(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4596644号
(P4596644)

(45)発行日　平成22年12月8日(2010.12.8)　(24)登録日　平成22年10月1日(2010.10.1)

(51)Int.Cl.		F I		
G06F 12/14	(2006.01)	G06F	12/14	320F
H04N 5/907	(2006.01)	H04N	5/907	B
H04N 5/765	(2006.01)	H04N	5/91	L
H04N 5/91	(2006.01)	H04N	5/91	P

請求項の数 1　(全 11 頁)

(21)出願番号　特願2000-557400 (P2000-557400)
(86)(22)出願日　平成11年5月11日 (1999.5.11)
(65)公表番号　特表2002-519911 (P2002-519911A)
(43)公表日　平成14年7月2日 (2002.7.2)
(86)国際出願番号　PCT/US1999/010390
(87)国際公開番号　WO2000/000895
(87)国際公開日　平成12年1月6日 (2000.1.6)
審査請求日　平成15年9月19日 (2003.9.19)
審判番号　不服2007-16989 (P2007-16989/J1)
審判請求日　平成19年6月18日 (2007.6.18)
(31)優先権主張番号　09/105,593
(32)優先日　平成10年6月26日 (1998.6.26)
(33)優先権主張国　米国(US)

(73)特許権者　508113527
セキュア　ストレージ　ソリューションズ　・エルエルシイ
アメリカ合衆国・０３８０１・ニューハンプシャー州・ポーツマス・フリート　ストリート・１５５
(74)代理人　100064621
弁理士　山川　政樹
(74)代理人　100098394
弁理士　山川　茂樹
(72)発明者　ステインバーグ，イーラン
アメリカ合衆国・９４１１４・カリフォルニア州・サンフランシスコ・ダグラス　ストリート・３７２

最終頁に続く

(54)【発明の名称】デジタル・カメラ・データの転送のための安全記憶デバイス

(57)【特許請求の範囲】
【請求項１】
（ａ）安全でないデジタル・カメラ・データをデジタル・カメラから、デジタル・カメラに着脱可能に取り付けられる安全記憶デバイスへダウンロードするステップと、
（ｂ）前記安全でないデジタル・カメラ・データに対して安全データを作成するために前記安全記憶デバイス内でデジタル処理を実行することによって、前記安全でないデジタル・カメラ・データを安全データにするステップとを含むデジタル・カメラ・データの安全化方法。
【発明の詳細な説明】
【０００１】
（発明の背景）
（発明の分野）
本発明は、一般に、デジタル・スチールおよびビデオ・カメラ、および、デジタル・カメラからコンピュータへのデータの転送に関し、より詳細には、記憶デバイス内のデータの埋め込みセキュリティを透過的に与えるため、かつ、デジタル・カメラからコンピュータへ転送中である間にデータを安全に保つ装置に関する。
【０００２】
（従来技術の簡単な説明）
多数の応用例では、写真データが保護される必要があり、すなわち、無許可の閲覧、修正または配布に対して安全にされる必要がある。ネガ、ポジおよびプリントは、いくらかの

努力により処理され、正確な文書画像として使用されるときに保護される必要である。このような場合、元のネガおよびプリントが、典型的には、署名され、封印され、証明された一連の保管により、ロックされた状態に保たれる。デジタル・カメラの出現は、いっそう大きいセキュリティの問題を提示する。デジタル・データが完全に複製することができるので、元のデジタル画像の概念は疑わしいものである。加えて、デジタル画像データは、急速かつ容易にコンピュータで修正することができ、データを、証拠とするためには無用にする。現在、デジタル・カメラ画像データは、直接コンピュータへカメラからある通信機構を介して、あるいは、ＰＣＭＣＩＡカードなどの取外し可能記憶デバイスを通じて、ダウンロードされる。データをコンピュータへダウンロードするとき、画像データを暗号化することができ、あるいは、認証データを作成して無許可の人物がデータを修正することを防止することができる。この点から、解読キーへのアクセスを有するこれらの人物によって、証明された一連の保管を維持することで、大幅にセキュリティ問題が容易になる。

【０００３】

上記の従来技術の記載から、画像データをカメラからダウンロードする前に、あるいはその一部として、カメラ・データを自動的に安全に保つ方法および装置の必要性があることが明らかであろう。このような方法および装置は、デジタル・カメラ・データのセキュリティを大幅に向上させることになる。

【０００４】

（発明の概要）

したがって、本発明の目的は、デジタル・スチールおよびビデオ・カメラからのデータを、カメラからコンピュータへ転送する処理中に、安全に保つ方法および装置を提供することである。

【０００５】

本発明の目的はさらに、デジタル・カメラからのデータをデジタルで保存するための安全記憶デバイスを提供することである。

【０００６】

本発明の目的はさらに、スチールおよびビデオ・カメラからのデータを、カメラからコンピュータへ転送する処理中に、安全に保つ方法および装置を提供することであり、安全に保つ処理がカメラによって検出されない、あるいは、すなわち、カメラに対して透過的であり、したがって、いかなるデジタル・カメラでも使用することができる方法および装置を提供する。

【０００７】

本発明の目的はさらに、ロードされたデジタル・カメラ・データを自動的に暗号化する、安全記憶および／または通信デバイスを提供することである。

【０００８】

本発明の別の目的は、ロードされたデジタル・カメラ・データを自動的に安全に保つ機能を実行中である間に、デジタル・カメラおよび宛先コンピュータによって標準ＰＣＭＣＩＡカードとして受け入れられる、ＰＣＭＣＩＡカードの形式の寸法およびコネクタを有する装置を提供することである。

【０００９】

本発明の目的はさらに、セキュリティ・キーでプログラムすることができ、ロードされた元のデジタル・カメラ・データを自動的に格納し、暗号化された認証データを準備する、安全記憶および／または通信デバイスを提供することである。

【００１０】

本発明の別の目的は、情報を、ロードされたデジタル・カメラ画像データに挿入する、フィンガープリント法を実行する、安全記憶および／または通信デバイスを提供することである。

【００１１】

本発明の目的はさらに、獲得の絶対時間、一意で連続した画像カウンタ、および、一意の

画像およびデバイス識別番号など、追加情報を画像データと共に含む、すなわち、注釈を提供する、安全記憶および／または通信デバイスを提供することである。

【００１２】

簡単には、本発明の好ましい実施態様は、デジタル・カメラ・データの獲得段階で安全に保つための、ＰＣＭＣＩＡカードの外部寸法を有する安全記憶デバイスを含む。元のデジタル・カメラ・データが、安全記憶デバイスのメモリに保存され、これが、暗号化、認証ファイルの作成、フィンガープリント法などデータを画像データへ追加すること、および、画像ヘッダに含まれた別々のデータなどの安全注釈を追加することを含む、１つまたは複数のセキュリティ機能を実行する機能を有する。このデバイスは、元の認証データを元のデジタル・カメラ・データから準備し、元の認証データと元の画像データを共に暗号化し、格納する。このデバイスの使用は、元の画像データを第１のコンピュータへ、暗号化された元の認証データを第２のコンピュータへダウンロードすることを含む。第２のコンピュータは、ソフトウェアによりプログラムすることができ、それにより、暗号化された元の認証データを、キーを有するユーザによって解読することができる。次いで、ソフトウェアにより、ユーザが対応する第２の認証データを、疑わしい認証性の第２の画像データから準備することができる。第２の認証データが元の認証データと同じである場合、疑わしい第２の画像データが、元の画像データの正確なコピーであると見なされる。

【００１３】

本発明の利点は、データを格納かつ転送中である間に安全に保つ方法および装置を提供することであり、そうでない場合、コンピュータへ転送するためのデジタル・カメラから受信された、安全にされていない画像データとなる。

【００１４】

本発明の利点はさらに、カメラからのデジタル・データの一連の保管を安全に保つ方法および装置を提供することであり、そうでない場合、安全にされていない画像データのみを提供する。

【００１５】

本発明の別の利点は、セキュリティ機能を取外し可能記憶デバイスに置くことによって、記憶装置を、カメラまたはＰＣ上の特殊ハードウェアの必要性を有していない特定のユーザ向けにカスタマイズすることができ、そうでなければ受け入れ不可能なカメラの改装を適切なセキュリティ機能性をもって可能にする。

【００１６】

本発明の方法および装置の利点はさらに、提供された処理が検出されない、すなわち、カメラおよびコンピュータに対して透過的であり、結果として、この方法および装置をいかなるデジタル・カメラにも、かつ、ピア・トゥ・ホストおよびピア・トゥ・ピア通信および／または取外し可能記憶装置を利用する様々な他のデバイスに適用することができる。

【００１７】

（好ましい実施形態の説明）

このとき、図１の図を参照すると、本発明の好ましい実施形態の方法および装置が例示される。好ましい実施形態は、電子デジタル信号処理装置を含む。これは安全記憶デバイス１０と呼ばれ、従来技術のデジタル・カメラ１４のＰＣＭＣＩＡカード・スロット１２と物理的に係合するように構成されている。図示のカメラ１４は典型的に、外観上はスチール・カメラであるが、この方法および装置は映画／ビデオ・カメラにも適用される。

【００１８】

本発明の方法によれば、デバイス１０が最初に、カメラからのパスワード／キーの必要性なしに、データをデジタル・カメラから受信し、かつ、カメラ１４からのデータを安全に保つために必要とされる処理を実行するようにプログラムされる。デバイス１０の最初のプログラミングは、固定、ＲＯＭの１度きりのプログラミングのいずれかにすることができ、かつ／またはユーザによってＰＣ１６などのＰＣからダウンロードされたプログラムにすることができる。このプログラミング・データは、追加データと同様に、デバイス１０へ、ＰＣＭＣＩＡ端末１８を通じて、ＰＣ１６の対応するＰＣＭＣＩＡスロット２０か

らロードすることができる。別法として、デバイス１０は、データを、たとえばケーブル・アセンブリ２４によりＰＣ１６の互換性のあるポート２６に接続された入力ポート２２を通じて、受信することができる。デバイス１０は、画像データの暗号化、および／または、暗号化された画像認証データの作成、または透かしを入れることなどを含む、データを安全に保つための様々な処理のいずれをも実行するようにプログラムすることができる。

【００１９】

動作において、プログラムされたデバイス１０はスチール／ビデオ・カメラ１４のスロット１２に挿入される。デバイス１０がデータをカメラ１４から受信するとき、これは、プログラムされた動作を実行し、データを格納する。次いで、デバイス１０がカメラ１４から除去され、コンピュータ１６のＰＣＭＣＩＡスロット２０へ挿入される。デバイス１０は、ＰＣ１６がデバイス１０を、パスワードを提示する必要なしに、ファイル・システム・レベル上で可読ファイルを有する通常の記憶デバイスとして、認識するように構成される。次いで、安全データがデバイス１０からコンピュータ１６へ転送される。ユーザが暗号化されたデータを閲覧するために、コンピュータ１６が、一般にパスワードの入力に応答して、データを解読するようにプログラムされなければならない。

【００２０】

再度図１を参照すると、従来技術によれば、デジタル・カメラ１４がコンピュータ１６へ、カメラ・コネクタ１７からＰＣコネクタ２６への直接ケーブル接続を作る回線２８によって示された、直接ケーブル接続によって接続される。この方法では、安全でないカメラ・データが直接ＰＣ１６へ転送される。次いで、無許可のユーザが容易にＰＣ１６によりデータを修正することができる。本発明の方法および装置は、最初にカメラ・データを安全記憶デバイス１０へ転送し、これが自動的にデータを安全に保つことによって、この問題を解決する。本発明の２つの代替実施形態も図１に示される。

【００２１】

第１の代替実施形態は、安全データ転送デバイス３０を含む。これは、カメラ１４のコネクタ１７からセキュリティ・デバイス３４へ接続するための入力ケーブル・アセンブリ３２を有する。セキュリティ・デバイス３４は、画像データを安全に保つための、デバイス１０に関して論じたものと同じあるいは類似の動作を実行し、データをＰＣ１６へ、出力ケーブル３６を通じて出力し、これは動作においてはＰＣ１６のコネクタ２６へ接続される。デバイス３４はプログラム可能であり、追加データをデバイス１０と同じ方法で、ケーブル・アセンブリ３２または３６を通じた、あるいは別法としてコネクタ３８を通じた、あるいはＰＣＭＣＩＡカードによりＰＣＭＣＩＡカード・スロット４０を通じた、コンピュータへの接続によって受信することができる。

【００２２】

第２の代替実施形態も図１に示され、無線安全データ転送デバイス４２を含む。これは、カメラ１４へケーブル・アセンブリ４６により接続することができるセキュリティ・デバイス４４を含む。デバイス４４はプログラム可能であり、追加データを、ＰＣからケーブル・アセンブリ４６またはコネクタ４８を通じて、あるいはＰＣＭＣＩＡカードによりスロット５０を通じて、受信する。デバイス４４はトランシーバを含み、これは、赤外線トランシーバ５４へデータを伝送する赤外線信号５２を生成するための、変調された赤外線送信部を有し、赤外線トランシーバ５４はその信号を受信して復調し、データをコンピュータ１６へ、ケーブル・アセンブリ５６を通じて出力する。デバイス４４およびトランシーバ５４のトランシーバ特性は、加えて、プログラミングを可能にし、他のデータがＰＣ１６からデバイス４４へ無線赤外線接続を通じて流れることを可能にする。

【００２３】

上記のすべての実施形態では、デバイス１０、３０および４２が、カメラ１４およびＰＣ１６への標準のインタフェースを提示する。カメラから見ると、通信は、ＰＣへの直接接続が行われるかのように見える。同様に、ＰＣが、直接カメラへ向かうように見える接続を観察する。このデバイス１０、３０、４２の透過性の特徴により、本発明の装置および

方法を、いかなるデジタル・カメラ、および、デジタル・カメラ・データを受信するようにプログラムされるいかなるＰＣにも適用することができる。セキュリティがデバイス１０、３０、４２の内側で実行され、カメラまたはＰＣには効果を生じない。

【００２４】

図１のコンピュータ１６は、カメラ・データが転送の宛先を表す。ＰＣが図示されているが、この宛先は、データを受信することができるいかなるコンピュータ化ネットワーク、システムなどにもすることができる。図１は、データ入力接続５９を有する第２の宛先５７も示す。第２の宛先５７は、本発明の方法の重要な代替実施形態を例示するように図示され、ユーザがデバイス１０、３０、または４２の出力を第１の宛先１６へ結び付けて第１の組のデータ、たとえば、暗号化された認証データをダウンロードし、次いで、第２の宛先５７へ結び付けて第２の組のデータ、たとえば、認証された画像データをダウンロードすることができる。

【００２５】

図２は、基本処理をブロック形式において示す。ブロック５８は、デジタル・カメラが、パスワードを提示する必要なしに、元のデジタル・カメラ・データを安全記憶デバイスへ書き込む動作を含む。そのデータは、記憶デバイスによって受信され、安全にされ（ブロック６０）、処理は事前にプログラムされたキーを必要とする。次いで、記憶デバイスが、安全にされたデータを書き込み（ブロック６２）、再度パスワードを受信する必要がなく、コンピュータによって読み取られる（ブロック６４）。この動作では、ユーザが、必要とされるオペレーティング・ソフトウェアをコンピュータにロードしてあると仮定する。次いで、ユーザが、安全データを解読するか、あるいは認証動作を実行するために、パスワード／キーをコンピュータに提示しなければならない（ブロック６５）。

【００２６】

このとき、本明細書に記載された記憶デバイスは、カメラがデータをダウンロードするように設計されている従来技術のデバイスと同じであるようにカメラには見えるように、カメラへ外部挙動／インタフェースを与えることを指摘することが重要である。デジタル・カメラのために設計され、使用された従来技術の記憶デバイスと、本発明の安全デバイスの間の主な違いは、開示されたデバイスがデータ／情報を受信するとき、データを安全に保つための動作を実行することである。これはカメラからのパスワードまたはキーを必要とせずに行われる。これは本発明の重要な特徴である。類似の方法で、コンピュータが安全データを記憶デバイスから、パスワード／キーを与えることなく受信することができる。安全データがコンピュータにロードされた後、安全データを解読するためにキーを与えなければならない。

【００２７】

この方法の利点は、データを従来技術のデジタル・カメラからコンピュータへ安全に転送するために、安全記憶デバイス以外の特殊なプログラミングまたは装置が必要とされないことである。

【００２８】

安全記憶デバイスの好ましい外部物理構成は、標準ＰＣＭＣＩＡカードのものであり、たとえば図１の接続２２がないデバイス１０である。この構成では、ユーザもカメラもコンピュータも安全記憶デバイスを標準のＰＣＭＣＩＡカードから区別することができない。デバイスがデータをカメラから受け入れ、このデバイスが通常のＰＣＭＣＩＡカードであるかのように、標準プロトコルを使用してデータをコンピュータへ送信する。唯一の違いは、データが、暗号化、認証など、様々な手段のいずれかを通じて安全に保たれていることであり、これが以下の明細書において記載される。このデバイスのユニークな性質に関するユーザの唯一の手がかりは、コンピュータへデバイスからロードされた暗号化データが、解読されるまで理解可能にならず、処理が、パスワードおよび／またはキーを含む、特殊なソフトウェアをコンピュータにおいて必要とすることである。図２に例示された新規な点は、ブロック５８、６２および６４において示されるように、データをカメラからデバイスへ、あるいはデバイスからコンピュータへダウンロードするために、パスワード

またはキーが必要とされないことである。この方法により、データの最大のセキュリティが可能となり、標準デジタル・カメラおよびコンピュータの使用を、発見ステップ（ブロック６５）以外のすべての段階について可能にし、ユーザは、暗号化されたデータの解読のために、キーにより適切なソフトウェアをコンピュータへロードしなければならない。

【００２９】

安全記憶デバイスの他の物理的実施形態は、図１を参照して例示され、論じられた通りである。加えて、別法として、デバイス１０をＳＳＦＤＣ（スマート・メディア）カードまたはフラッシュ・カードなどにすることができる。

【００３０】

図３は、デバイス１０内で必要とされる典型的な回路ブロックを例示する。コネクタ／接続１８がデータをカメラ１４からカード・インタフェース６６へ渡し、カメラとの通信のために必要なプロトコルを提供する。バスライン６８が、様々な回路ブロックを必要に応じて相互接続する。一つはメモリ７０であり、ＥＥＰＲＯＭおよび／またはＲＯＭおよびＲＡＭを特定の設計において必要とされるように含むことができる。カード記憶ブロック７２が、データを記憶のために保持してコンピュータへ転送するための、フロッピー・ディスク、またはミニ・ディスクなどの使用を示している。カード・コントローラ７４が標準／通常のカード動作を実行し、追加の処理がプロセッサ７６によって実施され、これは、クロック７８、カウンタ８０、および、追加データ（ブロック８２）をＰＣからコネクタ１８を通じて、あるいは、任意選択でＰＣインタフェース・コントローラ８４を通じてコネクタ２２から受信するための機能を含むことが好ましい。プロセッサは、セキュリティ処理８８を含む、画像処理作業８６も実行する。電源９０が任意選択として設計に含まれ、たとえば、クロックを含み、あるいは電力をカメラおよびコンピュータから得ることができない。

【００３１】

図４は、デバイス３０または４２のための典型的な回路ブロック機能を例示する。デバイス３０は、カメラへのケーブル・コネクタ・アセンブリ３２、コンピュータへのケーブル・コネクタ・アセンブリ３６、およびセキュリティ・デバイス３４を含む。デバイス４２は、ケーブル・コネクタ・アセンブリ４６および５６、および、トランシーバ回路構成５４が追加されたセキュリティ・デバイス３４における回路構成を含むセキュリティ・デバイス４４、および分離したトランシーバ５４を含む。

【００３２】

デバイス３４の回路構成は、カメラ接続コントローラ９２、電源９４、メモリ９６、カード接続５０へのインタフェースを提供する取外し可能記憶装置コントローラ９８、ケーブル・コネクタ・アセンブリ４８および３６へのインタフェースを提供するＰＣインタフェース・コントローラ１００、クロック１０４、カウンタ１０６、追加データ１０８、画像処理１１０およびセキュリティ・エンジン１１２を有するプロセッサ１０２を含む。記憶装置１１４は、データ転送デバイス３０および４２に対して任意選択的であり、カメラからコンピュータへ転送されるデータを格納するためのものであり、フロッピー・ディスク、ミニ・ディスクなどにすることができる。デバイス３０および４２の使用が、カメラおよび宛先へ同時に接続することを含むことが好ましいので、メモリ９６が十分な記憶／バッファリングを提供できるように、データを通常は十分高速で転送することができる。応用例がより長い記憶装置を必要とする場合、任意選択の記憶装置１１４を設計に含めることができる。

【００３３】

図５は、元のデジタル・カメラ・データの暗号化のための、安全記憶デバイス１０、３０、４２の処理を例示する。この処理によれば、記憶デバイスが最初にセキュリティ・キーによりプログラムされる（ブロック１２６）。この動作は、デバイスの初期セットアップとして、その通常の使用より前に行われる。このキー・プログラミングは永久設定にすることができ、あるいはプログラム可能にすることができる。デバイス１０、３０、４２が通常の使用のために準備できると、次いで、これがカメラに接続され、元のデジタル・カ

メラ・データを受信する（ブロック１２８）。次いで、デバイスが元のデジタル・カメラ・データを暗号化する（ブロック１３０）。この後に続いて、デバイスがカメラから除去され、互換性のあるソフトウェアがロードされたコンピュータに接続される。次いで、デバイス１０、３０、４２がデータをコンピュータへ書き込む（ブロック１３２）。次いで、セキュリティ・キーを知っているユーザがコンピュータを操作して、暗号化されたデータを解読する（ブロック１３４）。図２において示された方法を参照して説明したように、デバイス１０、３０、４２は、データをカメラから受信するため、あるいはデータをコンピュータへダウンロードするためにパスワード／キーの受信を必要としない。キーは暗号化処理において使用され、ユーザがコンピュータの使用を通じて元のデータを閲覧したいと望むときの唯一の要素である。

【００３４】

安全記憶デバイスを、認証データを作成するようにプログラムすることもできる。これは、図６において例示される。図５の場合におけるように、記憶デバイスは、デバイスの使用の前に、最初にセキュリティ・キーによりプログラムされる（ブロック１３６）。次いで、デバイスがカメラに接続されて、元のカメラ・データが受信される（ブロック１３８）。次いで、認証データが記憶デバイス内で元のカメラ・データから作成され、次いで暗号化される（ブロック１４０）。

【００３５】

次いで、いかなる人物もカメラ・データをダウンロードすることができ、すなわち、記憶デバイスにカメラ・データ（ブロック１４２）、および認証データ／ファイル（ブロック１４４）をコンピュータへ書き込ませることができる。これで記憶デバイスの機能が完了する。次いで、ユーザが進行して、図７に示されたようにコンピュータを使用して、１組の疑わしいデータの認証性を検証することができる。ユーザがまず適切なソフトウェアおよびキーを使用して、検証認証データを疑わしい画像データ・ファイルから作成し（ブロック１４６）、暗号化された元の認証データを解読する（ブロック１４８）。次いで、この２組のデータが比較される（ブロック１５０）。これらが同じである場合、疑わしい画像データが、有効、すなわち、元の画像データの正確な複製であると見なされる。これらの２組が異なる場合、疑わしいデータが元のものとは異なると確認される。

【００３６】

図８は、２つの類似した、「フィンガープリント法」および「注釈付け(annotationg）」と呼ばれる処理を例示する。フィンガープリント法は、追加情報が可視的あるいは不可視的に画像データ自体に挿入される処理である。追加することができる追加情報の例には、カメラのシリアル番号、日付および時間、一意のカウンタ、画像記憶ＩＤ、および、カメラ画像データを受信する前に記憶デバイスへダウンロードされるいかなるテキスト情報もが含まれる。注釈付けの処理はフィンガープリント法と類似しており、ただし、情報が、画像データではなく、ヘッダなどの非画像領域に配置される。図８を参照すると、記憶デバイスがコンピュータに接続され、必要とされたデータが入力され、すなわち、ダウンロードされる（ブロック１５２）。これは、ＰＣＭＣＩＡカードが構成されたデバイス１０のための接続１８を通じて、あるいは、代替デバイス１０のコネクタ２２を通じて行うことができる。デバイス４２は図４に示されたように構成されて、データを、ポート４８を通じてあるいはケーブル・アセンブリ４６を通じてあるいはケーブル・アセンブリ５０を通じてＰＣから、あるいはポート５６を通じてＰＣから、あるいはポート５０を通じてＰＣＭＣＩＡカードから、受信する。同様に、デバイス３０は、データを、別法として、ケーブル・アセンブリ３２または３６を通じて、あるいはコネクタ３８を通じてＰＣから、あるいはポート４０を通じてＰＣＭＣＩＡカードから、受信するように構成される。次いで、記憶デバイスがカメラに接続され、カメラ・データを受信し、すなわち、カメラ・データがダウンロードされる（ブロック１５４）。次いで、デバイスが、データをフィンガープリントするかあるいはデータ・ファイルに注釈を付けるかの、プログラムされた処理（ブロック１５６）を、記憶デバイスの特定のプログラミングに応じて実行する。次いで、記憶デバイスがカメラから除去され、コンピュータへ接続され、データが書き込まれ、

すなわち、コンピュータへダウンロードされる（ブロック１５８）。上記で説明したように、これはすべて、カメラまたはコンピュータからのパスワードまたはキーの提示なしに行われる。しかし、データがコンピュータに入った後、元のデータまたは認証が、パスワード／キーの提出を必要とする。

【００３７】

いくつかの場合、署名ファイルまたは認証ファイルを安全な専用位置に保ち、パブリック・アクセスを認証された画像にのみ可能にすることが好ましい。これらの処理が図９に例示されている。画像データがカメラ１６０から安全記憶デバイス１６２へダウンロードされ、これが必要とされるセキュリティ機能を実行する。次いで、デバイス１６２が画像セキュリティ・データを安全位置１６４へ、認証された画像をパブリック・アクセス１６６へダウンロードする。

【００３８】

本発明を、特定の実施形態に関して上記に記載したが、この変更および修正は、当業者には疑いなく明らかになるであろうことが予想される。したがって、以下の特許請求の範囲が、本発明の真の精神および範囲内に入るこのようなすべての変更および修正を包含するとして解釈されることが、意図されるものである。

【図面の簡単な説明】

【図１】　データを転送するための本発明の使用を例示する斜視図である。

【図２】　安全データ転送の方法ステップを示すブロック図である。

【図３】　安全記憶デバイスのブロック図である。

【図４】　安全データ転送デバイスのブロック図である。

【図５】　データ暗号化による安全データの転送を例示する図である。

【図６】　認証データの作成を通じた安全データ転送のための記憶デバイスを例示する図である。

【図７】　認証データの使用を通じて画像データ認証性を検証するためのホスト・コンピュータの処理を例示する図である。

【図８】　フィンガープリント法および／または注釈による安全データ転送の方法を示す図である。

【図９】　安全にされたデータを安全記憶デバイスから第１の位置へ、パブリック・データを第２の位置へ送信することを例示する図である。

【図１】

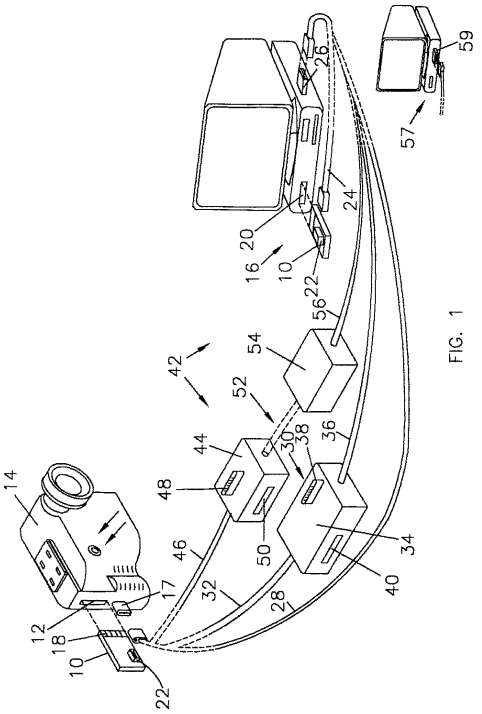
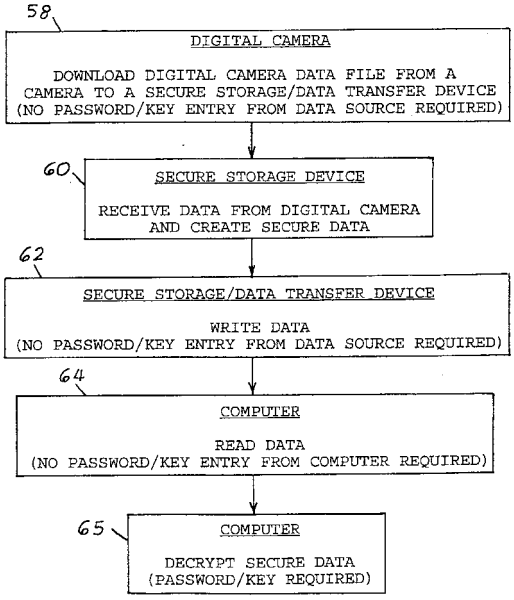


FIG. 1

【図２】



５８　デジタル・カメラ
デジタル・カメラ・データ・ファイルをカメラから安全記憶／データ転送デバイスへダウンロードする
（データ・ソースからのパスワード／キー入力が必要とされない）

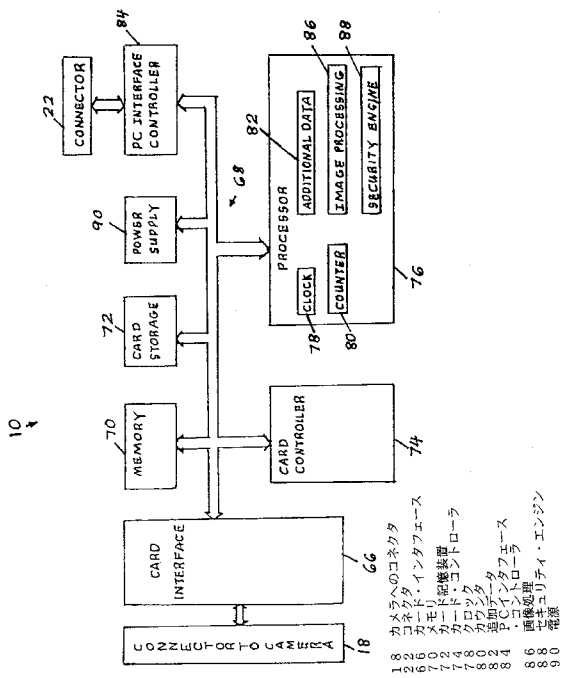
６０　安全記憶デバイス
データをデジタル・カメラから受信し、安全データを作成する

６２　安全記憶／データ転送デバイス
データを書き込む
（データ・ソースからのパスワード／キー入力が必要とされない）

６４　コンピュータ
データを読み取る
（コンピュータからのパスワード／キー入力が必要とされない）

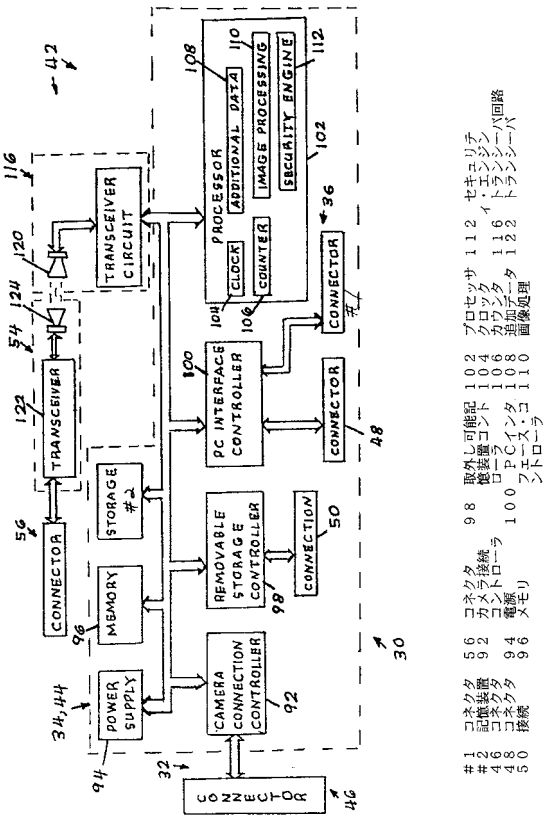
６５　コンピュータ
安全データを解読する
（パスワード／キーが必要とされる）

【図３】



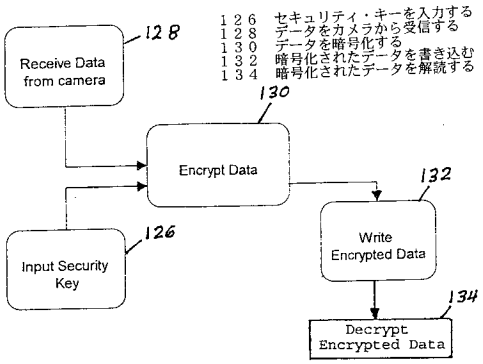
１８　カメラへのコネクタ
２２　コネクタ・インタフェース
６６　カード記憶装置
７０　メモリ
７２　カード・コントローラ
７４　カード・インタフェース
７６　カウンタ
７８　追加データ
８２　P.C.インタフェース・コントローラ
８４　P.C.コントローラ
８６　画像処理
８８　セキュリティ・エンジン
９０　電源

【図４】

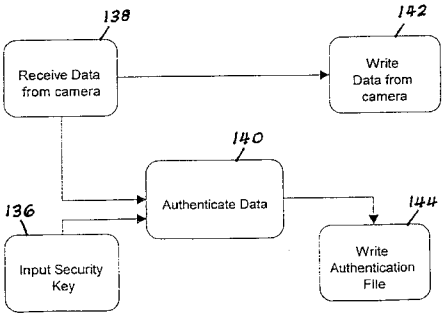


#1　コネクタ　56　取外し可能記憶装置　98
#2　記憶装置　92　コネクタ　102　プロセッサ　112　セキュリティ・エンジン
46　コネクタ　94　コントローラ　104　クロック　116　トランシーバ回路
48　コネクタ　96　電源　106　カウンタ　122　トランシーバ
50　接続　96　メモリ　108　追加データ　100　PCインタフェース・コントローラ　110　画像処理

【図５】

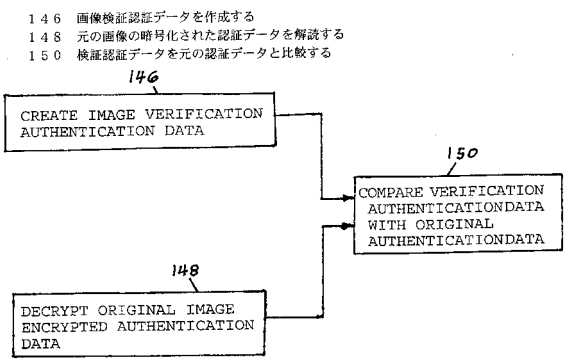


【図６】

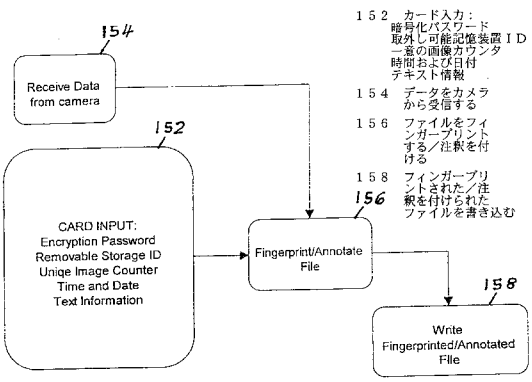


136 セキュリティ・キーを入力する
138 データをカメラから受信する
140 データを認証する
142 データをカメラから書き込む
144 認証ファイルを書き込む

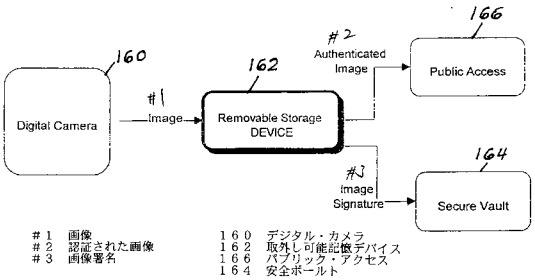
【図７】



【図８】



【図９】



#１ 画像
#２ 認証された画像
#３ 画像署名
160 デジタル・カメラ
162 取外し可能記憶デバイス
166 パブリック・アクセス
164 安全ボールト

フロントページの続き

合議体
審判長　藤内　光武
審判官　小池　正彦
審判官　佐藤　直樹

(56)参考文献　特開平１０－１０５６５８（ＪＰ，Ａ）
国際公開第９７／３６４２６（WO，Ａ１）
米国特許第５７５１８０９（ＵＳ，Ａ）
米国特許第５０２７４０１（ＵＳ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04N5/76-5/956,G06F12/14