

(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2012-120102

(P2012-120102A)

(43) 公開日 平成24年6月21日(2012.6.21)

(51) Int.Cl.		F I				テーマコード (参考)
H04L	9/32	(2006.01)	H04L	9/00	675B	5B017
G09C	1/00	(2006.01)	G09C	1/00	640D	5J104
G06F	21/24	(2006.01)	G06F	12/14	560C	

審査請求 未請求 請求項の数 7 O L (全 14 頁)

(21) 出願番号	特願2010-270477 (P2010-270477)	(71) 出願人	000002897
(22) 出願日	平成22年12月3日 (2010.12.3)		大日本印刷株式会社
			東京都新宿区市谷加賀町一丁目1番1号
		(74) 代理人	100111659
			弁理士 金山 聡
		(74) 代理人	100135954
			弁理士 深町 圭子
		(74) 代理人	100119057
			弁理士 伊藤 英生
		(74) 代理人	100122529
			弁理士 藤枿 裕実
		(74) 代理人	100131369
			弁理士 後藤 直樹
		(74) 代理人	100164987
			弁理士 伊藤 裕介

最終頁に続く

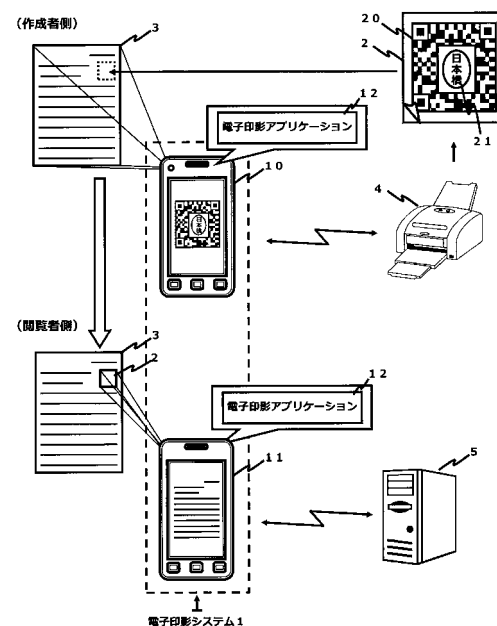
(54) 【発明の名称】 電子印影システム及びアプリケーションプログラム

(57) 【要約】

【課題】 特殊な装置を用意せずとも、電子印影をエンコードした光学コードを用いて文書の偽造防止が図れる電子印影システムを提供する。

【解決手段】 電子印影システム1において、第1の携帯端末装置10は、カメラ機能で撮影した文書3の画像から生成した署名対象データのデジタル署名を少なくとも含む電子印影を生成し、電子印影をエンコードした光学コード20が印刷された電子印影シール2をシールプリンタ4に出力させる。第2の携帯端末装置11は、カメラ機能で撮影された電子印影シール2の画像に含まれる光学コード20をデコードし、デコードした電子印影に含まれるデジタル署名を検証し、該デジタル署名の検証結果として署名対象データを第2の携帯端末装置11のディスプレイに表示する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

写真を撮影するカメラと、該カメラで撮影された文書の画像から署名対象データを生成し、秘密鍵からデジタル署名を生成するコマンドが実装された U S I M に前記署名対象データを送信して、前記 U S I M から前記署名対象データのデジタル署名を取得した後、前記 U S I M から取得したデジタル署名、前記署名対象データの保存先を示すデータソースを少なくとも含む電子印影を生成し、前記電子印影をエンコードした光学コードの印刷データをプリンタに送信することで、前記光学コードが印刷された電子印影シールをプリンタに出力させる印影生成手段を備えた第 1 の携帯端末装置と、

写真を撮影するカメラと、該カメラで撮影された電子印影シールの画像に含まれる前記光学コードをデコードし、デコードされた前記電子印影に含まれる前記データソースで示される保存先から前記署名対象データを取得した後、前記 U S I M に記憶された秘密鍵と対になる公開鍵を用いて、デコードされた前記電子印影に含まれるデジタル署名を検証し、該デジタル署名の検証に成功すると、該署名対象データをディスプレイに表示させる印影検証手段を備えた第 2 の携帯端末装置と、
から少なくとも構成されたことを特徴とする電子印影システム。

10

【請求項 2】

前記秘密鍵と対になる公開鍵が公開されている認証局の U R I が前記 U S I M に記憶され、前記第 1 の携帯端末装置の前記印影生成手段は、前記 U S I M から読み出した前記認証局の U R I を前記電子印影に含ませ、前記第 1 の携帯端末装置の前記印影検証手段は、
デコードされた前記電子印影に含まれる前記認証局の U R I にアクセスしてデジタル署名の検証に利用する公開鍵を取得することを特徴とする、請求項 1 に記載の電子印影システム。

20

【請求項 3】

前記 U S I M の所持者の氏名データ又は印影データが前記 U S I M に記憶され、前記第 1 の携帯端末装置の前記印影生成手段は、前記 U S I M から読み出した氏名データ又は印影データ入りの前記光学コードの印刷データを生成することを特徴とする、請求項 1 又は請求項 2 に記載の電子印影システム。

【請求項 4】

前記第 1 の携帯端末装置の前記印影生成手段は、前記文書の画像を文字認識して得られたテキストデータを前記署名対象データとし、前記データソースとして該テキストデータを前記光学コードに少なくともエンコードすることを特徴とする、請求項 1 から請求項 3 のいずれか一つに記載の電子印影システム。

30

【請求項 5】

前記第 1 の携帯端末装置の前記印影生成手段は、前記文書の画像そのものを前記署名対象データとし、前記文書の画像をネットワーク上のサーバに保存した後、前記文書の画像の保存先を示す U R I を前記データソースとして前記電子印影含ませることを特徴とする、請求項 1 から請求項 3 のいずれか一つに記載の電子印影システム。

【請求項 6】

請求項 1 から請求項 5 に記載の第 1 の携帯端末装置の印影生成手段としてカメラ付き携帯端末装置を機能させるためのアプリケーションプログラム。

40

【請求項 7】

請求項 1 又は請求項 2 に記載の第 2 の携帯端末装置の印影検証手段としてカメラ付き携帯端末装置を機能させるためのアプリケーションプログラム。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、電子印影をエンコードした光学コードを用いて紙媒体の文書の偽造防止を図るための技術に関する。

50

【背景技術】

【0002】

従来の印鑑は、その造形の複雑さから文書の偽造防止するための本人証明として用いられてきたが、印鑑による捺印の代わりに、電子印影をエンコードした光学コードを用いて紙媒体の文書の偽造防止を図ることが考案されている。例えば、特許文献1では、非対称鍵暗号を利用して文書のデジタル署名を生成し、文書のデジタル署名を含む電子印影をエンコードした光学コードを文書に印字する装置が提案されている。

【0003】

しかし、特許文献1で開示されている発明では、文書のイメージを読み取る機能、該イメージから生成したデジタル署名を含む電子印影をエンコードした光学コードを印字する機能などの機能、文章に印字された光学コードにエンコードされた電子印影を検証する機能などを備えた特殊な装置が必要となってしまう、実際の運用性に欠けていた。

10

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特開2003-29629号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

そこで、本発明は、特殊な装置を用意せずとも、電子印影をエンコードした光学コードを用いて紙媒体の文書の偽造防止を図ることができる電子印影システム、及び、電子印影システムで必要なる電子印影アプリケーションを提供することを目的とする。

20

【課題を解決するための手段】

【0006】

上述した課題を解決する第1の発明は、汎用のカメラ付き携帯端末装置を利用できるように発案された電子印影システムであって、第1の発明の電子印影システムは、写真を撮影するカメラと、該カメラで撮影された文書の画像から署名対象データを生成し、秘密鍵からデジタル署名を生成するコマンドが実装されたUSIMに前記署名対象データを送信して、前記USIMから前記署名対象データのデジタル署名を取得した後、前記USIMから取得したデジタル署名、前記署名対象データの保存先を示すデータソースを少なくとも含む電子印影を生成し、前記電子印影をエンコードした光学コードの印刷データをプリンタに送信することで、前記光学コードが印刷された電子印影シールをプリンタに出力させる印影生成手段を備えた第1の携帯端末装置と、写真を撮影するカメラと、該カメラで撮影された電子印影シールの画像に含まれる前記光学コードをデコードし、デコードされた前記電子印影に含まれる前記データソースで示される保存先から前記署名対象データを取得した後、前記USIMに記憶された秘密鍵と対になる公開鍵を用いて、デコードされた前記電子印影に含まれるデジタル署名を検証し、該デジタル署名の検証に成功すると、該署名対象データをディスプレイに表示させる印影検証手段を備えた第2の携帯端末装置とから少なくとも構成されることを特徴とする。

30

【0007】

40

更に、第2の発明は、認証局から公開鍵を取得できるように、第1の発明の電子印影システムにおいて、前記秘密鍵と対になる公開鍵が公開されている認証局のURIが前記USIMに記憶され、前記第1の携帯端末装置の前記印影生成手段は、前記USIMから読み出した前記認証局のURIを前記電子印影に含ませ、前記第1の携帯端末装置の前記印影検証手段は、デコードされた前記電子印影に含まれる前記認証局のURIにアクセスしてデジタル署名の検証に利用する公開鍵を取得することを特徴とする。

【0008】

更に、第3の発明は、電子印影シールの作成者を目視で確認できるように、第1の発明又は第2の発明の電子印影システムにおいて、前記USIMの所持者の氏名データ又は印影データが前記USIMに記憶され、前記第1の携帯端末装置の前記印影生成手段は、前

50

記 U S I M から読み出した氏名データ又は印影データ入りの前記光学コードの印刷データを生成することを特徴とする。

【 0 0 0 9 】

更に、第 4 の発明は、署名対象データを光学コードにエンコードできるように、第 1 の発明から第 3 の発明のいずれか一つに記載の電子印影システムにおいて、前記第 1 の携帯端末装置の前記印影生成手段は、前記文書の画像を文字認識して得られたテキストデータを前記署名対象データとし、前記データソースとして該テキストデータを前記光学コードに少なくともエンコードすることを特徴とする。

【 0 0 1 0 】

更に、第 5 の発明は、図やグラフを含む文書でも対応が取れるように、第 1 の発明から第 3 の発明のいずれか一つに記載の電子印影システムにおいて、前記第 1 の携帯端末装置の前記印影生成手段は、前記文書の画像そのものを前記署名対象データとし、前記文書の画像をネットワーク上のサーバに保存した後、前記文書の画像の保存先を示す U R I を前記データソースとして前記電子印影含ませることを特徴とする。

10

【 0 0 1 1 】

更に、第 6 の発明は、第 1 の発明から第 5 の発明に記載の第 1 の携帯端末装置の印影生成手段としてカメラ付き携帯端末装置を機能させるためのアプリケーションプログラムである。

【 0 0 1 2 】

また、第 7 の発明は、第 1 の発明又は第 2 の発明に記載の第 2 の携帯端末装置の印影検証手段としてカメラ付き携帯端末装置を機能させるためのアプリケーションプログラムである。

20

【発明の効果】

【 0 0 1 3 】

このように、本発明によれば、特殊な装置を用意せずとも、電子印影をエンコードした光学コードを用いて紙媒体の文書の偽造防止を図ることができる電子印影システム、及び、電子印影システムで必要な電子印影アプリケーションを提供できる。

【図面の簡単な説明】

【 0 0 1 4 】

【図 1】本実施形態に係る電子印影システムを説明する図。

30

【図 2】本発明で利用されるカメラ付き携帯端末装置のブロック図。

【図 3】電子印影シールを作成するときのフローを説明する図。

【図 4】電子印影シールを検証するときのフローを説明する図。

【図 5】変形例に係る電子印影システムを説明する図。

【図 6】変形例における電子印影アプリケーションを説明する図。

【図 7】変形例において電子印影シールを作成するときのフローを説明する図。

【図 8】変形例において電子印影シールを検証するときのフローを説明する図。

【発明を実施するための形態】

【 0 0 1 5 】

ここから、本発明の実施形態について、本発明の技術分野に係わる当業者が、発明の内容を理解し、発明を実施できる程度に説明する。なお、これから説明する実施形態は本発明の一実施形態にしか過ぎず、本発明は、これから説明する実施形態に限定されることなく、種々の変形や変更が可能である。

40

【 0 0 1 6 】

図 1 は、本実施形態に係る電子印影システム 1 を説明する図である。本実施形態に係る電子印影システム 1 は、デジタル署名等を含む電子印影をエンコードした光学コード 2 0 (図 1 では、2 次元バーコード) が印刷された電子印影シール 2 を用い、公開鍵暗号方式を利用して光学コード 2 0 にエンコードされたデジタル署名の生成・検証を行うことで、紙媒体の文書 3 の偽造防止を図るために開発されたシステムである。

【 0 0 1 7 】

50

本実施形態に係る電子印影システム１は、電子印影シール２を作成する作成者が所持する第１の携帯端末装置１０と、電子印影シール２を検証する検証者が所持する第２の携帯端末装置１１とから少なくとも構成され、図１では、第１の携帯端末装置１０と第２の携帯端末装置１１以外に、無線通信機能を有するシールプリンタ４と、様々な人や会社の公開鍵を公開している認証局５を図示している。

【００１８】

図１で図示した電子印影システム１では、電子印影シール２の生成及び検証機能を携帯端末装置用のアプリケーションプログラムである電子印影アプリケーション１２で実現することで、第１の携帯端末装置１０及び第２の携帯端末装置１１として機能する特別な装置を用意せずとも、汎用的なカメラ付き携帯端末装置を第１の携帯端末装置１０及び第２の携帯端末装置１１として利用できるようにし、電子印影アプリケーション１２が実装された汎用的なカメラ付き携帯端末装置は、電子印影シール２の作成に利用されるとき第１の携帯端末装置１０として機能し、電子印影シール２の検証に利用されるとき第２の携帯端末装置１１として機能する。

【００１９】

図１で図示した電子印影システム１において、作成者が、電子印影シール２を貼り付ける文書３を第１の携帯端末装置１０のカメラ機能で撮影すると、第１の携帯端末装置１０に実装された電子印影アプリケーション１２は、カメラ機能で撮影された文書３の画像から生成した署名対象データのデジタル署名を公開鍵暗号方式の秘密鍵で生成し、署名対象データのデジタル署名、署名対象データの保存先を示すデータソース、デジタル署名を検証する際に利用する公開鍵、すなわち、デジタル署名を生成するときに利用した秘密鍵と対になる公開鍵を公開している認証局５のＵＲＩを少なくとも含む電子印影を生成し、電子印影をエンコードした光学コード２０の印刷データをシールプリンタ４に送信する処理を行い、シールプリンタ４は、該光学コード２０が印刷された電子印影シール２を出力する。

【００２０】

作成者がシールプリンタ４から出力された電子印影シール２を文書３に貼ることで、文書３に電子印影シール２が押印され、検証者が、第２の携帯端末装置１１を利用して文書３に押印された電子印影シール２を検証する際、検証者が文書３に押印された電子印影シール２を第２の携帯端末装置１１のカメラ機能で撮影すると、第２の携帯端末装置１１に実装された電子印影アプリケーション１２は、カメラ機能で撮影された電子印影シール２の画像に含まれる光学コード２０をデコードし、デコードした電子印影に含まれる認証局５のＵＲＩを利用して公開鍵を認証局５から取得した後、デコードした電子印影に含まれるデータソースを利用して取得した署名対象データと認証局５から取得した公開鍵を用いて、デコードした電子印影に含まれるデジタル署名を検証し、該デジタル署名の検証結果を第２の携帯端末装置１１のディスプレイに表示する処理を実行する。

【００２１】

電子印影に含まれるデジタル署名の検証結果そのものを第２の携帯端末装置１１に表示させることもできるが、作成者が文書３に押印する意志があったことを目視で確認できるように、本実施形態では、電子印影に含まれるデジタル署名の検証に成功すると、該デジタル署名の署名対象となった署名対象データを第２の携帯端末装置１１に表示させるようにしている。

【００２２】

本発明において、デジタル署名の対象となる署名対象データは、文書３の画像を文字認識することで得られるテキスト又は文書３の画像そのものとしてすることができ、本実施形態では、署名対象データを該テキストとするときの形態について説明し、署名対象データを文書３の画像とする形態については変形例にて説明する。

【００２３】

図２は、本発明で利用されるカメラ付き携帯端末装置のブロック図である。上述しているように、本実施形態では、電子印影シール２の生成及び検証機能を電子印影アプリケー

ション１２で実現しているため、第１の携帯端末装置１０及び第２の携帯端末装置１１は汎用のカメラ付き携帯端末装置で実現することができ、図２で図示したように、第１の携帯端末装置１０及び第２の携帯端末装置１１として利用される汎用のカメラ付き携帯端末装置には、カメラ付き携帯端末装置の所持者のＵＳＩＭ１０７が組み込まれ、更に、電気回路として、アプリケーションプロセッサなどで実現される制御回路１００、公衆無線通信網を利用して無線通信する無線通信回路１０３、写真を撮影するカメラ回路１０１、文字や映像を表示するディスプレイ回路１０２、テンキーなどの操作回路１０５、様々なアプリケーションが記憶されるメモリ１０４、汎用のカメラ付き携帯端末装置に実装されるＵＳＩＭ１０７とデータ通信するためのＵＳＩＭ回路１０６が組み込まれている。

【００２４】

メモリ１０４には、電子印影シール２の生成及び検証機能に係わる処理を制御回路１００に実行させるための電子印影アプリケーション１２が実装され、この電子印影アプリケーション１２には、電子印影シール２を生成するときに作動し、本発明の印影生成手段として機能する印影生成モジュール１２０と、電子印影シール２を検証するときに作動し、本発明の印影検証手段として機能する印影検証モジュール１２１が含まれる。

【００２５】

本実施形態において、光学コード２０にエンコードする電子印影に含ませるデジタル署名の生成に利用する秘密鍵は、汎用のカメラ付き携帯端末装置に組み込まれるＵＳＩＭ１０７に記憶され、秘密鍵を利用するコマンドとして、秘密鍵を利用して、外部装置（ここでは、制御回路１００）から送信されたデータのデジタル署名を生成するデジタル署名生成コマンドが実装されている。

【００２６】

デジタル署名生成コマンドにて生成されたデジタル署名の検証に利用する公開鍵は、ＵＳＩＭ１０７には記憶されておらず、ＵＳＩＭ１０７には、デジタル署名の検証に利用する公開鍵を取得するための情報として、ＵＳＩＭ１０７に記憶された秘密鍵と対になる公開鍵が公開されている認証局５のＵＲＩが記憶され、ＵＳＩＭ１０７には、認証局５のＵＲＩなど、ＵＳＩＭ１０７に記憶されたデータを読み出すためのリードコマンドが実装されている。

【００２７】

また、図１に図示したように、電子印影シール２を文書３に押印した作成者を検証者が目視にて確認できるように、電子印影シール２の光学コード２０の中央部に作成者の印影２１を印刷させるようにしているため、本実施形態のＵＳＩＭ１０７には、ＵＳＩＭ１０７の所持者の印影画像が記憶されている。ＵＳＩＭ１０７に記憶されている印影画像はＵＳＩＭ１０７の所持者の氏名データとすることもでき、印影画像を氏名データとするときは、光学コード２０の中央に氏名データが印刷されることになる。

【００２８】

なお、作成者と検証者のＵＳＩＭ１０７は同じ機能を備えているが、作成者のＵＳＩＭ１０７と検証者のＵＳＩＭ１０７とでは、ＵＳＩＭ１０７に記憶されているデータ（秘密鍵、認証局５のＵＲＩ、印影画像）が異なる。

【００２９】

図３は、電子印影シール２を作成するときのフローを説明する図である。作成者が電子印影シール２を生成する際、作成者は第１の携帯端末装置１０に実装されている電子印影アプリケーション１２の印影生成モジュール１２０を起動させた後、電子印影シール２を押印する文書３を携帯端末装置のカメラ回路１０１で撮影すると（Ｓ１）、第１の携帯端末装置１０に実装された電子印影アプリケーション１２の印影生成モジュール１２０は、カメラ回路１０１で撮影された画像を文書３の画像として取得する（Ｓ２）。

【００３０】

第１の携帯端末装置１０に実装された電子印影アプリケーション１２の印影生成モジュール１２０は、文書３の画像を取得すると、デジタル署名の対象となる署名対象データを文書３の画像から生成する（Ｓ３）。

10

20

30

40

50

【 0 0 3 1 】

デジタル署名の対象となる署名対象データは、文書 3 の画像そのものとすることもできるが、文書 3 の画像を光学コード 2 0 にエンコードすることは光学コード 2 0 の容量的に無理なので、本実施形態では、文書 3 の画像を文字認識することで得られるテキストを署名対象データとして生成する。光学コード 2 0 を 2 次元バーコードとすると、最大で 1 8 0 0 文字程度の文字を 2 次元バーコードにエンコード可能であるため、文書 3 の画像を文字認識することで得られるテキストを圧縮すれば、該テキスト全てを 2 次元バーコードにエンコードできる。

【 0 0 3 2 】

第 1 の携帯端末装置 1 0 に実装された電子印影アプリケーション 1 2 の印影生成モジュール 1 2 0 は、デジタル署名の対象となる署名対象データを生成すると、署名対象データのメッセージダイジェストとなるハッシュ値を算出し (S 4)、第 1 の携帯端末装置 1 0 の U S I M 回路 1 0 6 を作動させて、該ハッシュ値をデータ部に含ませたデジタル署名生成コマンドを U S I M 1 0 7 に送信することで、該ハッシュ値のデジタル署名を第 1 の携帯端末装置 1 0 の U S I M 1 0 7 に生成させ、第 1 の携帯端末装置 1 0 の U S I M 1 0 7 からデジタル署名を取得する (S 5)。なお、U S I M 1 0 7 にデジタル署名を生成する際、汎用的な技術であるパスワードの認証の成功を U S I M 1 0 7 側で必要とすることが好適である。

【 0 0 3 3 】

また、第 1 の携帯端末装置 1 0 に実装された電子印影アプリケーション 1 2 の印影生成モジュール 1 2 0 は、第 1 の携帯端末装置 1 0 の U S I M 回路 1 0 6 を作動させて、作成者の U S I M 1 0 7 にリードコマンドを送信することで、認証局 5 の U R I と印影データを作成者の U S I M 1 0 7 から読み出す (S 6)。

【 0 0 3 4 】

次に、第 1 の携帯端末装置 1 0 に実装された電子印影アプリケーション 1 2 の印影生成モジュール 1 2 0 は、第 1 の携帯端末装置 1 0 の U S I M 1 0 7 から取得したデジタル署名、デジタル署名の対象となった署名対象データの保存先を示すデータソース、及び、第 1 の携帯端末装置 1 0 の U S I M 1 0 7 から読み出した認証局 5 の U R I を含む電子印影を生成した後 (S 7)、第 1 の携帯端末装置 1 0 の U S I M 1 0 7 から読み出した印影画像を中央部に配置し、該電子印影をエンコードした光学コード 2 0 の印刷データを生成し (S 8)、生成した印刷データをシールプリンタ 4 に送信して、該光学コード 2 0 が印刷された電子印影シール 2 をシールプリンタ 4 に出力させる (S 9)。

【 0 0 3 5 】

本実施形態では、文書 3 の画像を文字認識することで得られたテキストを署名対象データをテキストとしているため、電子印影アプリケーション 1 2 の印影生成モジュール 1 2 0 は、署名対象データの保存先を示すデータソースとして、署名対象データの保存先が光学コード 2 0 であることを示す情報に加え、文書 3 の画像を文字認識することで得られたテキストの圧縮データを光学コード 2 0 にエンコードする。

【 0 0 3 6 】

図 4 は、電子印影シール 2 を検証するときのフローを説明する図である。電子印影シール 2 の検証者が、第 2 の携帯端末装置 1 1 を利用して文書 3 に貼られた電子印影シール 2 を検証する際、検証者は第 2 の携帯端末装置 1 1 に実装されている電子印影アプリケーション 1 2 の印影検証モジュール 1 2 1 を起動させた後、文書 3 に貼られた電子印影シール 2 を第 2 の携帯端末装置 1 1 のカメラ回路 1 0 1 で撮影すると (S 1 0)、第 2 の携帯端末装置 1 1 に実装された電子印影アプリケーション 1 2 の印影検証モジュール 1 2 1 は、カメラ回路 1 0 1 で撮影した電子印影シール 2 の画像に含まれる光学コード 2 0 をデコードし、署名対象データから算出されたデジタル署名、デジタル署名を生成した署名対象データの保存先を示すデータソース、及び、認証局 5 の U R I を含む電子印影を取得する (S 1 1)。

【 0 0 3 7 】

次に、第2の携帯端末装置11に実装された電子印影アプリケーション12の印影検証モジュール121は、無線通信回路103を利用して、デコードした電子印影に含まれる認証局5のURIにアクセスし、ここでは、認証局5のURIで公開されている公開鍵証明書と認証局5の公開鍵を取得し(S12)、認証局5の公開鍵を用いて該公開鍵証明書を検証する(S13)。

【0038】

認証局5の公開鍵を用いた公開鍵証明書の検証に成功すると、第2の携帯端末装置11に実装された電子印影アプリケーション12の印影検証モジュール121は、デコードした電子印影に含まれるデータソースを利用して、デジタル署名の対象となった署名対象データを取得する(S14)。本実施形態では、署名対象データは圧縮された状態で光学コード20にエンコードされているため、光学コード20にエンコードされた署名対象データの圧縮データを解凍することで、署名対象データを得ることができる。

【0039】

そして、第2の携帯端末装置11に実装された電子印影アプリケーション12の印影検証モジュール121は、デコードした電子印影に含まれるデータソースを利用して取得した署名対象データのメッセージダイジェストとなるハッシュ値を算出した後、公開鍵証明書に記述されている公開鍵を用いてデジタル署名を復号した値と、光学コード20から取得した署名対象データから算出したハッシュ値が一致するか確認することで、デコードした電子印影に含まれるデジタル署名を検証する(S15)。

【0040】

そして、第2の携帯端末装置11に実装された電子印影アプリケーション12の印影検証モジュール121は、デコードした電子印影に含まれるデジタル署名の検証に成功すると、該デジタル署名の検証の成功結果として、デコードした電子印影に含まれるデータソースを利用して取得した署名対象データ、ここでは、光学コード20にエンコードされていたテキストを第2の携帯端末装置11のディスプレイ回路102に表示させ(S16)、この手順を終了する。

【0041】

[変形例]

ここから、署名対象データを文書の画像とする形態について説明する。図5は、変形例に係る電子印影システム6を説明する図である。なお、図5では、図1と同じものについては同じ符号を付加している。

【0042】

図5で図示したように、変形例に係る電子印影システム6は、図1と同様に、電子印影シール2を作成する作成者が所持する第1の携帯端末装置60と、電子印影シール2を検証する検証者が所持する第2の携帯端末装置61とから少なくとも構成され、図5では、第1の携帯端末装置60と第2の携帯端末装置61以外に、無線通信機能を有するシールプリンタ4と、様々な人や会社の公開鍵を公開している認証局5に加え、データを記憶する機能を有するストレージサーバ7を図示している。

【0043】

上述した実施形態では、文字の画像を文字認識することで得られたテキストを署名対象データとしていたため、署名対象データを光学コード20にエンコードすることができたが、署名対象データを文書3の画像とする変形例の場合、圧縮しても文書3の画像の容量は光学コード20の容量をオーバーしてしまうため、署名対象データとする文書3の画像をストレージサーバ7に保存し、署名対象データの保存先を示すURLをデータソースとして電子印影に含ませるようにしている。

【0044】

変形例においても、電子印影シール2の生成及び検証機能を電子印影アプリケーション62で実現しているため、第1の携帯端末装置10と第2の携帯端末装置11は汎用のカメラ付き携帯端末装置で実現することができ、第1の携帯端末装置60と第2の携帯端末装置61として利用される汎用のカメラ付き携帯端末装置には、図2で図示したような電

10

20

30

40

50

気回路等が組み込まれている。

【 0 0 4 5 】

図 6 は、変形例における電子印影アプリケーション 6 2 を説明する図である。変形例においても、電子印影シール 2 の生成及び検証機能に係わる処理を制御回路 1 0 0 に実行させるための電子印影アプリケーション 6 2 には、電子印影シール 2 を生成するときに作動し、本発明の印影生成手段として機能する印影生成モジュール 6 2 0 と、電子印影シール 2 を検証するときに作動し、本発明の印影検証手段として機能する印影検証モジュール 6 2 1 が含まれるが、上述した実施形態とは、それぞれモジュールが実行する処理が異なる。

【 0 0 4 6 】

図 7 は、変形例において電子印影シール 2 を作成するときのフローを説明する図である。作成者が電子印影シール 2 を生成する際、作成者は第 1 の携帯端末装置 6 0 に実装されている電子印影アプリケーション 6 2 の印影生成モジュール 6 2 0 を起動させた後、電子印影シール 2 を押印する文書 3 を第 1 の携帯端末装置 6 0 のカメラ回路 1 0 1 で撮影すると (S 2 0)、第 1 の携帯端末装置 6 0 に実装された電子印影アプリケーション 1 2 の印影生成モジュール 6 2 0 は、カメラ回路 1 0 1 で撮影された画像を文書 3 の画像として取得する (S 2 1)。

【 0 0 4 7 】

第 1 の携帯端末装置 6 0 に実装された電子印影アプリケーション 1 2 の印影生成モジュール 6 2 0 は、文書 3 の画像を取得すると、デジタル署名の対象となる署名対象データを文書 3 の画像から生成する (S 2 2)。上述した実施形態では、文書 3 の画像を文字認識することで得られるテキストを署名対象データとして生成していたが、変形例では、文書 3 の画像そのものを署名対象データとする。

【 0 0 4 8 】

第 1 の携帯端末装置 6 0 に実装された電子印影アプリケーション 6 2 の印影生成モジュール 6 2 0 は、デジタル署名の対象となる署名対象データを生成すると、署名対象データのメッセージダイジェストとなるハッシュ値を演算し (S 2 3)、第 1 の携帯端末装置 6 0 の U S I M 回路 1 0 6 を作動させて、該ハッシュ値をデータ部に含ませたデジタル署名生成コマンドを第 1 の携帯端末装置 6 0 の U S I M 1 0 7 に送信することで、該ハッシュ値のデジタル署名を該 U S I M 1 0 7 に算出させ、作成者の U S I M 1 0 7 からデジタル署名を取得する (S 2 4)。

【 0 0 4 9 】

また、第 1 の携帯端末装置 6 0 に実装された電子印影アプリケーション 6 2 の印影生成モジュール 6 2 0 は、第 1 の携帯端末装置 6 0 の U S I M 回路 1 0 6 を作動させて、第 1 の携帯端末装置 6 0 の U S I M 1 0 7 にリードコマンドを送信することで、認証局 5 の U R I と印影データを該 U S I M 1 0 7 から読み出す (S 2 5)。

【 0 0 5 0 】

次に、第 1 の携帯端末装置 6 0 に実装された電子印影アプリケーション 6 2 の印影生成モジュール 6 2 0 は、第 1 の携帯端末装置 6 0 の無線通信回路 1 0 3 を利用して、署名対象データとなった文書 3 の画像をストレージサーバ 7 に送信することで、署名対象データとなった文書 3 の画像をストレージサーバ 7 に保存させ、署名対象データとなった文書 3 の画像の保存先を示す U R I をストレージサーバ 7 から受信する (S 2 6)。

【 0 0 5 1 】

そして、第 1 の携帯端末装置 6 0 に実装された電子印影アプリケーション 6 2 の印影生成モジュール 6 2 0 は、第 1 の携帯端末装置 6 0 の U S I M 1 0 7 から取得したデジタル署名、デジタル署名の対象となった署名対象データの保存先を示すデータソース (ここでは、文書 3 の画像の保存先を示す U R I) 及び、第 1 の携帯端末装置 6 0 の U S I M 1 0 7 から読み出した認証局 5 の U R I を含む電子印影を生成した後 (S 2 7)、第 1 の携帯端末装置 6 0 の U S I M 1 0 7 から読み出した印影画像が中央部に配置され、電子印影をエンコードした光学コード 2 0 の印刷データを生成し (S 2 8)、生成した印刷データを

10

20

30

40

50

シールプリンタ 4 に送信して、該光学コード 2 0 が印刷された電子印影シール 2 がシールプリンタ 4 から出力される (S 2 9)。

【 0 0 5 2 】

図 8 は、変形例において電子印影シール 2 を検証するときのフローを説明する図である。電子印影シール 2 の検証者が、第 2 の携帯端末装置 6 1 を利用して文書 3 に貼られた電子印影シール 2 を検証する際、検証者は第 2 の携帯端末装置 6 1 に実装されている電子印影アプリケーション 6 2 の印影検証モジュール 6 2 1 を起動させた後、文書 3 に貼られた電子印影シール 2 を第 2 の携帯端末装置 1 1 のカメラ回路 1 0 1 で撮影すると (S 3 0)、第 2 の携帯端末装置 1 1 に実装された電子印影アプリケーション 6 2 の印影検証モジュール 6 2 1 は、カメラ回路 1 0 1 で撮影した電子印影シール 2 の画像に含まれる光学コード 2 0 をデコードし、署名対象データから算出されたデジタル署名、デジタル署名を生成した署名対象データの保存先を示すデータソース、及び、認証局 5 の U R I を含む電子印影を取得する (S 3 1)。

10

【 0 0 5 3 】

次に、第 2 の携帯端末装置 6 1 に実装された電子印影アプリケーション 6 2 の印影検証モジュール 6 2 1 は、第 2 の携帯端末装置 6 1 の無線通信回路 1 0 3 を利用して、デコードした電子印影に含まれる認証局 5 の U R I にアクセスし、ここでは、認証局 5 の U R I で公開されている公開鍵証明書と認証局 5 の公開鍵を取得し (S 3 2)、認証虚無の公開鍵を用いて該公開鍵証明書を検証する (S 3 3)。

【 0 0 5 4 】

20

認証局 5 の公開鍵を用いた公開鍵証明書の検証に成功すると、第 2 の携帯端末装置 6 1 に実装された電子印影アプリケーション 6 2 の印影検証モジュール 6 2 1 は、デコードした電子印影に含まれるデータソースを利用して、デジタル署名の対象なった署名対象データを取得する (S 3 4)。変形例では、文書 3 の画像の保存先を示す U R I をデータソースとしているため、第 2 の携帯端末装置 6 1 に実装された電子印影アプリケーション 6 2 の印影検証モジュール 6 2 1 は、第 2 の携帯端末装置 6 1 の無線通信回路 1 0 3 を利用して、文書 3 の画像の保存先を示す U R I にアクセスし、署名対象データを取得する。

【 0 0 5 5 】

そして、第 2 の携帯端末装置 6 1 に実装された電子印影アプリケーション 6 2 の印影検証モジュール 6 2 1 は、デコードした電子印影に含まれるデータソースを利用して取得した署名対象データのメッセージダイジェストとなるハッシュ値を算出した後、公開鍵証明書に記述されている公開鍵を用いてデジタル署名を復号した値と、光学コード 2 0 から取得した署名対象データから算出したハッシュ値が一致するか確認することで、デコードした電子印影に含まれるデジタル署名を検証する (S 3 5)。

30

【 0 0 5 6 】

そして、第 2 の携帯端末装置 6 1 に実装された電子印影アプリケーション 6 2 の印影検証モジュール 6 2 1 は、デコードした電子印影に含まれるデジタル署名の検証に成功すると、該デジタル署名の検証の成功結果として、デコードした電子印影に含まれるデータソースを利用して取得した署名対象データ、ここでは、文書 3 の画像を第 2 の携帯端末装置 6 1 のディスプレイ回路 1 0 2 に表示させ、この手順を終了する。

40

【符号の説明】

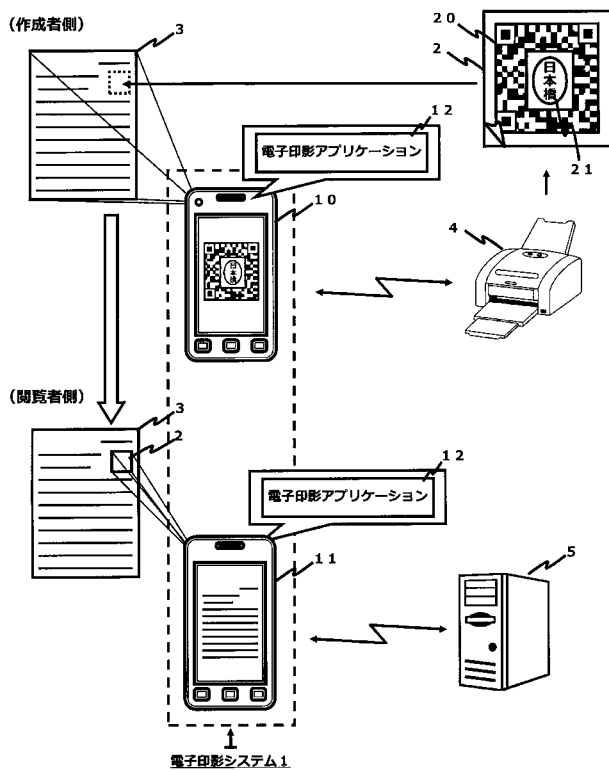
【 0 0 5 7 】

- 1, 6 電子印影システム
- 1 0, 6 0 第 1 の携帯端末装置
- 1 1, 6 1 第 2 の携帯端末装置
- 1 2, 6 2 電子印アプリケーション
- 1 2 0, 6 2 0 印影生成モジュール
- 1 2 1, 6 2 1 印影検証モジュール
- 2 電子印影シール
- 2 0 光学コード

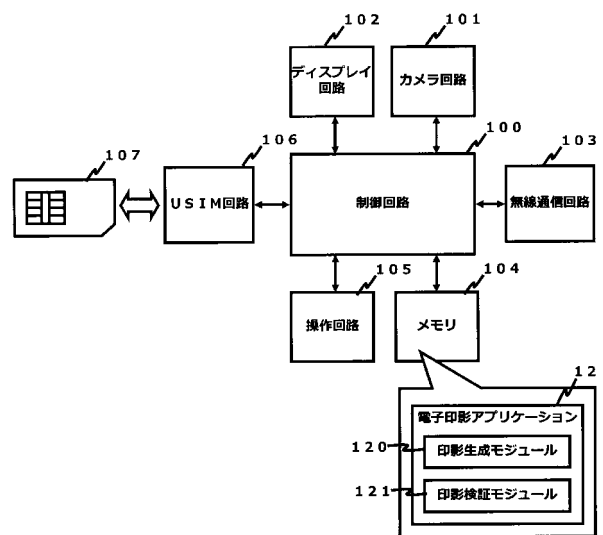
50

- 2 1 印影
- 3 文書
- 4 シールプリンタ
- 5 認証局
- 7 ストレージサーバ

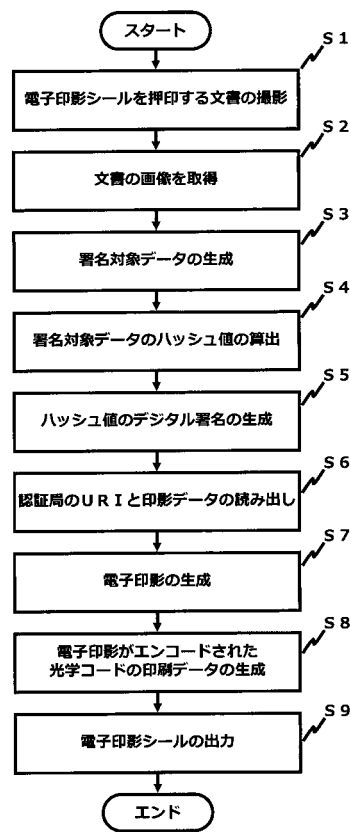
【図 1】



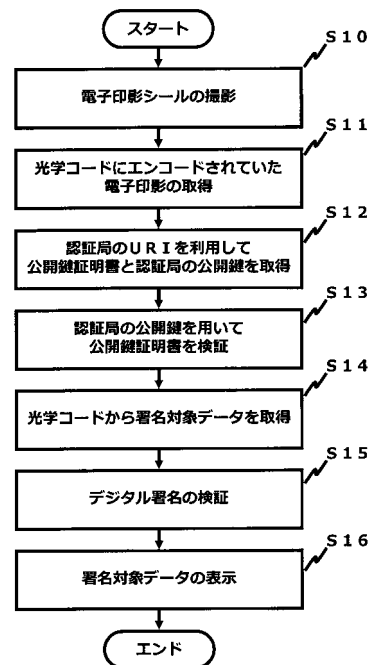
【図 2】



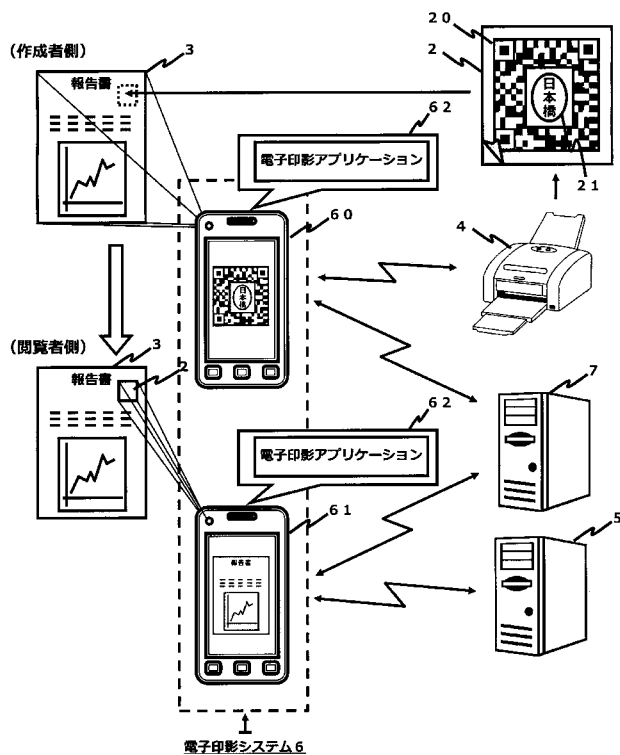
【図 3】



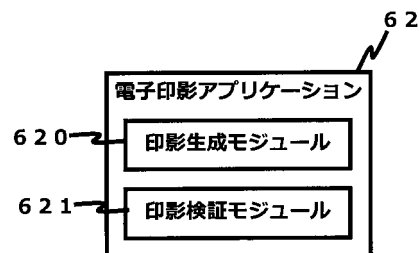
【図 4】



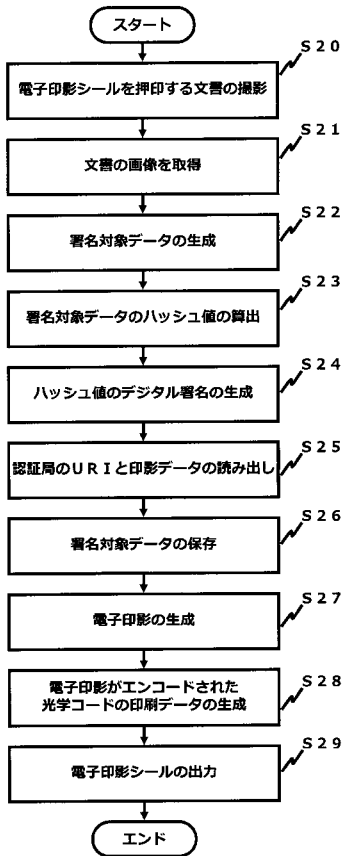
【図 5】



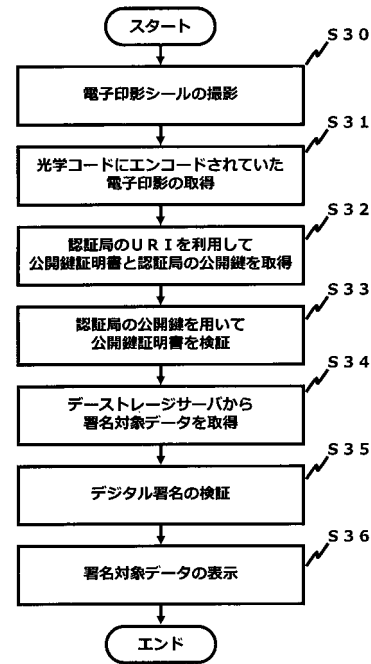
【図 6】



【 図 7 】



【 図 8 】



フロントページの続き

- (72)発明者 西岡 一樹
東京都新宿区市谷加賀町一丁目1番1号 大日本印刷株式会社内
- (72)発明者 岩佐 聖和
東京都新宿区市谷加賀町一丁目1番1号 大日本印刷株式会社内
- (72)発明者 高木 景子
東京都新宿区市谷加賀町一丁目1番1号 大日本印刷株式会社内
- (72)発明者 山本 綾子
東京都新宿区市谷加賀町一丁目1番1号 大日本印刷株式会社内

Fターム(参考) 5B017 AA02 BA09 BB02 CA16
5J104 AA09 AA16 AA32 EA05 EA08 EA19 JA21 LA05 LA06 NA02
NA12 NA37 NA38 PA07