(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2005-45486
(P2005-45486A)
(43)公開日　平成17年2月17日(2005.2.17)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04N 5/91	H04N 5/91	Z	5C022
G09C 1/00	G09C 1/00	640D	5C053
H04N 5/225	H04N 5/225	A	5J104
// H04N 101:00	H04N 5/225	F	
	H04N 101:00		

審査請求 未請求　請求項の数 16　ＯＬ　（全 28 頁）

(21)出願番号　特願2003-202396(P2003-202396)
(22)出願日　平成15年7月28日(2003.7.28)

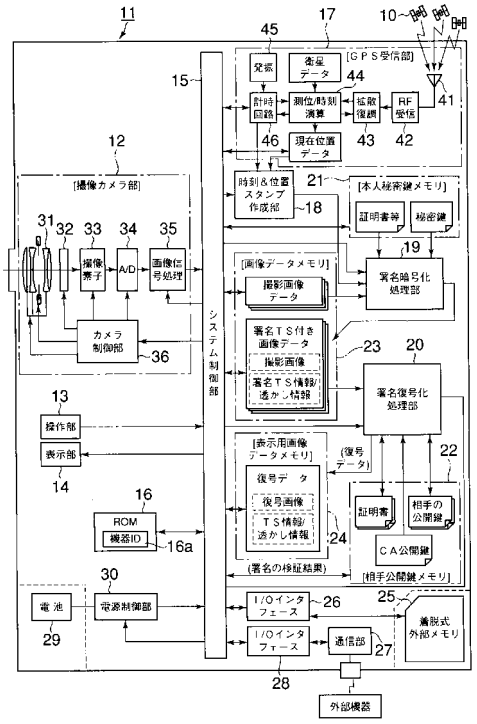
（特許庁注：以下のものは登録商標）
フロッピー

(71)出願人　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎

最終頁に続く

(54)【発明の名称】撮像装置、撮影画像の認証方法及びプログラム

(57)【要約】
【課題】ネットワークを介して特定の認証機関などへアクセスすることなく、撮影した画像の日時や場所を第三者に証明することができる撮像装置を提供する。
【解決手段】撮像装置１１はＧＰＳ受信部１７を備えて現在時刻を計時すると共に現在位置を検出する。撮像カメラ部１２による撮影時に、署名暗号化処理部１９により現在の時刻情報に基づいて撮影日時を示すタイムスタンプが作成され、現在の位置情報に基づいて撮影場所を示す位置スタンプが作成される。そして、署名暗号化処理部１９により、このタイムスタンプおよび位置スタンプの電子署名が作成され、これらのスタンプと共に画像データに付加される。これにより、認証機関へのアクセスなどを必要とせずに日時・位置認証署名付きの画像データを簡単に得て、その画像の撮影日時、場所を第三者に証明することができる。
【選択図】　図１



【特許請求の範囲】
【請求項１】
現在の時刻情報を計時する計時手段と、
被写体を撮影する撮影手段と、
この撮影手段によって被写体の画像データが得られたときに、前記計時手段によって計時された現在の時刻情報に基づいて撮影日時を示すタイムスタンプを作成するタイムスタンプ作成手段と、
このタイムスタンプ作成手段によって作成されたタイムスタンプを含む被署名データをハッシュ化した後、これを所定の暗号鍵で暗号化することで前記タイムスタンプの正当性を内部的に証明するための電子署名を作成する署名手段と、
この署名手段によって作成された電子署名を前記タイムスタンプと共に前記画像データに付加して記録する記録手段と
を具備したことを特徴とする撮像装置。
【請求項２】
現在の時刻情報を計時する計時手段と、
現在の位置情報を検出する位置検出手段と、
被写体を撮影する撮影手段と、
この撮影手段によって被写体の画像データが得られたときに、前記計時手段によって計時された現在の時刻情報に基づいて撮影場所を示すタイムスタンプを作成するタイムスタンプ作成手段と、
前記位置検出手段によって検出された現在の位置情報に基づいて撮影場所を示す位置スタンプを作成する位置スタンプ作成手段と、
前記タイムスタンプ作成手段によって作成されたタイムスタンプと前記位置スタンプ作成手段によって作成された位置スタンプを含む被署名データをハッシュ化した後、これを所定の暗号鍵で暗号化することで前記タイムスタンプおよび前記位置スタンプの正当性を内部的に証明するための電子署名を作成する署名手段と、
この署名手段によって作成された電子署名を前記タイムスタンプおよび前記位置スタンプと共に前記画像データに付加して記録する記録手段と
を具備したことを特徴とする撮像装置。
【請求項３】
前記所定の暗号鍵は、事前に特定の認証局によって証明された電子署名用の鍵であって、
前記記録手段は、前記認証局が発行した前記暗号鍵の証明書を前記画像データに加えて記録することを特徴とする請求項１または２記載の撮像装置。
【請求項４】
前記記録手段は、少なくとも前記電子署名を透かし情報として当該画像データ中に埋め込んで記録することを特徴とする請求項１または２記載の撮像装置。
【請求項５】
操作者が予め登録された所有者本人であることを認証する本人認証手段と、
この本人認証手段によって所有者本人であることが確認された場合のみ、前記電子署名を作成するように前記署名手段を制御する署名制御手段と
を備えたことを特徴とする請求項１または２記載の撮像装置。
【請求項６】
画像再生時に署名付き画像データを特定のマーク付きで表示する表示手段と、
この表示手段によって表示された画像データを復号化し、その画像データに付加された電子署名が正しいか否かを検証する署名検証手段と、
この署名検証手段によって前記電子署名が正しいことが検証された場合に、前記電子署名と共に前記画像データに付加された所定の情報を表示する表示制御手段と
を備えたことを特徴とする請求項１または２記載の撮像装置。
【請求項７】
前記表示制御手段は、前記電子署名が正しいことが検証された場合に、その旨を示す特定

のマークを前記所定の情報に付して表示することを特徴とする請求項６記載の撮像装置。
【請求項８】
前記所定の情報には、当該画像の撮影日時を示すタイムスタンプまたは撮影場所を示す位置スタンプが含まれることを特徴とする請求項６記載の撮像装置。
【請求項９】
撮影装置によって撮影された画像を認証するための認証方法であって、
現在の時刻情報を計時するステップと、
被写体の撮影により、その画像データが得られたときに、前記現在の時刻情報に基づいて撮影日時を示すタイムスタンプを作成するステップと、
この作成されたタイムスタンプを含む被署名データをハッシュ化した後、これを所定の暗号鍵で暗号化することで前記タイムスタンプの正当性を内部的に証明するための電子署名を作成するステップと、
この作成された電子署名を前記タイムスタンプと共に前記画像データに付加して記録するステップと
を備えたことを特徴とする撮影画像の認証方法。
【請求項１０】
撮影装置によって撮影された画像を認証するための認証方法であって、
現在の時刻情報を計時するステップと、
現在の位置情報を検出するステップと、
被写体の撮影により、その画像データが得られたときに、前記現在の時刻情報に基づいて撮影日時を示すタイムスタンプを作成するステップと、
前記現在の位置情報に基づいて撮影場所を示す位置スタンプを作成するステップと、
前記タイムスタンプおよび前記位置スタンプを含む被署名データをハッシュ化した後、これを所定の暗号鍵で暗号化することで前記タイムスタンプおよび前記位置スタンプの正当性を内部的に証明するための電子署名を作成するステップと、
この作成された電子署名を前記タイムスタンプおよび前記位置スタンプと共に前記画像データに付加して記録するステップと
を備えたことを特徴とする撮影画像の認証方法。
【請求項１１】
さらに、
操作者が予め登録された所有者本人であることを認証するステップと、
この認証の結果、所有者本人であることが確認された場合のみ、前記電子署名を作成するように制御するステップと
を備えたことを特徴とする請求項９または１０記載の撮影画像の認証方法。
【請求項１２】
さらに、
画像再生時に署名付き画像データを特定のマーク付きで表示するステップと、
この表示された画像データを復号化し、その画像データに付加された電子署名が正しいか否かを検証するステップと、
前記電子署名が正しいことが検証された場合に、前記電子署名と共に前記画像データに付加された所定の情報を表示するステップと
を備えたことを特徴とする請求項９または１０記載の撮影画像の認証方法。
【請求項１３】
撮影装置に搭載されたコンピュータによって実行される撮影画像認証プログラムであって、
前記コンピュータに、
現在の時刻情報を計時する機能と、
被写体の撮影により、その画像データが得られたときに、前記現在の時刻情報に基づいて撮影日時を示すタイムスタンプを作成する機能と、
この作成されたタイムスタンプを含む被署名データをハッシュ化した後、これを所定の暗

号鍵で暗号化することで前記タイムスタンプの正当性を内部的に証明するための電子署名を作成する機能と、
この作成された電子署名を前記タイムスタンプと共に前記画像データに付加して記録する機能と
を実現させるためのプログラム。
【請求項１４】
撮影装置に搭載されたコンピュータによって実行される撮影画像認証プログラムであって、
前記コンピュータに、
現在の時刻情報を計時する機能と、
現在の位置情報を検出する機能と、
被写体の撮影により、その画像データが得られたときに、前記現在の時刻情報に基づいて撮影日時を示すタイムスタンプを作成する機能と、
前記現在の位置情報に基づいて撮影場所を示す位置スタンプを作成する機能と、
前記タイムスタンプおよび前記位置スタンプを含む被署名データをハッシュ化した後、これを所定の暗号鍵で暗号化することで前記タイムスタンプおよび前記位置スタンプの正当性を内部的に証明するための電子署名を作成する機能と、
この作成された電子署名を前記タイムスタンプおよび前記位置スタンプと共に前記画像データに付加して記録する機能と
を実現させるためのプログラム。
【請求項１５】
さらに、
操作者が予め登録された所有者本人であることを認証する機能と、
所有者本人であることが確認された場合のみ、前記電子署名を作成するように制御する機能と
を実現させるための請求項１３または１４記載のプログラム。
【請求項１６】
さらに、
画像再生時に署名付き画像データを特定のマーク付きで表示する機能と、
この表示された画像データを復号化し、その画像データに付加された電子署名が正しいか否かを検証する機能と、
前記電子署名が正しいことが検証された場合に、前記電子署名と共に前記画像データに付加された所定の情報を表示する機能と
を実現させるための請求項１３または１４記載のプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、例えばデジタルカメラ等の撮像装置に係り、特に撮影画像に対する時刻や位置の認証、さらには本人の認証機能を備えた撮像装置と、この撮像装置に用いられる撮影画像の認証方法及びプログラムに関する。
【０００２】
【従来の技術】
電子化された文書の正当性を保証する技術として、デジタル署名が知られている。デジタル署名とは、電子署名、電子捺印とも呼ばれ、デジタルデータに署名情報を付加することで文書の正当性を保証するものである。署名には、公開鍵暗号が用いられる。署名者はハッシュ関数で圧縮された文書（ダイジェストと呼ぶ）と自分だけが知っている秘密鍵から署名文を作り、元の文書と一緒に送る。検証者は署名者の公開鍵と署名文と元の文書から署名が正しいかどうかを検査する。
【０００３】
このデジタル署名は第三者や受取人（検証者）によって偽造できない機能と、署名を行っ

た本人が後でそれを否認できない機能を持つ。ＰＫＩ（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ：公開鍵基盤）では、認証局と呼ばれる機関が利用者に公開鍵証明書を発行することで、公開鍵の正当性を証明している。

【０００４】

一方、電子文書などの作成日時を相手や第三者に証明するため、ネットワークを利用した時刻認証サービスやタイムスタンプサービスが考えられている。このサービスでは、時刻認証局と呼ばれる特定の機関が利用者の文書（時刻を証明したいデジタルデータのダイジェスト）にタイムスタンプを付加すると共に、その時刻認証局のデジタル署名を付与して返信することで、当該文書に付加したタイムスタンプに改ざんがないこと、そして、そのタイムスタンプが正確な日時を示していることを証明している。

【０００５】

従来、タイムスタンプに関する発明として、例えば特許文献１や特許文献２などが知られている。特許文献１では、複数の秘密鍵でデジタル署名を行うことによりタイムスタンプの信頼性を上げることを提案している。特許文献２では、携帯装置において、タイムスタンプを自動発行することを提案している。

【０００６】

また、時刻の認証とは別に、現在の位置を認証するものとして、例えば特許文献３などが知られている。特許文献３では、デジタルカメラにおいて、ＧＰＳ（ｇｌｏｂａｌ　ｐｏｓｉｔｉｏｎｉｎｇ　ｓｙｓｔｅｍ）を利用し、カメラの撮影画像に位置情報を付加することで撮影場所を証明することを提案している。

【０００７】

さらに、デジタルカメラでは、特許文献４に時刻と位置の認証に加え、電子署名を行うものが開示されている。

【０００８】

【特許文献１】

特開２０００－２３５３４０号公報

【０００９】

【特許文献２】

特開平７－２５４８９７号公報

【００１０】

【特許文献３】

特開２００１－３３５３７号公報

【００１１】

【特許文献４】

特開２００２－２１５０２９号公報

【００１２】

【発明が解決しようとする課題】

上述した時刻認証サービスやタイムスタンプサービスでは、その都度、特定機関である認証局にタイムスタンプの発行を依頼する必要があり、非常に手間のかかる問題がある。この場合、前記特許文献１など、その多くはネットワークによる認証サービスであり、自分の機器で簡易にタイムスタンプを作成することはできない。

【００１３】

また、前記特許文献２では、ネットワークによらずに自分の機器内でタイムスタンプを自動発行するものであるが、そのタイムスタンプが正しい時刻を示していることの保証はないため、信頼性に欠けるといった問題がある。

【００１４】

また、前記特許文献３では、写真を撮影した位置を記録するデジタルカメラの位置認証であるが、ネットワークを介して位置サーバへのアクセスを必要とする。このため、システムが大規模になり、さらに、撮影した画像に対する日時・場所を認証することができても、そこに本人が居たことまでを含めて証明することはできない。

【００１５】
また、前記特許文献４についても、デジタルカメラで撮影した画像に対し、日時や位置の認証を行い、さらに、その正当性を証明するために電子署名を行うようにしているが、前記各特許文献と同様にネットワークを介して認証機関へのアクセスを必要とし、電子署名を得るまでに面倒な作業と時間がかかるなどの問題がある。
【００１６】
本発明は前記のような点に鑑みなされたもので、ネットワークを介して特定の認証機関などへアクセスすることなく、撮影した画像の日時や場所を第三者に証明することができる認証機能付きの撮像装置と、この撮像装置に用いられる撮影画像の認証方法及びプログラムを提供することを目的とする。
【００１７】
【課題を解決するための手段】
本発明の請求項１に係る撮像装置は、現在の時刻情報を計時する計時手段と、被写体を撮影する撮影手段と、この撮影手段によって被写体の画像データが得られたときに、前記計時手段によって計時された現在の時刻情報に基づいて撮影日時を示すタイムスタンプを作成するタイムスタンプ作成手段と、このタイムスタンプ作成手段によって作成されたタイムスタンプを含む被署名データをハッシュ化した後、これを所定の暗号鍵で暗号化することで前記タイムスタンプの正当性を内部的に証明するための電子署名を作成する署名手段と、この署名手段によって作成された電子署名を前記タイムスタンプと共に前記画像データに付加して記録する記録手段とを具備したことを特徴とする。
【００１８】
このような構成によれば、例えばＧＰＳあるいは電波時計などを利用して現在の時刻情報が計時される。そして、被写体の撮影により、その画像データが得られたときに、そのときの時刻情報に基づいて撮影日時を示すタイムスタンプが作成される。さらに、この作成されたタイムスタンプの電子署名が内部的に作成され、前記タイムスタンプと共に前記画像データに付加される。これにより、認証機関へのアクセスなどを必要とせずに日時認証署名付きの画像データを簡単に得ることができ、その画像の撮影日時を第三者に証明することができる。
【００１９】
本発明の請求項２に係る撮像装置は、現在の時刻情報を計時する計時手段と、現在の位置情報を検出する位置検出手段と、被写体を撮影する撮影手段と、この撮影手段によって被写体の画像データが得られたときに、前記計時手段によって計時された現在の時刻情報に基づいて撮影場所を示すタイムスタンプを作成するタイムスタンプ作成手段と、前記位置検出手段によって検出された現在の位置情報に基づいて撮影場所を示す位置スタンプを作成する位置スタンプ作成手段と、前記タイムスタンプ作成手段によって作成されたタイムスタンプと前記位置スタンプ作成手段によって作成された位置スタンプを含む被署名データをハッシュ化した後、これを所定の暗号鍵で暗号化することで前記タイムスタンプおよび前記位置スタンプの正当性を内部的に証明するための電子署名を作成する署名手段と、この署名手段によって作成された電子署名を前記タイムスタンプおよび前記位置スタンプと共に前記画像データに付加して記録する記録手段とを具備したことを特徴とする。
【００２０】
このような構成によれば、例えばＧＰＳあるいは電波時計などを利用して現在の時刻情報が計時され、また、現在の位置情報が検出される。そして、被写体の撮影により、その画像データが得られたときに、そのときの時刻情報に基づいて撮影日時を示すタイムスタンプが作成され、また、位置情報に基づいて撮影場所を示す位置スタンプが作成される。さらに、この作成されたタイムスタンプおよび位置スタンプの電子署名が内部的に作成され、前記タイムスタンプおよび前記位置スタンプと共に前記画像データに付加される。これにより、認証機関へのアクセスなどを必要とせずに日時・位置認証署名付きの画像データを簡単に得ることができ、その画像の撮影日時を第三者に証明することができる。
【００２１】

また、本発明の請求項３では、前記請求項１または２記載の撮像装置において、前記所定の暗号鍵は、事前に特定の認証局によって証明された電子署名用の鍵であって、前記記録手段は、前記認証局が発行した前記暗号鍵の証明書を前記画像データに加えて記録することを特徴とする。

【００２２】

このような構成によれば、事前に特定の認証局によって証明された暗号鍵を用いて電子署名が作成され、その電子署名の証明書を含めて画像データに付加されるので、撮影画像に対して内部的に付した時刻認証あるいは位置認証としての信頼性をさらに高めることができる。

【００２３】

また、本発明の請求項４では、前記請求項１または２記載の撮像装置において、前記記録手段は、少なくとも前記電子署名を透かし情報として当該画像データ中に埋め込んで記録することを特徴とする。

【００２４】

このような構成によれば、電子署名が作成された際に、透かし情報として画像データ中に埋め込まれるので、その電子署名のデータを勝手に改ざんするができず、また、当該画像の不正利用を防止することができる。

【００２５】

また、本発明の請求項５では、前記請求項１または２記載の撮像装置において、操作者が予め登録された所有者本人であることを認証する本人認証手段と、この本人認証手段によって所有者本人であることが確認された場合のみ、前記電子署名を作成するように前記署名手段を制御する署名制御手段とを備えたことを特徴とする。

【００２６】

このような構成によれば、本人認証により所有者本人であることが確認された場合のみ電子署名の作成がなされ、その電子署名と共にタイムスタンプ（または位置スタンプを含む）が画像データに付加される。したがって、この署名付きの画像データを用いて、所有者本人がその画像を撮影した日時に所在していたことを証明することができ、また、その撮影場所に所在していたことを証明することができる。

【００２７】

また、本発明の請求項６では、前記請求項１または２記載の撮像装置において、画像再生時に署名付き画像データを特定のマーク付きで表示する表示手段と、この表示手段によって表示された画像データを復号化し、その画像データに付加された電子署名が正しいか否かを検証する署名検証手段と、この署名検証手段によって前記電子署名が正しいことが検証された場合に、前記電子署名と共に前記画像データに付加された所定の情報を表示する表示制御手段とを備えたことを特徴とする。

【００２８】

このような構成によれば、例えば他の機器から受け取った画像データを再生する場合において、その画像データが署名付きであった場合にその旨を示す特定のマーク付きで表示される。そして、この画像データの復号化により、そこに付加された電子署名が検証され、正しいことが検証された場合にのみ、前記電子署名と共に付加されていた所定の情報が表示されることになる。

【００２９】

また、本発明の請求項７では、前記請求項５記載の撮像装置において、前記表示制御手段は、前記電子署名が正しいことが検証された場合に、その旨を示す特定のマークを前記所定の情報に付して表示することを特徴とする。

【００３０】

このような構成によれば、特定のマークの表示により、画像データに付加されていた電子署名が正しいことを確認することができる。

【００３１】

また、本発明の請求項８では、前記請求項５記載の撮像装置において、前記所定の情報に

は、当該画像の撮影日時を示すタイムスタンプまたは撮影場所を示す位置スタンプが含まれることを特徴とする。

【００３２】

このような構成によれば、前記電子署名の検証結果として、当該画像データの撮影日時を示すタイムスタンプまたは撮影場所を示す位置スタンプを確認することができる。

【００３３】

【発明の実施の形態】

以下、図面を参照して本発明の実施形態を説明する。

【００３４】

（第１の実施形態）

図１は本発明の第１の実施形態に係る日時・位置認証機能付きの撮像装置１１の構成を示すブロック図である。

【００３５】

この撮像装置１１は、例えばデジタルカメラやカメラ付き携帯電話などからなり、被写体の画像を撮影するための撮像機能の他に、ＧＰＳ受信機を内蔵し、ＧＰＳ衛星から高精度の時刻信号と測位信号を受信する機能と、このＧＰＳ受信機によって受信された高精度な時刻信号に基づいて現在日時を計時し、撮影時にその撮影日時を示すタイムスタンプを作成する機能、前記ＧＰＳ受信機によって受信された高精度な測位信号に基づいて現在位置を検出し、撮影時にその撮影場所を示す位置スタンプを作成する機能、このタイムスタンプおよび位置スタンプの正当性を証明するための電子署名を作成する機能を備える。

【００３６】

また、時刻や位置の認証に用いる秘密鍵とその秘密鍵に対応した公開鍵が正当なものであることを証明した証明書を記憶する機能、そして、これらの証明書を含めてタイムスタンプおよび位置スタンプを電子署名付きで撮影画像に記録する機能、さらに、電子署名などを透かし情報として撮影画像に埋め込む機能などを備える。前記証明書は、所定の手続きを経て特定の認証局から事前に発行されたものであり、後述するように耐タンパー性の認証モジュールなどに秘密鍵や公開鍵などと共に記憶されている。　図１では、これらの機能を含めた構成が示されている。

【００３７】

すなわち、本実施形態における撮像装置１１には、撮像カメラ部１２、操作部１３、表示部１４、システム制御部１５、ＲＯＭ１６などのカメラとしての基本構成部品の他に、ＧＰＳ受信部１７、時刻＆位置スタンプ作成部１８、署名暗号化処理部１９、署名復号化処理部２０、本人秘密鍵メモリ２１、相手公開鍵メモリ２２、画像データメモリ２３、表示用画像データメモリ２４などが設けられている。

【００３８】

また、この撮像装置１１には、例えばフラッシュメモリカードなどの着脱式の外部メモリ２５とそのＩ／Ｏインタフェース２６、ＰＣ等の外部機器との間のデータ通信を行うための通信部２７とそのＩ／Ｏインタフェース２８、さらに、電池２９とその電源制御部３０などが設けられている。

【００３９】

撮像カメラ部１２は、光学系３１、シャッター機構３２、撮像素子３３、Ａ／Ｄ変換器３４、画像信号処理回路３５、カメラ制御部３６などからなり、カメラ制御部３６の制御の下で図示せぬシャッターキーの押下により被写体を撮影し、その撮影画像をデジタルデータに変えて処理する。このカメラ制御部３６による制御には、例えばズーム制御、絞り制御、シャッター制御、タイミング制御、フラッシュ制御などが含まれる。

【００４０】

なお、この撮像カメラ部１２の構成については特に限定されるものではなく、被写体の画像を取得可能な構成であれば良い。この撮像カメラ部１２で得られた画像データは、所定の圧縮方式で圧縮されて画像データメモリ２３に格納される。

【００４１】

操作部１３は、例えば電源キーやシャッターキー、メニューキー、カーソールキーなど、カメラ操作に必要な各種キーなどを含む入力デバイスからなる。表示部１４は、例えばカラー液晶表示デバイスからなり、被写体の画像を表示する場合などに用いられる。

【００４２】

システム制御部１５は、本装置全体の制御を行うマイクロプロセッサ（ＣＰＵ）からなり、ＲＯＭ１６などに記憶されたプログラムを読み込むことにより、そのプログラムに記述された手順に従って各種処理を実行する。ＲＯＭ１６には、プログラムなどのシステム制御部１５の処理動作に必要な各種データが記憶されている。

【００４３】

ＧＰＳ受信部１７は、ＧＰＳ衛星１０から発振される高精度な時刻信号を含む測位信号を受信するものである。このＧＰＳ受信部１７は、ＧＰＳ受信アンテナ４１、ＲＦ受信回路４２、スペクトル拡散復調回路４３、測位／時刻演算回路４４、発振器４５、計時回路４６などから構成される。

【００４４】

ＧＰＳ測位の原理は、ＧＰＳ受信機により複数のＧＰＳ衛星から高精度の時刻信号を含む測位信号とそれに含まれた航法メッセージデータを受信し、各衛星毎の疑似乱数符号を作成してスペクトル逆拡散復調および復号し、各衛星の詳細軌道情報を求め、各衛星の３次元位置座標を推測演算し、測位電波信号から求めた各衛星からの疑似距離と各衛星の３次元位置座標とから３次元測量で逆算することにより、機器の地上位置座標を求めるといったものである。

【００４５】

また、その際にＧＰＳ系の標準時間（ＧＰＳ時）を高精度で算出することができる。ＧＰＳ時は、国際原子時と１９秒遅れ、協定世界時と約８秒遅れであるが、計時精度はほぼ同等の高精度であり、これを、協定世界時（ＵＴＣ）や日本標準時（ＪＳＴ）などに換算して内蔵時計を間欠的に補正すれば、高精度の時刻データ（タイムスタンプデータ）を作成できる。

【００４６】

時刻＆位置スタンプ作成部１８は、ＧＰＳ受信部１７にて受信された高精度の時刻信号に基づいて現在日時を示すタイムスタンプを作成すると共に、前記時刻信号と共に受信される測位信号に基づいて現在位置を示す位置スタンプを作成する処理を行う。この時刻＆位置スタンプ作成部１８で作成されたタイムスタンプと位置スタンプのデータは署名暗号化処理部１９に与えられる。

【００４７】

署名暗号化処理部１９は、データのダイジェストを作成する処理を含み、そのダイジェストを秘密鍵で暗号化して電子署名を作成して撮影画像に付加する処理を行う。本人秘密鍵メモリ２１には、このときに用いられる秘密鍵やその証明書などが記憶されている。また、この署名暗号化処理部１９は、前記電子署名などを撮影画像中に埋め込むための電子透かし処理を行う機能を有する。

【００４８】

署名復号化処理部２０は、電子署名付きの画像データを復号化する処理を行う。相手公開鍵メモリ２２には、このときに用いられる相手の公開鍵やその証明書などが記憶されている。また、この署名復号化処理部２０には、画像データ中に埋め込められた透かし情報を復号化する機能を有する。

【００４９】

なお、これらの時刻および位置の認証に関係する各回路（署名暗号化処理部１９、署名復号化処理部２０、本人秘密鍵メモリ２１、相手公開鍵メモリ２２）は集積化して１チップの認証チップとして構成したり、あるいは、耐タンパー性の認証モジュールに格納することが望ましい。これにより、偽造やハッキングに強く、第三者に対して信頼度の高い認証機器を実現できる。

【００５０】

画像データメモリ２３には、撮像カメラ部１２によって得られた撮影画像が記憶される。また、その撮影画像を元データとして署名暗号化処理部１９によって生成された署名ＴＳ付きの画像データが記憶される。なお、図中の「ＴＳ」とはタイムスタンプのことであるが、本実施形態では位置スタンプも含むものとする。

【００５１】

表示用画像データメモリ２４には、署名復号化処理部２０によって復号化されデータが記憶される。この復号データは、撮影画像と、その撮影画像に透かし情報として埋め込まれていた電子署名やＴＳ情報（タイムスタンプと位置スタンプ）などからなる。

【００５２】

外部メモリ２５は、例えばフラッシュメモリカードなどからなり、撮像装置１１に設けられたメモリスロットに着脱自在に装着される。この外部メモリ２５には、撮影画像などが記録される。

【００５３】

通信部２７は、例えばパーソナルコンピュータやＰＤＡ等の外部機器と接続し、その外部機器との間で画像等のデータの送受信処理を行う。なお、外部機器との接続手段としては、シリアルケーブルやＵＳＢケーブルによる有線接続、赤外線や無線電波による無線接続などがあり、その接続形態については特に限定されるものではない。

【００５４】

電池２９は、リチウム充電池やニッケル水素充電池などからなり、携帯時における駆動源として用いられる。電源制御部３０は、この電池２９を駆動源として各部の駆動に必要な電圧の供給制御を行う。

【００５５】

このような構成において、例えば取引相手等に撮像装置１１で撮影した画像を送る場合に、その撮影画像データとタイムスタンプ等をハッシュ化し、これを秘密鍵で暗号化した電子署名を付して送信する。

【００５６】

受信者側では、ＣＡの公開鍵により、その画像データ内の証明書を復号して、発信者の正当な公開鍵を入手し、発信者の公開鍵で電子署名を復号したハッシュ値と、受信データ（被ハッシュ化部分）をハッシュ化した値とを照合すれば、発信者が撮影画像データに署名した本人であり、撮影画像データに改ざんがないことを確認できる。

【００５７】

また、この撮影画像データには、正確な標準時刻信号に基づく高精度計時による日時データや位置データも記録され、また、この日時データや位置データも電子署名の検証により、偽造改ざんを容易に検証確認できるので、発信者の正当性やデータの真正性だけでなく、撮影日時、撮影場所の正確性や信頼性（真偽）も第三者に証明できる。

【００５８】

次に、本実施形態における撮像装置１１の各機能について詳しく説明する。

【００５９】

［日時・位置認証］

撮像装置１１は、現在時刻を示すタイムスタンプと現在位置を示す位置スタンプを作成する機能（時刻＆位置スタンプ作成部１８）を備えると共に、これらのスタンプの正当性を証明するための電子署名を作成する機能（署名暗号化処理部１９）を備えており、これらを撮影画像に付加して記録し、さらに必要に応じて外部機器に送信することができる。

【００６０】

図２はタイムスタンプ（位置スタンプを含む）と電子署名の作成方法（第１の方法）を説明するための図であり、図中の括弧内の数字はその作成手順の番号を示す。

【００６１】

（１）まず、撮像装置１１に備えられた撮像カメラ部１２によって撮影された被写体の画像データを元データとして得る。

【００６２】

（２）次に、時刻＆位置スタンプ作成部１８によってタイムスタンプと位置スタンプを作成し、これらのスタンプデータを元データである撮影画像データに付加する。また、このときに機器のＩＤや証明書等も付加する。機器ＩＤは本機器（撮像装置１１）に付けられた識別時情報であり、図１に示すＲＯＭ１６の所定の領域１６ａなどに記憶されている。また、ここでの証明書とは、本機器がデータの暗号化に用いる秘密鍵が正当なものであることを証明したものであり、事前に認証局で発行してもらったものである。この証明書は電子機器１１内の本人秘密鍵メモリ２１に秘密鍵と共に記憶されている。

【００６３】

（３）ここで、元データである撮影画像データに少なくともタイムスタンプと位置スタンプを結合し、その結合データを被署名データとしてハッシュ関数にてハッシュ化（圧縮化）して当該データのダイジェストを作成し、これを秘密鍵で暗号化することにより電子署名を内部的に作成する。なお、ダイジェストを作成する場合に、元データにタイムスタンプ、位置スタンプの他に、例えばＩＤや証明書等の他のデータを含ませることでも良い。また、タイムスタンプや位置スタンプのみからダイジェストを作成することも可能である。

【００６４】

（４）このようにして作成された電子署名をタイムスタンプ、位置スタンプなどと共に元データである撮影画像に付加する。これにより、日時・位置認証署名付きの画像データが得られる。

【００６５】

図３はタイムスタンプ（位置スタンプを含む）と電子署名の作成方法（第２の方法）を説明するための図である。第２の方法では、元データである撮影画像のハッシュ値とタイムスタンプや他のデータそのものとを結合し、それを秘密鍵で暗号化して電子署名を作成する。図中の括弧内の数字はその作成手順の番号を示す。

【００６６】

（１）まず、撮像装置１１に備えられた撮像カメラ部１２によって撮影された被写体の画像データを元データとして得る。

【００６７】

（２）前記元データである画像データをハッシュ関数にてハッシュ化（圧縮化）する。

【００６８】

（３）このとき得られたハッシュ値に少なくともタイムスタンプと位置スタンプを結合する。なお、タイムスタンプと位置スタンプの他に、例えばＩＤや証明書等の他のデータを含ませることでも良い。

【００６９】

（４）続いて、前記（３）で得られた結合データを被署名データとして秘密鍵で暗号化することにより電子署名を内部的に作成する。

【００７０】

（５）このようにして作成された電子署名をタイムスタンプ、位置スタンプなどと共に撮影画像のハッシュ値に付加する。

【００７１】

図４はタイムスタンプ（位置スタンプを含む）と電子署名の作成方法（第３の方法）を説明するための図である。第３の方法では、電子署名に加え、その電子署名を透かし情報として撮影画像に埋め込むようにしている。図中の括弧内の数字はその処理手順の番号を示す。

【００７２】

（１）まず、撮像装置１１に備えられた撮像カメラ部１２によって撮影された被写体の画像データを取得する。そして、その撮影画像のファイル名や撮影条件、著作権情報等を元データとして、その元データに少なくともタイムスタンプと位置スタンプを結合する。

【００７３】

（２）次に、前記（１）で得られた結合データを被署名データとしてハッシュ関数にてハ

ッシュ化（圧縮化）して当該データのダイジェストを作成し、これを秘密鍵で暗号化することにより電子署名を内部的に作成する。なお、電子署名の作成方法としては、これに限るものではなく、前記図２や図３で説明したような方法、あるいは、その他の方法であっても良い。

【００７４】

（３）電子署名が作成されると、所定の変換演算により透かし情報として撮影画像に埋め込む。

【００７５】

（４）このようにして電子署名を透かし情報として埋め込んだ撮影画像が得られると、その撮影画像にタイムスタンプ、位置スタンプなどを付加する。この場合、撮影画像に電子署名の透かしが入っているため、その画像の正当性を証明でき、さらに、当該画像の不正利用を防止することができる。

【００７６】

［電子透かし］

撮像装置１１は、電子署名などを透かし情報として画像データ中に埋め込むための電子透かし機能（本実施形態では署名暗号化処理部１９に含まれているものとする）を備えている。

【００７７】

図５は電子透かしによる撮影画像の変換処理を模式的に示したものであり、上述した図４の処理手順に対応している。すなわち、撮影画像のファイル名や撮影条件、著作権情報等を元データとし、そのハッシュ値にタイムスタンプ、位置スタンプ、ＩＤなどを結合し、これらを圧縮演算した後、秘密鍵で暗号化することにより電子署名データを得る。この電子署名データを電子透かし変換演算して撮影画像中に埋め込むことにより、透かし入りの撮影画像が得られる。

【００７８】

なお、撮影画像に埋め込むべき透かし情報には、前記電子署名の他に、例えばＩＤ情報や証明書、さらに画像ファイル名や画像ＩＤ、画像フォーマットや画像サイズ、撮影条件（絞りやシャッタースピード、露出、使用レンズ、フィルタなど）などを加えても良い。

【００７９】

また、図６乃至図８に示すように、電子透かしのための変換処理には様々な方法がある。図６は基本的な方法であり、所定の変換処理にて電子署名等を含んだ透かし情報を撮影画像データの所定の位置に埋め込む方法を示している。

【００８０】

図７は周波数変換を利用した方法を示しており、撮影画像データの周波数成分に電子署名等を含んだ透かし情報を埋め込む場合である。この例では、例えばＦＦＴ高速フーリエ変換やＤＣＴ離散コサイン変換などの直交関数による周波数変換処理による方法が示されている。

【００８１】

図８は電子署名等を含んだ透かし情報を所定の鍵により発生した乱数ノイズで変調し、知覚特性モデルにより強度を調整して撮影画像データに埋め込む方法が示されている。この場合、復調時には同様に乱数ノイズで変調したデータを蓄積し、統計的推論復号を行う。

【００８２】

［メモリ格納形式］

図９は撮像装置１１のメモリ格納形式の一例を示す図であり、撮像装置１１の内部メモリである画像データメモリ２３と、メモリカード等からなる着脱式の外部メモリ２５に格納される画像ファイルの形式が示されている。

【００８３】

画像データメモリ２３と外部メモリ２５には、それぞれに対応した形式にて元データである画像データファイルの他に、上述した方法により作成されたタイムスタンプ、位置スタンプ、電子署名付きの画像データファイル（日時・位置認証署名付き画像データファイル

）や、これらを透かし情報として埋め込んだ画像データファイル（電子透かし埋込み画像データファイル）が格納される。

【００８４】

［署名検証］

撮像装置１１は、上述したようなタイムスタンプ、位置スタンプ、電子署名付きの画像データを他の機器から受け取った場合に、その画像データの署名検証を行う機能（署名復号化処理部２０）を備えている。

【００８５】

この場合、画像データを分解復号し、添付の証明書を認証局（ＣＡ）の公開鍵で復号して、発信者または発信元の機器の公開鍵を入手し、この公開鍵（署名検証鍵）で電子署名を復号化し、受信した画像データの該当部分のハッシュ値を同じハッシュ関数で生成して、電子署名の復号データと照合すれば、正当な発信者または機器による電子署名であること、撮影画像やタイムスタンプの時刻や位置スタンプの場所に偽造や改ざんがないことを検証できる。

また、署名検証結果が成功であった場合には、再生画像と共に復号したタイムスタンプや位置スタンプの情報、電子署名データ（ダイジェストのハッシュ値）や、検証の成功を示す特定のマークを合せて表示部１４に表示する。一方、署名検証結果が失敗であった場合には、再生画像と共に署名検証の失敗を示す特定のマークを合せて表示部１４に表示する。このように、画面の表示を見るだけで、署名検証結果を簡単に把握することができる。

【００８６】

ここで、上述した日時・位置認証と署名検証に関する処理について詳しく説明する。

【００８７】

図１０および図１１は撮像装置１１における日時・位置認証と署名検証に関する処理を示すフローチャートである。なお、このフローチャートを含め、以下の各フローチャートで示される処理は、撮像装置１１に設けられたシステム制御部１５（ＣＰＵ）がプログラムに記述された手順に従って各部の動作を制御することにより実行される。

【００８８】

まず、ホールド状態で計時キャリーがあると（ステップＡ１１、Ａ１２のＹｅｓ）、現在日時を計時するための計時処理が実行されて（ステップＡ１３）、その計時処理に伴い現在の日時データが更新される（ステップＡ１４）。

【００８９】

このときにＧＰＳ自動受信が設定されていれば（ステップＡ１５のＹｅｓ）、撮像装置１１に設けられたＧＰＳ受信部１７にてＧＰＳ衛星１０からのＧＰＳ信号（時刻信号と測位信号）が所定の間隔で自動受信される。そして、このＧＰＳ信号に基づいてＧＰＳ時刻と測位の演算処理が実行され（ステップＡ１６）、その演算結果に基づいて日時データと位置データが更新される（ステップＡ１７）。

【００９０】

また、所定のキー操作によりＧＰＳ強制受信が指示された場合には（ステップＡ１８、Ａ１９のＹｅｓ）、その指示に従ってＧＰＳ信号が強制受信される。そして、前記同様に、このＧＰＳ信号に基づいてＧＰＳ時刻と測位の演算処理が実行され（ステップＡ２０）、その演算結果に基づいて日時データと位置データが更新される（ステップＡ２１）。

【００９１】

このようにして、日時データと位置データが更新されると、これらのデータに基づいて現在日時と現在位置を示す情報が撮像装置１１の表示部１４の画面上に所定の表示形態で表示される（ステップＡ２２）。また、その他の情報が同画面上に表示される（ステップＡ２３）。

【００９２】

ここで、カメラ撮影が行われた場合（ステップＡ２４のＹｅｓ）、撮像カメラ部１２による所定の撮像処理が実行され、そのときの撮影画像のデータが画像データメモリ２３に記憶される（ステップＡ２５）。その際、所定の操作により撮影日時（撮影場所を含む）の

記録が指示されると（ステップＡ２６のＹｅｓ）、現在の日時データおよび位置データに基づいて当該撮影画像の撮影日時と撮影場所の記録が行われる（ステップＡ２７～Ａ３０）。

【００９３】

また、タイムスタンプと位置スタンプの記録要求があると（ステップＡ３１のＹｅｓ）、時刻＆位置スタンプ作成部１８により撮影日時を示すタイムスタンプと撮影場所を示す位置スタンプの作成が行われる（ステップＡ３２）。

【００９４】

続いて、署名暗号化処理部１９により、前記作成されたタイムスタンプと位置スタンプの正当性を証明するための電子署名が内部的に作成される（ステップＡ３３）。このときの電子署名の作成処理については、図２乃至図５で既に説明したいずれかの方法が用いられる。

【００９５】

この電子署名をタイムスタンプと位置スタンプなどと共に当該撮影画像に付加することで、日時・位置認証署名付きの画像データが得られる（ステップＡ３６）。この場合、日時・位置認証署名付きの画像データに、事前に認証局で発行された暗号鍵の証明書を加えておけば、撮影画像に対して内部的に付した時刻認証や位置認証としての信頼性をさらに高めることができる。この日時・位置認証署名付きの画像データは、画像データメモリ２３に記憶された後（ステップＡ３４）、表示部１４の画面上に表示される（ステップＡ３５）。

【００９６】

このように、ネットワークを介して認証機関にアクセスしなくとも、被写体を撮影したときに、本機器内にて、そのときの時刻を示すタイムスタンプと場所を示す位置スタンプを作成し、これらを証明するための電子署名を本機器内にて自動発行して撮影画像に付加して記録することができる。

【００９７】

なお、電子透かし機能を利用する場合には、前記電子署名などが透かし情報として当該撮影画像に埋め込まれることになるが、この電子透かしに関する処理について後に図１２および図１３を参照して説明する。

【００９８】

一方、例えば外部メモリ２５や通信部２７を通じて受け取った画像データを再生する場合において（ステップＡ３６のＹｅｓ）、その画像データが署名付きの画像であれば（ステップＡ３７）、所定の操作指示に従って署名復号化処理部２０により当該画像が復号化され、そこに付されていた電子署名の検証処理が行われる（ステップＡ３８～Ａ４３）。

【００９９】

詳しくは、画像データの復号、分解処理が行われ、その復号データから被署名データが復元される。また、復号データ内の証明書等が認証局（ＣＡ）の公開鍵で復号され、発信者または発信元の機器の公開鍵が入手される。この公開鍵（署名検証鍵）で電子署名を復号し、被署名データをハッシュ化することでダイジェストを作成することで、そのダイジェストと電子署名の復号データとの照合により、正当な発信者または機器による正しい電子署名であること、撮影画像やタイムスタンプの時刻や位置スタンプの場所に偽造や改ざんがないことを検証できる。

【０１００】

なお、後述するように、署名付きの画像を撮像装置１１で表示した場合には、その旨を示す特定のマーク（図２３、図２４に示す鍵マーク１０３）が表示されるようになっている。

【０１０１】

ここで、署名検証結果が成功であった場合には（ステップＡ４４のＹｅｓ）、署名検証の成功を示す特定のマーク（図２３、図２４に示す署名検証済みマーク１０６）と共に、この画像データに電子署名と共に付加されていたタイムスタンプや位置スタンプを含む所定

の情報が当該画像に対応付けられて表示される（ステップＡ４５、Ａ４６）。
【０１０２】
また、署名検証結果が失敗であった場合には（ステップＡ４４のＮｏ）、署名検証の失敗を示す特定のマーク（例えば“×”や“ＮＧ”など）が当該画像上に表示され、タイムスタンプや位置スタンプ等の情報は表示されない（ステップＡ４７、Ａ４８）。
【０１０３】
このように、画像データに付加されていた電子署名が正しかった場合のみ、その旨を示す特定のマークと共にタイムスタンプや位置スタンプなどが表示されるので、画面上で偽造改ざんを容易に検証確認することができる。
【０１０４】
次に、電子透かしに関する処理について説明する。
【０１０５】
図１２は撮像装置１１における電子透かし埋込み画像の作成処理を示すフローチャートであり、図１０のステップＡ３１以降の処理に対応している。すなわち、撮像装置１１によるカメラ撮影後、所定の操作によりタイムスタンプ、位置スタンプの記録要求があると、システム制御部１５の制御の下で以下のような処理が実行される。
【０１０６】
まず、撮影画像が得られたときのタイミングで、時刻＆位置スタンプ作成部１８により現在の日時データに基づいて撮影日時を示すタイムスタンプが作成されると共に、現在の位置データに基づいて撮影場所を示す位置スタンプが作成される（ステップＢ１１）。
【０１０７】
続いて、署名暗号化処理部１９によりタイムスタンプと位置スタンプの正当性を証明するための電子署名が作成される（ステップＢ１２～Ｂ１４）。詳しくは、撮影画像データ、タイムスタンプ、位置スタンプ、さらにＩＤや証明書を加えるなどして被署名データが作成される。そして、これらをハッシュ化してダイジェストが作成され、これを秘密鍵で暗号化することで日時・位置認証用の電子署名が作成される。
【０１０８】
ここで、前記作成された電子署名などに基づいて透かし情報が作成される（ステップＢ１５）。この場合、電子署名を透かし情報として画像中に埋め込むことは別に、タイムスタンプ、位置スタンプ、証明書などの情報と共に元画像に付加しても良し（図４参照）、これらの情報を透かし情報に含めて画像中に埋め込むようにしても良い。
【０１０９】
そして、所定の変換処理により、前記透かし情報を画像中に埋め込んだ画像データが作成されて（ステップＢ１６）、画像データメモリ２３に記憶される（ステップＢ１７）。前記所定の変換処理とは、例えば図７に示したように、画像データを直交変換などにより周波数データに変換し、所定の周波数帯域に透かし情報を埋込み処理した後、直交逆変換により元の画像データに戻すような処理を行う。
【０１１０】
このようにして得られた電子透かし埋込み画像は、日時・位置認証署名付きの画像として画像データメモリ２３に記憶される。この画像中の所定の位置には少なくとも電子署名が透かし情報として入っている。
【０１１１】
図１３は撮像装置１１における電子透かし埋込み画像の復号処理と署名検証処理を示すフローチャートであり、図１１のステップＡ４０以降の処理に対応している。すなわち、例えば外部メモリ２５や通信部２７を通じて受け取った他機器の画像データを再生する場合において、その画像データが電子透かし入りの画像データであった場合には、システム制御部１５の制御の下で以下のような処理が実行される。
【０１１２】
まず、署名復号化処理部２０により当該画像データが復号変換処理され、そこに埋め込まれていた透かし情報が復号化される（ステップＣ１１）。前記復号変換処理としては、例

えば画像データを直交変換などにより周波数データに変換し、所定の周波数帯域から透かし情報を取り出すような処理を行う。

【０１１３】

このようにして透かし情報が取り出されると、その透かし情報に含まれる電子署名の検証処理が行われる（ステップＣ１２～Ｃ１７）。詳しくは、透かし情報の復号、分解処理が行われ、その復号データから被署名データと電子署名が復元される。また、被署名データ内の証明書等が認証局（ＣＡ）の公開鍵で復号され、発信者または発信元の機器の公開鍵が入手される。この公開鍵（署名検証鍵）で電子署名を復号し、被署名データをハッシュ化することでダイジェストを作成することで、そのダイジェストと電子署名の復号データとの照合により、正当な発信者または機器による電子署名であること、撮影画像やタイムスタンプの時刻や位置スタンプの場所に偽造や改ざんがないことを検証できる。

【０１１４】

ここで、署名検証結果が成功であった場合には（ステップＣ１８のＹｅｓ）、署名検証の成功を示す特定のマーク（図２３、図２４に示す署名検証済みマーク１０６）と共に、この画像データに電子署名と共に付加されていたタイムスタンプや位置スタンプを含む所定の情報が当該画像に対応付けられて表示される（ステップＣ１９、Ｃ２０）。

【０１１５】

また、署名検証結果が失敗であった場合には（ステップＣ１８のＮｏ）、署名検証の失敗を示す特定のマーク（例えば“×”や“ＮＧ”など）が当該画像上に表示され、タイムスタンプや位置スタンプ等の情報については表示されない（ステップＣ２１、Ｃ２２）。

【０１１６】

このように、電子透かしにより電子署名等を撮影画像に埋め込んでおけば、その画像を再生する際に署名の検証により当該画像の偽造や改ざんがないことを確認することができ、また、撮影者に無断で当該画像を転用するなどの不正利用を防止することができる。

【０１１７】

なお、前記第１の実施形態では、撮像装置１１にＧＰＳ受信機を内蔵することで、ＧＰＳ衛星１０から高精度の時刻信号を受信するようにしたが、高精度の時刻信号を受信する手段としては、上述したようなＧＰＳ受信機を用いる他に、通信総合研究所（ＣＲＬ）所管のＪＪＹ（ＪＧ２ＡＳ）局の長波（４０ｋＨｚ／６０ｋＨｚ）の標準時刻電波を受信する、所謂「電波時計」の受信機を用いることでも良い。

【０１１８】

図１４に撮像装置１１の時刻受信手段として「電波時計」の受信機を用いた場合の構成を部分的に示す。図中の５０は標準時刻電波送信局であり、標準時計監視部５１、原子時計５２、標準時計５３、標準時刻信号エンコーダ５４、送信機５５、送信アンテナ５６などからなる。

【０１１９】

撮像装置１１には、この標準時刻電波送信局５０から発信される標準時刻信号を受信するための標準時刻受信部６０が備えられる。この標準時刻受信部６０は、受信アンテナ６１、同調回路６２、増幅器６３、検波器６４、デコーダ６５、発振器６６、計時回路６７などを備え、標準時刻電波送信局５０から発信される標準時刻信号を定期的に受信し、その標準時刻信号に基づく高精度の計時処理を行う。

【０１２０】

また、位置測定手段としては、ＧＰＳ受信機による方法の他に、例えば移動通信システムにおける位置情報サービスを利用することができる。位置情報サービスは、基地局の位置をその基地局の通信エリア内に存在する端末の位置として通知するサービスである。

【０１２１】

その他の方法としては、例えばＧＰＳに加えて、ディファレンシャルＧＰＳ（ＤＧＰＳ）方式で、固定受信局でもＧＰＳ信号を受信することで補正情報を計測し、ネットワークやＦＭデータ放送等により前記補正情報を撮像装置１１に送ることで、より精度の高い測位を行う。

【０１２２】
また、ネットワークアシスト型ＧＰＳ方式で、内蔵もしくは外部接続のＧＰＳ簡易受信ユニットにより、ＧＰＳ信号を受信してネットワークに送り、ネットワーク側で撮像装置１１の現在位置を精密測位演算し、その測位結果を返信する。ネットワークとの通信接続機能が必要となるが、衛星の捕捉追尾や測位演算はネットワーク側で行なうので、撮像装置１１に内蔵するＧＰＳ受信機は小型で低電力のものを使用できる。
【０１２３】
また、位置ビーコン方式で、例えばＶＩＣＳ（Ｖｅｈｉｃｌｅ Ｉｎｆｏｒｍａｔｉｏｎ ａｎｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ Ｓｙｓｔｅｍ：道路交通情報通信システム）やＩＴＳ（Ｉｎｔｅｌｌｉｇｅｎｔ Ｔｒａｎｓｐｏｒｔ：高度道路交通システム）などの路側帯に設けた位置情報ビーコンからの無線や赤外線による位置情報を専用受信機で受信することでも良い。
【０１２４】
（第２の実施形態）
次に、本発明の第２の実施形態について説明する。
【０１２５】
前記第１の実施形態では、撮像装置１１に時刻＆位置認証機能を設けて撮影画像の撮影日時や撮影場所を第三者に証明するようした。しかし、この時刻＆位置認証機能だけでは、撮像装置１１を用いて撮影を行ったユーザが必ずしもその所有者本人であることは証明できない。本人がその日時にその場所に所在したことを第三者に証明するためには、ユーザが本人その人であることを証明するための本人認証が必要である。なお、ここで言う「本人」とは、撮像装置１１の所有者のこと、つまり、予め登録された正規ユーザのことである。
【０１２６】
そこで、第２の実施形態では、指紋センサを用いた本人認証機能により所有者本人であることの検証をその場で行なうことで、所有者本人がその日時にその場所にいたことを第三者に対して証明するようにしている。
【０１２７】
図１５は本発明の第２の実施形態に係る日時・位置・本人認証機能付きの撮像装置１１の構成を示すブロック図である。なお、図１５において、前記第１の実施形態の構成（図１）と同じ部分には同一符号を付し、ここでは異なる部分についてのみ説明する。
【０１２８】
すなわち、第２の実施形態において、この撮像装置１１には指紋センサ７０、、生体情報解析＆認証部７１、生体情報メモリ７２が設けられている。指紋センサ７０は、ユーザの指の指紋パターンの読取りを行うものであり、撮像素子７３、画像メモリ７４、画像信号処理部７５などから構成される。生体情報解析＆認証部７１は、ユーザの生体情報（ここでは指紋パターン）を解析し、所有者本人であるか否かを認証する処理を行う。生体情報メモリ７２には、予め所有者本人の生体情報（ここでは指紋パターン）が登録されている。
【０１２９】
なお、この本人認証に関する各回路（生体情報解析＆認証部７１、生体情報メモリ７２）についても前記日時・位置認証に関する各回路と同様に１チップの認証チップとして構成したり、あるいは、耐タンパー性の認証モジュールに格納することが望ましい。
【０１３０】
このような構成において、図１６のフローチャートに示すように、指紋センサ７０によって読み取られた指紋パターンは、生体情報解析＆認証部７１にて生体情報メモリ７２に登録された本人の指紋パターンと照合される（ステップＤ１１、Ｄ１２）。そして、両者の指紋パターンが一致すれば、この撮像装置１１の利用者がユーザ本人であるものと認証される（ステップＤ１３）。
【０１３１】

ここで、システム制御部１５では、所有者本人であることを確認できた場合にのみ（ステップＤ１３のＹｅｓ）、署名暗号化処理部１９を起動して前記第１の実施形態で説明したような方法にて秘密鍵を用いてタイムスタンプ・位置スタンプ用の電子署名を作成し、あるいは、その電子署名を透かし情報として作成し、これを当該撮影画像に付加することで日時・位置認証署名付きの画像データを生成するように制御する（ステップＤ１４）。

【０１３２】

なお、所有者本人であることを確認できた場合に、別の秘密鍵を用いて所有者本人であることを証明するための本人認証用の電子署名を作成し、これを前記タイムスタンプ・位置スタンプ用の電子署名と共に当該撮影画像に付加するようにしても良い。

【０１３３】

一方、指紋パターンが一致せず、所有者本人であることを確認できなかった場合には（ステップＤ１３のＮｏ）、その旨のメッセージを表示するなどして、前記電子署名の作成を行わないように署名暗号化処理部１９を制御する（ステップＤ１５）。

【０１３４】

このように、撮像装置１１の操作者が所有者本人であると確認された場合にのみ、日時・位置認証署名付きの画像データが生成されることになるので、その画像データを所有者本人がその時刻にその場所にいたことの証明として用いることができる。

【０１３５】

なお、ここで指紋認証を例にして説明したが、例えば撮像装置１１が携帯電話などのように音声入力部８０を備えていれば、声紋認証を行うことでも良い。この音声入力部８０はマイク８１、アンプ８２、Ａ／Ｄ変換器８３、音声符号化部８４などから構成される。この場合、生体情報メモリ７２には予め所有者本人の声紋パターンが登録されており、生体情報解析＆認証部７１は音声入力部８０を通じて入力された音声信号から声紋パターンを解析し、その声紋パターンと生体情報メモリ７２の登録パターンとを照合することで、所有者本人であるか否かを認証する。

【０１３６】

また、その他の方法として、例えば撮像カメラ部１２を利用してユーザの顔の容貌による認証や、眼の虹彩パターンによる認証を行うことでも良い。

【０１３７】

また、操作部１３をタッチパネルで構成し、手書き筆跡署名（サイン）認証を行うことでも良い。さらに、手のひらや指の静脈血管パターン認証など、他の生体情報による本人認証機能を構成することでも良い。

【０１３８】

次に、上述した撮像装置１１の外観構成とその使用方法について説明する。

【０１３９】

図１７および図１８は撮像装置１１の外観構成を示す図であり、図１７は撮像装置１１がデジタルカメラである場合の外観例、図１８は撮像装置１１がカメラ付き携帯電話である場合の外観例である。図中の各符号は図１、図１４、図１５に対応しており、それぞれに撮像カメラ部１２を備えると共に、日時取得手段としてＧＰＳ受信部１７または標準時刻受信部６０を備える。

【０１４０】

また、署名暗号化処理部１９、署名復号化処理部２０、本人秘密鍵メモリ２１、相手公開鍵メモリ２２といった日時・位置認証に必要な各構成要素の他、さらに生体情報解析＆認証部７１、生体情報メモリ７２といった本人認証に必要な各構成要素が１チップの認証チップで構成されている。

【０１４１】

図１９乃至図２１はそれぞれ日時・位置認証の設定操作例を示している。

【０１４２】

図１９の例では、「ｄａｔｅ」キーの操作により「日時記録なし」→「時刻記録あり」→「日付記録あり」→「日時記録あり」→「日時記録＋日時認証」といった順で各モードが

順に設定される。このうちの「日時記録＋日時認証」が日時認証を行う場合のモードである。この「日時記録＋日時認証」モードを設定しておくことで、撮影画像に現在日時を示すタイムスタンプを電子署名付きで付加することができる。

【０１４３】

図２０の例では、「ｄａｔｅ」キーの操作により「日時記録なし」→「日時記録あり」→「日時記録＋日時認証」といった順で各モードが順に設定され、「日時記録あり」と「日時記録＋日時認証」のモードで「ｓｅｌｅｃｔ」キーを操作することで更に詳細な設定を行うように構成されている。このうちの「日時記録＋日時認証」が日時認証を行う場合のモードである。

【０１４４】

図２１の例では、メニュー画面上で「日時記録」、「位置記録」、「日時認証」、「位置認証」、「本人認証」の各モードを任意選択的にＯＮ／ＯＦＦするように構成されている。この中で「日時認証」モードをＯＮしておけば、撮影画像に現在日時を示すタイムスタンプを電子署名付きで付加することができる。同様に「位置認証」モードをＯＮしておけば、撮影画像に現在位置を示す位置スタンプを電子署名付きで付加することができる。また、「本人認証」モードをＯＮしておけば、本人認証機能が働き、ユーザ本人であることが確認された場合のみ、前記の「日時認証」モードと「位置認証」モードが有効となる。

【０１４５】

図２２は撮像装置１１の具体的な利用シーンを示す図であり、撮像装置１１で撮影した画像を印刷する場合が示されている。図中の９１はＰＣ等の外部の端末機器、９２はプリンタ装置、９３は印刷物である。

【０１４６】

例えば、図１７に示すようなデジタルカメラからなる撮像装置１１は、ＧＰＳ衛星１０あるいは標準時刻電波送信局５０からの電波を定期的に受信して、常に正確な時刻を計時している。また、ＧＰＳ衛星１０などから測位信号を定期的に受信し、常に現在位置を把握している。

【０１４７】

この撮像装置１１のカメラ機能を用いて撮影を行った場合、そのときの撮影日時を示すタイムスタンプと撮影場所を示す位置スタンプが電子署名と共に自動発行され、これらの情報が撮影画像に付加されて、日時・位置認証署名付きの画像が生成される。この日時・位置認証署名付きの画像は撮像装置１１内のメモリ（画像データメモリ２３）に記憶される。

【０１４８】

なお、撮像装置１１が本人認証機能を備えている場合には、例えば指紋センサ７０にてユーザ本人であることが確認されたときに、電子署名の自動発行がなされる。この電子署名がないものは、撮影画像にタイムスタンプや位置スタンプが付いていても、その時刻や位置は認証されておらず、また、ユーザ本人が撮影したことも認証されていないことになる。

【０１４９】

この撮像装置１１を無線あるいはＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）などを介してＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）等の端末機器９１に接続し、撮像装置１１に記憶された撮影画像を端末機器９１に接続されたプリンタ装置９２に転送すると、同図に示すような印刷物９３が得られる。

【０１５０】

この印刷物９３には、撮影画像９４の他に、この撮影画像９４に付加されていた各種情報９５と認証マーク９６が所定の形式で印刷されている。各種情報９５とは、画像ファイル名、撮影日時、撮影場所、画像のハッシュ値、発行者や機器のＩＤ、電子署名データ等である。また、認証マーク９６はここに記述されている情報が正しいことを証明するものである。

【０１５１】

次に、この撮像装置１１にて他機器から受け取った署名付きの画像を再生するときの表示方法について説明する。

【０１５２】

図２３は撮像装置１１における再生時の撮影画像と復号結果の表示例を示す図であり、図２３（ａ）が撮影画像、同図（ｂ）がその撮影画像に付加されていた情報である。図中の１０１はタイムスタンプであり、画像の撮影日時を示す。また、１０２は鍵マークであり、画像に電子署名データが付加されていることを示す。

【０１５３】

撮影画像にタイムスタンプまたは位置スタンプと共に電子署名データが付加されていると、図示のような鍵マーク１０３が当該画像中の所定の位置に付加されて表示される。撮影画像を受け取った相手は、この鍵マーク１０３により当該撮影画像に電子署名データが付加されていることが分かる。

【０１５４】

ここで、撮影者の公開鍵を用いて当該撮影画像を復号化すると、同図（ｂ）に示すように、当該撮影画像に関する所定の情報１０４が表示される。この所定の情報１０４には、画像のファイル名や撮影日時（タイムスタンプ）などの他に、電子署名データ１０５が含まれる。また、このときに署名検証済みマーク１０６が表示され、ここに記述されている情報が正しいことが証明される。なお、署名検証の具体的な処理については図１１や図１３で既に説明しているため、ここでは省略する。

【０１５５】

図２４は再生時の撮影画像と復号結果の別の表示例を示す図であり、図２４（ａ）が撮影画像、同図（ｂ）がその撮影画像に付加されていた情報である。この例では、タイプスタンプ１０１と位置スタンプ１０２が記録された画像が鍵マーク１０３付きで表示されている。

【０１５６】

前記同様に、この画像を公開鍵を用いて復号化することで、同図（ｂ）に示すように、当該撮影画像に関する所定の情報１０４が表示され、その中の電子署名データ１０５を署名検証済みマーク１０６と共に確認することができる。

【０１５７】

なお、前記情報１０４は当該撮影画像に所定の形式で付加されていても良いし、透かし情報として画像中に埋め込まれていても良い。撮影画像を受け取ったときには、この情報１０４は非表示状態であり、公開鍵を用いて復号化したときに表示される。したがって、公開鍵を持たない者が勝手に情報１０４を見ることはできない。

【０１５８】

このように、本発明の撮像装置によれば、ネットワークを介して特定の認証局にアクセスするなどの面倒な作業を必要とせずに、被写体の画像を撮影したときに、自機内にて高精度で正確な日時や場所を示すタイムスタンプ、位置スタンプを作成し、これらのスタンプデータに信頼性が高く、かつ、第三者にも偽造や改ざんが無いことを証明できる電子署名を簡単に付して当該画像データに記録することできる。

【０１５９】

これにより、いつ、どこで撮影した画像であるのかを第三者に証明することができるものであり、例えば建築工事など施行状況や業務の進行状況の記録、顧客や取引先への報告、交通事故や災害の発生状況や損害程度の証拠記録、あるいは、実施日時の進み遅れで報償金や補償金の支払が発生するような業務の証拠記録や、画像の精細度や真正性だけでなく、日時や場所の証明が必要な用途に広く利用できるものである。

【０１６０】

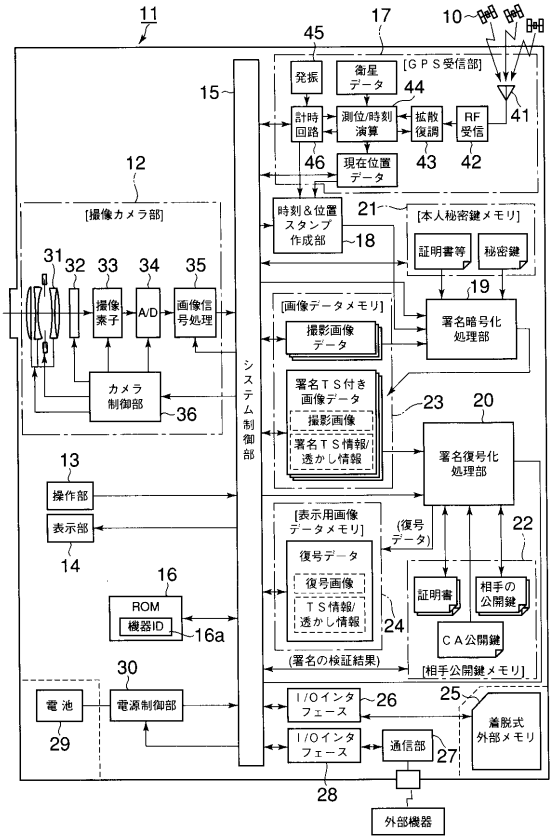
さらに、本人認証機能を加え、所有者本人であることが確認された場合のみ、上述した電子署名を作成して画像データに付加するようにしたことで、その署名付きの画像データが本装置の所有者本人が撮影したものであり、その画像を撮影した日時にその場所に確かに所在していたことを第三者に証明することができる。

【０１６１】
なお、本発明は、デジタルカメラやカメラ付きの携帯電話の他、カメラ機能を備えた電子機器であれば、その全てに適用可能である。要するに、本発明は前記各実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。
【０１６２】
更に、前記各実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば、実施形態で示される全構成要件から幾つかの構成要件が削除されても、「発明が解決しようとする課題」で述べた効果が解決でき、「発明の効果」の欄で述べられている効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。
【０１６３】
また、上述した各実施形態において記載した手法は、コンピュータに実行させることのできるプログラムとして、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリなどの記録媒体に書き込んで各種装置に適用したり、通信媒体により伝送して各種装置に適用することも可能である。本装置を実現するコンピュータは、記録媒体に記録されたプログラムを読み込み、このプログラムによって動作が制御されることにより、上述した処理を実行する。
【０１６４】
【発明の効果】
以上詳記したように本発明によれば、時刻認証機能を備えることで、認証機関へのアクセスなどを必要とせずに、画像を撮影したときにタイムスタンプを電子署名付きで自動発行することができ、その画像の撮影日時を第三者に証明することができる。
【０１６５】
また、位置認証機能を備えることで、前記同様に認証機関へのアクセスなどを必要とせずに、位置スタンプを含めて自動発行することができ、その画像の撮影場所を第三者に証明することができる。
【０１６６】
さらに、本人認証機能を備えることで、所有者本人以外のユーザが署名付きの画像を作成することを防止でき、また、その所有者本人が当該画像の撮影日時に撮影場所に居たことを第三者に証明することができる。
【図面の簡単な説明】
【図１】本発明の第１の実施形態に係る日時・位置認証機能付きの撮像装置の構成を示すブロック図。
【図２】前記撮像装置におけるタイムスタンプ（位置スタンプを含む）と電子署名の作成方法（第１の方法）を説明するための図。
【図３】前記撮像装置におけるタイムスタンプ（位置スタンプを含む）と電子署名の作成方法（第２の方法）を説明するための図。
【図４】前記撮像装置におけるタイムスタンプ（位置スタンプを含む）と電子署名の作成方法（第３の方法）を説明するための図。
【図５】前記撮像装置に備えられた電子透かし機能による撮影画像の変換処理を模式的に示した図。
【図６】前記撮像装置に備えられた電子透かし機能によって電子透かしを画像中に埋め込む方法を示す図。
【図７】前記撮像装置に備えられた電子透かし機能によって電子透かしを画像中に埋め込む別の方法を示す図。
【図８】前記撮像装置に備えられた電子透かし機能によって電子透かしを画像中に埋め込む別の方法を示す図。
【図９】前記撮像装置のメモリ格納形式の一例を示す図。
【図１０】前記撮像装置における日時・位置認証と署名検証に関する処理を示すフローチ

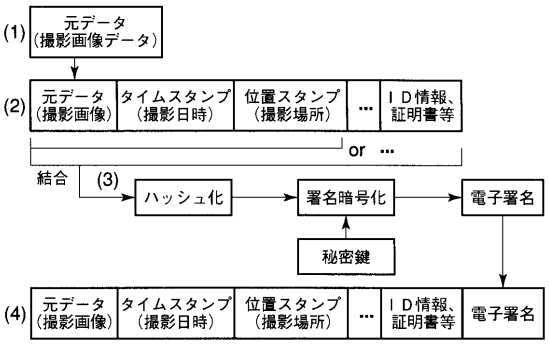
ャート。
【図１１】前記撮像装置における日時・位置認証と署名検証に関する処理を示すフローチャート。
【図１２】前記撮像装置における電子透かし埋込み画像の作成処理を示すフローチャート。
【図１３】前記撮像装置における電子透かし埋込み画像の復号処理と署名検証処理を示すフローチャート。
【図１４】前記撮像装置の時刻受信手段として「電波時計」の受信機を用いた場合の構成を部分的に示すブロック図。
【図１５】本発明の第２の実施形態に係る日時・位置・本人認証機能付きの撮像装置の構成を示すブロック図。
【図１６】前記撮像装置における本人認証処理を示すフローチャート。
【図１７】前記撮像装置がデジタルカメラである場合の外観構成を示す図。
【図１８】前記撮像装置がカメラ付き携帯電話である場合の外観構成を示す図。
【図１９】前記撮像装置における日時・位置認証の設定操作の一例（その１）を説明するための図。
【図２０】前記撮像装置における日時・位置認証の設定操作の一例（その２）を説明するための図。
【図２１】前記撮像装置における日時・位置認証の設定操作の一例（その３）を説明するための図。
【図２２】前記撮像装置の具体的な利用シーンを示す図であり、撮像装置で撮影した画像を印刷する場合を示す図。
【図２３】前記撮像装置における再生時の撮影画像と復号結果の表示例を示す図であり、図２３（ａ）が撮影画像、同図（ｂ）がその撮影画像に付加されていた情報を示す図。
【図２４】前記撮像装置における再生時の撮影画像と復号結果の別の表示例を示す図であり、図２４（ａ）が撮影画像、同図（ｂ）がその撮影画像に付加されていた情報を示す図。
【符号の説明】
１１…撮像装置
１２…撮像カメラ部
１３…操作部
１４…表示部
１５…システム制御部
１６…ＲＯＭ
１７…ＧＰＳ受信部
１８…時刻＆位置スタンプ作成部
１９…署名暗号化処理部
２０…署名復号化処理部
２１…本人秘密鍵メモリ
２２…相手公開鍵メモリ
２３…画像データメモリ
２４…表示用画像データメモリ
２５…外部メモリ
２６…Ｉ／Ｏインタフェース
２７…通信部
２８…Ｉ／Ｏインタフェース
２９…電池
３０…電源制御部
５０…標準時刻電波送信局
６０…標準時刻受信部

７０…指紋センサ
８０…音声入力部

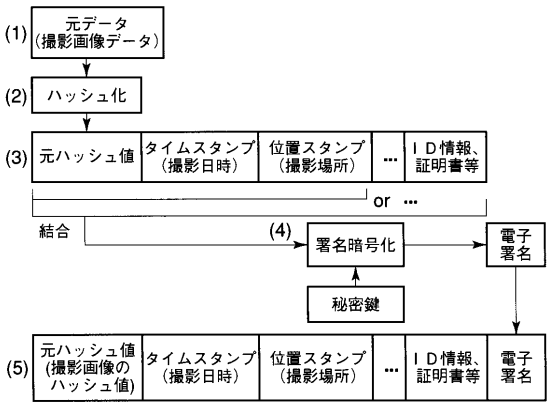
【図１】



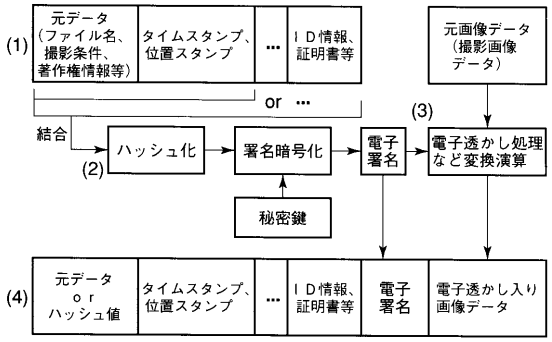
【図２】



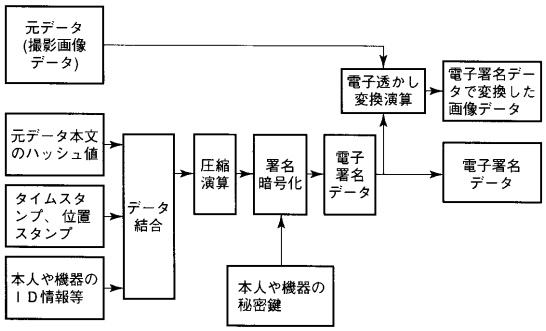
【図３】



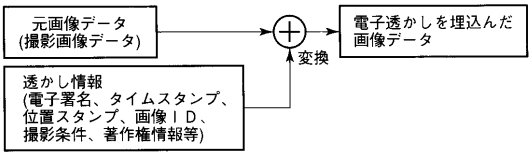
【図４】



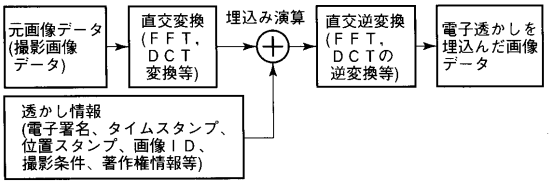
【図５】



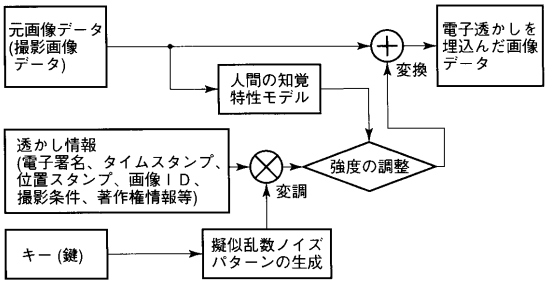
【図６】



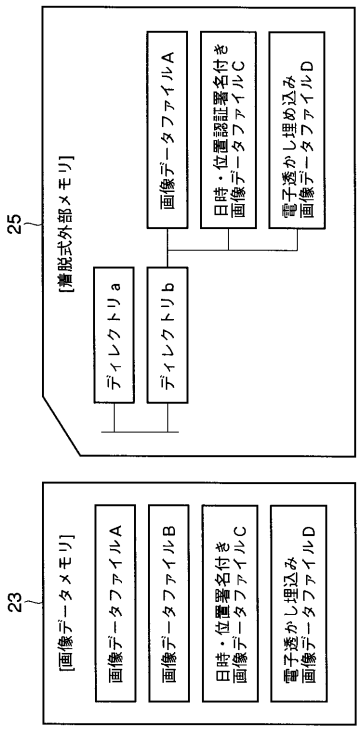
【図７】



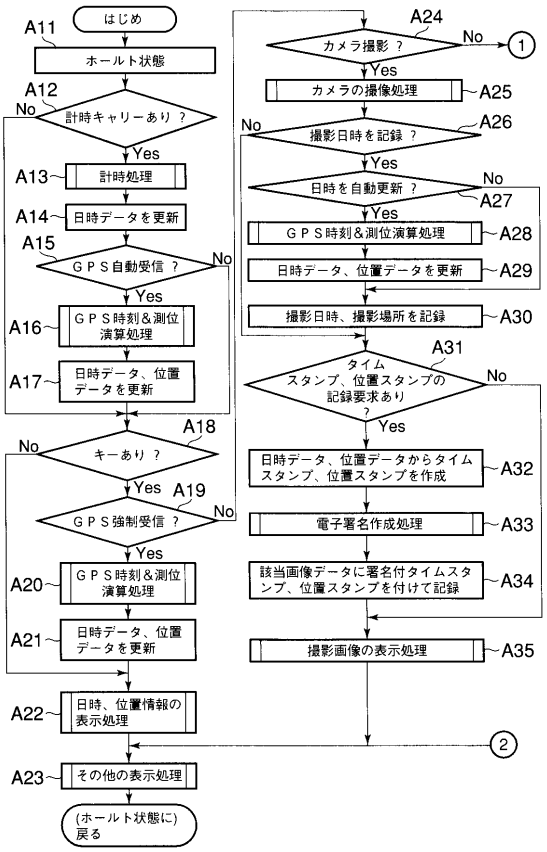
【図８】



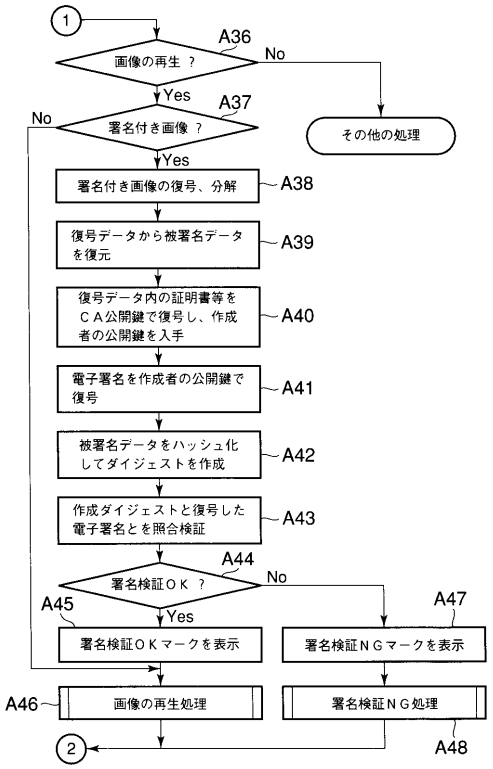
【図９】



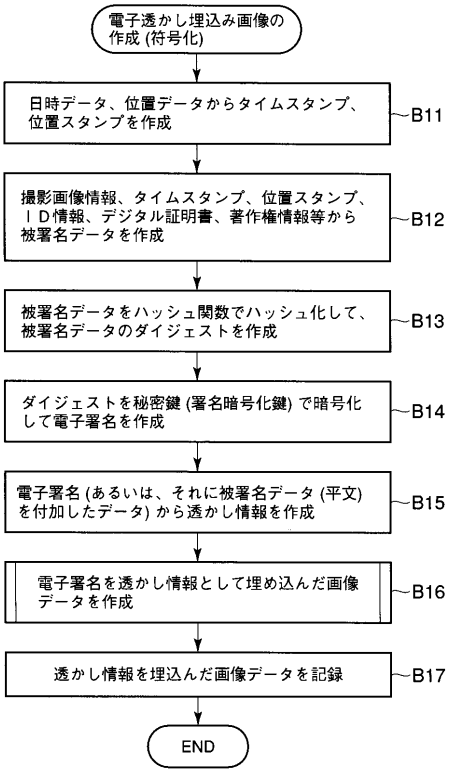
【図１０】



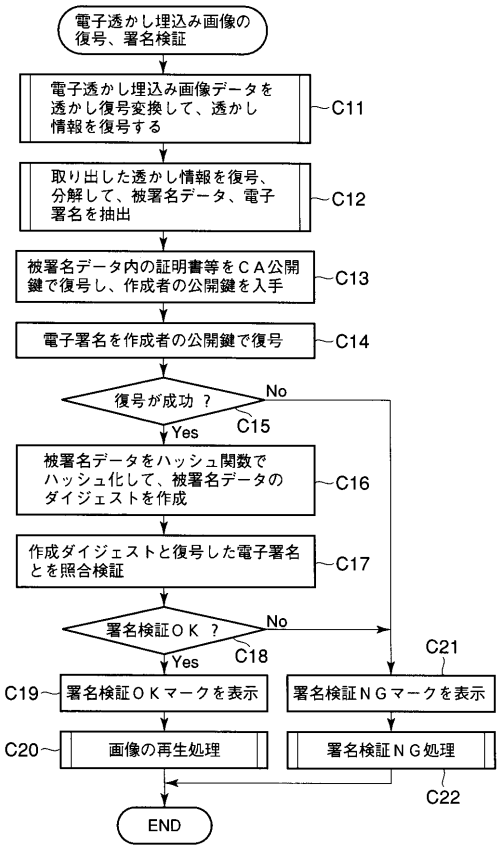
【図１１】



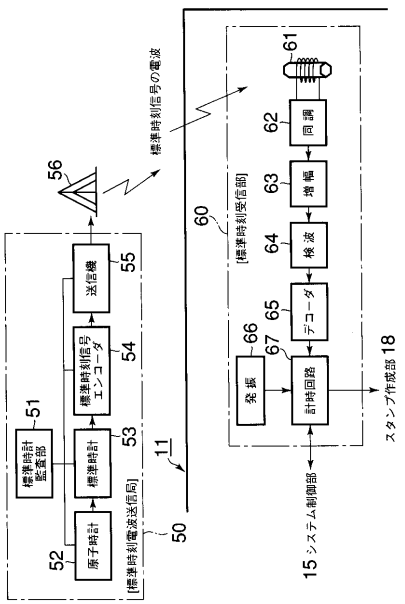
【図１２】



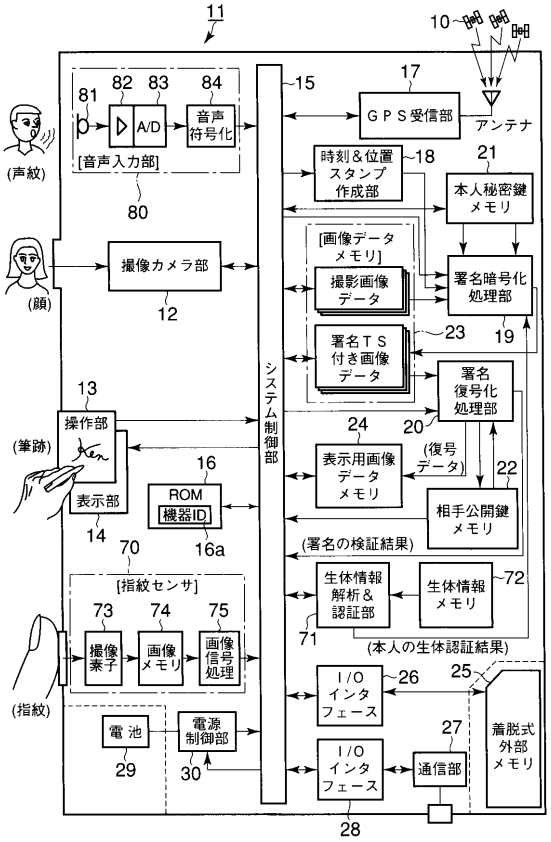
【図１３】



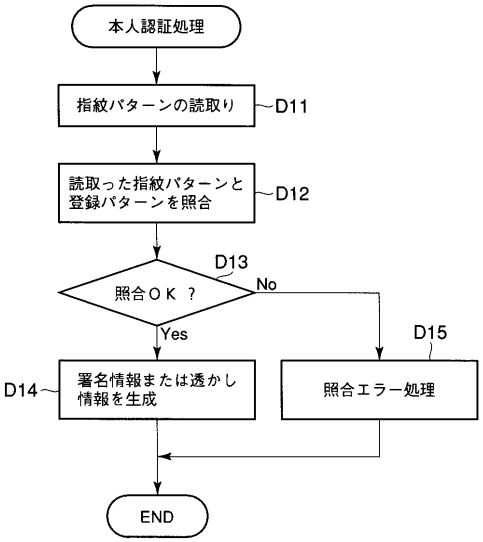
【図１４】



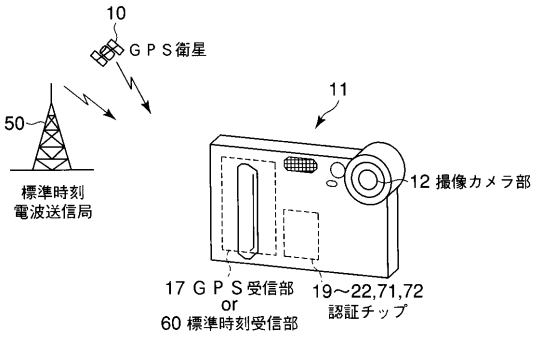
【図１５】



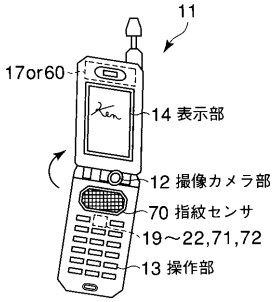
【図１６】



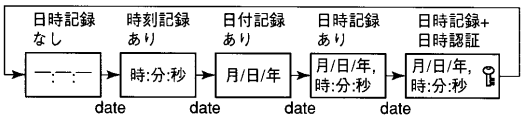
【図１７】



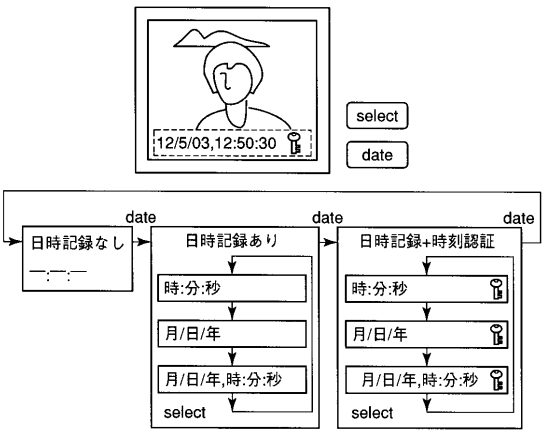
【図１８】



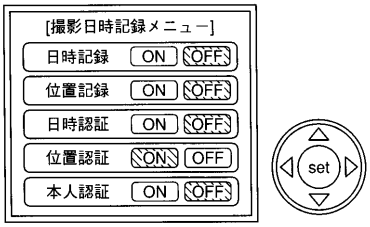
【図１９】



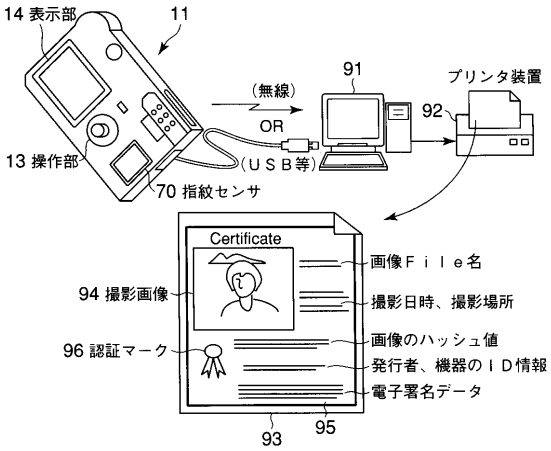
【図２０】



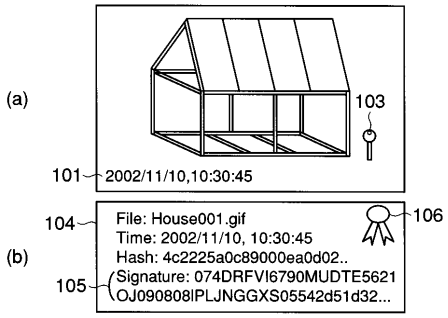
【図２１】



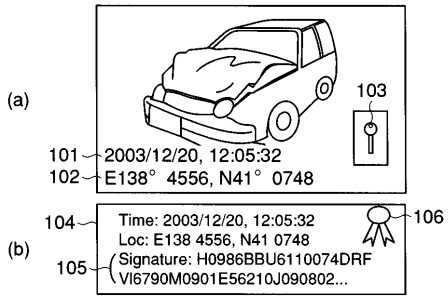
【図２２】



【図２３】



【図２４】



フロントページの続き

(72)発明者　喜多　一記
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内

Ｆターム(参考) 5C022 AA13 AC00 AC01 AC03 AC12 AC13 AC31 AC42 AC69 AC72
5C053 FA08 FA27 JA16 JA22 KA05 LA01 LA04
5J104 AA07 AA09 AA12 GA03 GA05 JA01 JA21 KA02 KA05 KA20
LA01 LA06 NA02 NA12 NA27 NA37 NA38 NA42 PA14