(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
2008 年12 月4 日 (04.12.2008)

PCT

(10) 国際公開番号
WO 2008/146332 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *G09C 5/00* (2006.01)
G06F 21/24 (2006.01)

(21) 国際出願番号: PCT/JP2007/000581

(22) 国際出願日: 2007 年5 月30 日 (30.05.2007)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP). 阿南泰三 (ANAN, Taizo) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 倉木健介 (KURAKI, Kensuke) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP). 中潟昌平 (NAKAGATA, Shohei) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 大菅義之 (OSUGA, Yoshiyuki); 〒1020084 東京都千代田区二番町８番地２０ 二番町ビル３Ｆ 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, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN,

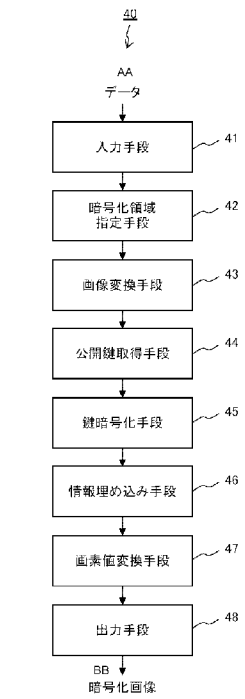
[続葉有]

WO 2008/146332 A1

(54) **Title:** IMAGE ENCRYPTING DEVICE, IMAGE DECRYPTING DEVICE, METHOD AND PROGRAM

(54) 発明の名称: 画像暗号化装置、画像復号装置、方法、及びプログラム

[図2]



AA DATA
41 INPUT MEANS
42 ENCRYPTED AREA DESIGNATION MEANS
43 IMAGE CONVERSION MEANS
44 PUBLIC KEY ACQUIREMENT MEANS
45 KEY ENCRYPTING MEANS
46 INFORMATION EMBEDDING MEANS
47 PIXEL VALUE CONVERSION MEANS
48 OUTPUT MEANS
BB ENCRYPTED IMAGE

(57) Abstract: An image encrypting device subjects an image of the designated area in an inputted image to conversion using an encoding key, embedding of information obtained by encrypting the encryption key using a public key paired with the secret key of a sending destination, and conversion of a pixel value one by one in this order to generate a final encrypted image. Then, the image encrypting device sends the encrypted image to the sending destination through a printed matter or a network. An image decrypting device converts the encrypted image of a form of printing data or electronic data to an image and inputs it. Then, the encrypted area in the encrypted image converted to image data is subjected to reverse processing as compared to the processing carried out by the image encrypting device so as to extract a decrypting key (the encrypting key) from the image of the encrypted area. Then, using the decrypting key, the image decrypting device decrypts the original image of the encrypted area to restore the whole encrypt image.

(57) 要約: 本発明の画像暗号化装置は、入力画像の指定された領域の画像に対して、暗号鍵による変換、その暗号鍵を送付先の秘密鍵と対になる公開鍵を用いて暗号化した情報の埋め込み、及び画素値変換を順に施し、最終的な暗号化画像を生成する。そして、該暗号化画像を印刷物またはネットワークを介して送付先に送る。本発明の画像復号装置は、印刷データまたは電子データの形式の前記暗号化画像を画像に変換して入力する。そして、その画像データに変換された暗号化画像の暗号化領域に対して、前記本発明の画像暗号化装置の処理と逆の処理を施して、該暗号化領域の画像から復号鍵（前記暗号鍵）を取り出す。そして、その復号鍵を用いて、該暗号化領域の原画像を復号し、前記暗号化画像全体を復元する。

KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, IS, IT, LT, LU, LV, MC, MT, 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

明　細　書

画像暗号化装置、画像復号装置、方法、及びプログラム

技術分野

[0001] 本発明は、個人情報などの重要な情報が視覚的に暗号化されている印刷物や電子データを、安全にやりとりするための技術に関する。

背景技術

[0002] 社会の情報化が進展するにつれ、秘密情報の漏洩が深刻な問題となっており、情報漏洩を防止する技術の重要性が増してきている。この情報漏洩技術に関しては、例えばデジタルデータにおいて、第三者が入手しても、その内容が分からないように、データを暗号化する技術が開発されている。この暗号化技術は、デジタルデータの情報漏洩を防ぐ有効な手段として既に利用されている。

[0003] 一方、紙媒体等に印刷された印刷物の情報漏洩を防止する技術は、まだ十分に確立されておらず、実用化された例もない。現代社会においては、情報漏洩の約半数が印刷物によるものだという統計もあり、印刷物についても、デジタルデータと同様に、情報漏洩を防ぐ技術の開発が急務となっている。

[0004] 情報漏洩対策が望まれる印刷物の具体例としては、商品購入時の請求書、クレジットカード等の明細書、病院のカルテ、学校の成績表、名簿などがある。ＰＣＴ出願のＪＰ／２００７／０００２１５（以後、特許文献１と呼ぶ）によれば、デジタル画像のみならず、紙に印刷された画像を、暗号化して、情報漏洩を防ぐことが可能である。ところで、紙に印刷された病院のカルテや明細書などは、一種の視覚情報として定義できる。したがって、本願の明細書（本明細書）では、それらを総称して“画像”と呼ぶことにする。

[0005] 特許文献１に開示されている画像暗号化の概要を説明する。

図１（Ａ）に示す入力画像１０について、その一部を暗号化領域１１として指定し、その暗号化領域１１の画像を暗号鍵を用いて暗号化する。この結果、図１（Ｂ）に示す暗号化画像２０が生成される。暗号化画像２０において

は、前記暗号化領域１１に該当する領域２１が暗号化されており、視覚的に判読不能になっている。

[0006] 上述した入力画像の暗号化においては、暗号化自体の処理はデジタルデータ処理により行なわれるので、暗号化画像はデジタルデータである。この暗号化画像は、その後、紙媒体等に印刷されてもよいし、デジタルデータのままやりとりされてもよい。特許文献１の発明の特徴は、一度印刷され、いわば、アナログデジタルデータに変換された暗号化画像を、再度復号可能なことである。

[0007] 特許文献１の発明では、画像の暗号化と復号に共通鍵（同一の鍵）を使用している。このため、暗号化した情報の送付先に、それとは別に、その暗号化情報を復号するための鍵を送る必要がある。このため、その復号鍵を第三者に盗まれる可能性があり、安全性の面で問題があった。

[0008] ところで、強力な認証サーバを構築し、その認証サーバを用いて共通鍵を安全にやりとりする電子認証システムが、既に、実用化されているが、このような認証サーバを用いる方式は、一般に普及している個人ユーザ用途の簡易な認証システムとは構成が大きく異なるので、特許文献１の発明の技術を享受できるユーザは制限されることになる。

特許文献1：ＰＣＴ／ＪＰ２００７／０００２１５

発明の開示

[0009] 本発明の目的は、既存の鍵管理システムを変更せずに、暗号化技術により作成された暗号化画像の復号に用いられる共通鍵を、誰でも容易に安全にやりとりできるようにすることである。

[0010] 本発明の画像暗号化装置は、画像を暗号化する画像暗号化装置を前提とする。

本発明の画像暗号化装置の第１態様は、入力手段、暗号化領域指定手段、画像変換手段、公開鍵取得手段、鍵暗号化手段、情報埋め込み手段、画素値変換手段及び出力手段を備える。

[0011] 前記入力手段は、暗号化の対象となる画像データを入力する。前記暗号化

領域指定手段は、該入力手段によって生成された画像について、暗号化の対象となる領域を指定する。画像変換手段は、該暗号化領域指定手段によって指定された暗号化領域を、暗号鍵を用いて、第１の画像に変換する。公開鍵取得手段は、前記暗号化対象のデータの送付先の公開鍵を取得する。鍵暗号化手段は、該公開鍵取得手段によって取得された公開鍵を用いて、前記暗号鍵を暗号化する。情報埋め込み手段は、該鍵暗号化手段によって暗号化された暗号鍵に関する情報である暗号鍵関連情報を、前記第１の画像内に埋め込み、前記暗号化領域を第２の画像に変換する。画素値変換手段は、前記暗号化領域指定手段によって指定された領域を特定可能となるように、前記第２の画像の画素値を変換し、前記暗号化領域を第３の画像に変換する。出力手段は、前記入力手段によって入力された画像において前記暗号化領域の画像が前記第３の画像に変換された暗号化画像を、所定の方式で出力する。

[0012] 本発明の画像暗号化装置の第１態様によれば、暗号鍵に関する情報である暗号鍵関連情報が画像に埋め込まれた、暗号化領域のデータ（情報）の暗号化画像を生成・出力するので、その暗号化画像の送信元と受信先との間で、その暗号化画像を復元するために必要となる復号鍵の安全な授受が可能となる。また、前記暗号鍵関連情報は、暗号化画像の受信先の公開鍵によって暗号化された暗号鍵に関する情報であるため、前記暗号鍵関連情報から前記復号鍵（前記暗号鍵に等しい）を取り出せるのは、前記公開鍵と対になる秘密鍵の保有者である暗号化画像の受信者だけである。したがって、該暗号化画像を第３者が入手しても、その復元は不可能であり、画像暗号化された情報の内容が第３者に漏洩することはない。

[0013] 本発明の画像暗号化装置の第２態様は、上記本発明の画像暗号化装置の第１態様を前提とし、前記暗号化領域指定手段は複数の暗号化領域を指定する。また、前記画像変換手段は、前記複数の暗号化領域の各領域の画像を、複数の暗号鍵を用いて個別に変換する。また、前記公開鍵取得手段は、複数の公開鍵を取得する。前記鍵暗号化手段は、前記画像変換手段が各暗号化領域の画像を変換するために用いた各暗号鍵を、前記公開鍵取得手段によって取

得された複数の公開鍵を用いて個別に暗号化する。

[0014] 本発明の画像暗号化装置の第２態様によれば、例えば、１つの文書について、複数の情報を画像暗号化することが可能となる。したがって、暗号化したい情報が散在している文書の暗号化に有効である。

[0015] 本発明の画像暗号化装置の第３態様は、上記本発明の第２態様の画像暗号化装置を前提とし、前記画像変換手段は、各暗号化領域の画像を、それぞれ、別個の暗号鍵を用いて変換する。

[0016] 本発明の画像暗号化装置の第３態様によれば、各暗号化領域、すなわち、各情報の画像を個別の暗号鍵を用いて暗号化するので、安全性の強度が高まる。

本発明の画像暗号化装置の第４態様は、上記画像暗号化装置の第２または第３の画像暗号化装置を前提とし、前記公開鍵取得手段が取得する複数の公開鍵は、複数の送付先の公開鍵である。

[0017] 本発明の画像暗号化装置の第５態様は、上記画像暗号化装置の第２乃至第４のいずれか１態様の画像暗号化装置を前提とし、前記公開鍵取得手段は、前記複数の暗号化領域と同数の公開鍵を取得する。

[0018] 本発明の画像暗号化装置の第６態様は、上記画像暗号化装置の第１または第２態様の画像暗号化装置を前提とし、前記出力手段は、前記暗号化画像を、前記送付先の公開鍵で暗号化してから出力する。

[0019] 本発明の画像暗号化装置の第７態様は、上記画像暗号化装置の第１または第２態様の画像暗号化装置を前提とし、前記鍵暗号化手段は、前記暗号鍵を、前記公開鍵と、前記送付先が前記暗号化画像を提出する相手の秘密鍵とを用いて暗号化する。

[0020] 本発明の画像暗号化装置の第８態様は、上記画像暗号化装置の第１または第２態様の画像暗号化装置を前提とし、前記入力手段は、前記暗号鍵を入力する。

本発明の画像暗号化装置の第９態様は、上記画像暗号化装置の第１乃至第８態様のいずれか１態様の画像暗号化装置を前提とし、前記公開鍵取得手段

は、前記公開鍵を、それを管理している公開鍵管理サーバから取得する。

[0021] 本発明の画像暗号化装置の第１乃至第９態様のいずれか１態様において、前記出力手段は、前記暗号化画像を印刷出力するような構成にしてもよい。または、前記出力手段は、前記暗号化画像を他のフォーマットに変換して出力するような構成にしてもよい。または、前記出力手段は、前記暗号化画像がネットワークを介して送信するような構成にしてもよい。このネットワーク送信において、前記暗号化画像を、例えば、電子メールにより送信するようにしてもよい。

[0022] 本発明の画像復号装置は、暗号化された画像を含む暗号化画像を原画像に復号する画像復号装置を前提とする。

本発明の画像復号装置の第１態様は、入力手段、暗号化位置検知手段、画素値変換手段、情報抽出手段と、該情報抽出手段、鍵復号化手段及び画像変換手段を備える。

[0023] 入力手段は、前記暗号化画像を、画像データとして入力する。暗号化位置検知手段は、該入力手段が入力した前記暗号化画像を解析して、前記暗号化画像における画像が暗号化された領域である暗号化領域の位置を検知する。画素値変換手段は、該暗号化位置検知手段により検知された前記暗号化領域の位置情報に基づいて前記暗号化領域の位置を特定するために、前記暗号化領域の画像の画素値を変換前の画素値に戻す。情報抽出手段は、該画素値変換手段により生成された前記暗号化領域の画像から、それに埋め込まれている暗号鍵に関する情報である暗号鍵関連情報を抽出する。鍵復号化手段は、該情報抽出手段によって抽出された前記暗号鍵関連情報の生成に用いられた第1の公開鍵と対になる第1の秘密鍵を用いて、前記暗号鍵関連情報から、前記暗号化領域の画像を復号するために用いる復号鍵を復号する。画像変換手段は、該鍵復号化手段によって復号された復号鍵を用いて前記暗号化領域の画像を復号して、前記原画像を復号する。

[0024] 本発明の画像復号装置の第１態様によれば、暗号化画像から、暗号化領域の画像を復号するたけに必要な復号鍵を抽出し、該暗号化画像を元の画像に

復元できる。

本発明の画像復号装置の第２態様は、上記画像復号装置の第１態様を前提とし、前記第１の秘密鍵は前記暗号化画像の送付先が保有する秘密鍵であり、前記第１の秘密鍵は前記送付先が前記暗号化画像を提出する相手が前記暗号化画像を復号するために使用する第２の公開鍵と対になる秘密鍵である。

[0025] 本発明の画像復号装置の第２態様によれば、送付先が保有する秘密鍵で暗号化された暗号化画像を元の画像に復元することができる。

本発明の画像復号装置の第３態様は、上記画像復号装置の第１または第２態様を前提とし、前記暗号鍵関連情報が前記第1の公開鍵と第２の秘密鍵によって暗号化されている場合に、前記第２の秘密鍵と対になる第２の公開鍵を取得する公開鍵を取得する公開鍵取得手段を、さらに備える。そして、前記鍵暗号化手段は、前記暗号鍵関連情報から、前記第１の秘密鍵と前記第２の公開鍵を用いて、前記復号鍵を復号する。

[0026] 本発明の画像復号装置の第３態様によれば、暗号化領域の画像を暗号化するために用いられた暗号鍵を、第１の公開鍵と第２の秘密鍵を用いて暗号化することによって得られた暗号鍵関連情報を暗号化画像から抽出し、その暗号鍵関連情報から前記暗号鍵（復号鍵に等しい）を取り出すことができる。そして、その復号鍵を用いて、暗号化画像を元の画像に復元できる。

[0027] 本発明の画像復号装置の第４態様は、上記画像復号装置の第１第または第２態様の画像復号装置を前提とし、前記暗号化領域は複数である。

本発明の画像復号装置の第４実施形態によれば、複数の暗号化領域を有する暗号化画像を元の画像に復元できる。

[0028] 本発明の画像復号装置の第５態様は、上記画像復号装置の第４態様を前提とし、各暗号化領域の画像に含まれる各暗号鍵関連情報は個別の暗号鍵に関する情報である。前記情報抽出手段は、前記各暗号化領域から個別の暗号鍵関連情報を抽出する。また、前記鍵復号化手段は、前記情報抽出手段により抽出された各暗号鍵関連情報から、それぞれの暗号鍵関連情報の生成に用いられた秘密鍵と対になる公開鍵を用いて、前記各暗号鍵関連情報が埋め込ま

れていた各暗号化領域の画像を復号するために用いる各復号鍵を復号する。

[0029] 本発明の画像復号装置の第５態様によれば、複数の暗号化領域が個別の暗号鍵で暗号化されている暗号化画像を元の画像に復元できる。

本発明の画像復号装置の第６態様は、上記画像復号装置の第５態様を前提とし、前記各暗号鍵関連情報は、別個の秘密鍵によって生成されている。

[0030] 本発明の画像復号装置の第６態様によれば、暗号化画像に埋め込まれている暗号鍵関連情報が個別の秘密鍵によって生成されている暗号化画像を元の画像に復元できる。

本発明の画像復号装置の第７態様は、上記画像復号装置の第１乃至第５態様のいずれか１態様の画像復号装置を前提とし、前記公開鍵取得手段は、前記公開鍵を、それを管理している公開鍵管理サーバから取得する。

[0031] 上記画像復号装置の第１乃至第７態様のいずれか１態様の画像復号装置において、前記暗号化画像は、例えば、印刷物に印刷された画像や所定のフォーマットの画像などである。また、さらに、前記暗号化画像を、ネットワークを介して受信するように構成してもよい。このネットワーク受信において、前記暗号化画像は、例えば、電子メールにより受信する。

[0032] 上記構成の画像復号装置において、前記暗号化画像は、前記画像暗号化装置によって生成された画像であってもよい。

本発明によれば、暗号化画像の暗号化と復号に用いられる共通鍵（暗号鍵と復号鍵）を、暗号化画像に埋め込んでやりとりすることができる。したがって、個人情報などの高い秘匿性が要求される重要情報を画像暗号化して、該重要情報を暗号化画像によりやりとりする際、一般に普及している認証サーバなどを備える認証システムを導入しなくても、共通鍵を、暗号化画像により安全にやりとりすることが可能となる。この場合、暗号化画像を紙媒体に印刷し、印刷物により、重要情報と共通鍵の両方を、第3者に盗聴されることなく、高度な安全性を確保してやりとりすることも可能である。また、さらに、共通鍵を送付先の公開鍵で暗号化し、その暗号化により得られた暗号鍵関連情報を暗号化画像に埋め込むことにより、暗号化と本人認証の仕組み

を、紙媒体にまで拡張することが可能となる。もちろん、本発明は、該暗号鍵関連情報を埋め込んだ暗号化画像を、電子データの形態で、ネットワークや記録媒体などを介してやりとりすることも可能である。

図面の簡単な説明

[0033] [図1]画像暗号化の一例を示す図である。

[図2]本発明の画像暗号化装置の基本構成を示す図である。

[図3]本発明の画像復号装置の基本構成を示す図である。

[図4]本発明を適用した応用システムの第1の実施形態の構成を示す図である。

[図5]本発明を適用した応用システムの第２の実施形態の構成と手法を示す図（その１）である。

[図6]本発明を適用した応用システムの第２の実施形態の構成と手法を示す図（その２）である。

[図7]本発明を適用した応用システムの第２の実施形態構成と手法を示す図（その３）である。

[図8]本発明を適用した応用システムの第２の実施形態の構成と手法を示す図（その４）である。

[図9]本発明を適用した応用システムの第３の実施形態の構成と手法示す図である。

[図10]本発明の暗号化装置として機能するパーソナルコンピュータのハードウェア構成とソフトウェア構成を示す図である。

[図11]図１０に示すパーソナルコンピュータのＣＰＵが、プログラム用メモリ領域に格納されているプログラムを実行することによって行なう画像暗号化処理を示すフローチャートである。

[図12]暗号化するデータ（暗号化データ）の一例を示す図である。

[図13]図１２の暗号化データの暗号化領域の指定方法を示す図である。

[図14]図１３の暗号化領域の画像変換後の状態を示す図である。

[図15]図１４に示す暗号化領域の画像に暗号鍵関連情報を埋め込む処理を行

なった後の、暗号化領域の画像状態を示す図である。

[図16]図１４に示す暗号化領域の画像に画素値変換処理を行なった後の、暗号化領域の画像状態を示す図である。

[図17]本発明の画像復号装置として機能するパーソナルコンピュータのハードウェア構成とソフトウェア構成を示す図である。

[図18]図１７の画像復号装置として機能するパーソナルコンピュータの処理手順を示すフローチャートである。

発明を実施するための最良の形態

[0034] 以下、図面を参照しながら本発明の実施形態について説明する。

まず、本発明の画像暗号化装置の基本構成について説明する。

{本発明の画素暗号化装置の基本構成}

図２は、本発明の画像暗号化装置の基本構成を示す図である。

[0035] 本発明の画像暗号化装置４０は、入力手段４１、暗号化領域指定手段４２、画像変換手段４３、公開鍵取得手段４４、鍵暗号化手段４５、情報埋め込み手段４６、画素値変換手段４７及び出力手段４８を備える。

[0036] 入力手段４１は、暗号化の対象となるデータを入力し、それを画像（以後、入力画像と呼ぶ）に変換する。該入力画像は、例えば、ビットマップ形式の画像である。入力手段４１に入力されるデータは、例えば、ワードプロセッサのソフトウェア（ソフト）で作成される文書データ、PDF(Portabale Document Format)形式のデータ、もしくはＨＴＭＬ(Hyper Text Transfet Protocol)形式のデータなどである。入力手段４１は、これらのデータの一部または全部を、ビットマップ形式などの画像（画像データ）に変換する。尚、入力手段４１に入力されるデータは、スキャナなどによって読み取られた印刷物の画像データであってもよい。

[0037] 入力手段４１は、さらに、上記画像の一部を暗号化するために用いる暗号鍵を入力する。この暗号鍵は、例えば、ＧＵＩ(Graphical User Interface)を介して入力されるパスワード、ＩＤカードに格納された鍵、または、指紋や静脈、虹彩などの生体認証装置が認証する際に使用する生体情報であって

もよい。

[0038] 暗号化領域指定手段４２は、入力手段４１から出力される画像の一部、すなわち、該画像において暗号化したい領域を指定する。この暗号化領域の指定は、例えば、ＧＵＩを介して行なわれる。また、前記画像が固定フォーマットのデータであるならば、暗号化領域は、予め、座標情報などによって指定するようにしてもよい。指定される暗号化領域は、１つに限定されるものではなく、複数であってもかまわない。

[0039] 画像変換手段４３は、入力手段４１から出力された画像の暗号化領域指定手段４２によって指定された領域（暗号化領域）を、入力手段４１を介して入力された暗号鍵を用いて暗号化する。この暗号化は、例えば、前記特許文献１の発明に開示されている手法により行なわれる。この暗号化によって、前記入力画像の暗号化領域は元の画像の内容が認識できないようになる。

[0040] 公開鍵取得手段４４は、公開鍵を保有している既存のサーバから、ネットワーク経由などにより、前記暗号化された入力画像（以後、暗号化画像と呼ぶ）の送付先の公開鍵を取得する。

[0041] 鍵暗号化手段４５は、公開鍵取得手段４４によって取得された公開鍵を用いて、入力手段４１に入力された暗号鍵を暗号化する。このようにして、公開鍵によって暗号化された暗号鍵は、送付先の秘密鍵を用いないと復号できない。したがって、この公開鍵によって暗号化された暗号鍵を、第三者が盗聴したとしても、暗号鍵を復号できないので、前記暗号化画像に公開鍵によって暗号化された暗号鍵を埋め込んで送っても、前記暗号化画像内の暗号化領域の画像を判読することは不可能である。

[0042] 情報埋め込み手段４６は、鍵暗号化手段４５によって暗号化された暗号鍵を画像情報として、画素値変換手段４３によって生成された暗号化画像の中に埋め込む。

画素値変換手段４７は、例えば、前記特許文献１の発明の手法により、画像の横方向と縦方向について、一定の周期で画素値を変換し、概ね縞状模様の画像を生成する。

[0043] 出力手段４８は、画素値変換手段４７によって生成された画像（便宜上、最終的暗号化画像と呼ぶ）を印刷装置、画像表示装置、もしくはネットワークに出力するか、記憶装置等に保存する。この保存においては、最終的暗号化画像のままではなく、PostScriptデータやＰＤＦ形式のファイルなどの他の形式に変換して保存するようにしてもよい。

｛本発明の画像復号装置の基本構成｝

図３は、本発明の画像復号装置の基本構成を示す図である。

[0044] 本発明の画像復号装置５０は、入力手段５１、暗号化位置検知手段５２、画素値変換手段５３、情報抽出手段５４、公開鍵取得手段５５、鍵復号化手段５６、画像変換手段５７及び出力手段５８を備える。但し、公開鍵取得手段５５は、必須ではない。公開鍵取得手段５５は、復号する暗号化画像に埋め込まれた暗号鍵関連情報が、暗号化画像を生成した側の公開鍵と、該暗号化画像を復号する側の秘密鍵を用いて生成されている場合にのみ必要となる。この場合、公開鍵取得手段５５は、該秘密鍵と対になる公開鍵を取得する。

[0045] 本発明の画像暗号化装置５０は、上述した画像暗号化装置４０によって生成された前記最終的暗号化画像を元の画像（入力手段４１に入力される画像）に復元する。

入力手段５１は、画像暗号化装置４０により生成された最終的暗号化画像を入力する。

[0046] 尚、入力手段５１に入力される最終的暗号化画像は画像暗号化装置４０によって暗号化後に印刷された印刷物の画像データを、スキャナなどによって読み取った最終的暗号画像であってもよい。

[0047] 暗号化位置検知手段５２は、該最終的暗号化画像内の暗号化領域の位置を検出する。該最終的暗号化画像が前記特許文献１の発明に手法を用いて生成されたものであるならば、該暗号化領域内の境界線の位置も検出する。この検出は、前記特許文献１の発明の手法により行なう。

[0048] 画素値変換手段５３は、画像暗号化装置４０の画素値変換手段４７が行な

った画素値変換処理と逆の変換処理を行い、暗号化位置検知手段５２によって検出された暗号化領域の画素値を解除する（元の画素値を復元する）。

[0049] 情報抽出手段５４は、画素値変換手段４７によって得られた復元画像に対して、画像暗号化装置４０の情報埋め込み手段４６が行なった処理と逆の処理を行い、該復元画像から前記公開鍵で暗号化された暗号鍵の情報（便宜上、暗号鍵情報と呼ぶ）を抽出する。

[0050] 公開鍵取得手段５５は、必要に応じて公開鍵を取得する。この公開鍵の取得は、例えば、画像暗号化装置４０の公開鍵取得手段４４と同様にして、その公開鍵を管理しているサーバから取得する。この公開鍵は、入力手段５１に入力した最終的暗号化画像を生成したユーザが、暗号鍵を暗号化して暗号鍵情報を生成するために使用したものである。

[0051] 鍵復号化手段５６は、情報抽出手段５４によって抽出された暗号鍵情報から、画像暗号化装置４０の鍵暗号化手段４５が暗号鍵を暗号化するために用いた公開鍵と対になる秘密鍵を用いて、暗号鍵を復号・抽出する。

[0052] 画像変換手段５７は、鍵復号化手段５６によって抽出された暗号鍵を用いて、画像暗号化装置４０が暗号化した、入力画像の暗号化領域の画像を復元し、該入力画像全体を復元する。

[0053] 出力手段５８は、画像変換手段５７が復元した入力画像を印刷装置、画像表示装置等に出力する。

この出力により、画像暗号化装置４０により暗号化された入力画像の暗号化領域の画像を認識することが可能になる。

[0054] 画像暗号化装置４０によって生成された最終的暗号化画像から、入力画像の暗号化領域の画像を復元することは、該最終的暗号化画像に埋め込まれた暗号鍵情報の生成に用いられた公開鍵と対になる秘密鍵を保有しているユーザだけが可能である。

[0055] このため、その暗号鍵情報が埋め込まれた入力画像の印刷物や電子データのみを送付先に送るだけで、送付先は、その公開鍵と対になる秘密鍵を用いて、その入力画像の暗号化領域の画像を復元し、その暗号化領域の画像であ

る重要情報を知ることができる。

[0056] 以上のようにして、本発明の画像暗号化装置４０と画像復号装置５０を利用することで、入力画像内の第三者には秘匿にしておきたい重要情報の暗号化に用いる暗号鍵（共通鍵）を公開鍵暗号方式の枠組みで安全に暗号化し、該暗号鍵を入力画像以外の手段でやりとりすることなく、入力画像内の重要情報を、正当な送信者と受信者との間で、安全にやりとりすることが可能となる。

[0057] 次に、本発明の画像暗号化装置と画像復号装置を適用した応用システム（以後、単に応用システムと呼ぶ）の実施形態について説明する。

{応用システムの第１の実施形態}

本発明の応用システムの第１の実施形態は、本発明を印刷物を媒体とした重要情報のやり取りに適用したシステムである。図4は、本発明の第1の実施形態のシステム構成を示す図である。

[0058] 図４を参照しながら、上記第1の実施形態のシステムの構成と動作を説明する。

本実施形態では、Ａさんが、本発明の画像暗号化装置を利用して、以下の（ａ）～（ｇ）の処理を行なう。

（ａ）Ａさんが、図４（ａ）に示す資料（文書）６０を印刷して、その印刷物を郵送によりＢさんに送るものとする。この資料６０には、第三者には見られたくない個人情報リスト６１が含まれているものとする。

（ｂ）この場合、Ａさんは、まず、パーソナルコンピュータ（ＰＣ）に接続されたスキャナなどの入力手段４１により、資料６０を画像として読み取り、パーソナルコンピュータ内部のメモリに取り込む。そして、その画像をパーソナルコンピュータ（ＰＣ）のディスプレイに表示する。Ａさんは、マウスなどの暗号化領域指定手段４２により、ディスプレイの画面上で個人情報リスト６１の画像部分を「暗号化領域」として指定する。そして、画像変換手段４３により、暗号化領域として指定した個人情報リスト６１の画像６１ａ（以後、個人情報リスト画像６１ａと呼ぶ）を、暗号鍵８１を用いて暗号

化する。この暗号化は、例えば、前記特許文献１の発明に開示されている手法により行なわれる。この暗号化により、個人情報リスト画像６１ａは画像変換画像６１ｂに変換される。

（ｃ）Ａさんは、公開鍵取得手段４４により、公開鍵管理サーバ９０からＢさんの公開鍵８２を取得する。

（ｄ）Ａさんは、鍵暗号化手段４５により、暗号鍵８１をＢさんの公開鍵８２を用いて暗号化する。この暗号化によって生成された暗号化データを、便宜上、暗号鍵関連情報８３と呼ぶことにする。

（ｅ）Ａさんは、情報埋め込み手段４６により、前記暗号鍵関連情報８３を画像変換画像６１ｂの暗号化領域に埋め込み、情報埋め込み画像６１ｃを生成する。

（ｆ）Ａさんは、画素値変換手段４７により、情報埋め込み画像６１ｃに対して、画素値変換処理を施し、画素値変換画像６１ｄを生成する。この画素値変換処理は、例えば、情報埋め込み画像６１ｃを市松模様化する処理である。

（ｇ）Ａさんは、個人情報リスト画像６１ａの部分が画素値変換画像６１ｄに変換された資料をプリンタ９１により紙に印刷する。そして、プリンタ９１から印刷出力された印刷物（印刷媒体）をＢさんに郵送する。

Ｂさんは、本発明の画像復号装置を利用して、以下の（ｈ）～（ｌ）の処理を行なう。

（ｈ）Ｂさんは、Ａさんが郵送した印刷物を受け取ると、その印刷物の印刷情報を入力手段５１であるスキャナ９３により画像として取り込む。この画像は、Ａさんが作成した画素値変換画像６１ｄにほぼ等しいので、便宜上、この画像を画素値変換画像６１ｄと呼ぶことにする。

（ｉ）Ｂさんは、画素値変換手段５３により、画素値変換画像６１ｄに施された画素値変換処理（この例では、市松模様化）を解除し、画素値変換画像６１ｄから情報埋め込み画像６１ｃを復元する。

（ｊ）Ｂさんは、情報抽出手段５４により、情報埋め込み画像６１ｃから暗

号鍵関連情報８３を抽出する。そして、Ｂさんの秘密鍵８４を用いて、暗号鍵関連情報８３から暗号鍵８１を復号する。この暗号鍵８１を抽出する過程で、情報埋め込み画像６１ｃから画像変換画像６１ｂが復元される。

（ｋ）Ｂさんは、画像変換手段５７により、暗号鍵８１を用いて、画像変換画像６１ｂのスクランブルを解除する。

（ｌ）上記スクランブル解除により、画像変換画像６１ｂから個人情報リスト画像６１ａを復元される。

[0059] 上記（ｉ）～（ｌ）の処理は、例えば、Ｂさんが保有するパーソナルコンピュータで行なわれ、復元された個人情報リスト画像６１ａは、Ｂさんのパーソナルコンピュータのディスプレイに表示される。

[0060] 以上のようにして、Ｂさんは、Ａさんが郵送した印刷物から、画像暗号化された個人情報リストを復元することができる。

第1の実施形態のシステムでは、ＡさんがＢさんに送る資料の個人情報リストは、暗号鍵８１で画像暗号化されており、暗号鍵８１は公開鍵８２で暗号化され、暗号鍵関連情報８３として情報埋め込み画像６１ｃに埋め込まれる。したがって、Ａさんが、画素値変換画像６１ｄの印刷物をＢさんに郵送した際、その郵送途中で、印刷物が第三者の手に入ったとしても、その第三者は、個人情報リストを復号することは困難であり、個人情報リストの内容を知ることはできない。

[0061] {応用システムの第２の実施形態}

上述した第1の実施形態は、本発明を印刷物の画像暗号化に適用した例であった。第１の実施形態では、資料の画像の一つの領域のみを暗号化するようにしていた。

[0062] 本発明の画像暗号化装置と画像復号装置を適用した応用システムの第２の実施形態は、画像上の複数の領域を暗号化するものである。この暗号化において、各領域の画像は個別の暗号鍵で暗号化する。そして、各領域の暗号化に用いられた暗号鍵を、それぞれ別個の公開鍵で暗号化し、この暗号化により得られた暗号鍵関連情報を、上記各領域が暗号化された画像内に埋め込む

。

[0063] 図５～図８は、本発明の応用システムの第２の実施形態の構成と手法を示す図である。

第２の実施形態は、本発明を病院のカルテの画像暗号化に適用したシステムである。本実施形態が適用されるシステムでは、Ａ病院が患者のカルテを管理しており、Ａ病院の患者は、Ｗｅｂ(World Wide Web)を利用して自分のカルテを閲覧することが許可されているものとする。したがって、Ａ病院の患者は、インターネットブラウザを利用して、Ａ病院に保管されている自分のカルテをパーソナルコンピュータ等にダウンロードすることが可能である。ここで、Ａ病院は、患者がセカンドオピニオンとして選んだ他の病院（ここでは、Ｂ病院とする）の医師に、Ａ病院のカルテを提出することを許可したいと考えているものとする。しかも、カルテの提出は紙でも可能にしたいと考えているものとする。但し、Ａ病院のカルテには、患者自身には見せたくないが、Ｂ病院の医師には見せる必要がある情報が含まれているものとする。ここで、Ａ病院のカルテは、個人情報保護の観点から、情報漏洩の防止は必須となる。

[0064] 以上のような条件を前提とした本実施形態のシステムについて、図5～図８を参照しながら説明する。

＜Ａ病院の処理＞

まず、図５から説明する。図５は、Ａ病院側の処理手順を示す図である。Ａ病院は、本発明の画像暗号化装置を利用して、以下の（ａ）～（ｇ）の処理を行なう。

（ａ）Ａ病院は、患者のカルテを画像化し、カルテの原画像１００（以後、カルテ原画像１００と呼ぶ）を生成する。カルテ原画像１００には、患者の個人情報の画像１０１（以後、患者個人情報画像１０１と呼ぶ）と患者の診断結果などを含む病院情報の画像１０２（以後、病院情報画像１０２と呼ぶ）が含まれている。このカルテ原画像１００は、入力手段４１により生成される。

（ｂ）Ａ病院は、公開鍵管理サーバ１９０から、患者の公開鍵１３４（第１の公開鍵）とＢ病院の公開鍵１３５（第２の公開鍵）を入手（取得）する。この公開鍵の入手は、公開鍵取得手段４４により行なわれる。

（ｃ）カルテ原画像１００において、（患者に見せてもよい）患者個人情報画像１０１については暗号鍵（共通鍵）１３１（第１の暗号鍵）で暗号化し、（患者には見せたくないが、Ｂ病院の医師には見せる必要がある）病院情報画像１０２については暗号鍵（共通鍵）１３２（第２の暗号鍵）で暗号化する。これにより、カルテ原画像１００について、患者個人情報画像１０１と病院情報画像１０２の２つの部分画像を暗号化した画像である画像変換画像１００ａが生成される。この画像変換画像１００ａの生成は、画像変換手段４３により行なう。ここで、画像変換画像１００ａ内における、暗号化された患者個人情報画像１０１と暗号化された病院情報画像１０２を、それぞれ、患者個人情報暗号化画像１０１ａ、病院情報暗号化画像１０２ａと呼ぶことにする。この画像変換画像１００ａは、画像変換手段４３により生成される。

（ｄ）暗号鍵１３１は患者に見せてもよいので患者の公開鍵１３３で暗号化し、暗号鍵１３２は患者に見せたくないのでＢ病院の公開鍵１３５で暗号化する。これらの暗号化は、鍵暗号化手段４５により行なわれる。

（ｅ）患者の公開鍵１３３で暗号化した暗号鍵１３１に関する情報（第１の暗号鍵関連情報１４１）とＢ病院の公開鍵１３５で暗号化した暗号鍵１３２に関する情報（第２の暗号鍵関連情報１４２）を、それぞれ、画像変換画像１００ａの患者個人情報暗号化画像１０１ａと病院情報暗号化画像１０２ａに埋め込み、情報埋め込み画像１００ｂを生成する。ここで、第１の暗号鍵関連情報１４１が埋め込まれた患者個人情報暗号化画像１０１ａと第２の暗号鍵関連情報１４２が埋め込まれた病院情報暗号化画像１０２ａを、それぞれ、患者個人情報埋め込み画像１０１ｂ、病院情報埋め込み画像１０２ｂと呼ぶことにする。

この情報埋め込み画像１００ｂの生成は、情報埋め込み手段４６により行な

われる。

（ｆ）情報埋め込み画像１００ｂについて、患者個人情報埋め込み画像１０１ｂと病院情報埋め込み画像１０２ｂを市松模様化する画素値変換処理を施し、画素値変換画像１００ｃを生成する。ここで、画素値変換画像１００ｃにおける市松模様化された患者個人情報埋め込み画像１０１ｂと病院情報埋め込み画像１０２ｂを、それぞれ、患者個人情報画素値変換画像１０１ｃ、病院情報画素値変換画像１０２ｃと呼ぶことにする。この画素値変換画像１００ｃの生成は、画素値変換手段４７により行なわれる。

（ｇ）画素値変換画像１００ｃをプリンタなどにより紙などの印刷媒体に印刷し、その印刷媒体を郵送等により患者及びＢ病院に送付するか、または、画素値変換画像１００ｃを電子メールにより患者及びＢ病院に送信する。

[0065] 以上のようにして、Ａ病院は、患者のみ復号できる暗号化領域とＢ病院のみ復号できる暗号化領域を含むカルテの画像（以後、カルテの暗号化画像と呼ぶ）を生成し、それを、患者とＢ病院に送付することができる。

[0066] ＜患者のカルテ復号処理＞

次に、Ａ病院から画素値変換画像１００ｃを受け取ったＡ病院の患者の処理を、図６を参照しながら説明する。図６は、該患者が、Ａ病院から受け取った画素値変換画像１００ｃから、患者個人情報画像１０１を復号する処理手順を示す図である。

[0067] Ａ病院の患者（以下、単に患者と呼ぶ）は、本発明の画像復号装置を利用して、以下の（ａ）～（ｇ）の処理を行なう。

（ａ）Ａ病院から「カルテの暗号化画像」が印刷された印刷媒体を受け取った患者は、その印刷媒体に印刷された情報を画像に変換する。この変換により、Ａ病院で作成した画素値変換画像１００ｃが得られる。この印刷情報から画像への変換は、入力手段５１によって行なわれる。一方、患者は、Ａ病院から「カルテの暗号化画像」を電子メールにより受け取った場合には、その電子メールに添付された「カルテの暗号化画像」を開くことで、画素値変換画像１００ｃを取得する。この取得は、入力手段５１により行なわれる。

（ｂ）画素値変換画像１００ｃ内の患者個人情報画素値変換画像１０１ｃに施された画素値変換（市松模様化）を解除する。これにより、患者個人情報画素値変換画像１０１ｃから患者個人情報埋め込み画像１０１ｂが復元される。この患者個人情報画素値変換画像１０１ｃの画素値変換の解除は、画素値変換手段５３により行なわれる。このようにして、患者個人情報埋め込み画像１０１ｂと病院情報画素値変換画像１０２ｃを含む画像１１０ａが得られる。

（ｃ）上記画像１１０ａの患者個人情報埋め込み画像１０１ｂから、患者の公開鍵１３３で暗号化された暗号鍵１３１に関する情報１４１（第１の暗号鍵関連情報１４１）を抽出する。この抽出は、情報抽出手段５４により行なわれる。この抽出により、患者個人情報埋め込み画像１０１ｂは患者個人情報暗号化画像１０１ａに変換される。

（ｄ）患者の秘密鍵１３４を用いて、第１の暗号鍵関連情報１４１から暗号鍵１３１を取り出す。この取り出しは、鍵復号化手段５６によって行なわれる。

（ｅ）暗号鍵１３１を用いて、患者個人情報暗号化画像１０１ａからカルテ上の個人情報１０１の画像を復号する。この復号は、画像変換手段５７によって行なわれる。

（ｇ）患者は、（ｅ）によって得られた画像１１０ｃを見ることによって、Ａ病院から許可されている患者の個人情報を閲覧する。

[0068] 以上のようにして、患者は、Ａ病院から送付された画素値変換画像１００ｃから、自分の秘密鍵１３４を用いて、自身の個人情報１０１を知ることができる。この場合、患者はＢ病院の秘密鍵１３６を所持していないので、画素値変換画像１００ｃから患者に閲覧が許されていない秘匿情報を復号して、それを見ることはできない。

[0069] ＜患者の病院へのカルテ送付処理＞

次に、患者が、上述したようにして、Ａ病院から受け取った、一部の情報が暗号化されたカルテ（画素値変換画像１００ｃ）の閲覧を終了した後、セ

カンドオピニオンの医師がいるＢ病院に、そのカルテを送付する処理について、図７を参照しながら説明する。この場合、患者は、図６（ｆ）に示す個人情報１０１が暗号化されていない画像１１０ｃ（以後、患者閲覧画像１１０ｃと呼ぶ）について、個人情報１０１を、再度、暗号化してから、Ｂ病院に送付する必要がある。

[0070] 患者は、本発明の画像暗号化装置を利用して、以下の（ａ）～（ｇ）の処理を行なう。

（ａ）患者は、入力手段４１により、患者閲覧画像１１０ｃを、例えば、パーソナルコンピュータのディスプレイに表示する。

（ｂ）患者は、公開鍵取得手段４４により、公開鍵管理サーバ１９０からＢ病院の公開鍵１３５を取得する。

（ｃ）患者は、暗号化領域指定手段４２により、ディスプレイ画面に表示されている患者閲覧画像１１０ｃ上の個人情報１０１を指定する。そして、画像変換手段４３により、その個人情報１０１を暗号鍵１３１で暗号化する。これにより、患者閲覧画像１１０ｃが、暗号化されたＡ病院の病院情報（病院情報画像１０２）と暗号化された患者の個人情報（患者個人情報画像１０１）を含む画像１１０ｂに変換される。

（ｄ）患者は、鍵暗号化手段４５により、暗号鍵１３１をＢ病院の公開鍵１３５で暗号化し、その暗号化により生成された暗号に関する情報である第３の暗号鍵関連情報１４３を生成する。

（e）患者は、情報埋め込み手段４６により、前記画像１１０ｂ上の患者の個人情報画像１０１ａに第３の暗号鍵関連情報１４３を埋め込み、情報埋め込み画像１１０ａを生成する。

（ｆ）患者は、画素値変換手段４７により、情報埋め込み画像１１０ａに対して画素値変換処理を施し、画素値変換画像１００ｃ’を生成する。

（ｇ）患者は、画素値変換画像１００ｃ’を印刷出力して、画素値変換画像１００ｃ’が印刷された印刷媒体をＢ病院に送付する。または、画素値変換画像１００ｃ’を、電子メールによりＢ病院に送付する。

[0071] 以上のようにして、患者は、個人情報１０１が復号されたカルテ画像１１０Ｃを、Ａ病院から受け取った画素値変換画像１００ｃ’にして、それをＢ病院に送る。

＜Ｂ病院のカルテ復号処理＞

患者が、印刷媒体により、または、電子メールの添付ファイルにより送ってくるカルテ（画素値変換画像１００ｃ’）を受信・復号するＢ病院の処理を、図８を参照しながら説明する。

[0072] Ｂ病院は、本発明の画像復号装置を利用して、以下の（ａ）～（ｅ）の処理を行なう。

（ａ）Ｂ病院のセカンドオピニオンの医師は、入力手段５１により、Ａ病院の患者（以後、単に患者と記載する）から受け取った印刷媒体または電子メールの添付ファイルから、カルテ（画素値変換画像１００ｃ’）を画像化する。

（ｂ）医師は、暗号化領域指定手段４２により、画素値変換画像１００ｃ’上の患者個人情報画素値変換画像１０１ｃ’と病院情報画素値変換画像１０２ｃを指定する。そして、画素値変換手段５３により、それらの画像１０１ｃ’、１０２ｃに画素値変換処理を行い、それらの画像１０１ｃ’、１０２ｃの市松模様を解除する。これにより、患者個人情報画素値変換画像１０１ｃ’と病院情報画素値変換画像１０２ｃは、それぞれ、患者個人情報埋め込み画像１０１ｂ’と病院情報埋め込み画像１０２ｂに変換される。

（ｃ）医師は、情報抽出手段５４により、患者個人情報埋め込み画像１０１ｂ’から暗号鍵関連情報１４３（Ｂ病院の公開鍵１３５で暗号化された暗号鍵１３１に関する情報）を取り出す。そして、B病院の秘密鍵１３６を用いて、暗号鍵関連情報１４２を取り出す。次に、暗号鍵関連情報１４３および１４２をＢ病院の秘密鍵１３６で復号し、暗号鍵１３１と１３２をとりだす。続いて、暗号鍵１３１を用いて画像変換画像１０１ａを画像変換手段５６を用いて復号し、暗号鍵１３２を用いて画像変換画像１０２ａを画像変換手段５６を用いて復号し、それぞれの復号により、患者個人情報画像１０１と病

院情報画像１０２を復号する。

（ｅ）医師は、患者個人情報画像１０１と病院情報画像１０２を含むカルテ全体を閲覧する。

[0073] 以上述べたように、第２の実施形態は、Ａ病院は、複数の暗号鍵と複数の公開鍵（患者の公開鍵とＢ病院の公開鍵）を用いて、「Ａ病院の患者の個人情報」並びに「患者には知られたくないＡ病院の病院情報」が画像暗号化されカルテを作成できる。Ａ病院の患者は、そのカルテを、Ａ病院から、印刷媒体または電子メールの添付ファイルとして受け取り、患者の秘密鍵を用いて、そのカルテ上の暗号化されている患者の個人情報を復号・閲覧することができる。また、さらに、患者は、カルテの閲覧が終了すると、Ｂ病院の公開鍵を用いて患者の個人情報を暗号化し、Ａ病院が作成したカルテと同様に、患者の個人情報とＡ病院の病院情報が画像暗号化されたカルテを、印刷媒体、または、電子メールの添付ファイルとして、Ｂ病院に送付する。Ｂ病院のセカンドオピニオンの医師は、Ａ病院の患者が送付したカルテを受け取ると、Ｂ病院の秘密鍵を用いて、そのカルテ上の暗号化された患者の個人情報とＡ病院の病院情報を復号し、それらの情報を閲覧できる。

[0074] このように，第２の実施形態においては、複数の暗号鍵と複数の公開鍵を用いて、Ａ病院、Ａ病院の患者、その患者のセカンドオピニオンであるＢ病院の医師の三者が、患者の個人情報とＡ病院の病院情報の安全性を確保しながら、カルテをやりとりすることが可能となる。

[0075] ｛応用システムの第３の実施形態｝

本発明の応用システムの第３の実施形態は、市民が市役所などの地方自治体から住民票を発行してもらい、それを学校や販売業者などに提出するモデルに、本発明を適用したものである。第３の実施形態は、Ａ市役所が、画像暗号化した住民票の作成する際、暗号鍵関連情報を作成するとき、送付先の公開鍵（Ｃさんの公開鍵）に加え、送付元の秘密鍵（Ａ市役所の秘密鍵）を用いるのが特徴である。上述した第１及び第２の実施形態では、送付先の公開鍵のみを用いて暗号鍵関連情報を作成するようにしている。

[0076] この第３の実施形態について、図９を参照しながら説明する。

図９は、本発明を、ＢさんがＡ市役所からネットワークを介して住民票をダウンロードし、それをＣさんに提出する例に適用した場合のシステム構成とその手法を示す図である。Ｃさんは、例えば、自動車の販売業者である。尚、図９では、暗号化された住民票の画像については、全体ではなく、暗号化された部分のみを示している。

[0077] Ａ市役所は、本発明の画像暗号化装置を利用して、以下の（ａ）～（ｆ）の処理を行なう。

（ａ）Ｂさんが、Ａ市役所に住民票の発行を求めると、Ａ市役所は、入力手段４１により、住民票の画像２００（以後、住民票原画像２００と呼ぶ）を取り込む。そして、暗号化領域指定手段４２により、住民票原画像２００の重要事項（個人のプライバシーに関係する事項など）部分を指定し、その部分を暗号鍵２３１を用いて暗号化する。この暗号化は、画像変換手段４３を用いて行なう。この暗号化により、住民票原画像２００は画像変換画像２００ａに変換される。

（ｂ）Ａ市役所は、公開鍵取得手段４４により、公開鍵管理サーバ２９０からＢさんの公開鍵２３６とＣさんの公開鍵２３４を取得する。

（ｃ）Ａ市役所は、鍵暗号化手段４５により、暗号鍵２３１をCさんの公開鍵２３４とA市役所の秘密鍵２３２を用いて暗号化する。このCさんの公開鍵２３４とＡ市役所の秘密鍵２３２によって暗号化された暗号鍵２３１を、便宜上、暗号鍵関連情報２４３と呼ぶことにする。

（ｄ）Ａ市役所は、情報埋め込み手段４６により、暗号鍵関連情報２４３を画像変換画像２００ａに埋め込み、暗号鍵関連情報２４３が画像として埋め込まれた情報埋め込み画像２００ｂを生成する。

（ｅ）Ａ市役所は、画素値変換手段４７により、情報埋め込み画像２００ｂに対して画素値変換処理を施し、情報埋め込み画像２００ｂを市松模様化する。この市松模様化により、画素値変換画像２００ｃが生成される。

（ｆ）Ａ市役所は、Ｂさんの公開鍵２３６を用いて、画素値変換画像２００

ｃを電子的に暗号化する。この暗号化は、公知のディジタル暗号化手法によって行なわれる。ここで、Ｂさんの公開鍵２３６で暗号化された画素値変換画像２００ｃを、便宜上、「暗号化住民票電子データ」と呼ぶことにする。

[0078] Ｂさんは、以下の（ｇ）、（ｈ）の処理を行い、Ａ市役所から受け取った、画像暗号化された住民票を印刷し、その印刷物を、Ｃさんに提出する。

（ｇ）Ｂさんは、パーソナルコンピュータを使用して、Ａ市役所の公開サーバ（不図示）にアクセスし、その公開サーバから、電子的に暗号化されたＢさんの住民票（前記暗号化住民票電子データ）をダウンロードする。そして、Ｂさんの秘密鍵２３７を用いて、その暗号化住民票電子データを復号し、その復号によって得られた画素値変換画像２００ｃを、プリンタ２６０により紙に印刷する。暗号化住民票電子データの復号は、公知のディジタル復号手法により行なう。

[0079] 重要事項部分のみが市松模様化された住民票（画素値変換画像２００ｃ）を印刷できたことで、その住民票の印刷者がＢさんであることが保証される。

（ｈ）Ｂさんは、重要事項が暗号化された住民票（印刷物）をＣさんに提出する。

[0080] Ｃさんは、本発明の画像復号装置を利用して、以下の（ｉ）～（ｌ）の処理を行なう。

（ｉ）Ｃさんは、Ｂさんから受け取った印刷物を、入力手段４１（この例では、スキャナ２７０）により、画像データとして取り込む。これにより、Ｃさんは、画素値変換画像２００ｃを得ることができる。

（ｊ）Ｃさんは、画素値変換手段５３を用いて、画素値変換画像２００ｃの市松模様を解除し、画素値変換画像２００ｃから情報埋め込み画像２００ｂを復元する。

（ｋ）Ｃさんは、情報抽出手段５４により、情報埋め込み画像２００ｂから暗号鍵関連情報２４３を抽出し、情報埋め込み画像２００ｂから画像変換画像２００ａを復元する。次に、鍵復号化手段５６により、Ｃさんの秘密鍵２

３５とＡ市役所の公開鍵２３３を用いて、暗号鍵関連情報２４３から暗号鍵２３１を取り出す。尚、Ｃさんは、Ａ市役所の公開鍵２３３を、公開鍵管理サーバ２９０から取得する。

（ｉ）Cさんは、画像変換手段５７により、暗号鍵２３１を用いて、画像変換画像２００ａの画像暗号を解除し、住民票原画像２００を復元する。これにより、Ｃさんは、住民票原画像２００を閲覧して、Ｂさんの住民票を読むことができる。

[0081] 第３の実施形態においては、Ｃさんの秘密鍵２３５とＡ市役所の公開鍵２３３を用いて、暗号鍵関連情報２４３から暗号鍵２３１を復号できたことで、ＣさんがＢさんから受け取った印刷物（住民票）は、Ａ市役所から正式に発行されたものであることが証明される。また、暗号鍵２３１を暗号鍵関連情報２４３から取り出すためには、A市役所の公開鍵２３３だけでなく、Cさんの秘密鍵２３５も必要であることから、Ｃさん以外は住民票を閲覧することはできない。

[0082] 第３の実施形態は、現在、市役所や区役所などの窓口でしか受け取れない住民票を、Bさん（市民または区民など）が、市役所や区役所に出向くことなく、自宅のパーソナルコンピュータなどの端末を利用してダウンロードし、それを印刷して、Cさん（Bさんが住民票を提出する必要がある人もしくは法人など）に印刷物として提出すること可能にしている。

[0083] これは、以下の（１）～（４）の条件が満たされるからである。

（１）Ａ市役所は、Cさんの公開鍵を用いることによって、住民票の提出先を、Cさんだけに限定することができる。

（２）Ａ市役所は、Bさんの公開鍵を用いることによって、住民票（重要事項が暗号化されている住民票）のダウンロード者を、Bさんに特定できる。

（３）Ａ市役所からダウンロードする住民票は重要事項が暗号化されているので、Bさんは住民票に記載されている個人情報の漏洩を守ることができる。

（４）ＢさんがＣさんに提出した画像暗号化された住民票を、Ａ市役所の公開鍵で復号できることから、ＣさんがＢさんから受け取った住民票が、間違い

なく、Ａ市役所で発行された住民票であることが保証される。

[0084] {本発明の画像暗号化装置の実施形態}

本発明の画像暗号化装置は、パーソナルコンピュータ等のコンピュータ上でプログラム（ソフトウェア）を実行することによって、コンピュータで実現できる。

[0085] ＜ハードウェア構成＞

図１０は、本発明の暗号化装置として機能するパーソナルコンピュータのハードウェア構成を示す図である。

[0086] 本実施形態の暗号化装置であるパーソナルコンピュータ（ＰＣ）１０００は、ＣＰＵ１００１、第１の外部入力インターフェース部１００４（外部入力インターフェース１）、第２の外部入力インターフェース部１００５（外部入力インターフェース２）、ネットワークインターフェース部１００６、第１の外部出力インターフェース部１００７（外部出力インターフェース１）、第２の外部出力インターフェース部１００８（外部出力インターフェース２）、メモリ装置１０１０及びデータ記憶装置１０２０を備えている。ＣＰＵ(Central Processinng Unit)１００１は、パーソナルコンピュータ１０００の他の構成要素とバス１０３０を介して接続されている。

[0087] 第１の外部入力インターフェース部１００４は、スキャナなどの画像読み取り機能を備える第１の外部入力装置１１００（外部入力装置１）とのインターフェースであり、第１の外部入力装置１１００が読み取った文書などのデジタル画像を、第１の外部入力装置１１００から入力する。第２の外部入力インターフェース部１００５は、キーボードやマウスなどのインターフェースであり、キーボードやマウスなどの第２の外部入力装置１２００（外部入力装置２）から、それらの入力データや操作信号などを入力する。

[0088] ネットワークインターフェース部１００６は、例えば、ＬＡＮ(loacal Area Network)インターフェースなどであり、ＬＡＮやルータなどを経由して、公開鍵管理サーバやインターネットに通信接続し、公開鍵管理サーバ９０から目的の公開鍵を受信する。

[0089] 第１の外部出力インターフェース部１００７は、プリンタなどの印刷機能を有する第１の外部出力装置１３００（外部出力装置１）のインターフェースであり、第１の外部出力装置１３００に印刷制御コマンドや印刷データを出力する。第２の外部出力インターフェース部１００８は、ディスプレイなどの画像表示機能を有する第２の外部出力装置１４００（外部出力装置２）のインターフェースであり、第２の外部出力装置１４００に画像表示制御コマンドや画像データを出力する。

[0090] メモリ装置１０１０は、ＣＰＵ１００１のメインメモリであり、プログラム用メモリ領域１０１１とデータ用メモリ領域１０１２を備えている。プログラム用メモリ領域１０１１は、パーソナルコンピュータ１０００を、画像暗号化装置として機能させるプログラム１０６０を格納する領域である。このプログラム１０６０は、例えば、ＣＰＵ１００１が実行可能な形式で、プログラム用メモリ領域１０１１にロードされる。

[0091] 該プログラム１０６０は、ＣＰＵ１００１により実行されることによって、パーソナルコンピュータ１０００を、図２に示す、入力手段４１、暗号化領域指定手段４２、画像変換手段４３、公開鍵取得手段４４、鍵暗号化手段４５、情報埋め込み手段４６、画素値変換手段４７、及び出力手段４８を備える画像暗号化装置４０として機能させる。

[0092] データ用メモリ領域１０１２は、暗号鍵や画像暗号化データの送付先の公開鍵１５００などを保存する。メモリ装置１０１０には、基本ソフト（ＯＳ：Operating Syatem））やＴＣＰ／ＩＰプロトコルスタックなどのミドルウェアなども格納される。データ用メモリ領域１０１２は、第１及び第２の外部入力装置１１００、１２００から入力されるデータ、第1及び第２の外部出力装置１３００、１４００に出力するデータ、及びＣＰＵ１００１が上記プログラムを実行する際に必要となる作業データを記憶する。

[0093] データ記憶装置１０２０は、例えば内蔵型ＨＤＤ(Hard Disk Drive)や、ＣＤ、ＤＶＤなどの可搬型の記録媒体が装着される記憶装置であり、暗号化（画像暗号化）の対象となるデータ１６００などを保存する。尚、データ記憶

装置１０２０は、ＵＳＢ(Univerasal Serial Bus)端子に接続されるＵＳＢメモリや、カードスロットに装着されるＳＤ(Secure Digital)メモリカードやメモリスティックなどの小型の可搬型記録媒体であってもよい。

[0094] ＣＰＵ１００１は、パーソナルコンピュータ全体を制御すると共に、他の構成要素を制御する。

＜画像暗号化装置の処理手順＞

図１１は、図１０に示すパーソナルコンピュータ１０００のＣＰＵ１００１が、プログラム用メモリ領域１０１１に格納されているプログラム１０６０を実行することによって行なう画像暗号化処理を示すフローチャートである。図１１を参照しながら、上記画像暗号化処理の手順を説明する。

[0095] 暗号化の対象となるデータ１６００（以後、暗号化対象データ１６００と呼ぶ）を、データ記憶装置１０２０に用意する（Ｓ１１０１）。

データ記憶装置１０２０からデータ用メモリ領域１０１２に、暗号化対象データ１６００を転送する(Ｓ１１０２)。プログラム用メモリ領域１０１１上の入力手段４１を実行し、該暗号化対象データ１６００を画像（ビットマップ形式などの画像データ）に変換する（Ｓ１１０３）。この暗号化対象データ１６００の画像（画像データ）は、データ用メモリ領域１０１２に格納される。

[0096] 暗号化対象データ１６００の画像を、第２の外部出力装置１４００に表示する（Ｓ１１０４）。プログラム用メモリ領域１０１１上の暗号化領域指定手段４２を実行し、第２の外部入力装置１２００（例えば、マウスなど）を用いて、第２の外部出力装置１４００の画面に画像表示されている暗号化対象データ１６００の画像の暗号化領域を指定する（Ｓ１１０５）。

[0097] 図１３に、暗号化対象データ１６００の画像の暗号化領域の指定方法の一例を示す。この例では、暗号化対象データ１６００は「暗号化画像」という用語となっており、その画像１７００の「暗号」という用語の画像を囲む領域（破線の矩形枠で囲まれた領域）が暗号化領域１７０１として指定されている。

[0098] プログラム用メモリ領域１０１１上の画像変換手段４３を実行し、データ用メモリ領域１０１２上の暗号化対象データ１６００の画像１７００の暗号化領域１７０１の画像（画像データ）を、暗号鍵（不図示）を用いて、画像変換画像に変換する（Ｓ１１０６）。この画像変換処理により、暗号化領域１７０１の画像が、図１３に示す判読可能な状態（原画像）から、図１４に示す判読不可能な状態（画像変換画像１７１１）に変換される。これにより、暗号化対象データ１６００の画像全体は、図１４に示すように、該画素値変換画像１７１１を含む画像１７１０に変換される。

[0099] プログラム用メモリ領域１０１１上の公開鍵取得手段４４を実行し、ネットワークインターフェース部１００６を介して、公開鍵管理サーバにアクセスする（Ｓ１１０７）。そして、公開鍵管理サーバから、データ送付先の公開鍵１５００を取得し、それをデータ用メモリ領域１０１２に格納・保存する（Ｓ１１０８）。

[0100] プログラム用メモリ領域１０１１上の鍵暗号化手段４５を実行し、上記公開鍵１５００を用いて、前記暗号鍵を暗号化する（Ｓ１１０９）。この暗号化処理において、例えば、、“１１１１１１１”の２値のビット列（バイナリデータ）の暗号鍵を、公開鍵１５００を用いて、“１０１１０１０１”の２値のビット列に暗号化する。ここでは、上記と同様に、この暗号化された暗号鍵を、“暗号鍵関連情報”と呼ぶことにする。

[0101] プログラム用メモリ領域１０１１上の情報埋め込み手段４６を実行し、データ用メモリ領域１０１２上の暗号化領域１７０１の画像（ステップＳ１１０６の処理で得られた画像変換画像１７１１）に、上記暗号鍵関連情報を埋め込む（Ｓ１１１０）。この結果、暗号化領域１７０１の画像は、図１４に示す状態（画像変換画像１７１１）から図１５に示す状態（情報埋め込み画像１７２１）に変換される。これにより、暗号化対象データ１６００の画像全体は、図１５に示すように、該情報埋め込み画像１７２１を含む画像１７２０に変換される。

[0102] プログラム用メモリ領域１０１１上の画素値変換手段４７を実行し、デー

タ用メモリ領域１０１２上の前記情報埋め込み画像１７２１を変換する（Ｓ１１１１）。この結果、暗号化領域１７０１の画像は、図１５に示す状態（情報埋め込み画像１７２１）から図１６に示す状態（市松模様の画素値変換画像１７３１）に変換される。これにより、暗号化対象データ１６００の画像全体は、図１６に示すように、該画素値変換画像１７３１を含む暗号化画像１７３０に変換される。

[0103] ステップＳ１１１１の処理で生成された該暗号化画像１７３０を、第２の外部出力装置１４００に表示する（Ｓ１１１２）。続いて、データ用メモリ領域１０１２上の前記暗号化画像１７３０を、データ記憶装置１０２０に転送・保存する（Ｓ１１１３）。

[0104] プログラム用メモリ領域１０１１上の出力手段４８を実行し、データ用メモリ領域１０１２またはデータ記憶装置１０２０に格納されている前記暗号化画像１７３０を、第１の外部出力装置１３００を用いて紙媒体等に印刷、または、ネットワークインターフェース部１００６を介して電子メールなどにより送付先に送信する（Ｓ１１１４）。

[0105] {本発明の暗号化復号装置の実施形態}

本発明の画像復号装置は、前記画像暗号化装置と同様に、パーソナルコンピュータ等のコンピュータ上でプログラム（ソフトウェア）を実行することによって、コンピュータで実現できる。

[0106] ＜ハードウェア構成＞

図１７は、本発明の画像復号装置として機能するパーソナルコンピュータのハードウェア構成を示す図である。図１７において、図１０と同じ構成要素には同じ符号を付与している。

[0107] 本実施形態の画像復号装置であるパーソナルコンピュータ（ＰＣ）２０００は、図１０に示す、パーソナルコンピュータ１０００と、ほぼ同じハードウェア構成である。したがって、上述したパーソナルコンピュータ１０００が備える構成要素と同一の構成要素については、その説明を省略する。

[0108] 画像復号装置として機能するパーソナルコンピュータ２０００と、画像暗

号化装置として機能するパーソナルコンピュータ１０００との構成上の差異は、メモリ装置１０１０内のプログラム用メモリ領域１０１１に格納される、ＣＰＵ１００１が実行するプログラムの内容である。

[0109] 本実施形態のパーソナルコンピュータ２０００は、図１０に示す、画像復号装置として機能するパーソナルコンピュータ１０００によって生成された画像暗号化データを復号する画像復号装置である。

[0110] パーソナルコンピュータ１０００においては、プログラム用メモリ領域１０１１には、図２に示す構成の画像暗号化処理用のプログラム１０６０が格納される。これに対し、パーソナルコンピュータ２０００のプログラム用メモリ領域２０１１には、図３に示す構成の画像復号処理用のプログラム２０６０が格納される。このプログラム２０６０は、ＣＰＵ１００１により実行されることにより、パーソナルコンピュータ２０００を、入力手段５１、暗号化位置検知手段５２、画素値変換手段５３、情報抽出手段５４、公開鍵取得手段５５、鍵復号化手段５６、画像変換手段５７及び出力手段５８を備える画像復号装置として機能させる。但し、公開鍵取得手段５５の機能は必須ではなく、前記暗号鍵関連情報が、暗号化画像の生成側の公開鍵と暗号化画像の復号側の秘密鍵を用いて生成される場合にのみ必要となる。この場合、公開鍵取得手段５５は、該秘密鍵と対になる公開鍵を取得する。

[0111] また、メモリ装置１０１０のデータ用メモリ領域１０１２は、第１の外部入力装置１１００、または、ネットワークインターフェース１００６を介して入力した暗号化データ（暗号化画像）２６００（図１０の画像暗号化装置（パーソナルコンピュータ１０００）によって生成された暗号化画像）を保存する。また、データ記憶装置１０２０は、前記画像暗号化データ２６００を生成する際に、暗号鍵を暗号化するために用いられた公開鍵１５００と対になる秘密鍵２５００を保存する。

[0112] ＜画像復号処理の手順＞

図１８は、図１７の画像復号装置として機能するパーソナルコンピュータ２０００の処理手順を示すフローチャートである。このフローチャートに示

す処理は、パーソナルコンピュータ２０００のＣＰＵ１００１が、プログラム用メモリ領域１０１１上のプログラム２０６０を実行することにより行なわれる。以後のフローチャートの説明では、図１６に示す暗号化データ１７００を復号する例を取り上げる。

[0113] まず、受信者（図１０のパーソナルコンピュータ１０００（画像暗号化装置）で生成された暗号化データの受信者）の秘密鍵を、データ記憶装置１０２０に準備する（Ｓ２１０１）。

[0114] この処理により、データ記憶装置１０２０に秘密鍵２５００が保存される。

第１の外部入力装置１１００またはネットワークインターフェース１００６から、図１０のパーソナルコンピュータ１０００（画像暗号化装置）で生成された暗号化データを取得し、データ用メモリ領域１０１２に保存する（Ｓ２１０２）。

[0115] この処理により、図１６に示す暗号化画像１７３０が、印刷物または電子データの形態（ここでは、暗号化データと呼ぶことにする）で取得され、データ用メモリ領域１０１２に保存される。

[0116] プログラム用メモリ領域１０１１上の入力手段５１を実行し、データ用メモリ領域１０１２上の前記暗号化データを、ビットマップ形式などの画像（画像データ）に変換する（Ｓ２１０３）。この変換により得られた画像を、暗号化画像と呼ぶことにする。この暗号化画像は、図１０の画像暗号化装置によって最終的に生成された暗号化画像（図１６に示す暗号化画像１７３０と同等の画像）である。

[0117] プログラム用メモリ領域１０１１上の暗号化位置検知手段５２を実行し、前記暗号化画像の暗号化領域の位置情報を検知し、それをデータ用メモリ領域１０１２に保存する（Ｓ２１０４）。

[0118] プログラム用メモリ領域１０１１上の画素値変換手段５３を実行し、データ用メモリ領域１０１２上の上記暗号化領域の位置情報を参照しながら、データ用メモリ領域１０１２上の前記暗号化画像の暗号化領域の画像（画素値

変換画像）を情報埋め込み画像に変換する（Ｓ２１０５）。

[0119] この処理により、図１６に示す暗号化画像１７３０の暗号化領域１７０１の画像が、図１６に示す状態（画素値変換画像１７３１）から図１５に示す状態（情報埋め込み画像１７２１）に変換される。

[0120] プログラム用メモリ領域１０１１上の情報抽出手段５４を実行し、データ用メモリ領域１０１２上の前記暗号化領域の位置情報を参照しながら、前記情報埋め込み画像から暗号鍵関連情報（暗号化された暗号鍵）を抽出し、それをデータ用メモリ領域１０１２に記憶する（Ｓ２１０６）。

[0121] この処理により、図１５に示す暗号化領域の画像（情報埋め込み画像１７２１）から、暗号鍵関連情報として、“１０１１０１０”が取り出される。また、この暗号鍵関連情報の抽出により、暗号化領域１７０１の画像が、図１５に示す状態（情報埋め込み画像１７２１）から図１４に示す状態（画像変換画像１７１１）に変換される。

[0122] 前記暗号鍵関連情報（暗号化された暗号鍵）の復号に公開鍵が別途必要であれば、プログラム用メモリ領域１０１１上の公開鍵取得手段５５を実行し、ネットワークインターフェース１００６を介して、公開鍵管理サーバ１９０から前記秘密鍵２５００と対になる公開鍵を取得する（Ｓ２１０７）。

[0123] プログラム用メモリ領域１０１１上の鍵復号化手段５６を実行し、データ用メモリ領域１０１２に保存された暗号鍵関連情報（暗号化された暗号鍵）を、データ記憶装置１０２０に準備した受信者の秘密鍵２５００を用いて、暗号鍵に復号する。そして、その暗号鍵をデータ用メモリ領域１０１２に保存する（Ｓ２１０８）。このステップＳ２１０８の暗号鍵の復号処理において、前記暗号鍵関連情報が、秘密鍵２５００と前記公開鍵管理サーバ９０から取得した公開鍵とで暗号化された暗号鍵であれば、その復号には、秘密鍵２５００と該公開鍵を用いる。

[0124] この処理により、暗号鍵関連情報（＝“１０１１０１０”）から暗号鍵（＝“１１１１１１１”）が復号される。

プログラム用メモリ領域１０１１上の画像変換手段５７を実行し、データ

用メモリ領域１０１２上の暗号鍵を用いて、データ用メモリ領域１０１２上の暗号化領域の画像を原画像に変換する（Ｓ２１０９）。

[0125] この処理により、暗号化領域１７０１の画像が、図１４に示す状態（画像変換画像１７１１）から図１３に示す状態（原画像）に変換される。これにより、本装置の入力手段５１により入力された暗号化画像１７３０の暗号化領域１７０１の暗号化画像１７３１が、最終的に、「暗号」という文字画像に復号され、その文字画像を含む「暗号化画像」という用語を表現する原画像１７００が復元される。

[0126] データ用メモリ領域１０１２上の前記原画像（原画像のデータ）を、データ記憶装置１０２０に保存する（Ｓ２１１０）。

データ記憶装置１０２０上の原画像を、第２の外部出力インターフェース１００８を介して、第２の外部出力装置１４００（例えば、ディスプレイ）に出力（表示）する（Ｓ２１１１）。

[0127] 本発明は、上述した実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲内で種々に変形して実施することができる。例えば、パーソナルコンピュータ以外でも、コピー機（複合機も含む）やFAX、プリンタ、スキャナ、オーバーヘッドリーダ、携帯電話、携帯端末、ディジタルカメラ、TVなどに本発明の機能が組み込まれてもよい。

産業上の利用可能性

[0128] 本発明は、紙媒体や記憶媒体、さらには、電子データなど各種メディアを利用して、個人情報など秘匿性が求められる重要な情報を、官公庁、企業、一般ユーザなど多くの利用者が、安全かつ安価なコストでやりとりすることができる。したがって、官公庁、企業、及び一般ユーザ間で、秘匿性を要求される重要情報をやりとりする際に、非常に便利である。

請求の範囲

[1] 画像を暗号化する画像暗号化装置において、

暗号化の対象となる画像データを入力する入力手段と、

該入力手段によって入力された画像データについて、暗号化の対象となる領域を指定する暗号化領域指定手段と、

該暗号化領域指定手段によって指定された暗号化領域を、暗号鍵を用いて、第１の画像に変換する画像変換手段と、

前記暗号化対象のデータの送付先の公開鍵を取得する公開鍵取得手段と、

該公開鍵取得手段によって取得された公開鍵を用いて、前記暗号鍵を暗号化する鍵暗号化手段と、

該鍵暗号化手段によって暗号化された暗号鍵に関する情報である暗号鍵関連情報を、前記第１の画像内に埋め込み、前記暗号化領域を第２の画像に変換する情報埋め込み手段と、

前記暗号化領域指定手段によって指定された領域を特定可能となるように、前記第２の画像の画素値を変換し、前記暗号化領域を第３の画像に変換する画素値変換手段と、

前記入力手段によって入力された画像において前記暗号化領域の画像が前記第３の画像に変換された暗号化画像を、所定の方式で出力する出力手段と、

を備えることを特徴とする画像暗号化装置。

[2] 請求項１記載の画像暗号化装置であって、

前記暗号化領域指定手段は複数の暗号化領域を指定し、

前記画像変換手段は、前記複数の暗号化領域の各領域の画像を、複数の暗号鍵を用いて個別に変換し、

前記公開鍵取得手段は、複数の公開鍵を取得し、

前記鍵暗号化手段は、前記画像変換手段が各暗号化領域の画像を変換するために用いた各暗号鍵を、前記公開鍵取得手段によって取得された複数の公開鍵を用いて個別に暗号化することを特徴とする。

[3] 請求項２記載の画像暗号化装置であって、

前記公開鍵取得手段が取得する複数の公開鍵は、複数の送付先の公開鍵であることを特徴とする。

[4] 請求項１または２記載の画像暗号化装置であって、

前記鍵暗号化手段は、前記暗号鍵を、前記公開鍵と、前記送付先が前記暗号化画像を提出する相手の秘密鍵とを用いて暗号化することを特徴とする。

[5] 請求項１乃至４のいずれか１項に記載の画像暗号化装置であって、

前記公開鍵取得手段は、前記公開鍵を、それを管理している公開鍵管理サーバから取得することを特徴とする。

[6] 暗号化された画像を含む暗号化画像を原画像に復号する画像復号装置であって、

前記暗号化画像を、画像データとして入力する入力手段と、

該入力手段が入力した前記暗号化画像を解析して、前記暗号化画像における画像が暗号化された領域である暗号化領域の位置を検知する暗号化位置検知手段と、

該暗号化位置検知手段により検知された前記暗号化領域の位置情報に基づいて前記暗号化領域の位置を特定するために、前記暗号化領域の画像の画素値を変換前の画素値に戻す画素値変換手段と、

該画素値変換手段により生成された前記暗号化領域の画像から、それに埋め込まれている暗号鍵に関する情報である暗号鍵関連情報を抽出する情報抽出手段と、

該情報抽出手段によって抽出された前記暗号鍵関連情報の生成に用いられた第1の公開鍵と対になる第1の秘密鍵を用いて、前記暗号鍵関連情報から、前記暗号化領域の画像を復号するために用いる復号鍵を復号する鍵復号化手段と、

該鍵復号化手段によって復号された復号鍵を用いて前記暗号化領域の画像を復号して、前記原画像を復号する画像変換手段と、

前記原画像を所定の方式で出力する出力手段と、

を備えることを特徴とする画像復号装置。

[7] 請求項６記載の画像復号装置であって、

前記第１の秘密鍵は前記暗号化画像の送付先が保有する秘密鍵であり、前記第１の秘密鍵は前記送付先が前記暗号化画像を提出する相手が前記暗号化画像を復号するために使用する第２の公開鍵と対になる秘密鍵であることを特徴とする。

[8] 請求項６または７記載の画像復号装置であって、

前記暗号鍵関連情報が前記第1の公開鍵と第２の秘密鍵によって暗号化されている場合に、前記第２の秘密鍵と対になる第２の公開鍵を取得する公開鍵を取得する公開鍵取得手段を、さらに備え、

前記鍵暗号化手段は、前記暗号鍵関連情報から、前記第１の秘密鍵と前記第２の公開鍵を用いて、前記復号鍵を復号することを特徴とする。

[9] 請求項６または７記載の画像復号装置であって、

前記暗号化領域は複数であることを特徴とする。

[10] 請求項９記載の画像復号装置であって、

各暗号化領域の画像に含まれる各暗号鍵関連情報は個別の暗号鍵に関する情報であり、

前記情報抽出手段は、前記各暗号化領域から個別の暗号鍵関連情報を抽出し、

前記鍵復号化手段は、前記情報抽出手段により抽出された各暗号鍵関連情報から、それぞれの暗号鍵関連情報の生成に用いられた秘密鍵と対になる公開鍵を用いて、前記各暗号鍵関連情報が埋め込まれていた各暗号化領域の画像を復号するために用いる各復号鍵を復号することを特徴とする。

[11] 請求項６乃至１０のいずれか１項に記載の画像復号装置であって、

前記公開鍵取得手段は、前記公開鍵を、それを管理している公開鍵管理サーバから取得することを特徴とする。

[12] 画像を暗号化する画像暗号化方法において、

暗号化の対象となる画像データを入力するステップと、

該入力ステップによって入力された画像データについて、暗号化の対象となる領域を指定するステップと、

該指定された暗号化領域を、暗号鍵を用いて、第１の画像に変換するステップと、

前記暗号化対象のデータの送付先の公開鍵を取得するステップと、

該取得された公開鍵を用いて、前記暗号鍵を暗号化するステップと、

該暗号化された暗号鍵に関する情報である暗号鍵関連情報を、前記第１の画像内に埋め込み、前記暗号化領域を第２の画像に変換するステップと、

前記暗号化の対象として指定された領域を特定可能となるように、前記第２の画像の画素値を変換し、前記暗号化領域を第３の画像に変換するステップと、

前記入力された暗号化対象の画像において前記暗号化領域の画像が前記第３の画像に変換された暗号化画像を、所定の方式で出力するステップと、

を備えることを特徴とする画像暗号化方法。

[13] 請求項１２記載の画像暗号化方法であって、

前記暗号化領域指定ステップにおいて、複数の暗号化領域を指定し、

前記画像変換ステップにおいて、前記複数の暗号化領域の各領域の画像を、複数の暗号鍵を用いて個別に変換し、

前記公開鍵取得ステップにおいて、複数の公開鍵を取得し、

前記鍵暗号化ステップにおいて、前記画像変換ステップにおいて各暗号化領域の画像を変換するために用いられた各暗号鍵を、前記公開鍵取得ステップにおいて取得された複数の公開鍵を用いて個別に暗号化することを特徴とする。

[14] 請求項１２または１３記載の画像暗号化方法であって、

前記公開鍵取得ステップにおいて取得する複数の公開鍵は、複数の送付先の公開鍵であることを特徴とする。

[15] 暗号化された画像を含む暗号化画像を原画像に復号する画像復号方法であって、

前記暗号化画像を、画像データとして入力するステップと、

該入力ステップにおいて入力された暗号化画像を解析して、前記暗号化画像における画像が暗号化された領域である暗号化領域の位置を検知するステップと、

該検知された前記暗号化領域の位置情報に基づいて前記暗号化領域の位置を特定するために、前記暗号化領域の画像の画素値を変換前の画素値に戻すステップと、

該画素値変換ステップにおいて生成された前記暗号化領域の画像から、それに埋め込まれている暗号鍵に関する情報である暗号鍵関連情報を抽出するステップと、

該抽出された前記暗号鍵関連情報の生成に用いられた第1の公開鍵と対になる第1の秘密鍵を用いて、前記暗号鍵関連情報から、前記暗号化領域の画像を復号するために用いる復号鍵を復号するステップと、

該復号された復号鍵を用いて前記暗号化領域の画像を復号して、前記原画像を復号するステップと、

前記原画像を所定の方式で出力するステップと、

を備えることを特徴とする画像復号方法。

[16] 請求項１５記載の画像復号方法であって、

前記第１の秘密鍵は前記暗号化画像の送付先が保有する秘密鍵であり、前記第１の秘密鍵は前記送付先が前記暗号化画像を提出する相手が前記暗号化画像を復号するために使用する第２の公開鍵と対になる秘密鍵であることを特徴とする。

[17] 請求項１５または１６記載の画像復号方法であって、

前記暗号鍵関連情報が前記第1の公開鍵と第２の秘密鍵によって暗号化されている場合に、前記第２の秘密鍵と対になる第２の公開鍵を取得する公開鍵を取得するステップを、さらに備え、

前記鍵暗号化ステップにおいて、前記暗号鍵関連情報から、前記第１の秘密鍵と前記第２の公開鍵を用いて、前記復号鍵を復号することを特徴とする

。

[18] 請求項１５または１６記載の画像復号方法であって、

前記暗号化領域は複数であることを特徴とする。

[19] 請求項１８記載の画像復号方法であって、

各暗号化領域の画像に含まれる各暗号鍵関連情報は個別の暗号鍵に関する情報であり、

前記情報抽出ステップにおいて、前記各暗号化領域から個別の暗号鍵関連情報を抽出し、

前記鍵復号化ステップにおいて、前記情報抽出ステップにおいて抽出された各暗号鍵関連情報から、それぞれの暗号鍵関連情報の生成に用いられた秘密鍵と対になる公開鍵を用いて、前記各暗号鍵関連情報が埋め込まれていた各暗号化領域の画像を復号するために用いる各復号鍵を復号することを特徴とする。

[20] 画像を暗号化するために、コンピュータを、

暗号化の対象となる画像データを入力する入力手段、

該入力手段によって入力された画像について、暗号化の対象となる領域を指定する暗号化領域指定手段、

該暗号化領域指定手段によって指定された暗号化領域を、暗号鍵を用いて、第１の画像に変換する画像変換手段、

前記暗号化対象のデータの送付先の公開鍵を取得する公開鍵取得手段、

該公開鍵取得手段によって取得された公開鍵を用いて、前記暗号鍵を暗号化する鍵暗号化手段、

該鍵暗号化手段によって暗号化された暗号鍵に関する情報である暗号鍵関連情報を、前記第１の画像内に埋め込み、前記暗号化領域を第２の画像に変換する情報埋め込み手段、

前記暗号化領域指定手段によって指定された領域を特定可能となるように、前記第２の画像の画素値を変換し、前記暗号化領域を第３の画像に変換する画素値変換手段、

前記入力手段によって入力された画像において前記暗号化領域の画像が前記第３の画像に変換された暗号化画像を、所定の方式で出力する出力手段、として機能させるための画像暗号化プログラム。

[21] 請求項２０記載の画像暗号化プログラムであって、

前記暗号化領域指定手段は複数の暗号化領域を指定し、

前記画像変換手段は、前記複数の暗号化領域の各領域の画像を、複数の暗号鍵を用いて個別に変換し、

前記公開鍵取得手段は、複数の公開鍵を取得し、

前記鍵暗号化手段は、前記画像変換手段が各暗号化領域の画像を変換するために用いた各暗号鍵を、前記公開鍵取得手段によって取得された複数の公開鍵を用いて個別に暗号化することを特徴とする。

[22] 請求項２１記載の画像暗号化プログラムであって、

前記画像変換手段は、各暗号化領域の画像を、それぞれ、別個の暗号鍵を用いて変換することを特徴とする。

[23] 請求項２１または２２記載の画像暗号化プログラムであって、

前記公開鍵取得手段が取得する複数の公開鍵は、複数の送付先の公開鍵であることを特徴とする。

[24] 請求項２０乃至２３のいずれか１項に記載の画像暗号化プログラムであって、

前記公開鍵取得手段は、前記公開鍵を、それを管理している公開鍵管理サーバから取得することを特徴とする。

[25] 暗号化された画像を含む暗号化画像を原画像に復号するために、コンピュータを、

前記暗号化画像を、画像データとして入力する入力手段、

該入力手段が入力した前記暗号化画像を解析して、前記暗号化画像における画像が暗号化された領域である暗号化領域の位置を検知する暗号化位置検知手段、

該暗号化位置検知手段により検知された前記暗号化領域の位置情報に基づ

いて前記暗号化領域の位置を特定するために、前記暗号化領域の画像の画素値を変換前の画素値に戻す画素値変換手段、

該画素値変換手段により生成された前記暗号化領域の画像から、それに埋め込まれている暗号鍵に関する情報である暗号鍵関連情報を抽出する情報抽出手段、

該情報抽出手段によって抽出された前記暗号鍵関連情報の生成に用いられた第1の公開鍵と対になる第1の秘密鍵を用いて、前記暗号鍵関連情報から、前記暗号化領域の画像を復号するために用いる復号鍵を復号する鍵復号化手段、

該鍵復号化手段によって復号された復号鍵を用いて前記暗号化領域の画像を復号して、前記原画像を復号する画像変換手段と、

前記原画像を所定の方式で出力する手段

として機能させるための画像復号プログラム。

[26] 請求項２５記載の画像復号プログラムであって、

前記第１の秘密鍵は前記暗号化画像の送付先が保有する秘密鍵でり、前記第１の秘密鍵は前記送付先が前記暗号化画像を提出する相手が前記暗号化画像を復号するために使用する第２の公開鍵と対になる秘密鍵であることを特徴とする。

[27] 請求項２５または２６記載の画像復号プログラムであって、

前記暗号鍵関連情報が前記第1の公開鍵と第２の秘密鍵によって暗号化されている場合に、前記第２の秘密鍵と対になる第２の公開鍵を取得する公開鍵を取得する公開鍵取得手段を、さらに備え、

前記鍵暗号化手段は、前記暗号鍵関連情報から、前記第１の秘密鍵と前記第２の公開鍵を用いて、前記復号鍵を復号することを特徴とする。

[28] 請求項２５または２６記載の画像復号プログラムであって、

前記暗号化領域は複数であることを特徴とする。

[29] 請求項２８記載の画像復号プログラムであって、

各暗号化領域の画像に含まれる各暗号鍵関連情報は個別の暗号鍵に関する

情報であり、

前記情報抽出手段は、前記各暗号化領域から個別の暗号鍵関連情報を抽出し、

前記鍵復号化手段は、前記情報抽出手段により抽出された各暗号鍵関連情報から、それぞれの暗号鍵関連情報の生成に用いられた秘密鍵と対になる公開鍵を用いて、前記各暗号鍵関連情報が埋め込まれていた各暗号化領域の画像を復号するために用いる各復号鍵を復号することを特徴とする。

[30] 請求項２５乃至２９のいずれか１項に記載の画像復号プログラムであって、

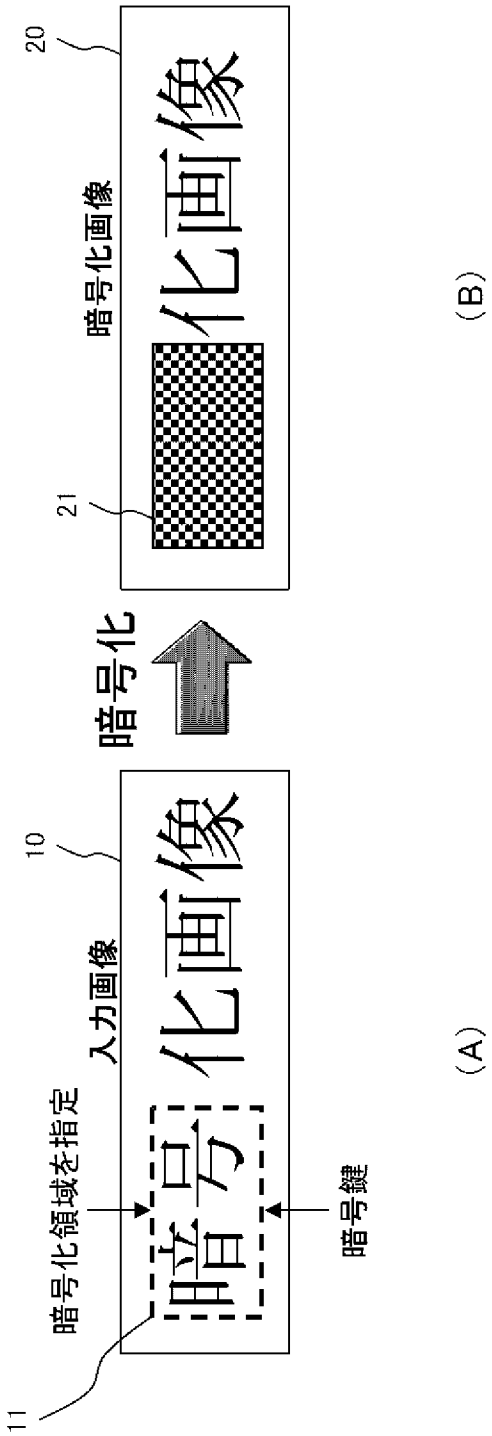
前記公開鍵取得手段は、前記公開鍵を、それを管理している公開鍵管理サーバから取得することを特徴とする。

[31] 請求項１記載の画像暗号化装置、請求項１２記載の画像暗号化方法、請求項２０記載の画像暗号化プログラム、請求項６記載の画像復号装置、請求項１５記載の画像復号方法、および請求項２５記載の画像復号プログラムにおいて、前記入力手段または前記入力ステップに入力される画像データは、画像もしくは、印刷物や非画像データを画像に変換したものであることを特徴とする。

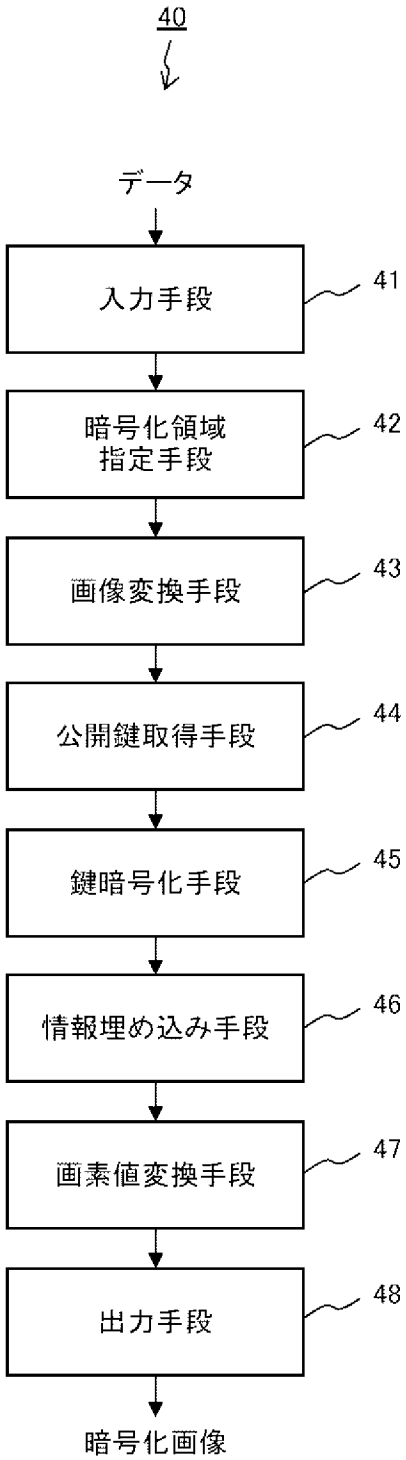
[32] 前記請求項１記載の画像暗号化装置、請求項１２記載の画像暗号化方法、請求項２０記載の画像暗号化プログラム、請求項６記載の画像復号装置、請求項１５記載の画像復号方法、および請求項２５記載の画像復号プログラムにおいて、

前記出力手段または前記出力ステップによって出力される出力データは、画像や印刷物、非画像データの少なくとも一つであることを特徴とする。

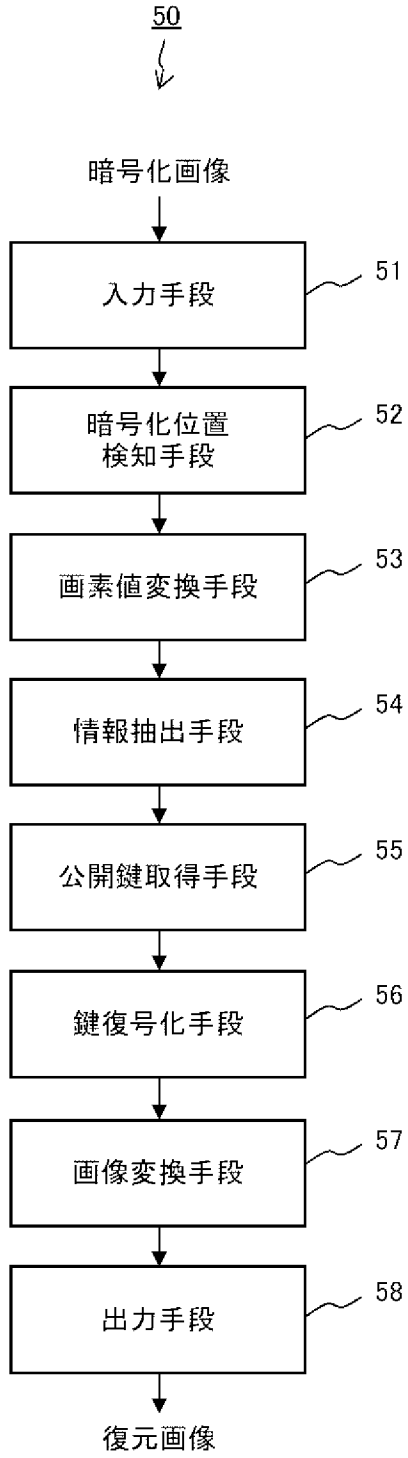
[図1]



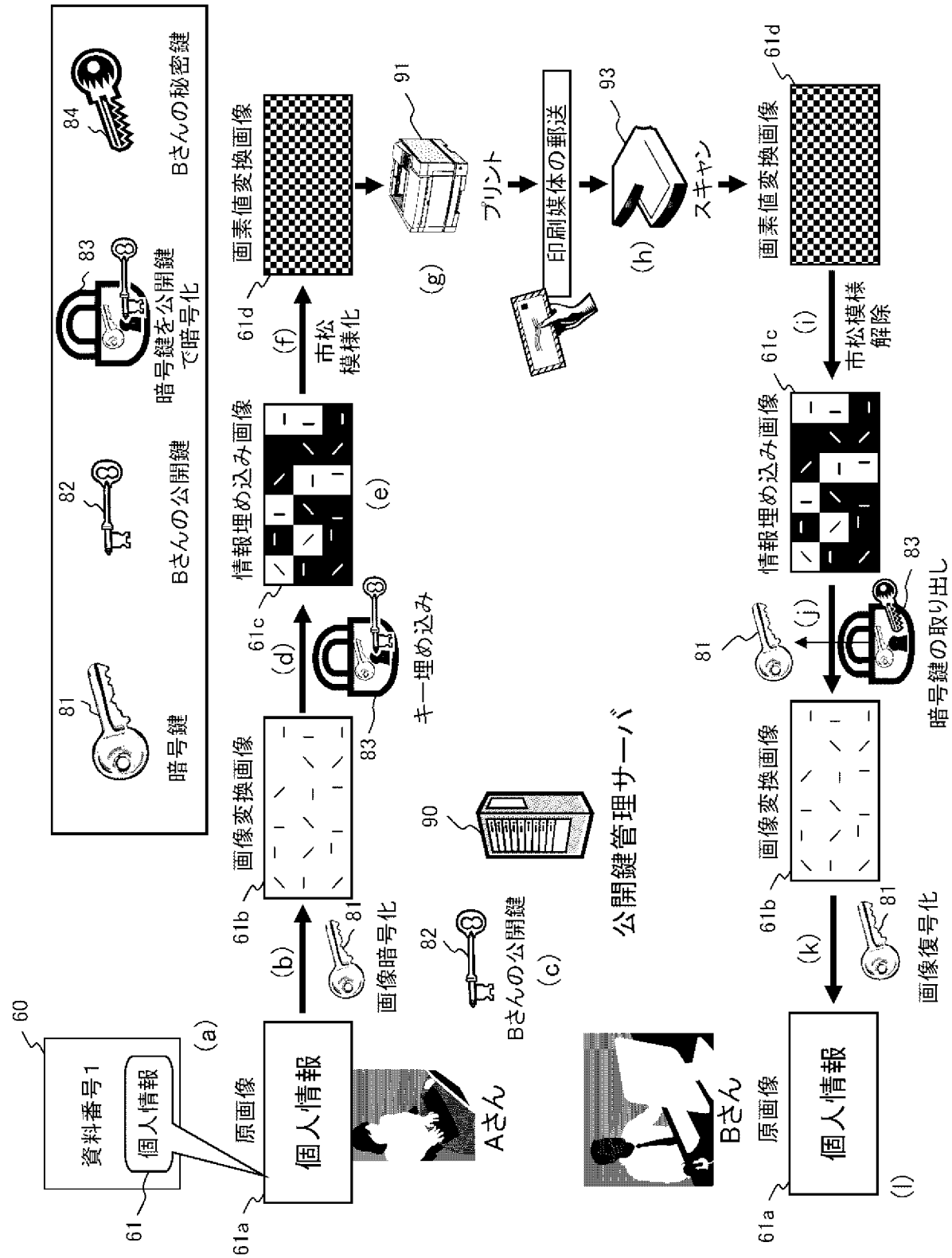
[図2]


40
データ
入力手段
41
暗号化領域
指定手段
42
画像変換手段
43
公開鍵取得手段
44
鍵暗号化手段
45
情報埋め込み手段
46
画素値変換手段
47
出力手段
48
暗号化画像

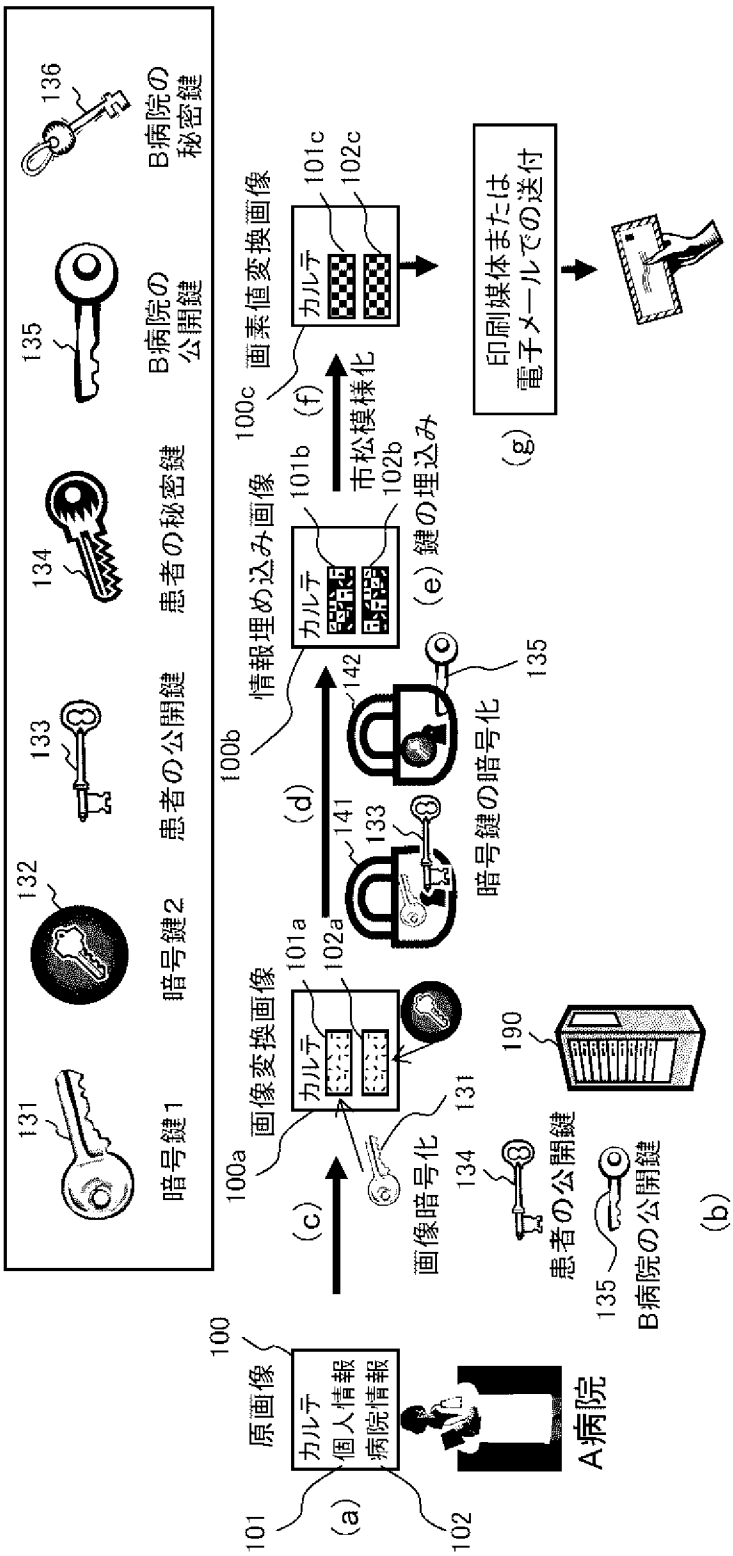
[図3]


50
暗号化画像
入力手段
51
暗号化位置
検知手段
52
画素値変換手段
53
情報抽出手段
54
公開鍵取得手段
55
鍵復号化手段
56
画像変換手段
57
出力手段
58
復元画像

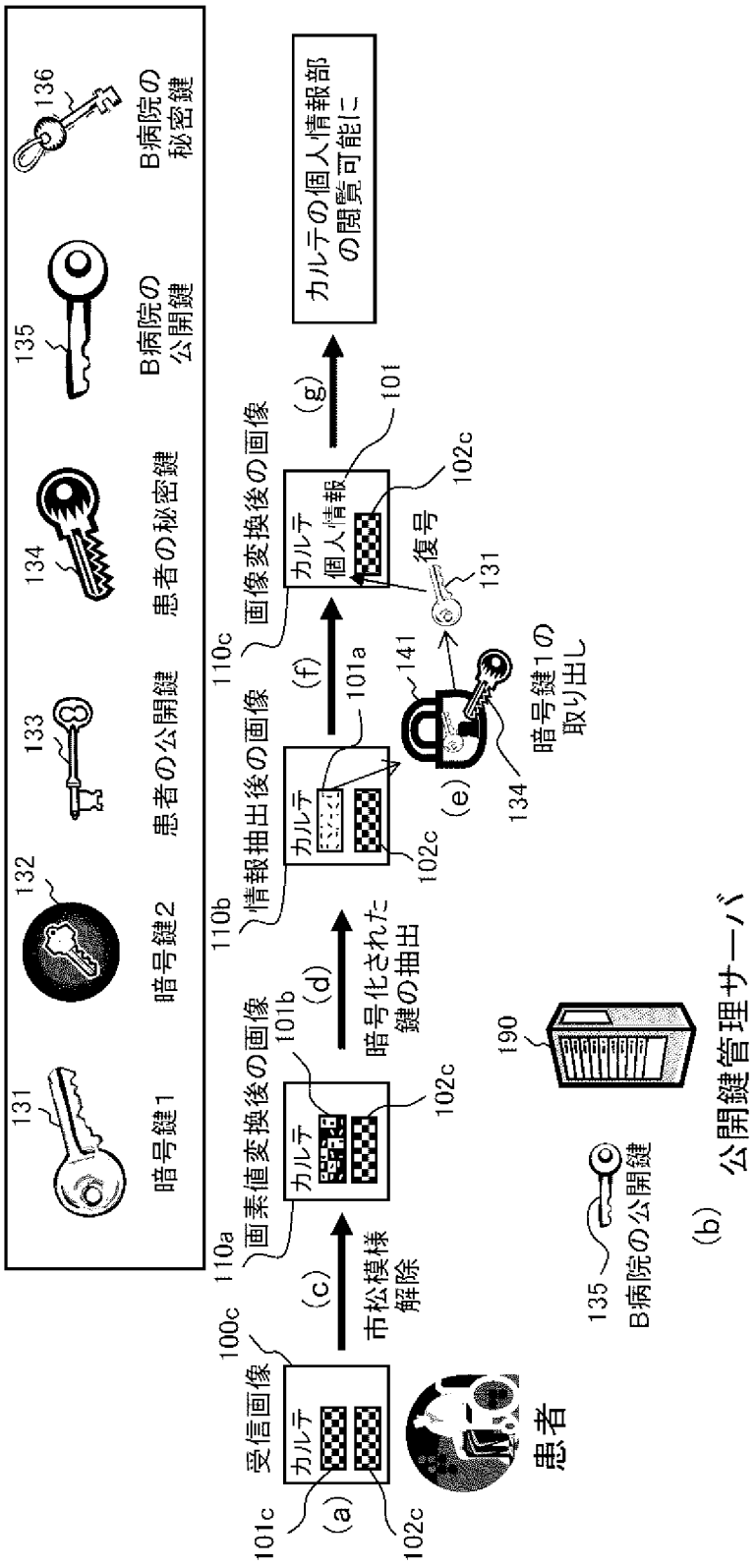
[図4]


60
資料番号1
個人情報
61
(a)
原画像
個人情報
61a
(b)
画像変換画像
61b
81
画像暗号化
82
Bさんの公開鍵
(c)
90
公開鍵管理サーバ
Aさん
Bさん
(d)
61c
情報埋め込み画像
83
キー埋め込み
(e)
81
暗号鍵
82
Bさんの公開鍵
83
暗号鍵を公開鍵で暗号化
84
Bさんの秘密鍵
(f)
市松模様化
61d
画素値変換画像
(g)
91
プリント
印刷媒体の郵送
(h)
93
スキャン
(i)
市松模様解除
(j)
暗号鍵の取り出し
(k)
画像復号化
(l)

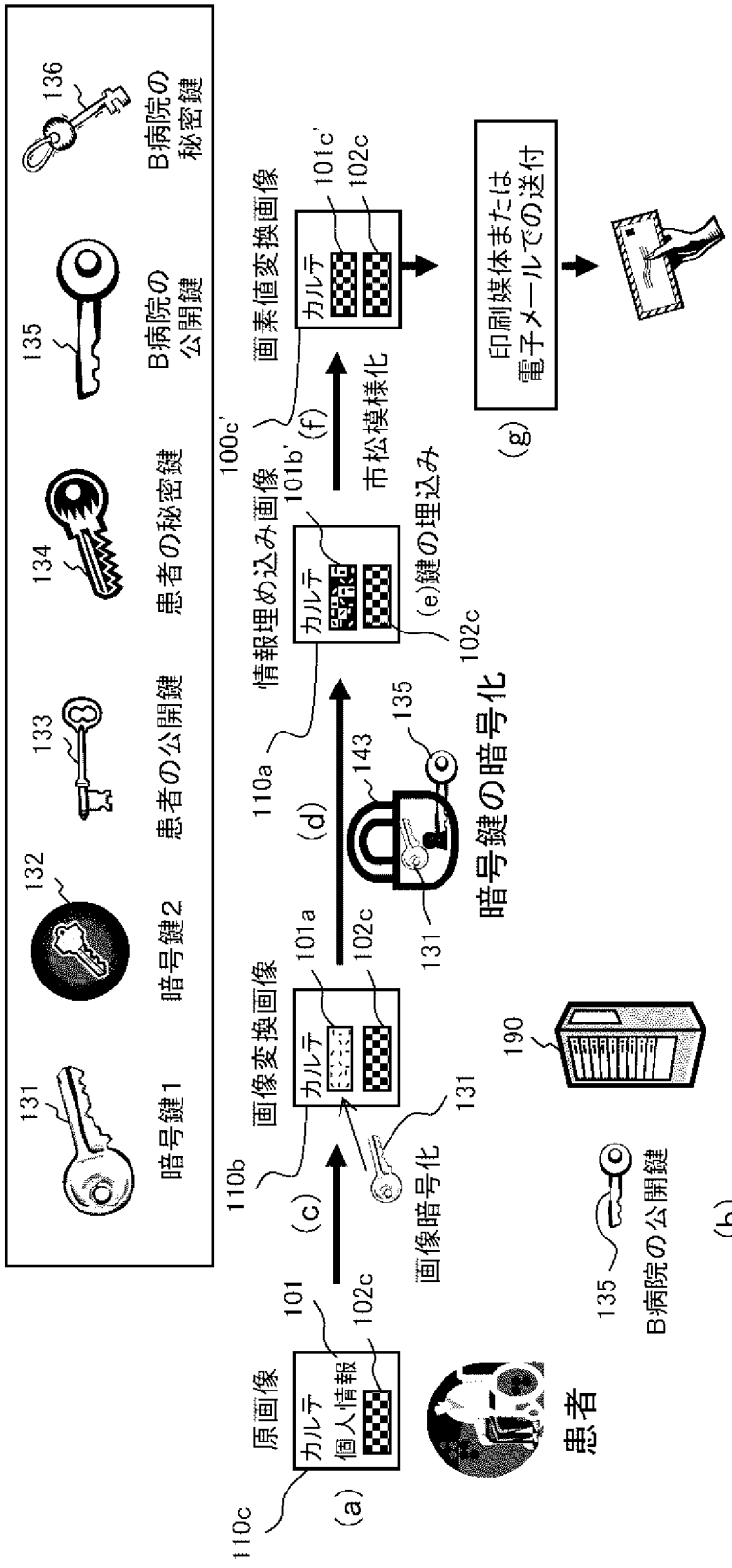
[図5]


暗号鍵1
暗号鍵2
患者の公開鍵
患者の秘密鍵
B病院の公開鍵
B病院の秘密鍵
131
132
133
134
135
136
100
原画像
カルテ
個人情報
病院情報
101
102
(a)
A病院
(b)
公開鍵管理サーバ
(c)
100a
画像変換画像
101a
102a
画像暗号化
131
134
患者の公開鍵
190
135
B病院の公開鍵
(d)
100b
情報埋め込み画像
141
133
142
暗号鍵の暗号化
135
(e) 鍵の埋込み
(f)
市松模様化
100c
画素値変換画像
101b
102b
101c
102c
(g)
印刷媒体または
電子メールでの送付

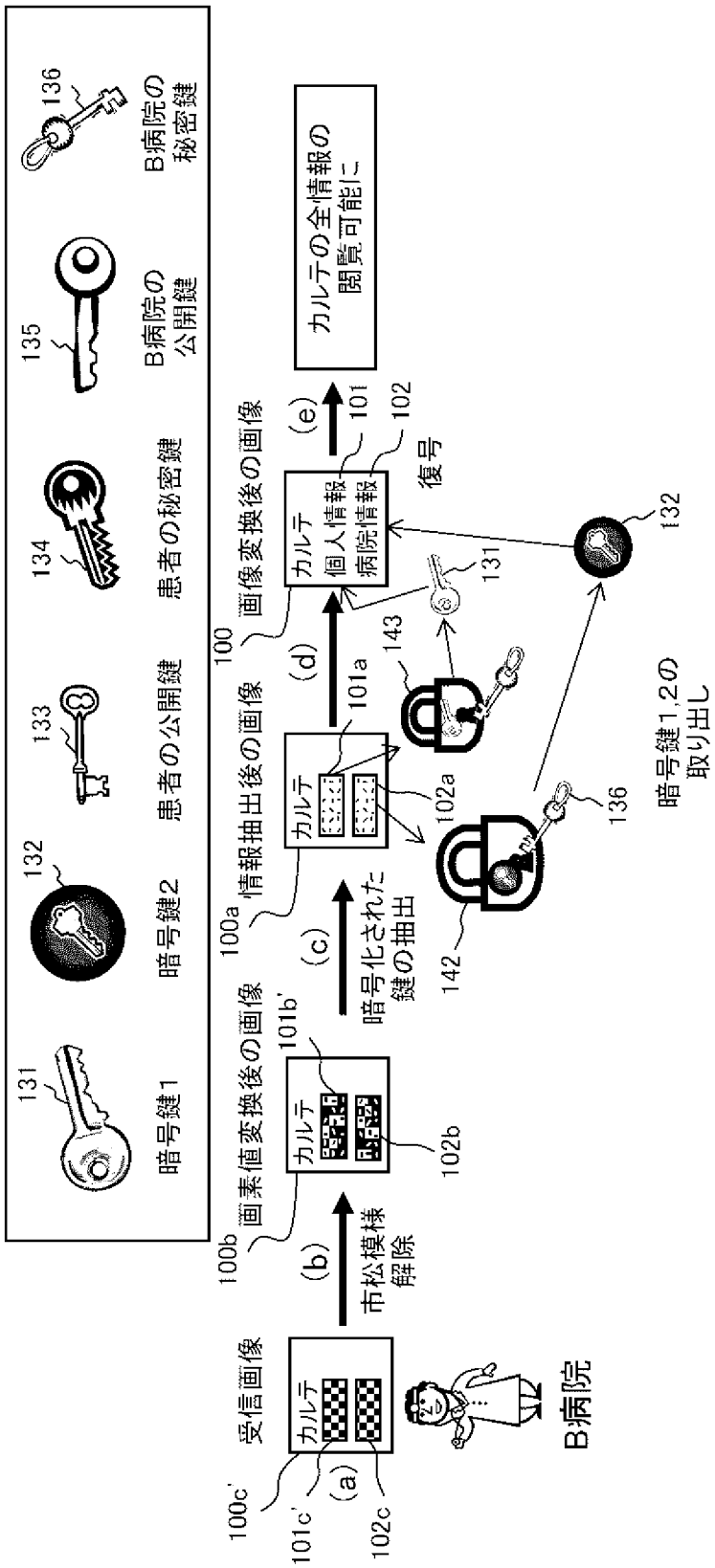
[図6]


131
暗号鍵1
132
暗号鍵2
133
患者の公開鍵
134
患者の秘密鍵
135
B病院の
公開鍵
136
B病院の
秘密鍵
(a)
(b)
(c)
(d)
(e)
(f)
(g)
100c
受信画像
101c
カルテ
102c
患者
110a
画素値変換後の画像
101b
カルテ
102c
市松模様
解除
暗号化された
鍵の抽出
110b
情報抽出後の画像
101a
カルテ
102c
141
暗号鍵1の
取り出し
134
復号
131
110c
画像変換後の画像
101f
カルテ
個人情報
102c
カルテの個人情報部
の閲覧可能に
190
135
B病院の公開鍵
公開鍵管理サーバ

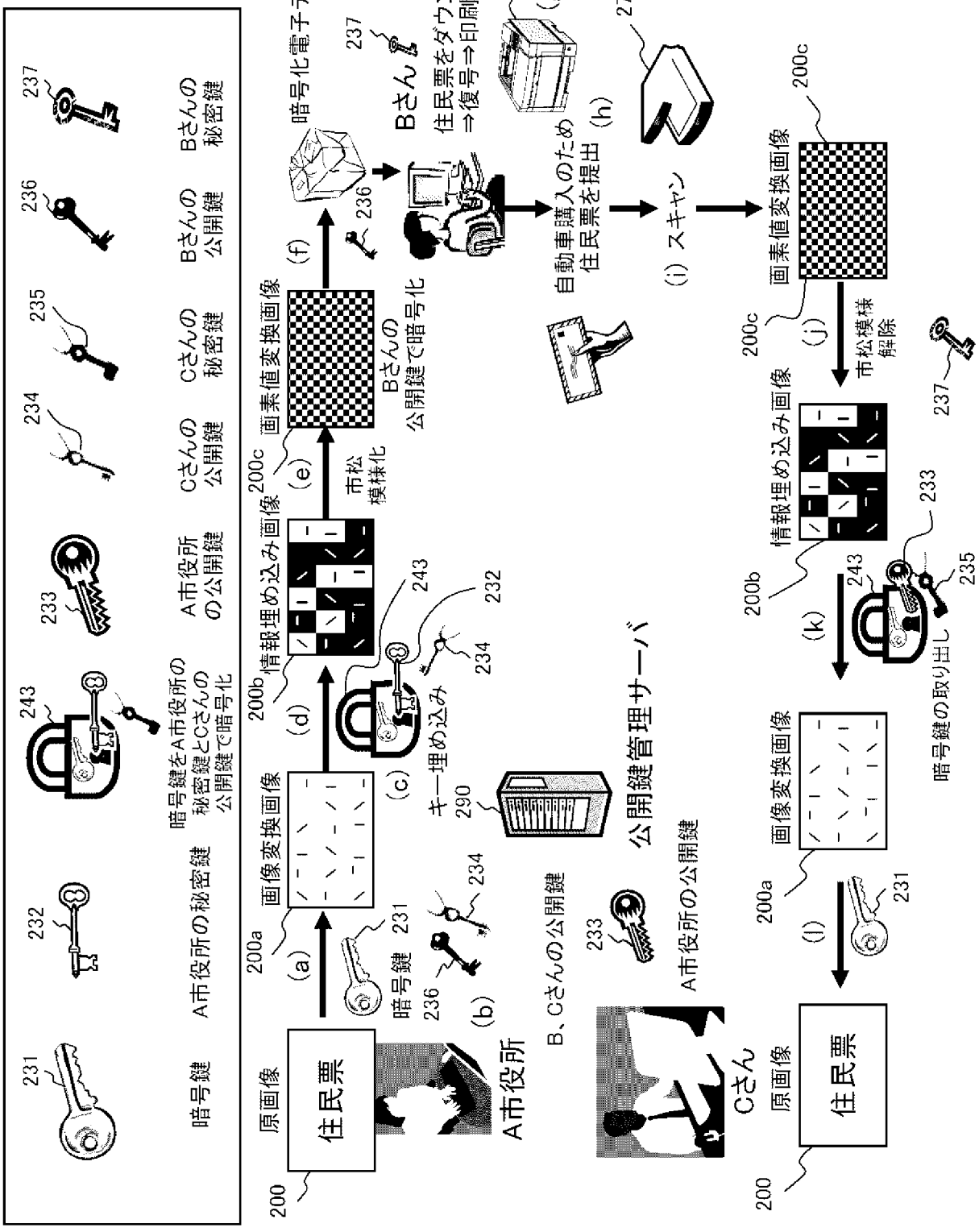
[図7]


暗号鍵1
暗号鍵2
患者の公開鍵
患者の秘密鍵
B病院の公開鍵
B病院の秘密鍵
131
132
133
134
135
136
110c
原画像
カルテ
個人情報
101
102c
(a)
患者
画像暗号化
131
110b
画像変換画像
カルテ
101a
102c
(c)
135
B病院の公開鍵
(b) 公開鍵管理サーバ
190
暗号鍵の暗号化
131
135
143
(d)
110a
情報埋め込み画像
カルテ
101b'
102c
(e)鍵の埋込み
(f)
市松模様化
100c'
画素値変換画像
カルテ
101c'
102c
(g)
印刷媒体または
電子メールでの送付

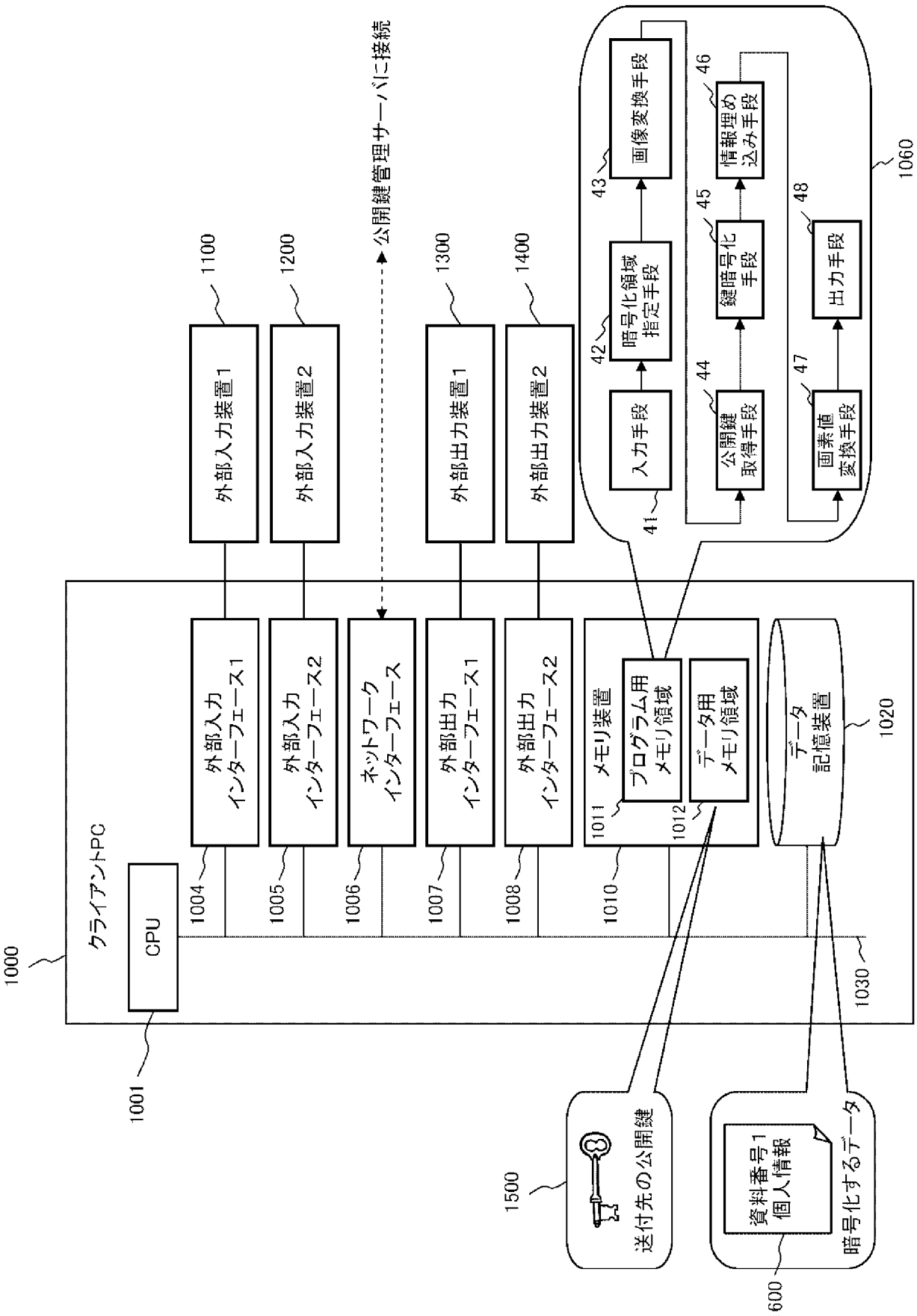
[図8]


暗号鍵1
暗号鍵2
患者の公開鍵
患者の秘密鍵
B病院の公開鍵
B病院の秘密鍵
131
132
133
134
135
136
受信画像
カルテ
(a)
(b)
市松模様解除
画素値変換後の画像
(c)
暗号化された鍵の抽出
情報抽出後の画像
(d)
画像変換後の画像
(e)
カルテの全情報の閲覧可能に
カルテ
個人情報
病院情報
復号
暗号鍵1,2の取り出し
B病院
100
100a
100b
100c'
101a
101b'
101c'
102a
102b
102c
131
132
136
142
143

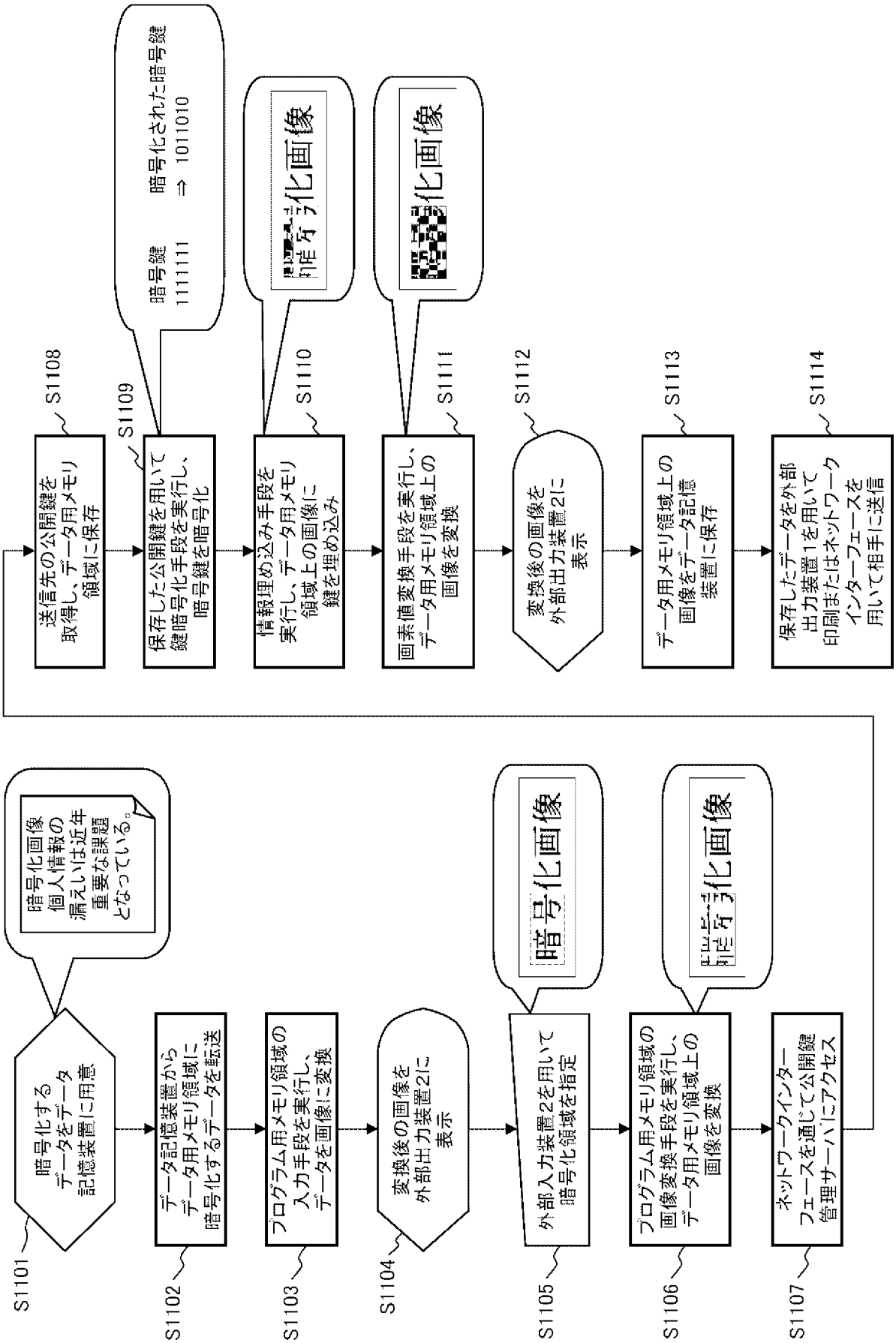
[図9]


暗号鍵
A市役所の秘密鍵
暗号鍵をA市役所の秘密鍵とCさんの公開鍵で暗号化
A市役所の公開鍵
Cさんの公開鍵
Cさんの秘密鍵
Bさんの公開鍵
Bさんの秘密鍵
231
232
233
234
235
236
237
243
200
原画像
住民票
200a
画像変換画像
(a)
暗号鍵
231
236
(b)
A市役所
キー埋め込み
290
234
232
243
(c)
200b
情報埋め込み画像
(d)
市松模様化
200c
画素値変換画像
(e)
B、Cさんの公開鍵
233
公開鍵管理サーバ
A市役所の公開鍵
Cさん
(f)
暗号化電子データ
236
237
Bさん
Bさんの公開鍵で暗号化
住民票をダウンロード
⇒復号⇒印刷
260
(g)
自動車購入のため
住民票を提出
(h)
270
(i) スキャン
200c
画素値変換画像
(j)
市松模様解除
200b
情報埋め込み画像
(k)
243
233
235
暗号鍵の取り出し
237
200a
画像変換画像
(l)
231
200
原画像
住民票

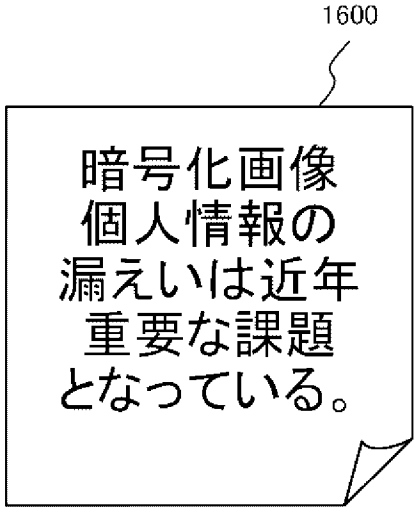
[図10]


1000
クライアントPC
CPU
1001
1004
1005
1006
1007
1008
1010
外部入力インターフェース1
外部入力インターフェース2
ネットワークインターフェース
外部出力インターフェース1
外部出力インターフェース2
メモリ装置
1011
プログラム用メモリ領域
1012
データ用メモリ領域
データ記憶装置
1020
1030
1100
1200
1300
1400
外部入力装置1
外部入力装置2
外部出力装置1
外部出力装置2
公開鍵管理サーバに接続
1060
41
入力手段
42
暗号化領域指定手段
43
画像変換手段
44
公開鍵取得手段
45
鍵暗号化手段
46
情報埋め込み手段
47
画素値変換手段
48
出力手段
1500
送付先の公開鍵
1600
資料番号1
個人情報
暗号化するデータ

[図11]

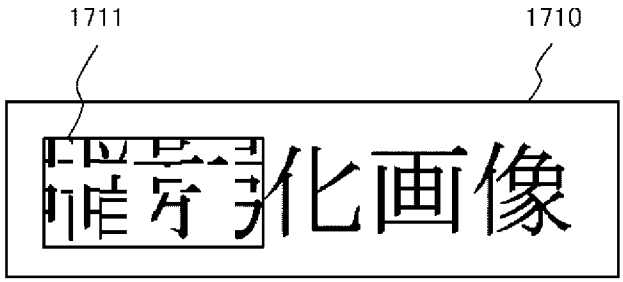

暗号化する
データをデータ
記憶装置に用意
暗号化画像
個人情報の
漏えいは近年
重要な課題
となっている。
S1101
データ記憶装置から
データ用メモリ領域に
暗号化するデータを転送
S1102
プログラム用メモリ領域の
入力手段を実行し、
データを画像に変換
S1103
変換後の画像を
外部出力装置2に
表示
S1104
外部入力装置2を用いて
暗号化領域を指定
S1105
暗号化画像
プログラム用メモリ領域の
画像変換手段を実行し、
データ用メモリ領域上の
画像を変換
S1106
暗号化画像
ネットワークインター
フェースを通じて公開鍵
管理サーバにアクセス
S1107
送信先の公開鍵を
取得し、データ用メモリ
領域に保存
S1108
保存した公開鍵を用いて
鍵暗号化手段を実行し、
暗号鍵を暗号化
S1109
暗号鍵 暗号化された暗号鍵
1111111 ⇒ 1011010
情報埋め込み手段を
実行し、データ用メモリ
領域上の画像に
鍵を埋め込み
S1110
暗号化画像
画素値変換手段を実行し、
データ用メモリ領域上の
画像を変換
S1111
暗号化画像
変換後の画像を
外部出力装置2に
表示
S1112
データ用メモリ領域上の
画像をデータ記憶
装置に保存
S1113
保存したデータを外部
出力装置1を用いて
印刷またはネットワーク
インターフェースを
用いて相手に送信
S1114

[図12]

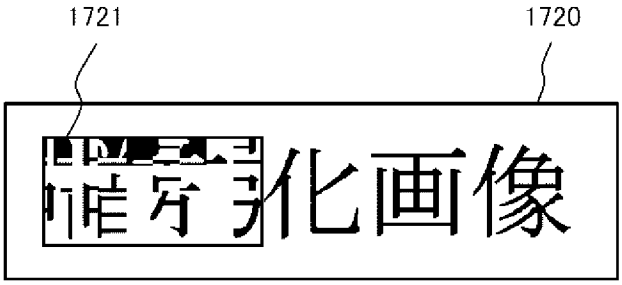


[図13]

[図14]

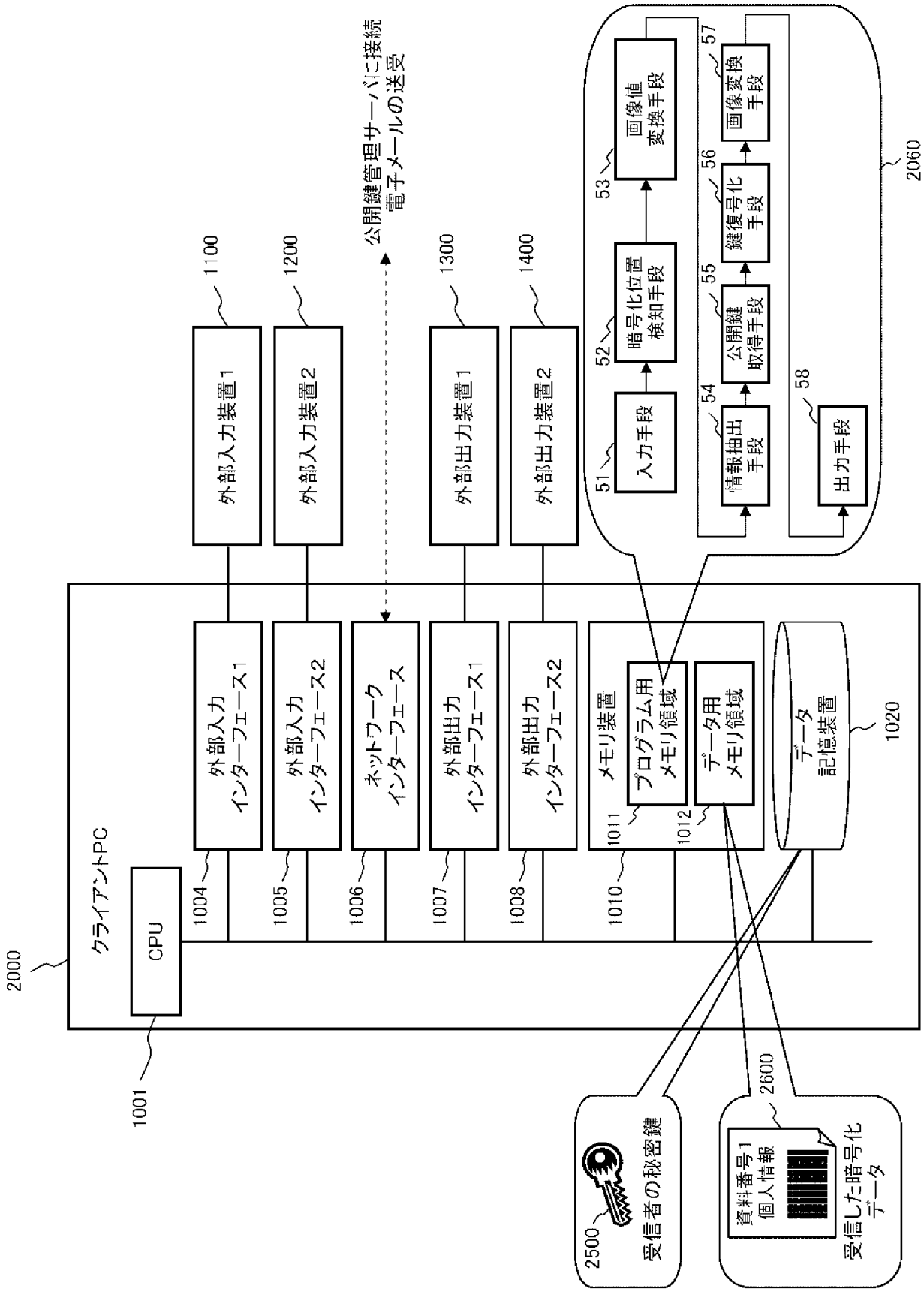


[図15]

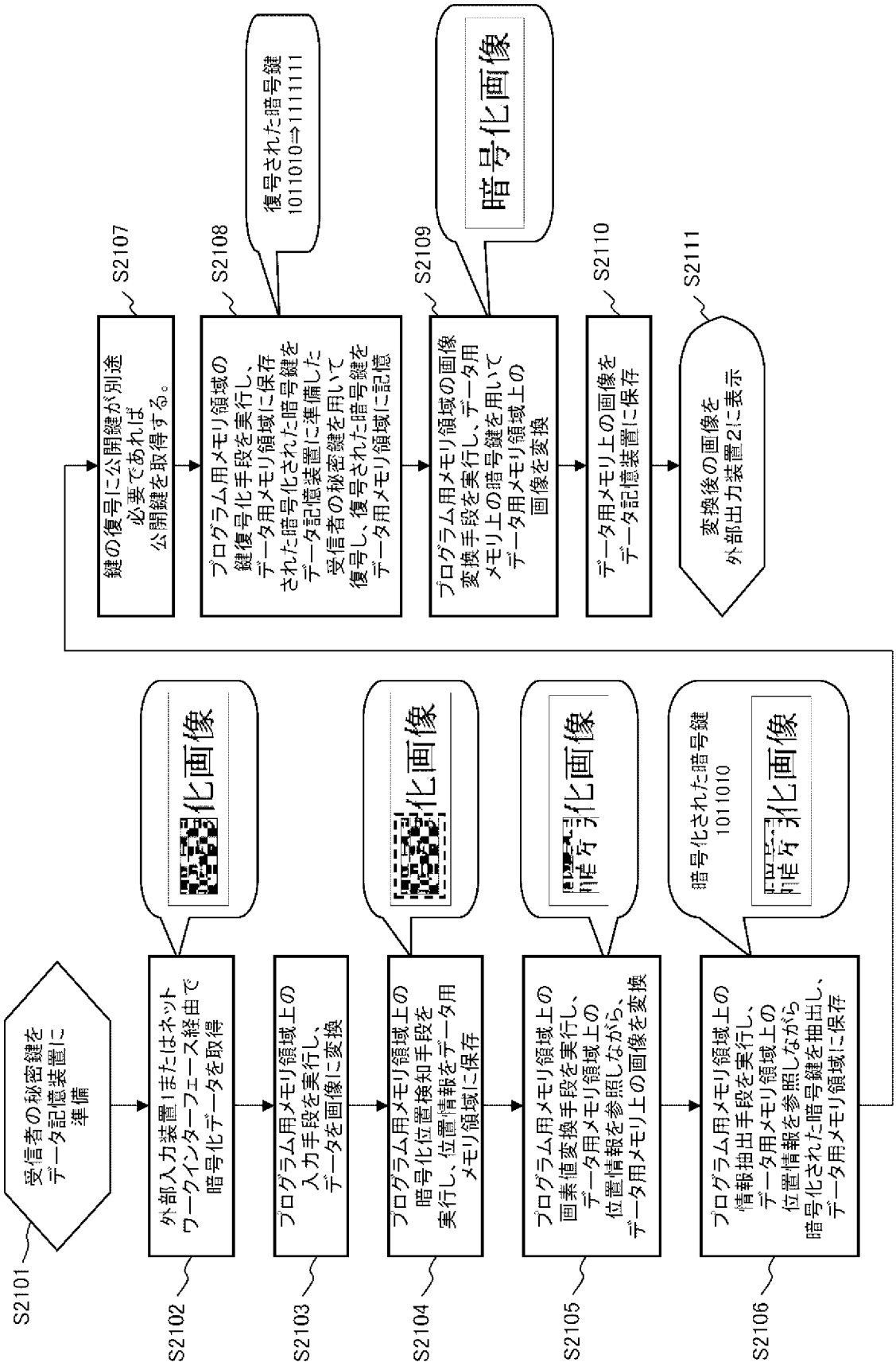


[図16]

[図17]


2000
クライアントPC
CPU
1001
外部入力インターフェース1
1004
外部入力インターフェース2
1005
ネットワークインターフェース
1006
外部出力インターフェース1
1007
外部出力インターフェース2
1008
メモリ装置
1010
プログラム用メモリ領域
1011
データ用メモリ領域
1012
データ記憶装置
1020
外部入力装置1
1100
外部入力装置2
1200
公開鍵管理サーバに接続
電子メールの送受
外部出力装置1
1300
外部出力装置2
1400
2060
入力手段
51
暗号化位置検知手段
52
画像値変換手段
53
情報抽出手段
54
公開鍵取得手段
55
鍵復号化手段
56
画像変換手段
57
出力手段
58
2500
受信者の秘密鍵
2600
資料番号1
個人情報
受信した暗号化データ

[図18]


受信者の秘密鍵をデータ記憶装置に準備
S2101
外部入力装置1またはネットワークインターフェース経由で暗号化データを取得
S2102
プログラム用メモリ領域上の入力手段を実行し、データを画像に変換
S2103
プログラム用メモリ領域上の暗号化位置検知手段を実行し、位置情報をデータ用メモリ領域に保存
S2104
プログラム用メモリ領域上の画素値変換手段を実行し、データ用メモリ領域上の位置情報を参照しながら、データ用メモリ上の画像を変換
S2105
プログラム用メモリ領域上の情報抽出手段を実行し、データ用メモリ領域上の位置情報を参照しながら暗号化された暗号鍵を抽出し、データ用メモリ領域に保存
S2106
暗号化された暗号鍵
1011010
暗号化画像
暗号化画像
暗号化画像
鍵の復号に公開鍵が別途必要であれば公開鍵を取得する。
S2107
プログラム用メモリ領域の鍵復号化手段を実行し、データ用メモリ領域に保存された暗号化された暗号鍵を用いてデータ記憶装置に準備した受信者の秘密鍵を用いて復号し、復号された暗号鍵をデータ用メモリ領域に記憶
S2108
復号された暗号鍵
1011010⇒1111111
プログラム用メモリ領域の画像変換手段を実行し、データ用メモリ領域上の暗号鍵を用いてデータ用メモリ領域上の画像を変換
S2109
暗号化画像
データ用メモリ上の画像をデータ記憶装置に保存
S2110
変換後の画像を外部出力装置2に表示
S2111

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/000581

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *G06F21/24*(2006.01)i, *G09C5/00*(2006.01)i

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)
H04L9/08, G06F21/24, G09C5/00

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 1996-2007
Kokai Jitsuyo Shinan Koho 1971-2007 Toroku Jitsuyo Shinan Koho 1994-2007

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.
A	JP 2005-107802 A (Canon Sales Co., Inc.), 21 April, 2005 (21.04.05), Par. Nos. [0056] to [0065]; Fig. 6 (Family: none)	1-32
A	JP 2003-264543 A (Oki Electric Industry Co., Ltd.), 19 September, 2003 (19.09.03), Abstract (Family: none)	1-32
A	JP 2000-315998 A (Hirokazu OKANO et al.), 14 November, 2000 (14.11.00), Par. Nos. [0008], [0009] & US 6839844 B1	1-32

☒ 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 July, 2007 (04.07.07)	17 July, 2007 (17.07.07)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/000581

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Michiharu NIIMI, Hideki NODA, Eiji KAWAGUCHI, "Zatsuondo ni yoru Ryoiki Bunkatsu o Riyo shita Junkagyaku Gazo Asshuku Ho", IEICE Technical Report IE99-122, Vol.99, No. 610, 03 February, 2000 (03.02.00), pages 13 to 18	1-32

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００７／０００５８１

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i, G06F21/24(2006.01)i, G09C5/00(2006.01)i

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.Cl.　H04L9/08, G06F21/24, G09C5/00

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	１９７１－２００７年
日本国実用新案登録公報	１９９６－２００７年
日本国登録実用新案公報	１９９４－２００７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
A	JP 2005-107802 A（キヤノン販売株式会社）2005.04.21, 【0056】-【0065】, 図６（ファミリーなし）	1-32
A	JP 2003-264543 A（沖電気工業株式会社）2003.09.19, 要約（ファミリーなし）	1-32
A	JP 2000-315998 A（岡野博一 他）2000.11.14, 【0008】, 【0009】& US 6839844 B1	1-32

☑　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 ０４．０７．２００７	国際調査報告の発送日 １７．０７．２００７
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）　５Ｓ　３３６５ 速水　雄太 電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　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
A	新見道治，野田秀樹，河口英二，雑音度による領域分割を利用した準可逆画像圧縮法，電子情報通信学会技術研究報告 IE99-122，Vol. 99，No. 610，2000.02.03，pp. 13-18	1-32