(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5 月8 日 (08.05.2008)

PCT

(10) 国際公開番号
WO 2008/053545 A1

(51) 国際特許分類:
H04N 1/387 (2006.01) *H04N 1/44* (2006.01)
G09C 5/00 (2006.01)

(21) 国際出願番号: PCT/JP2006/321794

(22) 国際出願日: 2006 年10 月31 日 (31.10.2006)

(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).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 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). 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). 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).

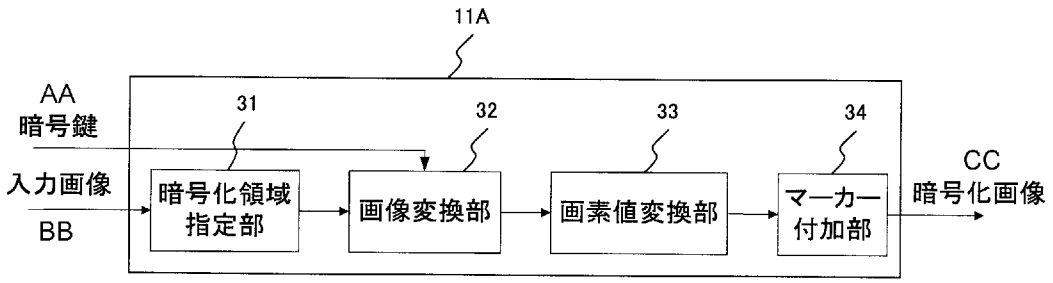
(74) 代理人: 大菅 義之 (OSUGA, Yoshiyuki); 〒1020084 東京都千代田区二番町８番地２０ 二番町ビル３Ｆ Tokyo (JP).

(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, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, 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.

[続葉有]

(54) **Title:** IMAGE ENCRYPTION/DECRYPTION DEVICE, METHOD AND PROGRAM

(54) 発明の名称: 画像暗号化／復号化装置、方法およびプログラム



AA... ENCRYPTION KEY
BB... INPUT IMAGE
31... ENCRYPTION REGION SPECIFYING UNIT
32... IMAGE CONVERSION UNIT
33... PIXEL VALUE CONVERSION UNIT
34... MARKER APPENDING UNIT
CC... ENCRYPTED IMAGE

(57) **Abstract:** An image encryption/decryption device is provided with a means for encrypting a part of an input image, regularly converting a pixel value in an encryption region in order to enable identification of the encryption region at a time of decryption and generating a specific pattern in response to the pixel value conversion, a means for appending a positioning marker for identification of an encryption position to at least two or more out of four corners in the encryption region and a means for appending at least one check mark for a validity test of a decrypted image within the encryption region before the encryption processing.

(57) 要約: 入力画像の一部分を暗号化して、復号化時に暗号化した領域を特定可能にするために、暗号化領域の画素値を規則的に変換し、画素値変換に対応した特有の模様を生成することで暗号化する手段、暗号化位置を特定するための位置決めマーカーを、暗号化領域の四隅のうち少なくとも２つ以上に付加する手段、および、復号化画像の妥当性を検証するためのチェック用マークを、暗号化処理の前に暗号化領域内に少なくとも１つ付加する手段を備える。

WO 2008/053545 A1

(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, 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／復号化装置、方法およびプログラム

技術分野

[0001] 本発明は、印刷物に印刷された画像やデジタル画像において、重要な部分等の画像の一部を視覚的に暗号化し、第三者への情報漏洩を防止する画像の暗号化および復号化の技術に関するものである。

背景技術

[0002] 社会の情報化が進む中で、秘密情報の漏洩が深刻な問題となっており、情報漏洩を防ぐ技術の開発が望まれている。例えばデジタルデータに関しては、第三者に情報が渡ってもその内容を見られないようにデータを暗号化する技術が開発され、情報漏洩を防ぐ有用な手段として既に利用されている。

[0003] 一方で、紙媒体等に印刷された印刷物の情報漏洩を防ぐ技術はまだ十分に開発されておらず、実用化された例もない。実際、約半分の情報漏洩が印刷物からであるとも言われており、デジタルデータと同様に印刷物からの情報漏洩を防ぐ技術の開発が急務となっている。

[0004] 印刷物の情報漏洩対策が望まれる具体例として、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、名簿などがあり、本発明は例えばこれらの重要な部分を暗号化して情報漏洩を防ぐ技術として利用可能である。

[0005] 従来、印刷物の暗号化を扱った公知例として、例えば、日本国特許公開公報特開平8－179689号公報（以下、特許文献1という。）がある。この特許文献1では、まず画像全体を複数のブロックに分割し、入力パスワード（暗号鍵）から得られるパラメータに基づき分割ブロックの画像を並び替え、さらにパラメータで指定されるブロックの画像を白黒反転およびミラー反転して画像を暗号化する。そして、暗号化画像を復号化する際は、画像の外側に位置決め用の枠を付加しパスワード（復号鍵）を入力後、暗号化と逆の手順で元の画像を復号化する。

[0006] また、他の従来技術として、例えば、特許第2938338号公報（以下、特許文献2という。）のように、バイナリデータを印刷物に画像化して埋め込む技術がある。この従

来技術においての画像化は、バイナリデータを指定の大きさの白黒の方形で表しマトリックス状に並べることで実現される。さらに、復号の際に画像化された位置がわかるように、印刷物には位置決め用のシンボルがマトリックスの指定の位置に付加される。この位置決めシンボルを基準とすることで、スキャナやカメラなどで画像を撮影し埋め込まれた情報を復号することが可能となる。

発明の開示

[0007] しかしながら、上述のような従来の技術においては、解決すべき以下の課題がある。

例えば、特許文献1のような技術は、画像全体にしか暗号化を適用することができず、暗号化が必要な領域が画像全体のほんの一部である場合に効率的な暗号化が行なえないという問題点があった。

[0008] さらに、特許文献1のような技術は、暗号化画像の外側に位置決め用の枠を付け加える必要があるため、枠を付加した部分にもともとあった画像情報が暗号化の際に犠牲になってしまうという問題点があった。

[0009] また、特許文献1のような技術は、画像内部の歪みが考慮されていないことにより、画像が大きくなるにつれ、スクランブルのブロック単位が正確に抽出できないという問題点があった。

[0010] 本発明では、画像全体の一部を暗号化することが可能であり、また上記特許文献1のような「位置決め枠」に対応するものを入力画像の画素値変換処理により生成するため、入力画像の情報の損失を最小限に抑えることができる。更に、スクランブルブロック単位が容易に検出できる特徴がある。

[0011] また、特許文献2のような技術は、テキスト情報など比較的情報量の少ないデータを埋め込むことはできるが、画像や音声情報などの情報量が多く、かつ復号誤りが多少起こっても差し支えのないデータを格納する場合には適していない。さらに、一定の大きさかつ正方形であることという縛りがあり、文字の一部を隠すといったアプリケーションに用いることができなかったという問題点があった。

[0012] さらに、特許文献2のような技術は、白黒の文字や図であることが前提であり、写真のような多階調をもつ画像には適用できないという問題点があった。

本発明は、上記特許文献2のような技術では暗号化が不可能な情報量の大きい画像データを、人間が視覚的にわからないように暗号化することが可能である。

[0013] 本発明では、入力画像の一部分を暗号化して、復号化時に暗号化した領域を特定可能にするために以下の3つの手段を用いる。

1つ目の手段は、暗号化領域の画素値を規則的に変換し、画素値変換に対応した特有の模様を生成することで暗号化する手段である。

[0014] 2つ目の手段は、暗号化位置を特定するための位置決めマーカーを、暗号化領域の四隅のうち少なくとも2つ以上に付加する手段である。

3つ目の手段は、復号化画像の妥当性を検証するためのチェック用マークを、暗号化処理の前に暗号化領域内に少なくとも1つ付加する手段である。

[0015] 本発明は、これら3つの手段により、入力画像の一部分を暗号化した場合でも、復号化時に暗号化した領域を正しく特定することができ、元の画像を人間が視覚的にわかるように復元することが可能となる。

[0016] すなわち、本発明の一態様によれば、本発明は、デジタル画像を暗号化画像に暗号化する画像暗号化装置において実行される画像暗号化であって、前記デジタル画像から暗号化する部分領域を指定し、前記選択された部分領域を暗号鍵に基づいて処理画像に変換し、前記部分領域の位置を特定可能にするために、前記変換された処理画像の画素値を規則的に変換することにより変換画像を生成することを特徴とする。

[0017] また、前記処理画像への変換は、前記部分領域を複数の微小領域に分割し、分割した複数の微小領域を前記暗号鍵に基づいて並べ替えるか、あるいは、前記部分領域を任意の圧縮方法で圧縮データに変換し、前記変換された圧縮データの各ビットを任意の大きさの白画素または黒画素として配列することが望ましい。

[0018] また、前記変換画像への変換は、前記処理画像の横方向に関して一定の周期で前記画素値を変換し、縦方向に関して一定の周期で前記画素値を変換することにより、概ね縞状の模様を成すような変換画像を生成することが望ましい。

[0019] また、前記部分領域の位置を特定するために、特定のマーカーを前記生成された変換画像に付加することにより前記暗号化画像を生成することが望ましい。

また、前記マーカーは、実線の円形状または多角形状であり、その内側に円形状または多角形の周と交わる線が複数存在する形状であるか、あるいは、前景が画素値変換により形成されることが望ましい。

[0020] また、本発明の一態様によれば、本発明は、暗号化画像をデジタル画像に復号化する画像復号化装置において実行される画像復号化であって、暗号化した部分領域の位置を特定するために、前記暗号化画像に付加された特定のマーカーを検出し、前記検出されたマーカーに基づいて、暗号化された暗号化画像領域を検出し、前記検出された暗号化画像領域のうち画素値が規則的に変換されている暗号化位置を検出し、前記検出された暗号化位置と復号鍵とに基づいて前記暗号化画像領域を前記デジタル画像に復号することを特徴とする。

[0021] また、本発明の一態様によれば、本発明は、暗号化画像をデジタル画像に復号化する画像復号化装置において実行される画像復号化であって、暗号化された暗号化画像領域を検出し、前記検出された暗号化画像領域のうち画素値が規則的に変換されている暗号化位置を検出し、前記検出された暗号化位置と復号鍵とに基づいて前記暗号化画像領域を前記デジタル画像に復号し、前記復号された前記デジタル画像から復号化の妥当性を検証するための特定のチェック用マークを検出することを特徴とする。

[0022] また、本発明の一態様によれば、本発明は、暗号化画像をデジタル画像に復号化する画像復号化装置において実行される画像復号化であって、暗号化した部分領域の位置を特定するために、前記暗号化画像に付加された特定のマーカーを検出し、前記検出されたマーカーに基づいて、暗号化された暗号化画像領域を検出し、前記検出された暗号化画像領域のうち画素値が規則的に変換されている暗号化位置を検出し、前記検出された暗号化位置と復号鍵とに基づいて前記暗号化画像領域を前記デジタル画像に復号し、前記復号された前記デジタル画像から復号化の妥当性を検証するための特定のチェック用マークを検出することを特徴とする。

[0023] 本発明では、特許文献1の技術のように暗号化画像の外側に位置決め用の枠を付加することで起こる画像情報の損失の問題を、暗号化領域の画素値を規則的に変換し、画素値変換に対応した特有の模様を生成する手段により解決する。暗号化領域

に文字などのエッジを持つ画像があると、上記の処理で得られる暗号化画像の模様の形は完全ではなくなるが、暗号化画像全体の統計的な性質を利用することで暗号化位置を正しく検出することできる。

[0024] さらに本発明における暗号化処理において、画素値の変換により生成する暗号化位置検出用の規則的な模様がある程度の幅を持っているため、暗号化画像を低解像度のカメラで読み込んだ場合でも暗号化位置を正しく検出することができ復号化できる。また、画像を圧縮して暗号化する方法を併用すれば、スキャナやカメラの解像度に依存しない画質の復号化画像が実現可能である。

図面の簡単な説明

[0025] [図1]本発明を適用した実施の形態の処理概要(その1)を示す図である。

[図2]本発明を適用した実施の形態の処理概要(その2)を示す図である。

[図3]第1の実施の形態における暗号化処理の概要を示す図である。

[図4]暗号化領域を選択する例を示す図である。

[図5]暗号鍵の入力例を示す図である。

[図6]画像変換部におけるスクランブル処理を示す図である。

[図7]画像変換部における圧縮処理を示す図である。

[図8]変換データを画像化する処理を示す図である。

[図9]画素値変換部における画素値変換処理の例(その1)を示す図である。

[図10]画素値変換部における画素値変換処理の例(その2)を示す図である。

[図11]暗号化処理で用いる位置決めマーカーの例を示す図である。

[図12]暗号化画像の例を示す図である。

[図13]グレースケール画像の暗号化の例を示す図である。

[図14]第1の実施の形態における復号化処理の概要を示す図である。

[図15]位置決めマーカーから暗号化領域を検出する過程を示す図である。

[図16]暗号化領域検出処理の流れを示すフローチャートである。

[図17]暗号化位置が検出された例を示す図である。

[図18]第2の実施の形態の全体イメージを示す図である。

[図19]第2の実施の形態における暗号化処理の概要を示す図である。

[図20]第2の実施の形態における復号化処理の概要を示す図である。

[図21]暗号化領域の検出方法を説明するための図である。

[図22]暗号化位置(横方向)の検出方法を説明するための図である。

[図23]暗号化位置の検出を誤った例を示す図である。

[図24]第3の実施の形態における暗号化処理の概要を示す図である。

[図25]第3の実施の形態における復号化処理の概要を示す図である。

[図26]本発明における暗号化処理および復号化処理を実行する処理装置の構成図である。

[図27]本発明における暗号化および復号化プログラムのコンピュータへのローディングを説明するための図である。

発明を実施するための最良の形態

[0026] 以下、図面に基づいて本発明を適用した実施の形態を説明する。

まず、図1および図2を用いて、本発明を適用した第1の実施の形態乃至第3の実施の形態における暗号化処理および復号化処理の概要を説明する。

[0027] 図1は、本発明を適用した実施の形態の処理概要(その1)を示す図である。

図1において、暗号化部11(第1乃至第3の各実施の形態においては、それぞれ暗号化部11A、11B、11Cという。)は、入力されたデジタル画像と暗号化方法を示す暗号鍵とに基づいて、前記デジタル画像の一部を暗号化した暗号化画像を出力する。プリンタ出力部12は、暗号化部11により暗号化されたデジタル画像を紙などの印刷可能な物理的媒体に印刷する。スキャナ(カメラ)読み込み部13は、プリンタ出力部12により出力された印刷画像を、スキャナまたはカメラを用いて読み込む。

[0028] そして、復号化部14(第1乃至第3の各実施の形態においては、それぞれ復号化部14A、14B、14Cという。)は、プリンタ出力部12により出力された印刷画像と入力された復号鍵とにより復号化画像を得る。この入力された復号鍵が正しい場合に限り暗号化画像を適切に復号化でき、暗号化部11による暗号化で隠された情報を見ることができる。

[0029] 図2は、本発明を適用した実施の形態の処理概要(その2)を示す図である。

図2に示したように、本発明を適用した第1の実施の形態乃至第3の実施の形態に

おける暗号化処理および復号化処理は、暗号化部11により暗号化されたデジタル画像をプリンタやスキャナを介さずに電子文書画像のまま復号化部14に入力し、復号化画像を得ることも可能である。

[0030] 次に、本発明を適用した第1の実施の形態乃至第3の実施の形態をそれぞれ説明する。

まず、本発明を適用した第1の実施の形態について説明する。

図3は、第1の実施の形態における暗号化処理の概要を示す図である。

[0031] 図3において、暗号化部11Aは、暗号化領域決定部31、画像変換部32、画素値変換部33およびマーカー付加部34を備えている。

暗号化領域指定部31は、暗号化したい領域を含む入力画像から暗号化する領域を選択する。

[0032] 図4は、暗号化領域を選択する例を示す図である。

すなわち、暗号化領域指定部31は、図4の(A)に示すように、暗号化したい領域を含むデジタル画像(入力画像)41から暗号化する領域42を選択する。この領域42が後述する画像変換部32および画素値変換部33の処理により、図4の(B)に示したように変換画像43に変換され、デジタル画像41が変換画像43を含む暗号化画像44に変換される。

[0033] 図3の説明に戻る。

暗号化領域指定部31により暗号化する領域42が選択されると、画像変換部32において暗号化する領域42および暗号鍵を入力し、暗号鍵に対応する変換方法で暗号化する領域42の画像を視覚的に変換する。その際の変換パラメータは、入力の暗号鍵から得られるバイナリデータにより作成する。

[0034] 図5は、暗号鍵の入力例を示す図である。

図5に示した例は、暗号鍵と、暗号鍵により生成されるバイナリデータの例である。例えば、暗号鍵としての数値「1234」は、バイナリデータ「100011010010」として入力され、暗号鍵としての文字列「ango」は、バイナリデータ「011000010110111001100111101101111」として入力される。

[0035] 画像変換方法として、本第1の実施の形態では、画像を微小領域に分割して微小

領域を並べ替える処理（スクランブル処理という。）による変換方法と、画像を圧縮処理することによる変換方法の2つを示す。

[0036] まず、スクランブル処理について説明する。

スクランブル処理は、まず、選択された領域42の画像を一定の大きさの微小領域に分割して、次に、暗号鍵から得られるバイナリデータにより微小領域の並び替えを行なう。

[0037] 図6は、画像変換部におけるスクランブル処理を示す図である。

図6の（A）に示したように、まず暗号化領域指定部31により選択された領域42を縦方向に分割し、暗号鍵61のバイナリ列の各ビットを分割された領域42の境界に左から順に対応させ、ビットが「1」の場合は隣り合う分割列を交換し、ビットが「0」の場合は何もしない処理を左側から順に行なう。分割境界の数に対してバイナリ列のビット数が足りない場合は、足りなくなった位置から同じバイナリ列を繰り返して領域42の右端まで交換処理を行なう。

[0038] 続いて、図6の（B）に示すように、上記交換処理を行なった画像領域62を横方向に分割し、暗号鍵61のバイナリ列の各ビットを分割された画像領域62の境界に上から順番に対応させ、縦分割で行ったのと同様の交換処理を行単位で上から順に行なう。

[0039] すると、図6の（C）に示すように、各分割画像に交換処理を行った結果、元の領域42がスクランブル処理された処理画像であるスクランブル画像63が得られる。

この交換処理の拡張法として、横方向、縦方向ともに2度以上行なうこともでき、また2度目以降の交換において分割領域の大きさを変えることも可能である。さらに、横方向と縦方向で分割領域の交換に別のバイナリ列を用いることもできる。これらの拡張法は、入力画像のサイズが小さく、かつ暗号鍵のビット長が長い場合に、異なる暗号鍵から全く同じ処理画像が生成されてしまうのを防ぐ手段として特に有効である。

[0040] 次に、画像を圧縮処理することによる変換方法について説明する。

図7は、画像変換部における圧縮処理を示す図である。

入力画像41が二値画像の場合に、まず図7の（A）に示したように暗号化領域指定部31により選択された領域42の画像を圧縮して、図7の（B）に示したようなバイナリ

列71を作成する。ここでの圧縮法は、ファクシミリ装置での二値画像データ転送の際に用いられるランレングス圧縮や、二値画像の標準圧縮方式であるJBIG（Joint Bi-level Image experts Group）圧縮など、あらゆる圧縮方式が適用可能である。

[0041] 図8は、変換データを画像化する処理を示す図である。

図7に示したような領域42の圧縮に続いて、変換圧縮データであるバイナリ列71の各ビットを、図8（B）に示したように、ビットが「0」ならば「白」、ビットが「1」ならば「黒」である指定サイズの方形に拡大して方形画像（処理画像）81を作成し、暗号化する画像の領域42に白黒の方形画像81として配列させる。

[0042] 変換圧縮データ（バイナリ列71）を選択された領域42の画像内に収まるよう配列させたい場合、方形画像81のサイズは選択された領域42の圧縮率に依存してくる。例えば圧縮率が1／4以下であれば方形画像81のサイズは高々2×2ピクセルであり、1／16以下ならば高々4×4ピクセルである。

[0043] 一方、予め方形画像81のサイズを指定し、かつ圧縮データを選択された領域42の画像内に収めたい場合は、最初の画像圧縮処理において方形画像81のサイズに依存した圧縮率を達成する必要がある。例えば方形を4×4ピクセルのサイズにする場合は1／16以上の圧縮率が必要となる。この場合には、選択された領域42の情報を予め落として圧縮する方法や、非可逆な圧縮方式を用いる方法が有効である。

[0044] 上記の圧縮データを拡大して画像化する暗号化処理により、例えば低解像度のカメラで暗号化画像を読み取った場合でも拡大された白黒のブロックを認識できるため、暗号化画像を正しく復号できる。

[0045] 図3の説明に戻る。

画素値変換部33では、画像変換部32で変換された処理画像63内の画素を一定の間隔を置いて変換し、変換画像43が概ね格子状の縞模様を成すようにする。

[0046] 図9は、画素値変換部における画素値変換処理の例（その1）を示す図である。

画素値変換部33では、画像変換部32により領域42がスクランブルされた処理画像63の画素を、一定の間隔で変換し、暗号化画像44が全体として概ね格子状の縞模様を成すようにする。例えば図9に示したように、図9の（A）に示したスクランブル画像63を（B）に示した市松模様（チェッカー模様）画像91の有色部分で反転処理する

ような変換を実行することにより、(C)に示したように暗号化画像44が全体として概ね格子状の縞模様を成す変換画像92が得られる。これにより、生成される縞状の模様は、暗号化画像44を復号する際に暗号化領域内の各画素の詳細な位置を検出するために用いられる。

[0047] これらの一連の処理に関して、別の変換を実施することも可能である。例えば画素値を反転する処理は、指定の値を加算する処理であってもよい。

また、図9の(B)に示した市松模様画像91は、(A)に示したスクランブル画像63と略同サイズであるが、スクランブル画像63より小さいサイズを用いることにより、スクランブル画像63の周辺以外の中心部分のみ反転処理するようにしてもよい。

[0048] 図10は、画素値変換部における画素値変換処理の例(その2)を示す図である。

また、画素値を変換する領域42は、図10の(A)や(B)に示したように種々の形状を適用することが可能である。例えば、図10の(B)のようにすれば、変換と非変換の境界がより細かい間隔で現れるため、復号化処理において暗号化画像44の画素位置をさらに詳細に検出できる。

[0049] 上述したように、本発明においては、暗号化位置を表す規則的な模様を、特許文献1のように入力画像に上書きして生成するのではなく、入力画像の画素値を変換することで生成している。したがって、従来の技術のように暗号化画像の端部分の画像情報が位置検出のために犠牲にされることがなく、元の画像情報に位置検出情報を共存させる形で効率よく暗号化を行なえる。

[0050] なお、模様を構成する部分に何らかの画像情報が含まれるとその規則性が多少崩れてしまうが、後述の復号化部14の処理で述べるように暗号化画像全体の統計的な性質を用いることで暗号化位置を検出することができる。

[0051] 図3の説明に戻る。

マーカー付加部34では、画素値変換部33で変換処理された変換画像92の四隅のうち、例えば右下以外の三箇所に位置決めマーカーを付加し暗号化画像44を作成する。

[0052] マーカー付加部34は、暗号化された領域42の位置を特定するための位置決めマーカーを、変換画像92の四隅のうち例えば右下以外の三箇所に配置する。

図11は、暗号化処理で用いる位置決めマーカーの例を示す図である。

[0053] 本第1の実施の形態で用いる位置決めマーカーは、図11の(A)に示すように丸十字の形をしたものとする。位置決めマーカーの形をより広く言えば、実線の円または多角形とその周と交わる複数の線で構成されるものであればよい。このような例として、図11の(B)の位置決めマーカーのように漢字の「田」の形をしたものや、(C)の位置決めマーカーのように中心から三つの線が円周に向かって放射線状に出ているもの、(D)の位置決めマーカーのように線が途中で切れているもの、などが挙げられる。

[0054] また、位置決めマーカーの色の構成は、最も単純には背景が白で前景を黒にすればよいが、これに限らず変換画像92の色(画素値)分布に応じて適宜変更しても差し支えない。また背景と前景に決まった色を指定するのではなく、背景の色はデジタル画像41のままで前景の画素値を反転するなどして位置決めマーカーを形作る方法も考えられる。このようにすれば、位置決めマーカー部分の入力画像情報も保持されたまま画像の暗号化を行なえる。

[0055] 図12は、暗号化画像の例を示す図である。

以上の暗号化部11Aの処理により、最終的には図12に示すような暗号化画像44が生成される。暗号化画像44には、変換画像92と位置決めマーカー121が含まれる。

[0056] さらに、本第1の実施の形態の暗号化方法において、画像変換部32で「微小領域を並べ替える処理(スクランブル処理)」を用いた場合は、二値画像だけでなくグレースケールやカラーの画像に対しても暗号化処理を適用できる。

[0057] 図13は、グレースケールの画像を暗号化した例である。

図13において、(A)に示したグレースケール画像131は、暗号化部11Aの処理により、(B)に示すように変換画像133と位置決めマーカー134を含む暗号化画像132が生成される。

[0058] 次に、復号化部14Aの説明を行なう。

図14は、第1の実施の形態における復号化処理の概要を示す図である。

図14において、復号化部14Aは、マーカー検出部141、暗号化領域検出部142、

暗号化位置検出部143および画像逆変換部144を備えている。

[0059] マーカー検出部141は、一般的な画像認識技術を用いて、上述のマーカー付加部34により付加した位置決めマーカーの位置を暗号化画像から検出する。検出方法としては、パターンマッチングや図形の連結性に関する解析などが適用可能である。

[0060] 暗号化領域検出部142は、マーカー検出部141により検出された3つの位置決めマーカーの位置関係に基づいて、暗号化されている画像の領域を検出する。

図15は、位置決めマーカーから暗号化領域を検出する過程を示す図である。

[0061] 図15の(A)に示されたように、マーカー検出部141によって暗号化画像151から少なくとも3つの位置決めマーカー152が検出されると、(B)に示すように、1つの暗号化領域153を検出することができる。すなわち、3つの位置決めマーカー152は、長方形の暗号化領域153の四隅に配置されているため、これら3つの点(位置決めマーカー152の位置)を線で結んで得られる図形はおおよそ直角三角形になる。そこで、位置決めマーカー152が3つ以上検出された場合は、3つの位置決めマーカー152の位置関係が直角三角形に近い形状で構成される領域を含み、3つの位置決めマーカー152の位置を4つの角部分のうち3つの角部分とする長方形を暗号化領域153とする。なお、検出位置決めマーカー152の数が2つ以下の場合は、対応する暗号化領域153を特定できないため、暗号化画像は存在しないとして復号化処理を終了する。

[0062] 図16は、暗号化領域検出処理の流れを示すフローチャートである。

暗号化領域検出部142で実行される暗号化領域検出処理は、まず、ステップS1601において、マーカー検出部141によって検出された位置決めマーカー152の数を変数nに代入し、ステップS1602において、暗号化領域153の検出用フラグreg_detectに0を代入する。

[0063] そして、ステップS1603において、位置決めマーカー152の数が代入された変数nが3以上であるか否かを判断し、変数nが3以上でなければ、すなわち変数nが2以下であれば(ステップS1603:No)、本暗号化領域検出処理を含む復号化処理を終了する。

[0064] 他方、変数nが3以上であれば(ステップS1603:Yes)、ステップS1604において、マーカー検出部141によって検出された位置決めマーカー152のうちの3つの位置決めマーカー152を選択し、ステップS1605において、その選択した3つの位置決めマーカー152の位置関係が略直角三角形であるか否かを判断する。

[0065] 選択した3つの位置決めマーカー152の位置関係が略直角三角形でなければ(ステップS1605:No)、ステップS1606において、マーカー検出部141によって検出された位置決めマーカー152の3点の組み合わせが全て終了したか否かを判断し、終了していなければ(ステップS1606:No)、ステップS1604に戻って他の3点を選択し、終了した場合(ステップS1606:Yes)、ステップS1608に進む。

[0066] 他方、選択した3つの位置決めマーカー152の位置関係が略直角三角形であれば(ステップS1605:Yes)、ステップS1607において、検出用フラグreg_detectに1を代入する。

[0067] そして、ステップS1608において、検出用フラグreg_detectに1が代入されているか、すなわち、3点の位置関係が直角三角形となる3つの位置決めマーカー152を検出することができたか否かを判断し、reg_detectに1が代入されていれば(ステップS1608:Yes)、暗号化位置検出部143の処理に進み、reg_detectに1が代入されていなければ(ステップS1608:No)、本暗号化領域検出処理を含む復号化処理を終了する。

[0068] 図14の説明に戻る。

暗号化位置検出部143は、暗号化画像151の復号を正確に行なうために、暗号化領域検出部142により検出された暗号化領域153の端の部分が規則的な画素分布を成すことを利用して、周波数解析やパターンマッチングなどにより暗号化領域153内の各画素の詳細な位置を検出する。この検出は、画素値変換部33の画素値変換(反転)処理により暗号化画像151の全体が周期的な模様を成すという性質を利用する。

[0069] 一つの検出方法として、まず模様の周期(幅)を画像の横方向および縦方向に関して高速フーリエ変換(Fast Fourier Transform:FFT)などの周波数解析法で求め、その後テンプレートマッチングなどによりの境界位置(オフセット)を検出する方法が考

えられる。

[0070] また、暗号化画像にエッジ検出フィルタ(ラプラシアンフィルタ等)をかけると境界部分が直線状になる性質を利用して、境界位置をハフ変換により検出することも可能である。

[0071] 図17は、暗号化位置が検出された例を示す図である。

暗号化されたデジタル画像41が複雑である場合は、暗号化画像44の周期性が著しく損なわれる部分が出てくる可能性もある。このような場合、模様の周期と境界位置の計算に用いる画像領域を周期性の比較的強い部分に限定して暗号化位置検出を行なう方法が有効である。

[0072] 図14の説明に戻る。

画像逆変換部144は、暗号化位置検出部143により検出された暗号化位置情報とユーザにより入力された復号鍵とを用いて、暗号化画像44を復号鍵に対応する方法で画像変換部32による変換処理の逆変換処理を実行し、復号化画像を生成する。復号化の処理手順は、暗号化処理と逆の手順で実現されるため説明を省略する。

[0073] 以上が本発明を適用した第1の実施の形態についての説明である。

次に、本発明を適用した第2の実施の形態について説明する。

図18は、第2の実施の形態の全体イメージを示す図である。

[0074] 第2の実施の形態は、暗号化処理の前に、暗号化画像183の復号化の妥当性を検証するための特定のチェック用マーク182を、暗号化する領域181の任意の場所に付加して(図18の(A))暗号化を行ない(図18の(B))、暗号化画像183を復号化した後に事前に付加したチェック用マーク182が復号化画像184から検出されれば正しく復号されたとして復号化処理を終了する(図18の(C))。チェック用マーク182が検出されない場合(図18の(D))は、暗号化位置を補正し、チェック用マーク182が検出されるまで、または指定の基準を満たすまで復号化処理を繰り返す。

[0075] 図19は、第2の実施の形態における暗号化処理の概要を示す図である。

図19において、暗号化部11Bは、暗号化領域決定部31、チェック用マーク付加部192、画像変換部32および画素値変換部33を備えている。

[0076] 第1の実施の形態と同様、暗号化領域指定部31は、暗号化したい領域を含む入力

画像から暗号化する領域を選択する。

そして、チェック用マーク付加部192は、暗号化画像183の復号化の妥当性を検証するための特定のチェック用マーク182を暗号化する領域181の任意の場所に付け加える。チェック用マーク182は、なるべく画像情報が少ない画素分布の平坦な領域に付加するのが望ましい。

[0077] 指定位置にチェック用マーク182を付け加えた後、第1の実施の形態と同様、画像変換部32において暗号化する領域181および暗号鍵を入力し、暗号鍵に対応する変換方法で暗号化する領域181の画像を視覚的に変換し、画素値変換部33では、画像変換部32で変換された処理画像内の画素を一定の間隔を置いて変換し、変換画像が概ね格子状の縞模様を成すようにする。

[0078] 図20は、第2の実施の形態における復号化処理の概要を示す図である。

図20において、復号化部14Bは、暗号化領域検出部201、暗号化位置検出部143、画像逆変換部144、チェック用マーク検出部204および暗号化位置補正部205を備えている。

[0079] まず初めに、暗号化領域検出部201は、暗号化画像183の大まかな領域を検出する。暗号化部11Bの暗号化処理により、暗号化画像183の画素分布はおおよそ市松模様状になっているため、それぞれ横方向と縦方向に関してFFTなどの周波数解析を行なうと、縞の周期に対応する周波数のパワーが際立って強くなる。

[0080] 図21は、暗号化領域の検出方法を説明するための図である。

図21の(A)に示したように、暗号化画像211を周波数解析すると、(B)に示すように、ある周波数(その周波数の整数倍の周波数)のパワーが突出する領域を「周期性強」214と表現している。暗号化領域内では画素分布の周期性が強くなる傾向にあるため、これにより大まかな暗号化領域と縞模様の周期を検出することができる。

[0081] 図20の説明に戻る。

暗号化位置検出部143は、暗号化領域検出部201による暗号化の大まかな領域を特定した後、暗号化領域をさらに正確に検出し、同時に暗号化領域内の各画素の詳細な位置を検出する。位置検出の一例として、まず暗号化領域検出部201で求めた縞模様の周期と画素絶対値差分の分布により画素値変換の境界位置(オフセット)

を求め、そこからさらに画素絶対値差分が相対的に大きい領域を絞り込む方法が考えられる。また、第1の実施の形態の暗号化位置検出部143と同様、暗号化位置検出にハフ変換を用いることも可能である。

[0082] 図22は、暗号化位置(横方向)の検出方法を説明するための図である。

上述のような暗号化領域の検出処理を横方向、縦方向それぞれに行なうと、図22のように暗号化位置221が検出される。

[0083] 図20の説明に戻る。

画像逆変換部144は、暗号化位置情報と復号鍵を用いて第1の実施の形態と同様の方法を行ない復号化画像を生成する。

[0084] チェック用マーク検出部204は、画像逆変換部144で復号化した復号化画像からチェック用マークの検出を試みる。検出方法は第1の実施の形態におけるマーカー検出処理と同様であるため説明を省略する。そして、チェック用マークが検出された場合は復号化画像を出力して処理を完了する。チェック用マークが検出されない場合は暗号化位置補正部205において暗号化位置を補正し、チェック用マークが検出されるまで、または指定の基準を満たすまで復号化処理(画像逆変換処理)をやり直す。

[0085] 図23は、暗号化位置の検出を誤った例を示す図である。

図23に示したように、暗号化画像の端を見落としてしまう場合(取りこぼしライン231)が考えられる。そこで、チェック用マーク221の検出に失敗した場合は、暗号化位置を表すラインを左右端と上下端に追加または削除して画像逆変換処理を行ない、チェック用マーク221が検出できるかどうかを各々検討する。ラインをどのように追加または削除してもチェック用マーク221を検出できない場合は、復号化画像を出力せずに処理を終了する。

[0086] 以上が本発明を適用した第2の実施の形態についての説明である。

次に、本発明を適用した第3の実施の形態について説明する。

本発明の第3の実施形態では、第1の実施の形態で示した暗号化領域を特定する位置決めマーカーと、第2実施の形態の復号化画像の妥当性を判断するためのチェック用マークの両方を用いて画像の暗号化、復号化を行なう。これら位置検出用の位

置決めマーカーと復号化画像確認用のチェック用マークの2種類を用いることで、正しい復号鍵が入力された場合の画像復号誤りを低減できる。

[0087] 図24は、第3の実施の形態における暗号化処理の概要を示す図である。

図24において、暗号化部11Cは、暗号化領域決定部31、チェック用マーク付加部192、画像変換部32、画素値変換部33およびマーカー付加部34を備えている。

[0088] まず暗号化領域指定部31で暗号化する画像領域を選択し、チェック用マーク付加部192で第2の実施の形態と同様の方法で復号化検証用のチェック用マークを付け加える。チェック用マークを付加した後、画像変換部32と画素値変換部33において、第1の実施の形態1および2と同様の方法で画像処理を行ない画像を暗号化し、マーカー付加部34で暗号化領域検出用の位置決めマーカーを第1の実施の形態と同様の方法で付加する。これら各処理の内容は、第1の実施の形態または第2の実施の形態と同様であるため説明を省略する。

[0089] 図25は、第3の実施の形態における復号化処理の概要を示す図である。

図25において、復号化部14Cは、マーカー検出部141、暗号化領域検出部142、暗号化位置検出部143、画像逆変換部144、チェック用マーク検出部204および暗号化位置補正部205を備えている。

[0090] まずマーカー検出部141において第1の実施の形態と同様の方法で位置決めマーカーを検出し、続く暗号化領域検出部142で第1の実施の形態と同様の方法で暗号化領域を検出する。さらに暗号化位置検出部143において、第1の実施の形態と同様の方法で暗号化領域内の各画素の詳細な位置を検出する。また、画像逆変換部144、チェック用マーク検出部204および暗号化位置補正部205で実行される各処理手順は、第2の実施の形態と同様であるため説明を省略する。

[0091] 以上が本発明を適用した第3の実施の形態についての説明である。

上述のように、本発明の実施の形態を、図面を参照しながら説明してきたが、本発明が適用される暗号化処理および復号化処理を実行する処理装置は、その機能が実行されるのであれば、上述の実施の形態に限定されることなく、単体の装置であっても、複数の装置からなるシステムあるいは統合装置であっても、LAN、WAN等のネットワークを介して処理が行なわれるシステムであってもよいことは言うまでもない。

[0092] また、図26に示しように、バス2608に接続されたCPU2601、ROMやRAMのメモリ2602、入力装置2603、出力装置2604、外部記録装置2605、媒体駆動装置2606、可搬記録媒体2609、ネットワーク接続装置2607で構成されるシステムでも実現できる。すなわち、前述してきた実施の形態のシステムを実現するソフトェアのプログラムコードを記録したROMやRAMのメモリ2602、外部記録装置2605、可搬記録媒体2609を、携帯端末に供給し、その携帯端末のコンピュータがプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

[0093] この場合、可搬記録媒体2609等から読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードを記録した可搬記録媒体2609等は本発明を構成することになる。

[0094] プログラムコードを供給するための可搬記録媒体2609としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD－ROM、CD－R、DVD－ROM、DVD－RAM、磁気テープ、不揮発性のメモリーカード、ROMカード、電子メールやパソコン通信等のネットワーク接続装置2607（言い換えれば、通信回線）を介して記録した種々の記録媒体などを用いることができる。

[0095] また、図10に示すように、コンピュータがメモリ2602上に読み出したプログラムコードを実行することによって、前述した実施の形態の機能が実現される他、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているOSなどが実際の処理の一部または全部を行ない、その処理によっても前述した実施の形態の機能が実現される。

[0096] さらに、可搬型記録媒体2609から読み出されたプログラムコードやプログラム（データ）提供者から提供されたプログラム（データ）が、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリ2602に書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPU2601などが実際の処理の一部または全部を行ない、その処理によっても前述した実施の形態の機能が実現され得る。

[0097] すなわち、本発明は、以上に述べた実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲内で種々の構成または形状を取ることができる。

請求の範囲

[1] デジタル画像を暗号化画像に暗号化する画像暗号化装置において、

前記デジタル画像から暗号化する部分領域を指定する暗号化領域指定手段と、

前記暗号化領域指定手段によって選択された部分領域を暗号鍵に基づいて処理画像に変換する画像変換手段と、

前記部分領域の位置を特定可能にするために、前記画像変換手段によって変換された処理画像の画素値を規則的に変換することにより変換画像を生成する画素値変換手段と、

を備えることを特徴とする画像暗号化装置。

[2] 前記画像変換手段は、前記部分領域を複数の微小領域に分割し、分割した複数の微小領域を前記暗号鍵に基づいて並べ替えることを特徴とする請求項1に記載の画像暗号化装置。

[3] 前記画像変換手段は、前記部分領域を任意の圧縮方法で圧縮データに変換し、前記変換された圧縮データの各ビットを任意の大きさの白画素または黒画素として配列することを特徴とする請求項1に記載の画像暗号化装置。

[4] 前記画素値変換手段は、前記処理画像の横方向に関して一定の周期で前記画素値を変換し、縦方向に関して一定の周期で前記画素値を変換することにより、概ね縞状の模様を成すような変換画像を生成することを特徴とする請求項1乃至3の何れか1項に記載の画像暗号化装置。

[5] 前記部分領域の位置を特定するために、特定のマーカーを前記画素値変換手段によって生成された変換画像に付加することにより前記暗号化画像を生成するマーカー付加手段、

をさらに備えることを特徴とする請求項1乃至4の何れか1項に記載の画像暗号化装置。

[6] 前記マーカーは、実線の円形状または多角形状であり、その内側に円形状または多角形の周と交わる線が複数存在する形状であることを特徴とする請求項5に記載の画像暗号化装置。

[7] 前記マーカーは、前景が画素値変換により形成されることを請求項5または6に記

載の画像暗号化装置。

[8] 前記暗号化領域指定手段による部分領域の指定の前に、前記暗号化画像の復号化の妥当性を検証するための特定のチェック用マークを前記デジタル画像に付加するチェック用マーク付加手段、

をさらに備えることを特徴とする請求項1乃至7の何れか1項に記載の画像暗号化装置。

[9] 暗号化画像をデジタル画像に復号化する画像復号化装置において、

暗号化した部分領域の位置を特定するために、前記暗号化画像に付加された特定のマーカーを検出するマーカー検出手段と、

前記マーカー検出手段によって検出されたマーカーに基づいて、暗号化された暗号化画像領域を検出する暗号化領域検出手段と、

前記暗号化領域検出手段によって検出された暗号化画像領域のうち画素値が規則的に変換されている暗号化位置を検出する暗号化位置検出手段と、

前記暗号化位置検出手段によって検出された暗号化位置と復号鍵とに基づいて前記暗号化画像領域を前記デジタル画像に復号する復号手段と、

を備えることを特徴とする画像復号化装置。

[10] 暗号化画像をデジタル画像に復号化する画像復号化装置において、

暗号化された暗号化画像領域を検出する暗号化領域検出手段と、

前記暗号化領域検出手段によって検出された暗号化画像領域のうち画素値が規則的に変換されている暗号化位置を検出する暗号化位置検出手段と、

前記暗号化位置検出手段によって検出された暗号化位置と復号鍵とに基づいて前記暗号化画像領域を前記デジタル画像に復号する復号手段と、

前記復号手段によって復号された前記デジタル画像から復号化の妥当性を検証するための特定のチェック用マークを検出するチェック用マーク検出手段と、

を備えることを特徴とする画像復号化装置。

[11] 暗号化画像をデジタル画像に復号化する画像復号化装置において、

暗号化した部分領域の位置を特定するために、前記暗号化画像に付加された特定のマーカーを検出するマーカー検出手段と、

前記マーカー検出手段によって検出されたマーカーに基づいて、暗号化された暗号化画像領域を検出する暗号化領域検出手段と、

前記暗号化領域検出手段によって検出された暗号化画像領域のうち画素値が規則的に変換されている暗号化位置を検出する暗号化位置検出手段と、

前記暗号化位置検出手段によって検出された暗号化位置と復号鍵とに基づいて前記暗号化画像領域を前記デジタル画像に復号する復号手段と、

前記復号手段によって復号された前記デジタル画像から復号化の妥当性を検証するための特定のチェック用マークを検出するチェック用マーク検出手段と、

を備えることを特徴とする画像復号化装置。

[12] 前記チェック用マーク検出手段によってチェック用マークが検出されなかった場合、前記暗号化位置検出手段によって検出された暗号化位置を補正する暗号化位置補正手段、

をさらに備えることを特徴とする請求項10または11に記載の画像復号化装置。

[13] 前記暗号化画像は、請求項1乃至8の何れか1項の記載の画像暗号化装置によって暗号化された画像であることを特徴とする請求項9乃至12の何れか1項に記載の画像復号化装置。

[14] 前記暗号化画像は、請求項1乃至8の何れか1項の記載の画像暗号化装置によって暗号化された画像を印刷し、該印刷した画像を読み込んだ画像であることを特徴とする請求項9乃至12の何れか1項に記載の画像復号化装置。

[15] デジタル画像を暗号化画像に暗号化する画像暗号化装置において実行される画像暗号化方法であって、

前記デジタル画像から暗号化する部分領域を指定し、

前記選択された部分領域を暗号鍵に基づいて処理画像に変換し、

前記部分領域の位置を特定可能にするために、前記変換された処理画像の画素値を規則的に変換することにより変換画像を生成する、

ことを特徴とする画像暗号化方法。

[16] 前記部分領域の位置を特定するために、特定のマーカーを前記生成された変換画像に付加することにより前記暗号化画像を生成する、

ことを特徴とする請求項15に記載の画像暗号化方法。

[17] 暗号化画像をデジタル画像に復号化する画像復号化装置において実行される画像復号化方法であって、

暗号化した部分領域の位置を特定するために、前記暗号化画像に付加された特定のマーカーを検出し、

前記検出されたマーカーに基づいて、暗号化された暗号化画像領域を検出し、

前記検出された暗号化画像領域のうち画素値が規則的に変換されている暗号化位置を検出し、

前記検出された暗号化位置と復号鍵とに基づいて前記暗号化画像領域を前記デジタル画像に復号する、

ことを特徴とする画像復号化方法。

[18] 暗号化画像をデジタル画像に復号化する画像復号化装置において実行される画像復号化方法であって、

暗号化された暗号化画像領域を検出し、

前記検出された暗号化画像領域のうち画素値が規則的に変換されている暗号化位置を検出し、

前記検出された暗号化位置と復号鍵とに基づいて前記暗号化画像領域を前記デジタル画像に復号し、

前記復号された前記デジタル画像から復号化の妥当性を検証するための特定のチェック用マークを検出する、

ことを特徴とする画像復号化方法。

[19] 暗号化画像をデジタル画像に復号化する画像復号化装置において実行される画像復号化方法であって、

暗号化した部分領域の位置を特定するために、前記暗号化画像に付加された特定のマーカーを検出し、

前記検出されたマーカーに基づいて、暗号化された暗号化画像領域を検出し、

前記検出された暗号化画像領域のうち画素値が規則的に変換されている暗号化位置を検出し、

前記検出された暗号化位置と復号鍵とに基づいて前記暗号化画像領域を前記デジタル画像に復号し、

前記復号された前記デジタル画像から復号化の妥当性を検証するための特定のチェック用マークを検出する、

ことを特徴とする画像復号化方法。

[20] デジタル画像を暗号化画像に暗号化する画像暗号化装置のコンピュータを、

前記デジタル画像から暗号化する部分領域を指定する暗号化領域指定手段、

前記暗号化領域指定手段によって選択された部分領域を暗号鍵に基づいて処理画像に変換する画像変換手段、

前記部分領域の位置を特定可能にするために、前記画像変換手段によって変換された処理画像の画素値を規則的に変換することにより変換画像を生成する画素値変換手段、

として機能させるための画像暗号化プログラム。

[21] 前記部分領域の位置を特定するために、特定のマーカーを前記画素値変換手段によって生成された変換画像に付加することにより前記暗号化画像を生成するマーカー付加手段、

をさらに備えることを特徴とする請求項20に記載の画像暗号化プログラム。

[22] 暗号化画像をデジタル画像に復号化する画像復号化装置のコンピュータを、

暗号化した部分領域の位置を特定するために、前記暗号化画像に付加された特定のマーカーを検出するマーカー検出手段、

前記マーカー検出手段によって検出されたマーカーに基づいて、暗号化された暗号化画像領域を検出する暗号化領域検出手段、

前記暗号化領域検出手段によって検出された暗号化画像領域のうち画素値が規則的に変換されている暗号化位置を検出する暗号化位置検出手段、

前記暗号化位置検出手段によって検出された暗号化位置と復号鍵とに基づいて前記暗号化画像領域を前記デジタル画像に復号する復号手段、

として機能させるための画像復号化プログラム。

[23] 暗号化画像をデジタル画像に復号化する画像復号化装置のコンピュータを、

暗号化された暗号化画像領域を検出する暗号化領域検出手段、

前記暗号化領域検出手段によって検出された暗号化画像領域のうち画素値が規則的に変換されている暗号化位置を検出する暗号化位置検出手段、

前記暗号化位置検出手段によって検出された暗号化位置と復号鍵とに基づいて前記暗号化画像領域を前記デジタル画像に復号する復号手段、

前記復号手段によって復号された前記デジタル画像から復号化の妥当性を検証するための特定のチェック用マークを検出するチェック用マーク検出手段、

として機能させるための画像復号化プログラム。

[24] 暗号化画像をデジタル画像に復号化する画像復号化装置のコンピュータを、

暗号化した部分領域の位置を特定するために、前記暗号化画像に付加された特定のマーカーを検出するマーカー検出手段、

前記マーカー検出手段によって検出されたマーカーに基づいて、暗号化された暗号化画像領域を検出する暗号化領域検出手段、

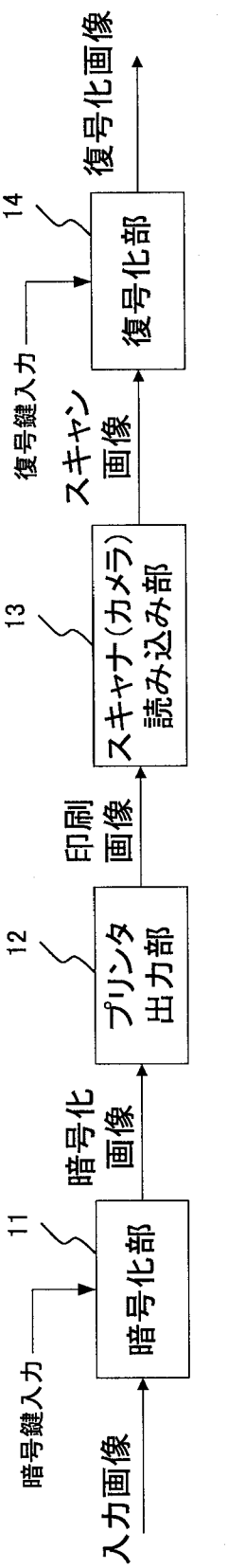
前記暗号化領域検出手段によって検出された暗号化画像領域のうち画素値が規則的に変換されている暗号化位置を検出する暗号化位置検出手段、

前記暗号化位置検出手段によって検出された暗号化位置と復号鍵とに基づいて前記暗号化画像領域を前記デジタル画像に復号する復号手段、

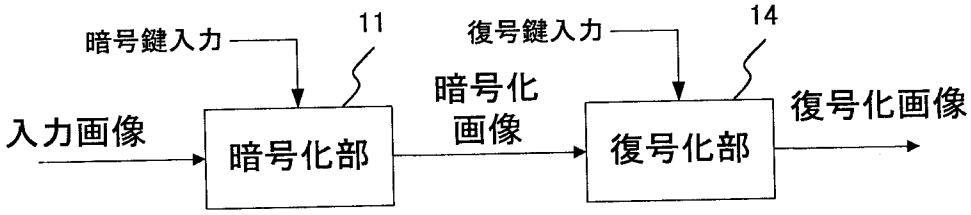
前記復号手段によって復号された前記デジタル画像から復号化の妥当性を検証するための特定のチェック用マークを検出するチェック用マーク検出手段、

として機能させるための画像復号化プログラム。

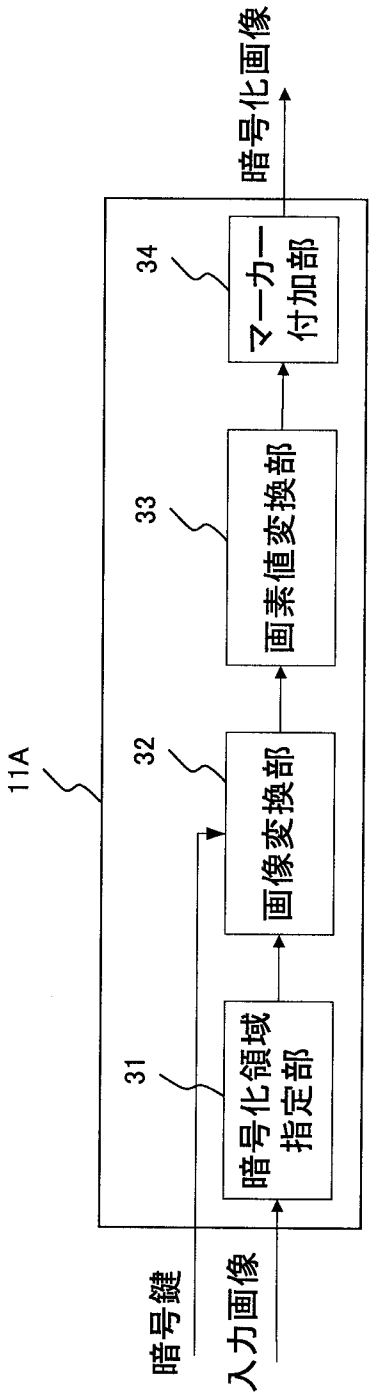
[図1]


入力画像
暗号鍵入力
11
暗号化部
暗号化画像
12
プリンタ出力部
印刷画像
13
スキャナ(カメラ)読み込み部
スキャン画像
復号鍵入力
14
復号化部
復号化画像

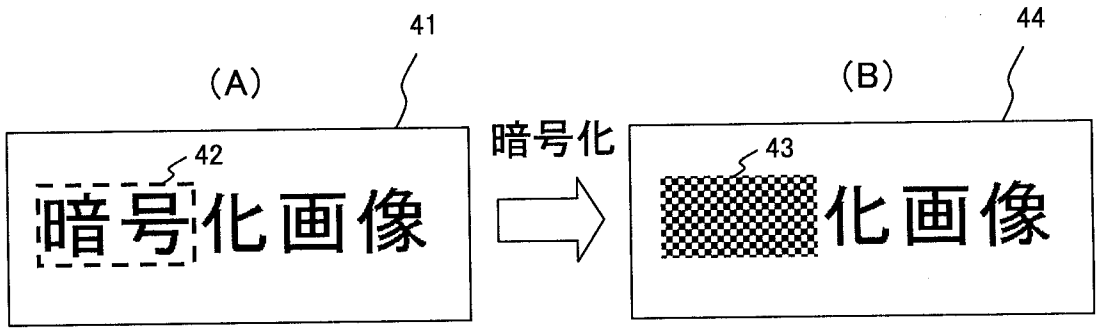
[図2]


暗号鍵入力
11
復号鍵入力
14
入力画像
暗号化部
暗号化画像
復号化部
復号化画像

[図3]


暗号化画像
34
マーカー付加部
33
画素値変換部
11A
32
画像変換部
31
暗号化領域指定部
暗号鍵
入力画像

[図4]



[図5]

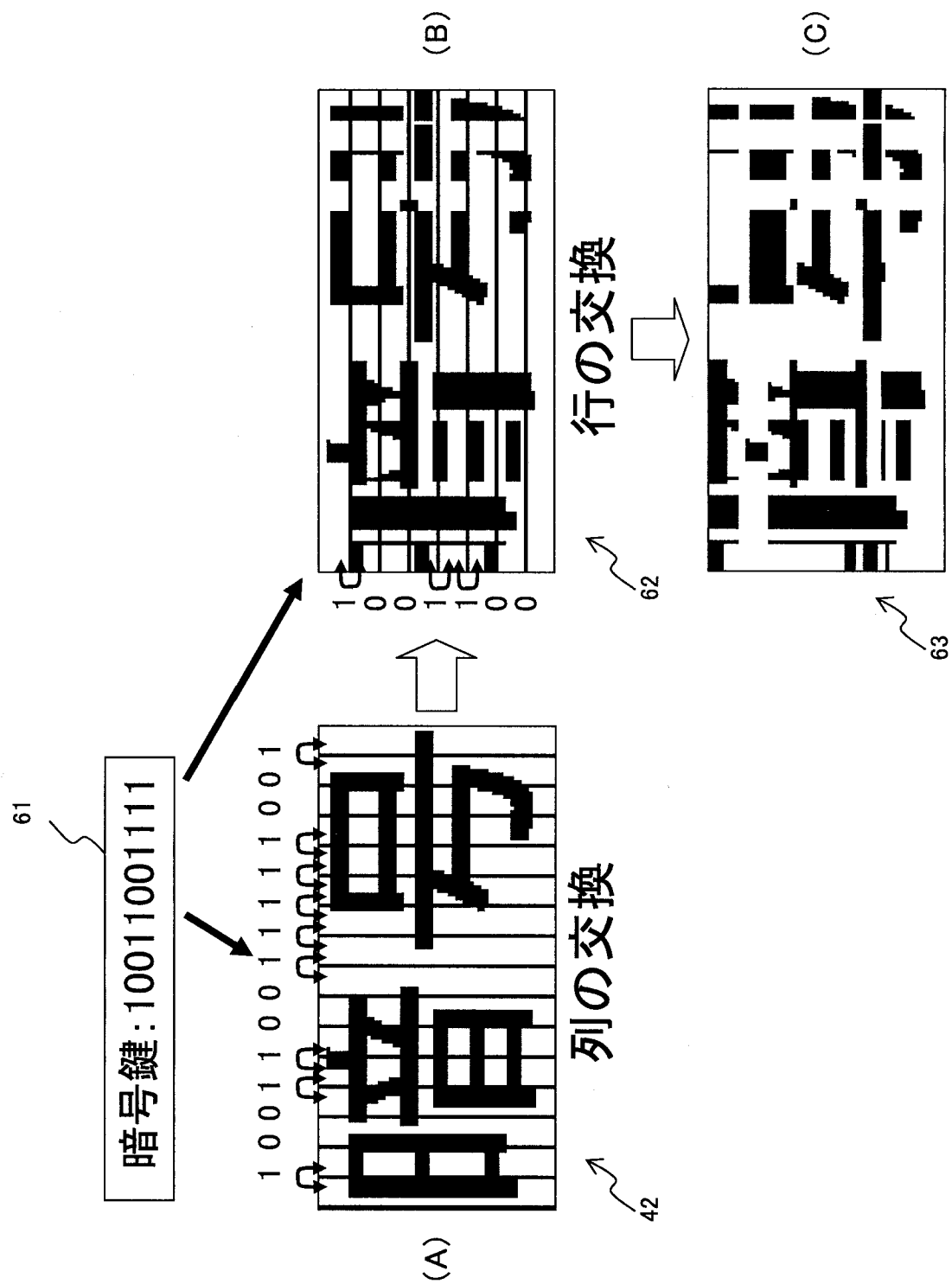
(A)

暗号鍵
1234(数値)
2006(数値)
ango(文字列)
code(文字列)

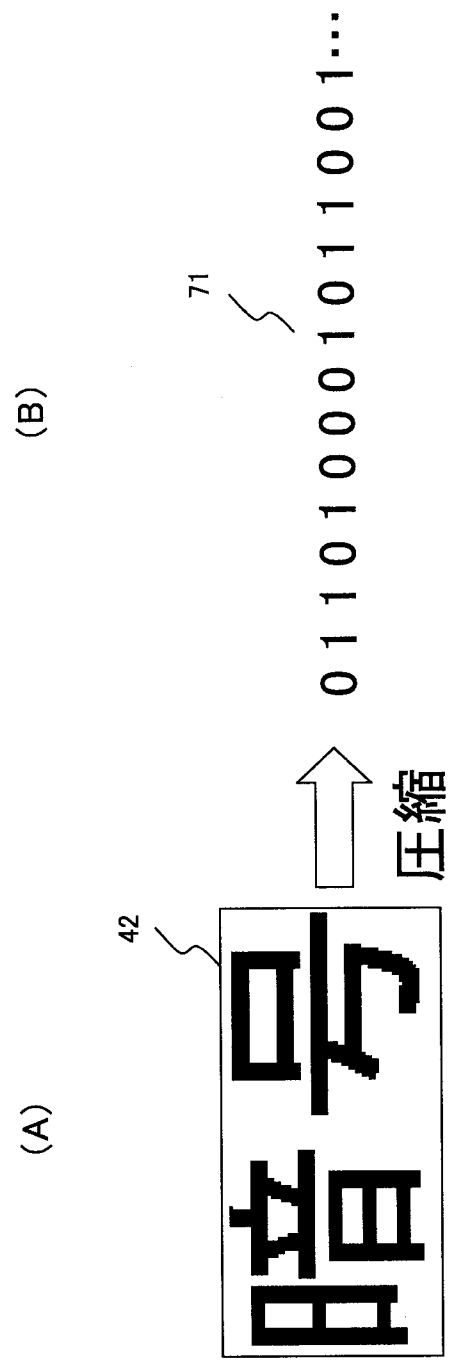
(B)

バイナリ表現
10011010010
11111010110
01100001011011100110011101101111
01100011011011110110010001100101

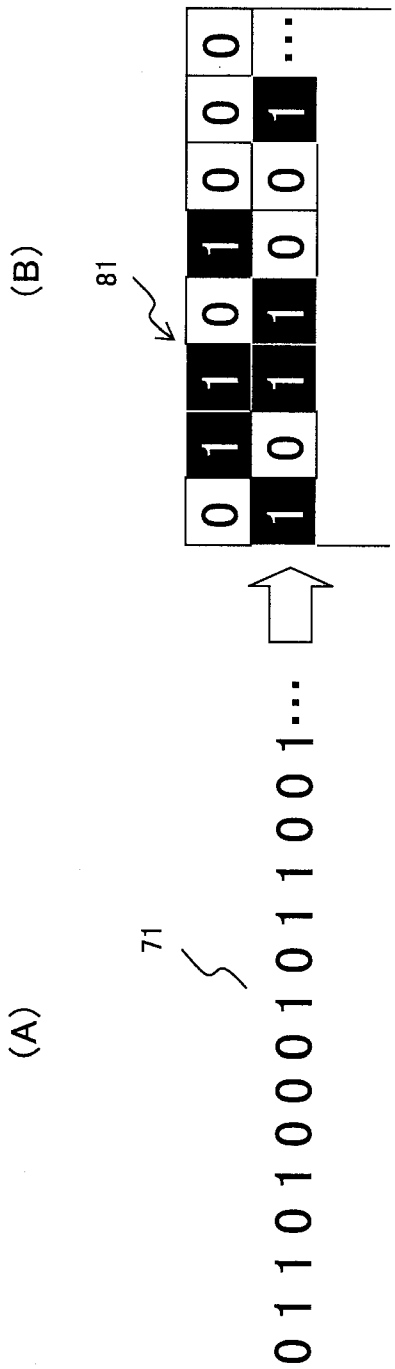
[図6]


(A)
(B)
(C)
暗号鍵:10011001111
1 0 0 1 1 0 0 1 1 1 1 1 1 0 0 1
1 0 0 1 1 0 0
列の交換
行の交換
61
42
62
63

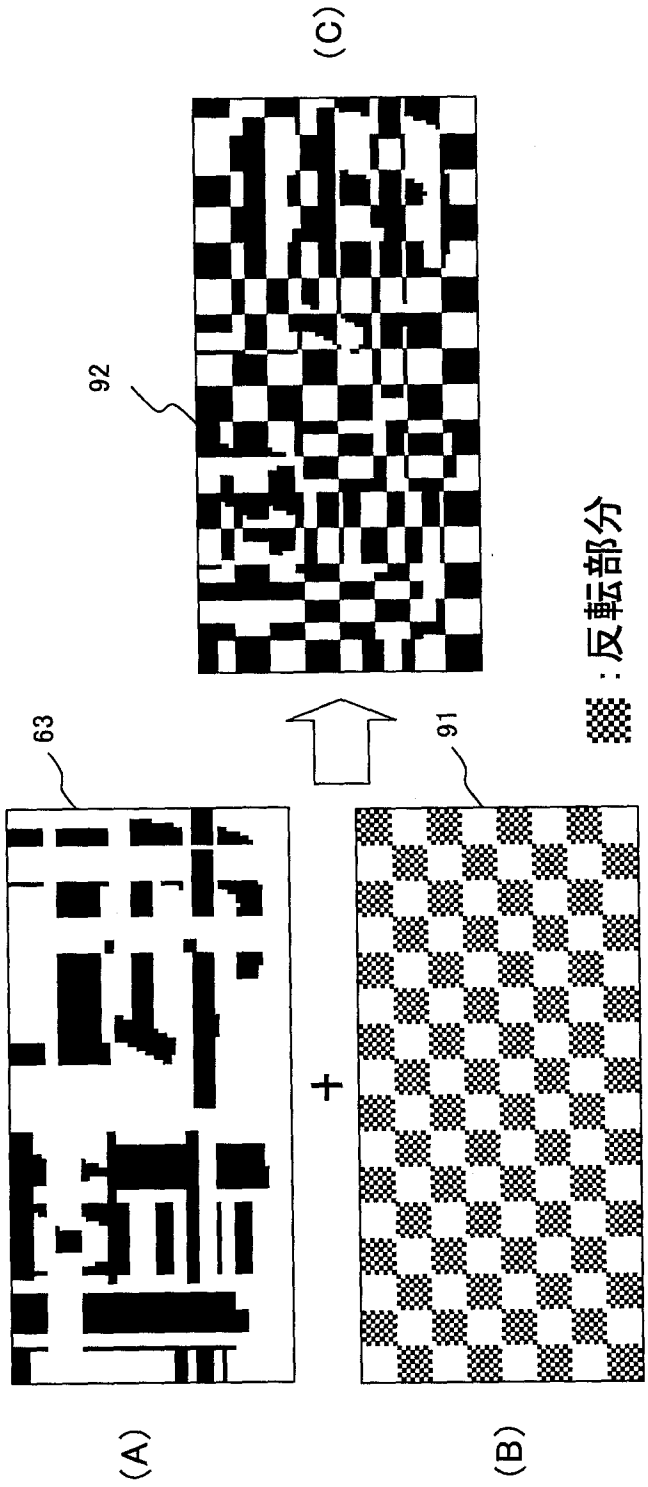
[図7]



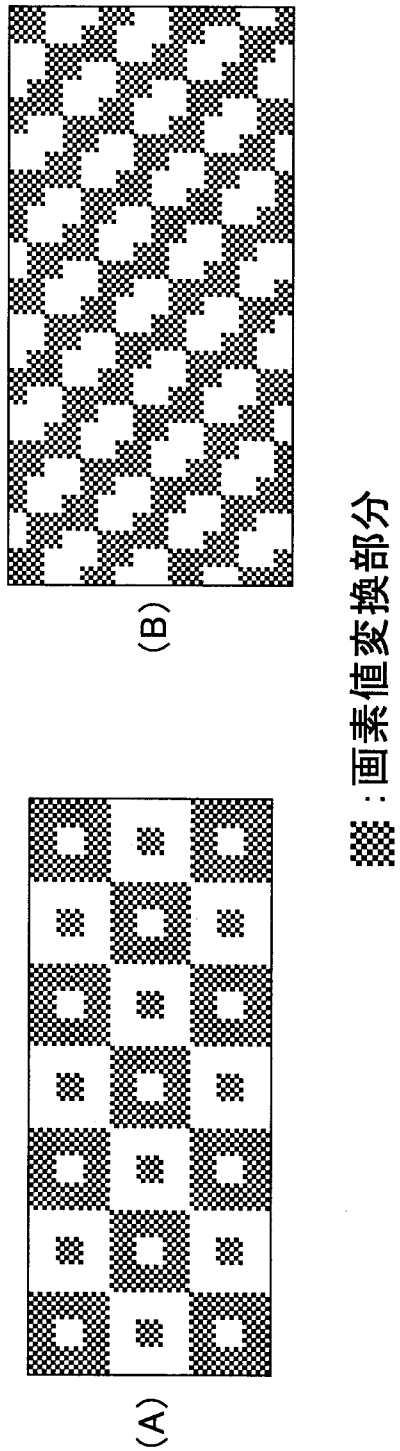
[図8]



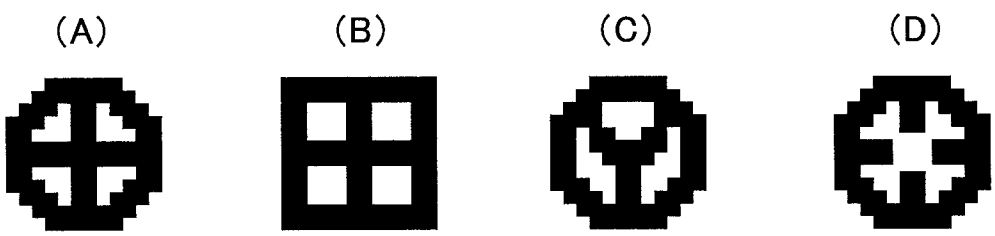
[図9]



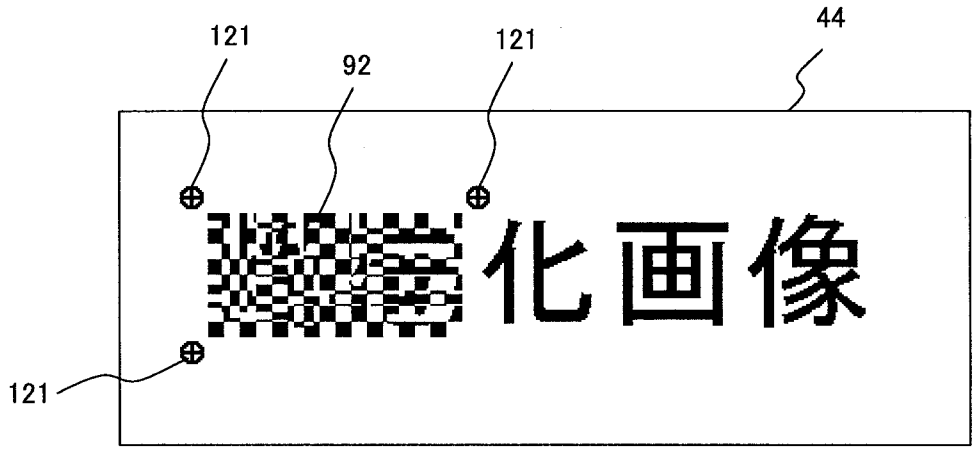
[図10]



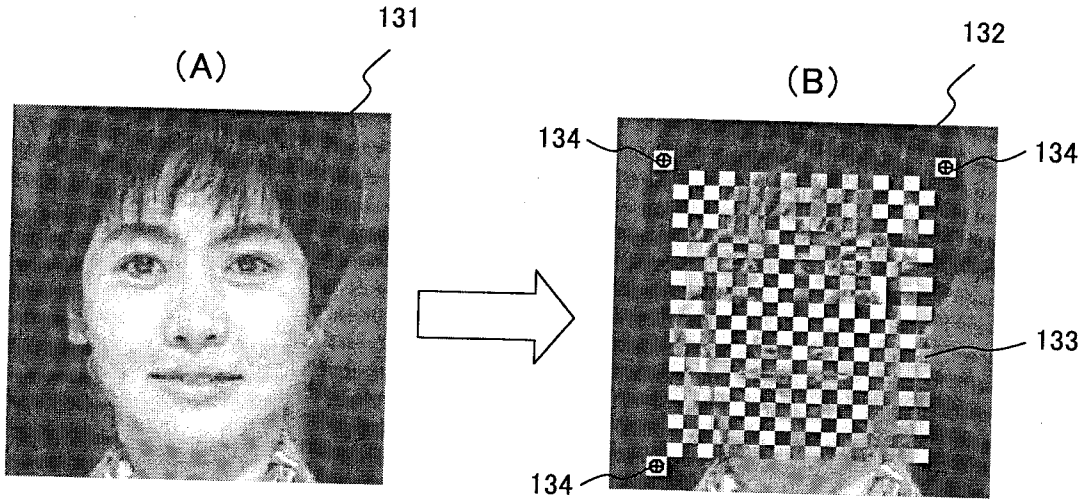
[図11]



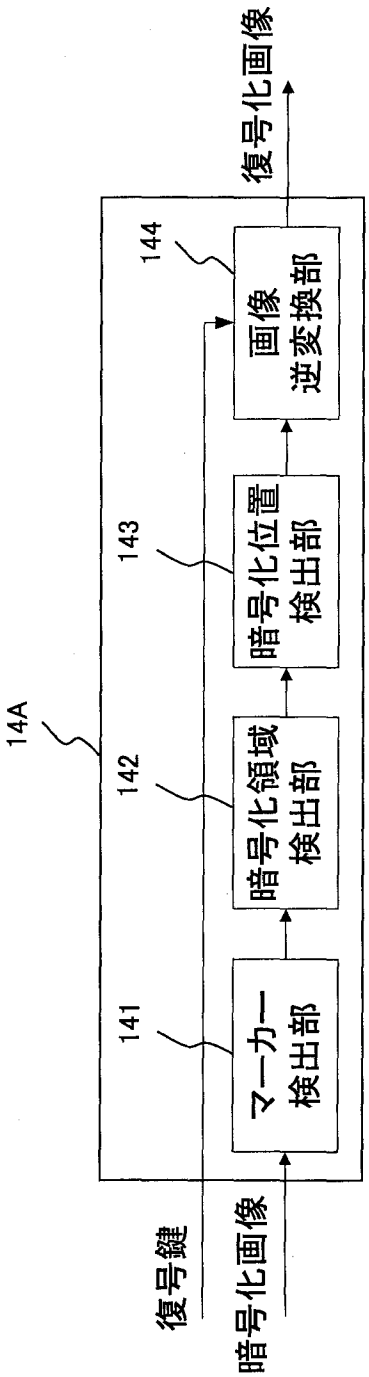
[図12]



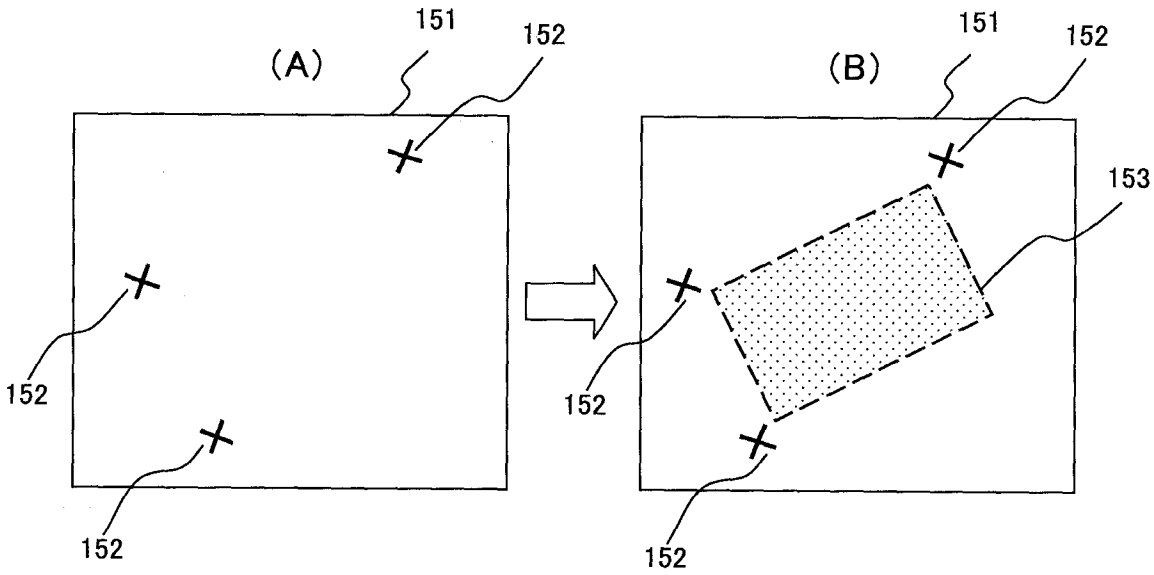
[図13]



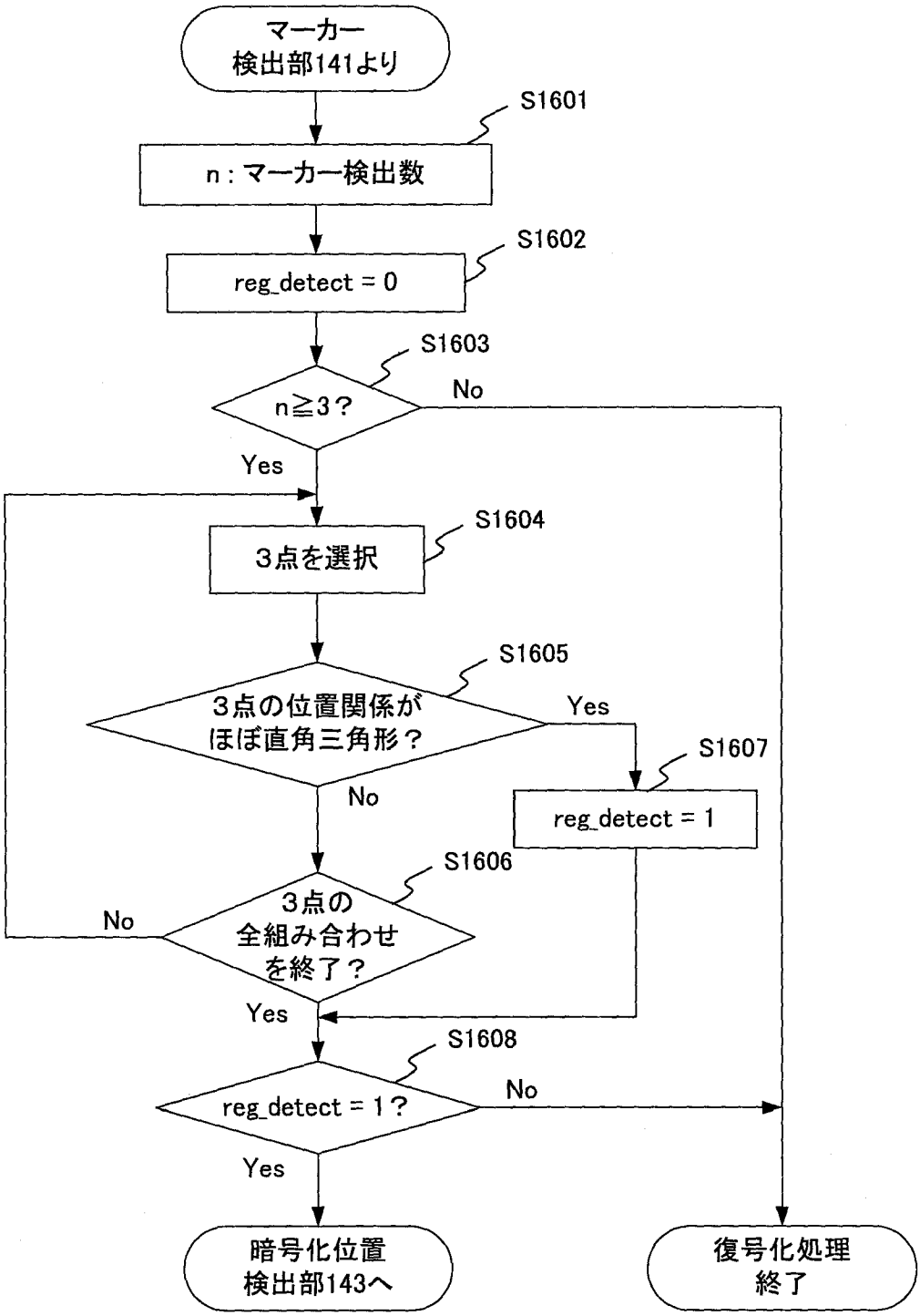
[図14]


復号化画像
144
画像
逆変換部
143
暗号化位置
検出部
142
暗号化領域
検出部
141
マーカー
検出部
14A
復号鍵
暗号化画像

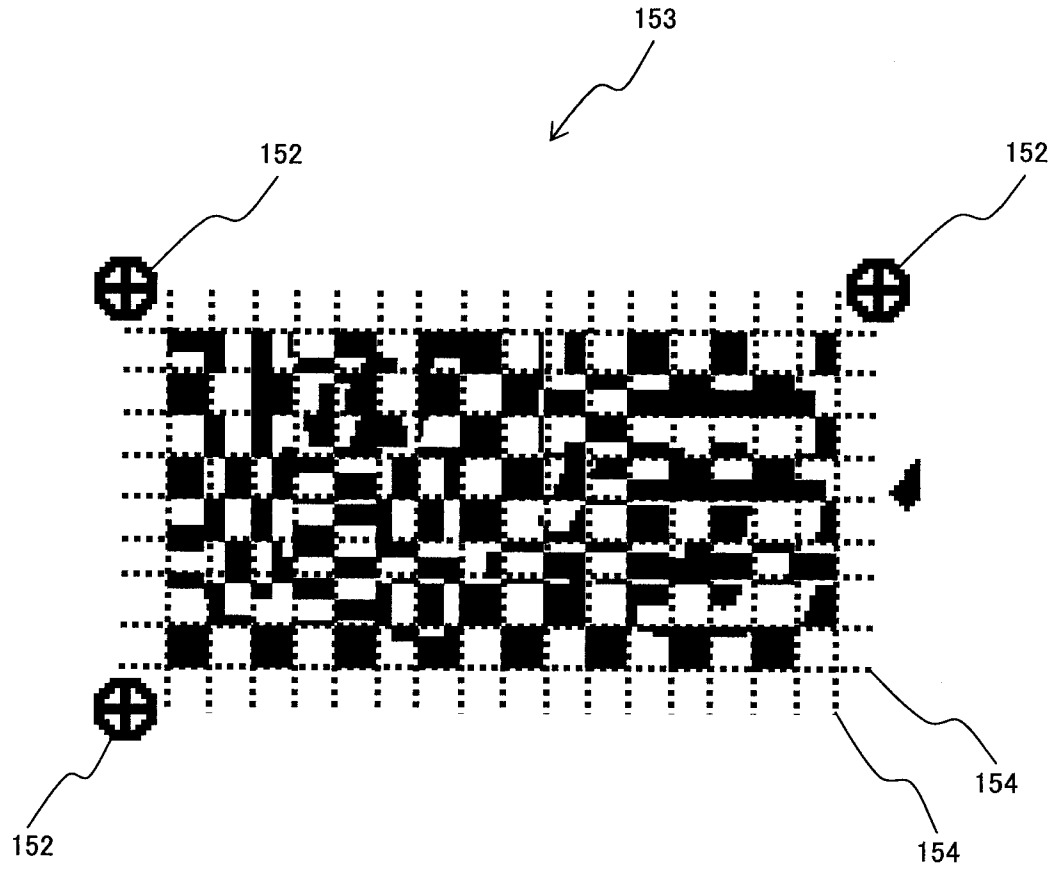
[図15]



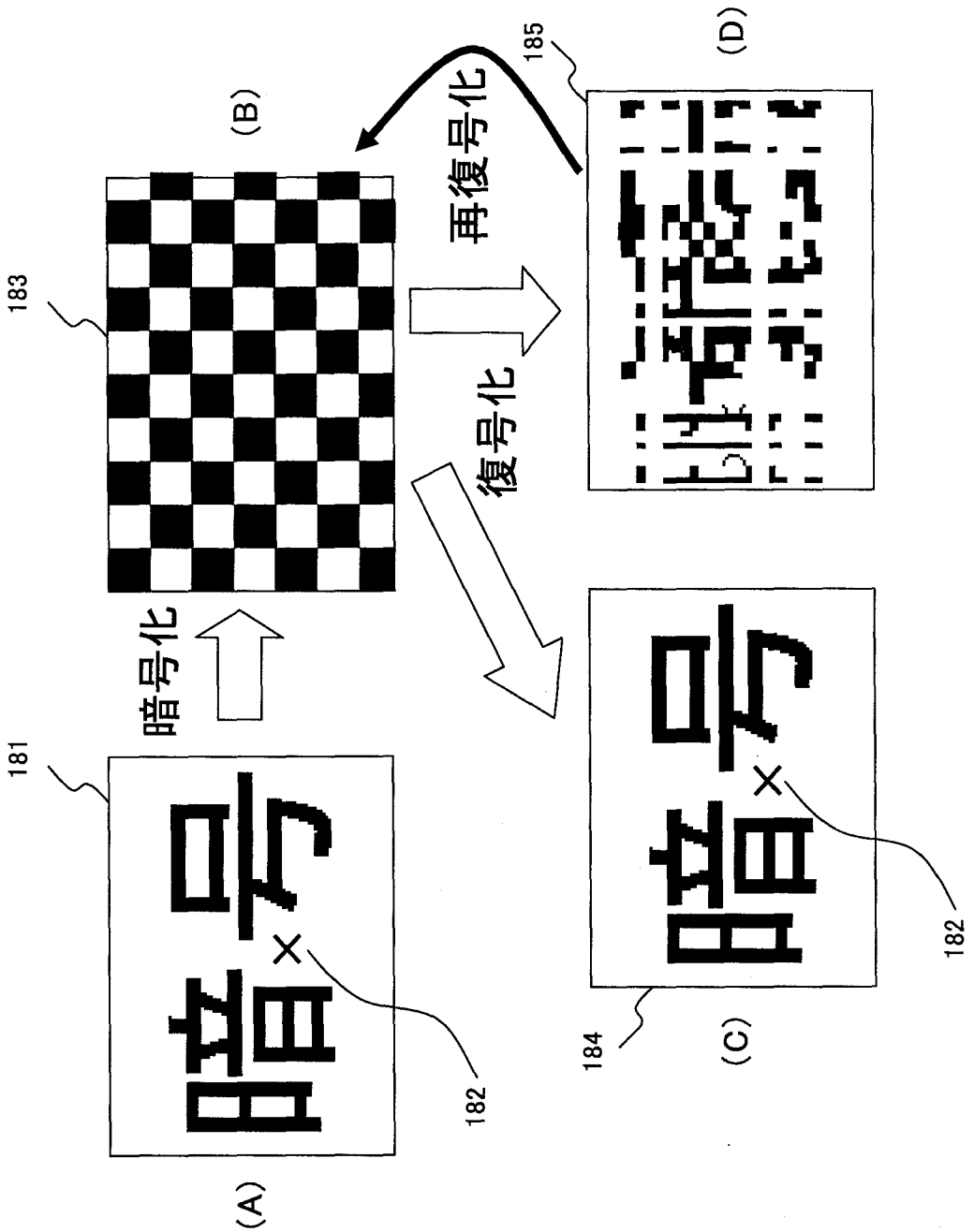
[図16]


マーカー
検出部141より
S1601
n：マーカー検出数
S1602
reg_detect = 0
S1603
n≧3？
No
Yes
S1604
3点を選択
S1605
3点の位置関係が
ほぼ直角三角形？
Yes
S1607
reg_detect = 1
No
S1606
3点の
全組み合わせ
を終了？
No
Yes
S1608
reg_detect = 1？
No
Yes
暗号化位置
検出部143へ
復号化処理
終了

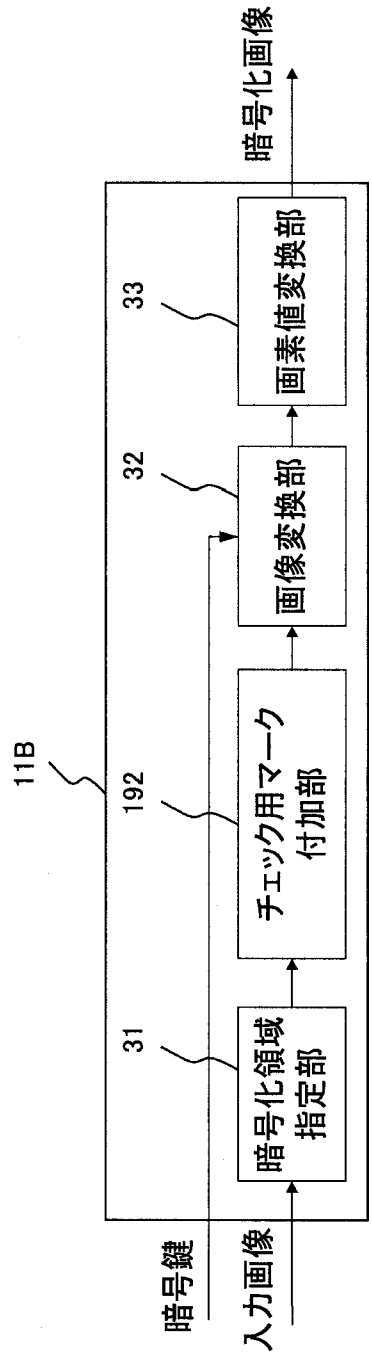
[図17]



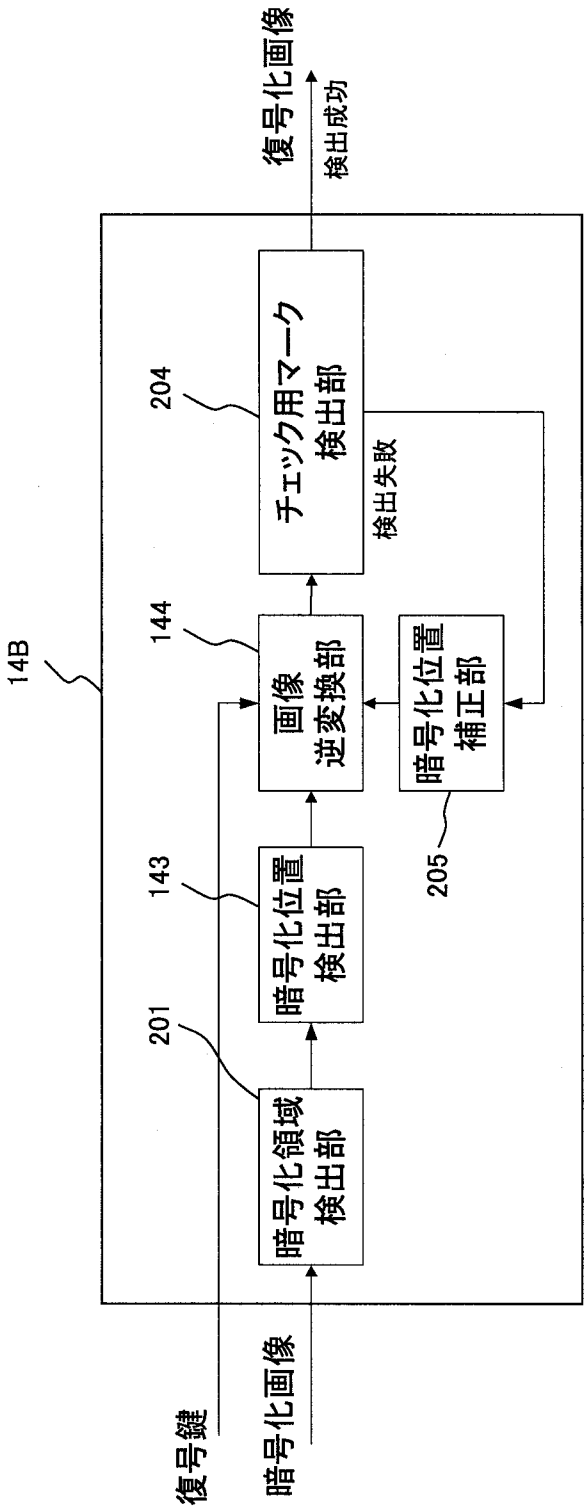
[図18]



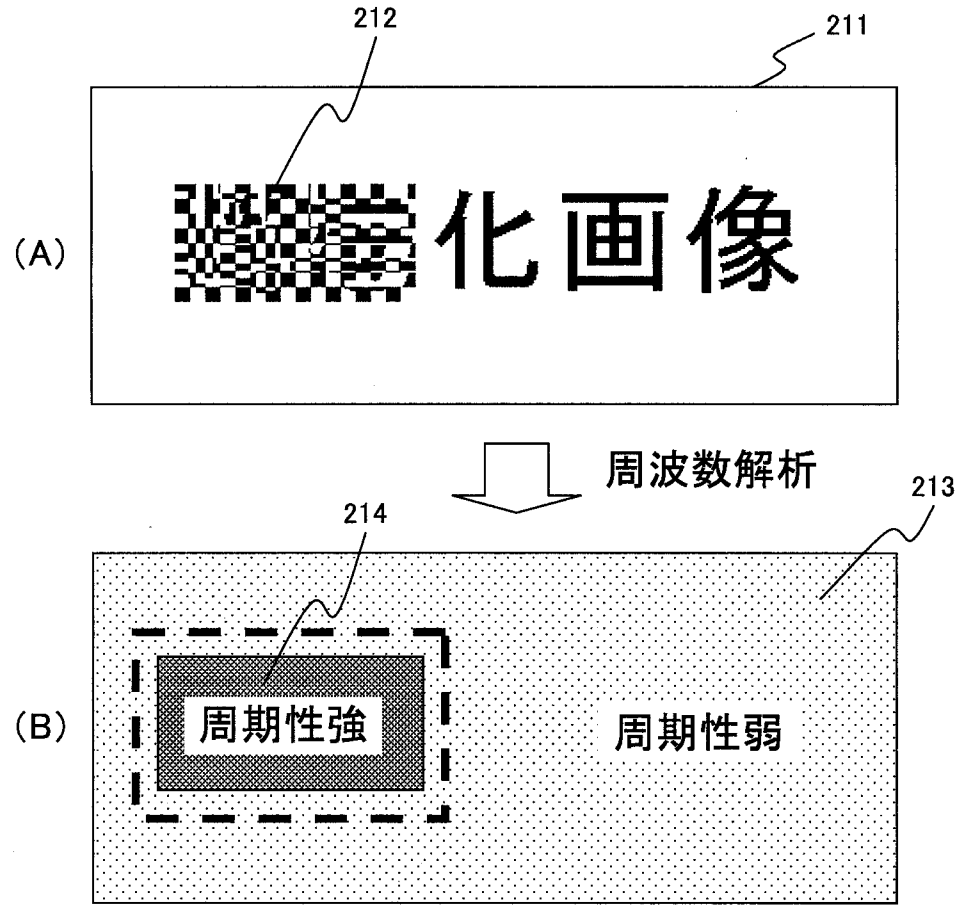
[図19]


暗号化画像
11B
192
31
32
33
暗号化領域
指定部
チェック用マーク
付加部
画像変換部
画素値変換部
暗号鍵
入力画像

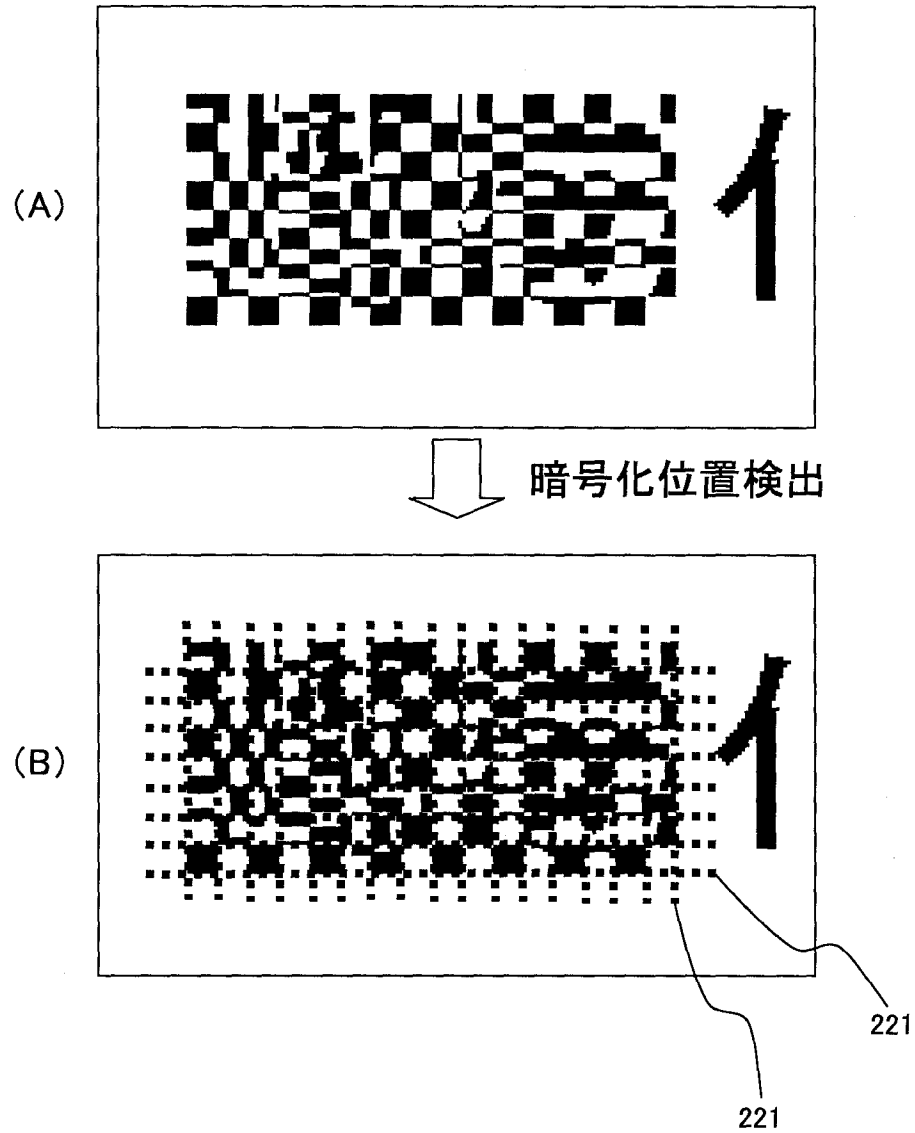
[図20]


復号化画像
検出成功
204
チェック用マーク
検出部
検出失敗
144
画像
逆変換部
暗号化位置
補正部
205
143
暗号化位置
検出部
201
暗号化領域
検出部
14B
復号鍵
暗号化画像

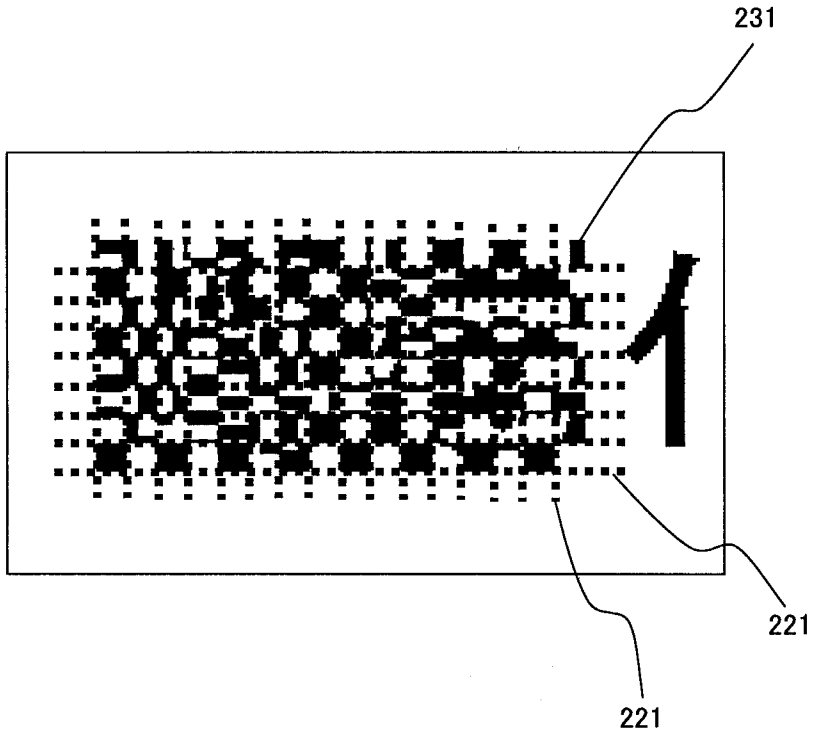
[図21]



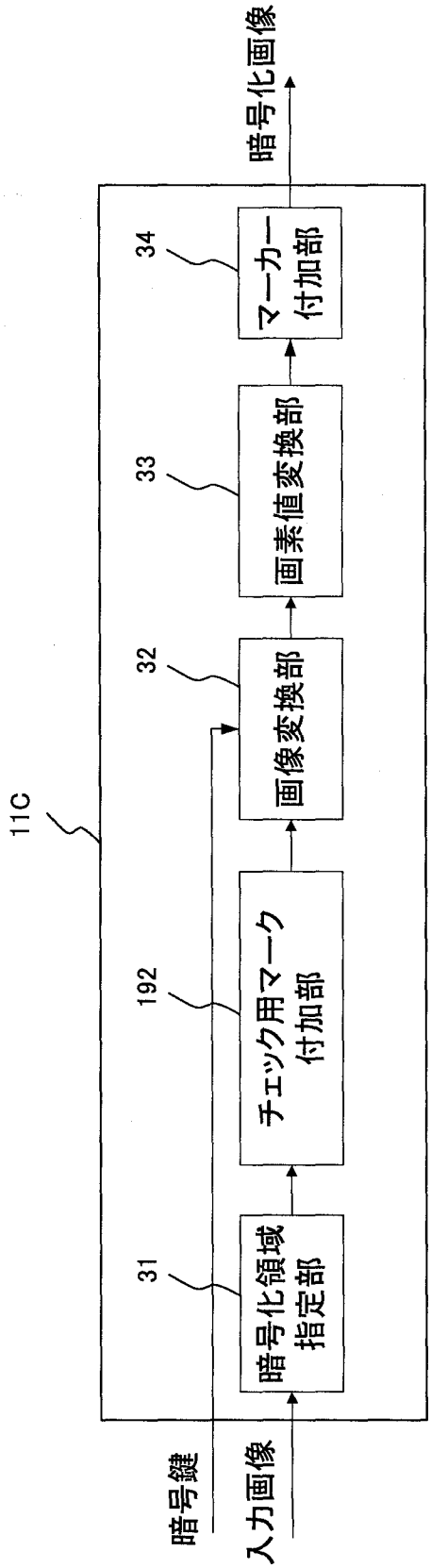
[図22]



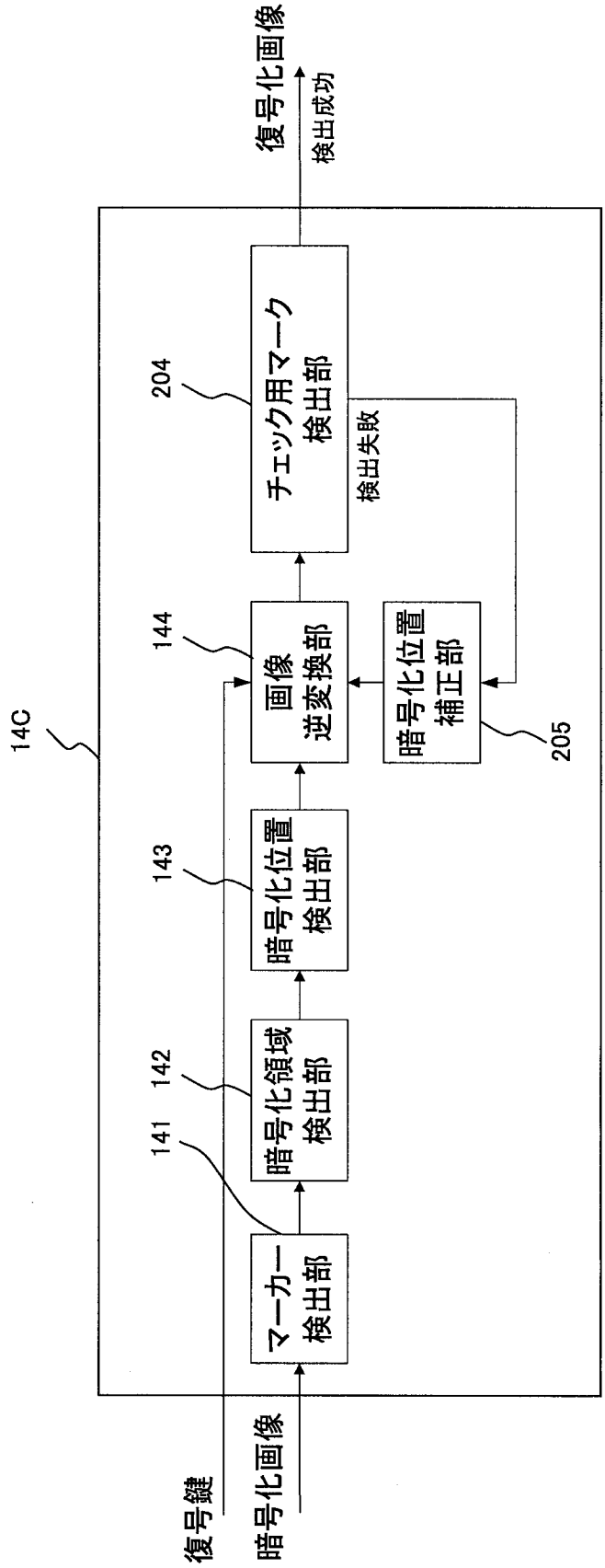
[図23]



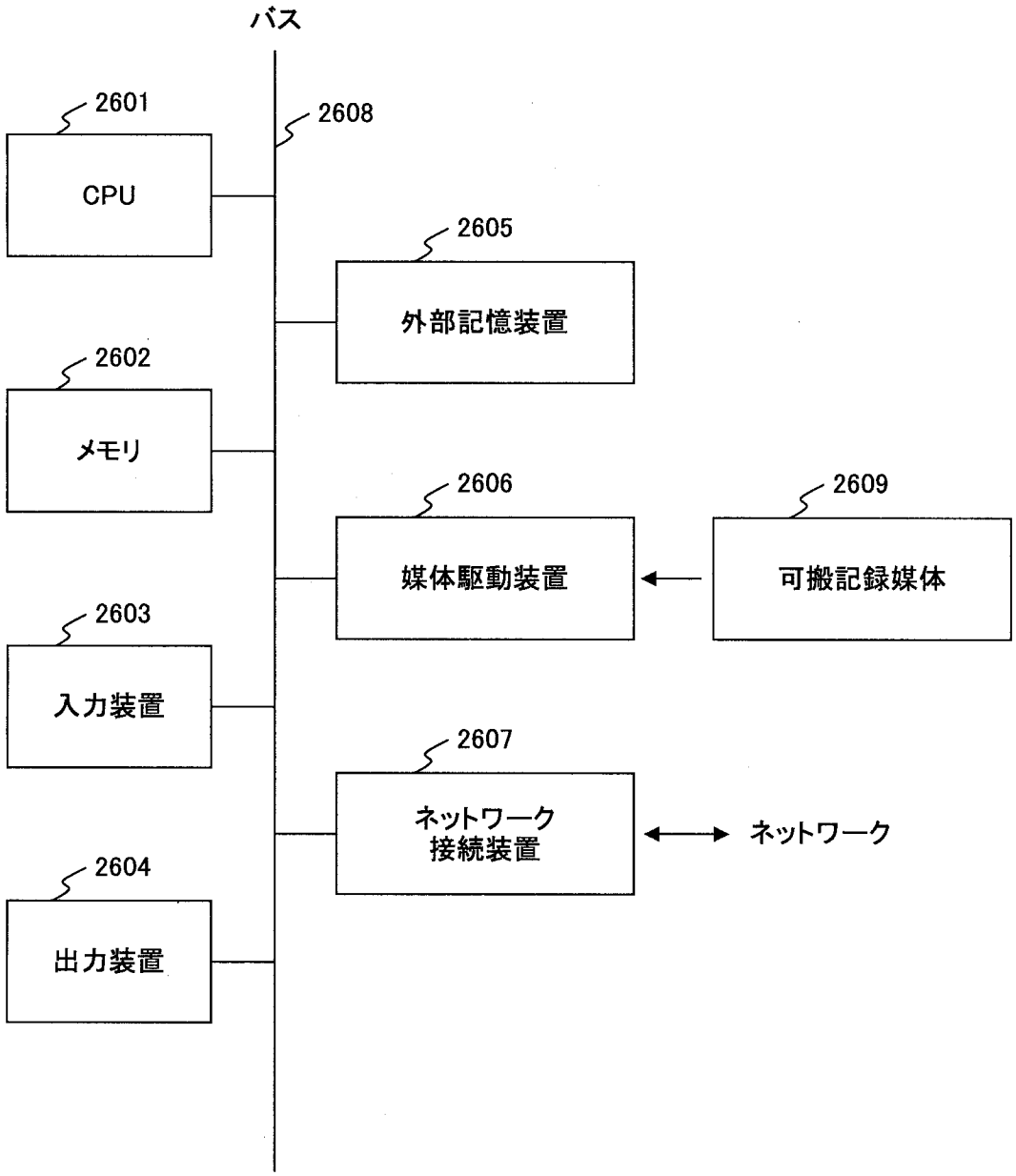
[図24]


暗号化画像
11C
34
マーカー付加部
33
画素値変換部
32
画像変換部
192
チェック用マーク付加部
31
暗号化領域指定部
暗号鍵
入力画像

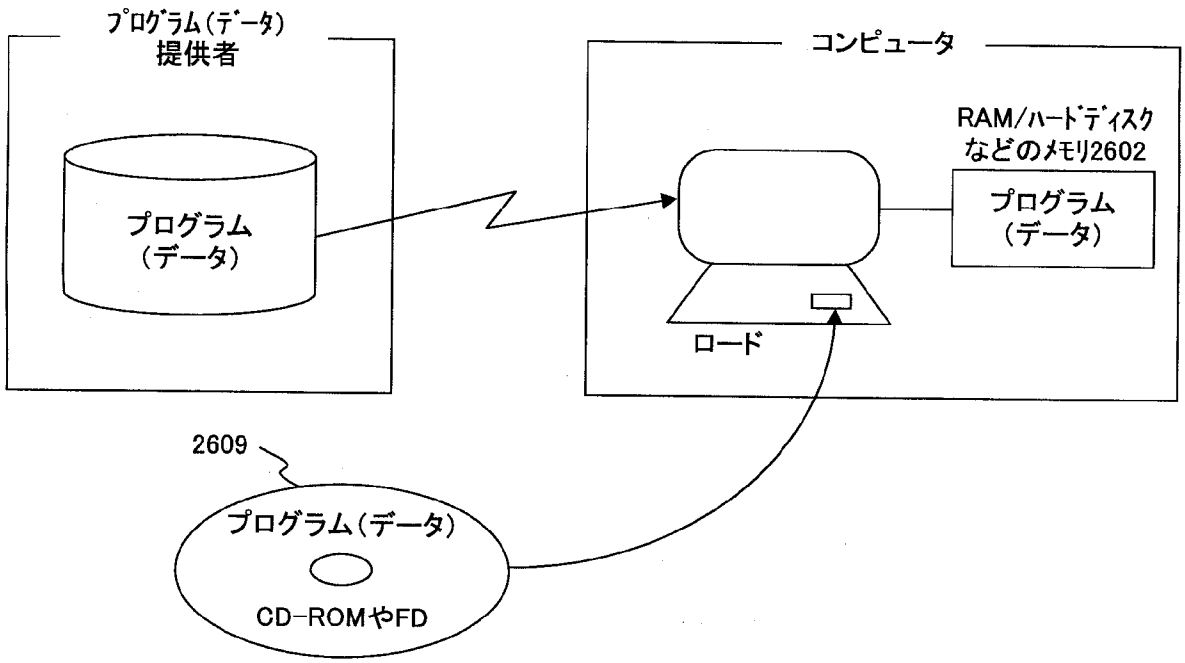
[図25]


復号鍵
暗号化画像
14C
マーカー検出部
141
暗号化領域検出部
142
暗号化位置検出部
143
画像逆変換部
144
暗号化位置補正部
205
チェック用マーク検出部
204
検出失敗
検出成功
復号化画像

[図26]


バス
2601
CPU
2608
2605
外部記憶装置
2602
メモリ
2606
媒体駆動装置
2609
可搬記録媒体
2603
入力装置
2607
ネットワーク
接続装置
ネットワーク
2604
出力装置

[図27]


ﾌﾟﾛｸﾞﾗﾑ(ﾃﾞｰﾀ)
提供者
プログラム
(データ)
コンピュータ
RAM/ﾊｰﾄﾞﾃﾞｨｽｸ
などのﾒﾓﾘ2602
プログラム
(データ)
ロード
2609
プログラム(データ)
CD-ROMやFD

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/321794

A. CLASSIFICATION OF SUBJECT MATTER
H04N1/387(2006.01)i, *G09C5/00*(2006.01)i, *H04N1/44*(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)
H04N1/387, G09C5/00, H04N1/44

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	1996-2006
Kokai Jitsuyo Shinan Koho	1971-2006	Toroku Jitsuyo Shinan Koho	1994-2006

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 5-199424 A (Ricoh Co., Ltd.), 06 August, 1993 (06.08.93), Full text; Figs. 1 to 12 & US 5287203 A1	1-24
A	JP 2000-232586 A (Ricoh Co., Ltd.), 22 August, 2000 (22.08.00), Full text; Figs. 1 to 16 (Family: none)	1-24
A	JP 2006-80623 A (Canon Inc.), 23 March, 2006 (23.03.06), Full text; Figs. 1 to 14 & WO 2006/028103 A1	1-24

☒ 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
19 December, 2006 (19.12.06)	26 December, 2006 (26.12.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/321794

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-32538 A (Canon Inc.), 29 January, 2004 (29.01.04), Full text; Figs. 1 to 19 (Family: none)	1-24

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３２１７９４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04N1/387(2006.01)i, G09C5/00(2006.01)i, H04N1/44(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.　H04N1/387, G09C5/00, H04N1/44

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	１９７１－２００６年
日本国実用新案登録公報	１９９６－２００６年
日本国登録実用新案公報	１９９４－２００６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　５－１９９４２４　Ａ（株式会社　リコー） １９９３．０８．０６，全文，第１－１２図 ＆　ＵＳ　５２８７２０３　Ａ１	１－２４
Ａ	ＪＰ　２０００－２３２５８６　Ａ（株式会社　リコー） ２０００．０８．２２，全文，第１－１６図 （ファミリーなし）	１－２４

☑　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	国際調査報告の発送日
１９．１２．２００６	２６．１２．２００６

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	５Ｖ	９８５６
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	白石　圭吾 電話番号　０３－３５８１－１１０１　内線　３５７１		

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	ＪＰ　２００６－８０６２３　Ａ（キャノン株式会社） ２００６．０３．２３，全文，第１－１４図 　＆　ＷＯ　２００６／０２８１０３　Ａ１	１－２４
Ａ	ＪＰ　２００４－３２５３８　Ａ（キャノン株式会社） ２００４．０１．２９，全文，第１－１９図 （ファミリーなし）	１－２４