(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2011-107279
(P2011-107279A)
(43)公開日　平成23年6月2日(2011.6.2)

(51)Int.Cl.			F I			テーマコード（参考）
G09C	5/00	(2006.01)	G09C	5/00		5B057
G06T	1/00	(2006.01)	G06T	1/00	500B	5C076
H04N	1/387	(2006.01)	H04N	1/387		5J104

審査請求 未請求　請求項の数 5　ＯＬ　（全 43 頁）

(21)出願番号　特願2009-260371 (P2009-260371)
(22)出願日　平成21年11月13日 (2009.11.13)

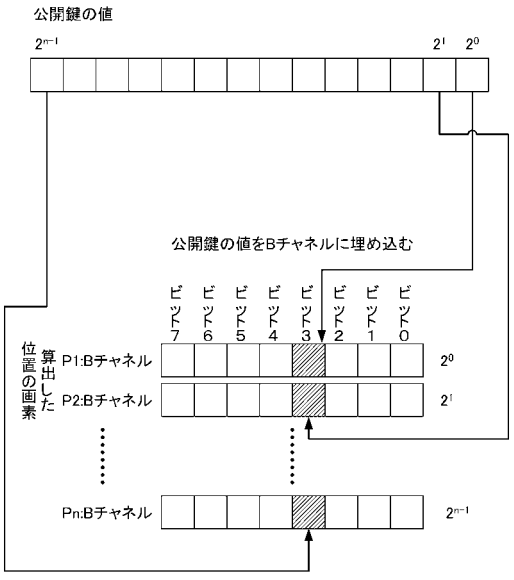
(71)出願人　592218300
学校法人神奈川大学
神奈川県横浜市神奈川区六角橋３丁目２７番１号
(74)代理人　100106002
弁理士　正林　真之
(74)代理人　100120891
弁理士　林　一好
(72)発明者　張　善俊
神奈川県平塚市東八幡４－９－２８－５０１

Ｆターム(参考)　5B057 AA20 CA01 CA08 CA12 CA16 CB01 CB08 CB12 CB16 CE08 CG07
5C076 AA14 BA06

最終頁に続く

(54)【発明の名称】暗号化装置及び方法

(57)【要約】
【課題】データが改竄されている場合には復号できないような暗号を作成することができる装置及び方法を提供すること。
【解決手段】暗号化装置４００は、画像を読み込み、読み込まれた画像を構成する３原色のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成し、生成された複数の各擬似乱数に基づいて、所定の演算を実行し、画像内の画素の位置を順に複数個算出する。そして、暗号化装置４００は、算出された複数個の各位置に係る画素を構成する３原色の階調値のうち、擬似乱数を生成するために用いた一の原色又は二の原色以外の原色の階調値を構成するビットのうち所定のビットに、擬似乱数を算出した順に、ビットの重みを対応付け、重みが対応付けられた所定のビットに、情報を構成するビットのうち、所定のビットに対応付けられた重みと同じ重みのビットの値を埋め込む。
【選択図】図５



【特許請求の範囲】
【請求項１】
画像に情報を埋め込むことによって分散する暗号化装置であって、
３原色の階調値から構成される画素によって構成される画像を読み込む画像読込手段と、
前記画像読込手段によって読み込まれた前記画像を構成する３原色のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成する擬似乱数生成手段と、
前記擬似乱数生成手段によって生成された複数の各前記擬似乱数に基づいて、所定の演算を実行し、前記画像内の画素の位置を順に複数個算出する位置算出手段と、
前記位置算出手段によって算出された複数個の各位置に係る画素を構成する３原色の階調値のうち、前記擬似乱数を生成するために用いた前記一の原色又は二の原色以外の原色の階調値を構成するビットのうち所定のビットに、前記位置算出手段が算出した順に、ビットの重みを対応付ける重み対応付手段と、
前記重み対応付手段によって前記重みが対応付けられた前記所定のビットに、前記情報を構成するビットのうち前記重みと同じ重みのビットの値を埋め込む埋込手段と、
を備える暗号化装置。
【請求項２】
前記画像内に領域を設定する領域設定手段をさらに備え、
前記擬似乱数生成手段は、前記領域設定手段によって設定された領域を構成する画素のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成する請求項１に記載の暗号化装置。
【請求項３】
画素の位置を引数としてハッシュ値を算出するハッシュ値算出手段をさらに備え、
前記位置算出手段は、
算出した画素の位置が重複する場合に、重複した画素の位置を引数として前記ハッシュ値算出手段によってハッシュ値を算出し、算出したハッシュ値に基づいて画素の位置を算出する請求項１又は２に記載の暗号化装置。
【請求項４】
画像に情報を埋め込むことによって分散する暗号化装置において実行される暗号化方法であって、
３原色の階調値から構成される画素によって構成される画像を読み込むステップと、
読み込まれた前記画像を構成する３原色のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成するステップと、
生成された複数の各前記擬似乱数に基づいて、所定の演算を実行し、前記画像内の画素の位置を順に複数個算出するステップと、
算出された複数個の各位置に係る画素を構成する３原色の階調値のうち、前記擬似乱数を生成するために用いた前記一の原色又は二の原色以外の原色の階調値を構成するビットのうち所定のビットに、前記算出した順に、ビットの重みを対応付けるステップと、
前記重みが対応付けられた前記所定のビットに、前記情報を構成するビットのうち前記重みと同じ重みのビットの値を埋め込むステップと、
を備える暗号化方法。
【請求項５】
画像に埋め込まれた情報を取得する復号装置であって、
３原色の階調値から構成される画素によって構成される画像を読み込む画像読込手段と、
前記画像読込手段によって読み込まれた前記画像を構成する３原色のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成する擬似乱数生成手段と、
前記擬似乱数生成手段によって生成された複数の各前記擬似乱数に基づいて、所定の演算を実行し、前記画像内の画素の位置を順に複数個算出する位置算出手段と、
前記位置算出手段によって算出された複数個の各位置に係る画素を構成する３原色の階

調値のうち、前記擬似乱数を生成するために用いた前記一の原色又は二の原色以外の原色の階調値を構成するビットのうち所定のビットに、前記位置算出手段が算出した順に、ビットの重みを対応付ける重み対応付手段と、
前記所定のビットの値を、前記重み対応付手段によって対応付けられた前記重みに従って２進数に変換した情報を取得する情報取得手段と、
を備える復号装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、画像データを利用して暗号化する暗号化装置及び方法に関する。
【背景技術】
【０００２】
近年、コンピュータの発達に伴い、コンピュータを利用した電子投票は、安全で迅速な処理が期待できることから関心が高まっている。コンピュータを利用した電子投票には、集計においてコンピュータを利用する電子投票や、投票する方法においてコンピュータを利用する電子投票、遠隔地からの投票においてネットワークコンピュータを利用する電子投票等が存在する。
【０００３】
このような電子投票は、どの投票者が誰に投票したのかは誰にも分からない、いわゆる秘匿性と、投票結果が正しく集計されたことが、集計後いつでも誰でも確認できること、等が要求される。
【０００４】
このような要求を考慮したシステムとして、特許文献１に開示された、認証機関と集計機関とを備える電子投票システムが知られている。
【０００５】
この特許文献１が開示するシステムにおいて、投票装置は、投票者のディジタル証明書を認証機関の公開鍵によって暗号化し、所定の情報（自己の投票が正しく集計されていることを知るための投票者のみが知る情報）を含む投票メッセージを集計機関の公開鍵によって暗号化し、暗号化されたディジタル証明書と、暗号化された投票メッセージとを連結して投票装置の秘密鍵によって暗号化した署名ブロックを認証機関に送る。認証機関は、投票装置の公開鍵によって署名ブロックを復号し、認証機関の秘密鍵によってディジタル証明書を復号して認証後、集計組織に転送する。集計組織は、投票装置の公開鍵によって署名ブロックを復号し、集計組織の秘密鍵によって投票メッセージを復号して集計する。したがって、特許文献１が開示するシステムにおいて、認証機関は投票メッセージを復号できず、集計機関はディジタル証明書を復号できないので、どの投票者が誰に投票したのかは誰にも分からない。そして、集計組織が公表した投票メッセージのうち所定の情報によって、投票者は自己の投票が正しく集計されたことを知ることができる。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特表２００５－５０９３６６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
しかしながら、特許文献１が開示するシステムは、ディジタル証明書と投票メッセージとを連結させている。よって、認証機関が集計組織の秘密鍵を入手したり、集計組織が認証機関の秘密鍵を入手したりすると、特許文献１が開示するシステムは、どの投票者が誰に投票したのかが分かってしまう。すなわち、特許文献１が開示するシステムは、秘匿性を確保することができない。
【０００８】

そして、特許文献１が開示するシステムは、ディジタル証明書及び投票メッセージが改竄されていたとしても、公開鍵によって暗号化されたディジタル証明書及び投票メッセージを秘密鍵によって復号し、復号したディジタル証明書及び投票メッセージに基づいて集計をしてしまう。

【０００９】

そこで、データが改竄されている場合には復号できないような暗号が求められている。

【００１０】

本発明は、データが改竄されている場合には復号できないような暗号を作成することができる装置及び方法を提供する。

【課題を解決するための手段】

【００１１】

本発明では、以下のような解決手段を提供する。

【００１２】

（１） 画像に情報を埋め込むことによって分散する暗号化装置であって、３原色の階調値から構成される画素によって構成される画像を読み込む画像読込手段と、前記画像読込手段によって読み込まれた前記画像を構成する３原色のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成する擬似乱数生成手段と、前記擬似乱数生成手段によって生成された複数の各前記擬似乱数に基づいて、所定の演算を実行し、前記画像内の画素の位置を順に複数個算出する位置算出手段と、前記位置算出手段によって算出された複数個の各位置に係る画素を構成する３原色の階調値のうち、前記擬似乱数を生成するために用いた前記一の原色又は二の原色以外の原色の階調値を構成するビットのうち所定のビットに、前記位置算出手段が算出した順に、ビットの重みを対応付ける重み対応付手段と、前記重み対応付手段によって前記重みが対応付けられた前記所定のビットに、前記情報を構成するビットのうち前記重みと同じ重みのビットの値を埋め込む埋込手段と、を備える暗号化装置。

【００１３】

（１）の構成によれば、本発明に係る暗号化装置は、画像に情報を埋め込むことによって分散する暗号化装置であって、３原色の階調値から構成される画素によって構成される画像を読み込み、読み込まれた画像を構成する３原色のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成し、生成された複数の各擬似乱数に基づいて、所定の演算を実行し、画像内の画素の位置を順に複数個算出する。そして、本発明に係る暗号化装置は、算出された複数個の各位置に係る画素を構成する３原色の階調値のうち、擬似乱数を生成するために用いた一の原色又は二の原色以外の原色の階調値を構成するビットのうち所定のビットに、擬似乱数を算出した順に、ビットの重みを対応付け、重みが対応付けられた所定のビットに、情報を構成するビットのうち、所定のビットに対応付けられた重みと同じ重みのビットの値を埋め込む。

【００１４】

すなわち、本発明に係る暗号化装置は、画像を構成する画素の階調値に基づいて算出した画素に、情報を埋め込むことによって情報を暗号化する。したがって、画像を構成する画素の階調値が変更されている場合には情報を埋め込んだ画素を算出することができないので、本発明に係る暗号化装置は、画像データが改竄されている場合には復号できないような暗号を作成することができる。

【００１５】

（２） 前記画像内に領域を設定する領域設定手段をさらに備え、前記擬似乱数生成手段は、前記領域設定手段によって設定された領域を構成する画素のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成する（１）に記載の暗号化装置。

【００１６】

（２）の構成によれば、（１）に記載の暗号化装置は、さらに、画像内に領域を設定し、設定された領域を構成する画素のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成する。

【００１７】
すなわち、（２）に記載の暗号化装置は、画像内に設定した領域を構成する画素の階調値に基づいて算出した画素に、情報を埋め込む。したがって、画像内の領域を構成する画素の階調値が変更されている場合には、情報を埋め込んだ画素を算出することができないので、（２）に記載の暗号化装置は、画像データが改竄されている場合には復号できないような暗号を作成することができる。さらに、情報を埋め込んだ画素を算出するための特定の領域が秘密なので、（２）に記載の暗号化装置は、復号することが困難な暗号を作成することができる。
【００１８】
（３）　画素の位置を引数としてハッシュ値を算出するハッシュ値算出手段をさらに備え、前記位置算出手段は、算出した画素の位置が重複する場合に、重複した画素の位置を引数として前記ハッシュ値算出手段によってハッシュ値を算出し、算出したハッシュ値に基づいて画素の位置を算出する（１）又は（２）に記載の暗号化装置。
【００１９】
（３）の構成によれば、（１）又は（２）に記載の暗号化装置は、さらに、算出した画素の位置が重複する場合に、重複した画素の位置を引数としてハッシュ値を算出し、算出したハッシュ値に基づいて画素の位置を算出する。
【００２０】
すなわち、（３）に記載の暗号化装置は、算出した画素の位置が重複する場合に、ハッシュ値に基づいて画素の位置を算出し、情報を埋め込む。したがって、（３）に記載の暗号化装置は、画像データが改竄されている場合には復号できないような暗号を作成することができる。さらに、情報を埋め込んだ位置が重複する場合に埋め込んだときと同じハッシュ値を得なければ復号できないので、（３）に記載の暗号化装置は、復号することがさらに困難な暗号を作成することができる。
【００２１】
（４）　画像に情報を埋め込むことによって分散する暗号化装置において実行される暗号化方法であって、３原色の階調値から構成される画素によって構成される画像を読み込むステップと、読み込まれた前記画像を構成する３原色のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成するステップと、生成された複数の各前記擬似乱数に基づいて、所定の演算を実行し、前記画像内の画素の位置を順に複数個算出するステップと、算出された複数個の各位置に係る画素を構成する３原色の階調値のうち、前記擬似乱数を生成するために用いた前記一の原色又は二の原色以外の原色の階調値を構成するビットのうち所定のビットに、前記算出した順に、ビットの重みを対応付けるステップと、前記重みが対応付けられた前記所定のビットに、前記情報を構成するビットのうち前記重みと同じ重みのビットの値を埋め込むステップと、を備える暗号化方法。
【００２２】
（４）の構成によれば、暗号化装置において実行される本発明に係る暗号化方法は、３原色の階調値から構成される画素によって構成される画像を読み込み、読み込まれた画像を構成する３原色のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成する。そして、本発明に係る方法は、生成された複数の各擬似乱数に基づいて、所定の演算を実行し、画像内の画素の位置を順に複数個算出し、算出された複数個の各位置に係る画素を構成する３原色の階調値のうち、擬似乱数を生成するために用いた一の原色又は二の原色以外の原色の階調値を構成するビットのうち所定のビットに、算出した順に、ビットの重みを対応付け、重みが対応付けられた所定のビットに、情報を構成するビットのうち、所定のビットに対応付けられた重みと同じ重みのビットの値を埋め込む。
【００２３】
したがって、画像を構成する画素の階調値が変更されている場合には情報を埋め込んだ画素を算出することができないので、本発明に係る方法は、画像データが改竄されている場合には復号できないような暗号を作成することができる。
【００２４】

（５）　画像に埋め込まれた情報を取得する復号装置であって、３原色の階調値から構成される画素によって構成される画像を読み込む画像読込手段と、前記画像読込手段によって読み込まれた前記画像を構成する３原色のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成する擬似乱数生成手段と、前記擬似乱数生成手段によって生成された複数の各前記擬似乱数に基づいて、所定の演算を実行し、前記画像内の画素の位置を順に複数個算出する位置算出手段と、前記位置算出手段によって算出された複数個の各位置に係る画素を構成する３原色の階調値のうち、前記擬似乱数を生成するために用いた前記一の原色又は二の原色以外の原色の階調値を構成するビットのうち所定のビットに、前記位置算出手段が算出した順に、ビットの重みを対応付ける重み対応付手段と、前記所定のビットの値を、前記重み対応付手段によって対応付けられた前記重みに従って２進数に変換した情報を取得する情報取得手段と、を備える復号装置。

【００２５】

（５）の構成によれば、本発明に係る復号装置は、３原色の階調値から構成される画素によって構成される画像を読み込み、読み込まれた画像を構成する３原色のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成し、生成された複数の各擬似乱数に基づいて、所定の演算を実行し、画像内の画素の位置を順に複数個算出する。そして、本発明に係る復号装置は、算出された複数個の各位置に係る画素を構成する３原色の階調値のうち、擬似乱数を生成するために用いた一の原色又は二の原色以外の原色の階調値を構成するビットのうち所定のビットに、算出した順に、ビットの重みを対応付け、所定のビットの値を、対応付けられた重みに従って２進数に変換した情報を取得する。

【００２６】

したがって、本は発明に係る復号装置は、画像を構成する画素の階調値に基づいて算出した画素に埋め込まれた情報を、復号することができる。

【発明の効果】

【００２７】

本発明は、画像データを構成する画素に基づいた暗号を作成するので、画像データが改竄されている場合には復号できないような暗号を作成することができる。

【００２８】

さらに、本発明は、画像データを構成する画素に基づいて算出した画素に情報を埋め込むので、復号することが困難な暗号を作成することができる。

【図面の簡単な説明】

【００２９】

【図１】本発明の一実施形態に係る電子投票システムの実施形態１の特徴を示す特徴図である。

【図２】本発明の一実施形態に係る全体画像データの例を示す図である。

【図３】本発明の一実施形態に係る分割画像データの例を示す図である。

【図４】本発明の一実施形態に係る分割画像データを構成する画素の階調値と、擬似乱数の生成とについて説明する説明図である。

【図５】本発明の一実施形態に係る分割画像データにおいて、データのバイナリ値をビットに分解して埋め込むことを説明する図である。

【図６】本発明の一実施形態に係る分割画像データの別の例を示す図である。

【図７】本発明の一実施形態に係る電子投票データのデータを埋め込むための複数の画素の位置を算出するために設定される領域の例を示す図である。

【図８】本発明の一実施形態に係る電子投票システムの実施形態２の特徴を示す特徴図である。

【図９】本発明の一実施形態に係る電子投票データ作成装置の機能を示す機能ブロック図である。

【図１０】本発明の一実施形態に係る電子投票装置の機能を示す機能ブロック図である。

【図１１】本発明の一実施形態に係る電子開票装置の機能を示す機能ブロック図である。

【図１２】本発明の一実施形態に係る電子投票データ作成装置の処理内容を示すフローチ

ャートである。
【図１３】本発明の一実施形態に係る暗号化処理の内容を示すフローチャートである。
【図１４】本発明の一実施形態に係るＧｅｔＰｏｓの処理内容を示すフローチャートである。
【図１５】本発明の一実施形態に係る電子投票装置の処理内容を示すフローチャートである。
【図１６】本発明の一実施形態に係る電子開票装置の処理内容を示すフローチャートである。
【図１７】本発明の一実施形態に係るビットの対応付けテーブルを示す図である。
【図１８】本発明の一実施形態に係る電子投票データ作成装置において、電子投票データ５２１を作成する例を示す図である。
【図１９】本発明の一実施形態に係る電子投票装置において、電子投票データを表示する例を示す図である。
【図２０】本発明の一実施形態に係る電子開票装置において、電子投票データを集計し、公表する例を示す図である。
【図２１】本発明の一実施形態に係る暗号化装置の機能を示す機能ブロック図である。
【図２２】本発明の一実施形態に係る電子投票媒体の機能を示す機能ブロック図である。
【図２３】本発明の一実施形態に係る電子投票媒体の例を示す図である。
【図２４】本発明の一実施形態に係る電子投票媒体を利用した電子投票システムの例を示す図である。
【図２５】本発明の一実施形態に係る電子投票媒体を利用する投票プログラムの処理内容を示すフローチャートである。
【図２６】本発明の一実施形態に係る電子投票媒体の処理内容を示すフローチャートである。
【図２７】本発明の一実施形態に係る電子投票媒体を利用する場合の電子投票データ作成装置の処理内容を示すフローチャートである。
【図２８】本発明の一実施形態に係る電子投票媒体を利用する場合の電子開票装置の処理内容を示すフローチャートである。
【発明を実施するための形態】
【００３０】
以下、本発明の実施形態について図を参照しながら説明する。すなわち、実施形態１において、本発明に係る暗号方法を利用する電子投票システム１０について説明し、実施形態２において、本発明に係る暗号方法を利用し、パスワードを用いる電子投票システム１０について説明し、実施形態３において、本発明に係る暗号化装置４００について説明し、実施形態４において、本発明に係る暗号方法を利用する電子投票媒体７００について説明する。
【００３１】
［実施形態１］
実施形態１は、電子投票システム１０の実施例である。実施形態１の電子投票システム１０は、電子投票データ作成装置１００と、電子投票装置２００と、電子開票装置３００とを備えている。そして、電子投票データ作成装置１００は、全体画像データ５０１に基づいて作成した鍵ペア（公開鍵と秘密鍵）のうち公開鍵を分割画像データ５１１に埋め込んで、電子投票データ５２１を作成する。電子投票装置２００は、受け付けた投票内容及び確認コードを、電子投票データ５２１に埋め込まれた公開鍵を用いて暗号化し電子投票データ５２１に埋め込む。電子開票装置３００は、収集した分割画像データ５１１に基づいて作成した鍵ペア（公開鍵と秘密鍵）のうち秘密鍵を用いて、電子投票データ５２１に埋め込まれた暗号化された投票内容及び確認コードを復号し、公表する。
【００３２】
本実施形態は、コンピュータ及びその周辺装置に適用される。本実施形態における電子投票データ作成装置１００、電子投票装置２００及び電子開票装置３００は、コンピュー

タ及びその周辺装置が備えるハードウェア並びに該ハードウェアを制御するソフトウェアによって構成される。

【００３３】

上記ハードウェアには、制御部としてのＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）の他、記憶部、通信装置、表示装置及び入力装置が含まれる。記憶部としては、例えば、メモリ（ＲＡＭ：Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ、ＲＯＭ：Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ等）、ハードディスクドライブ（ＨＤＤ：Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）及び光ディスク（ＣＤ：Ｃｏｍｐａｃｔ Ｄｉｓｋ、ＤＶＤ：Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ等）ドライブが挙げられる。通信装置としては、例えば、各種有線及び無線インターフェース装置が挙げられる。表示装置としては、例えば、液晶ディスプレイやプラズマディスプレイ等の各種ディスプレイが挙げられる。入力装置としては、例えば、キーボード及びポインティング・デバイス（マウス、トラッキングボール等）が挙げられる。

【００３４】

上記ソフトウェアには、上記ハードウェアを制御するコンピュータ・プログラムやデータが含まれる。コンピュータ・プログラムやデータは、記憶部により記憶され、制御部により適宜実行、参照される。また、コンピュータ・プログラムやデータは、通信回線を介して配布されることも可能であり、ＣＤ－ＲＯＭ等のコンピュータ可読媒体に記録して配布されることも可能である。

【００３５】

図１は、本発明の一実施形態に係る電子投票システム１０の実施形態１の特徴を示す特徴図である。特徴図に従って、電子投票システム１０の概要を各装置ごとに説明する。

【００３６】

電子投票データ作成装置１００は、全体画像データ５０１を分割し、当該分割された分割画像データ５１１に、全体画像データ５０１に基づいて作成した公開鍵を埋め込むことにより複数の電子投票データ５２１を固有に作成する。すなわち、電子投票データ作成装置１００は、分割画像データ５１１を構成する画素値に基づいて、電子投票データ５２１ごとに異なる位置に公開鍵を埋め込んで、電子投票データ５２１を作成する。

【００３７】

ここで、全体画像データ５０１は、画像の最小要素である画素によって構成されたデジタル画像データである。デジタル画像データは、画素の輝度や色をデジタル化した画素値によって構成される。画素値は、例えば、色の３原色のうち赤色をデジタル化した階調値を記憶するＲチャネル、緑色をデジタル化した階調値を記憶するＧチャネル、青色をデジタル化した階調値を記憶するＢチャネル等から構成される。そして、例えば、デジタル画像データは、画素値が２次元配列形式でメインメモリや、補助記憶装置等に記憶されている。分割画像データ５１１は、全体画像データ５０１を所定の数で分割した画像データである。

【００３８】

ここで、人間の視覚は、画像を構成する３原色のうち青色の変化に気づきにくい、という特徴がある。そこで、本発明は、画像を構成する３原色の階調値のうちＢチャネルにデータを隠すことによって、画像に暗号化ブックの役割をさせつつ、画像が視認されても違和感を与えないようにすることができる。

【００３９】

電子投票データ作成装置１００は、全体画像データ５０１を構成する画素値に基づいて所定の演算を行い、公開鍵を作成する。所定の演算とは、例えば、全体画像データ５０１を構成する画素値のうち、公開鍵を書き込む所定のチャネル（格納用チャネルといい、例えば、Ｂチャネル）以外のチャネル（算出用チャネルといい、例えば、Ｒチャネル及び／又はＧチャネル）の階調値を、加算することやビット演算を行うこと等である。そして、電子投票データ作成装置１００は、所定の演算の演算結果である全体画像コードに基づいて、例えば、ＲＳＡ暗号方式によって作成される鍵ペア（公開鍵と秘密鍵）を作成する。

【００４０】
例えば、電子投票データ作成装置１００は、まず、適当な正整数ｅ（例えば、６０００１）を選択する。次に、電子投票データ作成装置１００は、全体画像コードをパラメータにランダムに大きい素数の組み（ｐ、ｑ）を求め、ｐとｑとの積であるＮを求める。そして、電子投票データ作成装置１００は、得られた（ｅ、Ｎ）を公開鍵とする。この場合、秘密鍵ｄは、$d = e^{-1}$（ｍｏｄ（ｌｃｍ（ｐ－１）（ｑ－１））によって求められる。

【００４１】
さらに、電子投票データ作成装置１００は、全体画像コードと、入力されたコード（例えば、図９で後述する秘密コード）とに基づいて算出したコード（例えば、図９で後述する暗号秘密コード）に基づいて大きい素数の組み（ｐ、ｑ）を求め、鍵ペア（公開鍵と秘密鍵）を作成するとしてもよい。

【００４２】
そして、電子投票データ作成装置１００は、データを埋め込む方法によって、公開鍵を分割画像データ５１１に埋め込む。

【００４３】
データを埋め込む方法は、次の（１）から（３）の方法によってデータを埋め込む。
（１）データを埋め込むための複数の画素を算出する。複数の画素は次の様に算出される。
（１－１）分割画像データ５１１を構成する画素の各算出用チャネルの階調値に基づいて所定の演算を行う。すなわち、分割画像データ５１１を構成する各画素の階調値のビットの重みを用いて所定の個数の擬似乱数を生成する。所定の個数の擬似乱数は、分割画像データ５１１内に設定された領域内の画素に基づいて所定の演算によって算出されるとしてもよい。
（１－２）生成された所定の個数の擬似乱数に基づいて、分割画像データ５１１内の所定の個数の位置を算出する。例えば、位置の算出は、生成した擬似乱数を、分割画像データ５１１の総画素数（縦の画素数×横の画素数）で除算した剰余によって、分割画像データ５１１内の位置（縦及び横の位置）を算出することができる。このように、各画素の階調値から生成した擬似乱数に基づいて算出した位置は、分割画像データ５１１が異なると異なる位置になる。よって、位置の算出は、分割画像データ５１１ごとに、予測できない分散された位置を算出することができる。

【００４４】
（２）算出した複数の画素の各格納用チャネルの所定のビットに、ビットの重みを対応付ける。すなわち、各格納用チャネルの所定のビット（例えば、公開鍵を埋め込むビットは３）に、（１）で算出した順にビットの重みを対応付ける。例えば、最初に算出した画素の格納用チャネルの所定のビット（例えば、ビット３）にビットの重み「2^0」を対応付ける。同様にして、ｎ番目に算出した画素の格納用チャネルの所定のビット（例えば、ビット３）にビットの重み「2^n」を対応付ける。

【００４５】
（３）ビットの重みが対応付けられた所定のビットに、データのバイナリ値をビットに分解して書き込むことによりデータを埋め込む。すなわち、例えば、「2^0」が対応付けられた、最初に算出された画素の格納用チャネルのビット３に、公開鍵のバイナリ値を構成するビットのうち「2^0」ビットの値を書き込む。次に、「2^1」が対応付けられた、次に算出された画素の格納用チャネルのビット３に、公開鍵のバイナリ値を構成するビットのうち「2^1」ビットの値を書き込む。このように順次、「2^n」が対応付けられた、算出された画素の格納用チャネルのビット３に、公開鍵のバイナリ値を構成するビットのうち「2^n」ビットの値を書き込むことによって公開鍵を埋め込む。

【００４６】
格納用チャネルの所定のビットは、例えば、ビット１が暗号化された投票内容及び確認コードを埋め込むビット、ビット２が暗号化されたパスワードを埋め込むビット、ビット

３が公開鍵を埋め込むビット、ビット４が画像の固有コード（ＭＤ５）を埋め込むビット、ビット５が全体画像コードの冗長情報を埋め込むビット、ビット６が電子投票データ５２１の投票状態（例えば、白票状態を０、投票済み状態を１で示す）についての情報を埋め込むビットである。

【００４７】

データを埋め込む方法によって埋め込まれたデータは、データを復元する方法によって埋め込まれたデータを復元することができる。

【００４８】

データを復元する方法は、上述したデータを埋め込む方法の（３）において、埋め込まれたビットの値を、格納チャネルの所定のビットに対応付けられたビットの重みに従って、バイナリ値に合成することによってデータを復元する。

【００４９】

このように、データを埋め込む方法は、画像データによって異なる画素の位置にデータを埋め込む。そして、データを復元する方法は、データを埋め込む方法によって埋め込まれた画像データに基づいてデータを復元する。すなわち、データを埋め込む方法は、画像データを暗号ブックとしてデータを暗号化し、データを復元する方法は、暗号ブックである画像データに基づいてデータを復元する。したがって、画像データである電子投票データ５２１を用いる電子投票システム１０は、電子投票データ５２１ごとの異なる位置にデータを秘匿するという、従来の暗号化をさらに安全にした暗号化を実行する。

【００５０】

このように、電子投票データ作成装置１００は、分割画像データ５１１に公開鍵を埋め込むことにより複数の電子投票データ５２１をそれぞれ固有に作成できる。

【００５１】

ここで、電子投票データ５２１における鍵ペア（公開鍵と秘密鍵）による暗号化と復号とに付いて説明する。電子投票データ作成装置１００によって全体画像コードに基づいて作成された鍵ペア（公開鍵と秘密鍵）のうちの公開鍵を用いて暗号化されたデータ（例えば、投票内容及び確認コード）は、作成された鍵ペア（公開鍵と秘密鍵）のうちの秘密鍵を用いて復号される。

【００５２】

例えば、電子投票データ作成装置１００は、投票率が棄権票や白紙票を含めて１００パーセントであれば復号可能であることを条件として電子投票データ５２１を作成する。この場合には、収集した電子投票データ５２１によって全体画像データ５０１を構成する画素の全てを取得することができるので、復号は、電子投票データ作成装置１００と同様に、算出された全体画像コードに基づいて作成された鍵ペア（公開鍵と秘密鍵）のうちの秘密鍵を用いることによって可能である。

【００５３】

また、例えば、電子投票データ作成装置１００は、投票率が一定の割合以上であれば復号可能であることを条件として電子投票データ５２１を作成する。この場合には、電子投票データ作成装置１００は、信号訂正理論を利用して、複数の電子投票データ５２１に基づいて鍵ペア（公開鍵と秘密鍵）を算出することができるように、全体画像コードの冗長情報を作成し、電子投票データ５２１ごとに埋め込む。このようにして、複数の電子投票データ５２１に埋め込まれた冗長情報に基づいて復元された全体画像コードを取得することができるので、復号は、電子投票データ作成装置１００と同様に、復元された全体画像コードに基づいて作成された鍵ペア（公開鍵と秘密鍵）のうちの秘密鍵を用いることによって可能である。

【００５４】

また、例えば、電子投票データ作成装置１００は、ビット列をＳとする全体画像コードを含んだデータ（例えば、全体画像コードのビット列Ｓに余分のビット列を補足したデータ、「１０１０」＋Ｓや、Ｓ＋「１０１０」や、「１０」＋Ｓ＋「１０」等）を作成し、電子投票データ５２１ごとに埋め込む。そうすると、全体画像コードは、２件の電子投票

データ５２１から必ず取得される（２件の電子投票データ５２１に書き込まれた全体画像コードを含んだデータを比較することによって同じビット列である全体画像コードＳが取得される）。このようにして、複数の電子投票データ５２１に基づいて全体画像コードを取得することができるので、復号は、電子投票データ作成装置１００と同様に、取得された全体画像コードに基づいて作成された鍵ペア（公開鍵と秘密鍵）のうちの秘密鍵を用いることによって可能である。すなわち、電子投票データ作成装置１００は、全体画像データ５０１を分割画像データ５１１に分割する数を、求められる投票率に従って算出することにより、条件とする投票率に合致した電子投票データ５２１を作成することができる。

【００５５】

また、例えば、電子投票データ作成装置１００は、投票された電子投票データ５２１が１件でも復号可能であることを条件として電子投票データ５２１を作成する。この場合には、電子投票データ作成装置１００は、全体画像コードを電子投票データ５２１ごとに埋め込む。埋め込まれた全体画像コードによって、復号は、電子投票データ作成装置１００と同様に、埋め込まれた全体画像コードに基づいて作成された鍵ペア（公開鍵と秘密鍵）のうちの秘密鍵を用いることによって可能である。

【００５６】

電子投票装置２００は、電子投票データ５２１に埋め込まれている公開鍵に基づいて、受け付けた投票ごとの投票内容と、投票内容に対応付けた確認コードとを暗号化する。そして、電子投票装置２００は、当該暗号化された投票内容及び確認コードを電子投票データ５２１に埋め込む。ここで、投票内容は、例えば、立候補者を示す番号やコード等である。電子投票装置２００は、投票者によって操作された入力装置から投票内容を受け付ける。確認コードは、例えば、電子投票装置２００が投票内容に対応付けたコードである。

【００５７】

電子投票装置２００は、電子投票データ５２１から公開鍵を復元する。すなわち、電子投票装置２００は、電子投票データ作成装置１００によって埋め込まれた公開鍵を、復元する方法によって復元する。

【００５８】

電子投票装置２００は、復元した公開鍵によって、投票内容及び確認コードを暗号化する。そして、電子投票装置２００は、暗号化した投票内容及び確認コードを、データを埋め込む方法によって電子投票データ５２１に埋め込む（例えば、格納用チャネルのビット１）。

【００５９】

電子開票装置３００は、複数の電子投票装置２００によって暗号化された各電子投票データ５２１を収集する。次に、電子開票装置３００は、収集した各電子投票データ５２１に基づいて秘密鍵を作成し、作成した秘密鍵に基づいて、収集した各電子投票データ５２１から取得した暗号化された投票内容及び確認コードを復号する。そして、電子開票装置３００は、当該復号した投票内容及び確認コードを集計し、公表する。

【００６０】

ここで、秘密鍵は、電子投票データ作成装置１００と同様に作成される。すなわち、電子開票装置３００は、収集した電子投票データ５２１に基づいて全体画像コードを取得し、取得した全体画像コードに基づいて、例えば、ＲＳＡ暗号方式によって作成される鍵ペア（公開鍵と秘密鍵）のうちの秘密鍵を作成する。そして、電子開票装置３００は、作成した秘密鍵に基づいて、電子投票データ５２１から復元した、暗号化された投票内容及び確認コードを復号する。この場合に、正しい秘密鍵を作成することができるように電子投票データ５２１を収集できなかったり、不正な電子投票データ５２１が混じっていたりした場合には、作成した秘密鍵では投票内容を正しく復元し、復号することができないので、電子開票装置３００は、投票が正しく行われなかったことを検出することができる。

【００６１】

そして、電子開票装置３００は、復号した投票内容及び確認コードを集計し、公表する。確認コードは、投票内容に対応付けられたコードであるので、電子開票装置３００は、

投票内容及び確認コードを公表することによって、確認コードを覚えている投票者に、投票内容が正確に集計されていることを確認させることができる。

【００６２】

このように、電子投票データ作成装置１００とは独立して、電子開票装置３００が収集した電子投票データ５２１に基づいて秘密鍵を作成することによって、電子投票システム１０は、システムの安全性を向上させることができる。

【００６３】

図２から図７によって電子投票データ５２１の作成を説明する。

図２は、本発明の一実施形態に係る全体画像データ５０１の例を示す図である。図２の例は、全体画像データ５０１を、縦の破線５９１及び横の破線５９２によって、１６分割する例である。全体画像データ５０１を分割することによって分割画像データ５１１が作成される。

【００６４】

全体画像データ５０１を構成する画素値に基づいて、全体画像コードが算出される。例えば、全体画像データ５０１がＸ軸方向に６４０×４画素、Ｙ軸方向に４８０×４画素であるとする。画素を構成する３原色の階調値を記憶するチャネルのうち、格納用チャネルは、Ｂチャネルとし、算出用チャネルは、Ｒチャネル及びＧチャネルとする。各チャネルは、例えば、８ビット構成とする。

【００６５】

例えば、全体画像コード（例えば、１０２４ビット）は、ＲチャネルおよびＧチャネルの階調値を加算することにより得られる。加算は、チャネル単位（８ビットずつ）でなくてもよい。例えば、９ビットずつ（Ｒチャネルの８ビット及びＧチャネルのＬＳＢと、Ｇチャネルの残り７ビット及び次の画素のＲチャネルの２ビットとを）加算する。このようにすることで、特定のビットの値が周期的に加算されることを避けることができる。電子投票システム１０は、全体画像コードに基づいて鍵ペア（公開鍵及び秘密鍵）を作成する。

【００６６】

図３は、本発明の一実施形態に係る分割画像データ５１１の例を示す図である。図３が示す例は、分割画像データ５１１に基づいて、図４のようにデータを埋め込むための複数の画素（例えば、Ｐ１からＰ１０）を算出し、図５のようにデータを埋め込んだことを示す例である。

【００６７】

図３の分割画像データ５１１は、図２の全体画像データ５０１を、例えば１６分割した画像データである。分割画像データ５１１を構成する画素の位置は、二次元座標（例えば、ＸＹ平面のＸ軸及びＹ軸）を用いて表わされる。例えば、Ｘ軸方向の画素数をｗ（例えば、６４０画素）、Ｙ軸方向の画素数をｈ（例えば、４８０画素）とすると、画素の位置は、開始点（０、０）、終了点（６３９、４７９）、任意の画素の位置（ｘ、ｙ）で表わされる。ここで、図４に基づいて、分割画像データ５１１を構成する画素に基づいて生成した擬似乱数によって所定の個数の画素の位置を算出することについて説明する。

【００６８】

図４は、本発明の一実施形態に係る分割画像データ５１１を構成する画素の階調値と、擬似乱数の生成とについて説明する説明図である。

【００６９】

図４（１）は、分割画像データ５１１を構成する画素の階調値の構成の例を示している。図４（１）が示す例は、各画素を構成する３原色のうち赤色の階調値を記憶するＲチャネルと、緑色の階調値を記憶するＧチャネルと、青色の階調値を記憶するＢチャネルとをメモリ上に記憶していることを示す例である。そして、図４（１）が示す例は、各画素の画像データ内の位置を、ＸＹ平面上の位置で表わした場合を示す例である。

【００７０】

図４（２）は、画素の階調値に基づいて所定の個数の擬似乱数を生成するための所定の演算について説明する図である。電子投票システム１０は、所定の演算によって生成した

所定の個数の擬似乱数に基づいて、所定の個数の画素の位置を算出することができる。

【００７１】

ここで、１番目の画素のＲチャネルのそれぞれのビットの値をＰ０Ｒ０からＰ０Ｒ７で表わし、ｎ番目の画素のＲチャネルのそれぞれのビットの値をＰｎＲ０からＰｎＲ７で表わす。同様に、１番目の画素のＧチャネルのそれぞれのビットの値をＰ０Ｇ０からＰ０Ｇ７で表わし、ｎ番目の画素のＧチャネルのそれぞれのビットの値をＰｎＧ０からＰｎＧ７で表わす。すなわち、Ｒチャネル及びＧチャネルのビット値は次の様な並びで表わせる。

【００７２】

１番目のＲチャネルのビット値＝Ｐ０Ｒ０、Ｐ０Ｒ１、Ｐ０Ｒ２、Ｐ０Ｒ３、Ｐ０Ｒ４、Ｐ０Ｒ５、Ｐ０Ｒ６、Ｐ０Ｒ７

１番目のＧチャネルのビット値＝Ｐ０Ｇ０、Ｐ０Ｇ１、Ｐ０Ｇ２、Ｐ０Ｇ３、Ｐ０Ｇ４、Ｐ０Ｇ５、Ｐ０Ｇ６、Ｐ０Ｇ７

・

・

ｎ番目のＲチャネルのビット値＝ＰｎＲ０、ＰｎＲ１、ＰｎＲ２、ＰｎＲ３、ＰｎＲ４、ＰｎＲ５、ＰｎＲ６、ＰｎＲ７

ｎ番目のＧチャネルのビット値＝ＰｎＧ０、ＰｎＧ１、ＰｎＧ２、ＰｎＧ３、ＰｎＧ４、ＰｎＧ５、ＰｎＧ６、ＰｎＧ７

・

・

【００７３】

所定の演算は、データを埋め込むために必要なｎ個（例えば、１０２４個）の擬似乱数を生成する。所定の演算は、例えば、Ｄａｔ［ｉ］＝Ｄａｔ［ｉ］＋Ｘ（ｋ）＊２^{k}のように表わすことができる。ここで、Ｘ（ｋ）は、Ｒチャネル又はＧチャネルの階調値のｋビット目の値である。データを埋め込むために必要な個数より１個多い変数を用いて演算を実行することで、所定の演算は、ある特定のビットの数値がある特定の変数に演算されるような周期的配置になることを避けることができる。

【００７４】

例えば、１０２４個の擬似乱数を生成するための所定の演算は次の様に行われる。

１巡目

Ｄａｔ［０］＝Ｄａｔ［０］＋Ｐ０Ｒ０＊２^{0}

Ｄａｔ［１］＝Ｄａｔ［１］＋Ｐ０Ｇ０＊２^{0}

・

・

Ｄａｔ［１０２２］＝Ｄａｔ［１０２２］＋Ｐ６３Ｒ７＊２^{7}

Ｄａｔ［１０２３］＝Ｄａｔ［１０２３］＋Ｐ６３Ｇ７＊２^{7}

Ｄａｔ［１０２３＋１］＝Ｄａｔ［１０２３＋１］＋Ｐ６４Ｒ０＊２^{0}

２巡目

Ｄａｔ［０］＝Ｄａｔ［０］＋Ｐ６４Ｇ０＊２^{0}

Ｄａｔ［１］＝Ｄａｔ［１］＋Ｐ６４Ｒ１＊２^{1}

・

・

Ｄａｔ［１０２２］＝Ｄａｔ［１０２２］＋Ｐ１２７Ｇ７＊２^{7}

Ｄａｔ［１０２３］＝Ｄａｔ［１０２３］＋Ｐ１２８Ｒ０＊２^{0}

Ｄａｔ［１０２３＋１］＝Ｄａｔ［１０２３＋１］＋Ｐ１２８Ｇ０＊２^{0}

このような演算により、例えば、１０２５個の乱数のうち最初の１０２４個の疑似乱数を得る。

【００７５】

次に、生成された所定の個数（例えば、１０２４個）の擬似乱数に基づいて、分割画像データ５１１内の所定の個数（例えば、１０２４個）の画素の位置を算出する。例えば、

生成した擬似乱数（Ｄａｔ［０］からＤａｔ［１０２３］）を分割画像データ５１１の縦の画素数及び横の画素数でそれぞれ除算した剰余（Ｄａｔ［０］　ｍｏｄ　ｗ、Ｄａｔ［０］　ｍｏｄ　ｈ）によって、分割画像データ５１１内の位置（縦及び横の位置）を算出することができる。

【００７６】

ここで、位置の算出において、剰余演算の法をそれぞれ（ｗ－２）と（ｈ－１）にすることで、Ｄａｔ［ｉ］に基づく位置の生成は、画像の対角線の近くに集中することを回避することができる。

【００７７】

このようにして算出された位置が重複している場合には、ハッシュ変換が行われる。ハッシュ変換は、算出された位置を重複しない位置に変換する。例えば、分割画像データ５１１の画素の位置と、使用しているか否かのフラグを対応付けたハッシュテーブルを用いて、ハッシュ変換は、算出された位置が使用されている場合には、使用していない位置に変換することができる。または、ハッシュ変換は、ハッシュ変換のための演算（例えば、新格納位置ｘ＝（格納位置ｘ＋２３）ｍｏｄ（ｗ）、新格納位置ｙ＝（格納位置ｙ＋１１）ｍｏｄ（ｈ）を行うとしてもよい。

【００７８】

ここで、図３に戻って、図３が示すＰ１からＰ１０は、上述のようにして算出された分割画像データ５１１内の画素である。ここで、図５に基づいて、算出された画素にデータを埋め込むことについて説明する。

【００７９】

図５は、本発明の一実施形態に係る分割画像データ５１１において、データのバイナリ値をビットに分解して埋め込むことを説明する図である。

【００８０】

電子投票システム１０は、上述のようにして算出した複数の画素の各格納用チャネルの所定のビットに、ビットの重みを対応付ける。すなわち、電子投票システム１０は、各格納用チャネルの所定のビット（例えば、公開鍵を埋め込むビットは３）に、複数の画素を算出した順にビットの重みを対応付ける。例えば、電子投票システム１０は、擬似乱数Ｄａｔ［０］に基づいて位置を算出し、算出した画素Ｐ１の格納用チャネルの所定のビット（例えば、ビット３）にビットの重み「2^{0}」を対応付ける。同様にして、電子投票システム１０は、擬似乱数Ｄａｔ［ｎ－１］に基づいて位置を算出し、算出した画素Ｐｎの格納用チャネルの所定のビット（例えば、ビット３）にビットの重み「2^{n-1}」を対応付ける。

【００８１】

電子投票システム１０は、ビットの重みが対応付けられた所定のビットに、データのバイナリ値をビットに分解して書き込むことによりデータを埋め込む。すなわち、電子投票システム１０は、例えば、ビットの重み「2^{0}」が対応付けられた画素Ｐ１の格納用チャネルのビット３に、公開鍵のバイナリ値を構成するビットのうち「2^{0}」ビットの値を書き込む。次に、電子投票システム１０は、「2^{1}」が対応付けられた画素Ｐ２の格納用チャネルのビット３に、公開鍵のバイナリ値を構成するビットのうち「2^{1}」ビットの値を書き込む。このように順次、電子投票システム１０は、ビットの重み「2^{n-1}」が対応付けられた画素の格納用チャネルのビット３に、公開鍵のバイナリ値を構成するビットのうち「2^{n-1}」ビットの値を書き込むことによって公開鍵を埋め込む。このようにして、電子投票データ５２１は、作成される。

【００８２】

ここで、図３に戻って、図３が示すＰ１からＰ１０は、上述のようにして算出された分割画像データ５１１内の画素に、データを構成するビットを埋め込んだ画素である。

【００８３】

図６は、本発明の一実施形態に係る分割画像データ５１１の別の例を示す図である。図６が示す例は、データを埋め込むための画素が、分割画像データ５１１内に設定された領

域６０１内の画素の階調値に基づいて算出されることを示す例である。
【００８４】
分割画像データ５１１内に設定された領域６０１は、ＸＹ平面内において、開始点６１１（ａ、ｂ）と、終了点６１２（ａ＋Ａ、ｂ＋Ｂ）とによって表わされる。ここで、Ａは、Ｘ方向の幅、Ｂは、Ｙ方向の高さである。
【００８５】
分割画像データ５１１内に設定された領域６０１を構成する画素の階調値に基づいて、上述の様に擬似乱数が生成され、生成された擬似乱数に基づいてデータを埋め込む複数の画素の位置が、算出される。そして、算出された複数の画素の各格納用チャネルの所定のビットにデータが、埋め込まれる。
【００８６】
領域６０１は、開始位置及び領域の大きさを示すパラメータによって設定される。例えば、領域６０１を構成する画素に基づいてデータを埋め込むための複数の画素を算出する関数は、ＧｅｔＰｏｓ（＊ｐｏｓ，ｎｕｍ，ｐａｒ）のように表わされる。
【００８７】
ここで、＊ｐｏｓは、データを埋め込むための複数の画素へのポインタを示し、ｎｕｍは、データを埋め込むための複数の画素の個数を示し、ｐａｒは、開始位置へのパラメータを示す引数である。すなわち、ＧｅｔＰｏｓ（＊ｐｏｓ，ｎｕｍ，ｐａｒ）は、ｐａｒによって領域の開始位置（ａ＋ｐａｒ、ｂ＋ｐａｒ）を求め、領域の大きさ（幅がＡ、高さがＢ）を設定する。そして、ＧｅｔＰｏｓ（＊ｐｏｓ，ｎｕｍ，ｐａｒ）は、設定した領域を構成する画素の階調値に基づいて、上述の様にｎｕｍ個の擬似乱数を生成し、生成した擬似乱数に基づいて複数の画素の位置を算出し、算出した画素へのポインタを返す。ここで、ａ、ｂ、Ａ及びＢは、例えば、パラメータ記憶部（図９、図１０及び図１１で後述する作成パラメータ記憶部１３１、投票パラメータ記憶部２３１及び開票パラメータ記憶部３３１）に予め記憶されている。また、この値が、ａ＝ｂ＝０、Ａ＝電子投票データ５２１の幅、Ｂ＝電子投票データ５２１の高さの場合、ＧｅｔＰｏｓ（＊ｐｏｓ，ｎｕｍ，０）は、電子投票データ５２１全体を構成する画素に基づいてデータを埋め込むための複数の画素を算出する。
【００８８】
図７は、本発明の一実施形態に係る電子投票データ５２１のデータを埋め込むための複数の画素の位置を算出するために設定される領域の例を示す図である。
【００８９】
図７（１）が示す例は、領域６０１内の画素に基づいて、公開鍵と、冗長情報と、投票内容及び確認コードとを埋め込むことを示す例である。例えば、電子投票データ作成装置１００は、ＧｅｔＰｏｓ（＊ｐｏｓ，１０２４，０）によって得られる１０２４個の画素６２１のＢチャネルのビット３に、１０２４ビットの公開鍵を構成するビットを、対応付けられたビットの重みに従って書き込むことによって公開鍵を埋め込む。同様に、電子投票データ作成装置１００は、Ｂチャネルのビット５に冗長情報を埋め込む。電子投票装置２００は、同様に、ＧｅｔＰｏｓ（＊ｐｏｓ，１０２４，０）によって取得した画素のＢチャネルのビット３から公開鍵を復元する。そして、電子投票装置２００は、Ｂチャネルのビット１に、復元した公開鍵によって暗号化した投票内容及び確認コードを埋め込む。電子開票装置３００は、同様に、ＧｅｔＰｏｓ（＊ｐｏｓ，１０２４，０）によって取得した画素のＢチャネルのビット５から冗長情報を復元し、複数の電子投票データ５２１から復元した冗長情報に基づいて全体画像コードを作成し、作成した全体画像コードに基づいて算出した秘密鍵によって、Ｂチャネルのビット１から復元した投票内容及び確認コードを復号する。
【００９０】
図７（２）が示す例は、後述する実施形態２において、領域６０１内の画素に基づいて、公開鍵と、冗長情報と、暗号化されたパスワードとを埋め込み、領域６０２内の画素に基づいて、投票内容及び確認コードを埋め込むことを示す例である。ここで、パスワード

は、電子投票装置２００において受け付けられるコードである（後述する実施形態２の図１０参照）。また、領域６０２は、パスワードに基づいて作成した値（Ｃｉ）をパラメータ（ｐａｒ＝Ｃｉ）とする領域である。例えば、電子投票データ作成装置１００は、図７（１）と同様に、公開鍵と、冗長情報とを埋め込む。電子投票装置２００は、図７（１）と同様に、公開鍵を復元し、受け付けたパスワードを暗号化する。そして、電子投票装置２００は、ＧｅｔＰｏｓ（＊ｐｏｓ，１０２４，０）によって取得した画素６２１のＢチャネルのビット２に、暗号化したパスワードを埋め込むと共に、ＧｅｔＰｏｓ（＊ｐｏｓ，１０２４，Ｃｉ）によって取得した画素６２２のＢチャネルのビット１に、受け付けた投票内容及び確認コードを埋め込む。

【００９１】

図７（３）が示す例は、後述する実施形態２において、図７（２）の例に加えて、さらに領域６０３内の画素に基づいて、固有コード（ＭＤ５）を埋め込むことを示す例である。ここで、固有コード（ＭＤ５）は、電子投票データ作成装置１００が分割画像データ５１１に基づいて作成したコードである（後述する実施形態２の図９参照）。また、領域６０３は、電子投票データ作成装置１００が受け付けた秘密コードに基づいて作成した値（ＣＡＳ）を、パラメータ（ｐａｒ＝ＣＡＳ）とする領域である。例えば、電子投票データ作成装置１００は、秘密コードを受け付ける（後述する実施形態２の図９参照）。そして、電子投票データ作成装置１００は、秘密コードと、全体画像コードとに基づいて公開鍵と、冗長情報とを作成し、埋め込む。そして、電子投票データ作成装置１００は、ＧｅｔＰｏｓ（＊ｐｏｓ，１０２４，ＣＡＳ）によって取得した画素６２３のＢチャネルのビット４に、固有コード（ＭＤ５）を埋め込む。電子開票装置３００は、復元した固有コード（ＭＤ５）が同一の電子投票データ５２１同士を一の電子投票データ５２１とみなす。

【００９２】

［実施形態２］

実施形態２は、電子投票システム１０の実施例であって、実施形態１に加えて、電子投票データ作成装置１００は、全体画像コードと受け付けた秘密コードとに基づいて公開鍵を作成し、固有コード（ＭＤ５）を作成して電子投票データ５２１に埋め込む。電子投票装置２００は、パスワードを受け付け、投票内容及び確認コードをパスワードに基づいて電子投票データ５２１に埋め込み、パスワードを暗号化して電子投票データ５２１に埋め込む。電子開票装置３００は、同じ固有コード（ＭＤ５）の電子投票データ５２１を一の電子投票データ５２１とみなす。そして、電子開票装置３００は、開票条件を判断し、電子投票データ作成装置１００と同様に、全体画像コードと受け付けた秘密コードとに基づいて作成した秘密鍵に基づいて、電子投票データ５２１に埋め込まれた暗号化されたパスワードを復号し、復号したパスワードに基づいて投票内容及び確認コードを取得し、公表する。各装置の詳細について、図８から図２０に従って、説明する。

【００９３】

図８は、本発明の一実施形態に係る電子投票システム１０の実施形態２の特徴を示す特徴図である。実施形態２の電子投票システム１０は、実施形態１に加えて、秘密コードと、パスワードとを受け付け、固有コード（ＭＤ５）を作成する。特徴図に従って、電子投票システム１０の概要を各装置ごとに説明する。

【００９４】

電子投票データ作成装置１００は、実施形態１に加えて、投票管理委員会によって入力された秘密コードを受け付ける。そして、電子投票データ作成装置１００は、全体画像データ５０１の一部を変更し、受け付けた秘密コードと、全体画像コードとに基づいて算出した暗号秘密コードに基づいて鍵ペア（公開鍵と秘密鍵）を作成する。そして、電子投票データ作成装置１００は、分割画像データ５１１内に設定された領域を構成する画素に基づいて、公開鍵を埋め込む位置を算出し、公開鍵を埋め込む。さらに、電子投票データ作成装置１００は、電子投票データ５２１に基づいて固有コード（ＭＤ５）を作成し、電子投票データ５２１に埋め込む。

【００９５】

電子投票装置２００は、実施形態１に加えて、パスワードを受け付ける。そして、電子投票装置２００は、受け付けたパスワードに基づいて作成した値（Ｃｉ）をパラメータ（ｐａｒ＝Ｃｉ）とする電子投票データ５２１内の領域を設定し、設定した領域を構成する画素に基づいて算出した位置の画素に、受け付けた投票内容及び確認コードを埋め込む。そして、電子投票装置２００は、受け付けたパスワードを、復元した公開鍵に基づいて暗号化し、電子投票データ５２１に埋め込む。

【００９６】

電子開票装置３００は、実施形態１に加えて、収集した電子投票データ５２１において、同一の固有コード（ＭＤ５）が存在するか否かを判断し、同一の固有コード（ＭＤ５）を有する電子投票データ５２１を一の電子投票データ５２１とみなす。さらに、電子開票装置３００は、秘密コードを受け付け、受け付けた秘密コードと、収集した電子投票データ５２１に基づいて作成した全体画像コードとに基づいて鍵ペア（公開鍵と秘密鍵）のうち秘密鍵を作成する。そして、電子開票装置３００は、復元したパスワードを秘密鍵に基づいて復号し、復号したパスワードに基づいて作成した値（Ｃｉ）をパラメータ（ｐａｒ＝Ｃｉ）とする電子投票データ５２１内の領域を設定し、設定した領域を構成する画素に基づいて復元した投票内容及び確認コードを集計し、公表する。

【００９７】

図９は、本発明の一実施形態に係る電子投票データ作成装置１００の機能を示す機能ブロック図である。電子投票データ作成装置１００は、秘密コード受付部１０１と、全体画像データ変更部１０２と、全体画像コード算出部１０３と、暗号秘密コード算出部１０４と、暗号鍵作成部１０５と、分割数設定部１０６と、全体画像分割部１０７と、作成領域設定部１０８と、公開鍵位置算出部１０９と、固有コード作成部１１０と、固有コード位置算出部１１１と、冗長情報書込部１１２と、電子投票データ作成部１１３と、電子投票データ出力部１１４と、作成パラメータ記憶部１３１とを備えている。このような電子投票データ作成装置１００について各部ごとに説明する。

【００９８】

作成パラメータ記憶部１３１は、電子投票データ５２１内に設定する領域についての所定のパラメータを記憶している。例えば、作成パラメータ記憶部１３１は、図６における、開始点の値（ａ、ｂ）と、領域の幅Ａと、領域の高さＢとを記憶している。

【００９９】

秘密コード受付部１０１は、秘密コード（ＣＡＳ）の入力を受け付ける。秘密コードは、例えば、１６桁からなるコードであって、選挙管理委員会によって秘密に管理されている。

【０１００】

全体画像データ変更部１０２は、全体画像データ５０１の一部を、乱数に基づいて変更する。全体画像データ変更部１０２は、例えば、全体画像データ５０１を構成する画素であって、各分割画像データ５１１に少なくとも１個入るように乱数に基づいて算出した画素について、その画素の算出用チャネルのビット０を反転する。

【０１０１】

全体画像コード算出部１０３は、全体画像データ５０１に基づいて全体画像コード（ＣＡＩ）を算出する。全体画像コードは、例えば、全体画像データ５０１を構成する３原色のうちの算出用チャネルの各階調値を、加算やビット演算等することによって算出される。

【０１０２】

暗号秘密コード算出部１０４は、秘密コード受付部１０１によって受け付けられた秘密コード（ＣＡＳ）と、全体画像コード算出部１０３によって算出された全体画像コード（ＣＡＩ）とに基づいて暗号秘密コード（ＣＡ）を算出する。暗号秘密コードは、秘密コードと全体画像コードとを、例えば、加算やビット演算等することによって算出される。

【０１０３】

暗号鍵作成部１０５は、暗号秘密コード算出部１０４によって算出された暗号秘密コー

ドに基づいて公開鍵（Ｎ、ｅ）と、公開鍵（Ｎ、ｅ）に対応する秘密鍵（ｄ）とを作成する。

【０１０４】

分割数設定部１０６は、全体画像データ５０１を分割する数を設定する。分割する数は、例えば、全体画像データ５０１を等分割することができる整数である。設定は、分割する数を、縦の分割数と横の分割数とによって入力されてもよい。

【０１０５】

全体画像分割部１０７は、分割数設定部１０６によって設定された数に基づいて全体画像データ５０１を分割する。例えば、設定された数が３×４の場合、全体画像分割部１０７は、縦を３分割し、横を４分割する。

【０１０６】

作成領域設定部１０８は、所定のパラメータに基づいて、全体画像分割部１０７によって分割された各分割画像データ５１１内に領域を設定する。例えば、設定する領域の開始位置への所定のパラメータがｐａｒ＝０である場合、作成領域設定部１０８は、作成パラメータ記憶部１３１に記憶された値と、ｐａｒとに基づいて、図７（３）の領域６０１を設定する。

【０１０７】

公開鍵位置算出部１０９は、作成領域設定部１０８によって設定された領域を構成する画素に基づいて、公開鍵を埋め込む公開鍵位置を算出する。すなわち、公開鍵位置算出部１０９は、上述のように領域６０１を構成する画素の階調値に基づいて、擬似乱数を生成し、生成した擬似乱数に基づいて複数の画素の位置を算出する。

【０１０８】

固有コード作成部１１０は、電子投票データ５２１に基づいて固有コード（ＭＤ５）を作成する。固有コード作成部１１０は、例えば、電子投票データ５２１を構成する画素の算出用チャネルの階調値を、加算やビット演算等し、電子投票データ５２１ごとに固有の固有コード（ＭＤ５）を作成する。

【０１０９】

固有コード位置算出部１１１は、作成領域設定部１０８によって設定された領域を構成する画素に基づいて固有コード（ＭＤ５）を埋め込む固有コード位置を算出する。例えば、固有コード位置算出部１１１は、秘密コード受付部１０１によって受け付けられた秘密コード（ＣＡＳ）に基づいて電子投票データ５２１内に設定された領域（例えば、図７（３）の領域６０３）を構成する画素に基づいて、固有コード（ＭＤ５）を埋め込む固有コード位置を算出する。そして、電子投票データ作成部１１３は、固有コード位置算出部１１１によって算出された固有コード位置に、固有コード（ＭＤ５）を埋め込む。

【０１１０】

冗長情報書込部１１２は、算出された複数の画素の各格納用チャネルの所定のビットに、全体画像コードの冗長情報をビットに分解して埋め込む。

【０１１１】

電子投票データ作成部１１３は、公開鍵位置算出部１０９によって算出された公開鍵位置に、暗号鍵作成部１０５によって作成された公開鍵（Ｎ、ｅ）を埋め込むことによって複数の電子投票データ５２１を固有に作成する。すなわち、電子投票データ作成部１１３は、上述のように、算出された複数の画素の各格納用チャネルの所定のビットに、公開鍵の値をビットに分解して埋め込む。

【０１１２】

電子投票データ出力部１１４は、電子投票データ作成部１１３によって作成された電子投票データ５２１を電子投票装置２００に出力する。例えば、電子投票データ出力部１１４は、コンピュータネットワークを介して電子投票データ５２１を電子投票装置２００に出力する。そして、電子投票データ出力部１１４は、電子投票データ５２１の投票状態を投票済み状態にする。

【０１１３】

図１０は、本発明の一実施形態に係る電子投票装置２００の機能を示す機能ブロック図である。電子投票装置２００は、投票入力部２０１と、投票領域設定部２０２と、投票公開鍵位置算出部２０３と、公開鍵取得部２０４と、投票受付部２０５と、パスワード受付部２０６と、投票内容領域設定部２０７と、投票内容位置算出部２０８と、パスワード暗号化部２０９と、パスワード位置算出部２１０と、投票書込部２１１と、再投票受付部２１２と、投票出力部２１３と、投票パラメータ記憶部２３１とを備えている。このような電子投票装置２００について各部ごとに説明する。

【０１１４】

投票入力部２０１は、電子投票データ５２１を入力する。投票入力部２０１は、例えば、コンピュータネットワークを介して電子投票データ作成装置１００から電子投票データ５２１を入力する。

【０１１５】

投票パラメータ記憶部２３１は、所定のパラメータを記憶する。所定のパラメータは、電子投票データ作成装置１００によって電子投票データ５２１内に公開鍵を埋め込むために設定された領域のパラメータ（作成パラメータ記憶部１３１の値）と同じである。

【０１１６】

投票領域設定部２０２は、投票パラメータ記憶部２３１に記憶された所定のパラメータに基づいて、投票入力部２０１によって入力された電子投票データ５２１を構成する画像データ内に領域を設定する。例えば、設定する領域の開始位置への所定のパラメータがｐａｒ＝０である場合、投票領域設定部２０２は、電子投票データ作成装置１００と同様に、図７（３）の領域６０１を設定する。

【０１１７】

投票公開鍵位置算出部２０３は、投票領域設定部２０２によって設定された領域を構成する画素に基づいて公開鍵位置を算出する。すなわち、投票公開鍵位置算出部２０３は、電子投票データ作成装置１００と同様に、公開鍵位置を算出する。

【０１１８】

公開鍵取得部２０４は、投票公開鍵位置算出部２０３によって算出された公開鍵位置から、電子投票データ作成装置１００によって埋め込まれた公開鍵を取得する。

【０１１９】

投票受付部２０５は、投票内容と、確認コードとの入力を受け付ける。

【０１２０】

パスワード受付部２０６は、パスワードの入力を受け付ける。

【０１２１】

投票内容領域設定部２０７は、パスワード受付部２０６によって受け付けられたパスワードに基づいて、電子投票データ５２１を構成する画像データ内に領域を設定する。例えば、投票内容領域設定部２０７は、パスワードに基づいて、設定する領域の開始位置への所定のパラメータ（Ｃｉ）を算出し、算出したパラメータによって、図７（３）の領域６０２を設定する。

【０１２２】

投票内容位置算出部２０８は、投票内容領域設定部２０７によって設定された領域を構成する画素に基づいて投票内容及び確認コードを埋め込む投票内容位置を算出する。

【０１２３】

パスワード暗号化部２０９は、公開鍵取得部２０４によって取得された公開鍵に基づいて、パスワード受付部２０６によって受け付けられたパスワードを暗号化する。

【０１２４】

パスワード位置算出部２１０は、電子投票データ５２１を構成する画素に基づいて、パスワード暗号化部２０９により暗号化されたパスワードを埋め込むパスワード位置を算出する。

【０１２５】

投票書込部２１１は、パスワード位置算出部２１０によって算出されたパスワード位置

に、パスワード暗号化部２０９によって暗号化されたパスワードを埋め込むと共に、投票内容位置算出部２０８によって算出された投票内容位置に、投票受付部２０５によって受け付けられた投票内容及び確認コードを埋め込む。

【０１２６】

再投票受付部２１２は、再度の投票を受け付ける。例えば、再投票受付部２１２は、再度の投票であることを受け付けると、電子投票データ５２１の投票状態を白票状態にする。そして、投票書込部２１１は、新たに受け付けられた投票内容及び確認コードを、パスワードに基づいて埋め込む。または、後述する電子投票媒体７００を用いると、電子投票装置２００は、電子投票データ作成装置１００に電子投票データ５２１を要求し、要求した電子投票データ５２１を受信して電子投票データ５２１を作成する。

【０１２７】

投票出力部２１３は、投票書込部２１１によって埋め込まれた電子投票データ５２１を電子開票装置３００に出力する。例えば、投票出力部２１３は、コンピュータネットワークを介して電子投票データ５２１を電子開票装置３００に出力する。

【０１２８】

図１１は、本発明の一実施形態に係る電子開票装置３００の機能を示す機能ブロック図である。電子開票装置３００は、開票入力部３０１と、開票判断部３０２と、開票秘密コード受付部３０３と、開票固有コード位置算出部３０４と、固有コード取得部３０５と、電子投票データ検索部３０６と、電子投票データ決定部３０７と、開票全体画像コード算出部３０８と、開票暗号秘密コード算出部３０９と、秘密鍵作成部３１０と、開票領域設定部３１１と、開票パスワード位置算出部３１２と、暗号パスワード取得部３１３と、暗号パスワード復号部３１４と、開票投票内容領域設定部３１５と、開票投票位置算出部３１６と、投票データ取得部３１７と、開票公表部３１８と、開票パラメータ記憶部３３１と、電子投票データ記憶部３３２とを備えている。このような電子開票装置３００について各部ごとに説明する。

【０１２９】

開票入力部３０１は、電子投票装置２００から電子投票データ５２１を入力する。開票入力部３０１は、例えば、コンピュータネットワークを介して電子投票装置２００から電子投票データ５２１を入力し、入力時の時刻を対応付ける。

【０１３０】

電子投票データ記憶部３３２は、開票入力部３０１によって入力された電子投票データ５２１を記憶する。

【０１３１】

開票判断部３０２は、電子投票データ５２１を開票するための開票条件を満たすか否かを判断する。開票条件は、例えば、電子投票データ５２１を開票するために定められた開票日時等である。

【０１３２】

開票秘密コード受付部３０３は、開票判断部３０２が開票条件を満たすと判断した場合に、秘密コード（ＣＡＳ）の入力を受け付ける。この秘密コード（ＣＡＳ）は、電子投票データ作成装置１００が受け付けた秘密コード（ＣＡＳ）と同一のコードでなければならない。

【０１３３】

開票固有コード位置算出部３０４は、電子投票データ５２１を構成する画素に基づいて固有コード（ＭＤ５）を埋め込む固有コード位置を算出する。例えば、開票固有コード位置算出部３０４は、開票秘密コード受付部３０３によって受け付けられた秘密コード（ＣＡＳ）に基づいて電子投票データ５２１内に設定された領域（例えば、図７（３）の領域６０３）を構成する画素に基づいて、固有コード位置を算出する。

【０１３４】

固有コード取得部３０５は、開票固有コード位置算出部３０４によって算出された固有コード位置から、電子投票データ作成装置１００によって埋め込まれた固有コード（ＭＤ

５）を取得する。すなわち、固有コード取得部３０５は、上述のデータを復元する方法によって、固有コード（ＭＤ５）を復元する。

【０１３５】

電子投票データ検索部３０６は、固有コード取得部３０５によって取得された固有コード（ＭＤ５）に基づいて、電子投票データ記憶部３３２に記憶された電子投票データ５２１を検索する。

【０１３６】

電子投票データ決定部３０７は、電子投票データ検索部３０６によって固有コード（ＭＤ５）と同一の電子投票データ５２１が検索された場合には、検索された電子投票データ５２１の内から一の電子投票データ５２１を決定して電子投票データ記憶部３３２に記憶する。例えば、電子投票データ決定部３０７は、電子投票データ検索部３０６が検索した固有コード（ＭＤ５）が同一の複数の電子投票データ５２１において、開票入力部３０１が電子投票データ５２１に対応付けた時刻を比較し、最新の時刻に対応付けられた電子投票データ５２１を、入力した電子投票データ５２１として電子投票データ記憶部３３２に記憶する。なお、電子投票データ決定部３０７は、固有コード（ＭＤ５）が同一の複数の電子投票データ５２１において、最初に記憶した電子投票データ５２１のみを記憶するとしてもよい。

【０１３７】

開票全体画像コード算出部３０８は、電子投票データ記憶部３３２によって記憶された電子投票データ５２１に基づいて、投票後の画像コード（投票後ＣＡＩ）を算出する。例えば、投票率が１００パーセントであることが条件である場合には、投票後の画像コードは、収集した全ての電子投票データ５２１を構成する画素に基づいて、電子投票データ作成装置１００と同様に作成される。例えば、投票率が一定の割合以上であることが条件である場合には、投票後の画像コード（投票後ＣＡＩ）は、収集した電子投票データ５２１に電子投票データ作成装置１００によって埋め込まれた冗長情報に基づいて、作成される。例えば、電子投票データ５２１が１件であっても開票できることが条件である場合には、投票後の画像コード（投票後ＣＡＩ）は、収集した電子投票データ５２１に電子投票データ作成装置１００によって埋め込まれた冗長情報（全体画像コードと同一）に基づいて、作成される。

【０１３８】

開票暗号秘密コード算出部３０９は、開票秘密コード受付部３０３によって受け付けられた秘密コード（ＣＡＳ）と、開票全体画像コード算出部３０８によって算出された投票後の画像コード（投票後ＣＡＩ）と、に基づいて投票後の暗号秘密コード（投票後ＣＡ）を算出する。

【０１３９】

秘密鍵作成部３１０は、開票暗号秘密コード算出部３０９によって算出された投票後の暗号秘密コード（投票後ＣＡ）に基づいて、秘密鍵を作成する。

【０１４０】

開票パラメータ記憶部３３１は、所定のパラメータを記憶する。所定のパラメータは、電子投票データ作成装置１００によって電子投票データ５２１内に公開鍵を埋め込むために設定された領域のパラメータ（作成パラメータ記憶部１３１の値）と同じである。

【０１４１】

開票領域設定部３１１は、開票パラメータ記憶部３３１に記憶された所定のパラメータに基づいて、開票入力部３０１によって入力された電子投票データ５２１を構成する画像データ内に領域を設定する。例えば、設定する領域の開始位置への所定のパラメータがｐａｒ＝０である場合、開票領域設定部３１１は、電子投票データ作成装置１００と同様に、図７（３）の領域６０１を設定する。

【０１４２】

開票パスワード位置算出部３１２は、開票領域設定部３１１によって設定された領域を構成する画素に基づいてパスワード位置を算出する。

【０１４３】
暗号パスワード取得部３１３は、開票パスワード位置算出部３１２によって算出されたパスワード位置から、電子投票装置２００によって埋め込まれた暗号化されたパスワードを取得する。
【０１４４】
暗号パスワード復号部３１４は、秘密鍵作成部３１０によって作成された秘密鍵に基づいて、暗号パスワード取得部３１３によって取得された暗号化されたパスワードを復号する。
【０１４５】
開票投票内容領域設定部３１５は、暗号パスワード復号部３１４部によって復号されたパスワードに基づいて、電子投票データ５２１を構成する画像データ内の領域を設定する。例えば、設定する領域の開始位置への所定のパラメータがｐａｒ＝Ｃｉ（パスワードに基づいて算出した電子投票データ５２１内の位置）である場合、開票投票内容領域設定部３１５は、図７（３）の領域６０２を設定する。
【０１４６】
開票投票位置算出部３１６は、開票投票内容領域設定部３１５によって設定された領域を構成する画素に基づいて、投票内容位置を算出する。
【０１４７】
投票データ取得部３１７は、開票投票位置算出部３１６によって算出された投票内容位置から、電子投票装置２００によって埋め込まれた投票内容及び確認コードを取得する。すなわち、投票データ取得部３１７は、上述のデータを復元する方法によって、投票内容及び確認コードを復元する。
【０１４８】
開票公表部３１８は、投票データ取得部３１７によって取得された投票内容及び確認コードを集計し、公表する。
【０１４９】
図１２は、本発明の一実施形態に係る電子投票データ作成装置１００の処理内容を示すフローチャートである。
【０１５０】
ステップＳ１０１において、電子投票データ作成装置１００のＣＰＵ（以下、作成ＣＰＵという）は、秘密コード（ＣＡＳ）の入力を受け付ける。より具体的には、作成ＣＰＵは、入力端末１５０（図９参照）から秘密コード（ＣＡＳ）を受け付ける。そして、作成ＣＰＵは、全体画像データ５０１の一部を、乱数に基づいて変更する（例えば、秘密コード（ＣＡＳ）の値に基づいて作成した位置の算出用チャネルのビット０を反転する）。その後、作成ＣＰＵは、処理をステップＳ１０２に移す。
【０１５１】
ステップＳ１０２において、作成ＣＰＵは、全体画像データ５０１に基づいて全体画像コード（ＣＡＩ）を算出する。より具体的には、作成ＣＰＵは、全体画像データ５０１を構成する３原色のうちの算出用チャネルの各階調値を、加算して全体画像コード（ＣＡＩ）を算出する。その後、作成ＣＰＵは、処理をステップＳ１０３に移す。
【０１５２】
ステップＳ１０３において、作成ＣＰＵは、秘密コード（ＣＡＳ）と全体画像コード（ＣＡＩ）とに基づいて暗号秘密コード（ＣＡ）を算出する。より具体的には、作成ＣＰＵは、受け付けられた秘密コード（ＣＡＳ）と、算出された全体画像コード（ＣＡＩ）とを加算して暗号秘密コード（ＣＡ）を算出する。その後、作成ＣＰＵは、処理をステップＳ１０４に移す。
【０１５３】
ステップＳ１０４において、作成ＣＰＵは、暗号秘密コード（ＣＡ）に基づいて公開鍵及び秘密鍵を作成する。より具体的には、作成ＣＰＵは、正整数ｅ（例えば、６０００１）を選択する。次に、暗号秘密コード（ＣＡ）に基づいて大きい素数の組（ｐ、ｑ）を求

め、ｐとｑとの積であるＮを求める。そして、作成ＣＰＵは、得られた（ｅ、Ｎ）を公開鍵とする。その後、作成ＣＰＵは、処理をステップＳ１０５に移す。

【０１５４】

ステップＳ１０５において、作成ＣＰＵは、全体画像データ５０１を分割する。より具体的には、作成ＣＰＵは、設定によって入力された値に従って、全体画像データ５０１の縦及び横を分割し、分割画像データ５１１を作成する。その後、作成ＣＰＵは、処理をステップＳ１０６に移す。

【０１５５】

ステップＳ１０６において、作成ＣＰＵは、暗号化処理（後述する図１３参照）によって、公開鍵を電子投票データ５２１に埋め込む。より具体的には、作成ＣＰＵは、作成パラメータ記憶部１３１に記憶したパラメータによって、ＧｅｔＰｏｓ処理（後述する図１４参照）へのパラメータがｐａｒ＝０である領域を設定し、設定された領域を構成する画素に基づいて、公開鍵を書き込む公開鍵位置を算出する。そして、作成ＣＰＵは、算出された複数の公開鍵位置の画素の各格納用チャネルのビット３に、公開鍵の値をビットに分解して埋め込む。ここで、設定された領域は、作成パラメータ記憶部１３１に記憶されたａ、ｂ、Ａ及びＢによって設定され、電子投票データ５２１全体の場合や、電子投票データ５２１内に設定された領域（例えば図７）の場合がある。その後、作成ＣＰＵは、処理をステップＳ１０７に移す。

【０１５６】

ステップＳ１０７において、作成ＣＰＵは、全体画像コードの冗長情報を作成し、電子投票データ５２１に埋め込む。より具体的には、ステップＳ１０６と同様に、作成ＣＰＵは、作成した全体画像コードの冗長情報をビットに分解して各格納用チャネルのビット５に埋め込む。その後、作成ＣＰＵは、処理をステップＳ１０８に移す。

【０１５７】

ステップＳ１０８において、作成ＣＰＵは、電子投票データ５２１の固有コード（ＭＤ５）を作成し、電子投票データ５２１に埋め込む。より具体的には、ステップＳ１０６と同様に、作成ＣＰＵは、作成した固有コード（ＭＤ５）をビットに分解して各格納用チャネルのビット４に埋め込む。その後、作成ＣＰＵは、処理をステップＳ１０９に移す。

【０１５８】

ステップＳ１０９において、作成ＣＰＵは、電子投票データ５２１を出力する。より具体的には、作成ＣＰＵは、コンピュータネットワークを介して電子投票データ５２１を電子投票装置２００に出力する。そして、作成ＣＰＵは、電子投票データ５２１の投票状態を投票済み状態（算出された複数の画素の各格納用チャネルのビット６の例えば、2^0から2^9を１）にする。その後、作成ＣＰＵは、処理を終了する。

【０１５９】

図１３は、本発明の一実施形態に係る暗号化処理の内容を示すフローチャートである。なお、暗号化処理は、電子投票データ作成装置１００だけでなく、電子投票装置２００、電子開票装置３００及び電子投票媒体７００（後述する図２２参照）においても存在する。よって、本処理のＣＰＵは、電子投票データ作成装置１００のＣＰＵ、電子投票装置２００のＣＰＵ、電子開票装置３００のＣＰＵ又は電子投票媒体７００のＣＰＵに適宜読み替える。

【０１６０】

ステップＳ１２１において、ＣＰＵは、ＧｅｔＰｏｓ処理を実行する。その後、ＣＰＵは、処理をステップＳ１２２に移す。

【０１６１】

ステップＳ１２２において、ＣＰＵは、格納位置にビットの重みを対応付ける。より具体的には、ＣＰＵは、ＧｅｔＰｏｓ処理が算出した格納位置に、算出した順にビットの重み（2^0、2^1、・・・、2^{1023}）を対応付ける。その後、ＣＰＵは、処理をステップＳ１２３に移す。

【０１６２】

ステップＳ１２３において、ＣＰＵは、埋め込む値を構成するそれぞれのビットを、そのビットの重みと同じ重みに対応付けられた格納位置に、書き込む。より具体的には、ＣＰＵは、埋め込む値を構成するそれぞれのビットを、そのビットの重みと同じ重みに対応付けられた格納位置のうち格納用チャネルの所定のビットに、書き込む。その後、ＣＰＵは、処理を戻して本処理に移る処理の次の処理に移す。

【０１６３】

図１４は、本発明の一実施形態に係るＧｅｔＰｏｓの処理内容を示すフローチャートである。なお、ＧｅｔＰｏｓの処理は、例えば、引数が（＊ｐａｓ、ｎｕｍ、ｐａｒ）であり、電子投票データ作成装置１００だけでなく、電子投票装置２００、電子開票装置３００及び電子投票媒体７００（後述する図２２参照）においても存在する。よって、本処理のＣＰＵは、電子投票データ作成装置１００のＣＰＵ、電子投票装置２００のＣＰＵ、電子開票装置３００のＣＰＵ又は電子投票媒体７００のＣＰＵに適宜読み替える。

【０１６４】

ステップＳ１３１において、ＣＰＵは、格納位置を算出するための領域をｐａｒに基づいて設定する。例えば、ＣＰＵは、引数の値ｐａｒに基づいて、開始点及び終了点のＸＹ座標が（ａ＋ｐａｒ、ｂ＋ｐａｒ）、（ａ＋ｐａｒ＋Ａ、ｂ＋ｐａｒ＋Ｂ）とする領域（横Ａ、縦Ｂ）を設定する。ここで、ａ及びｂは開始点の初期座標値、ＡはＸ方向の幅、ＢはＹ方向の高さである。ａ、ｂ、Ａ及びＢは、所定の方法によって変更可能な値である。その後、ＣＰＵは、処理をステップＳ１３２に移す。

【０１６５】

ステップＳ１３２において、ＣＰＵは、設定した領域を構成する画素値のうちＲ及びＧチャネルの階調値に基づいて、引数の値ｎｕｍ個の擬似乱数を算出する。その後、ＣＰＵは、処理をステップＳ１３３に移す。

【０１６６】

ステップＳ１３３において、ＣＰＵは、算出した擬似乱数に基づいて格納位置を算出する。例えば、ＣＰＵは、格納位置ｘ＝擬似乱数ｍｏｄ（ｗ－２）、格納位置ｙ＝擬似乱数ｍｏｄ（ｈ－１）によって格納位置を算出する。その後、ＣＰＵは、処理をステップＳ１３４に移す。

【０１６７】

ステップＳ１３４において、ＣＰＵは、格納位置のハッシュ変換を行う。例えば、ＣＰＵは、算出した格納位置が重複していると判断した場合に、新格納位置ｘ＝（格納位置ｘ＋２３）ｍｏｄ（ｗ）、新格納位置ｙ＝（格納位置ｙ＋１１）ｍｏｄ（ｈ）によってハッシュ変換を行い、重複している格納位置を重複しない格納位置に変換する。そして、ＣＰＵは、算出したｎｕｍ個の格納位置へのポインタ（＊ｐｏｓ）を作成し、処理を戻して本処理に移る処理の次の処理に移す。

【０１６８】

図１５は、本発明の一実施形態に係る電子投票装置２００の処理内容を示すフローチャートである。電子投票装置２００は、電子投票データ作成装置１００の暗号化処理及びＧｅｔＰｏｓ処理と同様の処理を備えている。

【０１６９】

ステップＳ２０１において、電子投票装置２００のＣＰＵ（以下、投票ＣＰＵという）は、電子投票データ５２１を入力する。より具体的には、投票ＣＰＵは、コンピュータネットワークを介して電子投票データ作成装置１００から電子投票データ５２１を入力する。再投票の場合には、投票ＣＰＵは、既に入力済みの電子投票データ５２１の中から、固有コード（ＭＤ５）によって電子投票データ５２１を検索する。その後、投票ＣＰＵは、処理をステップＳ２０２に移す。

【０１７０】

ステップＳ２０２において、投票ＣＰＵは、電子投票データ５２１に基づいて、公開鍵を埋め込んだ位置を算出する。より具体的には、投票ＣＰＵは、ＧｅｔＰｏｓ処理（図１４参照）へのパラメータがｐａｒ＝０である領域を設定し、設定された領域を構成する画

素に基づいて、公開鍵位置を算出する。ここで、設定された領域は、投票パラメータ記憶部２３１のパラメータによって設定され、電子投票データ作成装置１００において設定された領域と同じである。その後、投票ＣＰＵは、処理をステップＳ２０３に移す。

【０１７１】

ステップＳ２０３において、投票ＣＰＵは、算出した位置から公開鍵を取得する。より具体的には、投票ＣＰＵは、算出した公開鍵位置の格納用チャネルのビット３から、公開鍵のビットを復元し、公開鍵を取得する。その後、投票ＣＰＵは、処理をステップＳ２０４に移す。

【０１７２】

ステップＳ２０４において、投票ＣＰＵは、投票内容及び確認コードの入力を受け付ける。より具体的には、投票ＣＰＵは、入力端末２５０（図１０参照）から投票内容及び確認コードの入力を受け付ける。その後、投票ＣＰＵは、処理をステップＳ２０５に移す。

【０１７３】

ステップＳ２０５において、投票ＣＰＵは、パスワードの入力を受け付ける。より具体的には、投票ＣＰＵは、入力端末２５０（図１０参照）からパスワードの入力を受け付ける。その後、投票ＣＰＵは、処理をステップＳ２０６に移す。

【０１７４】

ステップＳ２０６において、投票ＣＰＵは、パスワードに基づいて投票内容及び確認コードを埋め込む位置を算出する。より具体的には、投票ＣＰＵは、パスワードに基づいて領域設定用の値（Ｃｉ）を算出し、ＧｅｔＰｏｓ処理（図１４参照）へのパラメータがｐａｒ＝Ｃｉである領域を設定し、設定された領域を構成する画素に基づいて、投票内容及び確認コードを書き込む投票位置を算出する。その後、投票ＣＰＵは、処理をステップＳ２０７に移す。

【０１７５】

ステップＳ２０７において、投票ＣＰＵは、算出した位置に投票内容及び確認コードを埋め込む。より具体的には、投票ＣＰＵは、算出した位置の各格納用チャネルのビット１に、投票内容及び確認コードを構成するビットを書き込む。その後、投票ＣＰＵは、処理をステップＳ２０８に移す。

【０１７６】

ステップＳ２０８において、投票ＣＰＵは、公開鍵に基づいてパスワードを暗号化し、電子投票データ５２１に埋め込む。より具体的には、投票ＣＰＵは、ＧｅｔＰｏｓ処理（図１４参照）へのパラメータがｐａｒ＝０である領域を設定し、設定された領域を構成する画素に基づいて、パスワード位置を算出する。そして、投票ＣＰＵは、復元した公開鍵に基づいて、受け付けたパスワードを暗号化し、暗号化したパスワードを構成するビットを、算出したパスワード位置の各格納用チャネルのビット２に書き込む。その後、投票ＣＰＵは、処理をステップＳ２０９に移す。

【０１７７】

ステップＳ２０９において、投票ＣＰＵは、電子投票データ５２１を出力する。より具体的には、投票ＣＰＵは、コンピュータネットワークを介して電子投票データ５２１を電子開票装置３００に出力する。その後、投票ＣＰＵは、処理を終了する。

【０１７８】

図１６は、本発明の一実施形態に係る電子開票装置３００の処理内容を示すフローチャートである。電子開票装置３００は、電子投票データ作成装置１００の暗号化処理及びＧｅｔＰｏｓ処理と同様の処理を備えている。

【０１７９】

ステップＳ３０１において、電子開票装置３００のＣＰＵ（以下、開票ＣＰＵという）は、電子投票データ５２１を入力し、時刻を対応付けて記憶する。より具体的には、開票ＣＰＵは、コンピュータネットワークを介して電子投票データ５２１を電子投票装置２００から入力し、入力した時の時刻を電子投票データ５２１に対応付けて電子投票データ記憶部３３２に記憶する。その後、開票ＣＰＵは、処理をステップＳ３０２に移す。

【０１８０】
ステップＳ３０２において、開票ＣＰＵは、開票条件を満たすか否かを判断する。すなわち、開票ＣＰＵは、現在の時刻を取得し、開票する時刻になったか否かを判断する。この判断がＹＥＳの場合、開票ＣＰＵは、処理をステップＳ３０３に移し、ＮＯの場合、開票ＣＰＵは、処理をステップＳ３０１に移す。ここで、時刻の取得は、時計部（図示せず）を設けて、現在の時刻を取得するとしてもよいし、標準時を含む標準電波を受信して時刻を取得するとしてもよい。
【０１８１】
ステップＳ３０３において、開票ＣＰＵは、秘密コード（ＣＡＳ）の入力を受け付ける。より具体的には、開票ＣＰＵは、入力端末３５０（図１１参照）から秘密コード（ＣＡＳ）の入力を受け付ける。その後、開票ＣＰＵは、処理をステップＳ３０４に移す。
【０１８２】
ステップＳ３０４において、開票ＣＰＵは、電子投票データ５２１から固有コード（ＭＤ５）を取得し、同一の固有コード（ＭＤ５）を有する電子投票データ５２１が存在すると判断した場合に、最新の時刻に対応付けられた電子投票データ５２１を電子投票データ記憶部３３２に記憶する。より具体的には、開票ＣＰＵは、電子投票データ記憶部３３２に記憶された各々の電子投票データ５２１から各々の固有コード（ＭＤ５）を取得する。固有コード（ＭＤ５）は、電子投票データ作成装置１００によって埋め込まれた画素から復元することによって取得できる。そして、開票ＣＰＵは、取得した固有コード（ＭＤ５）によって電子投票データ記憶部３３２内を検索し、同一の固有コード（ＭＤ５）を有する電子投票データ５２１が存在すると判断した場合に、同一の固有コード（ＭＤ５）を有する電子投票データ５２１に対応付けられた時刻を比較し、最新の時刻に対応付けられた電子投票データ５２１を電子投票データ記憶部３３２に記憶する。その後、開票ＣＰＵは、処理をステップＳ３０５に移す。なお、開票ＣＰＵは、時刻を比較し、最初の電子投票データ５２１を電子投票データ記憶部３３２に記憶する、としてもよい。
【０１８３】
ステップＳ３０５において、開票ＣＰＵは、入力した電子投票データ５２１から投票後の画像コードを取得する。より具体的には、開票ＣＰＵは、収集した電子投票データ５２１に埋め込まれた冗長情報に基づいて、投票後の画像コードを取得する。その後、開票ＣＰＵは、処理をステップＳ３０６に移す。
【０１８４】
ステップＳ３０６において、開票ＣＰＵは、秘密コードと投票後の画像コードとに基づいて投票後の暗号秘密コードを算出する。より具体的には、開票ＣＰＵは、電子投票データ作成装置１００と同様に、受け付けられた秘密コード（ＣＡＳ）と、取得した投票後の画像コード（投票後のＣＡＩ）とを加算して投票後の暗号秘密コード（投票後のＣＡ）を算出する。その後、開票ＣＰＵは、処理をステップＳ３０７に移す。
【０１８５】
ステップＳ３０７において、開票ＣＰＵは、投票後の暗号秘密コードに基づいて秘密鍵を算出する。より具体的には、開票ＣＰＵは、電子投票データ作成装置１００と同様に、秘密鍵を算出する。その後、開票ＣＰＵは、処理をステップＳ３０８に移す。
【０１８６】
ステップＳ３０８において、開票ＣＰＵは、入力した電子投票データ５２１から暗号化されたパスワードを取得し、秘密鍵によって復号する。より具体的には、開票ＣＰＵは、ＧｅｔＰｏｓ処理（図１４参照）へのパラメータがｐａｒ＝０である領域を設定する。ここで、設定された領域は、開票パラメータ記憶部３３１のパラメータによって設定され、電子投票データ作成装置１００において設定された領域と同じである。次に、開票ＣＰＵは、設定された領域を構成する画素に基づいて、パスワードが書き込まれたパスワード位置を算出し、算出したパスワード位置の格納用チャネルのビット２から暗号化されたパスワードを復元する。そして、開票ＣＰＵは、復元したパスワードを秘密鍵に基づいて復号する。その後、開票ＣＰＵは、処理をステップＳ３０９に移す。

【０１８７】
ステップＳ３０９において、開票ＣＰＵは、復号したパスワードに基づいて、投票内容及び確認コードを取得する。より具体的には、開票ＣＰＵは、復号したパスワードに基づいて領域設定用の値（Ｃｉ）を算出し、ＧｅｔＰｏｓ処理（図１４参照）へのパラメータがｐａｒ＝Ｃｉである領域を設定し、設定された領域を構成する画素に基づいて、投票位置を算出する。そして、開票ＣＰＵは、算出した投票位置の格納用チャネルのビット１から、投票内容及び確認コードのビットを復元し、投票内容及び確認コードを取得する。その後、開票ＣＰＵは、処理をステップＳ３１０に移す。
【０１８８】
ステップＳ３１０において、開票ＣＰＵは、取得した投票内容及び確認コードを集計し、公表する。より具体的には、開票ＣＰＵは、取得した投票内容及び確認コードを投票内容によって集計して、投票結果を取得する。そして、開票ＣＰＵは、投票内容及び確認コードをランダムに表示装置３６０に表示する（図２０参照）。また、開票ＣＰＵは、集計内容の送信要求を受信し、受信した要求に従って集計内容を送信する。その後、開票ＣＰＵは、処理を終了する。
【０１８９】
図１７は、本発明の一実施形態に係るビットの対応付けテーブルを示す図である。
【０１９０】
ビットの対応付けテーブルは、画素の位置に階調値と、ビットの重みとを対応付けて記憶している。画素の位置は、ＧｅｔＰｏｓ処理によって算出された画素の位置である。ビットの重みは、ＧｅｔＰｏｓ処理が算出した順に、2^{0}から2^{n-1}を対応付けて記憶している。
【０１９１】
図１８は、本発明の一実施形態に係る電子投票データ作成装置１００において、電子投票データ５２１を作成する例を示す図である。
【０１９２】
図１８が示す例は、電子投票データ作成装置１００が、全体画像データ５０１を表示装置１６０に表示していることを示す例である。電子投票データ作成装置１００は、秘密コード入力欄１６１に入力された秘密コードを受け付ける。また、電子投票データ作成装置１００は、分割数設定欄１６２に入力された分割数を受け付けて、全体画像データ５０１を分割して電子投票データ５２１を作成する。
【０１９３】
図１９は、本発明の一実施形態に係る電子投票装置２００において、電子投票データ５２１を表示する例を示す図である。
【０１９４】
図１９が示す例は、電子投票装置２００が、電子投票データ５２１を表示装置２６０に表示していることを示す例である。電子投票装置２００は、投票入力欄２６１に入力された投票内容を受け付ける。そして、電子投票装置２００は、確認コード入力欄２６２に入力された確認コードを受け付ける。電子投票装置２００は、電子投票媒体７００（後述する図２２参照）が接続されている場合、電子投票媒体７００が確認コードを自動的に作成する。
【０１９５】
図２０は、本発明の一実施形態に係る電子開票装置３００において、電子投票データ５２１を集計し、公表する例を示す図である。
【０１９６】
図２０が示す例は、電子開票装置３００が、集計内容を表示装置３６０に表示していることを示す例である。電子開票装置３００は、表示装置３６０に、投票内容と、確認コードとを並べて表示することによって、投票者に投票結果が正しく集計されていることを示すことができ、投票者に投票結果を確認させることができる。
【０１９７】

［実施形態３］
実施形態３は、暗号化処理をする暗号化装置４００の実施形態である。
【０１９８】
図２１は、本発明の一実施形態に係る暗号化装置４００の機能を示す機能ブロック図である。暗号化装置４００は、画像読込部４０１と、領域設定部４０２と、擬似乱数生成部４０３と、位置算出部４０４と、ハッシュ値算出部４０５と、重み対応付部４０６と、埋込部４０７とを備える。
【０１９９】
画像読込部４０１は、３原色の階調値から構成される画素によって構成される画像を読み込む。
【０２００】
領域設定部４０２は、画像内に領域を設定する。
【０２０１】
擬似乱数生成部４０３は、画像読込部４０１によって読み込まれた画像を構成する３原色のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成する。さらに、擬似乱数生成部４０３は、領域設定部４０２によって設定された領域を構成する画素のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成する。
【０２０２】
位置算出部４０４は、擬似乱数生成部４０３によって生成された複数の各擬似乱数に基づいて、所定の演算を実行し、画像内の画素の位置を順に複数個算出する。さらに、ハッシュ値算出部４０５は、画素の位置を引数としてハッシュ値を算出する。そして、位置算出部４０４は、算出した画素の位置が重複する場合に、重複した画素の位置を引数としてハッシュ値算出部４０５によってハッシュ値を算出し、算出したハッシュ値に基づいて画素の位置を算出する。例えば、領域設定部４０２、擬似乱数生成部４０３、位置算出部４０４及びハッシュ値算出部４０５のフローチャートは、実施形態２の図１４と同様である。
【０２０３】
重み対応付部４０６は、位置算出部４０４によって算出された複数個の各位置に係る画素を構成する３原色の階調値のうち、擬似乱数を生成するために用いた一の原色又は二の原色以外の原色の階調値を構成するビットのうち所定のビットに、位置算出部４０４が算出した順に、ビットの重みを対応付ける。
【０２０４】
埋込部４０７は、重み対応付部４０６によって重みが対応付けられた所定のビットに、情報を構成するビットのうち、所定のビットに対応付けられた重みと同じ重みのビットの値を埋め込む。例えば、重み対応付部４０６及び埋込部４０７のフローチャートは、実施形態２の図１３と同様である。
【０２０５】
［実施形態４］
実施形態４は、電子投票媒体７００によって、電子投票データ５２１に投票内容及び確認コードを書き込み、再度の投票をする実施形態である。
【０２０６】
図２２は、本発明の一実施形態に係る電子投票媒体７００の機能を示す機能ブロック図である。電子投票媒体７００は、時刻取得部７０１と、投票識別コード作成部７０２と、投票識別コード出力部７０３と、投票データ入力部７０４と、確認コード作成部７０５と、パスワード作成部７０６と、投票内容書込部７０７と、公開鍵取得部７０８と、暗号化書込部７０９と、電子投票データ出力部７１０と、表示部７１１と、媒体パラメータ記憶部７３１と、投票データ記憶部７３２と、媒体識別情報記憶部７３３とを備える。
【０２０７】
媒体パラメータ記憶部７３１は、電子投票データ５２１内に設定する領域についての所定のパラメータを記憶している。例えば、媒体パラメータ記憶部７３１は、実施形態１の

図６における、開始点の値（ａ、ｂ）と、領域の幅Ａと、領域の高さＢとを記憶している。

【０２０８】

媒体識別情報記憶部７３３は、電子投票媒体を識別するための媒体識別情報（製品ＩＤ）を記憶する。

【０２０９】

時刻取得部７０１は、現在の時刻を取得する。

【０２１０】

投票識別コード作成部７０２は、媒体識別情報記憶部７３３によって記憶された媒体識別情報（製品ＩＤ）と、時刻取得部７０１によって取得された時刻を含むシリアル番号とに基づいて、投票ごとに投票識別コード（投票ＩＤという）を作成する。例えば、投票識別コード作成部７０２は、製品ＩＤをＰＱＲＳ０１２３４とすると、投票ＩＤとして、ＰＱＲＳ０１２３４－２００９０１２３１６５９－０００１を作成する。なお、電子投票データ作成装置１００は、受信した投票ＩＤに基づいて、初回と同じ電子投票データ５２１を送信する場合、投票ＩＤのうち固定である製品ＩＤの部分を利用する。

【０２１１】

投票識別コード出力部７０３は、投票ＩＤのうち最新の投票ＩＤを出力する。

【０２１２】

投票データ入力部７０４は、公開鍵が所定の方法によって書き込まれた画像データである電子投票データ５２１と、受け付けられた候補者を示す投票内容とを入力する。

【０２１３】

確認コード作成部７０５は、投票内容に対応付けて確認コードを作成する。

【０２１４】

パスワード作成部７０６は、投票内容及び確認コードを抽出するためのパスワードを作成する。

【０２１５】

投票内容書込部７０７は、電子投票データ５２１に、パスワード作成部７０６によって作成されたパスワードに基づいて、投票内容及び確認コードを埋め込む。例えば、投票内容書込部７０７は、実施形態２の電子投票装置２００と同様に、パスワード作成部７０６によって作成されたパスワードに基づいて、ＧｅｔＰｏｓ処理（図１４参照）へのパラメータ（ｐａｒ＝Ｃｉ）を算出し、算出したパラメータによって領域を設定する。次に、投票内容書込部７０７は、設定された領域を構成する画素に基づいて投票内容及び確認コードを埋め込む投票内容位置を算出し、算出した投票内容位置に、投票内容及び確認コードをビットに分解して埋め込む。

【０２１６】

公開鍵取得部７０８は、投票データ入力部７０４によって入力された電子投票データ５２１から公開鍵を取得する。

【０２１７】

暗号化書込部７０９は、電子投票データ５２１に、公開鍵取得部７０８によって取得された公開鍵に基づいてパスワードを暗号化して埋め込む。例えば、暗号化書込部７０９は、実施形態２の電子投票装置２００と同様に、ＧｅｔＰｏｓ処理（図１４参照）へのパラメータがｐａｒ＝０である領域を設定する。次に、暗号化書込部７０９は、設定された領域を構成する画素に基づいてパスワードを埋め込むパスワード位置を算出する。そして、暗号化書込部７０９は、算出したパスワード位置に、暗号化されたパスワードをビットに分解して埋め込む。

【０２１８】

電子投票データ出力部７１０は、投票内容及び確認コードと、パスワードとが書き込まれた電子投票データ５２１を出力する。

【０２１９】

投票データ記憶部７３２は、投票内容及び確認コードに、パスワードと、投票ＩＤとを

対応付けて記憶する。

【０２２０】

表示部７１１は、投票データ記憶部７３２に記憶された投票内容及び確認コードと、パスワードと、投票ＩＤとを対応付けて表示する。

【０２２１】

図２３は、本発明の一実施形態に係る電子投票媒体７００の例を示す図である。電子投票媒体７００は、ＣＰＵ（図示せず、以下媒体ＣＰＵという）、記憶部（図示せず、媒体パラメータ記憶部７３１、投票データ記憶部７３２及び媒体識別情報記憶部７３３を含む）、接続部７３４、表示装置７３５及び操作ボタン（ＩＤ作成ボタン７２１、確認コード作成ボタン７２２、表示ボタン７２３、投票ボタン７２４）を備えている。接続部７３４は、例えば、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）又は近距離無線通信等の接続インターフェースによって構成されている。表示装置７３５は、例えば、液晶ディスプレイ等によって構成される。

【０２２２】

電子投票媒体７００は、電子投票データ５２１を書き込む媒体として、例えば、次のように利用される。

（１）最初に、電子投票データ作成装置１００は電子投票媒体７００を接続する。電子投票データ作成装置１００は、電子投票媒体７００が作成した投票ＩＤを登録し、電子投票媒体７００に電子投票データ５２１を書き込む。電子投票媒体７００は、最新の投票ＩＤをアクティブにする。

（２）電子投票装置２００は、電子投票媒体７００を接続し、受け付けた投票内容を電子投票媒体７００に書き込む。電子投票媒体７００は、確認コードを作成し、パスワードを作成する。そして、電子投票媒体７００は、電子投票データ５２１に、投票内容及び確認コードと、パスワードとを埋め込む。

（３）電子開票装置３００は、電子投票媒体７００を接続し、投票内容及び確認コードを入力して集計し、公表する。

【０２２３】

さらに、電子投票媒体７００は、電子投票システム１０において次のように利用される。図２４は、本発明の一実施形態に係る電子投票媒体７００を利用した電子投票システム１０の例を示す図である。電子投票媒体７００が接続されたパソコンや携帯端末等（以下、電子投票媒体接続端末７９０という）は、電子投票データ作成装置１００及び電子開票装置３００と通信を行い、電子投票データ５２１の送受信を行う。電子投票媒体接続端末７９０は、電子投票システム１０用のプログラムをダウンロードして動作する。

【０２２４】

電子投票媒体接続端末７９０は、電子投票媒体７００を接続する。電子投票媒体７００は、投票ＩＤを作成する。電子投票媒体接続端末７９０は、電子投票媒体７００から読み込んだ投票ＩＤに基づいて、電子投票データ作成装置１００に電子投票データ５２１の送信要求を送信する。そして、電子投票媒体接続端末７９０は、電子投票データ作成装置１００から電子投票データ５２１を受信し、受信した電子投票データ５２１を表示する（例えば、図１９のような表示であって、確認コードを入力する欄がない表示をする）。そして、電子投票媒体接続端末７９０は、投票内容の入力を受け付け、受け付けた投票内容と、電子投票データ５２１とを電子投票媒体７００に書き込む。電子投票媒体７００は、電子投票データ５２１から公開鍵を取得し、取得した公開鍵に基づいて、自動生成したパスワードを暗号化し、投票内容及び自動生成した確認コードを電子投票データ５２１に書き込む。そして、電子投票媒体接続端末７９０は、電子投票媒体７００から、電子投票データ５２１を読み込み、電子開票装置３００に送信する。

【０２２５】

再投票をする場合、電子投票媒体接続端末７９０は、電子投票媒体７００からアクティブになっている最新の投票ＩＤを読み込み、読み込んだ投票ＩＤに基づいて、電子投票データ作成装置１００に電子投票データ５２１の送信要求を送信する。電子投票データ作成

装置１００は、受信した投票ＩＤに基づいて、初回と同じ電子投票データ５２１を送信する。そして、上述と同様に、電子投票媒体接続端末７９０は、受信した電子投票データ５２１に基づいて、新たな投票内容を受け付け、電子投票媒体７００が書き込んだ電子投票データ５２１を電子開票装置３００に送信する。

【０２２６】

図２５は、本発明の一実施形態に係る電子投票媒体７００を利用する投票プログラムの処理内容を示すフローチャートである。

【０２２７】

ステップＳ４０１において、電子投票媒体接続端末７９０のＣＰＵ（以下、端末ＣＰＵという）は、電子投票媒体７００から投票ＩＤを読み込む。その後、端末ＣＰＵは、処理をステップＳ４０２に移す。

【０２２８】

ステップＳ４０２において、端末ＣＰＵは、投票ＩＤに基づいて電子投票データ作成装置１００から電子投票データ５２１を受信する。その後、端末ＣＰＵは、処理をステップＳ４０３に移す。

【０２２９】

ステップＳ４０３において、端末ＣＰＵは、電子投票データ５２１を表示する。その後、端末ＣＰＵは、処理をステップＳ４０４に移す。

【０２３０】

ステップＳ４０４において、端末ＣＰＵは、投票内容を受け付ける。その後、端末ＣＰＵは、処理をステップＳ４０５に移す。

【０２３１】

ステップＳ４０５において、端末ＣＰＵは、投票内容と電子投票データ５２１とを電子投票媒体７００に書き込む。その後、端末ＣＰＵは、処理をステップＳ４０６に移す。

【０２３２】

ステップＳ４０６において、端末ＣＰＵは、電子投票媒体７００から暗号化された電子投票データ５２１を読み込む。その後、端末ＣＰＵは、処理をステップＳ４０７に移す。

【０２３３】

ステップＳ４０７において、端末ＣＰＵは、読み込んだ電子投票データ５２１を電子開票装置３００に送信する。その後、端末ＣＰＵは、処理を終了する。

【０２３４】

図２６は、本発明の一実施形態に係る電子投票媒体７００の処理内容を示すフローチャートである。

【０２３５】

ステップＳ５０１において、媒体ＣＰＵは、入力したデータが電子投票データ５２１か否かを判断する。この判断がＹＥＳの場合、媒体ＣＰＵは、処理をステップＳ５０２に移し、ＮＯの場合、媒体ＣＰＵは、処理をステップＳ５０３に移す。

【０２３６】

ステップＳ５０２において、媒体ＣＰＵは、投票内容と電子投票データ５２１とを記憶部に記憶する。その後、媒体ＣＰＵは、処理をステップＳ５０１に移す。

【０２３７】

ステップＳ５０３において、媒体ＣＰＵは、ＩＤ作成ボタン７２１押下か否かを判断する。この判断がＹＥＳの場合、媒体ＣＰＵは、処理をステップＳ５０４に移し、ＮＯの場合、媒体ＣＰＵは、処理をステップＳ５０５に移す。

【０２３８】

ステップＳ５０４において、媒体ＣＰＵは、投票ＩＤを作成する。より具体的には、媒体ＣＰＵは、現在の時刻を含んだシリアル番号と、媒体識別情報記憶部７３３に記憶された製品ＩＤとに基づいて投票ＩＤを作成する。そして、媒体ＣＰＵは、作成した最新の投票ＩＤのみをアクティブにする。その後、媒体ＣＰＵは、処理をステップＳ５０１に移す。

【０２３９】
ステップＳ５０５において、媒体ＣＰＵは、確認コード作成ボタン７２２押下か否かを判断する。この判断がＹＥＳの場合、媒体ＣＰＵは、処理をステップＳ５０６に移し、ＮＯの場合、媒体ＣＰＵは、処理をステップＳ５０７に移す。
【０２４０】
ステップＳ５０６において、媒体ＣＰＵは、確認コードとパスワードとを作成し、記憶する。より具体的には、媒体ＣＰＵは、確認コード作成ボタン７２２押下によって、確認コード用の乱数とパスワード用の乱数とを次々と発生させ、２度目の確認コード作成ボタン７２２押下によって押下時に発生させていた乱数を決定する。そして、媒体ＣＰＵは、決定した乱数と現在の時刻とを組合せて確認コードとパスワードとを作成し、投票内容に対応付けて確認コードとパスワードとを記憶部に記憶する。その後、媒体ＣＰＵは、処理をステップＳ５０１に移す。
【０２４１】
ステップＳ５０７において、媒体ＣＰＵは、表示ボタン７２３押下か否かを判断する。この判断がＹＥＳの場合、媒体ＣＰＵは、処理をステップＳ５０８に移し、ＮＯの場合、媒体ＣＰＵは、処理をステップＳ５０９に移す。
【０２４２】
ステップＳ５０８において、媒体ＣＰＵは、投票内容及び確認コードとパスワードとを表示する。より具体的には、媒体ＣＰＵは、検出した表示ボタン７２３押下によって投票内容及び確認コードとパスワードとを表示装置７３５に表示する。そして、媒体ＣＰＵは、検出した表示ボタン７２３押下ごとに記憶部に記憶している投票内容及び確認コードとパスワードとを表示装置７３５に表示する。その後、媒体ＣＰＵは、処理をステップＳ５０１に移す。
【０２４３】
ステップＳ５０９において、媒体ＣＰＵは、投票ボタン７２４押下か否かを判断する。この判断がＹＥＳの場合、媒体ＣＰＵは、処理をステップＳ５１０に移し、ＮＯの場合、媒体ＣＰＵは、処理をステップＳ５０１に移す。
【０２４４】
ステップＳ５１０において、媒体ＣＰＵは、電子投票データ５２１に投票内容及び確認コードと、パスワードとを埋め込む。より具体的には、媒体ＣＰＵは、パスワードに基づいてＧｅｔＰｏｓ処理（図１４参照）へのパラメータ（ｐａｒ＝Ｃｉ）を算出し、算出したパラメータによって電子投票データ５２１内に領域を設定し、設定した領域を構成する画素に基づいて算出した投票内容位置に、投票内容及び確認コードを埋め込む。次に、媒体ＣＰＵは、電子投票データ５２１から公開鍵を取得し、取得した公開鍵に基づいてパスワードを暗号化する。そして、媒体ＣＰＵは、ＧｅｔＰｏｓ処理（図１４参照、ｐａｒ＝０）によって算出された電子投票データ５２１内のパスワード位置に、暗号化したパスワードを埋め込む。その後、媒体ＣＰＵは、処理をステップＳ５０１に移す。
【０２４５】
図２７は、本発明の一実施形態に係る電子投票媒体７００を利用する場合の電子投票データ作成装置１００の処理内容を示すフローチャートである。
【０２４６】
ステップＳ１５１において、作成ＣＰＵは、電子投票データ５２１を作成する。作成ＣＰＵは、図１２のステップＳ１０１からステップＳ１０８と同様に電子投票データ５２１を作成する。その後、作成ＣＰＵは、処理をステップＳ１５２に移す。
【０２４７】
ステップＳ１５２において、作成ＣＰＵは、投票ＩＤを受信か否かを判断する。すなわち、作成ＣＰＵは、電子投票媒体接続端末７９０から投票ＩＤを受信したか否かを判断する。この判断がＹＥＳの場合、作成ＣＰＵは、処理をステップＳ１５３に移し、ＮＯの場合、作成ＣＰＵは、処理を終了する。
【０２４８】

ステップＳ１５３において、作成ＣＰＵは、最初か否かを判断する。すなわち、作成ＣＰＵは、投票ＩＤが記憶部（図示せず）に記憶されているか否かを判断する。この判断がＹＥＳの場合、作成ＣＰＵは、処理をステップＳ１５４に移し、ＮＯの場合、作成ＣＰＵは、処理をステップＳ１５６に移す。

【０２４９】

ステップＳ１５４において、作成ＣＰＵは、電子投票データ５２１に投票ＩＤを対応付けて記憶する。その後、作成ＣＰＵは、処理をステップＳ１５５に移す。

【０２５０】

ステップＳ１５５において、作成ＣＰＵは、電子投票データ５２１を送信する。すなわち、作成ＣＰＵは、投票ＩＤを送信した電子投票媒体接続端末７９０に電子投票データ５２１を送信する。その後、作成ＣＰＵは、処理を終了する。

【０２５１】

ステップＳ１５６において、作成ＣＰＵは、受信した投票ＩＤによって検索し、検索した投票ＩＤに対応付けられた電子投票データ５２１を取得する。すなわち、作成ＣＰＵは、電子投票データ５２１と投票ＩＤとを対応付けて記憶した記憶部（図示せず）を投票ＩＤによって検索し、検索した投票ＩＤに対応付けられた電子投票データ５２１を取得する。その後、作成ＣＰＵは、処理をステップＳ１５５に移す。

【０２５２】

図２８は、本発明の一実施形態に係る電子投票媒体７００を利用する場合の電子開票装置３００の処理内容を示すフローチャートである。

【０２５３】

ステップＳ３５１において、開票ＣＰＵは、電子投票データ５２１を入力する。すなわち、開票ＣＰＵは、図１６のステップＳ３０１と同様に、電子投票データ５２１を入力する。その後、開票ＣＰＵは、処理をステップＳ３５２に移す。

【０２５４】

ステップＳ３５２において、開票ＣＰＵは、投票ＩＤを受信か否かを判断する。すなわち、開票ＣＰＵは、電子投票媒体接続端末７９０から投票ＩＤを受信したか否かを判断する。この判断がＹＥＳの場合、開票ＣＰＵは、処理をステップＳ３５３に移し、ＮＯの場合、開票ＣＰＵは、処理をステップＳ３５５に移す。

【０２５５】

ステップＳ３５３において、開票ＣＰＵは、最初か否かを判断する。すなわち、開票ＣＰＵは、投票ＩＤが電子投票データ記憶部３３２に記憶されているか否かを判断する。この判断がＹＥＳの場合、開票ＣＰＵは、処理をステップＳ３５４に移し、ＮＯの場合、開票ＣＰＵは、処理をステップＳ３５７に移す。

【０２５６】

ステップＳ３５４において、開票ＣＰＵは、電子投票データ５２１に投票ＩＤを対応付けて電子投票データ記憶部３３２に記憶する。その後、開票ＣＰＵは、処理をステップＳ３５５に移す。

【０２５７】

ステップＳ３５５において、開票ＣＰＵは、開票条件を満たすか否かを判断する。すなわち、開票ＣＰＵは、図１６のステップＳ３０２と同様に、開票条件を満たすか否かを判断する。この判断がＹＥＳの場合、開票ＣＰＵは、処理をステップＳ３５６に移し、ＮＯの場合、開票ＣＰＵは、処理をステップＳ３５１に移す。

【０２５８】

ステップＳ３５６において、開票ＣＰＵは、開票処理を行う。すなわち、開票ＣＰＵは、図１６のステップＳ３０３からステップＳ３１０と同様に、開票処理を行う。その後、開票ＣＰＵは、処理を終了する。

【０２５９】

ステップＳ３５７において、開票ＣＰＵは、受信した投票ＩＤによって検索し、検索した投票ＩＤに対応付けられた電子投票データ５２１に上書きする。すなわち、開票ＣＰＵ

は、電子投票データ５２１と投票ＩＤとを対応付けて記憶した電子投票データ記憶部３３２を投票ＩＤのうち製品ＩＤによって検索し、検索した製品ＩＤを含む投票ＩＤに対応付けられた電子投票データ５２１に上書きして電子投票データ記憶部３３２に記憶する。その後、開票ＣＰＵは、処理をステップＳ３５５に移す。なお、開票ＣＰＵは、投票ＩＤに含まれる時刻に基づいて上書きするとしてもよい。

【０２６０】

本実施形態によれば、暗号化装置４００は、３原色の階調値から構成される画素によって構成される画像を読み込み、読み込まれた画像を構成する３原色のうち一の原色又は二の原色の階調値に基づいて複数の擬似乱数を生成し、生成された複数の各擬似乱数に基づいて、所定の演算を実行し、画像内の画素の位置を順に複数個算出する。そして、暗号化装置４００は、算出された複数個の各位置に係る画素を構成する３原色の階調値のうち、擬似乱数を生成するために用いた一の原色又は二の原色以外の原色の階調値を構成するビットのうち所定のビットに、擬似乱数を算出した順に、ビットの重みを対応付け、重みが対応付けられた所定のビットに、情報を構成するビットのうち、所定のビットに対応付けられた重みと同じ重みのビットの値を埋め込む。したがって、画像を構成する画素の階調値が変更されている場合には情報を埋め込んだ画素を算出することができないので、暗号化装置４００は、画像データが改竄されている場合には復号できないような暗号を作成することができる。

【０２６１】

さらに、暗号化装置４００は、画像内に領域を設定し、設定された領域を構成する画素の階調値に基づいて算出した画素に、情報を埋め込む。さらに、暗号化装置４００は、算出した画素の位置が重複する場合に、算出したハッシュ値に基づいて算出した画素に、情報を埋め込む。したがって、暗号化装置４００は、復号することが困難な暗号を作成することができる。

【０２６２】

以上、本発明の実施形態について説明したが、本発明は上述した実施形態に限るものではない。また、本発明の実施形態に記載された効果は、本発明から生じる最も好適な効果を列挙したに過ぎず、本発明による効果は、本発明の実施形態に記載されたものに限定されるものではない。

【符号の説明】

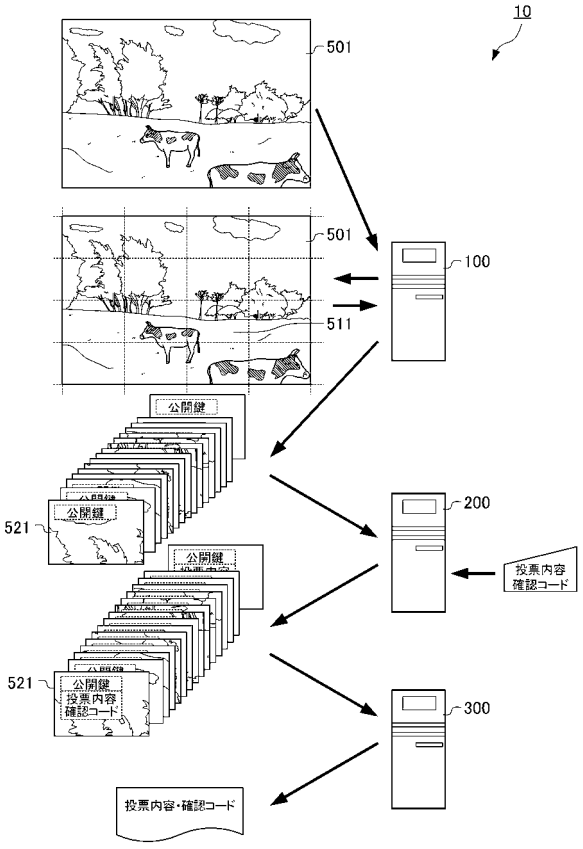
【０２６３】

１０　電子投票システム
１００　電子投票データ作成装置
１０１　秘密コード受付部
１０２　全体画像データ変更部
１０３　全体画像コード算出部
１０４　暗号秘密コード算出部
１０５　暗号鍵作成部
１０６　分割数設定部
１０７　全体画像分割部
１０８　作成領域設定部
１０９　公開鍵位置算出部
１１０　固有コード作成部
１１１　固有コード位置算出部
１１２　冗長情報書込部
１１３　電子投票データ作成部
１１４　電子投票データ出力部
１３１　作成パラメータ記憶部
２００　電子投票装置
２０１　投票入力部

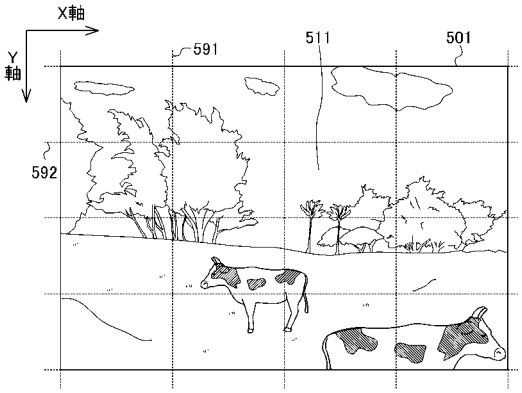
２０２　投票領域設定部
２０３　投票公開鍵位置算出部
２０４　公開鍵取得部
２０５　投票受付部
２０６　パスワード受付部
２０７　投票内容領域設定部
２０８　投票内容位置算出部
２０９　パスワード暗号化部
２１０　パスワード位置算出部
２１１　投票書込部
２１２　再投票受付部
２１３　投票出力部
２３１　投票パラメータ記憶部
３００　電子開票装置
３０１　開票入力部
３０２　開票判断部
３０３　開票秘密コード受付部
３０４　開票固有コード位置算出部
３０５　固有コード取得部
３０６　電子投票データ検索部
３０７　電子投票データ決定部
３０８　開票全体画像コード算出部
３０９　開票暗号秘密コード算出部
３１０　秘密鍵作成部
３１１　開票領域設定部
３１２　開票パスワード位置算出部
３１３　暗号パスワード取得部
３１４　暗号パスワード復号部
３１５　開票投票内容領域設定部
３１６　開票投票位置算出部
３１７　投票データ取得部
３１８　開票公表部
３３１　開票パラメータ記憶部
３３２　電子投票データ記憶部
４００　暗号化装置
４０１　画像読込部
４０２　領域設定部
４０３　擬似乱数生成部
４０４　位置算出部
４０５　ハッシュ値算出部
４０６　重み対応付部
４０７　埋込部
７００　電子投票媒体
７０１　時刻取得部
７０２　投票識別コード作成部
７０３　投票識別コード出力部
７０４　投票データ入力部
７０５　確認コード作成部
７０６　パスワード作成部
７０７　投票内容書込部

７０８　公開鍵取得部
７０９　暗号化書込部
７１０　電子投票データ出力部
７１１　表示部
７２１　ＩＤ作成ボタン
７２２　確認コード作成ボタン
７２３　表示ボタン
７２４　投票ボタン
７３１　媒体パラメータ記憶部
７３２　投票データ記憶部
７３３　媒体識別情報記憶部
７３４　接続部
７３５　表示装置

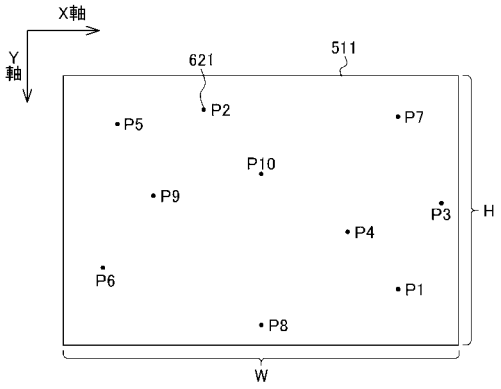
【図１】



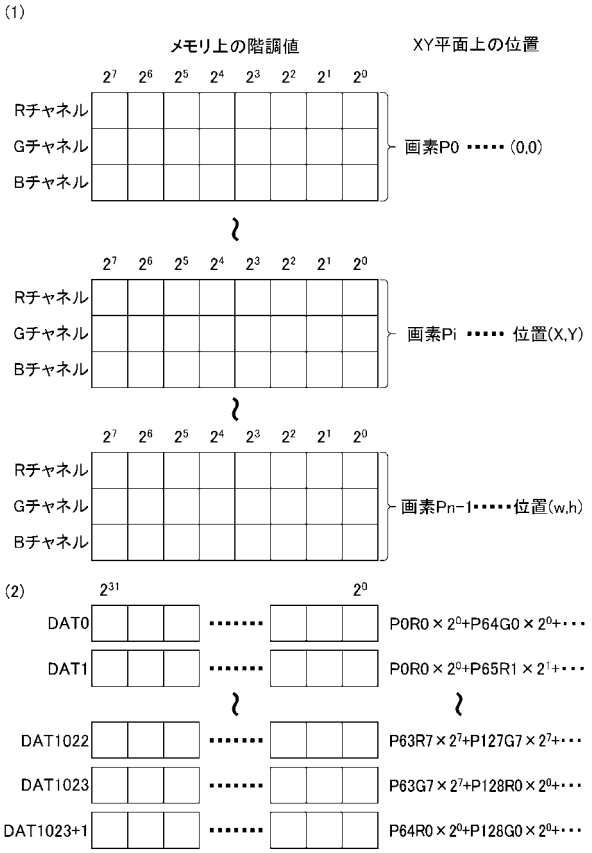
【図２】



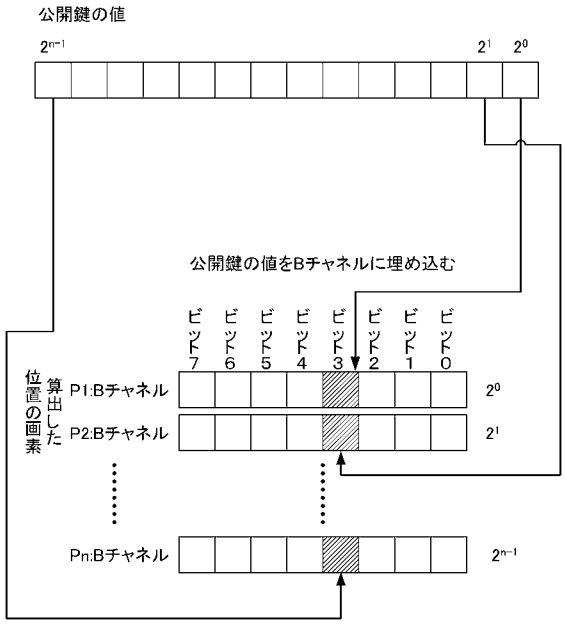
【図３】


X軸
Y軸
621
511
P2
P5
P7
P10
P9
P3
P4
P6
P1
P8
H
W

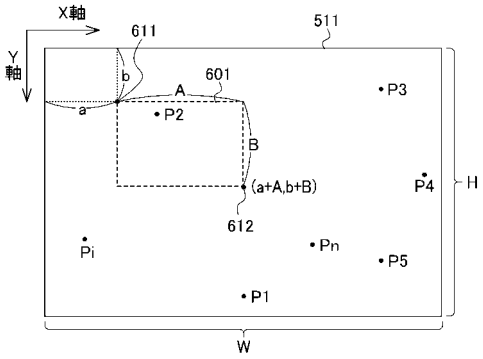
【図４】


(1)
メモリ上の階調値
XY平面上の位置
Rチャネル
Gチャネル
Bチャネル
画素P0 ・・・・・ (0,0)
画素Pi ・・・・・ 位置(X,Y)
画素Pn−1・・・・・位置(w,h)
(2)
DAT0
DAT1
DAT1022
DAT1023
DAT1023+1
P0R0×2^0+P64G0×2^0+・・・
P0R0×2^0+P65R1×2^1+・・・
P63R7×2^7+P127G7×2^7+・・・
P63G7×2^7+P128R0×2^0+・・・
P64R0×2^0+P128G0×2^0+・・・

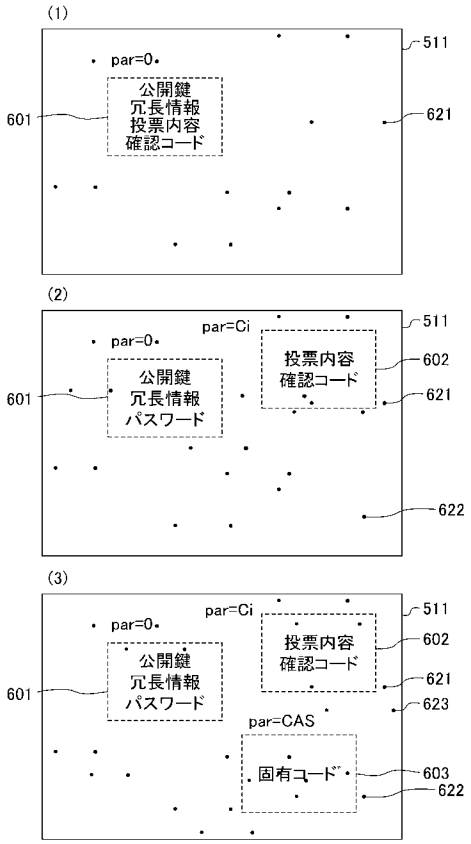
【図５】


公開鍵の値
公開鍵の値をBチャネルに埋め込む
ビット7
ビット6
ビット5
ビット4
ビット3
ビット2
ビット1
ビット0
算出した位置の画素
P1:Bチャネル
P2:Bチャネル
Pn:Bチャネル

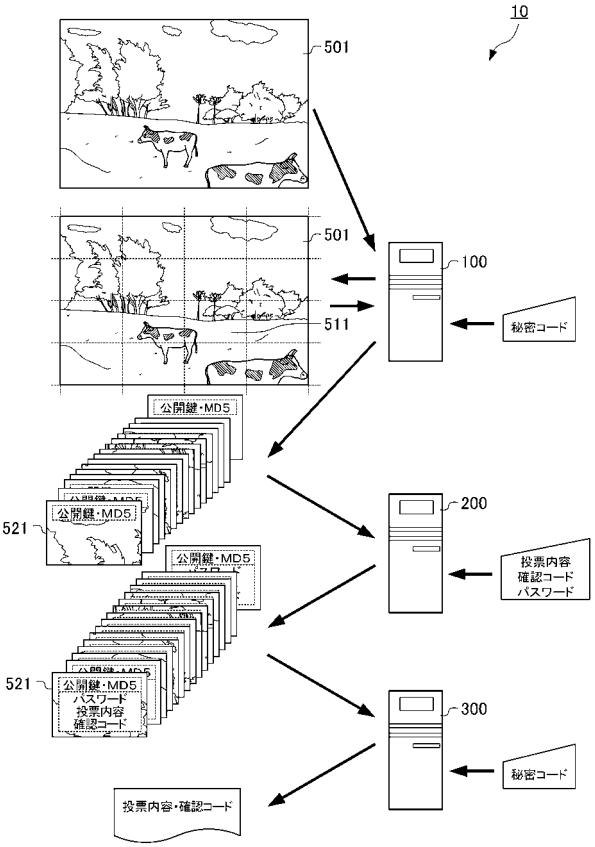
【図６】


X軸
Y軸
611
511
601
a
b
A
B
P2
P3
P4
P1
Pi
Pn
P5
(a+A,b+B)
612
H
W

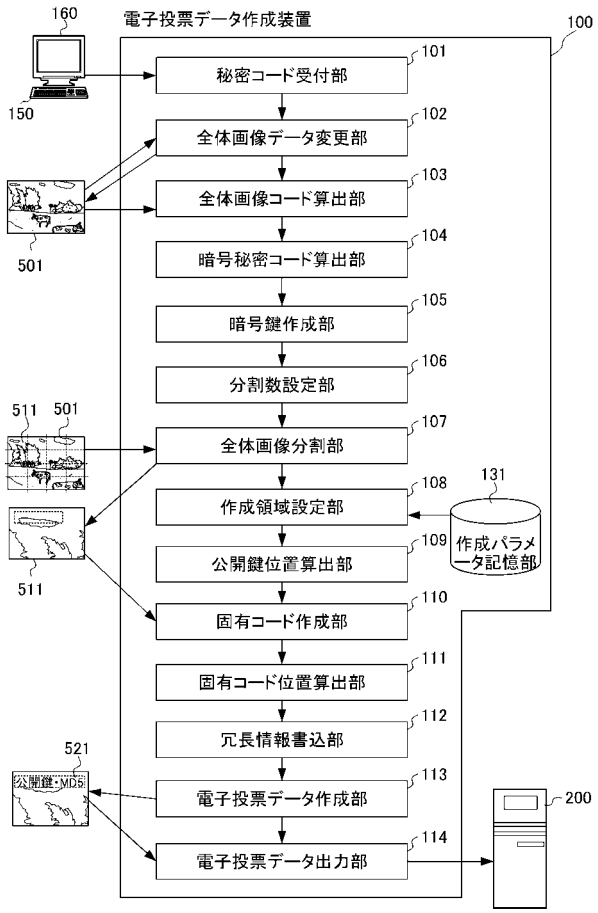
【図７】


(1)
par=0
公開鍵
冗長情報
投票内容
確認コード
601
511
621
(2)
par=0
par=Ci
公開鍵
冗長情報
パスワード
投票内容
確認コード
601
511
602
621
622
(3)
par=0
par=Ci
公開鍵
冗長情報
パスワード
投票内容
確認コード
par=CAS
固有コード
601
511
602
621
623
603
622

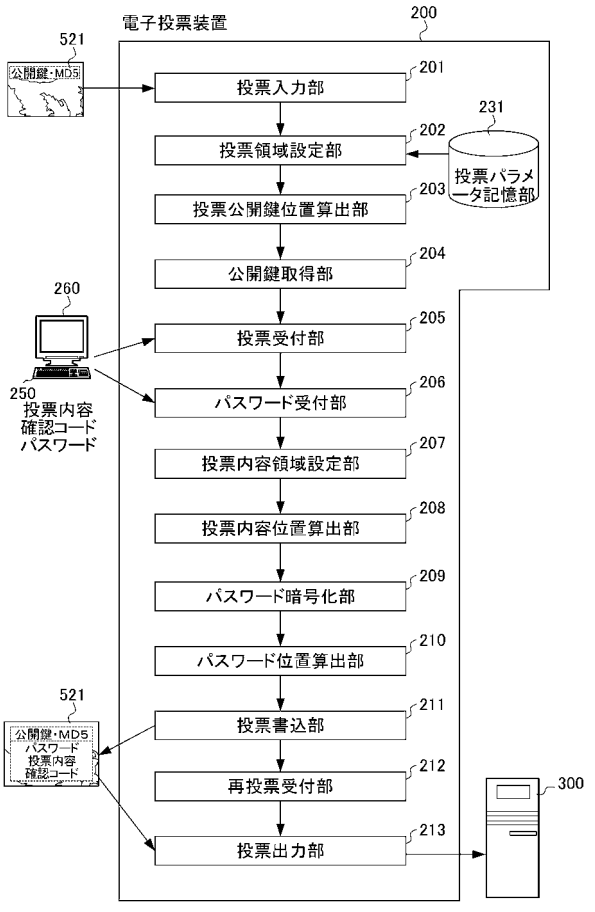
【図８】


10
501
501
511
100
秘密コード
公開鍵・MD5
521
200
投票内容
確認コード
パスワード
公開鍵・MD5
パスワード
投票内容
確認コード
521
300
秘密コード
投票内容・確認コード

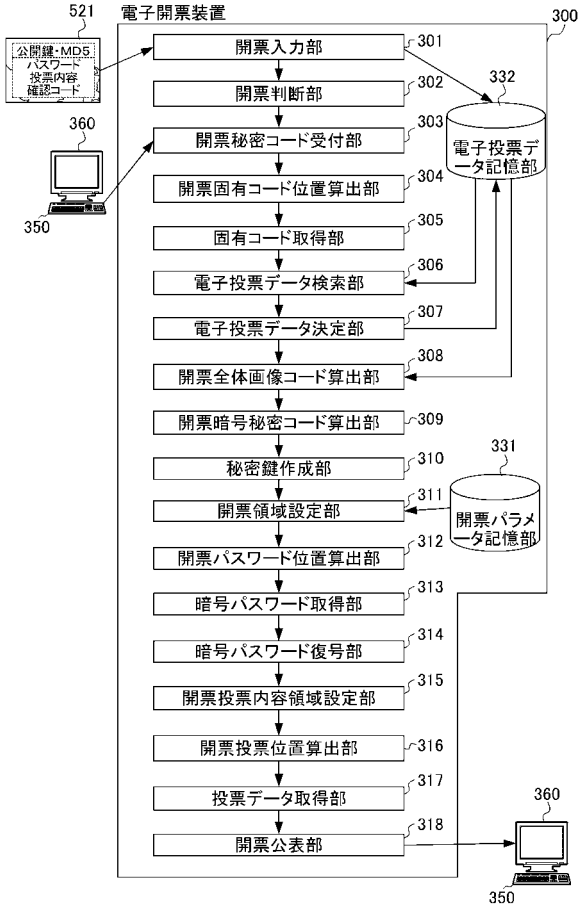
【図９】


160
電子投票データ作成装置
100
150
秘密コード受付部
101
全体画像データ変更部
102
501
全体画像コード算出部
103
暗号秘密コード算出部
104
暗号鍵作成部
105
分割数設定部
106
511
501
全体画像分割部
107
作成領域設定部
108
131
作成パラメータ記憶部
511
公開鍵位置算出部
109
固有コード作成部
110
固有コード位置算出部
111
冗長情報書込部
112
521
公開鍵・MD5
電子投票データ作成部
113
200
電子投票データ出力部
114

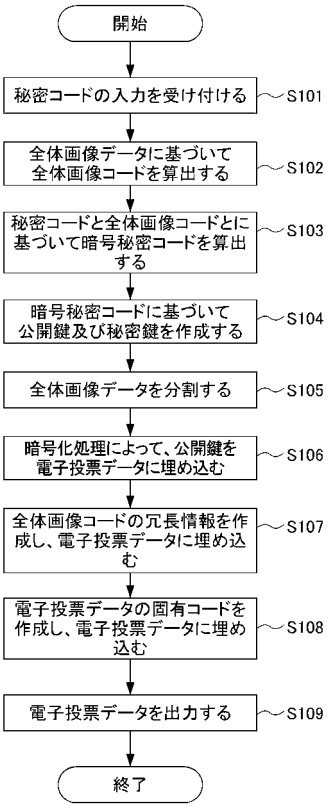
【図１０】


電子投票装置
200
521
公開鍵・MD5
投票入力部
201
投票領域設定部
202
231
投票パラメータ記憶部
投票公開鍵位置算出部
203
公開鍵取得部
204
260
投票受付部
205
250
投票内容
確認コード
パスワード
パスワード受付部
206
投票内容領域設定部
207
投票内容位置算出部
208
パスワード暗号化部
209
パスワード位置算出部
210
521
公開鍵・MD5
パスワード
投票内容
確認コード
投票書込部
211
再投票受付部
212
300
投票出力部
213

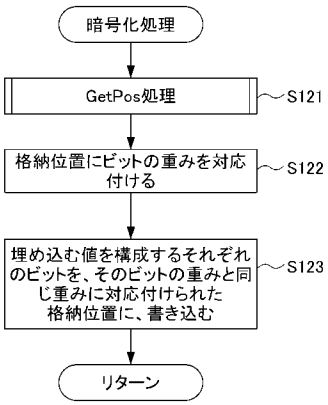
【図１１】



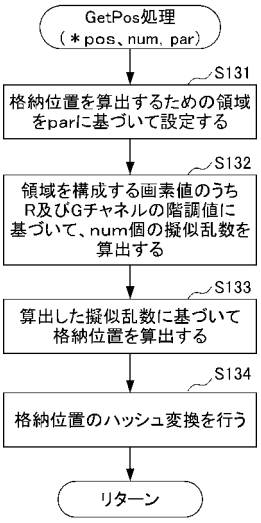
【図１２】



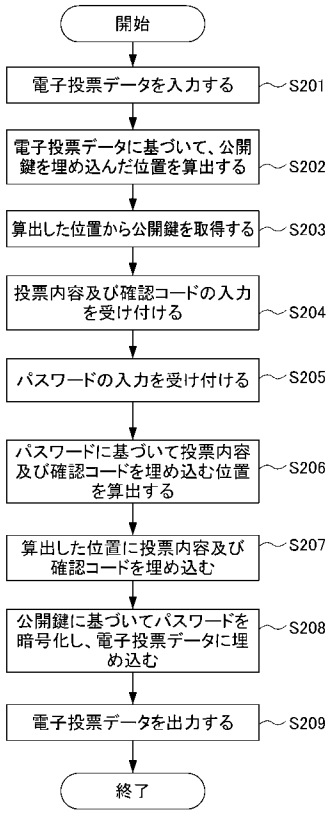
【図１３】



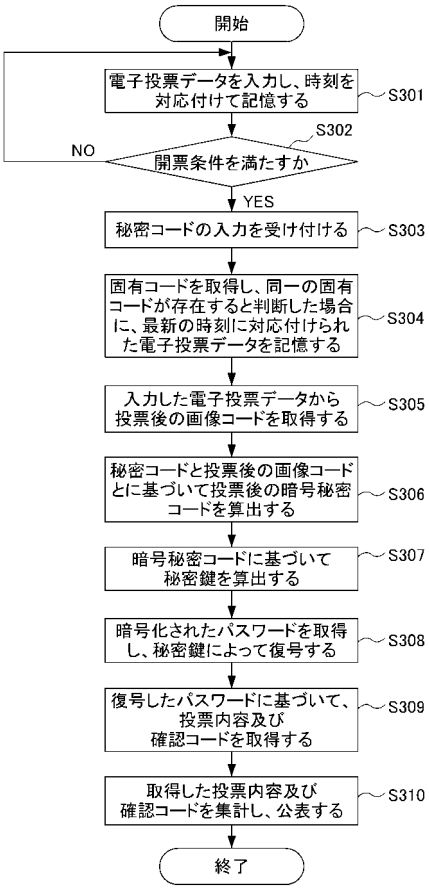
【図１４】



【図１５】



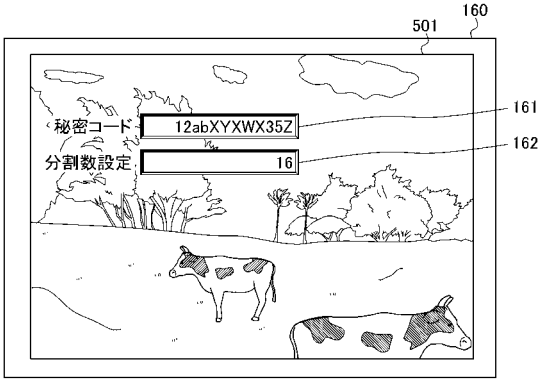
【図１６】



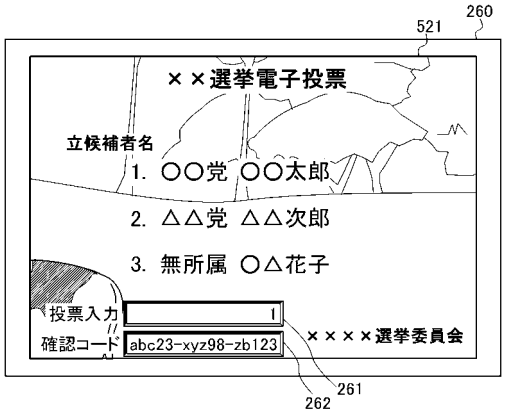
【図１７】

画素の位置			階調値(2進)			ビットの
番号	X	Y	R値	G値	B値	重み
P1	24	123	10000001	11000001	01000001	0
P2	521	150	10001001	01000000	10000001	1
・・・	・・・	・・・	・・・	・・・	・・・	・・・
・・・	・・・	・・・	・・・	・・・	・・・	・・・
・・・	・・・	・・・	・・・	・・・	・・・	・・・
P1023	200	100	00001001	11000101	00100101	1022
P1024	10	150	00010001	11001000	01010000	1023

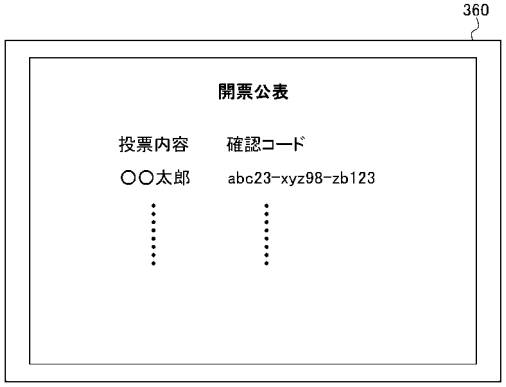
【図１８】



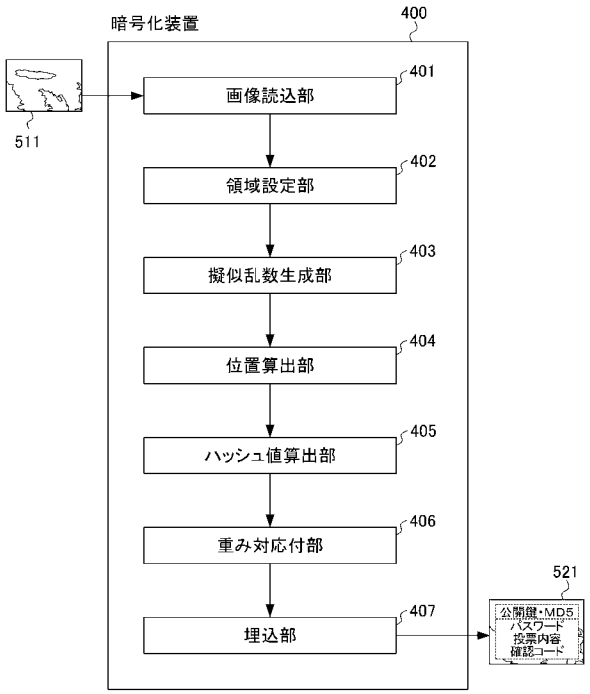
【図１９】



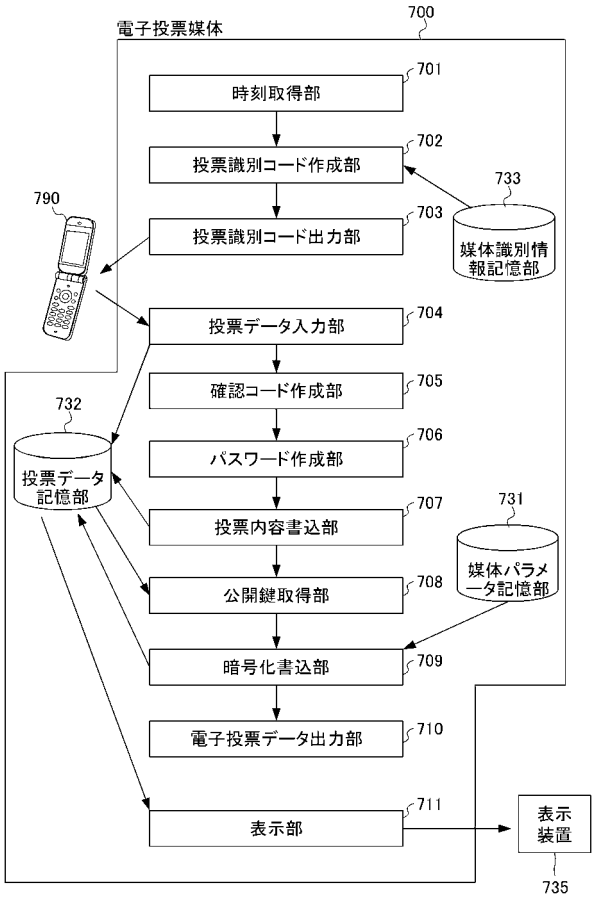
【図２０】



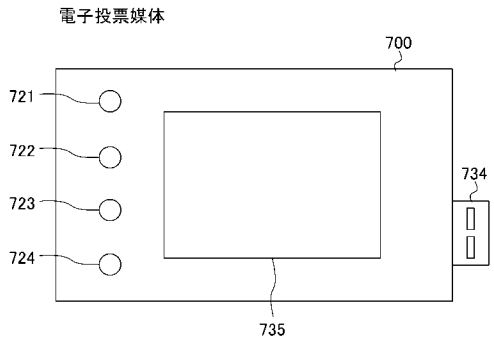
【図２１】



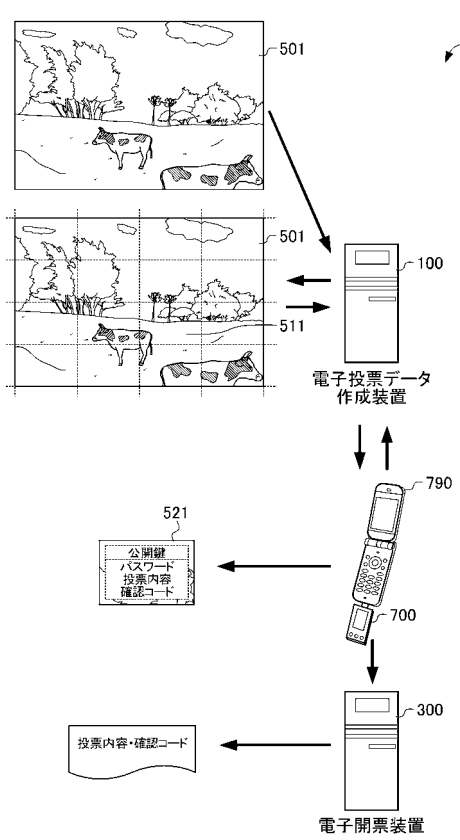
【図２２】



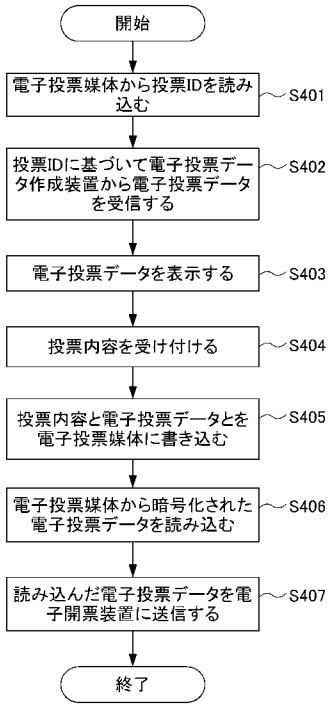
【図２３】



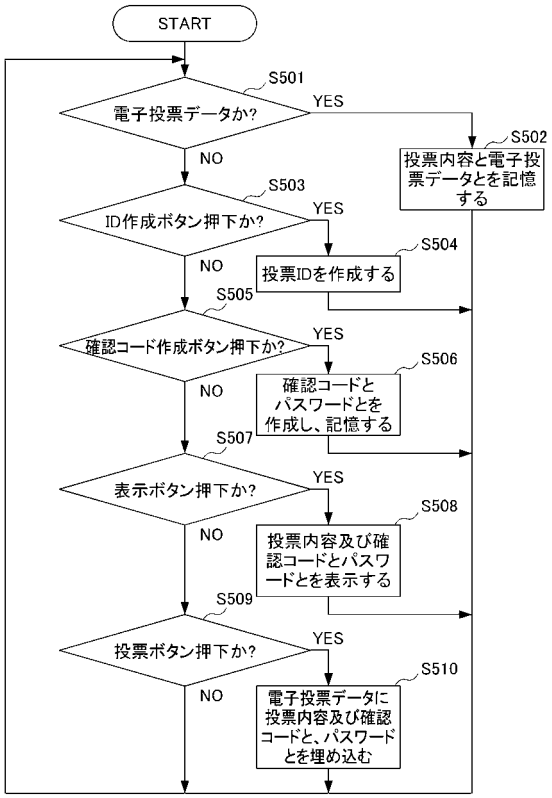
【図２４】



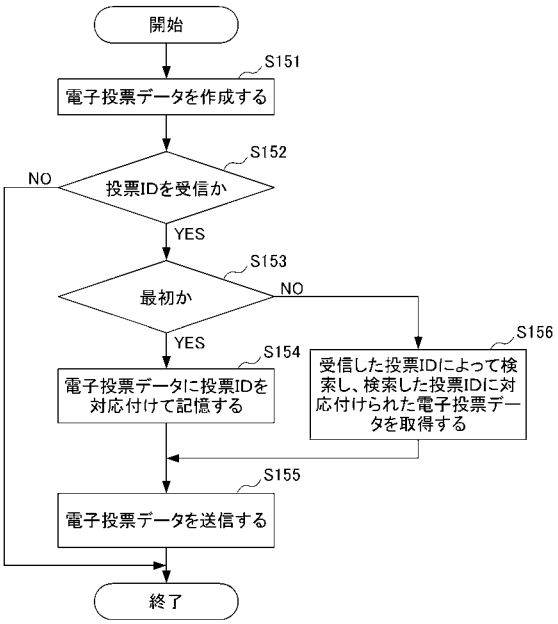
【図２５】



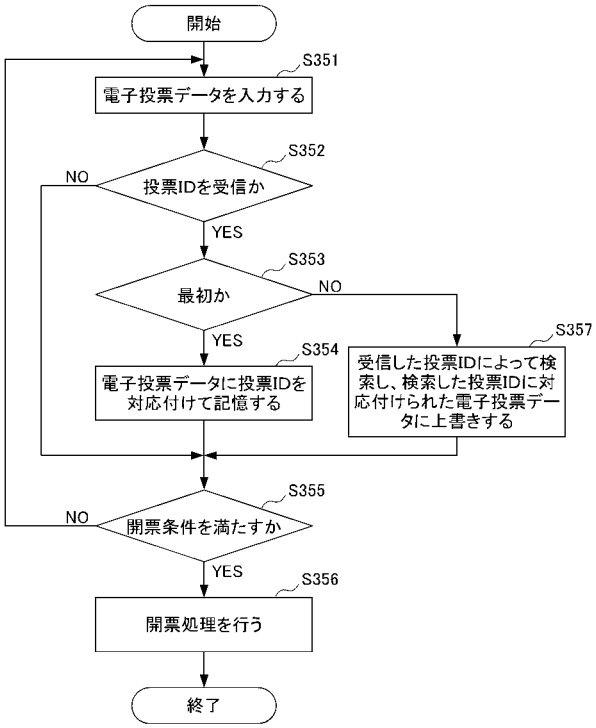
【図２６】



【図２７】



【図２８】



フロントページの続き

Ｆターム(参考) 5J104 AA08 AA14 LA02 NA27 NA38 PA14