(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2007-215162
(P2007-215162A)
(43)公開日　平成19年8月23日(2007.8.23)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601A	5J104
		H04L	9/00	601E	

審査請求 未請求　請求項の数 14　OL　（全 24 頁）

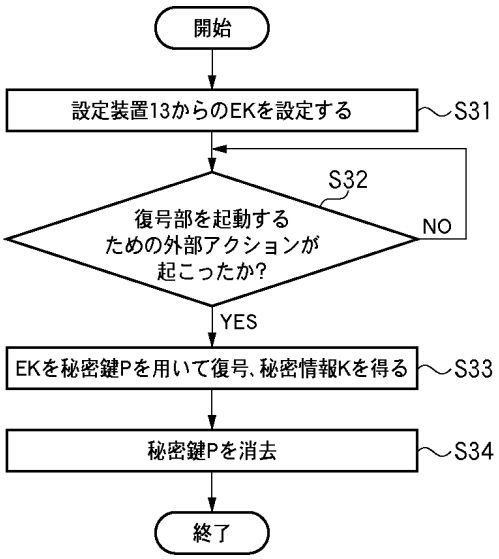
(21)出願番号　特願2006-350498 (P2006-350498)
(22)出願日　平成18年12月26日 (2006.12.26)
(31)優先権主張番号　特願2006-4194 (P2006-4194)
(32)優先日　平成18年1月11日 (2006.1.11)
(33)優先権主張国　日本国 (JP)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　林　淳一
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置及びその制御方法、プログラム、記憶媒体

(57)【要約】
【課題】　従来の手法よりも向上された安全性を確保しつつ秘密情報を装置に設定する技術を提供する。
【解決手段】　秘密情報を生成する情報処理装置であって、鍵情報を予め記憶する記憶手段と、演算対象情報を入力する入力手段と、対象とする情報に対して、前記記憶手段に記憶された前記鍵情報に基づき演算を行う演算手段と、予め定められたイベントを検出する検出手段と、前記検出手段において前記イベントが検出されたことを契機として、入力された前記演算対象情報を前記対象とする情報として前記演算手段に前記演算を行わせることで、前記秘密情報を生成するとともに、前記記憶手段に記憶されている前記鍵情報を利用不可能な状態となるように制御する、制御手段とを備える。
【選択図】　図３



【特許請求の範囲】
【請求項１】
秘密情報を生成する情報処理装置であって、
鍵情報を予め記憶する記憶手段と、
演算対象情報を入力する入力手段と、
対象とする情報に対して、前記記憶手段に記憶された前記鍵情報に基づき演算を行う演算手段と、
予め定められたイベントを検出する検出手段と、
前記検出手段において前記イベントが検出されたことを契機として、入力された前記演算対象情報を前記対象とする情報として前記演算手段に前記演算を行わせることで、前記秘密情報を生成するとともに、前記記憶手段に記憶されている前記鍵情報を利用不可能な状態となるように制御する、制御手段と
を備えることを特徴とする情報処理装置。
【請求項２】
前記制御手段は、前記鍵情報を利用不可能な状態とするために、前記記憶手段から前記鍵情報を消去する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項３】
撮像手段と、
前記撮像手段において撮像された画像データと、前記生成された秘密情報と、に基づいて、該画像データの改竄検出において用いられる改竄検出情報を生成する生成手段と、
をさらに備えることを特徴とする請求項１に記載の情報処理装置。
【請求項４】
撮像手段と、
前記生成された秘密情報を用いて、前記撮像手段において撮像された画像データを暗号化する暗号化手段と、
をさらに備えることを特徴とする請求項１に記載の情報処理装置。
【請求項５】
前記演算対象情報は暗号化された前記秘密情報であり、
前記鍵情報は、暗号化情報を復号するための復号鍵情報であり、
前記演算は、前記暗号化された前記秘密情報を前記鍵情報に基づいて復号する処理である
ことを特徴とする請求項１に記載の情報処理装置。
【請求項６】
前記演算対象情報は、前記情報処理装置に対応する公開情報であり、
前記鍵情報は暗号化処理を行うための暗号化鍵情報であり、
前記演算は、前記公開情報を前記鍵情報に基づいて暗号化する処理である
ことを特徴とする請求項１に記載の情報処理装置。
【請求項７】
前記イベントは、正当なパスワード情報の入力、正当な生体情報の入力、初めての電源投入、予め定められた装置の初めての操作、予め定められた操作のいずれかである
ことを特徴とする請求項１に記載の情報処理装置。
【請求項８】
鍵情報を予め記憶する記憶手段を備え、秘密情報を生成する情報処理装置の制御方法であって、
入力手段が、演算対象情報を入力する入力工程と、
検出手段が、予め定められたイベントを検出する検出工程と、
前記検出工程において前記イベントが検出されたことを契機として、制御手段が、入力された前記演算対象情報に対して前記記憶手段に記憶された前記鍵情報に基づき演算を行うことで、前記秘密情報を生成するとともに、前記記憶手段に記憶されている前記鍵情報

を利用不可能な状態となるように制御する、制御工程と
を備えることを特徴とする情報処理装置の制御方法。
【請求項９】
前記制御工程は、前記鍵情報を利用不可能な状態とするために、前記記憶手段から前記鍵情報を消去する
ことを特徴とする請求項８に記載の情報処理装置の制御方法。
【請求項１０】
前記演算対象情報は、暗号化された前記秘密情報であり、
前記鍵情報は、暗号化情報を復号するための復号鍵情報であり、
前記演算は、前記暗号化された前記秘密情報を前記鍵情報に基づいて復号する処理である
ことを特徴とする請求項８に記載の情報処理装置の制御方法。
【請求項１１】
前記演算対象情報は、前記情報処理装置に対応する公開情報であり、
前記鍵情報は、暗号化処理を行うための暗号化鍵情報であり、
前記演算は、前記公開情報を前記鍵情報に基づいて暗号化する処理である
ことを特徴とする請求項８に記載の情報処理装置の制御方法。
【請求項１２】
前記イベントは、正当なパスワード情報の入力、正当な生体情報の入力、初めての電源投入、予め定められた装置の初めての操作、予め定められた操作のいずれかである
ことを特徴とする請求項８に記載の情報処理装置の制御方法。
【請求項１３】
コンピュータを請求項１乃至７のいずれか１項に記載の情報処理装置として機能させるためのプログラム。
【請求項１４】
請求項１３に記載のプログラムを格納したコンピュータで読み取り可能な記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、秘密情報を装置に設定する技術に関する。
【背景技術】
【０００２】
近年、デジタルカメラが急速に普及している。デジタルカメラで撮影された画像は、電子的な画像データとして記憶保管することが可能である。このため、従来の銀塩写真のように現像、プリントといった手間が省けるだけでなく、経年劣化がない、保管や検索が容易に行える、データを通信回線を用いて遠隔地に送信できるといった様々なメリットがある。このような理由により、多くの業務分野でデジタルカメラが利用されている。
【０００３】
例えば、事故車の破損状況を撮影し、撮影された画像に基づいて事故査定を行う損害保険業界、建設現場での工事の進捗状況や仕様の確認のために建築物を撮影する建設業界が挙げられる。国土交通省では既に土木工事現場の記録用にデジタルカメラで撮影された画像の使用を認めている。
【０００４】
しかし、デジタル化されることによるデメリットも指摘されている。それは、市販のフォトレタッチツール等のアプリケーションプログラムを使用することで、パーソナルコンピュータ上で容易に加工や修正が出来てしまうことである。即ち、加工や修正が容易であるが故に、画像が証拠として扱われる事故の写真や報告書において、デジタルカメラで撮影された画像の信頼性が銀塩写真の画像と比較して低くなってしまうという点である。
【０００５】
銀塩写真でも画像の改変を行うことは不可能ではないが、その改変を行うためのコスト

が改変で得られるコストよりも非常に大きいか、画像の改変結果が不自然であることから実際には改変は行われにくく、それが証拠として採用される根拠になっている。従って損害保険業界、建設業界ではこの問題が将来大きな問題になることが懸念されており、このような欠点を克服するための仕組みが必要とされている。

【０００６】

現在では、暗号技術を利用したデジタル署名データによる画像データの改竄検出システムが提案されている（特許文献１）。

【０００７】

このシステムは、画像データを生成する画像生成装置（カメラ）と、画像データの完全性（改変されていないこと）を検証する画像検証装置で構成される。カメラは、カメラ固有の秘密情報と、撮影してデジタル化した画像データとに基づいて所定の演算を実行し、画像データを識別する情報（改竄を検知する）であるデジタル署名データを生成する。そして、デジタル署名データと画像データとを出力する。画像検証装置では、所定の演算を画像データに施した結果のデータと、デジタル署名データを上記生成時の演算の逆演算を施したデータとを比較することで検証を行う。また、上記特許ではデジタル署名データの生成にハッシュ関数（圧縮関数）と公開鍵暗号を使用している。

【０００８】

また、上記のデジタル署名データの代わりにＭＡＣ（Message Authentication Code）が用いられることもある。ＭＡＣは共通鍵暗号やハッシュ関数等を使用して生成されるものであり、処理速度が公開鍵暗号よりも高速であることが特徴である。しかし、ＭＡＣの生成、及び、検証に同一の共通鍵が用いられるため、共通鍵をカメラと画像検証装置の双方において厳重に管理する必要がある。

【０００９】

カメラで撮像した画像データは通常、カメラに接続されている小型のメモリーカード（不揮発性メモリ）に記憶され、メモリーカードは主としてフラッシュＥＥＰＲＯＭによって構成される。最近の微細化技術によりメモリの高密度化が図られており、４ｃｍ四方の面積、高さ２～３ｍｍ程度のメモリーカードで数百Ｍバイトの記憶容量を持つものが製品化されている。さらに、上記フラッシュＥＥＰＲＯＭに加えてＣＰＵ、ＲＡＭ、ＲＯＭで構成される演算部を持ち、セキュリティー機能を実装している、メモリーカードやＩＣカードが実用化されつつある。これらの演算機能を用いることにより、カメラの外部である、メモリーカードやＩＣカードにおいて、画像データ等の改竄を検出するためのデータを生成することが可能となっている。

【特許文献１】米国特許第５４９９２９４号公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

特許文献１に開示された構成のように、デジタル署名データやＭＡＣ等の検証用データを用いて、画像データ等のデータの改竄を検出する、カメラ等の画像生成装置に係る構成を考える。上述のように、このような構成においては検証用データを生成する際に鍵データを用いるが、この鍵データが流出すると改竄防止に係る安全性が保たれない。このため、鍵データ等の秘密管理が要求される秘密情報を、画像生成装置等の装置に対し、安全性を確保しながら設定することが必要となる。

【００１１】

このような安全性を確保して秘密情報を設定する手法としては、以下のものが考えられる。

（１）秘密情報を暗号化し、装置内部で復号する。ただし、暗号化された秘密情報の復号は復号鍵を用いて行う。

（２）公開情報を装置へ入力し、予め設定された鍵情報を用いて、装置内部で秘密情報を生成する。

【００１２】

しかし、これらの手法は、不正な解析等により装置内部の鍵情報が漏洩すると、秘密情報が流出してしまう。

【００１３】

本発明は上記問題に鑑みなされたものであり、従来の手法よりも向上された安全性を確保しつつ秘密情報を装置に設定する技術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】

【００１４】

上記目的を達成するため、本発明による情報処理装置は以下の構成を備える。即ち、秘密情報を生成する情報処理装置であって、鍵情報を予め記憶する記憶手段と、演算対象情報を入力する入力手段と、対象とする情報に対して、前記記憶手段に記憶された前記鍵情報に基づき演算を行う演算手段と、予め定められたイベントを検出する検出手段と、前記検出手段において前記イベントが検出されたことを契機として、入力された前記演算対象情報を前記対象とする情報として前記演算手段に前記演算を行わせることで、前記秘密情報を生成するとともに、前記記憶手段に記憶されている前記鍵情報を利用不可能な状態となるように制御する、制御手段とを備える。

【００１５】

また、本発明による情報処理装置の制御方法は以下の構成を備える。即ち、鍵情報を予め記憶する記憶手段を備え、秘密情報を生成する情報処理装置の制御方法であって、入力手段が、演算対象情報を入力する入力工程と、検出手段が、予め定められたイベントを検出する検出工程と、前記検出工程において前記イベントが検出されたことを契機として、制御手段が、入力された前記演算対象情報に対して前記記憶手段に記憶された前記鍵情報に基づき演算を行うことで、前記秘密情報を生成するとともに、前記記憶手段に記憶されている前記鍵情報を利用不可能な状態となるように制御する、制御工程とを備える。

【発明の効果】

【００１６】

本発明によれば、従来の手法よりも向上された安全性を確保しつつ秘密情報を装置に設定する技術を提供することができる。

【発明を実施するための最良の形態】

【００１７】

以下、添付図面を参照して本発明に係る実施の形態を詳細に説明する。ただし、この実施の形態に記載されている構成要素はあくまでも例示であり、本発明の範囲をそれらのみに限定する趣旨のものではない。

【００１８】

＜＜第１実施形態＞＞

（装置構成）

図１は本実施形態に係る情報処理装置が含まれるシステム構成を例示的に示したブロック図である。図１のように、本実施形態においては本実施形態に係る情報処理装置としての画像生成装置１１と、秘密情報生成機関１２と、秘密情報設定機関１３が存在する。

【００１９】

[画像生成装置１１]

画像生成装置１１は、基本的には、画像処理部１４と検証用データ生成処理部１５とＲＯＭ１６と復号処理＆秘密鍵消去処理部１７等の機能構成を有する。

【００２０】

画像処理部１４は、画像データを生成/撮影する機能と、補助パラメータを生成する機能と、検証用データ付き画像ファイルを生成する機能等を有する。ただし、画像生成装置１１がカメラの場合、補助パラメータには、例えば、撮影時刻、焦点距離、絞り値、ＩＳＯ感度、測光モード、画像ファイルサイズ、撮影者情報等が含まれる。また、検証用データ付き画像ファイルは、例えば、画像データ、検証用データ（改竄検出情報）、補助パラメータ等で構成される。

【００２１】

検証用データ生成処理部１５は、検証用データ作成用の秘密情報と画像生成装置１１固有の公開情報を設定する機能と、生成した画像データに対する検証用データを生成する機能等を有する。

【００２２】

ＲＯＭ１６は、秘密鍵を安全に保持・管理する機能等を有する。例えば、耐タンパ技術を用いることで秘密鍵を安全に管理することができる。なお、ＲＯＭ１６は、後述するように、例えば、上書きの指示の入力等によって格納された情報を消去する機能を有する。このため、本実施形態において、ＲＯＭ１６は厳密な意味での読み出し専用メモリ（Read-Only Memory）ではない。なお、ＲＯＭ１６は、所定の指示入力によって、秘密鍵へのアクセスを除外する処理を行うメモリ装置によっても構成することができる。この場合、後述の秘密鍵の「消去」は、秘密鍵へのアクセスを除外するための処理の指示をＲＯＭ１６に入力することに該当する。

【００２３】

復号処理＆秘密鍵消去処理部１７は以下のような機能を有する。

・演算対象情報としての、暗号化された検証用データ作成用の秘密情報を、上記の秘密鍵を用いて復号する機能。

・上記復号する機能の初回実行時を判定する機能。

・上記初回実行後に秘密鍵をＲＯＭ１６から消去する機能。

ただし、後述するように、暗号化された秘密情報は秘密情報設定機関１３により設定される。

【００２４】

なお、本実施形態に係る情報処理装置としての画像生成装置１１は、デジタルカメラ、デジタルビデオカメラ、スキャナなどの撮像装置や、カメラユニットを有する電子機器、カメラが接続されたコンピュータ装置、携帯電話、ＰＤＡ等により実現される。以下、簡単のため、画像生成装置１１はカメラとして説明する。

【００２５】

[秘密情報生成機関１２]

秘密情報生成機関１２は、上記のカメラ１１固有の秘密情報を管理する機能と、暗号化鍵情報としての秘密鍵を用いて秘密情報を暗号化する機能と、暗号化された秘密情報を秘密情報設定機関１３へ配送する機能等を有する。ただし、秘密鍵及び秘密情報は秘密情報生成機関１２において安全に管理されているが、配送中の経路は安全性が保証できない、即ち、配送中のデータが外部から参照される可能性があるものとする。

【００２６】

なお、秘密情報生成機関１２は、例えば、ＰＣ（Personal Computer）やＷＳ（workstation）、ＰＤＡ（Personal Digital Assistance）等の情報処理装置により実現することができる。そして、例えば、情報処理装置にデータを蓄積し、該データを配信可能なＷｅｂサーバとして機能するようにソフトウェアをインストールするように構成することができる。

【００２７】

また、秘密情報生成機関１２から秘密情報設定機関１３への情報の配送は、例えば、トラックや郵便のような物理的な配送システムやインターネットに代表されるネットワークを経由して電子的通信によって行われる。

【００２８】

以下、簡単のため、秘密情報生成機関１２はＰＣにより実現されるものとし、そのＰＣを生成装置１２と呼んで説明する。

【００２９】

[秘密情報設定機関１３]

秘密情報設定機関１３は、生成装置１２から配送された、暗号化された秘密情報を受け取る機能と、暗号化された秘密情報をカメラ１１に設定する機能等を有する。なお、秘密情報設定機関１３は、郵便物として送られてきた暗号化された秘密情報を受け取り、カメ

ラ１１に設定する機関であってもよい。或いは、ＰＣとして実現され、ＵＳＢメモリやネットワークを介して配送された上記暗号化された秘密情報を受け取り、カメラ１１に設定する機能を有する構成でもよい。以下、簡単のため、秘密情報設定機関１３はＰＣとして実現されるものとし、そのＰＣを設定装置１３と呼んで説明する。

【００３０】

なお本実施形態では、説明の便宜のため、カメラ１１、生成装置１２、設定装置１３をそれぞれ１つの装置で実現した構成について述べるが、複数の装置にリソースを分散した構成によって実現してもよい。例えば、記憶や演算のリソースを複数の装置に分散した形に構成してもよい。或いは、装置上で仮想的に実現される構成要素毎にリソースを分散し、並列処理を行うようにしてもよい。

【００３１】

（前提）

次に、処理の前提として、各装置が有するデータについて説明する。

【００３２】

生成装置１２は、図５に示すように予め定められた秘密鍵Ｐ及び秘密情報Ｋ、公開情報Ｉを、鍵管理部５１、秘密情報管理部５２及び公開情報管理部５６に格納して保有する。この秘密鍵Ｐ及び秘密情報Ｋは数値を表し、所定のビット長をもつ数値として設定される。公開情報Ｉは、カメラ１１固有の情報にバインド、即ち、関連づけられている。カメラ固有の情報には、例えば、カメラを識別する識別情報としてのカメラＩＤ、製造番号、シリアル番号等が含まれる。一方、秘密鍵Ｐは全てのカメラ１１に共通の情報である。

【００３３】

なお、秘密情報Ｋは、公開情報Ｉと上記Ｐとは異なる秘密鍵Ｐ'を入力とし、所定の関数による演算により出力されたデータを用いることができる。ここで、秘密鍵Ｐ‘も、秘密鍵Ｐと同様に全てのカメラ１１に共通のデータであるものとする。

【００３４】

ここで上記所定の関数とは、数式で表すと、Ｋ＝Ｅ(Ｉ,Ｐ')のようなＥ( )を指す。Ｅ( )には、共通鍵暗号、公開鍵暗号、ＭＡＣ、ハッシュ関数等に係る演算を適用することができる。Ｅ( )として共通鍵暗号に係る演算を用いる場合、Ｅ（ｘ，ｙ）は平文ｙを鍵ｘで暗号化すれば良い。或いは、Ｅ（ ）としてハッシュ関数に係る演算を用いる場合、Ｅ（ｘ，ｙ）はメッセージｘとメッセージｙを連結したメッセージに対するハッシュ値を算出すれば良い。何れの場合も、生成された秘密情報Ｋは、全てのカメラ１１に共通の秘密情報Ｐ‘からカメラ毎に異なる公開情報Ｉを用いて生成される。結果として、秘密情報Ｋはカメラ１１固有の情報と言える。

【００３５】

尚、本実施形態では、公開情報Ｉは公開情報管理部５６に予め保有しているものとして説明をするが、本発明はこれに限定されることない。例えば、秘密情報Ｋを生成する際に、動的にカメラ１１毎に異なる値を発生させ、発生した値を公開情報Ｉとして利用するようにしても良い。この場合、不図示の乱数生成器等を用いて生成した乱数を公開情報Ｉとして利用することが可能である。また、発生した公開情報Ｉを公開情報管理部５６に記録するようにしても良い。

【００３６】

ここで、生成装置１２の構成について図５を参照して説明する。図５は、秘密情報生成機関（生成装置）１２の詳細な構成を模式的に示したブロック図である。

【００３７】

図５において、鍵管理部５１は秘密鍵Ｐを管理する機能要素であり、例えば、耐タンパ技術が施されたメモリ装置等により実現することができる。秘密情報管理部５２は、秘密情報Ｋを管理する機能要素であり、例えば、耐タンパ技術が施されたメモリ装置等により実現することができる。暗号化部５３は、共通鍵暗号、公開鍵暗号等の暗号処理を実行する機能要素である。公開情報管理部５６は、カメラ１１の公開情報Ｉを管理する機能要素である。

【００３８】
なお、配送部５４、制御部５５の説明は、その機能要素を利用する処理の説明とともに示される。
【００３９】
（秘密情報暗号化処理）
次に、生成装置１２による秘密情報の暗号化及び設定装置１３への秘密情報の配送に係る処理（秘密情報暗号化処理）の流れについて、図６を参照して説明する。図６は秘密情報暗号化処理の流れを示したフローチャートである。
【００４０】
まず、秘密情報管理部５２に保持されているカメラ１１毎に異なる秘密情報Ｋを、暗号化部５３にロードする。（ステップＳ６１）。
【００４１】
次に、鍵管理部５１に保持されている暗号化鍵情報としての秘密鍵Ｐを用いて、入力された秘密情報Ｋを暗号化する（ステップＳ６２）。暗号化された秘密情報をＥＫとする。
【００４２】
次に、上記のＥＫを配送部５４を用いて設定装置１３へ送出する（ステップＳ６３）。
【００４３】
ただし、鍵管理部５１及び秘密情報管理部５２は、秘密鍵Ｐ及び秘密情報Ｋを暗号化部５３のみがアクセスできるように保持するメモリである。暗号化部５３以外の外部は秘密鍵Ｐ及び秘密情報Ｋを読み出すことができないため、秘密鍵Ｐ及び秘密情報Ｋの漏洩が防止される。鍵管理部５１、秘密情報管理部５２は、例えば、パスワードや正当なユーザの生体情報等を用いてアクセス制御を行うように構成することができ、或いは、公知の耐タンパ技術を用いて構成することができる。
【００４４】
暗号化部５３は、秘密情報Ｋを、秘密鍵Ｐと所定の関数を用いて暗号化するＣＰＵ（演算装置）によって構成することができる。この所定の関数は、数式で表すと、ＥＫ＝Ｅ'(Ｋ,Ｐ)のようなＥ'( )に相当する。Ｅ'( )は、共通鍵暗号、公開鍵暗号、ＭＡＣ等に基づくアルゴリズムを適用することができるが、以後Ｅ'( )は共通鍵暗号として説明する。
【００４５】
配送部５４は、外部とネットワークを経由して通信する通信装置で構成されてもよいし、ＵＳＢメモリのような媒体を通して、トラックや郵便等の配送システムによって配送を行ってもよい。
【００４６】
制御部５５は上述の処理を制御するものである。
【００４７】
（暗号化情報設定処理）
次に、設定装置１３が、生成装置１２から上記の暗号化された秘密情報ＥＫを受け取り、カメラ１１へ上記のＥＫを設定する手順について、図８を用いて説明する。図８は暗号化情報設定処理の流れを示したフローチャートである。
【００４８】
まず、受取部７２にて、設定装置１３は生成装置１２から配送されたＥＫを受け取る（ステップＳ８１）。ただし、受取部７２は秘密情報設定機関（設定装置）１３の機能要素の一つである。図７は、秘密情報設定機関（設定装置）１３の詳細な構成を模式的に示したブロック図である。図７のように、設定装置１３は、カメラと通信する通信部７１と、生成装置１２から暗号化された秘密情報ＥＫを受けとる受取部７２とを備えている。
【００４９】
受取部７２は、配送部５４に対応する受取装置を有している。例えば、ＥＫが生成装置１２の配送部５４によりネットワークを介して配送されてきた場合、受取部７２は、ネットワーク経由で暗号化された秘密データＥＫを受け取る。また、ＥＫが配送部５４により郵便により配送されてきた場合は、郵便物を受け取ることで、ＥＫを受け取る。

【００５０】
次に、通信部７１は、受け取ったＥＫをカメラ１１に設定する（ステップＳ８２）。通信部７１は、例えば、設定装置１３とカメラ１１とがネットワークによって接続されている状況において、受取部７２により受け取られたＥＫを、カメラ１１の秘密情報管理部２２に書き込む。ただし、秘密情報管理部２２は、秘密情報を管理する機能要素であり、例えば、情報漏洩のために耐タンパ技術が施された、フラッシュメモリ、ＨＤ等の不揮発性メモリ装置等により実現することができる。また、設定装置１３とカメラ１１との接続は、ネットワークに限定されず、例えば、ＵＳＢメモリやメモリーカードのような物理的記憶媒体を介した情報転送も含まれる。
【００５１】
（秘密情報復元処理）
次に、カメラ１１による、上記暗号化された秘密情報ＥＫの復号、及び、復号用の秘密鍵Ｐの消去等に関する処理手順について、図３を用いて説明する。図３は秘密情報復元処理の流れを示したフローチャートである。
【００５２】
カメラ１１は、処理の前提として、予め定められた秘密鍵Ｐを図２に示すＲＯＭ１６に有する。この秘密鍵Ｐは生成装置１２が保持する秘密鍵Ｐと同じ鍵である。なお、図２は、カメラ１１の詳細な構成を模式的に示したブロック図である。カメラ（画像生成装置）１１を構成する各機能要素の説明は、その機能要素を利用する処理の説明とともに示される。
【００５３】
図３の説明に戻る。まず、設定装置１３により、通信部２４を介して秘密情報管理部２２に暗号化された秘密情報ＥＫが設定される（ステップＳ３１）。ただし、通信部２４は通信部７１と同様である。即ち、設定装置１３等との通信を行うための通信インタフェースとして、例えば、ＬＡＮカード、無線ＬＡＮカード、無線アンテナ等により実現することができる。また、例えば、ＵＳＢメモリやメモリーカードのような物理的記憶媒体のメディアインタフェースにより通信部２４を実現することができる。なお、暗号化された秘密情報の設定は、例えば、予め定められたディレクトリに所定のファイル名のファイル（ＥＫ）をコピーすることにより行われる。
【００５４】
次に、ステップＳ３２において、復号処理＆秘密鍵消去処理部１７は、復号部１０２を起動するか否かを判定する。ただし、復号部１０２は復号処理＆秘密鍵消去処理部１７の機能要素の一つである。
【００５５】
ここで、復号処理＆秘密鍵消去処理部１７の機能構成について図１０を参照して説明する。図１０は、復号処理＆秘密鍵消去処理部１７の機能要素を示したブロック図である。図１０において、秘密情報復号処理起動部１０１は、復号部１０２を起動するか否かを判定する処理を行う。復号部１０２は、暗号化された秘密情報ＥＫを復号する処理を行う。秘密鍵消去部１０３は、秘密鍵Ｐをカメラ１１から消去する処理を行う。
【００５６】
復号処理＆秘密鍵消去処理部１７は、ステップＳ３２においては、秘密情報復号処理起動部１０１によって、復号部１０２を起動するか否かを判定する。ただし、この判定は、予め定められた外部からのアクション（イベント）が発生したか否かに基づいて行う。このアクションは、例えば、通信部２４もしくは画像処理部１４の操作部９４を介して、外部からパスワードや生体情報が入力され、秘密情報復号処理起動部１０１が正しい情報であると認識したこととすることができる。
【００５７】
パスワードの正当性の検証は、例えば、次のように行うことができる。即ち、カメラ１１の製造番号（シリアル番号）に対応するパスワードを予めカメラ１１に設定しておき、カメラ１１の出荷時にそのパスワードを記載した書面（例えば、顧客登録カード等）を製

品パッケージに同封する。そして、カメラ１１の制御部２３は、ユーザが顧客登録カード等を参照して入力したパスワードと、予め設定されたパスワードとが一致した場合に入力されたパスワードが正当であると判断する。

【００５８】

また、生体情報の正当性の検証は、例えば、次のように行うことができる。即ち、カメラ１１の製造者は、予め、ユーザの生体情報（例えば、指紋情報、声紋情報、虹彩情報等）を取得しておき、そのユーザにカメラ１１を提供する際に、そのユーザの生体情報をカメラ１１に設定する。そして、カメラ１１の制御部２３は、ユーザにより入力された生体情報と、予め設定された生体情報とが一致した場合に入力された生体情報が正当であると判断する。

【００５９】

なお、アクションはこれらに限られないことは言うまでもない。なお、このアクションを通常の操作においては余り行わないユニークな操作にすることで、安全性がより高められるであろう。

【００６０】

ステップＳ３２において復号部１０２を起動すると判定されなかった場合（ステップＳ３２でＮＯ）は、上記アクションが発生するまで待機する。上記アクションが発生した場合（ステップＳ３２でＹＥＳ）には、ステップＳ３３へ進む。

【００６１】

ステップＳ３３では、復号部１０２が、暗号化された秘密情報ＥＫの復号処理を実行する。復号部１０２は、まず、秘密情報管理部２２に保持されている暗号化された秘密情報ＥＫを取得する。次に、ＲＯＭ１６に保持されている秘密鍵Ｐを用いて、ＥＫを復号する。以上の処理によって、秘密情報Ｋを取得する。Ｋは検証用データ作成用の秘密情報として、秘密情報管理部２２に格納される。

【００６２】

ステップＳ３３の処理を実行した後、直ちに復号処理＆秘密鍵消去処理部１７の秘密鍵消去部１０３は、秘密鍵Ｐを消去する処理を実行する（ステップＳ３４）。秘密鍵消去部１０３は、ＲＯＭ１６上に保持している秘密鍵Ｐに対応するデータ領域を、所定の値、或いはランダムな値等により上書きすることによってカメラ１１から消去、或いは破壊する。或いは、秘密鍵Ｐを保持しているＲＯＭ１６に、所定のメモリ領域に対するアクセスを無効化する機能が備わっている場合は、秘密鍵Ｐを保持しているメモリ領域に対するアクセスを無効化するようにしても良い。何れにしても、秘密鍵消去部１０３は、秘密鍵Ｐを利用不可能な状態にする。そして、秘密情報復元処理を終了する。

【００６３】

ただし、ＲＯＭ１６及び秘密情報管理部２２は、秘密鍵Ｐ及び秘密情報Ｋが漏れないように復号部１０２以外の外部への読み出しが出来ないような構成されたメモリである。例えば、耐タンパ技術を用いて構成することができる。パスワードや正当なユーザの生体情報などに基づいて認証を行い、ユーザの正当性が確認された場合にのみ外部から参照できるように構成してもよい。

【００６４】

以上説明したように秘密情報復元処理を実行することにより、生成装置１２で生成した秘密情報Ｋを安全に画像生成装置１１内の秘密情報管理部２２に記録することが可能になる。つまり、秘密情報Ｋは、生成装置１２内部で秘密鍵Ｐを用いて暗号化されているため、生成装置１２と画像生成装置１１の間で悪意のある攻撃者による盗聴を防止することができる。

【００６５】

また、秘密情報Ｋを復号した後、復号に用いた秘密鍵Ｐを画像生成装置１１内部から消去するようにしているため、悪意のある攻撃者が画像生成装置１１内部の秘密鍵Ｐを取得しようとしても、秘密鍵Ｐを取得することができない。

【００６６】

もし、画像生成装置１１内の秘密鍵Ｐを消去していない場合、悪意のある攻撃者がＲＯＭ１６を解析することにより秘密鍵Ｐを取得できてしまう可能性がある。秘密鍵Ｐを取得した攻撃者は、生成装置１２と画像生成装置１１の間で通信される暗号化された秘密情報Ｋを取得し、且つ、取得した暗号化された秘密情報Ｋを秘密鍵Ｐを用いて復号することにより、容易に秘密情報Ｋを取得できてしまう。

【００６７】

本実施形態では、前述したように秘密鍵Ｐは全ての画像生成装置１１で共通の値を保持するようにしている。結果として、秘密鍵Ｐを取得した攻撃者は、原理的には全ての画像生成装置１１に対応する秘密情報Ｋを取得できてしまうことになる。このような問題を解決するため、本実施形態によれば、秘密情報Ｋを設定した後、秘密鍵Ｐを画像生成装置１１の内部から消去するようにしている。これにより、秘密鍵Ｐの取得をより困難にすることが可能となる。

【００６８】

復号部１０２は暗号化部５３の復号用関数を実装しており、暗号化された秘密データＥＫを秘密鍵Ｐを用いて復号処理を行う。復号部１０２は、例えば、ＣＰＵによって構成することができる。なお、復号用関数とは、数式で表すと、Ｋ＝Ｄ'(ＥＫ,Ｐ)のようなＤ'( )を指す。

【００６９】

制御部２３は上記の機能要素を制御して処理を実行する。

【００７０】

（検証用データ生成処理）

次に、カメラ１１が画像Ｄに対する検証用データＭを生成する処理について、図４を用いて説明する。図４は検証用データ生成処理の流れを示したフローチャートである。

【００７１】

まず、カメラ１１は、画像処理部１４の撮像部９１から画像（画像データ）Ｄを入力する（ステップＳ４１）。ただし、撮像部９１は画像処理部１４の機能要素である。

【００７２】

ここで、画像処理部１４の機能構成について、図９を参照して説明する。図９は、画像処理部１４の機能構成を示したブロック図である。

【００７３】

図９において、撮像部９１はＣＣＤ（電荷結合素子）などの光学センサーを有する撮像装置であり、操作部９４に入力された指示に基づいて、被写体の画像データ及び補助パラメータを生成する。

【００７４】

ハッシュ生成部９２は、指定されたデータにハッシュ演算を行い、ハッシュ値を取得する。ハッシュ生成部９２が実行するハッシュ演算は、例えば、公知のハッシュ関数に基づいて行うことができる。公知のハッシュ関数としては、ＭＤ５、ＳＨＡ１、ＲＩＰＥＭＤ等が一般的に知られている。

【００７５】

画像ファイル生成部９３は、撮像部９１から得られた画像に基づいて所定のファイル形式の画像ファイルを生成する。画像ファイル生成部９３が生成するファイルの形式は、例えば公知のファイル形式を利用することができる。例えば、ＪＰＥＧ、ＪＦＩＦ、ＴＩＦＦ、ＧＩＦや、これらを拡張したもの、或いは、他の画像ファイルフォーマット等を利用することができる。ただし、ＪＰＥＧはJoint Photographic Experts Groupの略称である。ＪＦＩＦはJPEG File Interchange Formatの略称である。ＴＩＦＦはTagged Image File Formatの略称である。ＧＩＦはGraphics Interchange Formatの略称である。

【００７６】

操作部９４は、ユーザの指示入力を受け付けるユーザインタフェースであり、例えば、操作ボタン、スイッチ、ジョグダイアル、タッチパネル等により実現される。

【００７７】

図４の説明に戻る。ステップＳ４１の処理を終了すると、ステップＳ４２において、画像Ｄに対するハッシュ値Ｈを計算する。ただし、ハッシュ値Ｈの計算は、画像処理部１４の機能要素の一つであるハッシュ生成部９２を用いて行う。

【００７８】

次に、ステップＳ４３において、秘密情報管理部２２に保持された上記のＫを鍵として、そのハッシュ値Ｈに対する検証用データを検証用データ生成処理部１５において計算する。ただし、検証用データ生成処理部１５で用いることが可能なアルゴリズムには、上述のように、例えば、公開鍵暗号方式に基づくデジタル署名方式、ＭＡＣ方式等が含まれる。デジタル署名方式によればデジタル署名情報が生成され、ＭＡＣ方式によればＭＡＣ情報が生成される。

【００７９】

次に、ステップＳ４４において、カメラ１１の制御部２３は、画像処理部１４の画像ファイル生成部９３において、画像Ｄの画像ファイルに、ステップＳ４３で生成した検証用データと公開情報Ｉを添付するように制御する。ただし、公開情報Ｉは上述のように、カメラ１１固有の公開情報であり、公開情報管理部２１に保持されている。なお、公開情報管理部２１は、公開情報Ｉを管理する機能要素であり、例えば、フラッシュメモリ、ＨＤ等の不揮発性メモリにより構成することができる。Ｉは、通信部２４を通して外部から取得する。以上の各ステップの処理は制御部２３によって制御される。そして、処理を終了する。

【００８０】

なお、公開鍵暗号の署名生成アルゴリズムとしては、ＲＳＡ（Rivest Shamir Adleman）やＤＳＳ(Digital Signature Standard)などが知られている。また、ＭＡＣデータの生成アルゴリズムとしては、ＤＥＳやＡＥＳなどの共通鍵暗号のＣＢＣ（Cipher Block Chaining）モードを用いる手法と、ＨＭＡＣと呼ばれる鍵付きのハッシュ関数を用いる手法等が知られている。ただし、ＤＥＳはData Encryption Standardの略称である。ＡＥＳはAdvanced Encryption Standardの略称である。ＨＭＡＣはKeyed-Hashing for Message Authentication Codeの略称である。例えば、ＤＥＳのＣＢＣモードを用いる場合は、対象となるデータをＣＢＣモードで暗号化し、その最後のブロックの前半の３２ビットをＭＡＣデータとして利用する。

【００８１】

以上、検証用データ生成処理部１５において、カメラ１１に設定された秘密情報Ｋを用いて、撮影された画像データＤの検証用データMを生成する例を説明した。しかしながら本発明はこれに限定されることなく、カメラ１１に設定された秘密情報Ｋを種々の処理に適用可能であることは明らかである。この場合、秘密情報Ｋを用いる種々の処理が、検証用データ生成処理部１５の内部で実行されるものと考えれば良い。

【００８２】

例えば、カメラ１１に設定された秘密情報Ｋを用いて、撮影された画像データＤを暗号化する処理について、図２０を用いて説明する。図２０は撮影された画像データＤを暗号化する場合の処理の流れを示したフローチャートである。

【００８３】

まず、カメラ１１は、画像処理部１４の撮像部９１から画像（画像データ）Ｄを入力する（ステップＳ２０１）。尚、ステップＳ２０１は前述したステップＳ４１と同様の処理とすることができるので詳細な説明は省略する。

【００８４】

ステップＳ２０１の処理を終了すると、秘密情報管理部２２に保持された秘密情報Ｋを鍵として、ステップＳ２０１において生成された画像データＤを暗号化する。暗号化アルゴリズムには、例えば共有鍵方式としてAESやDES、公開鍵方式としてRSAなどが含まれる。そして、暗号化された画像データを出力する。

【００８５】

或いは、秘密情報Ｋを用いて直接画像Ｄを暗号化するのではなく、画像Ｄは別途生成し

た画像鍵で暗号化し、前記画像鍵を秘密情報Ｋを用いて暗号化するようにしても良い。画像鍵を暗号化する処理について、図２１を用いて説明する。図２１は画像鍵を暗号化する場合の処理の流れを示したフローチャートである。

【００８６】

まず、カメラ１１は、画像処理部１４の撮像部９１から画像（画像データ）Dを入力する（ステップＳ２１１）。尚、ステップＳ２１１は前述したステップＳ４１と同様の処理とすることができるので詳細な説明は省略する。

【００８７】

ステップＳ２１１の処理を終了すると、ステップ２１２において画像Ｄを暗号化する画像鍵DKを生成する。画像鍵としては画像毎に異なる値であれば良く、例えば不図示の擬似乱数生成器を用いて生成した擬似乱数や、画像Ｄのハッシュ値などを適用可能である。ステップＳ２１２で画像鍵を生成した後、ステップＳ２１１で入力した画像ＤをステップＳ２１２で生成した画像鍵DKを用いて暗号化する（ステップＳ２１３）。その後、秘密情報管理部２２に保持された秘密情報Ｋを鍵として、画像鍵DKを暗号化する(ステップＳ２１４)。最終的に、ステップＳ２１５において、カメラ１１の制御部２３は、画像処理部１４の画像ファイル生成部９３において、ステップＳ２１３で暗号化した画像ファイルに、ステップＳ２１４で暗号化した秘密情報を添付するように制御する。尚、ステップＳ２１３、及びステップＳ２１４で適応する暗号アルゴリズムは特に限定することなく、例えば共有鍵方式としてAESやDES、公開鍵方式としてRSAなど適用可能である。

【００８８】

上記のように、本実施形態に係る情報処理装置としての画像生成装置１１は、暗号化された秘密情報を入力し、カメラ内部で秘密情報を復号するため、カメラ外部の情報経路が安全でない場合においても、秘密情報の機密性を確保することができる。また、カメラ１１は、秘密情報を復号するとともに、復号処理に用いる鍵情報をメモリから消去するため、復号鍵（復号鍵情報）の漏洩に対する安全性を高めることができる。

【００８９】

また、本実施形態においては、カメラ１１は、暗号化された鍵情報を入力し、カメラ内部で鍵情報を復号するとともに、復号に用いる復号鍵をメモリから消去するように制御する。そして、復号した鍵情報を用いて撮像した画像データに改竄検出において用いられる情報（デジタル署名、ＭＡＣ等の検証用データ）を生成する。上述のように、本実施形態に係る構成においては復号鍵の漏洩に対する安全性を高められているため、画像データの改竄検出において用いられる情報の信頼性を高めることができる。

【００９０】

また、本実施形態では、正当なパスワード情報の入力、正当な生体情報の入力等、予め定められたイベントに応じて、秘密情報の復号及び復号処理に用いる鍵情報の消去を行う。このため、復号鍵の漏洩に対する安全性が更に高められている。

【００９１】

（変形例）

上述した実施形態では、生成装置１２がＰＣにより実現されているものとして説明したが、本発明はこれに限定されることなく、生成装置１２がＩＣカード等の耐タンパな装置により実現することも可能である。この場合、生成装置１２であるＩＣカードを設定装置１３であるＰＣに接続し、ＩＣカード及びＰＣ間で、暗号化された秘密情報Ｋ等のデータを通信するようにすれば良い。

【００９２】

また、上述した実施形態では、復号処理＆秘密鍵消去処理部１７は、ユーザ認証が成功したことをアクションとして、復号処理＆秘密鍵消去処理を実行していた。即ち、外部からパスワードや生体情報等を入力するようにし、入力された情報が正しい情報であると認識されたことをアクションとして、復号処理＆秘密鍵消去処理を実行するようにしていた。しかしながら本発明はこれに限定されることなく、設定装置１３上で、不図示のマウスやキーボードを用い、モニタに表示されている所定のボタンを押下したり、所定のメニュ

ーを選択したりすることをアクションとするようにしても良い。この場合、ユーザが所定のボタンを押下することにより、図３に示した一連の処理（Ｓ３１、Ｓ３３、及びＳ３４）が自動的に実行されることになる。

【００９３】

或いは、設定装置１３において、画像生成装置１１が設定装置１３に接続されているか否かを常時監視するようにしておき、接続されたことが確認されたことをアクションとするようにしても良い。この場合、設定装置１３に画像生成装置１１を接続することにより、図３に示した一連の処理（Ｓ３１、Ｓ３３、及びＳ３４）が自動的に実行されることになる。

【００９４】

＜＜第２実施形態＞＞

第１実施形態では、カメラ１１内において復号処理＆秘密鍵除去処理部１７の実行の契機となるアクションの例として、外部から入力されたパスワードや生体情報の正当性を確認することを示した。しかし、パスワードの入力等の操作は通常の使用における操作とは異なるため、ユーザビリティを低下させる状況が考えられる。なお、上述のように、復号処理＆秘密鍵除去処理を予め実行しておかない限り、検証用データを作成することができない。このため、本実施形態に係る構成では、初めてユーザが撮影する時までに検証用データが作成できる状態であればよいことを踏まえ、カメラ１１に対して必ず行う動作を、復号処理＆秘密鍵除去処理部１７を実行する契機とする。これにより、ユーザビリティを向上することができる。

【００９５】

本実施形態に係る構成は第１実施形態に係る構成と大部分が同様であるため、第１実施形態に係る構成との相違点のみ説明する。生成装置１２の構成および動作は図５および図６に示すものと同じであり、設定装置１３の構成および動作は図７および図８に示すものと同じであるので、説明を省略する。また、本実施形態に係る情報処理装置としての画像生成装置（カメラ）１１の構成は、図２と同様である。また、第１実施形態と同様に、カメラ１１は、予め定められた秘密鍵Ｐを図２に示すＲＯＭ１６に有する。この秘密鍵Ｐは生成装置１２が保持する秘密鍵Ｐと同じ鍵である。

【００９６】

以下、暗号化された秘密情報ＥＫの復号と、復号用の秘密鍵Ｐの消去に関する処理手順を図１１を用いて説明する。図１１は、本実施形態においてカメラ（画像生成装置）１１が実行する処理の手順を示したフローチャートである。

【００９７】

まず、設定装置１３により、通信部２４を介して秘密情報管理部２２に暗号化された秘密情報ＥＫが設定される（ステップＳ１１１）。ただし、通信部２４は通信部７１と同様である。

【００９８】

次に、ステップＳ１１２において、復号処理＆秘密鍵消去処理部１７は、復号部１０２を起動するか否かを判定する。この判定は、秘密情報復号処理起動部１０１に予め登録された、カメラ１１に対して必ず行われる動作（アクション）が実行されたか否かに基づいて行う。この動作は、例えば、カメラ１１の電源が初めて投入されたこと、或いは、カメラ１１のシャッターが初めて押下されたこと等とすることができる。或いは、画像生成装置１１をスキャナとして実現した場合は、上記は、スキャナ１１の電源が初めて投入されたこと、スキャナ１１の始動ボタンが初めて押下されたこととすることができる。或いは、通信部２４によって、設定装置１３からカメラ１１にＥＫが設定されたこととしてもよい。

【００９９】

ステップＳ１１２において復号部１０２を起動すると判定されなかった場合（ステップＳ１１２でＮＯ）は、上記のアクションが発生するまで待機する。上記アクションが発生した場合（ステップＳ１１２でＹＥＳ）には、ステップＳ１１３へ進む。

【０１００】
ステップＳ１１３では、復号部１０２が、暗号化された秘密情報ＥＫの復号処理を実行する。復号部１０２は、まず、秘密情報管理部２２に保持されている暗号化された秘密情報ＥＫを取得する。次に、ＲＯＭ１６に保持されている秘密鍵Ｐを用いて、ＥＫを復号する。以上の処理によって、秘密情報Ｋを取得する。Ｋは検証用データ作成用の秘密情報として、秘密情報管理部２２に格納される。
【０１０１】
ステップＳ１１３の処理を実行した後、直ちに復号処理＆秘密鍵消去処理部１７の秘密鍵消去部１０３は、秘密鍵Ｐを消去する処理を実行する（ステップＳ１１４）。秘密鍵消去部１０３は、秘密鍵Ｐを、メモリの上書き等によってカメラ１１から消去する。そして、処理を終了する。
【０１０２】
なお、カメラ１１における画像Ｄに対する検証用データＭの生成処理（検証用データ生成処理）は、第１実施形態と同様に、図４に示されるため、説明を省略する。
【０１０３】
上記のように、本実施形態に係る情報処理装置としての画像生成装置１１は、初めての電源投入、予め定められた生成装置の初めての操作等の通常の操作において発生するイベントに応じて、秘密情報の復号及び復号処理に用いる鍵情報の消去を行う。このため、本実施形態に係る構成によれば、安全性を保ちつつユーザビリティを向上することができる。
【０１０４】
＜＜第３実施形態＞＞
まず、第１及び第２実施形態に係る構成の処理の概要について、図１２を参照して要約する。図１２は、第１及び第２実施形態に係る構成の処理の概要を模式的に示したブロック図である。
【０１０５】
上述のように、生成装置１２は、関数Ｅ( )に演算対象情報としての公開情報Ｉと秘密鍵Ｐ'を入力して秘密情報Ｋを生成し、生成したＫに秘密鍵Ｐを用いて暗号化を行い秘密情報ＥＫを作成する。次に、安全性が保証されない経路を経由してＥＫを設定装置１３に配送する。
【０１０６】
設定装置１３は、暗号化された秘密情報ＥＫを受け取ると、カメラ１１にＥＫを設定する
最後に、カメラ１１は、所定のアクションを契機として、秘密鍵Ｐを用いてＥＫを復号し、秘密情報Ｋを取得するとともに、秘密鍵Ｐをメモリから消去するように制御する。
【０１０７】
このように、上記の構成では、秘密情報は、安全性が保証されない経路においては暗号化されているため、秘密情報が漏洩することはない。また、カメラ１１は、秘密鍵Ｐを利用すると秘密情報Ｋを消去するように制御するため、秘密情報Ｋは安全に管理される。
【０１０８】
なお、図１２において、Ｅ'( )、Ｄ'( )はそれぞれ暗号化部５３、復号部１０２の説明で述べたＥ'( )、Ｄ'( )と同じものである。
【０１０９】
上記のような構成に対して、本実施形態に係る構成は、図１３のように模式的に示される。図１３は、本実施形態に係る構成の処理の概要を模式的に示したブロック図である。
【０１１０】
図１３に示されているように、本実施形態においては、基本的には本実施形態に係る情報処理装置としての画像生成装置（カメラ）１１と公開情報設定機関（設定装置）１３のみが存在する。図１３のように、設定装置１３はカメラ１１に対応する公開情報Ｉをカメラ１１へ送る。カメラ１１は、送られてきた公開情報Ｉと秘密鍵Ｐ'を入力として関数Ｅ(

)の処理を実行し、秘密情報Ｋを取得するとともに秘密鍵Ｐ'を消去するように制御する。ただし、秘密鍵Ｐ'は、カメラ１１に予め設定されているものとする。

【０１１１】

このような構成によれば、暗号化処理を行うことなく改竄検出において用いられる情報の設定を行うことができるとともに、公開情報の暗号化とともに鍵情報をカメラから消去するため、鍵情報の漏洩に対する安全性を高めることができる。

【０１１２】

本実施形態に係る構成は第１及び第２実施形態に係る構成と大部分が同様であるため、これらの実施形態に係る構成との相違点のみ説明する。

【０１１３】

（装置構成）

図１４は、本実施形態に係る情報処理装置が含まれるシステム構成を例示的に示したブロック図である。図１４のように、本実施形態においては画像生成装置（カメラ）１４１と、公開情報設定機関（公開情報設定装置）１４２が存在する。

【０１１４】

図１４のように、画像生成装置１４１は、基本的には、画像処理部１４３と検証用データ生成処理部１４４とＲＯＭ１４５と検証データ用秘密情報生成処理＆秘密鍵消去処理部１４６と通信を行う機能を有する。検証データ用秘密情報生成処理＆秘密鍵消去処理部１４６は、公開情報設定装置１４２から入力された、公開情報Ｉと、ＲＯＭ１４５内にある秘密鍵Ｐ'を、関数Ｅ( )に入力し秘密情報Ｋを計算・出力する機能を有する。検証データ用秘密情報生成処理＆秘密鍵消去処理部１４６は、更に、秘密情報Ｋ作成の初回実行時を判定する機能と、初回実行後に秘密鍵Ｐ'をＲＯＭ１４５から消去する機能を有する。

【０１１５】

図１４のその他の機能要素（画像処理部１４３、検証用データ生成処理部１４４、ＲＯＭ１４５等）は図２と同様であるため、説明を省略する。なお、画像生成装置１４１は、デジタルカメラ、デジタルビデオカメラ、スキャナなどの撮像装置であっても、カメラユニットを有する電子機器であってもよいが、簡単のため、以下ではカメラ１４１として説明する。

【０１１６】

公開情報設定機関１４２は、カメラ固有の公開情報Ｉをカメラ１１に設定する機能を有する。なお、公開情報設定機関１４２は、人手により、直接上記公開情報Ｉをカメラ１１に設定する機関であってもよいし、ＰＣのような、ＵＳＢメモリやネットワークを通して、公開情報Ｉをカメラ１１に設定する機能を有する構成でもよい。以下では簡単のため、ＰＣにより実現したものとし、公開情報設定機関１４２を公開情報設定装置１４２と呼んで説明する。

【０１１７】

ここで、公開情報設定装置１４２の機能構成について図１８を参照して説明する。図１８は公開情報設定装置の詳細な構成を模式的に示したブロック図である。図１８において、通信部１８１はカメラ１４１を含む外部装置との通信インタフェースとして機能する機能要素である。公開情報設定装置１４２は通信部１８１を介して公開情報Ｉをカメラ１４１に設定する。

【０１１８】

（公開情報設定処理）

次に、公開情報設定装置１４２が実行する公開情報設定処理について図１９を参照して説明する。図１９は、公開情報設定処理の流れを示したフローチャートである。

【０１１９】

公開情報設定装置１４２は、図１９に示されている通り、公開情報Ｉを通信部１８１を用いてカメラ１４１に送る（ステップＳ１９１）。通信部１８１は、通信部７１と同様である。

【０１２０】

（秘密情報復元処理）
カメラ１４１は、処理の前提として、図１５に示すように予め定められた秘密鍵Ｐ'をＲＯＭ１４５に持つとする。ただし、図１５はカメラ１４１の詳細な構成を模式的に示したブロック図である。図５の機能要素のうち、検証データ用秘密情報生成処理＆秘密鍵消去処理部１４６以外の要素は図２の機能要素と同様であるため、説明を省略する。
【０１２１】
この秘密鍵Ｐ'は、上述のように、カメラ１４１固有の秘密情報Ｋを作成するための入力として用いられるものである。また、検証データ用秘密情報生成処理＆秘密鍵消去処理部１４６は、公開情報設定装置１４２から入力された、公開情報Ｉと、ＲＯＭ１４５内にある秘密鍵Ｐ'を、関数Ｅ( )の入力とし、秘密情報Ｋを計算・出力する機能を有する。検証データ用秘密情報生成処理＆秘密鍵消去処理部１４６は、更に、秘密情報Ｋ作成の初回実行時を判定する機能と、初回実行後に秘密鍵Ｐ'をＲＯＭ１４５から消去する機能を有する。
【０１２２】
次に、カメラ１１での、秘密情報Ｋの作成と、秘密情報Ｋ作成用の秘密鍵Ｐ'の消去に関する処理手順を図１７を用いて説明する。図１７は、カメラ１１が実行する秘密情報復元処理の流れを示したフローチャートである。
【０１２３】
まず、公開情報設定装置１４２により、通信部１５４を介して公開情報管理部１５１に公開情報Ｉが設定される（ステップＳ１７１）。
【０１２４】
次に、ステップＳ１７２において、検証データ用秘密情報生成処理＆秘密鍵消去処理部１４６は、検証データ用秘密情報生成部１６２を起動するか否かを判定する。なお、検証データ用秘密情報生成部１６２は検証データ用秘密情報生成処理＆秘密鍵消去処理部１４６の機能要素の一つである。
【０１２５】
ここで、検証データ用秘密情報生成処理＆秘密鍵消去処理部１４６の機能構成について、図１６を参照して説明する。図１６は検証データ用秘密情報生成処理＆秘密鍵消去処理部１４６の機能構成を示したブロック図である。
【０１２６】
図１６において、秘密情報生成処理起動部１６１は、検証データ用秘密情報生成部１６２を起動するか否かを判定する処理を行う。検証データ用秘密情報生成部１６２は、演算対象情報としての公開情報Ｉ等に基づいて検証用データ用秘密情報を生成する処理を行う。秘密鍵消去部１６３は、秘密鍵Ｐ'をカメラ１４１から消去する処理を行う。
【０１２７】
図１７の説明に戻る。検証データ用秘密情報生成処理＆秘密鍵消去処理部１４６は、ステップＳ１７２においては、秘密情報生成処理起動部１６１によって、検証データ用秘密情報生成部１６２を起動するか否かを判定する。ただし、この判定は、この判定は、第１、２実施形態に係る構成と同様に行う。即ち、予め定められたアクションが発生したか否かに基づいて行う。
【０１２８】
ステップＳ１７２において検証データ用秘密情報生成部１６２を起動すると判定されなかった場合（ステップＳ１７２でＮＯ）は、予め定められたアクションが発生するまで待機する。所定のアクションが発生し、検証データ用秘密情報生成部１６２を起動すると判定された場合（ステップＳ１７２でＹＥＳ）は、ステップＳ１７３へ進む。
【０１２９】
ステップＳ１７３では、検証データ用秘密情報生成部１６２が秘密情報Ｋを生成する処理を実行する。
【０１３０】
検証データ用秘密情報生成部１６２は、まず、公開情報管理部１５１に保持されている

Ｉを取得する。次に、ＲＯＭ１４５に保持されている秘密鍵Ｐ'を用いて、Ｋ＝Ｅ(Ｉ,Ｐ')の処理を行い、秘密情報Ｋを得る。以上の処理によって秘密情報Ｋを取得する。Ｋは検証用データ作成用の秘密情報として、秘密情報管理部１５２に格納される。

【０１３１】

ステップＳ１７３の処理を実行した後、直ちに検証データ用秘密情報生成処理＆秘密鍵消去処理部１４６の秘密鍵消去部１６３は、秘密鍵Ｐ'を消去する処理を実行する（ステップＳ１７４）。秘密鍵消去部１６３は、秘密鍵Ｐ'を、メモリの上書き等によってカメラ１４１から消去する。そして、秘密情報復元処理を終了する。

【０１３２】

なお、カメラ１４１における画像Ｄに対する検証用データＭの生成処理は、第１、第２実施形態と同様に図４に示されるため、説明を省略する。

【０１３３】

上記のように、本実施形態に係る情報処理装置としての画像生成装置１４１は、カメラ１４１に対応する公開情報を入力し、この公開情報を予め記憶された鍵情報に基づいて暗号化して、画像データの改竄検出において用いられる情報の生成等に用いる。このため、暗号化処理を行うことなく、改竄検出において用いられる情報の設定を行うことができる。また、公開情報の暗号化とともに鍵情報をカメラ１４１から消去するため、鍵情報の漏洩に対する安全性を高めることができる。

【０１３４】

＜＜その他の実施形態＞＞

以下、第１乃至第３実施形態に係る構成を基本とするその他の実施形態を示す。

【０１３５】

カメラ１１又はカメラ１４１（以後カメラとする。）内で、復号処理＆秘密鍵消去処理部１７または秘密情報生成処理＆秘密鍵消去処理部１４６を起動するか否かの判断の基となるアクションは、時間に係るイベントの発生としてもよい。例えば、上記の起動を行う時刻又は時間を予め設定しておき、カメラ等の内蔵タイマーもしくは外部からの電波時計等から設定された時刻又は時間に到達したことを認識したこと等を、上記の起動を行うアクションとして構成してもよい。

【０１３６】

また、復号処理＆秘密鍵消去処理部１７或いは秘密情報生成処理＆秘密鍵消去処理部１４６の起動回数を保持する実行回数確認カウンタや実行回数確認フラグ等をカメラに構成するようにしてもよい。これにより、上記の起動が行われた場合にカウンタをカウントする、もしくはフラグを立てることにより、上記の起動判定を２度以上実行しないようにすることができる。なお、カウンタおよびフラグを、上記の起動時における参照以外には内部及び外部からアクセスできないメモリ領域に保持することで、誤動作を更に抑制することができる。

【０１３７】

また、第１実施形態では、検証用データ生成処理を被写体の画像データに対して行う構成について述べたが、検証用データの生成対象はこれに限られない。例えば、補助パラメータ（例えば、撮影時刻、焦点距離、絞り値、ＩＳＯ感度、測光モード、画像ファイルサイズ、撮影者情報等）のような画像データのメタデータに当たる情報に対しても、画像データと同様の処理によって検証用データを生成することができる。補助パラメータに係る検証用データ検証処理も、画像データに係る検証用データの検証と同様の処理によって実行することができる。

【０１３８】

これは、画像データ及びメタデータはどちらも二値のデータであるからであり、画像データをメタデータに置き換える、即ち、ハッシュ関数への入力を画像データからメタデータに切り替えることによって実現可能であることは明らかである。このデータ切り替えは、例えば、制御部により実行することができる。このため、補助パラメータに検証用データを付与して検証する場合は、図２の処理において画像Ｄを補助パラメータとして同様の

処理を実行すればよい。

【０１３９】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードをシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が実行することによっても、達成されることは言うまでもない。この場合、記録媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記録した記録媒体は本発明を構成することになる。なお、前述のプログラムは、例えば、プログラムを記録した記録媒体（または記憶媒体）をシステムあるいは装置に供給し、システムあるいは装置が記録媒体に格納されたプログラムコードを読み出することにより、供給することができる。

【０１４０】

また、本発明の技術的範囲は、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現される場合に限られない。例えば、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（ＯＳ）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１４１】

さらに、コンピュータに挿入又は接続された機能拡張カードや機能拡張ユニットのメモリに書込まれたプログラムの指示に基づいて処理を行い、その処理により前述した実施形態の機能が実現される場合も、本発明の技術的範囲に含まれることは言うまでもない。具体的には、例えば、記録媒体から読み出されたプログラムコードを、コンピュータに挿入又は接続された機能拡張カードや機能拡張ユニットに備わるメモリに書込む。その後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行う。このような処理によって前述の実施形態の機能が実現される場合も本発明の技術的範囲に含まれる。

【０１４２】

本発明を上記記録媒体に適用する場合、その記録媒体には、先に説明したフローチャートに対応するプログラムコードが格納されることになる。

【図面の簡単な説明】

【０１４３】

【図１】第１及び第２実施形態に係る情報処理装置が含まれるシステム構成を例示的に示したブロック図である。

【図２】画像生成装置の詳細な構成を模式的に示したブロック図である。

【図３】秘密情報復元処理の流れを示したフローチャートである。

【図４】検証用データ生成処理の流れを示したフローチャートである。

【図５】秘密情報生成機関の詳細な構成を模式的に示したブロック図である。

【図６】秘密情報暗号化処理の流れを示したフローチャートである。

【図７】秘密情報設定機関の詳細な構成を模式的に示したブロック図である。

【図８】暗号化情報設定処理の流れを示したフローチャートである。

【図９】画像処理部の機能構成を示したブロック図である。

【図１０】復号処理＆秘密鍵消去処理部の機能構成を示したブロック図である。

【図１１】第２実施形態において画像生成装置が実行する処理の手順を示したフローチャートである。

【図１２】第１及び第２実施形態に係る構成の処理の概要を模式的に示したブロック図である。

【図１３】第３実施形態に係る構成の処理の概要を模式的に示したブロック図である。

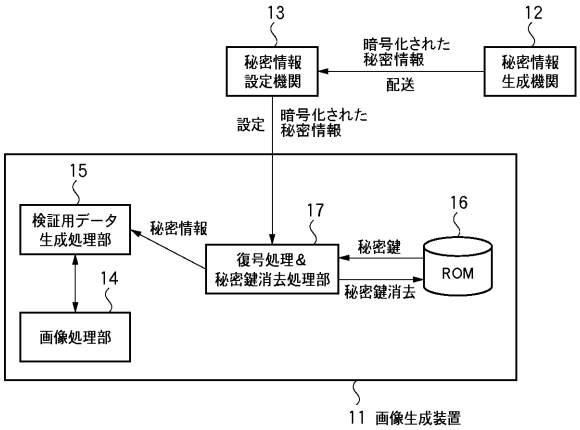
【図１４】第３実施形態に係る情報処理装置が含まれるシステム構成を例示的に示したブロック図である。

【図１５】カメラの詳細な構成を模式的に示したブロック図である。

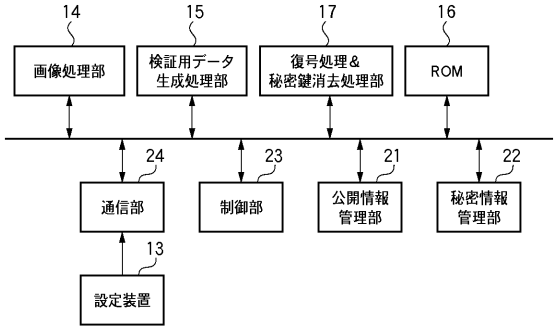
【図１６】検証データ用秘密情報生成処理＆秘密鍵消去処理部の機能構成を示したブロッ

ク図である。
【図１７】秘密情報復元処理の流れを示したフローチャートである。
【図１８】公開情報設定装置の詳細な構成を模式的に示したブロック図である。
【図１９】公開情報設定処理の流れを示したフローチャートである。
【図２０】撮影された画像データＤを暗号化する場合の処理の流れを示したフローチャートである。
【図２１】画像鍵を暗号化する場合の処理の流れを示したフローチャートである。

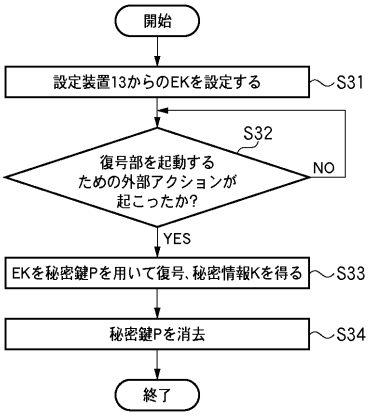
【図１】



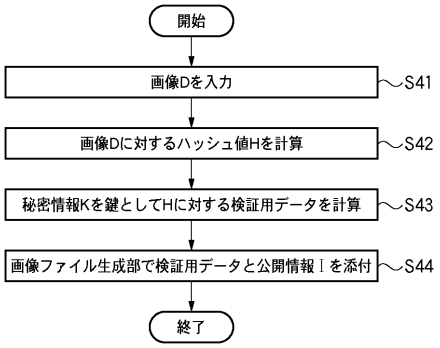
【図２】



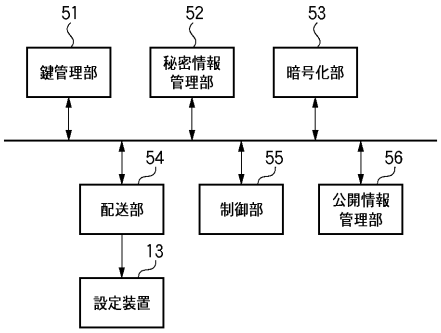
【図３】



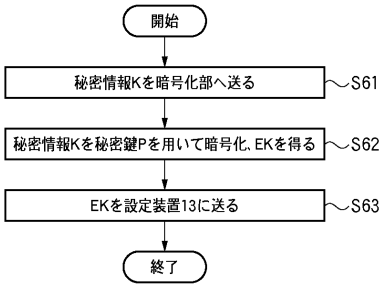
【図４】



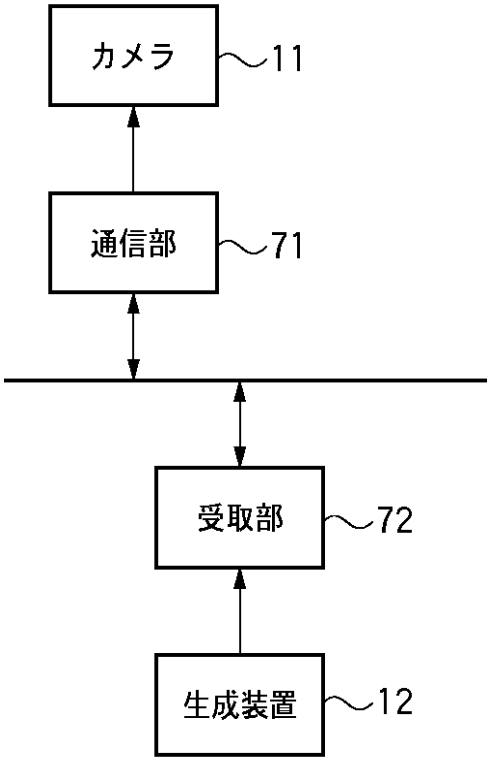
【図５】



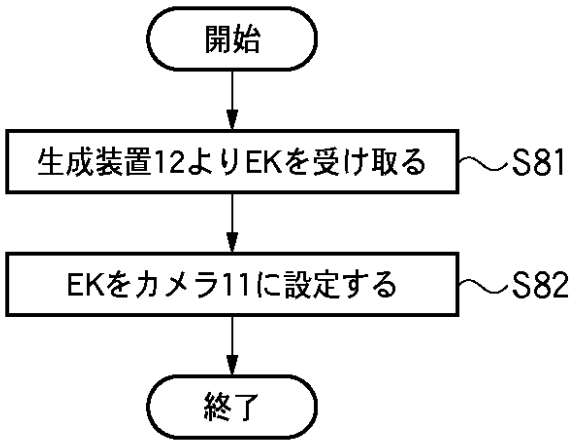
【図６】



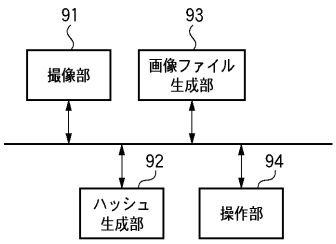
【図７】



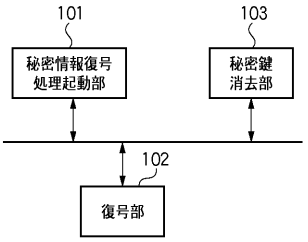
【図８】



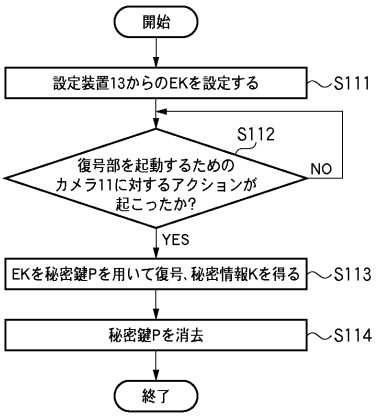
【図９】



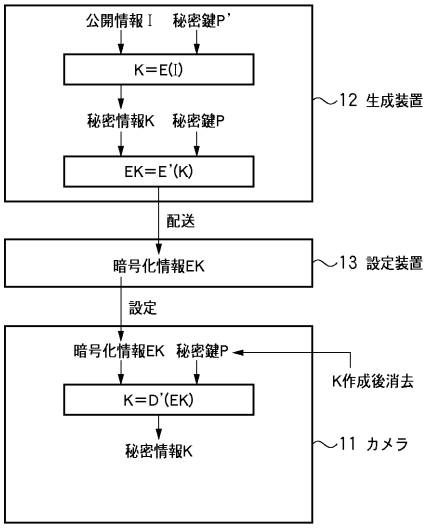
【図１０】



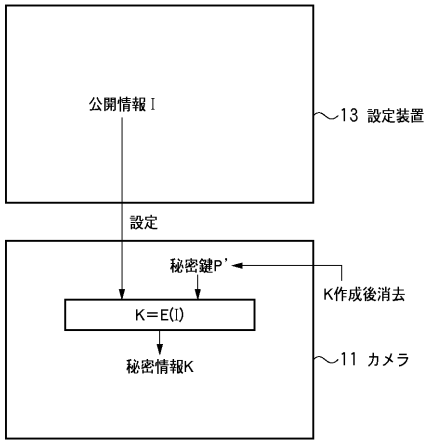
【図１１】



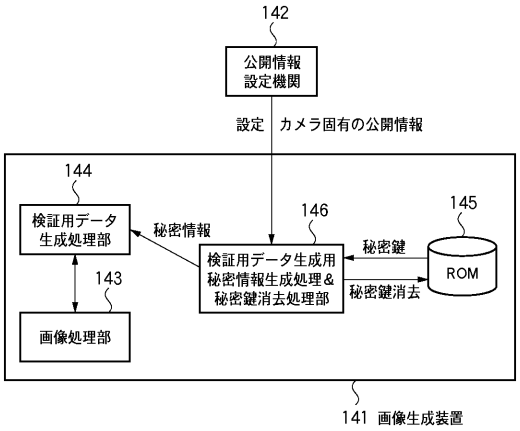
【図１２】



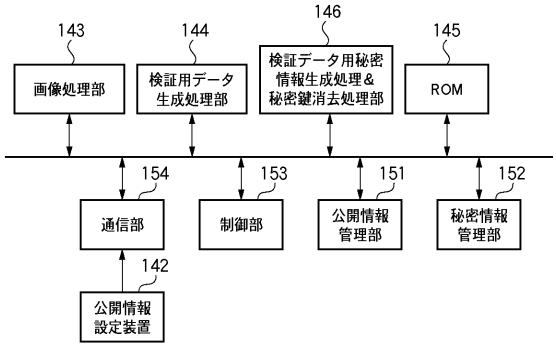
【図１３】



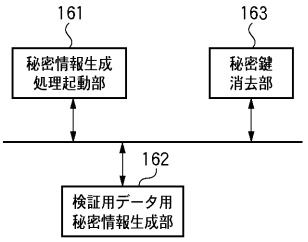
【図１４】



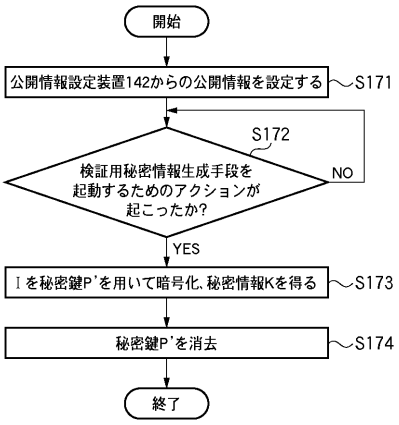
【図１５】



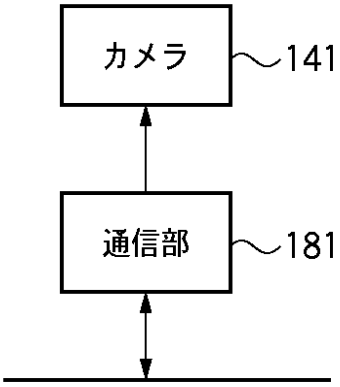
【図１６】



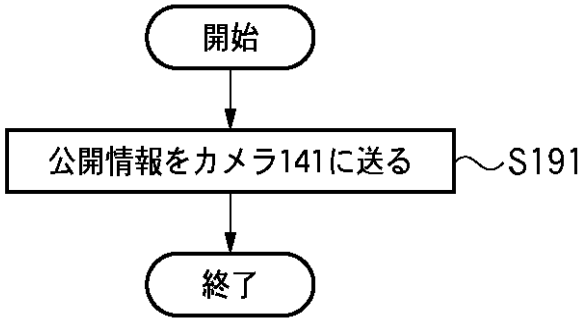
【図１７】



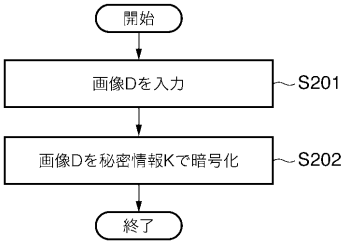
【図１８】



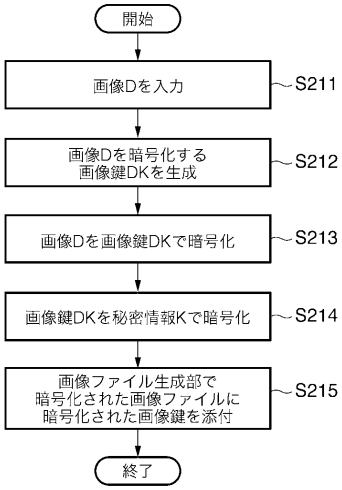
【図１９】



【図２０】



【図２１】



フロントページの続き

(72)発明者　中本　泰弘
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

Ｆターム(参考) 5J104 EA09 PA14