメントのグループに関する組合せに基づいて決定されることを特徴とする方法。

【請求項１４】

復号されたファイルが、暗号化されたグローバル暗号化鍵と共に挿入された署名を用いて検証されることを特徴とする請求項１３に記載の方法。

【請求項１５】

（ａ）プロセッサにより、グローバル暗号化鍵を初期決定する手順と、

（ｂ）プロセッサにより、断片化可能ファイルを前記グローバル暗号化鍵の関数として暗号化して、第１の暗号化されたファイルを形成する手順と、

（ｃ）プロセッサにより、グローバル暗号化鍵を非対称暗号化アルゴリズムによって暗号化して、暗号化されたグローバル暗号化鍵を得る手順と、

（ｄ）プロセッサにより、暗号化されたグローバル暗号化鍵を表す値を前記暗号化されたファイルのフラグメントの間に挿入して、第２の暗号化されたファイルを形成する手順と、

（ｅ）転送手段により、前記第２の暗号化されたファイルを転送する手順と

を実行するように構成された暗号化システムを具備した送受信システムであって、

前記（ｂ）手順は、連続したフラグメントに対して、

（ｂ１）プロセッサにより、各カレントフラグメントへ、以前に暗号化されたフラグメントのグループに関する組合せに基づいて決定されたダイナミック暗号化鍵を割り当てる手順と、
（ｂ２）プロセッサにより、カレントフラグメントの値へ、該カレントフラグメントの初期値及び前記ダイナミック暗号化鍵によって決まる値を割り当てる手順と
を有することを特徴とする送受信システム。
【請求項１６】
コンピュータに、
（ａ）プロセッサにより、グローバル暗号化鍵を初期決定する手順と、
（ｂ）プロセッサにより、断片化可能ファイルを前記グローバル暗号化鍵の関数として暗号化して、第１の暗号化されたファイルを形成する手順と、
（ｃ）プロセッサにより、グローバル暗号化鍵を非対称暗号化アルゴリズムによって暗号化して、暗号化されたグローバル暗号化鍵を得る手順と、
（ｄ）プロセッサにより、暗号化されたグローバル暗号化鍵を表す値を前記暗号化されたファイルのフラグメントの間に挿入して、第２の暗号化されたファイルを形成する手順と、
（ｅ）転送手段により、前記第２の暗号化されたファイルを転送する手順と
を実行させるための、複数のフラグメントに断片化可能なファイルのセキュアな転送のためのコンピュータプログラムであって、
前記（ｂ）手順は、連続したフラグメントに対して、
（ｂ１）プロセッサにより、各カレントフラグメントへ、以前に暗号化されたフラグメントのグループに関する組合せに基づいて決定されたダイナミック暗号化鍵を割り当てる手順と、
（ｂ２）プロセッサにより、カレントフラグメントの値へ、該カレントフラグメントの初期値及び前記ダイナミック暗号化鍵によって決まる値を割り当てる手順と
を有することを特徴とするコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、セキュアなデータ転送のための方法と、この種の方法を実行するデバイスとに関し、特に、サイズの大きい断片化可能なデータファイルの転送に適する。
【背景技術】
【０００２】
画像のようなサイズの大きいファイルをセキュアな方法で転送するために、対称暗号化システムを使用することができる。しかしながら、このタイプの暗号化は、転送されるファイルの復号及び暗号化に用いられる秘密鍵の送信を必要とする。その結果、このようなセキュアなデータを転送する方法は、データファイルの復号を可能にする鍵を横取り（interception）されるリスクを負う。さらに、受信者は送信者が使用した鍵を知ることとなる。従ってこれは、使用する秘密鍵の定期的な、本当に規則的な変更を余儀なくさせる。
【０００３】
さらに、送信者によって各ファイルフラグメントを暗号化するためのプライベート鍵と、このフラグメントを復号するために受信者へ転送される公開鍵とを実装する非対称暗号化システムは非常に扱いづらい。特に、受信者の部分的な鍵の知識のせいで、非対称システムは、桁数の大きい素数、具体的には、（特に、ＲＳＡアルゴリズムにおいて、）各ファイルフラグメントを暗号化するためには、１０２４ビットを越えるサイズの素数の使用を必要とする。その結果、このような暗号化された転送方法の実行に要するリソース及び時間は膨大となる。
【特許文献１】国際公開第２００４／０１２３７８号パンフレット
【発明の開示】
【発明が解決しようとする課題】

【０００４】
本発明の目的は、これらの欠点を緩和することにある。
【０００５】
本発明は、サイズの大きなデータの送信を可能にするセキュアなデータ転送方法、特に、画像の高速かつ効率的な転送方法を提案する。
【０００６】
さらに、本発明の目的は、ノイズ又はデータ損失に強いセキュアなデータ転送方法、特に、データパケットの不正な横取りによるノイズ又はデータ損失に強いセキュアなデータ転送方法を提供することにある。
【課題を解決するための手段】
【０００７】
この目的のために、本発明は、以下のような、複数のフラグメントに断片化可能なファイルのセキュアな転送方法を提案する。
（ａ）グローバル暗号化鍵を初期決定する。
（ｂ）断片化可能ファイルを上記グローバル鍵の関数として暗号化して、第１の暗号化されたファイルを形成する。
（ｃ）グローバル鍵を非対称暗号化アルゴリズムによって暗号化して、暗号化されたグローバル鍵を得る。
（ｄ）暗号化されたグローバル鍵を表す値を上記暗号化されたファイルのフラグメントの間に挿入して、第２の暗号化されたファイルを形成する。
（ｅ）上記第２の暗号化されたファイルを転送する。
【０００８】
このように、転送されるファイルへ暗号化された方法でグローバル鍵を挿入することによって、受信者は、非対称アルゴリズムの公開鍵によってグローバル鍵を有利に復号できる。グローバル鍵のサイズが減少することで、このグローバル鍵の暗号化は容易に成し遂げられる。従って、ファイルの暗号化は、実行しづらさの少ない暗号化アルゴリズムを使用でき、暗号化された後、ファイルへ挿入されるこのグローバル鍵を使用する。それによって、暗号化／復号時間を短縮する。
【０００９】
ほぼ同様な一連のステップが、特許文献１から読み取れる。しかしながら、本発明は、さらに踏み込んで、以下に従う著しく有利な特徴を提案する。ステップ（ｂ）において、連続したフラグメントに対し、
（ｂ１）各カレントフラグメントへ、以前に暗号化されたフラグメントのグループに関する組合せに基づいて決定されたダイナミック暗号化鍵を割り当てる。
（ｂ２）カレントフラグメントの値へ、その初期値及び上記ダイナミック鍵によって決まる値を割り当てる。
【００１０】
このタイプの暗号化は、断片化可能ファイルのデータの高速な暗号化を可能とし、それによって、全ての完全性問題を解決できるようになる。特に、データパケットが失われた場合に、暗号化されたファイル全体が改変されることとなる。さらに、このタイプの暗号化によって、受信の際、暗号化されたファイルの全体を受信する前に、復号を開始できるようになる。従って、このタイプの暗号化は、インターネットなどのネットワークを介した大容量ファイルの転送に特に適している。
【００１１】
本発明の一実施態様において、暗号化されたグローバル鍵を表す値に加えて、断片化可能ファイルの署名を表す値が、暗号化されたファイルに挿入される。この署名によって、受信時、転送された画像が正しく復号されているかを検証できるように、特に、この画像の完全性を検証できるようになる。特に、転送中のデータの横取りは、復号されたイメージがイメージへ挿入された署名にもはや対応しない、といったシフトを引き起こす。
【００１２】

また、有利な実施態様において、以前に暗号化されたフラグメントの値の線形結合が、グローバル鍵によって決まる係数α_jの実行に用いられる。係数α_jは次式で表される。

【００１３】

【数１】

$$\begin{cases} \alpha_j = \beta_j - 2^{l-1} - 1 & if\ \beta_j \in \{0,\ldots,2^l - 2\} \\ \alpha_j = \pm 2^{l-1} & if\ \beta_j = 2^l - 1 \end{cases}$$

【００１４】

このとき、β_jを以下のようにおく。

【００１５】

【数２】

$$\beta_j = \sum_{n=1}^{l} 2^{l-n} b_{lj-l+n}$$

【００１６】

ここで、b_{lj-l+n}は、グローバル鍵のｌ個の連続した値である。

【００１７】

この関係式によって、これらの係数の合計がゼロに極めて近くなるようにα_jを選択できるようになる。故に、ファイルへのデータの挿入が実行されるのと同様に、ノイズ（予測のつかない変化（vagaries））もまた挿入される。それらの合計がゼロにほぼ等しくなるようにα_jを選択することによって、復号フェーズの間にノイズを減らすことができるようになる。従って、α_jは、各値の見かけの確率密度がほぼ均一となるように選択される。

【００１８】

その後、本発明は、以下のような、複数のフラグメントに断片化可能な暗号化されたファイルのセキュアな受信方法を提案する。

（ａ’）暗号化されたファイルを受信する。

（ｂ’）暗号化されたグローバル鍵を表す値を上記暗号化されたファイルのフラグメントの間から抽出する。

（ｃ’）暗号化されたグローバル鍵を公開鍵を用いて復号して、復号されたグローバル鍵を得る。

（ｄ’）暗号化された断片化可能ファイルを上記復号されたグローバル鍵の関数として復号する。

【００１９】

本発明の有利な一般的な特徴に従って、受信時、具体的には、ステップ（ｂ’）において、各カレントフラグメントに固有のダイナミック暗号化鍵が、以前に暗号化されたフラグメントのグループに関する組合せに基づいて決定される。

【００２０】

さらに、本発明は、本発明による断片化可能なファイルのセキュアな転送方法を実行する送受信システムを提案する。

【００２１】

さらにまた、本発明は、コンピュータへのインストールによって、本発明によるセキュアな転送方法及び／又は本発明による受信方法の実行を可能にするコンピュータプログラム製品を提案する。

【発明を実施するための最良の形態】

【００２２】

本発明のその他の特徴及び利点が、添付の図面の参照と共に、限定を意図しない例示的な実施形態の以下の記載から明らかとなる。

【００２３】
図１は、例えばインターネットなどのコンピュータベースのネットワーク２にリンクされた第１端末１を表す。第１端末１は、ネットワーク２を介して第２端末３へデータを転送するように構成されている。
【００２４】
例えば画像のようなサイズの大きいデータファイルをコンピュータベースのネットワーク２を介して安全に転送するために、本発明は、図２の例によって具体的に示された方法を提案する。ステップＳ１０１において、かつ本発明による方法に従って、グローバル暗号化鍵K_{glob}が決定される。この鍵は、例えばＴ個のワードに分割されたｋビットの形を成す。
【００２５】
ここで、Ｔ＝ｋ／ｌであり、ｌはそれぞれのポイントの長さである。
【００２６】
このグローバル鍵は、以下に記載したフローに基づく暗号化を実行するために使用できる。しかしながら、このグローバル鍵は、対称ブロック暗号化アルゴリズム又はその他のいかなるタイプの暗号化アルゴリズムのための秘密鍵になれる。
【００２７】
この鍵は、暗号化と暗号化されたファイルの転送とを実行する暗号化システムに格納できるとともに、暗号化鍵生成部によって生成されることもできる。
【００２８】
ステップＳ１０２において、暗号化されたファイルと共に転送されてもよい画像の署名Ｓを算出することが可能である。特に、この署名によって、転送に起因するパケットの横取り又は欠損が無いかを検査するために、受信時のファイルの完全性を検証することができるようになる。その結果、この署名Ｓによって、画像のセキュリティを高めることができるようになる。特に、例えば、医療用撮影検査室と、そこで得られた画像を分析しなければならない医師との間といった、医療用画像の転送用途の枠組みの中では、転送された画像にデータの追加又は改変がなされていないことの保証は重要である。署名によって、受信した画像と、転送した画像との比較を行なうことができるようになる。
【００２９】
その後、本方法は、フローに基づく暗号化アルゴリズム、特に、示された例にあるようなネットワークを介したファイル転送に適した暗号化アルゴリズムを実行できる。特に、このタイプの暗号化によると、ファイルが完全に受信される前であっても、暗号化されたデータの復号を開始することができるようになる。しかしながら、例えば、秘密鍵ブロック暗号化などの別の暗号化方法が使用でき、この場合、秘密鍵がグローバル鍵K_{glob}となる。とはいえ、フローに基づく暗号化アルゴリズムは、ブロックアルゴリズムに対するさまざまな長所を有する。まず第１に、フローに基づくアルゴリズムは、ブロックアルゴリズムと対照的に、ノイズの影響を受けにくい。従って、画像の完全性が向上する。さらに、フローに基づくアルゴリズムは、暗号化前の画像が一様な区域を示す場合であっても、模様つき（textured）の区域を出現させない。ステップＳ１０３に従って、暗号化されるファイルのフラグメント毎に、例えば、画像の画素又は画素のグループp_i毎に、ダイナミック鍵K_{dyn}が、フローに基づく暗号化アルゴリズムの枠組みの中で算出される。このフローに基づく暗号化は、同期式または非同期式と呼ぶことができる。同期式のフローに基づく暗号化の場合、ダイナミック鍵K_{dyn}は、暗号化されるデータ又は暗号化されたデータに依存しない。逆に、非同期式暗号化の場合、ダイナミック鍵は、以前に暗号化された画素の関数として規定される。例えば、このダイナミック鍵は、さまざまな鍵生成関数によって、及び本発明の好適な実施形態にあるように、以下の式で示されるような線形結合によって得ることができる。
【００３０】

【数３】

$$\begin{cases} z_i = \left(\sum_{j=1}^{n} \alpha_j p'_{i-j} \right) \bmod X \\ p'_i = (z_i + p_i) \bmod X \end{cases}$$

【００３１】

ここで、ｚ$_{i}$は、値ｐ$_{i}$のカレント画素又はフラグメントに割り当てられたダイナミック鍵の値であり、ｉは、１からｎの間で変化する。ここで、ｎは、ピクセル又はフラグメントの数である。

α$_{j}$は、カレント画素又はフラグメントに適用される線形結合を実行するための係数一式であり、このとき、ｊは、１からｎの間の値をとる。

ｐ’$_{i-j}$は、ｎ個の以前に暗号化された画素の値一式であり、このとき、ｉ－ｊは、ｉ－ｎからｉ－１の間の値をとる。

ｐ’$_{i}$は、暗号化されたカレント画素の値である。

ｍｏｄ　Ｘは、上記フラグメントのサンプリングに固有の合同式に対応する。

【００３２】

この実施例において、Ｘは、カレント画素の暗号化された値の計算に割り当てられたメモリのサイズによって決まる。通常、Ｘは２５６ポイントである。従って、ステップＳ１０４において、各画素ｐ$_{i}$はピクセルｐ’$_{i}$へ暗号化される。さらに、線形結合の係数α$_{j}$が、グローバル鍵Ｋ$_{glob}$に基づいて得られる。例示的な実施形態が、以下の式によって示される。

【００３３】

【数４】

$$\begin{cases} \alpha_j = \beta_j - 2^{l-1} - 1 & if\ \beta_j \in \{0, \ldots, 2^l - 2\} \\ \alpha_j = \pm 2^{l-1} & if\ \beta_j = 2^l - 1 \end{cases}$$

【００３４】

このとき、β$_{j}$を以下のようにおく。

【００３５】

【数５】

$$\beta_j = \sum_{n=1}^{l} 2^{l-n} b_{lj-l+n}$$

【００３６】

ここで、ｂ$_{lj-l+n}$は、グローバル鍵のｌ個の連続した値である。

【００３７】

この場合、グローバル鍵Ｋ$_{glob}$は、ｌビットの長さのｎ個のワードから形成され、各ビットは、ｂ$_{j}$と示される。このような式を用いることによって、係数α$_{j}$を変更すること、具体的には、全てのα$_{j}$の合計がほぼゼロとなるように変更することが可能となる。特に、これによって、本発明による暗号化アルゴリズムからノイズの影響を減らすことができるようになる。

【００３８】

ファイル全体が暗号化されたとき、グローバル鍵Ｋ$_{glob}$は、例えば、公開鍵及びプライベート鍵を用いる非対称暗号化アルゴリズムによって、入れ替わりに暗号化される。グローバル鍵はそれほど大きなサイズのファイルではないので、この場合には、上記の暗号化アルゴリズムを使用することが可能である。

【００３９】
ステップＳ１０５で暗号化が行なわれると、その後、暗号化されたグローバル鍵Ｋ’$_{glob}$は、暗号化されたファイルへ挿入される（Ｓ１０６）。また、署名は、この同じステップの最中で暗号化できる。データの挿入は、挿入されるメッセージ長及び所望の強度の関数として、さまざまな方法で行なうことができる。画像へのデータファイルの挿入に対して、２つの主要な手順グループがある。それは、空間領域での処理手順及び周波数領域での処理手順であり、特に、ＤＣＴ（Discrete Cosine Transform, 離散コサイン変換）が用いられる。また、空間領域及び周波数領域の組合せも可能である。データを画像の画素に直接埋め込む組合せを用いることが可能であり、具体的には、例えば、擬似乱数生成系を用いることによって、挿入の影響を受ける一連の画素を選択することが可能である。しかしながら、本発明に好ましい手順では、情報を画像の下位ビットに埋め込むアルゴリズムを使用する。その目的は、暗号化された秘密鍵と元画像の署名とから成るｎビットのメッセージを画像に埋め込むためである。ついで、メッセージを画像のいたるところに分散させるように、挿入因子を算出する必要がある。この分散によって、データの挿入に起因するノイズを減らすことができるようになり、かつ画像の視覚的完全性を画像全体まで拡張することもできるようになる。従って、画像は、等しいサイズのｎ個の部位へ分割され、これらの部位のそれぞれは、メッセージの１ビットを埋め込むために用いられる。挿入のためのアルゴリズムの反復は、隠されたデータの挿入によるこれらの部位のサイズに少なくとも等しくなっている。

【００４０】
全データがファイルに挿入されると、ステップＳ１０７において、このように暗号化されたファイルは、例えば、図１の第２端末３などの受信者へ送信される。

【００４１】
その後、受信者は、図３に示された逆復号方法を用いて画像を復号できる。すなわち、Ｓ２０１段で受信した画像から、署名S_{EMM}と同様に暗号化されたグローバル鍵を抽出し始める（Ｓ２０２）。次に、ユーザは、公開鍵によってこのグローバル鍵を復号できる（Ｓ２０３）。公開鍵は、例えば、あらかじめ送信者によってユーザへ送信されている。ステップＳ２０４及びＳ２０５において、ユーザは、使用された暗号化アルゴリズムに類似した手法で復号されたこのグローバル鍵によって画像全体を復号する。最後に、ステップＳ２０６において、復号された受信画像の署名S_{MEC}が算出され、ついで、ステップＳ２０７において、画像の完全性を検証し、かつ転送されたデータが転送中に攻撃を受けているかどうかを判断するために、元画像の署名S_{EMM}が受信された画像の署名S_{REC}と比較される。

【００４２】
当然ながら、本発明は、例示を目的とした上記の実施形態に限定されず、その他の変形が加えられる。

【００４３】
故に、有利な実現化に従って、さらに、暗号化過程でのデータファイルの圧縮が可能である。

【図面の簡単な説明】

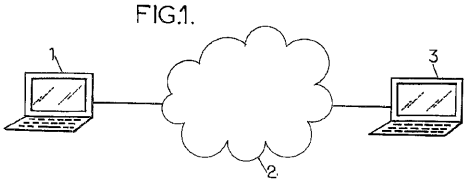
【００４４】
【図１】本発明の方法が実行されるネットワークを示す図である。
【図２】本発明によるセキュアな転送方法を表したフローチャートである。
【図３】本発明による受信方法を表したフローチャートである。

【符号の説明】

【００４５】
１　第１端末
２　ネットワーク
３　第２端末

【図１】

FIG.1.



【図２】

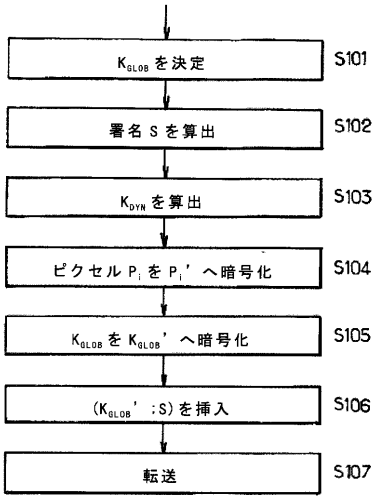


FIG.2.

【図３】

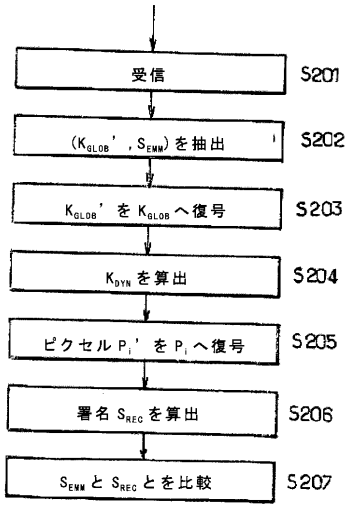


FIG.3.

フロントページの続き

(74)代理人 100089037
弁理士 渡邊 隆
(74)代理人 100108453
弁理士 村山 靖彦
(74)代理人 100110364
弁理士 実広 信哉
(72)発明者 ウィリアム・ピュエッシュ
フランス・Ｆ－３００００・ニーム・アンパス・ヴァランダ・１４
(72)発明者 ジョゼ・マルコーニ・ロドリゲス
フランス・Ｆ－８４０００・アヴィニョン・ブールヴァール・ポール・フローレ・１８

審査官 青木 重徳

(56)参考文献 特開２００２－１１１６５２（ＪＰ，Ａ）
特開２０００－２２４１５８（ＪＰ，Ａ）
特開２００４－０５３９６９（ＪＰ，Ａ）
特開２００５－２１７５９８（ＪＰ，Ａ）
特開２００２－０４４１３５（ＪＰ，Ａ）
特開２０００－２５２９７４（ＪＰ，Ａ）
特開平１１－０２７２４０（ＪＰ，Ａ）
特開平０９－２００１９５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／０８