(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2010-532880
(P2010-532880A)
(43)公表日　平成22年10月14日(2010.10.14)

(51)Int.Cl.		F I			テーマコード（参考）
G09C 1/00	(2006.01)	G09C	1/00	610A	5B017
G06F 21/24	(2006.01)	G06F	12/14	540A	5B065
G06F 12/00	(2006.01)	G06F	12/00	537H	5B082
G06F 3/06	(2006.01)	G09C	1/00	660D	5J104
		G06F	3/06	304H	

審査請求 未請求　予備審査請求 未請求　（全 21 頁）　最終頁に続く

(21)出願番号　特願2010-515265 (P2010-515265)
(86)(22)出願日　平成20年7月2日 (2008.7.2)
(85)翻訳文提出日　平成22年1月26日 (2010.1.26)
(86)国際出願番号　PCT/US2008/069096
(87)国際公開番号　WO2009/009400
(87)国際公開日　平成21年1月15日 (2009.1.15)
(31)優先権主張番号　11/774,521
(32)優先日　平成19年7月6日 (2007.7.6)
(33)優先権主張国　米国 (US)

(71)出願人　509306177
エヌサイファー・コーポレーション・リミテッド
イギリス・ＣＢ１・２ＪＤ・ケンブリッジ・ステーション・ロード・（番地なし）・ジュピター・ハウス
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100110364
弁理士　実広　信哉

最終頁に続く

(54)【発明の名称】データセキュリティのためにデータを処理するシステム及び方法

(57)【要約】
データセキュリティのためにデータを処理するためのシステム及び方法に関する。データファイルを暗号化する方法は、入力長によって特徴付けられる入力ファイルを提供するステップと、第１出力ファイルと第２出力ファイルとを含む多数のデータファイルを提供するステップとを含む。第１出力は第１出力長によって特徴付けられる。第１出力長は入力長と多数の出力ファイルとに関連付けられる。第１出力ファイルは、ヘッダセクションとデータセクションとを含む。ヘッダセッションは、数に関連付けられた情報を含む。加えて、方法は、入力ファイルの第１ロケーションと第２ロケーションとを決定するステップを含む。第２ロケーションは、既知の長さだけ第１ロケーションの後ろである。

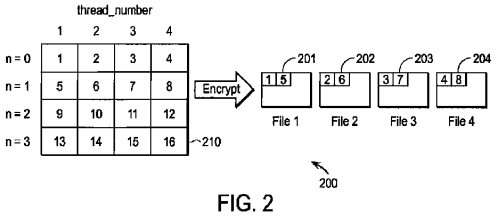

FIG. 2

【特許請求の範囲】
【請求項１】
データファイルを暗号化するための方法であって、
前記方法は、
入力ファイルを提供するステップであって、前記入力ファイルは、入力長によって特徴付けられるステップと、
多数の出力ファイルを提供するステップであって、前記出力ファイルは、第１出力ファイルと第２出力ファイルとを含み、前記第１出力ファイルは、第１出力長によって特徴付けられ、前記第１出力長は、前記入力長と、前記多数の出力ファイルとに関連付けられ、前記第１出力ファイルは、ヘッダセクションとデータセクションとを含み、前記ヘッダセクションは、前記数に関連付けられた情報を含むステップと、
前記入力ファイルの第１ロケーションと第２ロケーションとを決定するステップであって、前記第２ロケーションは、既知の長さで前記第１ロケーションからオフセットされるステップと、
前記既知の長さのために、第１スレッドによって、前記第１ロケーションで、前記入力ファイルを読み取るステップから、第１セグメントを得るステップと、
第２スレッドによって、前記第２ロケーションで、前記入力ファイルを読み取るステップから、第２データセグメントを得るステップと、
前記第１データセグメントを暗号化するステップと、
前記第１出力ファイルの前記データセクションで、前記暗号化された第１データセグメントを格納するステップと
を具備することを特徴とする方法。
【請求項２】
前記第１出力ファイルの前記データセクションの終わりに、パディングセクションを設けるステップをさらに具備することを特徴とする請求項１に記載の方法。
【請求項３】
前記第１出力ファイルはパディングセクションを含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記第２データセグメントを暗号化するステップと、
前記第２出力ファイルで、前記暗号化された第２データセグメントを格納するステップと
をさらに具備することを特徴とする請求項１に記載の方法。
【請求項５】
前記多数の出力ファイルは、ユーザ入力によって決定されることを特徴とする請求項１に記載の方法。
【請求項６】
前記多数の出力ファイルは、多数の利用可能なプロセッサに関連付けられることを特徴とする請求項１に記載の方法。
【請求項７】
前記多数の出力ファイルは、多数の使用に適したスレッドに関連付けられることを特徴とする請求項１に記載の方法。
【請求項８】
前記多数の出力ファイルは、多数の利用可能なストレージデバイスに関連付けられることを特徴とする請求項１に記載の方法。
【請求項９】
前記入力ファイルは、第１ストレージデバイス内に格納され、かつ、
前記第１出力ファイルは、第２ストレージデバイス内に格納されることを特徴とする請求項１に記載の方法。
【請求項１０】

前記第１データセグメントを前記暗号化するステップは、ブロック暗号モードの下で動作することを特徴とする請求項１に記載の方法。
【請求項１１】
前記第１データセグメントを前記暗号化するステップは、暗号ブロック連鎖（CBC）を含むことを特徴とする請求項１に記載の方法。
【請求項１２】
前記第１出力ファイルは、第１ストレージデバイス内に格納され、かつ、
前記第２出力ファイルは、第２ストレージデバイス内に格納されることを特徴とする請求項１に記載の方法。
【請求項１３】
前記第１出力ファイルは、メッセージ認証コードを格納するためのセクションをさらに含むことを特徴とする請求項１に記載の方法。
【請求項１４】
前記ヘッダセクションは、前記第１出力長に関連付けられた情報を含むことを特徴とする請求項１に記載の方法。
【請求項１５】
前記ヘッダセクションは、バージョン番号を含むことを特徴とする請求項１に記載の方法。
【請求項１６】
前記第１出力ファイルは、前記第１出力ファイルに関連付けられる識別子を格納するためのセクションをさらに含むことを特徴とする請求項１に記載の方法。
【請求項１７】
前記第１出力ファイルは、パディングセクションをさらに含むことを特徴とする請求項１に記載の方法。
【請求項１８】
前記第１出力ファイルは、前記第１データセグメントを前記暗号化するステップに関連付けられるメッセージ認証コードを格納するためのセクションをさらに含むことを特徴とする請求項１に記載の方法。
【請求項１９】
前記第１出力ファイルは、ノンスセクションをさらに含むことを特徴とする請求項１に記載の方法。
【請求項２０】
前記第１出力ファイルと前記第２出力ファイルとは、等しいファイル長によって特徴付けられることを特徴とする請求項１に記載の方法。
【請求項２１】
前記第１データセグメントと前記第２データセグメントとは、等しいファイル長によって特徴付けられることを特徴とする請求項１に記載の方法。
【請求項２２】
データファイルを暗号化するための方法であって、
前記方法は、
入力ファイルを提供するステップであって、前記入力ファイルは、入力長によって特徴付けられるステップと、
多数の出力ファイルを提供するステップであって、前記出力ファイルは、第１出力ファイルと第２出力ファイルとを含み、前記第１出力ファイルは、第１出力長によって特徴付けられ、前記第１出力長は、前記入力長と、前記多数の出力ファイルとに関連付けられ、前記第１出力ファイルは、第１複数のブロックを含み、前記第１複数のブロックは、第１ブロックと第２ブロックとを含み、前記第１ブロックと前記第２ブロックとは、同じブロックサイズによって特徴付けられ、前記第１複数のブロックのそれぞれは、ヘッダセクションとデータセクションとを含み、前記ヘッダセクションは、前記数を伴う情報を含むステップと、

前記入力ファイルの第１ロケーションと第２ロケーションとを決定するステップであって、前記第２ロケーションは、既知の長さで前記第１ロケーションからオフセットされるステップと、
前記既知の長さのために、第１スレッドによって、前記第１ロケーションで、前記入力ファイルを読み取るステップから、第１データセグメントを得るステップと、
第２スレッドによって、前記第２ロケーションで、前記入力ファイルを読み取るステップから、第２データセグメントを得るステップと、
前記第１データセグメントを暗号化するステップと、
前記第１ブロックで、前記暗号化された第１データセグメントを格納するステップと
を具備することを特徴とする方法。

【請求項２３】
第３ロケーションを決定するステップと、
前記既知の長さのために、前記第１スレッドによって、前記第３ロケーションで、前記入力ファイルを読み取るステップから、第３データセグメントを得るステップと、
前記第３データセグメントを暗号化するステップと、
前記暗号化された第３データセグメントを格納するステップと
をさらに具備し、
前記第３ロケーションは、前記第２ロケーションからオフセットされることを特徴とする請求項２２に記載の方法。

【請求項２４】
データを復号化するための方法であって、
複数の入力データファイルを特定するステップであって、前記複数の入力データファイルは、第１入力データファイルと第２入力データファイルとを含み、入力データファイルのそれぞれは、出力データファイルに関連付けられるステップと、
前記第１入力データファイルを処理するステップと、
前記第１入力データファイルから、前記出力データファイルに関連付けられた情報を得るステップであって、前記情報は、ブロックサイズを含むステップと、
前記第１入力データファイルで、２つの隣接したブロックを決定するステップであって、前記２つの隣接したブロックは、第１ブロックと第２ブロックとを含むステップと、
前記第２入力データファイルで、２つの隣接したブロックを決定するステップであって、前記２つの隣接したブロックは、第３ブロックを含むステップと、
前記第１ブロックを復号化することによって、第１データセグメントを得るステップと、
前記第３ブロックを復号化することによって、第２データセグメントを得るステップと、
前記出力データファイルの連続した部分に、前記第１データセグメントと第２データセグメントとを格納するステップと
を具備することを特徴とする方法。

【請求項２５】
前記複数のデータファイルは、同じ長さによって特徴付けられることを特徴とする請求項２４に記載の方法。

【請求項２６】
前記複数のデータファイルは、異なるストレージデバイスによって格納されることを特徴とする請求項２４に記載の方法。

【請求項２７】
前記第１ブロックを復号化するための鍵を得るステップをさらに具備することを特徴とする請求項２４に記載の方法。

【請求項２８】
前記方法は、前記第２ブロックを復号化することによって、第３データセグメントを得るステップをさらに具備することを特徴とする請求項２４に記載の方法。

【請求項２９】
データを格納するためのシステムであって、
入力ファイルを格納するように構成された、第１ストレージデバイスであって、前記入力ファイルは、第１セクションと第２セクションとを含む第１ストレージデバイスと、
複数のデータファイルを格納するように構成された、第２ストレージデバイスであって、前記複数のデータファイルは、第１出力ファイルと第２出力ファイルとを含み、前記第１出力ファイルと前記第２出力ファイルとは、等しい長さを有する第２ストレージデバイスと、
前記第１ストレージデバイスにアクセスするように構成された、第１アクセスコンポーネントと、
前記第１ストレージデバイスにアクセスするように構成された、第２アクセスコンポーネントと、
第１スレッドと第２スレッドとを設けるように構成された、プロセッサコンポーネントと、
を備え、
前記第１アクセスコンポーネントは、前記第１セクションから、データを読み取り、
前記第１スレッドは、前記第１セクションを暗号化することによって、第１出力データを生成し、
前記第２アクセスコンポーネントは、前記第２セクションから、データを読み取り、
前記第２スレッドは、前記第２セクションを暗号化することによって、第２出力データを生成し、
前記第２ストレージデバイスは、前記第１出力ファイルで前記第１出力データを、及び、前記第２出力ファイルで前記第２出力データを格納することを特徴とするシステム。
【請求項３０】
前記第１アクセスコンポーネントと前記第１ストレージデバイスとは、インターフェースによって接続され、
前記インターフェースは、IDEインターフェース、SCSIインターフェース、SATAインターフェース、USBインターフェース、又は、ファイバーチャネルであることを特徴とする請求項２９に記載のシステム。
【請求項３１】
前記プロセッサコンポーネントは、プロセッサユニットからなり、
前記プロセッサユニットは、スレッディング可能であることを特徴とする請求項２９に記載のシステム。
【請求項３２】
前記プロセッサコンポーネントは、複数のプロセッサを備え、
前記複数のプロセッサは、並列に動作するように構成されたことを特徴とする請求項２９に記載のシステム。
【請求項３３】
前記第２ストレージデバイスは、第１ハードドライブと第２ハードドライブとを備え、
前記第１出力ファイルは、前記第１ハードドライブで格納され、
前記第２出力ファイルは、前記第２ハードドライブで格納されることを特徴とする請求項２９に記載のシステム。
【請求項３４】
前記第１スレッドと前記第２スレッドとは並列に動作することを特徴とする請求項２９に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
一般に、本発明はデータセキュリティ及びストレージに関し、かつ、特に２つ以上の暗号化された出力データファイルとして、入力データファイルを格納するための方法に関す

る。
【背景技術】
【０００２】
情報技術の到来で、ますます多くの情報が電子的に格納されている。電子的に格納された情報を保護するために、様々な従来技術が開発されてきた。ハードウェアストレージ機器（即ち、ハードディスク、テープ、コンパクトディスクなど）を保護すること以外に、データバックアップ及びアーカイブは、格納された情報を保護するための一般的かつ信頼できる方法である。
【０００３】
一般に、データバックアップは、データのコピーを作り、かつ、これらのコピーを格納することを指す。オリジナルのデータを失うか、又は無効にしたとき、オリジナルのデータからの情報はこれらのコピーから回復される。さらにデータの安全を確実にするために、ストレージデバイス内に格納されるデータは、最初に暗号化され、次いで、暗号化されたデータは異なったストレージデバイス（即ち、異なったハードドライブ）に格納される。過去に、様々な従来技術が、データ暗号化及びストレージを実行するために開発されてきた。残念ながら、多くの場合、これらの従来技術は不十分である。
【０００４】
データを暗号化及び格納するための従来技術は、情報技術における最近の進展の観点から不十分である（ファイルサイズがますます大きくなる）。特に、多くの場合、従来技術を用いて、大きなデータファイルを暗号化及び格納するのは、遅過ぎて、かつ、効率が悪い。
【０００５】
様々な従来技術によると、データファイルをセキュアに格納するプロセスは、入力データファイルを読み取るステップと、入力データファイルを暗号化するステップと、最終的に、出力ファイルとして暗号化された入力データファイルを格納するステップとを含んでいる。通常、全プロセスは、１つのスレッドによって順番に実行される。例えば、同じスレッドが全体の入力データファイルを読み取る。その結果、プロセスの速度は、スレッドが入力ファイルを読み取る速度によって制限されている。本質的には、全プロセスは最も遅いステップより速いはずがない（この場合、通常、ファイルを読み取るステップである）。入力データファイルのサイズが小さいとき、プロセスの速度は通常許容可能である。しかしながら、入力データファイルサイズが大きいとき（例えば、１ギガバイト以上）、多くの場合、プロセスの速度は多くのアプリケーションに対してあまりに低速である。
【発明の概要】
【発明が解決しようとする課題】
【０００６】
したがって、データを暗号化及び格納するためのシステム及び方法を改善することが望まれている。
【課題を解決するための手段】
【０００７】
本発明の態様は、２つ以上の暗号化された出力データファイルとして（後で、復号化及び再結合されて、入力データファイルと同一のファイルを形成することができる）、入力データファイルを格納するための方法及びシステムを提供する。特に、本発明の態様は、単一の入力データファイルが複数のスレッドによって並列に処理され、かつ、複数の暗号化された出力ファイルが異なるロケーションに格納されることを可能にする。とりわけ、本発明の態様は、従来技術に比べて、暗号化されたデータを格納するためのより効率的な方法を提供する。ほんの一例として、本発明は、大規模なファイルに対して、セキュアなバックアップソリューションを提供するのに使用されるが、本発明はより幅広い範囲の適応性を有することが認識される。
【０００８】
１態様によれば、本発明はデータファイルを暗号化するための方法を提供する。方法は

、入力長によって特徴付けられる、入力ファイルを提供するステップを具備している。また、方法は、第１出力ファイルと第２出力ファイルとを含む、多数の出力ファイルを提供するステップを具備している。前記第１出力は、第１出力長によって特徴付けられる。前記第１出力長は、前記入力長と、前記多数の出力ファイルとに関連付けられている。前記第１出力ファイルは、ヘッダセクションとデータセクションとを含んでいる。代表的な態様では、前記ヘッダセクションは、前記数に関連付けられた情報を含んでいる。加えて、方法は、前記入力ファイルの第１ロケーションと第２ロケーションとを決定するステップを具備している。前記第２ロケーションは、既知の長さで前記第１ロケーションより後ろである。また、方法は、前記既知の長さのために、第１スレッドによって、前記第１ロケーションで、前記入力ファイルを読み取るステップから、第１セグメントを得るステップを具備している。さらに、方法は、第２スレッドによって、前記第２ロケーションで、前記入力ファイルを読み取るステップから、第２データセグメントを得るステップを具備している。その上、方法は、前記第１データセグメントを暗号化するステップを具備している。さらに、方法は、前記第１出力ファイルの前記データセクションで、前記暗号化された第１データセグメントを格納するステップを具備している。

【０００９】

別の態様によれば、本発明は、データファイルを暗号化するための方法を提供する。方法は、入力長を有する入力ファイルを提供するステップを具備している。また、方法は、多数の出力ファイルを提供する方法を具備している。前記出力ファイルは、第１出力ファイルと第２出力ファイルとを含んでいる。前記第１出力ファイルは、前記入力長と、前記多数の出力ファイルとに関連付けられた、第１出力長によって特徴付けられる。前記第１出力ファイルは、第１ブロックと第２ブロックとを含む、第１複数のブロックを含んでいる。前記第１ブロックと前記第２ブロックとは、同じブロックサイズによって特徴付けられる。前記第１複数のブロックのそれぞれは、ヘッダセクションとデータセクションとを含んでいる。前記ヘッダセクションは、前記数を伴う情報を含んでいる。さらに、方法は、前記入力ファイルの第１ロケーションと第２ロケーションとを決定するステップを具備している。前記第２ロケーションは、既知の長さで前記第１ロケーションより後ろである。また、方法は、前記既知の長さのために、第１スレッドによって、前記第１ロケーションで、前記入力ファイルを読み取るステップから、第１データセグメントを得るステップを具備している。加えて、方法は、第２スレッドによって、前記第２ロケーションで、前記入力ファイルを読み取るステップから、第２データセグメントを得るステップを具備している。その上、方法は、前記第１データセグメントを暗号化するステップを具備している。さらに、方法は、前記第１ブロックで、前記暗号化された第１データセグメントを格納するステップを具備している。

【００１０】

さらに別の態様によれば、本発明は、データを復号化するための方法を提供する。方法は、複数の入力データファイルを特定するステップを具備している。前記複数の入力データファイルは、第１入力データファイルと第２データファイルとを含んでいる。入力データファイルのそれぞれは、出力データファイルに関連付けられている。また、方法は、前記第１データファイルを処理するステップを具備している。さらに、方法は、前記第１入力データファイルから、前記出力データファイルに関連付けられた情報を得るステップを具備している。とりわけ、前記情報はブロックサイズを含んでいる。加えて、方法は、前記第１入力データファイルで、２つの隣接したブロックを決定するステップを具備している。前記２つの隣接したブロックは、第１ブロックと第２ブロックとを含んでいる。加えて、方法は、前記第２入力データファイルで、２つの隣接したブロックを決定するステップを具備している。前記２つの隣接したブロックは、第３ブロックを含んでいる。また、方法は、前記第１ブロックを復号化することによって、第１データセグメントを得るステップを具備している。さらに、方法は、前記第３ブロックを復号化することによって、第２データセグメントを得るステップを具備している。また、方法は、前記出力データファイルの連続した部分に、前記第１データセグメントと第２データセグメントとを格納する

ステップを具備している。

【００１１】

さらに別の態様によれば、本発明はデータを格納するためのシステムを提供する。システムは、入力ファイルを格納するように構成された第１ストレージデバイスを備えている。前記入力ファイルは、第１セクションと第２セクションとを含んでいる。また、システムは、複数のデータファイルを格納するように構成された第２ストレージデバイスを備えている。前記複数のデータファイルは、第１出力ファイルと第２出力ファイルとを含んでいる。前記第１出力ファイルと前記第２出力ファイルとは、同じ長さを有する。加えて、システムは、前記第１ストレージデバイスにアクセスするように構成された、第１アクセスコンポーネントを備えている。また、システムは、前記第１ストレージデバイスにアクセスするように構成された、第２アクセスコンポーネントを備えている。さらに、システムは、第１スレッドと第２スレッドとを設けるように構成された、プロセッサコンポーネントを備えている。前記第１アクセスコンポーネントは、前記第１セクションから、データを読み取る。前記第１スレッドは、前記第１セクションを暗号化することによって、第１出力データを生成する。前記第２アクセスコンポーネントは、前記第２セクションから、データを読み取る。前記第２スレッドは、前記第２セクションを暗号化することによって、第２出力データを生成する。前記第２ストレージデバイスは、前記第１出力ファイルで前記第１出力データを、及び、前記第２出力ファイルで前記第２出力データを格納する。

【００１２】

本発明が従来技術に様々な利点を提供することが理解される。特に、オペレーションが並列に実行されるので、従来技術と比べて、本発明の態様に従って動作するスレッディングは、より迅速なデータ・アクセス及び暗号化を可能にする。さらに具体的には、本発明の態様は、大きなファイル（例えば、10GBより大きなファイルのバイナリバックアップ）の暗号化に特に適している。様々な態様によれば、暗号化オペレーションの間、ファイルが別々の暗号化されたファイルに分解されるので、システム管理者が、追加的なセキュリティのために、複数の別のロケーションに暗号化されたファイルを格納することができる。他の利点も存在する。

【００１３】

本発明の様々な追加的目的、特徴、及び利点は、以下の詳述な説明及び添付図面に関連して、より完全に理解することができる。

【図面の簡単な説明】

【００１４】

【図１】本発明の実施例を実施するのに利用されるコンピュータシステムを図示した略図である。

【図２】本発明の実施例による暗号化オペレーションを図示した略図である。

【図３】本発明の実施例によるストリップファイルのファイルフォーマットを図示した略図である。

【図４】本発明の実施例による復号化オペレーションを図示した略図である。

【図５】本発明の実施例による暗号化プロセスを図示した簡易なフローチャートである。

【図６】本発明の実施例による復号化プロセスを図示した簡易なフローチャートである。

【発明を実施するための形態】

【００１５】

本発明の様々な実施例は効率的にデータを暗号化及び格納するための方法を提供する。特に、本発明のある実施例は、異なったスレッドによって入力データファイルの並列処理を可能にする（実質的に処理速度全体を改良する）。

【００１６】

本発明の実施例は各種タイプのシステムによって実装してもよい。例えば、本発明の特定の実施例はコンピュータ・ワークステーションで実装される。別の例として、本発明の実施例はコンピュータサーバで実装される。本発明の実施例を他のタイプのシステムによ

って実装してもよいことが理解される（例えば、パーソナルコンピュータなど）。図１は、本発明の実施例を実装するのに利用されるコンピュータシステムを図示した略図である。この図は単に例であり、特許請求の範囲を過度に制限してはならない。当業者の１人は多くのバリエーション、代替例、及び変形例を認識する。

【００１７】

図1に示されたように、ワークステーションシステム100は、ディスプレイ101と、ケース102と、キーボード103と、マウス104と、ハードドライブ107のクラスタとを備えている。例として、ワークステーションシステムは、ケース102の中に入れられる１又は複数の中央演算処理装置（CPU）105と、ランダムアクセスメモリー（RAM）106とを含んでいる。特定の実施例によると、ワークステーションシステム100は、並列で動作することができる２つ以上のCPUを含んでいる。別の実施例によると、ワークステーションシステム100は、マルチタスキング、及び／又は、インターリービングが可能な単一のCPUを含んでいる。

【００１８】

ハードドライブ107のクラスタは、データを格納及びバックアップするのに使用される。例えば、ハードドライブ107のクラスタは、RAID（redundant array of independent disks）（データが複数のディスクにわたる冗長ストリップ108及び109内に格納される）として配置される。別の例として、ハードドライブ107のクラスタは、ハードドライブ（ワークステーションシステム100のCPUに対して相互に独立し、かつ、アクセス可能である）を含んでいる。図示されているように、ハードドライブ107は、ドライブ110、ドライブ111、及びドライブ112を含み、各ドライブが独立して情報を格納することができる。特定の実施例では、ソースファイルはドライブ107で暗号化され、かつ、システム100はインターフェースを通して接続される。アプリケーションによって、インターフェースは、SCSI、SATA、ファイバーチャネル、USB、IDEなどである。

【００１９】

代替の実施例では、コンピュータシステム100は、単一のハードドライブ（同時にハードドライブの異なった部分で読み取りオペレーションを実行することができ、その結果、複数のアクセスを可能にする）を利用する。

【００２０】

図２は、本発明の実施例に従って、暗号化オペレーション200を図示した略図である。この例では、入力ファイル210が暗号化され、かつ、暗号化されたファイルは別々のファイル201、202、203、及び204として格納される。上記したように、本発明の実施例は非常にフレキシブルであり、したがって、種々のアプリケーションを有するが、それらは大きなファイルを暗号化及び格納するのに非常に適していることを理解しなければならない。例えば、１ギガバイトより大きな入力ファイルを暗号化及び格納するプロセスで、本発明の様々な実施例は、並列データ処理の可能性のため、従来技術より効率的である。

【００２１】

ストライピング（striping）オペレーションが実行されるので、ファイル201、202、203、及び204をストリップファイル（strip file）と呼ぶことができる。特定の実施例によると、各ストリップファイルは別々のスレッドによって処理される。特定のアプリケーションによって、ストリップファイル（又は、ストリップ幅（strip width）と呼ばれる）の数は変化する。例えば、ハードウェア（多数のストリップファイル（例えば、５つ以上）を可能にする）が生成される。特定の実施例では、ストリップ幅は、様々な要素に基づきコンピュータで自動的に決定される（例えば、利用可能なスレッドの数、利用可能なプロセッサの数、利用可能なストレージデバイスの数など）。ある実施例では、ストリップ幅はユーザによって指定される。例えば、ユーザは、簡単なファイル管理のために、少数のストリップファイルを選択してもよい。別の例として、ユーザは、より良いセキュリティ、及び／又は、より良いパフォーマンスのために、多数のストリップファイルを選択してもよい。

【００２２】

ストリップファイルのサイズは等しい。例えば、図２に示すように、ストリップファイルのそれぞれは、同じサイズによって特徴付けられ、一般に、入力ファイル210の四分の一より少し大きい（即ち、ヘッダセクションなどを計上するため）。代表的なストリップファイルの詳細な説明を以下で行う。

【００２３】

本発明の実施例がスレッディングスキームを提供することを理解しなければならない。一度に大きなデータを読み取るステップが多くの場合に減速を引き起こすので、本発明の実施例はスキーム（各スレッドが、一度に入力ファイル210のデータの小規模なブロックを読み取る）を提供する。図２に示されるように、データ処理の見解から、入力ファイル210は、多数のブロックに分割される。入力ファイル210にアクセスするとき、各スレッドは、ブロックサイズのための長さのために特定のロケーションで、入力ファイル210を読み取る。ほんの一例として、第１スレッドは、入力ファイル210のブロック「１」を読み取り、ブロック「１」に格納されたデータを暗号化し、かつ、暗号化されたデータをストリップファイル201のデータ部内に格納する。同様に、第２スレッドは、入力ファイル210のブロック「２」を読み取り、ブロック「２」に格納されたデータを暗号化し、かつ、暗号化されたデータをストリップファイル202のデータ部内に格納するなど。

【００２４】

アプリケーションによって、各種タイプの暗号化方法を使用してもよい。好ましい実施例では、暗号ブロック連鎖（CBC）が使用される。例えば、暗号化される前に、それぞれのブロックのデータは、前の暗号ブロック（データストリングによって通常初期化される第１ブロックを除いた）で排他的論理和をとられる。特に、それぞれの暗号化されたデータは、そのポイントまでのすべての前のデータブロックに依存している。通常、CBC暗号化は並列な暗号化及び復号化を可能にする。

【００２５】

本発明が、他のタイプの暗号化の方法に関連して実行されることを理解しなければならない。様々な実施例では、他のタイプの暗号化方法が使用される（例えば、電子符号表、初期化ベクトル、暗号フィードバック、出力フィードバックなど）。

【００２６】

ここで、図２に戻る。図示されているように、各ストリップファイルによって格納された暗号化されたデータブロックは、不連続である。例えば、ストリップファイル201は、暗号化されたデータブロック「１」及び「５」（連続データブロックではない）を連続して格納する。

【００２７】

スレッディングから所望の効率を達成することができるように、それぞれのスレッドは、入力ファイル210の適切なデータブロックを処理するように構成されている。好ましい実施例は、正しいオフセットロケーション（各スレッドが入力ファイル210の「n番目」のブロックを読み取る）を決定するのに以下の式を使用する。

オフセット=［（ストリップ_カウント*ブロック_サイズ）*n］+（スレッド_数*ブロック_サイズ）　　（式１）

ここで、「ストリップカウント」は、書き込まれているストリップファイルの数であり、

「n」は、０～［（ファイル内の総ブロック／ストリップカウント）-1］の整数であり、

「スレッド番号」は、１～ストリップカウント（包括的な）の整数であり（通常、ストリップファイルあたり1スレッド）、かつ、

「ブロックサイズ」は、量データ（各スレッドが単一の読み取りオペレーションで入力ファイルから読み取る）、及び、量データ（各スレッドが単一の書き込みオペレーションでストリップファイルに書き込む）である。

【００２８】

入力ファイル210のブロックを読み取るステップ、読み取られたブロックを暗号化する

ステップ、及び、最終的に、暗号化されたブロックを各ストリップファイル内に格納するステップのプロセスは、入力ファイル210全体が暗号化及び格納されるまで継続される。

【００２９】

図３は、本発明の実施例に従って、ストリップファイル300のファイルフォーマットを図示した略図である。この実施例では、ストリップファイル300は、以下のセクションを含んでいる。

1．ヘッダセクション301
2．ノンス（nonce）セクション302
3．データセクション303
4．パディングセクション304
5．データ長セクション305
6．MACセクション306
7．XORのノンスセクション307

【００３０】

ストリップファイル300のファイルフォーマットが単に特定の例を提供することを理解しなければならない。ストリップファイルは、特定の実施例に基づき、他のセクション又はフィールドを含むようにフォーマットしてもよい。例えば、本発明の実施例によるストリップファイルは、UNIX（登録商標）オペレーティングシステムに従ってフォーマットされ、かつ、図３に図示されたものと異なったデータセクションを有する。例えば、特定のデータ・フィールドを加えるか、又は取り除いてもよく、したがって、ストリップファイルはUNIX（登録商標）フォーマットに一致する。

【００３１】

ヘッダセクション301はファイルを特定するための情報を含んでいる。例えば、以下の表１は、本発明のある実施例に従って、代表的なヘッダセクションを図示している。

【００３２】

【表１】

フィールド	説明
ファイル識別子	一意の既知の識別子
バージョン	ファイル及び／又はプロトコルのバージョン
ブロック_サイズ	入力ファイルから読み取り、かつ、ストリップファイルへ書き込むためのスレッドにより使用されるI/Oサイズ
ファイルグループGUID	多くのストリップグループとしてファイルを一意に特定するグローバル一意識別子（GUID）
ファイルの総数	ストリップグループでのファイルの数
ファイル番号及びファイルの総数	オリジナルファイルを作成するストリップファイルの中のこのストリップファイルの位置、及び、ファイルの総数
ヘッダHMAC	ヘッダ情報の完全性を確実にするために使用されるキー-ハッシュメッセージ認証コード(HMAC)

【００３３】

アプリケーションによって、ヘッダセクション301の種々のフィールドを、追加、除去、及び／又は、再配置してもよい。例えば、また、ヘッダセクション301は、パディングフィールド（ヘッダセクションの終わりまで０で埋められた）を有して、ヘッダブロックがデータブロック及び他のブロックと同じサイズであることを確実にしてもよい。

【００３４】

ノンスセクション302はノンス数、及び／又は、ベクトルを含んでいる。１実施例によると、ノンスセクション302は、ランダムに生成されたノンスベクトル（CBC暗号化に使用される初期化ベクトルとして使用される）を含んでいる。一般に、ノンスベクトルは、各

ストリップファイルに対して異なっている。本発明の様々な実施例におけるランダムノンスベクトルの利用は、セキュリティ違反のリスクを実質的に減少させる。好ましい実施例では、ランダムノンスベクトルは、タイムスタンプを使用することによって生成される。アプリケーションによって、ノンスセクション302に格納されたノンス数は、多様な長さを有してもよく、かつ、多様な方法で生成することができる。

【００３５】

データセクション303は、暗号化されたデータのブロックを含んでいる。上記したように、スレッディング及び暗号化方法によって、データセクション303に格納されたコンテンツデータブロックは変化する。暗号化されたデータブロックは、以下の関数によって表してもよい。

E{（ノンス、ペイロード、パッド、長さ、ノンス、

【００３６】

【数１】

⊕

【００３７】

数）、鍵}　　（式2）

【００３８】

パディングセクション304は、ストリップファイルが長さにおいて等しくなるのを確実にするために設けられる。各暗号化されたデータブロックが長さにおいて等しいので、時々、最後のブロックをパディングデータで埋める必要がある。例えば、ストリップファイルのための総データが複数の５バイトよりも１バイト多い場合、５つの５バイトのブロックが、入力ファイルを格納するのに使用され、かつ、最後のブロックは、１バイトのデータと４バイトのパディングとを含んでいる。通常、パディングは、残りのスペースに０を埋めるステップを具備するが、他の値又はコンテンツをパディングに使用してもよいことを理解しなければならない。

【００３９】

データ長セクション305は、パディングを含まない、データセクション303に格納された有効データ長に関連付けられた情報を格納する。例えば、データ長セクション305は、データセクション303に格納される暗号化されたデータのバイトの数を含んでいる。別の例では、データ長セクション305自体は、多数のパディングのバイトを含んでいる。

【００４０】

MACセクション306はファイルを認証するための情報を格納する。特定の実施例では、MACセクション306は、キー-ハッシュメッセージ認証コード（HMAC）を含んでいる。例えば、HMACは、MACセクション306に格納され、かつ、秘密鍵を使用することによって決定される。アプリケーションによって、HMACは、格納されたデータのデータ完全性、及び／又は、信憑性を検証するステップに使用してもよい。特定の実施例では、HMACは、以下の関数を使用することで指定される。

HMAC{E（ヘッダ、ノンス、ペイロード、パッド、長さ、ノンス、

【００４１】

【数２】

⊕

【００４２】

数）、鍵}　　（式3）

【００４３】
XORノンスセクション307は、特別な数（special number）（データの暗号化及び復号化に使用される）を含んでいる。例えば、512ビット（又は、64バイト）の乱数は、既知の値で、排他的論理和をとられる。乱数はノンスセクション302に格納された乱数と同じである。特別な数は、検証目的のために、以下の式を使用することで計算される。
特別_数=ノンス
【００４４】
【数３】

⊕

【００４５】
（ノンス
【００４６】
【数４】

⊕

【００４７】
特別_数）　　（式4）
【００４８】
上記したように、アプリケーションによって、ストリップファイルは、特定のアプリケーションに合う異なったフィールドを有してもよい。例えば、異なったタイプの暗号化又はストライピング方法が実施される場合、異なったタイプのフィールドを使用してもよい。
【００４９】
様々な実施例によると、ストリップファイルは別々に格納される。例えば、同じファイルによって生じるストリップファイルは、異なったストレージデバイスで格納される。必要であれば、暗号化されたストリップファイルは、復号化及び再結合される。
【００５０】
図４は、本発明の実施例に従って、復号化オペレーションを図示した略図である。この実施例では、４つのストリップファイル410、420、430、及び440は、復号化され、かつ、出力ファイル400に結合される。別々のストリップファイルが追加的なセキュリティ手段を提供することを理解しなければならない（復号化されたデータの重要なセグメントを得ることができる前に、未認証のエンティティがすべてのストリップファイルを必要とするので）。例えば、単一のストリップファイルを復号化することによって、復号化されたデータの代表的なブロックだけが得られる。
【００５１】
図４に示されているように、それぞれのストリップファイルは、オリジナルファイルに対して、不連続なデータのブロックを含んでいる（ストリップファイルが、上で説明されたように、複数のスレッドによって生成されるので）。例として、ストリップファイル410は、暗号化されたデータブロック411と412を含み、ストリップファイル420は、暗号化されたデータブロック421と422を含み、ストリップファイル430は、暗号化されたデータブロック431と431を含み、かつ、ストリップファイル440は、暗号化されたデータブロック441と442を含んでいる。代表的な復号化プロセスの間、データブロック411、421、431、及び441は、４つのスレッドによって復号化され、次いで、出力ファイル400のデータセグメ

ント401、402、403、及び404として格納される。例えば、データブロック411、421、431、及び441は、４つの異なったストリップファイルにそれぞれ格納されるが、データセグメント401、402、403、及び404は、出力ファイル400の連続データセグメントである。例として、データ復号化と出力ファイル構築は、図１のワークステーションシステム100によって実行される。

【００５２】

特定のアプリケーションによって、本発明の様々な実施例による暗号化及び復号化プロセスは異なった方法で実装してもよい。例として、図５は、本発明の実施例に従って暗号化プロセス500を図示した簡易なフローチャートである。この図が単に例であり、かつ、フローチャートにおける様々なステップを、追加、削除、再配置、置換え、反復、オーバーラップ、及び／又は、部分的にオーバーラップしてもよい。

【００５３】

ステップ501では、暗号化される入力ファイルが提供される。例として、入力ファイルはハードドライブによって格納される。通常、入力ファイルは、サイズが大きく、かつ、機密情報を含んでいる（効率的なデータ暗号化が望まれている）。

【００５４】

ステップ502では、暗号化オペレーションのための様々なパラメータが決定される。アプリケーションによって、これらのパラメータは、出力ストリップファイルの数、ブロックサイズ、暗号化方法などを含んでもよい。ある実施例によると、これらのパラメータは、様々な要素（例えば、入力ファイルのサイズ、システムの処理能力など）に基づいて自動的に決定される。様々な代替の実施例によると、これらのパラメータはユーザによって提供される。

【００５５】

ステップ503では、ストリップファイルが準備される。特定のアプリケーションによって、ストリップファイルは様々なフォーマットに従ってもよい。例えば、ストリップファイルは、図４に図示されたようなフォーマットを有してもよい。

【００５６】

ステップ504では、スレッドがデータを暗号化するために割り当てられる。ある実施例によると、スレッドの数はストリップ幅と等しい。例えば、４のストリップ幅に対して（即ち、生成される４つの出力ストリップファイル）、４つのスレッドが設けられる。アプリケーションによって、スレッドの数はより少ないか、又は、より多くてもよい。

【００５７】

ステップ505では、入力ファイルがアクセスされる。様々な実施例によると、入力ファイルは、異なったセグメントで並列に、複数のスレッドによってアクセスされる（各スレッドが所定のロケーションでデータのブロックを読み取る）。例えば、第１スレッドは、第１ロケーションで、入力ファイルから、データのブロックを読み取り、かつ、第２スレッドは、第２ロケーションで、別のデータのブロックを読み取るなど。特定の実施例では、入力ファイルは、複数のアクセスを提供するハードディスクに格納される。例として、ストリップサイズの関数としてのオフセットロケーションは、上記した式１を使用することで決定してもよい。

【００５８】

ステップ506では、データブロックが暗号化される。特定の実施例では、ステップ505でアクセスされた各データブロックは、指定されたスレッドによって暗号化される。アプリケーションによって、様々なエンコーディングスキーム10を用いてもよい。例えば、CBC方法は、データを暗号化するのに使用してもよい。

【００５９】

ステップ507では、暗号化されたデータは、ストリップファイルの中に格納される。ある実施例では、ストリップファイルは、異なった物理的エンティティ（例えば、ハードディスク）に格納される。一部の実施例では、ストリップファイルは、同じ物理的エンティティに格納される。ほんの一例として、暗号化されたデータブロックは、ストリップファ

イルのデータセクションの中に格納される。

【００６０】

分岐ステップ508では、入力ファイルが最初から最後まで読み取られたか否かが決定される。全体の入力ファイルが暗号化及び格納された場合、プロセスはステップ509に進む。他方では、入力ファイルがまだ暗号化及び格納されるデータをまだ含んでいる場合、プロセスは、ステップ505に戻って、データブロックを暗号化及び格納する。

【００６１】

ステップ509では、暗号化されたデータのファイルHMACが、ストリップファイルに付加される。例えば、ファイルHMACは、特定の暗号化鍵、及び／又は、方法に関連付けられた情報を含んでいる。ある実施例では、ファイルHMACは他の関連情報を含んでいる。

【００６２】

ステップ510では、暗号化及びストレージのためのプロセスが終了する。様々な実施例によると、ストリップファイルはそれに従って処理される。例えば、パディングを、ストリップファイルのサイズを均一にするために、ストリップファイルのデータセクションの終わりに加えてもよい。さらに、ストリップファイルを、ある所定のファイルフォーマット（例えば、図４に示されたファイルフォーマット）に一致するようにさらに処理してもよい。

【００６３】

入力ファイルと同一のファイルを作成するために、後で、ストリップファイルを復号化及び再結合することができる。

【００６４】

図６は、本発明の実施例に従って復号化プロセス600を図示した簡易フローチャートである。この図が単に例であり、かつ、フローチャートにおける様々なステップは、追加、削除、再配置、置換え、反復、オーバーラップ、及び／又は、部分的にオーバーラップしてもよい。

【００６５】

ステップ601では、復号化に必要であるストリップファイルが決定される。上記したように、入力ファイルに関連付けられたストリップファイルが復号化のために選択される。例えば、ストリップファイルは、これらのストリップファイルのヘッダに格納された情報に基づいて収集される。ある実施例によると、１セットのストリップファイルに関連付けられた情報は別々のファイルに格納される。

【００６６】

ステップ602では、様々なパラメータが、ストリップファイルから収集される。１実施例によると、パラメータ（例えば、ストリップ幅、ブロックサイズ、暗号化ベクトルなど）は、ストリップファイルの様々なセクションから抽出される。例えば、パラメータは、ストリップファイルのヘッダセクションから抽出される。

【００６７】

ステップ603では、ストリップファイルを復号化するためのプロセスが決定される。１実施例では、多数のスレッドを、ストリップファイルを復号化するために割り当ててもよい。別の実施例では、復号化プロセスの詳細は、ストリップファイルから収集された様々なパラメータ（例えば、スレッドの数、ブロックサイズ、復号鍵など）に基づいてもよい。

【００６８】

ステップ604では、ストリップファイルがアクセスされる。様々な実施例によると、それぞれのストリップファイルは、指定されたスレッドによって読み取られる。例えば、各スレッドは、並列でストリップファイルからデータの特定のブロックを読み取る。

【００６９】

ステップ605では、暗号化されたデータのブロックが復号化される。好ましい実施例では、それぞれのブロックの暗号化されたデータは、指定されたスレッドによって復号化される。

【００７０】
ステップ606では、復号化されたブロックのデータが出力ファイルに書き込まれる。例として、データ書き込みプロセスは、高速オペレーションのために、並列で、指定されたスレッドによって実行される。
【００７１】
分岐ステップ607では、復号化プロセスが完了であるか否かが決定される。例えば、いったんスレッドがストリップファイルからファイルの終り、及び／又は、パディングを読み取れば、復号化プロセスは完了であることが決定される。別の例として、いったん所定数のブロックが復号化すれば、復号化プロセスは完了であると考えられる。復号化プロセスが完了であることが決定された場合、プロセスはステップ608に進む。他方では、復号化プロセスが完了でないと決定された場合、プロセスはステップ604に戻る。
【００７２】
ステップ608では、復号化プロセスが完了する。特定のアプリケーションによって、様々な手段を、プロセスを終了させるために実施してもよい。例えば、プロセスを終了させるために、各ストリップファイルを閉じてもよい。
【００７３】
上で説明されたように、暗号化プロセスと復号化プロセスは、柔軟に異なったタイプのハードウェアシステムに関連して実装されて、幅広いアプリケーションを有することを理解しなければならない。
【００７４】
本発明の特定の実施例が説明されたが、説明された実施例に同等な他の実施例が存在することが当業者には理解される。従って、本発明が、特定の図示された実施例で制限されるのではなく、添付の特許請求の範囲だけで制限されることを理解しなければならない。
【符号の説明】
【００７５】
100　ワークステーションシステム
101　ディスプレイ
102　ケース
103　キーボード
104　マウス
105　中央演算処理装置（CPU）
106　ランダムアクセスメモリー（RAM）
107　ハードドライブ
108,109　冗長ストリップ
110,111,112　ドライブ

【図１】

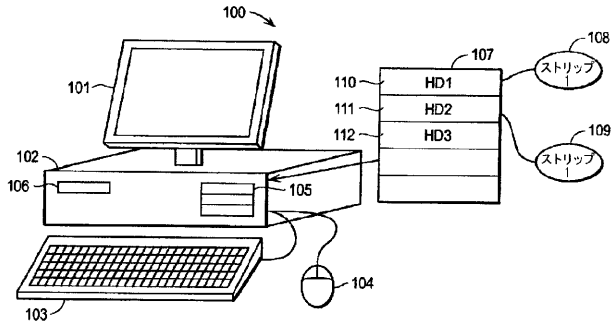

FIG. 1

【図２】

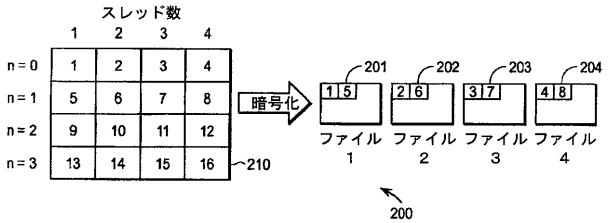

FIG. 2

【図３】

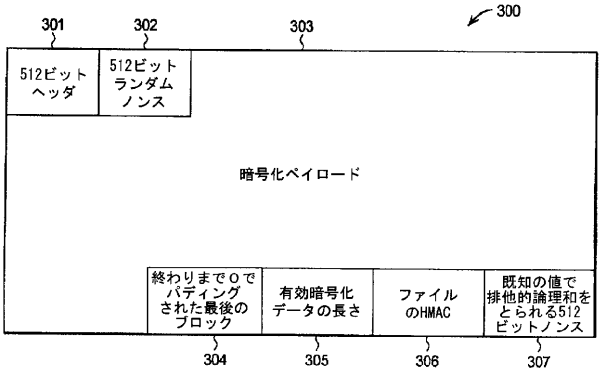

FIG. 3

【図４】

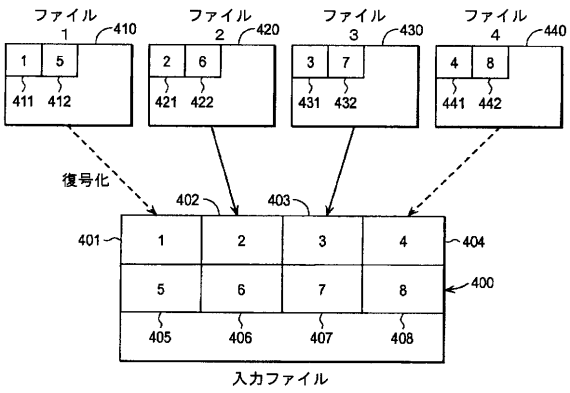

FIG. 4

【図５】

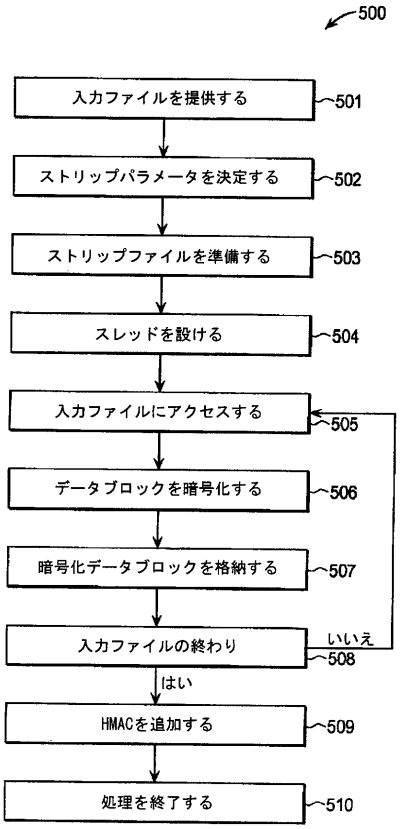

FIG. 5

【図６】

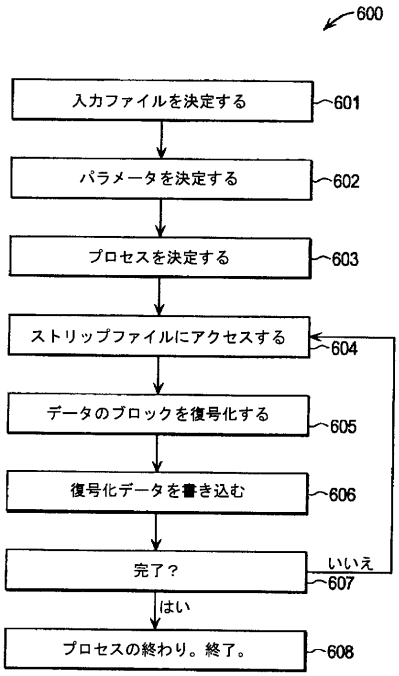
600
入力ファイルを決定する
601
パラメータを決定する
602
プロセスを決定する
603
ストリップファイルにアクセスする
604
データのブロックを復号化する
605
復号化データを書き込む
606
完了？
いいえ
607
はい
プロセスの終わり。終了。
608

FIG. 6

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/069096

A. CLASSIFICATION OF SUBJECT MATTER

G06F 12/16(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC : G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models since 1975
Japanese utility models and applications for utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKIPASS(Kipo Internal), NDSL, Google
keywords: encrypt*, encod*, compress*, divid*, partti*, file, length, header, thread*, shred*, parallel*

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US2005/0108484 A1 (PARK, S.W.) 19 MAY 2005 See paragraphs [9][10][43][44][49].	1-34
Y	US2005/0204210 A1 (LOBO, A. et al.) 15 SEPTEMBER 2005 See figures 7, 8; paragraphs [64]~[71].	1-34
A	US06070198 A (KRAUSE, M. et al.) 30 MAY 2000 See claims 1-5.	1-34
A	JACOBS, T. et al. 'A Thread and Data-Parallel MPEG-4 Video Encoder for a System-On-Chip Multiprocessor' In: Proceedings of the 16 International Conference on ASAP, 2005. See abstract, section 1. Introduction.	1-34
PA	US2007/0276953 A1 (TAKEUCHI, T. et al.) 29 NOVEMBER 2007 See figure 3 and its description.	1-34

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 FEBRUARY 2009 (02.02.2009)	**03 FEBRUARY 2009 (03.02.2009)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea	YOON, Hye Sook
Facsimile No. 82-42-472-7140	Telephone No. 82-42-481-8370

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2008/069096

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005-0108484 A1	19.05.2005	AU 2002-244980 A1	15.07.2003
		CA 2472443 A1	10.07.2003
		JP 2005-513672 A	12.05.2005
		KR 10-0354923 B1	21.10.2002
		WO 2003-056434 A1	10.07.2003
US 2005-0204210 A1	15.09.2005	CN 1652611 A	10.08.2005
		KR 1020050079418 A	10.08.2005
US 06070198 A	30.05.2000	JP 10-190649 A	21.07.1998
US 2007-0276953 A1	29.11.2007	None	

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	G06F 3/06 302B	

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,NO,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 ランドン・カート・ノール
アメリカ合衆国・カリフォルニア・９４０８６・サニーヴェール・ベルモント・テラス・９６４．１
(72)発明者 チャールズ・アドレー・レブラン
アメリカ合衆国・カリフォルニア・９５１２２・サン・ノゼ・ルクレツィア・アヴェニュー・２２８２・＃１

Ｆターム(参考) 5B017 AA03 BA07 CA16
5B065 BA01 CH11 PA16 ZA16
5B082 GA02 GA11
5J104 AA16 AA20 AA32 EA04 JA03 NA02 NA37 PA14