(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年11 月25 日 (25.11.2004)

PCT

(10) 国際公開番号
WO 2004/102947 A1

(51) 国際特許分類[7]: H04N 1/00

(21) 国際出願番号: PCT/JP2004/006372

(22) 国際出願日: 2004 年5 月12 日 (12.05.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-134824 2003 年5 月13 日 (13.05.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社ＰＦＵ (PFU LIMITED) [JP/JP]; 〒9291192 石川県かほく市宇野気ヌ９８番地の２ Ishikawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 楠 忠和 (KUSUNOKI, Tadakazu) [JP/JP]; 〒9291192 石川県かほく市宇野気ヌ９８番地の２ 株式会社ＰＦＵ内 Ishikawa (JP). 中島 俊樹 (NAKAJIMA, Toshiki) [JP/JP]; 〒9291192 石川県かほく市宇野気ヌ９８番地の２ 株式会社ＰＦＵ内 Ishikawa (JP). 北川 光一 (KITAGAWA, Koichi) [JP/JP]; 〒9291192 石川県かほく市宇野気ヌ９８番地の２ 株式会社ＰＦＵ内 Ishikawa (JP). 鬱田 大介 (KUTSUWADA, Daisuke) [JP/JP]; 〒9291192 石川県かほく市宇野気ヌ９８番地の２ 株式会社ＰＦＵ内 Ishikawa (JP). 金光 憲雄 (KANEMITSU, Norio) [JP/JP]; 〒9291192 石川県かほく市宇野気ヌ９８番地の２ 株式会社ＰＦＵ内 Ishikawa (JP).

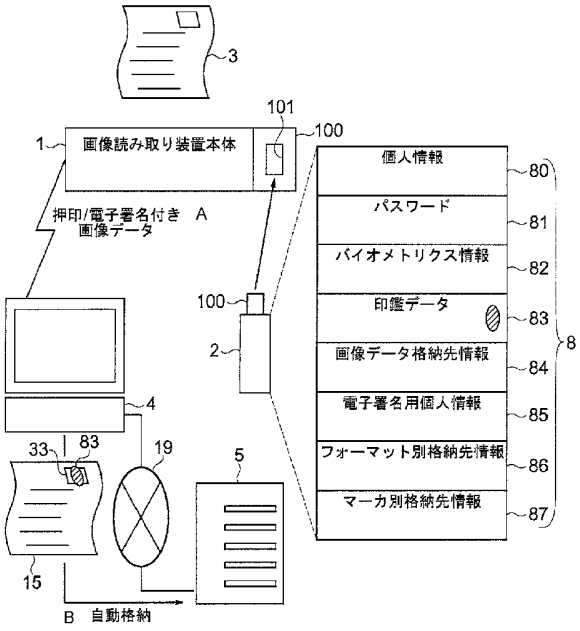
(74) 代理人: 渡部 章彦 (WATANABE, Akihiko); 〒1160013 東京都荒川区西日暮里５丁目１１番８号 三共セントラルプラザビル５階 開明国際特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,

[続葉有]

(54) Title: IMAGE READER

(54) 発明の名称: 画像読み取り装置



1...IMAGE READER BODY
A...IMAGE DATA WITH SEAL/DIGITAL SIGNATURE
B...AUTOMATICALLY STORED
80...PERSONAL INFORMATION
81...PASSWORD
82...BIOMETRICS INFORMATION
83...SEAL IMPRESSION DATA
84...IMAGE DATA STORAGE INFORMATION
85...DIGITAL SIGNATURE PERSONAL INFORMATION
86...STORAGE LOCATION INFORMATION BY FORMAT
87...STORAGE INFORMATION BY MARKER

(57) Abstract: An image reader (100) has a removal memory device (2) in which authentication information for authenticating a user is stored. An image reader body (1) has authentication means that authenticates the user by comparing authentication information (8) stored in the removal memory device (2) with authentication information (9) pre-registered in the image reader (100). Only when authenticated by the authentication means, the user reads a document (3) using the image reader (100) and adds digital signature and approval information to image the data (15) that is read.

(57) 要約: 画像読み取り装置（１００）は使用者の本人認証を行うための認証情報を格納した着脱可能なメモリデバイス（２）を備える。画像読み取り装置本体（１）は、着脱可能なメモリデバイス（２）に格納された認証情報（８）と、画像読み取り装置（１００）に予め登録された認証情報（９）を照合することで、使用者が本人であるか本人認証を行う手段を備える。本人認証を行う手段により認証された場合にのみ、画像読み取り装置（１００）を使用して原稿文書（３）の読み取りを行い、読み取られた画像データ（１５）に電子署名や承認情報を付加する。

WO 2004/102947 A1

BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

画像読み取り装置

技術分野

[0001] この発明は、原稿となる文書を光学的に読み取り、電子化して画像データを得ることができる画像読み取り装置に関し、特に、着脱可能なメモリデバイスを備え、この着脱可能なメモリデバイスに使用者の認証情報を格納しておくことで、画像読み取り装置を使用する使用者の本人認証を行えるようにし、認証後に読み取った画像データに承認情報や電子署名情報の付加を行うことができる画像読み取り装置に関する。

背景技術

[0002] 企業などでは、情報の共有化や保存場所の問題を解決するために、紙などに印刷された文書を、電子化して画像データとして保存を行うことが、一般化してきている。このような画像データを活用して行くにあたり、その画像データが改ざんされたり、その画像データの作成者として別の者がなりすましたりなどの不正な使用を防ぐことが求められてきている。

[0003] 従来、画像読み取り装置が接続されたパーソナルコンピュータ側でパスワードなどによる使用者の本人認証処理を行い、認証された者のみが画像読み取り装置を使用して画像の読み取りを実行でき、これにより読み取られた画像データに、ホストであるパーソナルコンピュータやより高機能なワークステーションで管理されている電子認証のための秘密鍵を使用して、電子署名情報を付加したり、承認情報を付加したりする装置が考案されている。

特許文献1:特開平8−139717号公報

発明の開示

発明が解決しようとする課題

[0004] しかし、近年、画像読み取り装置をホストであるパーソナルコンピュータ(ホスト)側と接続せずに、単体で使用し、読み取った画像データを着脱可能なメモリデバイスに直接格納するような使用方法が用いられるようになっている。このような場合に、前記のパーソナルコンピュータ側で本人認証処理や電子署名処理を行なう構成では、本

人認証処理や電子署名処理ができない。

[0005]

本発明の目的は、画像読み取り装置がパーソナルコンピュータなどのホスト装置に接続されずに使用されたり、本人認証や電子署名処理の機能のないホスト装置に接続されて使用されたりするような場合でも、確実に本人認証が可能で、読み取った画像データを、改ざんやなりすましなどの不正な使用から防ぐことができる画像読み取り装置を提供することにある。

課題を解決するための手段

[0006] 画像読み取り装置の使用者の本人認証を行うための認証情報を格納した着脱可能なメモリデバイスを備え、この着脱可能なメモリデバイスに格納された認証情報を使用して本人認証を行う手段を備えるように構成する。

[0007] この着脱可能なメモリデバイスに格納する認証情報として、パスワードを格納しておき、画像読み取り装置の使用開始時に使用者が、画像読み取り装置に備えられたパスワード入力手段からパスワードを入力し、これと着脱可能なメモリデバイスに格納されたパスワードを照合することで、使用者が本人であるか認証を行うように構成してもよい。

[0008] 着脱可能なメモリデバイスに格納する認証情報として、使用者本人のバイオメトリクス情報を格納しておき、画像読み取り装置側に指紋読み取り装置や声紋検出装置を備えることで、これらの装置から入手した使用者のバイオメトリクス情報と、着脱可能なメモリデバイスに格納されたバイオメトリクス情報との照合を行うことで、使用者が本人であるか認証を行うように構成してもよい。

[0009] 上記の本人認証を行う手段により本人認証がされた場合、読み取った画像に、承認済みを示す印鑑、シグニチャー、ロゴなどの画像を付加する手段を備えるように構成する。

[0010] 承認済みを示す画像を付加する手段において、着脱可能なメモリデバイスに格納された使用者固有の承認済みを示す画像を使用して、画像を付加する処理を行うように構成してもよい。

[0011] 承認済みを示す画像を付加する手段において、画像読み取り装置により読み取っ

た画像が所定のフォーマットの原稿画像であった場合には、予め決められた位置に承認済みを示す画像を付加するように構成してもよい。

[0012] 承認済みを示す画像を付加する手段において、原稿に記されたマーカを検出し、マーカの記入内容により色やサイズを変更して承認済みを示す画像を付加するように構成してもよい。

[0013] 承認済みを示す画像を付加する手段において、原稿に記されたマーカを検出し、マーカの記入内容により複数の種類の承認済みを示す画像を切り替えて付加するように構成してもよい。

[0014] 本人認証を行う手段により認証された場合、読み取った画像データに電子署名処理を施す手段を備えるように構成する。

[0015] 電子署名処理を施す手段として、着脱可能なメモリデバイスに格納された情報を使用して電子署名処理を行うように構成してもよい。

[0016] 本人認証を行う手段により認証された場合、読み取った文書のフォーマットを認識する手段により、読み取った文書のフォーマットを判定し、このフォーマット情報と、着脱可能なメモリデバイスに格納された、フォーマットごとの画像データ格納先情報を用いて、指定された格納先に読み取った画像データを格納する画像データ格納手段を備えるように構成する。

[0017] 本人認証を行う手段により認証された場合、原稿に記されたマーカを検出し、マーカの記入内容と、着脱可能なメモリデバイスに格納された、マーカの記入内容ごとの画像データ格納先情報を用いて、指定された格納先に読み取った画像データを格納する画像データ格納手段を備えるように構成してもよい。

発明の効果

[0018] 着脱可能なメモリデバイスに格納された認証情報を使用して本人認証を行うことにより、画像読み取り装置に正当な認証情報が格納された着脱可能なメモリデバイスを装着しない限り、画像読み取り装置を使用することができないようにでき、正当な認証情報を有した着脱可能なメモリデバイスをもっていない者が、不正に装置を使用することを防ぐことができる。

[0019] 入力したパスワードと着脱可能なメモリデバイスに格納されたパスワードとを照合す

ることにより、画像読み取り装置に正当なパスワード情報が格納された着脱可能なメモリデバイスを装着しない限り、画像読み取り装置を使用することができないようにでき、正当なパスワード情報を有した着脱可能なメモリデバイスをもっていない者が、不正に装置を使用することを防ぐことができる。

[0020] 使用者のバイオメトリクス情報と着脱可能なメモリデバイスに格納されたバイオメトリクス情報との照合を行うことにより、偽造が困難な本人認証のデータを使用した認証処理が行えるようになり、より厳格な本人認証を行うことで、不正に装置を使用することを防ぐことができるようになる。

[0021] 読み取った画像に、承認済みを示す印鑑、シグニチャー、ロゴなどの画像を付加することにより、本人と認証された者が画像読み取り装置により承認が必要な文書を読み取ることで、紙文書の電子化と承認処理とを同時に行うことができる。

[0022] 着脱可能なメモリデバイスに格納された使用者固有の承認済みを示す画像を付加することにより、本人のみが所有している前記メモリデバイスに格納された本人固有の承認済みを示す画像を、画像読み取り装置による読み取り時に画像データに付加することができ、これにより読み取られた画像データの承認の信頼性を高めることができる。

[0023] 読み取った画像が所定のフォーマットの原稿画像であった場合に、予め決められた位置に承認済みを示す画像を付加することにより、定型文書を読み取る場合、承認印の押すべき位置が決まっている場合に、文書のフォーマットを判定することで、自動的に位置を判断して、適正な位置に承認済みを示す印鑑などの画像を付与することができるようになる。

[0024] 原稿に記されたマーカの記入内容に応じて承認済みを示す画像を付加することにより、フォーマットが定まっていない文書を読み取る場合でも、使用者がマーカを原稿に記入することで、このマーカを検出して自動的に承認済みを示す画像を付与する位置や、画像の色、サイズなどを適正な画像として画像データに付加することができるようになる。

[0025] 原稿に記されたマーカの記入内容に応じて複数の種類の承認済みを示す画像を切り替えて付加することにより、複数の種類の承認済みを示す画像がある場合、使用

者が必要な承認済みを示す画像の種類に合わせたマーカを、原稿の必要な位置に記すことで、このマーカを検出して自動的に適正な位置に、適正な種類の画像を付加することができるようになる。

[0026] 本人認証後に、着脱可能なメモリデバイスに格納された情報を使用して、読み取った画像データに電子署名処理を行うことにより、画像読み取り装置により読み取った画像データに、作成者本人を示す電子署名情報が付加され、その後にこの画像データを活用するにあたり、改ざんしたり、他人がなりすましたりするなどの不正な使用を防止することができるようになる。このとき、本人のみが所有している着脱可能なメモリデバイスに格納された認証情報により本人認証が行われており、また、電子署名にも本人のみが所有している着脱可能なメモリデバイスに格納された電子署名用の情報を使用することで、本人がその画像データを作成したことを確実に保証することができるようになる。

[0027] 本人認証後に、読み取った文書のフォーマット情報と着脱可能なメモリデバイスに格納された画像データ格納先情報とを用いて、指定された格納先に読み取った画像データを格納することにより、使用者である本人を着脱可能なメモリデバイスに格納された情報により確実に認証するとともに、認証された使用者が、読み取った画像データを格納したい格納先を読み取り対象である文書のフォーマットごとに、予め着脱可能なメモリデバイスに格納しておくことで、読み取りを行うと同時に、自動的に所定のフォーマットの原稿画像データを指定先の格納場所に格納できるようになる。

[0028] 本人認証後に、原稿に記されたマーカの記入内容と着脱可能なメモリデバイスに格納された画像データ格納先情報とを用いて、指定された格納先に読み取った画像データを格納することにより、使用者である本人を着脱可能なメモリデバイスに格納された情報により確実に認証するとともに、認証された使用者が、読み取った画像データを格納したい格納先を、マーカの記入内容ごとに予め着脱可能なメモリデバイスに格納しておき、読み取り対象の原稿に使用者が所定のマーカを記すことで、そのマーカの記された文書を読み取ると、マーカを検出して自動的にそのマーカの記された原稿画像データを指定先の格納場所に格納できるようになる。

発明を実施するための最良の形態

[0029] 図1に示すように、画像読み取り装置100は、原稿文書3を読み取る画像読み取り装置本体1と、使用者の本人認証を行うための認証情報8を格納した着脱可能なメモリデバイス2とを備える。画像読み取り装置本体1には、着脱可能なメモリデバイス2に格納された認証情報8(例えば、個人情報80)と、画像読み取り装置本体1に予め登録された認証情報を照合することで、使用者が本人であるか本人認証を行う手段を備えるように構成する。

[0030] 着脱可能なメモリデバイス2に格納する認証情報8として、パスワード81を格納しておくように構成してもよい。この場合、画像読み取り装置100の使用開始時に、画像読み取り装置本体1に備えられたパスワード入力手段により使用者にパスワードの入力を行わせ、入力されたパスワードと着脱可能なメモリデバイス2に格納されたパスワード81を照合することで、本人認証を行うように構成する。

[0031] 着脱可能なメモリデバイス2に格納する認証情報8として、使用者本人のバイオメトリクス情報82(指紋、声紋などの個人識別情報)を格納しておくように構成してもよい。この場合、格納したバイオメトリクス情報82と、画像読み取り装置本体1に備えられた指紋読み取り装置や声紋検出装置から読み取った使用者の情報とを照合することで、使用者が本人であるか本人認証を行う手段を備えるように構成する。

[0032] 上記の本人認証を行う手段により認証された場合にのみ、画像読み取り装置100を使用して、原稿文書3の読み取りを行うことができるように構成する。

[0033] 上記の本人認証を行う手段による認証後、読み取った画像データ15に承認済みを示す印鑑、シグニチャーやロゴなどの画像83を付加する手段を備えるよう構成する。

[0034] この承認済みを示す画像を付加する手段において、着脱可能なメモリデバイス2に格納された使用者固有の承認済みを示す画像83(例えば、印鑑データ83)を用いて画像付加処理を行うように構成してもよい。

[0035] 承認済みを示す画像を付加する手段において、読み取った画像データ15が所定のフォーマットであった場合には、予め決められた位置33に承認済みを示す画像83を付加するように構成してもよい。

[0036] 承認済みを示す画像を付加する手段において、原稿に記されたマーカを検出し、

マーカの記入内容により色やサイズを変更して承認済みを示す画像83を付加するように構成してもよい。

[0037] 承認済みを示す画像を付加する手段において、原稿に記されたマーカを検出し、マーカの記入内容により複数の種類の承認済みを示す画像83のいずれかを付加するように構成してもよい。

[0038] 本人認証を行う手段による認証後、読み取った画像データ15に電子署名処理を施す手段を備えるように構成する。

[0039] 電子署名処理を施す手段として、着脱可能なメモリデバイス2に格納された情報(電子署名用個人情報)85を使用して電子署名処理を行うように構成してもよい。

[0040] 本人認証を行う手段による認証後、読み取った文書のフォーマットを認識する手段により、読み取った文書のフォーマットを判定し、このフォーマット情報と、着脱可能なメモリデバイス2に格納された、フォーマットごとの画像データ格納先情報86を用いて、指定された格納先に読み取った画像データ15を格納する画像データ格納手段を備えるように構成する。

[0041] また、画像データ格納手段は、本人認証を行う手段による認証後、原稿に記されたマーカを検出し、マーカの記入内容と、着脱可能なメモリデバイス2に格納された、マーカの記入内容ごとの画像データ格納先情報87を用いて、指定された格納先に読み取った画像データ15を格納するように構成してもよい。

[0042] この画像データ格納先として、図1に示すように、画像読み取り装置100を接続しているパーソナルコンピュータ4や、さらに、このパーソナルコンピュータ4の接続されているネットワーク19上のサーバ5が指定される場合がある。この場合には、パーソナルコンピュータ4側に画像読み取り装置100側の画像データ格納手段からの指示により、読み取った画像データ15を格納する処理を行うPC側画像データ格納手段を備えるように構成する。

[0043] 以上のように、本発明の画像読み取り装置100は、装置の使用者を認証する情報などを格納した着脱可能なメモリデバイス2を備える画像読み取り装置である。本発明の画像読み取り装置100を使用する使用者は、予めその使用者が正当な使用権限を有する者である本人であるか、本人認証を行うための認証情報が格納された個

別の着脱可能なメモリデバイス2を持つようにしている。

[0044] この着脱可能なメモリデバイス2としては、画像読み取り装置本体1とUSB(Universal Serial Bus)で接続するフラッシュメモリを使用するように構成してもよい。

[0045] この着脱可能なメモリデバイス2を所有している使用者は、画像読み取り装置100により原稿文書3の読み取り処理を行う場合、まず画像読み取り装置本体1(の装着部101)に当該着脱可能なメモリデバイス2を装着する。着脱可能なメモリデバイス2を装着された画像読み取り装置本体1は、着脱可能なメモリデバイス2を装着されたことを検出し、本人認証処理を実行するように構成している。

[0046] 本人認証処理は、以下のように行われる。即ち、図2に示すように、画像読み取り装置本体1の認証処理部6が、着脱可能なメモリデバイス2に格納された使用者個別の認証情報8(例えば、個人情報80)を取得し、これと、画像読み取り装置本体1に予め登録された登録済み認証情報9とを照合し、本人であるか判定する。更に、認証された場合は、認証処理部6が装置制御部7に使用許諾を示す情報を送信することで、画像読み取り装置100を使用可能状態とする。

[0047] このときに使用する使用者個別の認証情報8としては、使用者の氏名や住所、会社の所属などの個人情報80であってもよいし、使用者個別のコード番号などの識別情報であってもよい。

[0048] 登録済み認証情報9と着脱可能なメモリデバイス2に格納された使用者個別の認証情報8とを照合することで本人認証を行う代わりに、図3に示すように、着脱可能なメモリデバイス2に使用者個別の認証情報8として使用者個別のパスワード81を格納しておくように構成してもよい。この場合、画像読み取り装置100の使用開始時に、画像読み取り装置本体1に備えられたパスワード入力手段10により、使用者にパスワードを入力させる。そして、これと着脱可能なメモリデバイス2に格納されたパスワード81を認証処理部6が照合することで本人認証を行う。

[0049] また、図4に示すように、使用者個別の認証情報8として使用者のバイオメトリクス情報82(指紋、声紋など)を着脱可能なメモリデバイス2に格納しておくように構成してもよい。この場合、画像読み取り装置本体1に備えられた指紋読み取り装置11や声紋検出装置12により、画像読み取り装置100の使用開始時に、使用者のバイオメトリク

ス情報を取得し、これと着脱可能なメモリデバイス2に格納されたバイオメトリクス情報82とを認証処理部6で照合することで本人認証を行う。

[0050] このようにして本人認証を行い、認証された場合、その後使用者は自由に画像読み取り装置100を使用することができることとなる。読み取り対象となる原稿文書3が承認処理の必要な文書であった場合には、読み取った原稿文書3の画像に、図5に示すように、承認済みを示す画像83(印鑑の印影の画像、即ち、印鑑データ83など)を付加するように構成している。

[0051] これは、以下のように処理される。即ち、図5に示すように、原稿文書3を読み取ったときに、画像読み取り装置本体1のフォーマット判定部13において、読み取られた原稿文書3の画像(図6参照)が予め登録してある所定の定型フォーマットの形式であるかパターン認識により判定する。そして、所定の定型フォーマットであった場合には、そのフォーマットに対応する承認用画像83を付加すべき位置33や種類の情報を、承認用画像83を付加する処理を行う承認用画像付加部14に送る。

[0052] 送られてきた承認用画像83の位置や種類の情報を受けた承認用画像付加部14では、承認用画像83をその情報で指定された位置33にあわせて、読み取った画像データ15に埋め込む処理を行う。このとき、埋め込む承認用画像83として、着脱可能なメモリデバイス2に格納されている、使用者個別の承認用画像83を使用するようにしてもよい。

[0053] このような処理を行うことで、図5に示すように、原稿文書3の読み取り画像15に承認用画像83を付加した画像データ15を出力するように構成している。

[0054] また、承認用画像の位置や種類を決定するフォーマット判定部13では、図6(A)に示すような、定型フォーマットをパターン認識により判定し、そのフォーマットごとに承認用画像83の位置や種類を決定するようにしてもよい。また、図6(B)に示すように、定型フォーマットでない原稿文書3を読み取る場合には、原稿文書3に使用者がマーカ34を記入することで、このマーカ34をフォーマット判定部13において検出するようにしてもよい。この場合、検出されたマーカ34の記入内容により、承認用画像83の位置や種類を決定するように構成してもよい。

[0055] このマーカ34の記入内容による承認用画像83の指定により、例えば、使用者が蛍

光ペンなどで承認用画像83の位置を指示することができる。また、その色の種類により、例えば、イエローの蛍光ペンによるマーカ34の場合は、日付入りの特殊な印鑑データ83を付加することを指示し、オレンジの蛍光ペンによるマーカ34の場合は、通常の印鑑データ83を付加することを指示することができる。このように、予め決めた規則に従って処理を行わせることができるようになる。

[0056] 図7に示すように、本人認証後の原稿文書3の読み取りにより読み取った画像データ15が、その後の利用や保存において、改ざんされたり、他人が作成者としてなりすましたりするなどの不正な使用行為が行われることから防ぐように、電子署名を行えるように構成している。

[0057] これは、以下のように処理される。即ち、図7に示すように、画像読み取り装置本体1の電子署名処理部16において、原稿文書3を読み取った画像データ15に、着脱可能なメモリデバイス2に格納されている電子署名用個人情報85を使用して電子署名データ155を付加することで、読み取った画像15に使用者本人が作成したことを示す電子署名を行うようにしている。

[0058] 以上のように、原稿文書3の画像読み取り処理により読み取られた画像データ15は、図8に示すように、着脱可能なメモリデバイス2に格納されている画像データの格納先情報84に基づいて、自動的に指定先の場所への格納が行われるように構成している。

[0059] この処理は、以下のように行われる。即ち、読み取った画像データ15のフォーマットをフォーマット判定部13において判定し、判定されたフォーマット種別情報を画像データ15の格納処理を行う画像データ格納処理部17に送る。画像データ格納処理部17では、このフォーマット種別情報と、着脱可能なメモリデバイス2に格納されている、フォーマット種別ごとの画像データの格納先情報86から、読み取った画像データ15の格納先を判定する。当該格納先が着脱可能なメモリデバイス2の画像データ格納域21の場合は、直接画像データ15を着脱可能なメモリデバイス2に格納する処理を実行する。当該格納先がこれ以外の場合は、パーソナルコンピュータ4のPC側画像データ格納処理部18に画像データ15及び格納先情報84を送信する。

[0060] この情報を受けたPC側画像データ格納処理部18では、格納先がパーソナルコン

ピュータ4の場合は、直接パーソナルコンピュータに画像データ15を格納する処理を実行し、格納先がネットワーク19に接続されている他のサーバ5のような場合には、ネットワーク通信処理を実行して、指定のサーバ5に画像データ15を格納する処理を実行する。

[0061] 以上のようにして、読み取った画像データ15を自動的に指定先の格納場所に格納する処理を行う。この時、読み取った画像データ15のフォーマット種別ごとに格納先を指定する代わりに、原稿に記されたマーカ34の記入内容により格納先を指定できるようにしてもよい。

[0062] この場合には、着脱可能なメモリデバイス2に格納されているフォーマットごとの画像データの格納先情報86の代わりに、マーカ34の記入内容ごとの画像データの格納先情報87(図1参照)を格納しておく。そして、フォーマット判定部13は、原稿文書3に記されたマーカ34を検出し、そのマーカ34の記入内容情報を画像データ格納処理部17に送る。画像データ格納処理部17はこれらの情報から格納先を決定する。

産業上の利用可能性

[0063] 本発明を利用することにより、ホスト側に認証機能などのセキュリティ機能を持たないシステムで使用される場合や、ホストに接続することなく画像読み取り装置単体で画像読み取りを行いフラッシュメモリなどのメモリデバイス2に直接画像データを格納するといった使われ方の場合でも、確実に使用権限のある本人のみがその画像読み取り装置を使用できることを保証することができ、また、読み取られた画像にも本人が作成したことを示す承認情報や電子署名情報などを付加することで、不正な使用から防ぐことができる画像読み取り装置を提供することができる。

図面の簡単な説明

[0064] [図1]本発明の全体構成図である。

[図2]予め登録された認証情報と照合を行う場合の説明図である。

[図3]パスワード入力による認証処理の説明図である。

[図4]認証情報としてバイオメトリクス情報を使用した場合の説明図である。

[図5]承認用画像情報付加処理の説明図である。

[図6]フォーマット又はマーカの種別による承認用画像の選択処理説明図である。

[図7]電子署名処理の説明図である。

[図8]読み取り画像データの自動格納処理説明図である。

請求の範囲

[1] 原稿を光学的に読み取り、電子化して画像データとして読み取ることができる画像読み取り装置において、

本人認証を行うための認証情報を格納した着脱可能なメモリデバイスと、

前記着脱可能なメモリデバイスに格納された認証情報を用いて、本人認証を行う手段とを備える

ことを特徴とする画像読み取り装置。

[2] 前記本人認証を行う手段は、前記着脱可能なメモリデバイスに格納された認証情報と、予め画像読み取り装置に登録してある認証情報とを照合することにより、前記本人認証を行う

ことを特徴とする請求項1記載の画像読み取り装置。

[3] 当該画像読み取り装置は、更に、

パスワードを入力させる入力手段を備え、

前記本人認証を行う手段は、前記入力手段から入力されたパスワードと前記着脱可能なメモリデバイスに格納された認証情報であるパスワード情報とを照合することにより、前記本人認証を行う

ことを特徴とする請求項1記載の画像読み取り装置。

[4] 当該画像読み取り装置は、更に、

指紋、声紋などのバイオメトリクス情報を検知する検知手段を備え、

前記本人認証を行う手段は、前記検知手段により検知されたバイオメトリクス情報と前記脱着可能なメモリデバイスに格納された認証情報であるバイオメトリクス情報とを照合することにより、前記本人認証を行う

ことを特徴とする請求項1記載の画像読み取り装置。

[5] 当該画像読み取り装置は、更に、

読み取った原稿画像に印鑑、シグニチャーやロゴなどの承認済みを示す画像を付加する手段を備える

ことを特徴とする請求項1記載の画像読み取り装置。

[6] 前記着脱可能なメモリデバイスは、更に、承認用の画像データを格納し、

前記承認済みを示す画像を付加する手段は、前記承認用の画像データを使用して承認済みを示す画像を前記読み取った原稿画像に付加する

ことを特徴とする請求項5記載の画像読み取り装置。

[7] 前記承認済みを示す画像を付加する手段は、前記読み取った原稿画像が所定のフォーマットであった場合、原稿画像の所定の位置に承認済みを示す画像を付加する

ことを特徴とする請求項5記載の画像読み取り装置。

[8] 前記承認済みを示す画像を付加する手段は、前記読み取った原稿画像から前記原稿に記された所定のマーカを検出した場合、そのマーカの記入内容に対応して、その色、サイズなどを切り替えて承認済みを示す画像を付加する

ことを特徴とする請求項5記載の画像読み取り装置。

[9] 前記承認済みを示す画像を付加する手段は、前記読み取った原稿画像から前記原稿に記された所定のマーカを検出した場合、前記検出したマーカの記入内容に対応して、複数の種類の承認済みを示す画像のいずれかを付加する

ことを特徴とする請求項5記載の画像読み取り装置。

[10] 当該画像読み取り装置は、更に、

読み取った原稿画像に電子署名処理を施す手段を備える

ことを特徴とする請求項1記載の画像読み取り装置。

[11] 前記電子署名処理を施す手段は、前記着脱可能なメモリデバイスに格納された情報を使用して電子署名処理を行う

ことを特徴とする請求項10記載の画像読み取り装置。

[12] 当該画像読み取り装置は、更に、

読み取った原稿画像のフォーマットを認識するフォーマット認識手段と、

前記読み取った原稿画像を格納する画像データ格納手段とを備え、

前記着脱可能なメモリデバイスは、文書のフォーマットに対応した、原稿画像の格納先を示す情報を格納し、

画像データ格納手段は、前記フォーマット認識手段により認識されたフォーマットの情報と前記格納先を示す情報とに基づいて、前記読み取った原稿画像を前記指定の格納先に格納する

ことを特徴とする請求項1記載の画像読み取り装置。

[13] 当該画像読み取り装置は、更に、

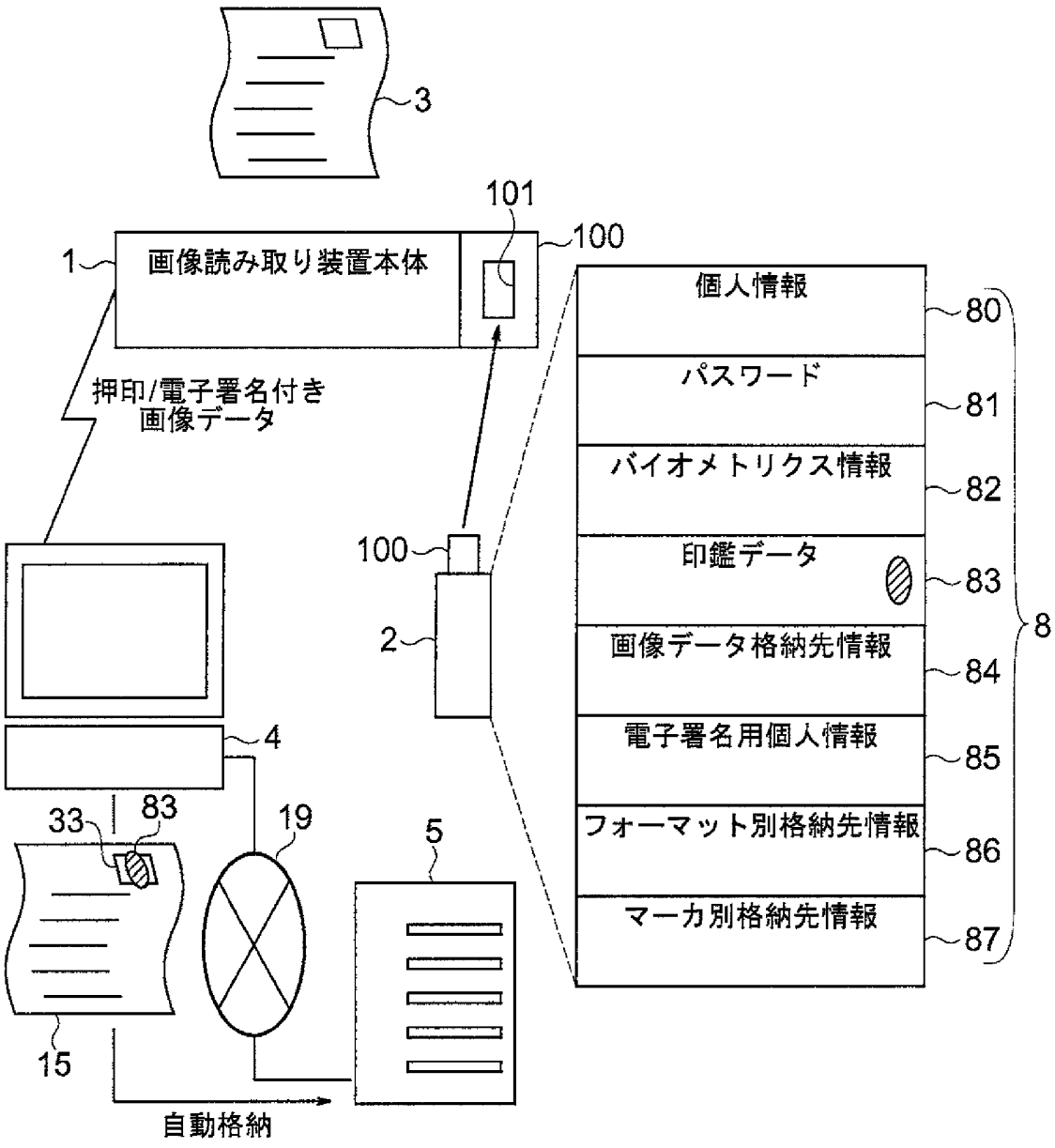
読み取った原稿画像を格納する画像データ格納手段を備え、

前記着脱可能なメモリデバイスは、所定のマーカの記入内容に対応した、原稿画像の格納先を示す情報を格納し、

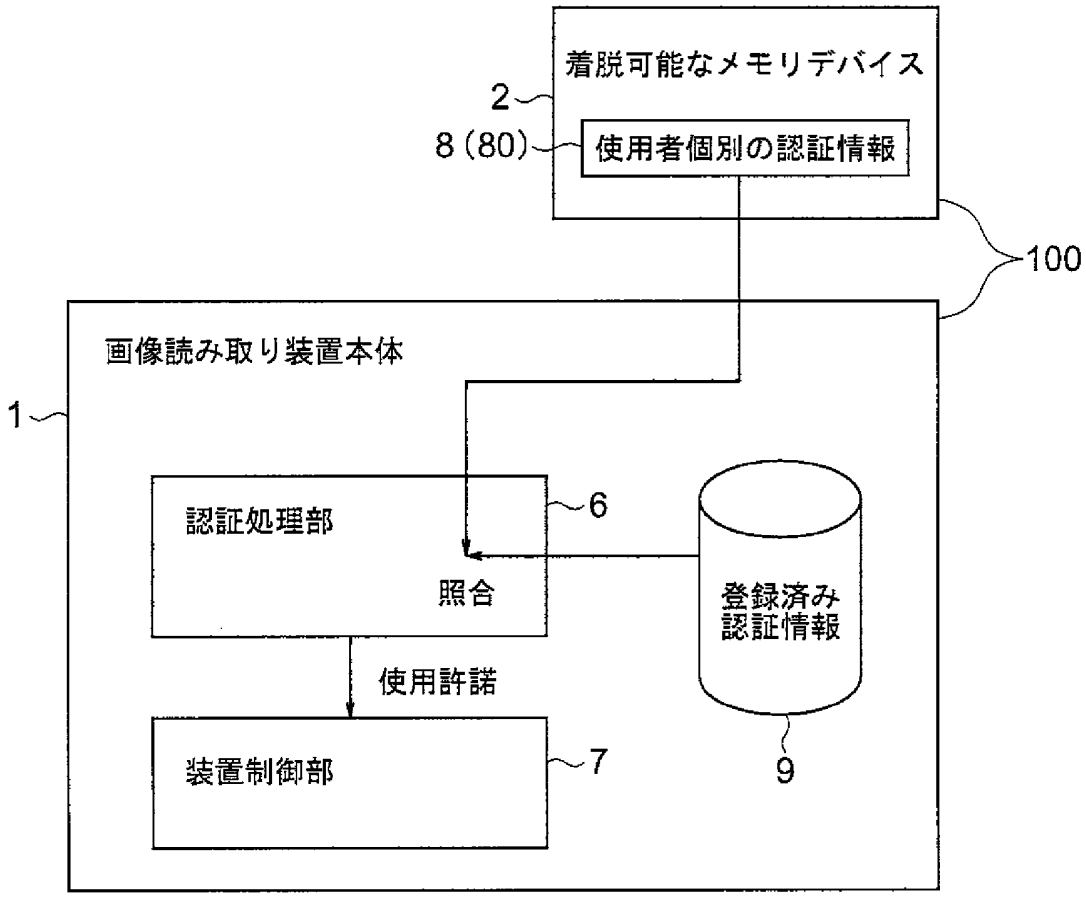
前記画像データ格納手段は、原稿に記されたマーカを検出した場合、前記マーカの記入内容と前記格納先を示す情報とに基づいて、前記読み取った原稿画像を前記指定の格納先に格納する

ことを特徴とする請求項1記載の画像読み取り装置。

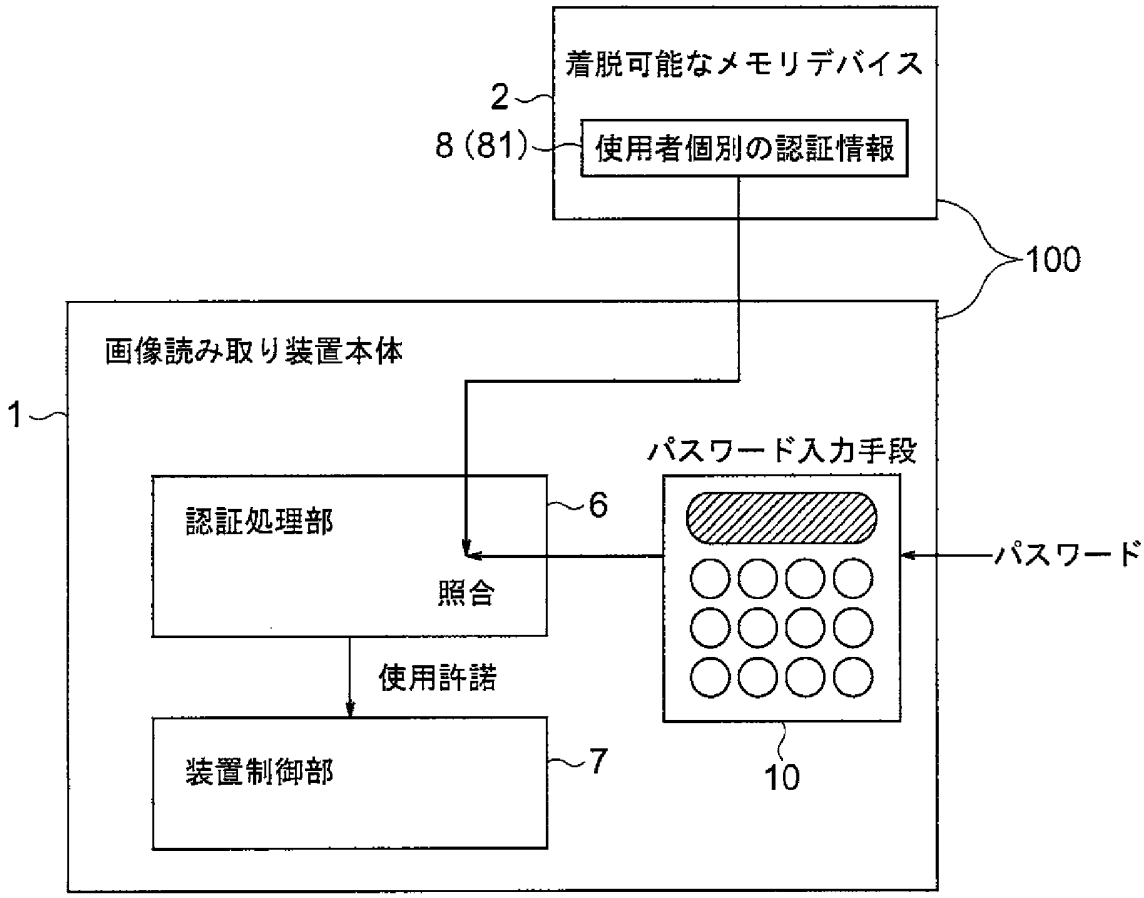
[図1]


3
101
100
1
画像読み取り装置本体
押印/電子署名付き
画像データ
100
2
4
33
83
19
5
15
自動格納
個人情報
80
パスワード
81
バイオメトリクス情報
82
印鑑データ
83
画像データ格納先情報
84
電子署名用個人情報
85
フォーマット別格納先情報
86
マーカ別格納先情報
87
8

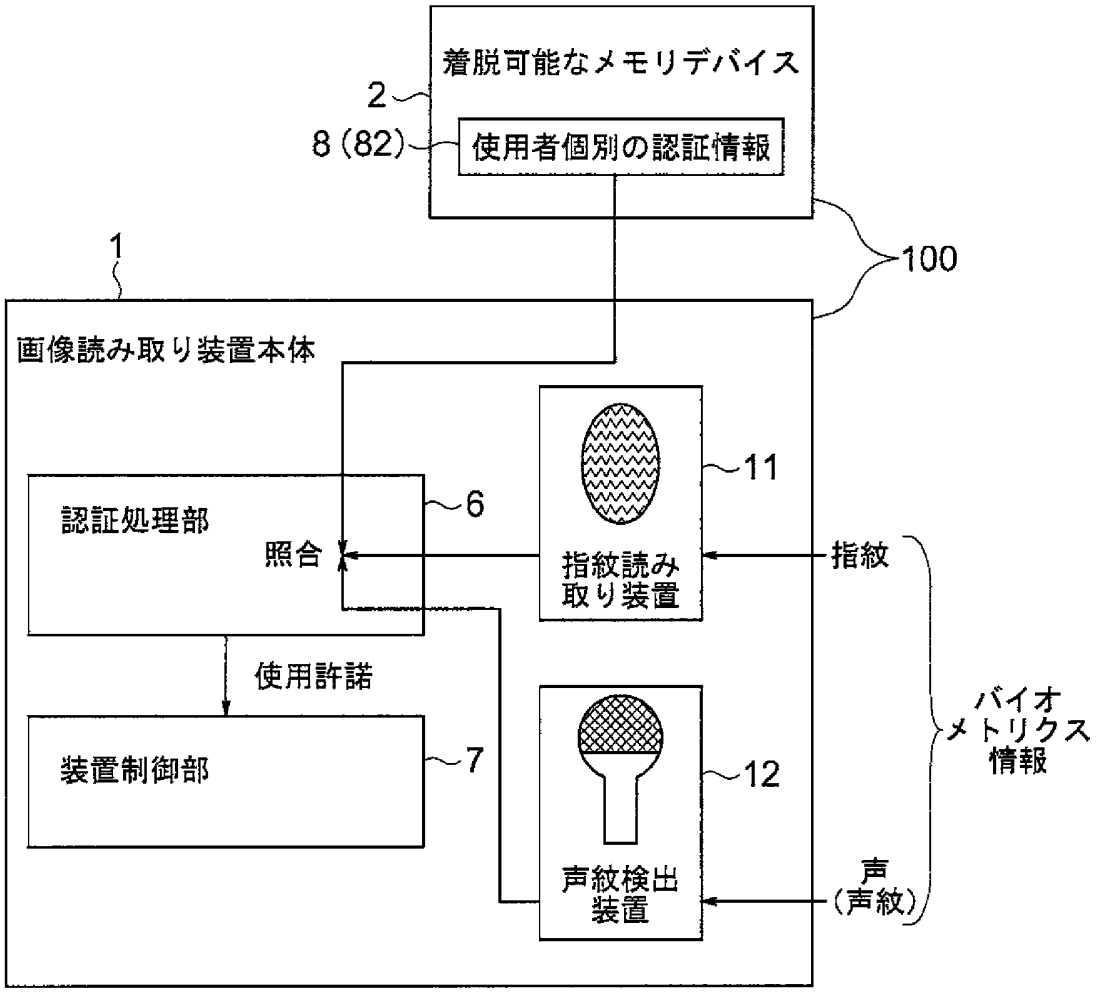
[図2]


着脱可能なメモリデバイス
2
8 (80)
使用者個別の認証情報
100
画像読み取り装置本体
1
認証処理部
6
照合
登録済み
認証情報
使用許諾
装置制御部
7
9

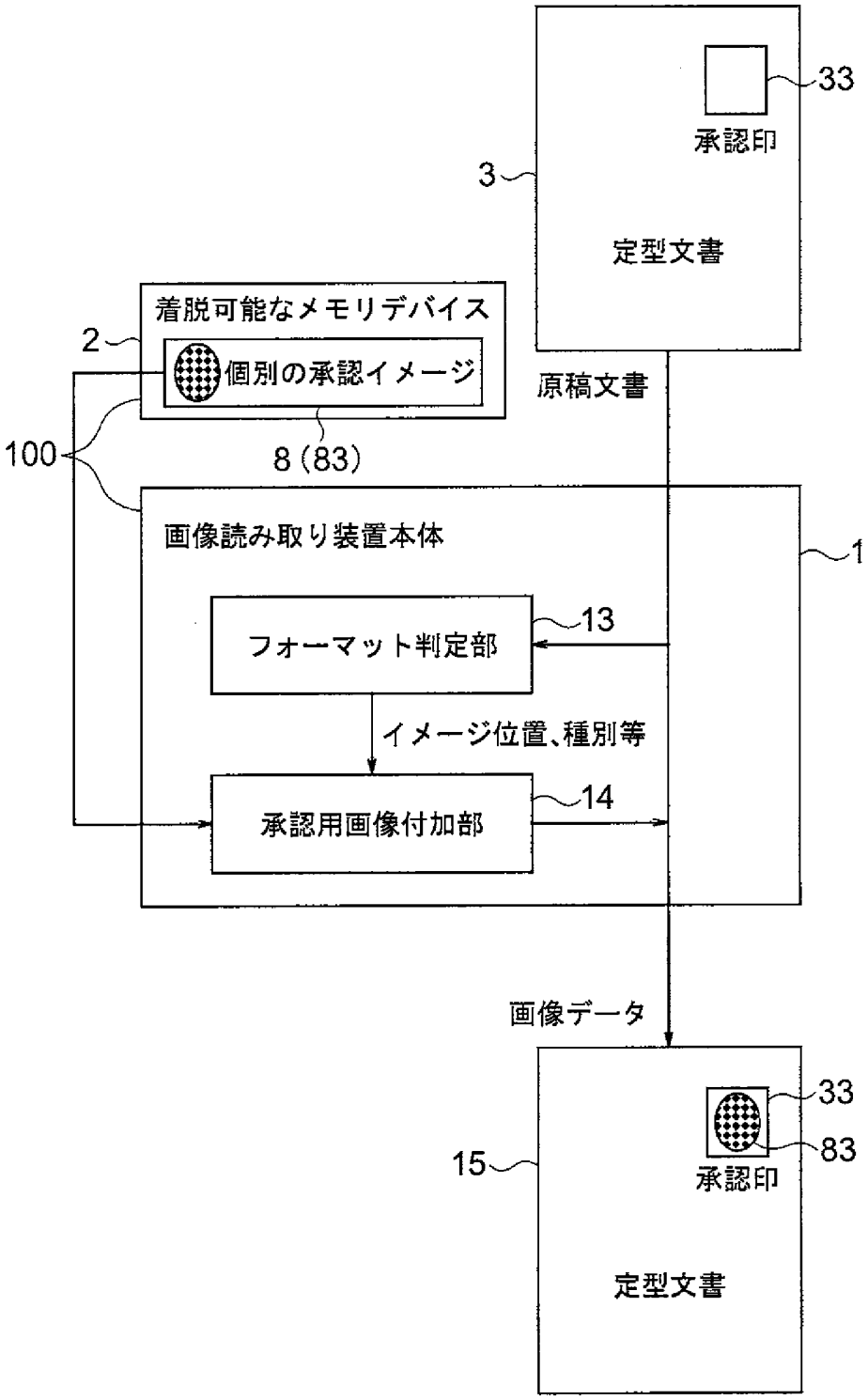
[図3]


着脱可能なメモリデバイス
2
8 (81)
使用者個別の認証情報
100
画像読み取り装置本体
1
パスワード入力手段
認証処理部
6
照合
パスワード
使用許諾
装置制御部
7
10

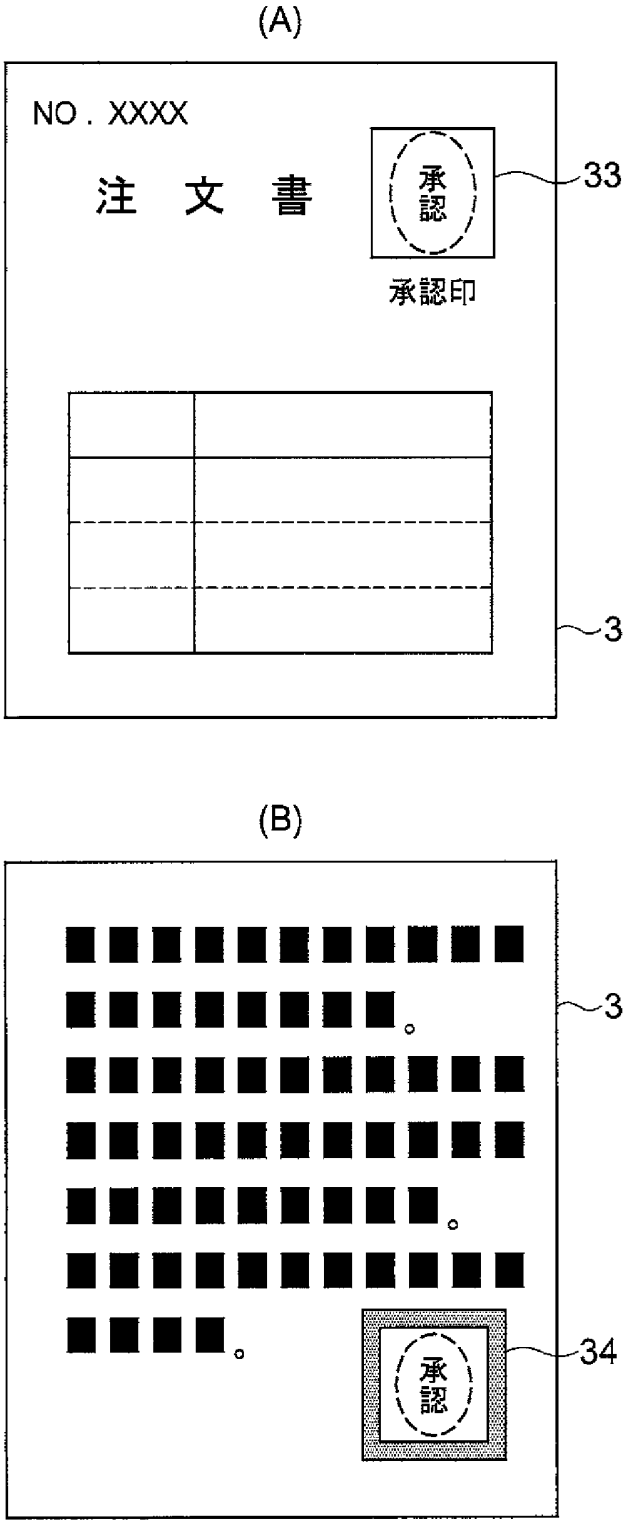
[図4]


着脱可能なメモリデバイス
2
8 (82)
使用者個別の認証情報
100
1
画像読み取り装置本体
11
認証処理部
6
照合
指紋読み取り装置
指紋
使用許諾
バイオメトリクス情報
装置制御部
7
12
声紋検出装置
声(声紋)

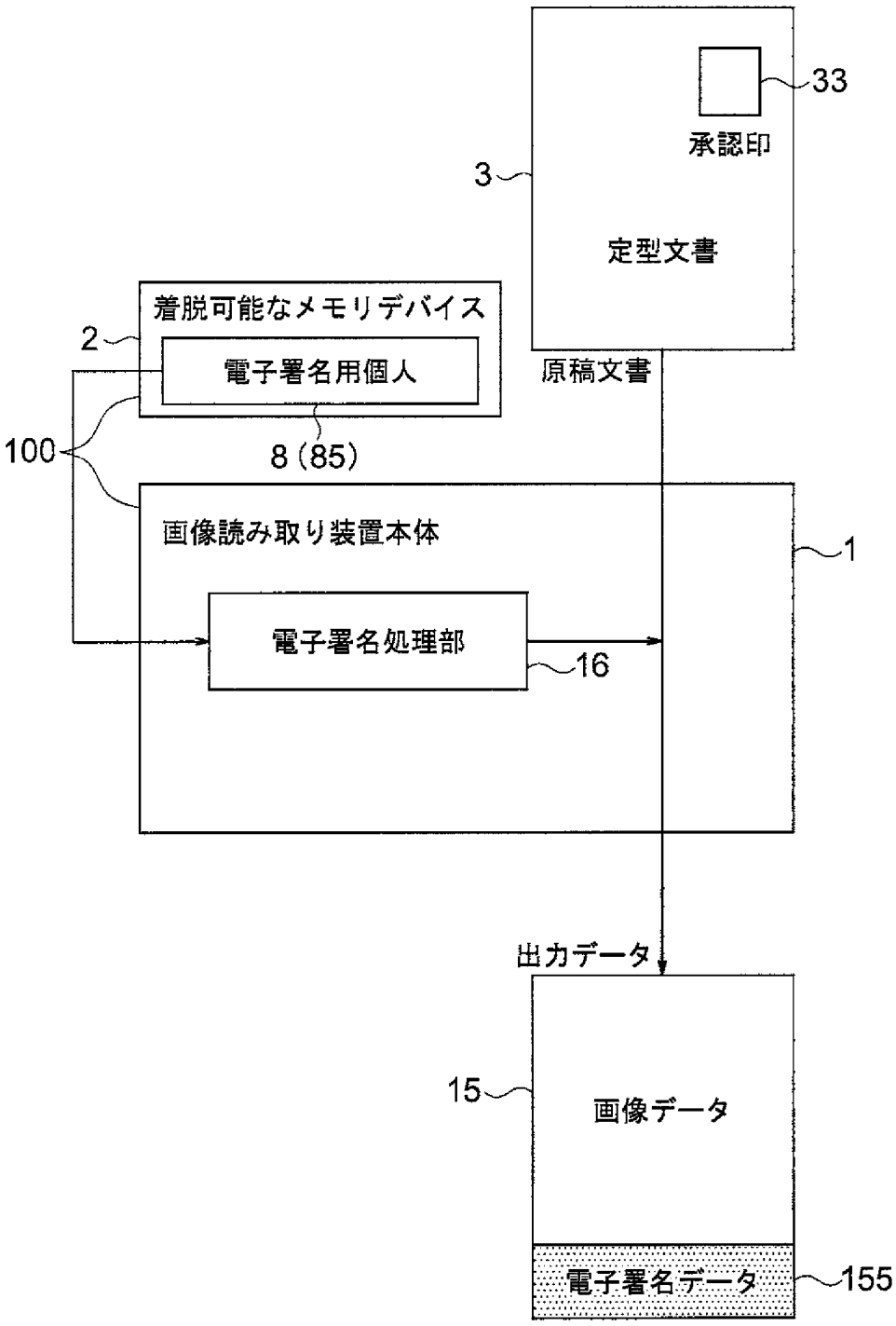
[図5]


33
承認印
3
定型文書
着脱可能なメモリデバイス
2
個別の承認イメージ
原稿文書
100
8 (83)
画像読み取り装置本体
1
フォーマット判定部
13
イメージ位置、種別等
承認用画像付加部
14
画像データ
33
83
15
承認印
定型文書

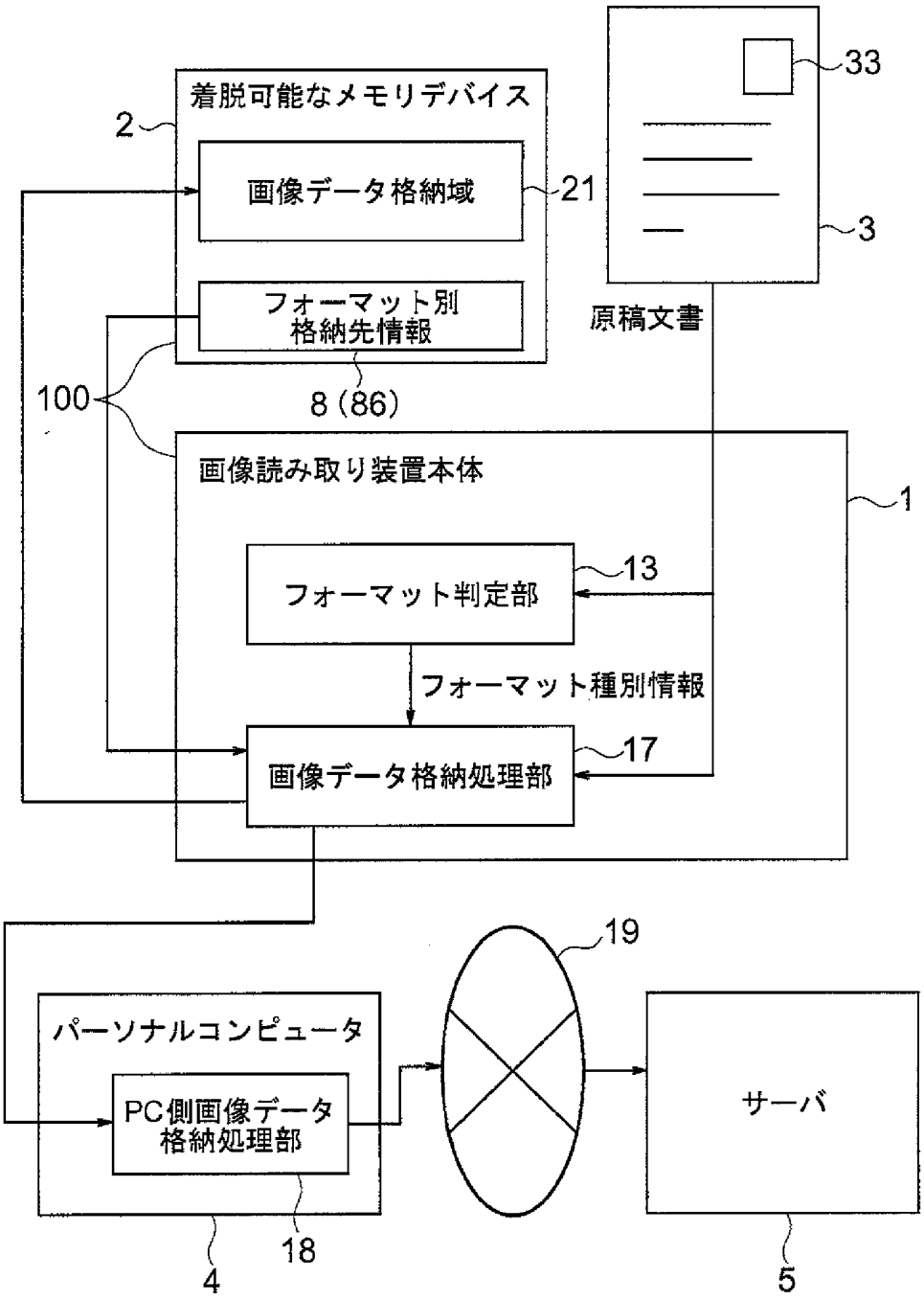
[図6]



[図7]


33
承認印
3
定型文書
着脱可能なメモリデバイス
2
電子署名用個人
原稿文書
100
8 (85)
画像読み取り装置本体
1
電子署名処理部
16
出力データ
15
画像データ
電子署名データ
155

[図8]


着脱可能なメモリデバイス
2
画像データ格納域
21
フォーマット別
格納先情報
8 (86)
33
3
原稿文書
100
画像読み取り装置本体
1
フォーマット判定部
13
フォーマット種別情報
画像データ格納処理部
17
19
パーソナルコンピュータ
PC側画像データ
格納処理部
18
4
サーバ
5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/006372

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04N1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04N1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 2001-320517 A (Fuji Xerox Co., Ltd.), 16 November, 2001 (16.11.01), Full text (Family: none)	1,2 3-7,10,11 8,9,12,13
Y	JP 2001-67322 A (Tsuneyoshi OCHIAI), 16 March, 2001 (16.03.01), Full text (Family: none)	3,4
Y	JP 11-345270 A (NTT Data Corp.), 14 December, 1999 (14.12.99), Par. Nos. [0064] to [0067]; Fig. 9 (Family: none)	5-7,10,11

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 August, 2004 (04.08.04)	17 August, 2004 (17.08.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／００６３７２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．ｃｌ⁷　Ｈ０４Ｎ１／００

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．ｃｌ⁷　Ｈ０４Ｎ１／００

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００４年
日本国実用新案登録公報	１９９６－２００４年
日本国登録実用新案公報	１９９４－２００４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	ＪＰ　２００１－３２０５１７　Ａ（富士ゼロックス株式会社）２００１．１１．１６、全文、（ファミリーなし）	1、2
Ｙ		3-7、10、11
Ａ		8、9、12、13
Ｙ	ＪＰ　２００１－６７３２２　Ａ（落合庸良）２００１．０３．１６、全文、（ファミリーなし）	3、4
Ｙ	ＪＰ　１１－３４５２７０　Ａ（株式会社エヌ・ティ・ティ・データ）１９９９．１２．１４、【００６４】－【００６７】、図９（ファミリーなし）	5-7、10、11

☐ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日　０４．０８．２００４	国際調査報告の発送日　17.8.2004
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｖ　８９３８ 千葉　輝久 電話番号　０３－３５８１－１１０１　内線　３５７１