(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2017-192076
(P2017-192076A)
(43)公開日　平成29年10月19日(2017.10.19)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
H04L	9/14	(2006.01)	H04L	9/00	641	
G06F	21/64	(2013.01)	G06F	21/64		

審査請求 未請求　請求項の数 14　ＯＬ　（全 17 頁）

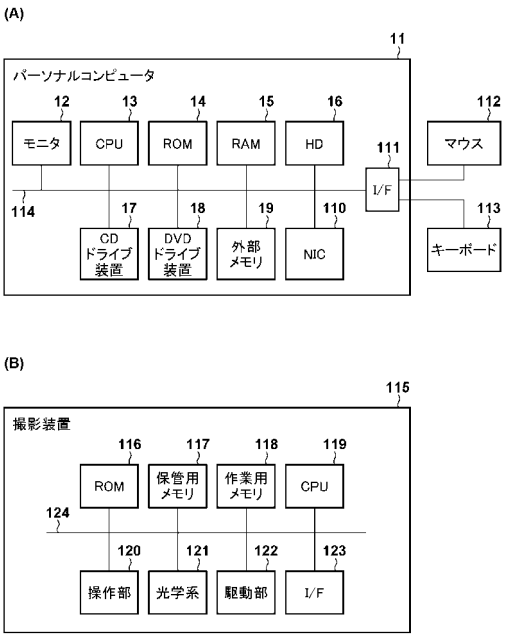
(21)出願番号　特願2016-81462(P2016-81462)
(22)出願日　平成28年4月14日(2016.4.14)

(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　100115071
弁理士　大塚　康弘
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】署名装置、署名方法、検証装置、検証方法、コンピュータプログラム

(57)【要約】
【課題】　装置のユーザが切り替わったとしても、該装置のユーザ認証を可能にする技術を提供すること。
【解決手段】　ユーザに割り当てられた署名鍵である第１の署名鍵を用いて、入力画像の署名データを第１の署名データとして生成する。署名装置に割り当てられた署名鍵である第２の署名鍵を用いて、入力画像及び第１の署名データを含むデータの署名データを第２の署名データとして生成する。第１の署名データ、第２の署名データ、入力画像を含む結合データを出力する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
署名装置であって、
ユーザに割り当てられた署名鍵である第１の署名鍵を用いて、入力画像の署名データを第１の署名データとして生成する第１の生成手段と、
前記署名装置に割り当てられた署名鍵である第２の署名鍵を用いて、前記入力画像及び前記第１の署名データを含むデータの署名データを第２の署名データとして生成する第２の生成手段と、
前記第１の署名データ、前記第２の署名データ、前記入力画像を含む結合データを出力する出力手段と
を備えることを特徴とする署名装置。
【請求項２】
前記第１の生成手段は、前記署名装置に着脱可能なメモリに格納されている前記第１の署名鍵を取得することを特徴とする請求項１に記載の署名装置。
【請求項３】
前記第２の生成手段は、耐タンパ性のメモリに格納されている前記第２の署名鍵を取得することを特徴とする請求項１又は２に記載の署名装置。
【請求項４】
前記結合データは更に、前記第１の署名鍵に対応する証明書、前記第２の鍵に対応する証明書を含むことを特徴とする請求項１乃至３の何れか１項に記載の署名装置。
【請求項５】
前記署名装置は、前記入力画像を撮影により取得する撮影装置であることを特徴とする請求項１乃至４の何れか１項に記載の署名装置。
【請求項６】
ユーザに割り当てられた署名鍵を用いて生成された入力画像の第１の署名データと、署名装置に割り当てられた署名鍵を用いて生成された、前記入力画像及び前記第１の署名データを含むデータの第２の署名データと、を取得する取得手段と、
前記第２の署名データに対応する署名もと、前記第１の署名データに対応する署名もと、に応じて、前記署名装置のユーザの認証の可否判断を行う判断手段と
を備えることを特徴とする検証装置。
【請求項７】
前記判断手段は、前記第２の署名データ、前記第１の署名データの順に検証処理を行った結果、前記第２の署名データに対する検証及び前記第１の署名データに対する検証の両方の検証が成功した場合に、前記署名装置のユーザの認証の可否判断を行うことを特徴とする請求項６に記載の検証装置。
【請求項８】
前記判断手段は、前記両方の検証が成功した場合に、前記第１の署名データに対応する証明書を用いて前記第１の署名データに対応する署名もとを特定し、前記第２の署名データに対応する証明書を用いて前記第２の署名データに対応する署名もとを特定することを特徴とする請求項７に記載の検証装置。
【請求項９】
前記判断手段は、
前記第２の署名データに対応する署名もとが前記署名装置であり、前記第１の署名データに対応する署名もとが前記署名装置のユーザである場合には、前記署名装置のユーザの認証は成功したと判断することを特徴とする請求項６乃至８の何れか１項に記載の検証装置。
【請求項１０】
前記判断手段は、
前記第２の署名データに対応する署名もとが前記署名装置のユーザであり、前記第１の署名データに対応する署名もとが前記署名装置である場合には、前記署名装置のユーザの

認証は失敗したと判断することを特徴とする請求項６乃至９の何れか１項に記載の検証装置。
【請求項１１】
署名装置が行う署名方法であって、
前記署名装置の第１の生成手段が、ユーザに割り当てられた署名鍵である第１の署名鍵を用いて、入力画像の署名データを第１の署名データとして生成する第１の生成工程と、
前記署名装置の第２の生成手段が、前記署名装置に割り当てられた署名鍵である第２の署名鍵を用いて、前記入力画像及び前記第１の署名データを含むデータの署名データを第２の署名データとして生成する第２の生成工程と、
前記署名装置の出力手段が、前記第１の署名データ、前記第２の署名データ、前記入力画像を含む結合データを出力する出力工程と
を備えることを特徴とする署名方法。
【請求項１２】
検証装置が行う検証方法であって、
前記検証装置の取得手段が、ユーザに割り当てられた署名鍵を用いて生成された入力画像の第１の署名データと、署名装置に割り当てられた署名鍵を用いて生成された、前記入力画像及び前記第１の署名データを含むデータの第２の署名データと、を取得する取得工程と、
前記検証装置の判断手段が、前記第２の署名データに対応する署名もと、前記第１の署名データに対応する署名もと、に応じて、前記署名装置のユーザの認証の可否判断を行う判断工程と
を備えることを特徴とする検証方法。
【請求項１３】
コンピュータを、請求項１乃至５の何れか１項に記載の署名装置の各手段として機能させるためのコンピュータプログラム。
【請求項１４】
コンピュータを、請求項６乃至１０の何れか１項に記載の検証装置の各手段として機能させるための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、署名及び署名の検証に係る技術に関する。
【背景技術】
【０００２】
デジタルカメラ等で撮影された画像データが警察や建設工事における証拠写真で用いられるようになった。そこで、画像データが撮影後改変されていないことを証明可能な技術が提案されており、暗号技術を利用した電子署名データによる画像データの改ざん検出システムが開示されている。
【０００３】
例えば特許文献１に開示されたシステムは、画像データを生成するデジタルカメラと、画像データが改竄されていないことを検証する画像検証装置と、により構成されている。デジタルカメラでは、画像生成装置固有の秘密鍵とデジタルカメラにて撮影してデジタル化した画像データとに基づき、所定の演算を実行して電子署名データを生成する。電子署名データと画像データとをデジタルカメラの出力とする。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、電子署名データに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。
【０００４】
また、特許文献２に開示された技術では、予め管理サーバ上で、撮影者とカメラ機体ＩＤとを紐づけする。署名時に画像に撮影情報としてカメラ機体ＩＤを紐づけしておくことで、画像と撮影者の関連付けが署名の確認により可能となる。

【先行技術文献】
【特許文献】
【０００５】
【特許文献１】米国特許第５４９９２９４号
【特許文献２】特開２００５－１９７９０１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、従来技術によれば、撮影者とカメラ機体とは一対一対応であり、例えば、カメラ機体を扱う撮影者が複数存在する場合に、この従来技術は対処していない。本発明はこのような問題に鑑みてなされたものであり、装置のユーザが切り替わったとしても、該装置のユーザ認証を可能にする技術を提供する。
【課題を解決するための手段】
【０００７】
本発明の一様態は、署名装置であって、ユーザに割り当てられた署名鍵である第１の署名鍵を用いて、入力画像の署名データを第１の署名データとして生成する第１の生成手段と、前記署名装置に割り当てられた署名鍵である第２の署名鍵を用いて、前記入力画像及び前記第１の署名データを含むデータの署名データを第２の署名データとして生成する第２の生成手段と、前記第１の署名データ、前記第２の署名データ、前記入力画像を含む結合データを出力する出力手段とを備えることを特徴とする。
【０００８】
また、本発明の一様態は、ユーザに割り当てられた署名鍵を用いて生成された入力画像の第１の署名データと、署名装置に割り当てられた署名鍵を用いて生成された、前記入力画像及び前記第１の署名データを含むデータの第２の署名データと、を取得する取得手段と、前記第２の署名データに対応する署名もと、前記第１の署名データに対応する署名もと、に応じて、前記署名装置のユーザの認証の可否判断を行う判断手段とを備えることを特徴とする。
【発明の効果】
【０００９】
本発明の構成によれば、装置のユーザが切り替わったとしても、該装置のユーザ認証を可能にする。
【図面の簡単な説明】
【００１０】
【図１】検証装置、署名装置のハードウェア構成例を示すブロック図。
【図２】撮影装置１１５の機能構成例、結合データの構成例を示す図。
【図３】署名装置の動作を示すフローチャート。
【図４】ステップＳ３２における処理の詳細を示すフローチャート。
【図５】ＰＣ１１の機能構成例を示すブロック図。
【図６】ＰＣ１１の動作を示すフローチャート及び画面の表示例を示す図。
【図７】ステップＳ６２における処理の詳細を示すフローチャート及び公開鍵証明書７１０を示す図。
【図８】ステップＳ６２における処理の詳細を示すフローチャート、結合データの構成例を示す図、画面の表示例を示す図。
【発明を実施するための形態】
【００１１】
以下、添付図面を参照し、本発明の実施形態について説明する。なお、以下説明する実施形態は、本発明を具体的に実施した場合の一例を示すもので、特許請求の範囲に記載した構成の具体的な実施例の１つである。
【００１２】
［第１の実施形態］

本実施形態では、入力画像の署名データを生成し、該入力画像を該署名データと共に出力する署名装置、該署名データを検証して該署名装置のユーザを認証する検証装置、のそれぞれについて説明する。

【００１３】

先ず、本実施形態に係る検証装置のハードウェア構成例について、図１（Ａ）のブロック図を用いて説明する。本実施形態では、検証装置としてＰＣ（パーソナルコンピュータ）１１を適用したが、検証装置が行うものとして後述する各処理を実行可能な装置であれば如何なる装置を検証装置として適用しても良い。例えば、スマートフォン、タブレット端末装置、画像のコピー／スキャン／プリント等を実行可能な画像処理装置を検証装置に適用しても良い。

【００１４】

ＣＰＵ１３は、ＲＯＭ１４やＲＡＭ１５に格納されているコンピュータプログラムやデータを用いて処理を実行する。これによりＣＰＵ１３は、ＰＣ１１全体の動作制御を行うと共に、ＰＣ１１が行うものとして後述する各処理を実行若しくは制御する。

【００１５】

ＲＯＭ１４には、ＰＣ１１の書き換え不要の設定データやブートプログラムなどが格納されている。

【００１６】

ＲＡＭ１５は、ＲＯＭ１４やＨＤ（ハードディスク）１６、ＣＤドライブ装置１７、ＤＶＤドライブ装置１８、外部メモリ１９からロードされたコンピュータプログラムやデータを格納するためのエリアを有する。更にＲＡＭ１５は、ＮＩＣ（ネットワークインターフェースカード）１１０を介して外部から受信したコンピュータプログラムやデータを格納するためのエリアを有する。また、ＲＡＭ１５は、ＣＰＵ１３が各種の処理を実行若しくは制御する際に用いるワークエリアを有する。このように、ＲＡＭ１５は、各種のエリアを適宜提供することができる。

【００１７】

ＨＤ１６には、ＯＳ（オペレーティングシステム）や、ＰＣ１１が行うものとして後述する各処理をＣＰＵ１３に実行若しくは制御させるためのコンピュータプログラムやデータが保存されている。ＨＤ１６に保存されているコンピュータプログラムやデータは、ＣＰＵ１３による制御に従って適宜ＲＡＭ１５にロードされ、ＣＰＵ１３による処理対象となる。

【００１８】

ＣＤドライブ装置１７は、ＣＤ－ＲＯＭ（ＣＤ－Ｒ）に格納されているコンピュータプログラムやデータを読み出して、ＲＡＭ１５やＨＤ１６に対して出力する機器である。ＤＶＤドライブ装置１８は、ＤＶＤ－ＲＯＭ（ＤＶＤ－ＲＡＭ）に格納されているコンピュータプログラムやデータを読み出して、ＲＡＭ１５やＨＤ１６に対して出力する機器である。なお、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭは、コンピュータプログラムやデータを格納するための記憶媒体の一例に過ぎず、他の種の記憶媒体を適用しても良い。その場合、ＰＣ１１には、対応するドライブ装置を設ける必要がある。外部メモリ１９は、ＵＳＢメモリなどの外付けのメモリである。

【００１９】

ＮＩＣ１１０は、有線若しくは無線でもって外部の機器とのデータ通信を行うためのものであり、例えば、ＮＩＣ１１０は、後述する署名装置との間のデータ通信を行うことができる。

【００２０】

モニタ１２は、ＣＰＵ１３による処理結果を画像や文字などでもって表示することができる。Ｉ／Ｆ（インターフェース）１１１には、マウス１１２及びキーボード１１３が接続されている。

【００２１】

マウス１１２及びキーボード１１３は、ユーザが各種の操作入力を行うためのユーザイ

ンターフェースの一例である。なお、マウス１１２及びキーボード１１３等のユーザインターフェースとモニタ１２とを一体化させてタッチパネル画面を構成しても良い。

【００２２】

モニタ１２、ＣＰＵ１３、ＲＯＭ１４、ＲＡＭ１５、ＨＤ１６、Ｉ／Ｆ１１１、ＣＤドライブ装置１７、ＤＶＤドライブ装置１８、外部メモリ１９、ＮＩＣ１１０は何れも、バス１１４に接続されている。

【００２３】

次に、本実施形態に係る署名装置のハードウェア構成例について、図１（Ｂ）のブロック図を用いて説明する。本実施形態では、署名装置として静止画像や動画像を撮影可能な撮影装置１１５を適用したが、署名装置が行うものとして後述する各処理を実行可能な装置であれば如何なる装置を署名装置として適用しても良い。例えば、スキャナ装置や複合機を署名装置に適用しても良い。

【００２４】

ＲＯＭ１１６には、撮影装置１１５が行うものとして後述する各処理をＣＰＵ１１９に実行若しくは制御させるためのコンピュータプログラムやデータが格納されている。

【００２５】

保管用メモリ１１７は、後述する光学系１２１によって取得した撮影画像等を一時的に格納するためのメモリである。作業用メモリ１１８は、ＣＰＵ１１９による処理対象となるデータを格納するためのメモリである。例えば、保管用メモリ１１７に一時的に格納した撮影画像に対して各種の処理を施す場合、この撮影画像は保管用メモリ１１７から作業用メモリ１１８にコピーされてから、処理が施されることになる。なお、メモリの数やそれぞれのメモリの使用用途については上記の説明に限ったものではなく、様々な変形例が考えられる。

【００２６】

ＣＰＵ１１９は、ＲＯＭ１１６や作業用メモリ１１８に格納されているコンピュータプログラムやデータを用いて処理を実行する。これによりＣＰＵ１１９は、撮影装置１１５全体の動作制御を行うと共に、撮影装置１１５が行うものとして後述する各処理を実行若しくは制御する。

【００２７】

操作部１２０は、撮影指示を入力するためのシャッターボタンや電源ボタン等のユーザインターフェースである。光学系１２１は、電荷結合素子ＣＣＤ、或いは相補型金属酸化物半導体ＣＭＯＳ等の光学センサを含むものであり、外界の光を電気信号に変換し、該電気信号に対する様々な信号処理、画像処理を行うことで撮影画像を生成する。駆動部１２２は、ＣＰＵ１１９による制御の下で、光学系１２１の駆動制御など、撮影に係る様々な機械的な動作を行う。

【００２８】

例えばユーザが操作部１２０を操作して撮影指示を入力すると、ＣＰＵ１１９による制御の下、駆動部１２２は被写体にピントが合うように光学系１２１の動作制御を行い、光学系１２１は該被写体を含む撮影画像を生成して保管用メモリ１１７に出力する。そしてＣＰＵ１１９は、保管用メモリ１１７に格納された撮影画像を作業用メモリ１１８にコピーし、該コピーした撮影画像に対して圧縮符号化処理を行って圧縮符号化画像を生成する。そしてＣＰＵ１１９は、後述する署名処理を行うことで、署名データ、証明書、撮影画像、を含む結合データを生成して出力する。

【００２９】

Ｉ／Ｆ１２３は、メモリカードなどのメモリ装置を撮影装置１１５に接続するためのインターフェース、有線若しくは無線でもって外部の機器とのデータ通信を行うためのインターフェース等、様々なインターフェースにより構成されている。

【００３０】

ＲＯＭ１１６、保管用メモリ１１７、作業用メモリ１１８、ＣＰＵ１１９、操作部１２０、光学系１２１、駆動部１２２、Ｉ／Ｆ１２３は何れも、バス１２４に接続されている

。
【００３１】
次に、撮影装置１１５の機能構成例について、図２（Ａ）のブロック図を用いて説明する。図２（Ａ）には、撮影画像に基づいて結合データを生成して出力するための一連の処理に係る構成を示している。
【００３２】
上記の光学系１２１及び駆動部１２２を含む撮影部２１によって撮影画像（画像データ）を取得する。画像署名部２２は、撮影部２１によって取得した撮影画像の署名データを生成し、撮影画像、署名データ、証明書を含む上記の結合データを出力する。書き出し部２６は、該結合データをＩ／Ｆ１２３に接続されているメモリカードなどの記憶媒体２７に書き込む。画像署名部２２（ユーザ署名部２２１，カメラ署名部２２２を含む）や書き出し部２６は専用のハードウェアで実現しても良いし、コンピュータプログラムで実現させても良い。本実施形態では、画像署名部２２及び書き出し部２６をコンピュータプログラムで実装したケースについて説明する。なお、以下では、画像署名部２２（ユーザ署名部２２１，カメラ署名部２２２についても同様）や書き出し部２６を処理の主体として説明するが、実際には対応するコンピュータプログラムをＣＰＵ１１９が実行することで、対応する機能部の機能を実現させる。
【００３３】
ユーザ署名部２２１は、Ｉ／Ｆ１２３としての接続部２３に着脱可能に接続されているＩＣカード２５から、撮影装置１１５のユーザに割り当てられている署名鍵であるユーザ署名鍵と、該ユーザ署名鍵に対応する証明書であるユーザ証明書と、を読み出す。つまり、接続部２３に接続させるＩＣカード２５を変更することで、ユーザ署名部２２１は、任意のユーザのユーザ署名鍵及びユーザ証明書を取得することができる。ＩＣカード２５は、例えば演算機能をもつスマートカードや記憶媒体等、任意の機器を用いてよい。
【００３４】
そしてユーザ署名部２２１は、ユーザ署名鍵を用いて、撮影部２１からの撮影画像の署名データを、ユーザ署名データとして生成する。本実施形態では、署名データを生成する署名アルゴリズムは特定のアルゴリズムに限らず、ＲＳＡやＤＳＡなど種々の署名アルゴリズムを適用することができる。例えば、撮像画像のハッシュ値を算出し、該ハッシュ値及びユーザ署名鍵を用いてユーザ署名データを生成しても良い。また、ハッシュ値を生成するためのハッシュ関数についても特定のハッシュ関数に限るものではなく、ＳＨＡ１やＳＨＡ２５６など種々のハッシュ関数を適用しても良い。そしてユーザ署名部２２１は、撮影画像、ユーザ署名データ、ユーザ証明書を含む結合データを、後段のカメラ署名部２２２に対して送出する。図２（Ａ）では説明上、ユーザ証明書の図示は省いている。
【００３５】
カメラ署名部２２２は、耐タンパ記憶部２４から、撮影装置１１５に割り当てられている署名鍵であるカメラ署名鍵と、該カメラ署名鍵に対応する証明書であるカメラ証明書と、を読み出す。耐タンパ記憶部２４には、例えばＴＰＭ（Ｔｒｕｓｔｅｄ　Ｐｌａｔｆｏｒｍ　Ｍｏｄｕｌｅ）（不図示）のような、外部攻撃に対して、物理的にセキュアであるメカニズムを用いる（耐タンパ性のメモリを使用する）。
【００３６】
そしてカメラ署名部２２２は、カメラ署名鍵を用いて、ユーザ署名部２２１から受けた結合データからユーザ証明書を省いた残りのデータ、即ち、撮影画像とユーザ署名データとから成るデータの署名データを、カメラ署名データとして生成する。署名データの生成方法については上記の通りである。
【００３７】
カメラ署名鍵を撮影装置毎に固有の情報であるとすると、耐タンパ記憶部２４内のカメラ署名鍵は、撮影装置１１５内のみ存在することが保証される。従って、カメラ署名鍵による署名の対象に、ユーザ署名データを含めることで、ユーザ署名が撮影装置１１５内で実行されたことを証明できる。本実施形態では、ユーザ署名鍵の所有者を撮影者とみなす

ことで、撮影者認証可能な署名を生成することができる。

【００３８】

なお、カメラ署名鍵は、撮影装置ごとに別個のカメラ署名鍵であっても良いし、撮影装置のモデル、仕向け地域、シリアル番号等でグループ化されたグループ毎に固有のカメラ署名鍵であっても良い。

【００３９】

そしてカメラ署名部２２２は、ユーザ署名部２２１から受けた結合データに、ユーザ署名データ、カメラ署名データ、カメラ証明書を追加登録して結合データを更新し、該更新後の結合データを書き出し部２６に対して出力する。

【００４０】

ここで、結合データの構成例について、図２（Ｂ）を用いて説明する。結合データは、第１の署名フィールド１２７、第２の署名フィールド１２８、画像フィールド１２９を有し、ユーザ署名部２２１は、第１の署名フィールド１２７にユーザ署名データ及びユーザ証明書を格納し、画像フィールド１２９に撮影画像を格納する。この時点で第２の署名フィールド１２８には何も格納されていない。そしてカメラ署名部２２２は、第２の署名フィールド１２８に、カメラ証明書２８１、ユーザ署名データ２８２、カメラ署名データ２８３を格納する。

【００４１】

書き出し部２６は、カメラ署名部２２２によって更新された結合データを記憶媒体２７に格納する。なお、結合データの出力先については、記憶媒体２７に限るものではなく、様々な出力先が考えられる。例えば、有線若しくは無線でもって、外部の装置に対して送信しても良いし、検証装置に対して送信しても良い。

【００４２】

次に、上記の署名装置の動作について、図３のフローチャートに従って説明する。なお、図３の各ステップにおける処理の詳細については上記の通りであるため、ここでは簡単に説明する。

【００４３】

ステップＳ３１では、撮影部２１によって撮影画像を取得する。撮影画像のフォーマットについては特定のフォーマットに限らず、ＪＰＥＧ、ＴＩＦＦ、ＲＡＷなど種々のフォーマットが適用可能である。ステップＳ３２では、画像署名部２２は、ステップＳ３１で取得した撮影画像に対する署名処理を行って、結合データを生成する。ステップＳ３２の処理の詳細については、図４を用いて後述する。ステップＳ３３では、書き出し部２６は、ステップＳ３２で生成された結合データを記憶媒体２７等の適当な出力先に対して出力する。

【００４４】

次に、上記のステップＳ３２における処理の詳細について、図４のフローチャートに従って説明する。ステップＳ４１では、ユーザ署名部２２１は、結合データ内に第１の署名フィールドを生成する。ステップＳ４２では、ユーザ署名部２２１は、ＩＣカード２５からユーザ署名鍵を読み出す。ステップＳ４３では、ユーザ署名部２２１は、ステップＳ４２で読み出したユーザ署名鍵を用いて、ステップＳ３１で取得した撮影画像の署名データを、ユーザ署名データとして生成する。そしてユーザ署名部２２１は、ユーザ署名データを、ＩＣカード２５から読み出したユーザ証明書と共に第１の署名フィールドに格納する。また、ユーザ署名部２２１は、ステップＳ３１で取得した撮影画像を画像フィールドに格納する。

【００４５】

ステップＳ４４では、カメラ署名部２２２は、結合データ内に第２の署名フィールドを生成する。ステップＳ４５では、カメラ署名部２２２は、ユーザ署名データを第２の署名フィールドに格納する。ステップＳ４６では、カメラ署名部２２２は、耐タンパ記憶部２４からカメラ署名鍵を読み出す。ステップＳ４７では、カメラ署名部２２２は、カメラ署名鍵を用いてカメラ署名データを生成し、該生成したカメラ署名データと、耐タンパ記憶

部２４から読み出したカメラ証明書と、を第２の署名フィールドに格納する。

【００４６】

次に、ＰＣ１１の機能構成例について、図５のブロック図を用いて説明する。図５には、結合データに基づく撮影者認証処理に係る構成を示している。入力部５１は、ＣＤドライブ装置１７やＤＶＤドライブ装置１８によって記憶媒体２７から読み取られた上記の結合データを取得する。なお、記憶媒体２７は上記の外部メモリ１９であっても良い。また、ＰＣ１１による結合データの取得方法については記憶媒体２７を介した取得方法に限らない。

【００４７】

検証部５２は、入力部５１が取得した結合データに基づいて検証処理を行うと共に、検証成功時には署名順序を判定し、検証結果表示部５３は、検証部５２による検証結果をモニタ１２に表示させる。

【００４８】

なお、入力部５１、検証部５２（署名検証部５２１、署名順序判定部５２２を含む）、検証結果表示部５３は専用のハードウェアで実現しても良いし、コンピュータプログラムで実現させても良い。本実施形態では、これらの機能部をコンピュータプログラムで実装したケースについて説明する。また、以下では、これらの機能部を処理の主体として説明するが、実際には対応するコンピュータプログラムをＣＰＵ１３が実行することで、対応する機能部の機能を実現させる。

【００４９】

署名検証部５２１は、第２の署名フィールド、第１の署名フィールドの順に、それぞれのフィールド内の署名データを検証する。第２の署名フィールドの場合、カメラ署名データ２８３を、画像フィールド１２９内の撮影画像、カメラ証明書２８１、ユーザ署名データ２８２を用いて検証する。カメラ証明書２８１の正当性については、ルート認証局の公開鍵（不図示）を用いて予め検証されていることを前提とする。ルート認証局の公開鍵は、予めＨＤ１６などに信頼するルート認証局の公開鍵証明書を記録しておき、ルート認証局の公開鍵証明書に含まれる公開鍵を利用する。これにより、カメラ証明書２８１が、信頼するルート認証局から発行されていることを検証することができる。また、撮影画像のハッシュ値を生成し、該生成したハッシュ値及び公開鍵を用いて検証するようにしても良い。署名検証するためのアルゴリズム及びハッシュ関数は、前述した画像署名部２２において利用した署名アルゴリズムに対応する検証アルゴリズムを適用する。このため、署名フィールドに記録されている署名アルゴリズム及びハッシュ関数を識別する情報を用いて、アルゴリズムを決定してもよい。また、予め撮影装置１１５とＰＣ１１との間で合意した検証アルゴリズムを用いてもよい。第２の署名フィールドに対する検証処理が完了すると、次に、第１の署名フィールドに対する検証処理、すなわち、ユーザ署名データの検証を行う。第１の署名フィールド及び第２の署名フィールドの両方に対する検証処理が成功した場合は、検証成功とし、一方でも検証処理が失敗した場合には、検証失敗とする。署名データの検証処理については周知の技術であるので、これに係る説明は省略する。

【００５０】

署名順序判定部５２２は、署名検証部５２１から検証成功の旨の通知を受けると、署名の順序を判定する。例えば図２（Ｂ）の結合データの場合、署名順序判定部５２２は、撮影者認証成功／撮影者認証不能の何れかを判定結果として出力する。

【００５１】

検証結果表示部５３は、検証成功（検証成功の場合は、撮影者認証成功／撮影者認証不能の何れか）、検証失敗、の何れかを検証結果としてモニタ１２に表示する。

【００５２】

次に、ＰＣ１１の動作について、図６（Ａ）のフローチャートに従って説明する。ステップＳ６１では、入力部５１は、記憶媒体２７等から結合データを取得する。ステップＳ６２では、署名検証部５２１は、結合データを用いて検証処理を行い、署名順序判定部５２２は、署名の順序判定を行う。ステップＳ６２の処理の詳細については、図７（Ａ）を

用いて後述する。次に、ステップＳ６３では、検証結果表示部５３は、ステップＳ６２における結果をモニタ１２に表示させる。

【００５３】

次に、上記のステップＳ６２における処理の詳細について、図７（Ａ）のフローチャートに従って説明する。ステップＳ７１では、署名検証部５２１は、結合データ内の署名フィールドの数を取得し、変数Ｎに代入する。本実施形態ではＮ＝２となる。ステップＳ７２では、署名検証部５２１は、Ｎ＞０であるか否かを判定する。この判定の結果、Ｎ＞０であれば、処理はステップＳ７３に進み、Ｎ＝０であれば、ステップＳ７８に進む。

【００５４】

ステップＳ７３では、署名検証部５２１は、結合データの先頭から、第１の署名フィールド、第２の署名フィールド、…、というように順番に並んで設けられている署名フィールドのうち、Ｎ場目の署名フィールド、すなわち、第Ｎの署名フィールドを取得する。本実施形態では、第１回目のステップＳ７３では第２の署名フィールドを取得し、第２回目のステップＳ７３では、第１の署名フィールドを取得することになる。

【００５５】

ステップＳ７４では、署名検証部５２１は、第Ｎの署名フィールドから署名データ及び証明書を取得する。第２の署名フィールドの場合は、カメラ証明書、カメラ署名データ、ユーザ署名データを取得し、第１の署名フィールドの場合は、ユーザ証明書、ユーザ署名データを取得する。

【００５６】

ステップＳ７５では、署名検証部５２１は、ステップＳ７４で取得した署名データを検証する。この検証に成功した場合には、処理はステップＳ７６に進み、失敗した場合には、処理はステップＳ７１１に進む。

【００５７】

署名データの検証に成功した場合は、画像フィールドに格納されている撮影画像の署名検証処理は成功であると判定する。該撮影画像について、改竄されていないこと（完全性）、後述するＳｕｂｊｅｃｔ（主体者識別情報）で識別される主体者によって署名されたこと（認証性）、主体者が署名していないと否認できないこと（否認防止性）が確認できる。本実施形態では、これを合わせて正当性と呼ぶ。一方、署名データの検証に失敗した場合は、該撮影画像の署名検証処理は失敗であると判定する。即ち、前述した正当性（完全性、認証性、否認防止性）が確認できないことになる。

【００５８】

ステップＳ７６では、署名検証部５２１は、ステップＳ７４で取得した証明書の主体者名取得処理を実行する。ここで、本実施形態における公開鍵証明書について詳細に説明する。図７（Ｂ）に示す如く、公開鍵証明書７１０には、バージョン７１１、証明書識別子７１２、署名アルゴリズム７１３、発行者識別情報７１４、有効期限７１５、Ｓｕｂｊｅｃｔ（主体者識別情報）７１６、公開鍵７１７、及び署名７１８が含まれる。

【００５９】

バージョン７１１は、公開鍵証明書７１０のバージョンである。証明書識別子７１２は、公開鍵証明書７１０を一意に識別可能な識別子である。署名アルゴリズム７１３は、後述する署名７１８を生成・検証するための署名アルゴリズムの識別子である。発行者識別情報７１４は、公開鍵証明書７１０を発行した発行者を一意に識別可能な識別子である。有効期限７１５は、公開鍵証明書７１０の開始日及び終了日時を示す情報である。

【００６０】

Ｓｕｂｊｅｃｔ（主体者識別情報）７１６は、証明を受ける主体、即ち後述する公開鍵７１７の所有者を一意に識別可能な識別子である。本実施形態においては、公開鍵証明書７１０は撮影装置毎に固有であるため、主体者は個々の撮影装置である。尚、公開鍵証明書が撮影装置のモデル、仕向け地域、シリアル番号等でグループ化されたグループ、或いは撮影装置の利用者、グループ、役割毎に固有である場合は、これら固有のものを主体者名とする。

【００６１】
公開鍵７１７は、公開鍵証明書７１０の主体者の保有する公開鍵である。署名７１８は、バージョン７１１、証明書識別子７１２、署名アルゴリズム７１３、発行者識別情報７１４、有効期限７１５、Ｓｕｂｊｅｃｔ（主体者識別情報）７１６、公開鍵７１７、から生成した署名データである。署名データを生成するためには、ルート認証局の署名鍵（不図示）を用いる。
【００６２】
ステップＳ７６では、上記のＳｕｂｊｅｃｔ（主体者識別情報）を取得する。ここで、主体者名確認処理により署名フィールドの署名がカメラ署名のものであるかどうかを判定する方法について、カメラ証明書であることを示すＳｕｂｊｅｃｔ名の一覧７１９を用いて説明する。一覧７１９は、例えばＲＯＭ１４内に保管しておき、必要に応じて読み出してもよい。また、検証時に撮影装置１１５と接続し、撮影装置１１５からＳｕｂｊｅｃｔを取得してもよい。ステップＳ７６の判定では、取得した証明書のＳｕｂｊｅｃｔ名が、一覧７１９に含まれるかどうかを判定する。含まれる場合はカメラ証明書、含まれない場合はユーザ証明書と判定する。
【００６３】
ステップＳ７７では、署名検証部５２１は、変数Ｎの値を１つデクリメントする。そして処理はステップＳ７２に戻る。ステップＳ７８では、署名順序判定部５２２は、署名順序を判定する。例えば図２（Ｂ）の結合データの場合、第２の署名フィールドの署名がカメラ署名によるもので、第１の署名フィールドの署名がユーザ署名によるものである場合、撮影者認証成功とする。さもなければ、撮影者認証不能とする。撮影者認証成功と判定した場合は、処理はステップＳ７９に進み、撮影者認証不能と判定した場合は、処理はステップＳ７１０に進む。
【００６４】
ステップＳ７９では、署名順序判定部５２２は、画像署名検証に成功及び撮影者認証成功を示す情報を検証結果表示部５３に対して出力する。一方、ステップＳ７１０では、署名順序判定部５２２は、画像署名検証に成功及び撮影者認証不能を示す情報を検証結果表示部５３に対して出力する。ステップＳ７１１では、署名検証部５２１は、画像署名検証に失敗を示す情報を検証結果表示部５３に対して出力する。検証結果表示部５３は、署名検証部５２１や署名順序判定部５２２から受けた情報に応じた表示画面をモニタ１２に表示させる。
【００６５】
上記のＰＣ１１における検証処理は、例えば、次のようなアプリケーションソフトウェア上に実装可能である。このアプリケーションソフトウェアは、ＨＤ１６、ＣＤ－ＲＯＭ，ＤＶＤ－ＲＯＭ等に保存されている。ユーザがキーボード１１３やマウス１１２を操作してアプリケーションソフトウェアの実行指示を入力すると、ＣＰＵ１３はＨＤ１６、ＣＤドライブ装置１７、ＤＶＤドライブ装置１８等を制御し、アプリケーションソフトウェアをＲＡＭ１５にロードさせる。そしてＣＰＵ１３がこのアプリケーションソフトウェアを実行すると、モニタ１２の表示画面上には、図６（Ｂ）の左側の画面６４が表示される。画面６４には、ＨＤ１６等のメモリに格納されている画像のうち、検証対象となる画像としてユーザがキーボード１１３やマウス１１２を操作して選択した画像のファイル名（サムネイル画像等、他の情報でも良い）が一覧表示されている。更に画面６４には、画像選択ボタン、画像検証ボタンも設けられている。ユーザがキーボード１１３やマウス１１２を操作して画像選択ボタンを指示すると、モニタ１２の表示画面上には、検証対象となる画像を選択するためのＧＵＩ（不図示）が表示され、ユーザはこのＧＵＩ上で、検証対象となる画像を選択することができる。選択する画像の数は１であっても良いし、複数であっても良い。そしてユーザがキーボード１１３やマウス１１２を操作して画像選択を行った後、画像選択を終了させる指示を入力すると、このＧＵＩは画面から消去され、該ＧＵＩを用いて選択した画像のファイル名が画面６４上に追加表示される。そしてユーザがキーボード１１３やマウス１１２を操作して、画面６４上の画像検証ボタンを指示すると

、ＰＣ１１は図６（Ａ）及び図７（Ａ）に示したフローチャートに沿った検証処理を開始する。

【００６６】

図６（Ａ）及び図７（Ａ）に示したフローチャートに沿った検証処理が完了すると、モニタ１２の表示画面上には、図６（Ｂ）の右側の画面６５が表示される。画面６５では、画面６４にて一覧表示された各画像ファイル名に対し、対応する検証結果及び撮影者認証結果が表示されている。「検証結果」として、検証に成功した場合は「○」、検証に失敗した場合は「×」が表示されている。また、「撮影者認証結果」として、撮影者認証成功と判定した場合は「○」、撮影者認証不能と判定した場合は「×」が表示されている。「－」は撮影者認証の判定を実施しなかったことを示す。

【００６７】

このように、本実施形態によれば、署名フィールドの署名の順序を判定することで、撮影者認証を行うことができる。また、撮影者が複数存在する場合においても、撮影者に対応したＩＣカード２５による署名の付与及び撮影者認証を行うことができる。

【００６８】

［第２の実施形態］

第１の実施形態では、撮影装置１１５内で実施した署名について撮影者認証を行った。本実施形態では、撮影装置１１５による署名の後に、ＰＣ１１による追加署名が施された場合であっても、撮影者認証を可能にする。本実施形態を含め、以下の各実施形態では、第１の実施形態との差分について重点的に説明し、以下で特に触れない限りは、第１の実施形態と同様であるものとする。

【００６９】

以下では一例として、ＰＣ１１が図２（Ｂ）に示した構成を有する結合データ内の画像フィールドに格納されている画像に対して新たに署名を行って、その署名データ及び対応する証明書を第３の署名フィールド（図８（Ｂ））に格納した場合について説明する。もちろん、第３の署名フィールドに格納した署名データの求め方については特定の求め方に限らない。

【００７０】

本実施形態では、上記のステップＳ６２において、図８（Ａ）に示したフローチャートに沿った処理を実行する。図８（Ａ）において、図７（Ａ）に示した処理ステップと同じ処理ステップには同じステップ番号を付しており、その説明も上記の通りであるため、以下では該処理ステップについては説明は省略する。

【００７１】

図８（Ａ）のフローチャートの場合、ステップＳ７８において撮影者認証成功と判定した場合は、処理はステップＳ８１に進み、撮影者認証不能と判定した場合は、処理はステップＳ７１０に進む。

【００７２】

ステップＳ８１では、署名検証部５２１は、第２の署名フィールドの１つ前の署名フィールド、すなわち、第１の署名フィールドに格納されている証明書のＳｕｂｊｅｃｔを確認する。ステップＳ８２では、署名検証部５２１は、画像署名検証に成功及び撮影者認証成功を示す情報に加えて、ステップＳ８１の確認にて特定した撮影者の情報を検証結果表示部５３に対して出力する。

【００７３】

上記のＰＣ１１における検証処理は、例えば、次のようなアプリケーションソフトウェア上に実装可能である。このアプリケーションソフトウェアは、ＨＤ１６、ＣＤ－ＲＯＭ，ＤＶＤ－ＲＯＭ等に保存されている。ユーザがキーボード１１３やマウス１１２を操作してアプリケーションソフトウェアの実行指示を入力すると、ＣＰＵ１３はＨＤ１６、ＣＤドライブ装置１７、ＤＶＤドライブ装置１８等を制御し、アプリケーションソフトウェアをＲＡＭ１５にロードさせる。そしてＣＰＵ１３がこのアプリケーションソフトウェアを実行すると、モニタ１２の表示画面上には、図６（Ｂ）の左側の画面６４が表示される

。ユーザがキーボード１１３やマウス１１２を操作して、画面６４上の画像検証ボタンを指示すると、ＰＣ１１は図６（Ａ）及び図８（Ａ）に示したフローチャートに沿った検証処理を開始する。

【００７４】

図６（Ａ）及び図８（Ａ）に示したフローチャートに沿った検証処理が完了すると、モニタ１２の表示画面上には、図８（Ｃ）の画面８３が表示される。画面８３では、画面６４にて一覧表示された各画像ファイル名に対し、対応する検証結果及び撮影者認証結果に加え、撮影者名が表示されている。撮影者認証成功と判定した撮影画像について、ステップＳ８１で確認した証明書のＳｕｂｊｅｃｔを撮影者として表示する。「－」は撮影者名の確認を実施しなかったことを示す。

【００７５】

［第３の実施形態］

第１，２の実施形態では、結合データに署名が複数付与されている、またその中にカメラ署名を必ず含む場合の例を説明した。以下では、結合データに含まれる署名が一つのみの例について説明する。また、カメラ署名が含まれない例について説明する。

【００７６】

署名が一つのみの場合において、以上説明した撮影者認証はできない。つまり撮影者認証不能となる。したがって、第１の実施形態で説明した検証処理のうち、ステップＳ７８を省略し、画像署名検証処理のみを実施することで検証処理を単純化できる。

【００７７】

また、結合データにカメラ署名が含まれない場合においても、以上説明した撮影者認証はできない。つまり撮影者認証不能となる。したがって、第１の実施形態で説明した画像署名検証処理のうち、ステップＳ７６の証明書のＳｕｂｊｅｃｔの確認において、カメラ証明書が一つも含まれない場合は、ステップＳ７８を省略し、検証処理を単純化できる。

【００７８】

［第４の実施形態］

第１の実施形態では、各署名フィールドには、該署名フィールドに格納した署名データに対応する証明書が格納されており、これにより署名データと証明書とは同じ署名フィールド内で対応付けて管理することができる。しかし、署名データと対応する証明書とを関連づけて管理することができるのであれば、証明書の管理方法は上記の管理方法に限らない。例えば、結合データ内に証明書フィールドを設け、そこに証明書を、対応する署名データと関連づけて格納するようにしても良い。また、結合データとは別個のファイルを作成し、そこに証明書を、対応する署名データと関連づけて格納するようにしても良い。

【００７９】

なお、以上説明した署名装置は、次のような構成の署名装置の一例として説明したものである。すなわち、ユーザに割り当てられた署名鍵である第１の署名鍵を用いて、入力画像の署名データを第１の署名データとして生成する（第１の生成）。また、署名装置に割り当てられた署名鍵である第２の署名鍵を用いて、入力画像及び第１の署名データを含むデータの署名データを第２の署名データとして生成する（第２の生成）。そして、第１の署名データ、第２の署名データ、入力画像を含む結合データを出力する。

【００８０】

また、以上説明した検証装置は、次のような構成の検証装置の一例として説明したものである。即ち、ユーザに割り当てられた署名鍵を用いて生成された入力画像の第１の署名データと、署名装置に割り当てられた署名鍵を用いて生成された、入力画像及び第１の署名データを含むデータの第２の署名データと、を取得する。そして、第２の署名データに対応する署名もと、第１の署名データに対応する署名もと、に応じて、署名装置のユーザの認証の可否判断を行う。

【００８１】

（その他の実施例）

本発明は、上述の実施形態の１以上の機能を実現するプログラムを、ネットワーク又は

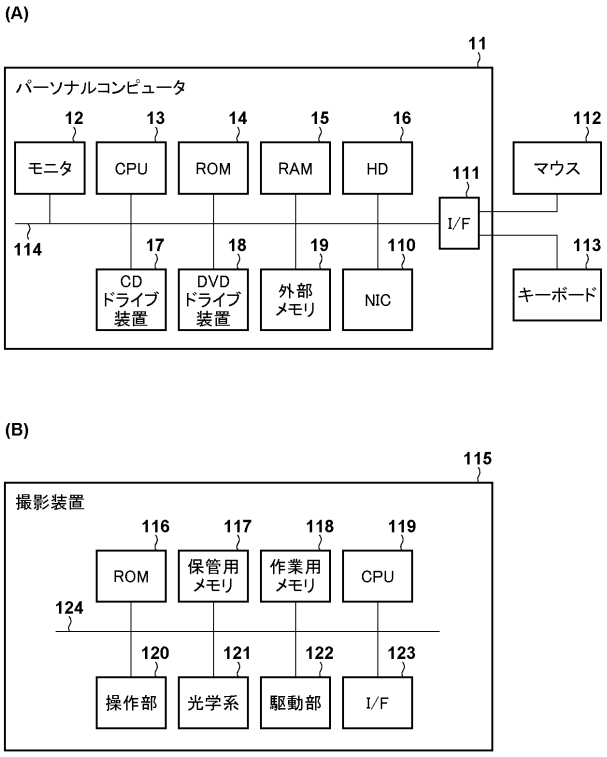
記憶媒体を介してシステム又は装置に供給し、そのシステム又は装置のコンピュータにおける１つ以上のプロセッサーがプログラムを読出し実行する処理でも実現可能である。また、１以上の機能を実現する回路（例えば、ＡＳＩＣ）によっても実現可能である。

【符号の説明】

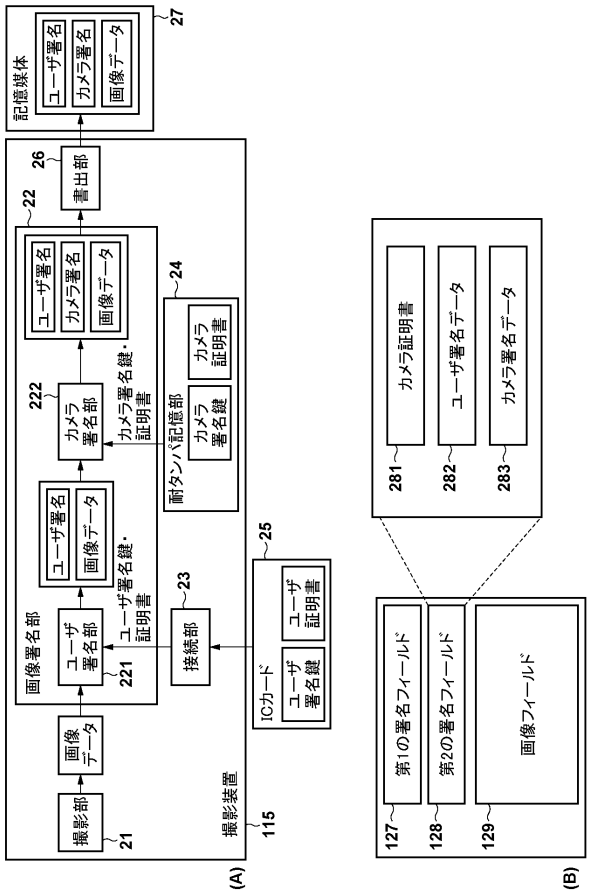
【００８２】

２２１：ユーザ署名部　２２２：カメラ署名部　２６：書き出し部

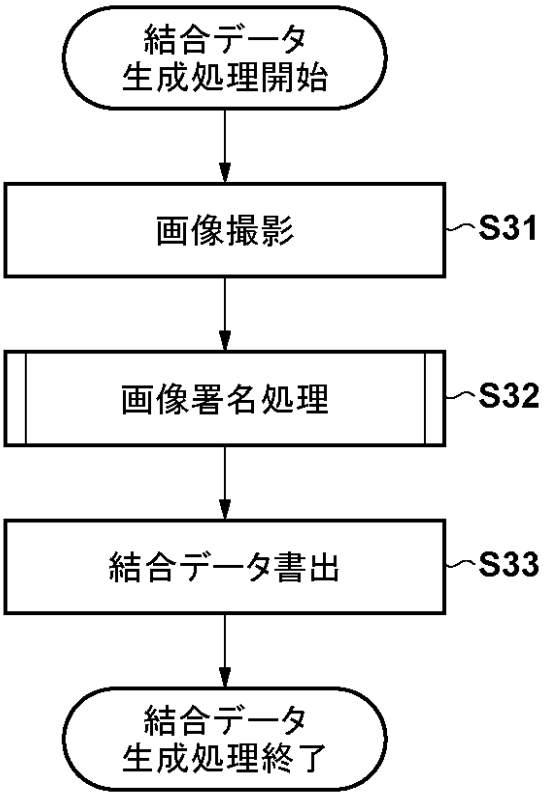
【図１】



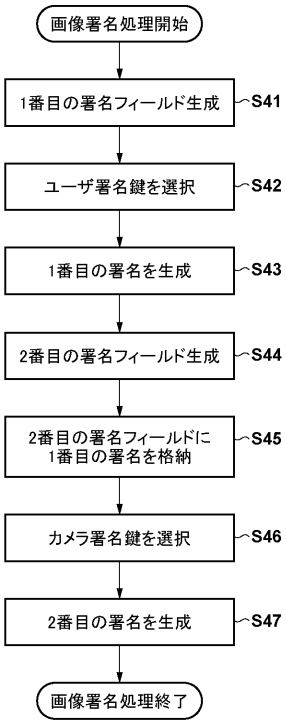
【図２】



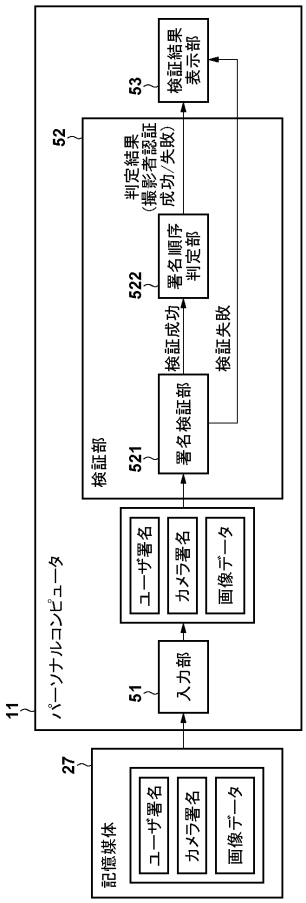
【図３】


結合データ
生成処理開始
画像撮影
S31
画像署名処理
S32
結合データ書出
S33
結合データ
生成処理終了

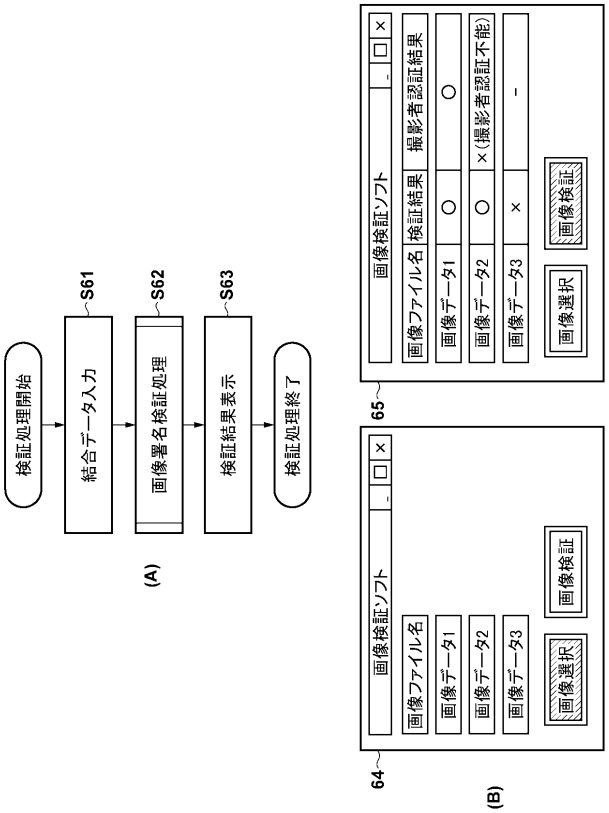
【図４】


画像署名処理開始
1番目の署名フィールド生成
S41
ユーザ署名鍵を選択
S42
1番目の署名を生成
S43
2番目の署名フィールド生成
S44
2番目の署名フィールドに
1番目の署名を格納
S45
カメラ署名鍵を選択
S46
2番目の署名を生成
S47
画像署名処理終了

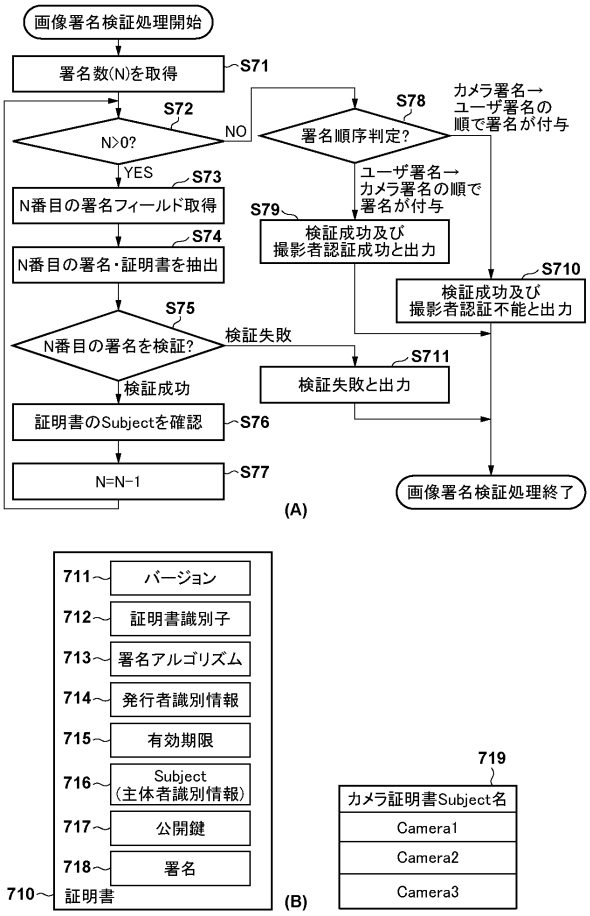
【図５】


11
パーソナルコンピュータ
51
入力部
ユーザ署名
カメラ署名
画像データ
検証部
521
署名検証部
検証成功
検証失敗
522
署名順序
判定部
判定結果
(撮影者認証
成功/失敗)
52
53
検証結果
表示部
27
記憶媒体
ユーザ署名
カメラ署名
画像データ

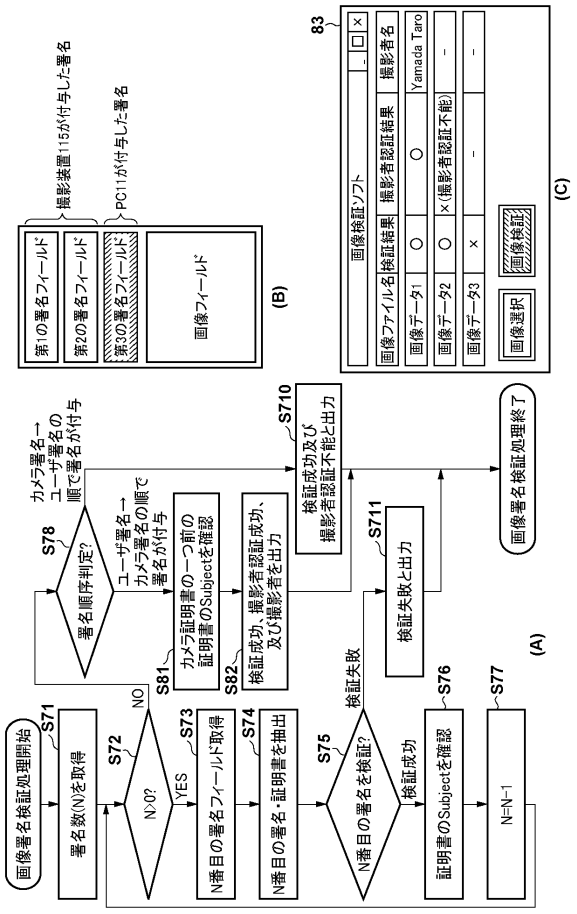
【図６】


検証処理開始
S61
結合データ入力
S62
画像署名検証処理
S63
検証結果表示
検証処理終了
(A)
画像検証ソフト
画像ファイル名
検証結果
撮影者認証結果
画像データ1
○
○
画像データ2
○
×(撮影者認証不能)
画像データ3
×
-
画像選択
画像検証
65
画像検証ソフト
画像ファイル名
画像データ1
画像データ2
画像データ3
画像選択
画像検証
64
(B)

【図７】


画像署名検証処理開始
署名数(N)を取得
S71
N>0?
S72
NO
YES
署名順序判定?
S78
カメラ署名→
ユーザ署名の
順で署名が付与
ユーザ署名→
カメラ署名の順で
署名が付与
N番目の署名フィールド取得
S73
検証成功及び
撮影者認証成功と出力
S79
N番目の署名・証明書を抽出
S74
検証成功及び
撮影者認証不能と出力
S710
N番目の署名を検証?
S75
検証失敗
検証失敗と出力
S711
検証成功
証明書のSubjectを確認
S76
N=N−1
S77
画像署名検証処理終了
(A)
711 バージョン
712 証明書識別子
713 署名アルゴリズム
714 発行者識別情報
715 有効期限
716 Subject
(主体者識別情報)
717 公開鍵
718 署名
710 証明書
(B)
719
カメラ証明書Subject名
Camera1
Camera2
Camera3

【図８】


撮影装置115が付与した署名
PC11が付与した署名
第1の署名フィールド
第2の署名フィールド
第3の署名フィールド
画像フィールド
(B)
83
画像検証ソフト
画像ファイル名
検証結果
撮影者認証結果
撮影者名
画像データ1
○
○
Yamada Taro
画像データ2
○
×(撮影者認証不能)
-
画像データ3
×
-
-
画像検証
画像選択
(C)
カメラ署名→
ユーザ署名の
順で署名が付与
S78
署名順序判定?
ユーザ署名→
カメラ署名の順で
署名が付与
S710
検証成功及び
撮影者認証不能と出力
画像署名検証処理終了
S81
カメラ証明書の一つ前の
証明書のSubjectを確認
S82
検証成功、撮影者認証成功、
及び撮影者を出力
S711
検証失敗と出力
(A)
画像署名検証処理開始
S71
署名数(N)を取得
S72
N>0?
NO
YES
S73
N番目の署名フィールド取得
S74
N番目の署名・証明書を抽出
S75
検証失敗
N番目の署名を検証?
検証成功
S76
証明書のSubjectを確認
S77
N=N−1

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 AA07 AA09 AA16 AA32 EA04 EA08 EA19 JA21 KA01 LA03
LA06 NA02 NA12 NA36 NA37 NA38 PA14