

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5397858号
(P5397858)

(45) 発行日 平成26年1月22日(2014.1.22)

(24) 登録日 平成25年11月1日(2013.11.1)

(51) Int. Cl. F I
G06Q 30/08 (2012.01) G O 6 Q 30/08
H04L 9/08 (2006.01) H O 4 L 9/00 6 O 1 Z

請求項の数 2 (全 42 頁)

| | |
|---|--|
| <p>(21) 出願番号 特願2009-260370 (P2009-260370) (22) 出願日 平成21年11月13日(2009.11.13) (65) 公開番号 特開2011-107842 (P2011-107842A) (43) 公開日 平成23年6月2日(2011.6.2) 審査請求日 平成24年11月6日(2012.11.6)</p> | <p>(73) 特許権者 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 審査官 鹿野 博嗣</p> |
|---|--|

最終頁に続く

(54) 【発明の名称】 電子投票媒体

(57) 【特許請求の範囲】

【請求項1】

投票の内容を書き込むための電子投票媒体であって、
 電子投票媒体を識別するための媒体識別情報を記憶する媒体識別情報記憶手段と、
 現在の時刻を取得する時刻取得手段と、
 前記媒体識別情報記憶手段によって記憶された前記媒体識別情報と、前記時刻取得手段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を作成する投票識別コード作成手段と、
 前記投票識別コードのうち最新の前記投票識別コードを出力する投票識別コード出力手段と、
 公開鍵が所定の方法によって書き込まれた電子投票データと、受け付けられた候補者を示す投票内容とを入力する投票データ入力手段と、
 前記投票内容に対応付けて確認コードを作成する確認コード作成手段と、
 前記投票内容及び前記確認コードを抽出するためのパスワードを作成するパスワード作成手段と、
 前記電子投票データに、前記パスワード作成手段によって作成されたパスワードに基づいて、前記投票内容及び前記確認コードを埋め込む投票内容書込手段と、
 前記投票データ入力手段によって入力された前記電子投票データから前記公開鍵を取得する公開鍵取得手段と、
 前記電子投票データに、前記公開鍵取得手段によって取得された前記公開鍵に基づいて

前記パスワードを暗号化して埋め込む暗号化書込手段と、

前記暗号化書込手段によって書き込まれた電子投票データを出力する電子投票データ出力手段と、

を備える電子投票媒体。

【請求項 2】

前記投票内容及び前記確認コードに、前記パスワードと、前記投票識別コードとを対応付けて記憶する投票データ記憶手段と、

前記投票データ記憶手段に記憶された前記投票内容及び前記確認コードと、前記パスワードと、前記投票識別コードとを対応付けて表示する表示手段と、

をさらに備える請求項 1 に記載の電子投票媒体。

10

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、電子投票に利用される電子投票媒体に関する。

【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。

20

【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】

30

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。

40

【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、デジタル証明書と投票メッセージ

50

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】

また、特許文献1が開示するシステムにおいて、認証機関は投票者に一意のシリアル番号を発行する。そして、特許文献1が開示するシステムは、不正な投票を防ぐために、シリアル番号によって投票が1回しかできないようにしている。このようなシステムは、一意のシリアル番号を発行するために、投票者を一人一人認証する必要があるので、煩雑になりかねない。

10

【0009】

そこで、電子投票において、不正な投票を防止することができ、かつ、同一人であるならば定められた開票日まで何度でも投票をすることができる装置が望まれている。

【0010】

本発明は、電子投票において、同一人であるならば定められた開票日まで何度でも投票をすることができ、かつ、不正な投票を容易に防止することができる装置を提供することを目的とする。

【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。

20

【0012】

(1) 投票の内容を書き込むための電子投票媒体であって、電子投票媒体を識別するための媒体識別情報を記憶する媒体識別情報記憶手段と、現在の時刻を取得する時刻取得手段と、前記媒体識別情報記憶手段によって記憶された前記媒体識別情報と、前記時刻取得手段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を作成する投票識別コード作成手段と、前記投票識別コードのうち最新の前記投票識別コードを出力する投票識別コード出力手段と、公開鍵が所定の方法によって書き込まれた電子投票データと、受け付けられた候補者を示す投票内容とを入力する投票データ入力手段と、前記投票内容に対応付けて確認コードを作成する確認コード作成手段と、前記投票内容及び前記確認コードを抽出するためのパスワードを作成するパスワード作成手段と、前記電子投票データに、前記パスワード作成手段によって作成されたパスワードに基づいて、前記投票内容及び前記確認コードを埋め込む投票内容書込手段と、前記投票データ入力手段によって入力された前記電子投票データから前記公開鍵を取得する公開鍵取得手段と、前記電子投票データに、前記公開鍵取得手段によって取得された前記公開鍵に基づいて前記パスワードを暗号化して埋め込む暗号化書込手段と、前記暗号化書込手段によって書き込まれた電子投票データを出力する電子投票データ出力手段と、を備える電子投票媒体。

30

【0013】

(1)の構成によれば、本発明に係る電子投票媒体は、投票の内容を書き込むための電子投票媒体であって、電子投票媒体を識別するための媒体識別情報記憶手段を有する。そして、本発明に係る電子投票媒体は、現在の時刻を取得し、媒体識別情報記憶手段によって記憶された媒体識別情報と、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を作成し、投票識別コードのうち最新の投票識別コードを出力する。そして、本発明に係る電子投票媒体は、公開鍵が所定の方法によって書き込まれた電子投票データと、受け付けられた候補者を示す投票内容とを入力し、投票内容に対応付けて確認コードを作成し、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し、電子投票データに、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み、入力された電子投票データから公開鍵を取得し、電子投票データに、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み、書き込まれた電子投票データを出力する。

40

50

【 0 0 1 4 】

すなわち、本発明に係る電子投票媒体は、媒体を識別する媒体識別情報と、投票内容及び確認コード並びに暗号化したパスワードを埋め込んだ電子投票データと、を出力する。よって、電子投票データを開票するシステムは、媒体識別情報と共に出力された電子投票データを識別することができ、同一人が同じ電子投票媒体から開票日までに何度も投票した電子投票データを媒体識別情報によって一の投票とみなすことができる。したがって、本発明に係る電子投票媒体は、電子投票において、同一人であるならば定められた開票日までに何度でも投票をすることができる電子投票データを作成することができ、かつ、不正な投票を容易に防止することができる電子投票データを作成することができる。

【 0 0 1 5 】

さらに、電子投票データには投票内容及び確認コードがパスワードに基づいて埋め込まれているので、本発明に係る電子投票媒体は、秘密鍵による復号とは別に、本人の了承のもとに入手したパスワードによって投票内容を抽出することができる電子投票データを作成することができる。したがって、本発明に係る電子投票媒体は、投票後の集計が正しく行われたことを確認し、検証することができる電子投票データを作成することができる。

【 0 0 1 6 】

(2) 前記投票内容及び前記確認コードに、前記パスワードと、前記投票識別コードとを対応付けて記憶する投票データ記憶手段と、前記投票データ記憶手段に記憶された前記投票内容及び前記確認コードと、前記パスワードと、前記投票識別コードとを対応付けて表示する表示手段と、をさらに備える(1)に記載の電子投票媒体。

【 0 0 1 7 】

(2)の構成によれば、(1)に記載の電子投票媒体は、さらに、投票内容及び確認コードに、パスワードと、投票識別コードとを対応付けて記憶し、記憶された投票内容及び確認コードと、パスワードと、投票識別コードとを対応付けて表示する。

【 0 0 1 8 】

したがって、(2)に記載の電子投票媒体は、投票内容を確認するための確認コードと、投票内容を検証するためのパスワードとを容易に投票者に提供することができる。

【 発明の効果 】

【 0 0 1 9 】

本発明によれば、電子投票媒体は、電子投票において、同一人であるならば定められた開票日までに何度でも投票をすることができ、かつ、不正な投票を容易に防止することができる電子投票データを作成することができる。

【 0 0 2 0 】

さらに、電子投票媒体が作成した投票識別コードは、投票内容と対になった確認コードとは別に作成されるので、公表される確認コードから投票識別コードが関連付けられることはない。よって、電子投票媒体は、投票識別コードによって特定することができる電子投票データを作成できると共に、投票者の匿名性を満たした電子投票データを作成することができる。

【 0 0 2 1 】

さらに、電子投票媒体は、秘密鍵による復号とは別に、本人の了承のもとに入手したパスワードによって投票内容を抽出することができる電子投票データを作成することができる。よって、電子投票媒体は、投票後の集計が正しく行われたことを確認し、検証することができる電子投票データを作成することができる。

【 図面の簡単な説明 】

【 0 0 2 2 】

【 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

10

20

30

40

50

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。

10

【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 Get Pos 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。

20

【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 5 2 1 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。

30

【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。

40

【発明を実施するための形態】

【0023】

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、本発明に係る電子投票媒体 700 が前提と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、本発明に係る電子投票媒体 700 が前提とする、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、本発明に係る電子投票媒体 700 において利用する暗号化方法を実行する暗号化装置 400 について説明し、実施形態 4 において、本発明に係る電子投票媒体 700 について説明する。

【0024】

50

〔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。

10

【0025】

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。

【0026】

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、トラックボール等) が挙げられる。

20

【0027】

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。

30

【0028】

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。

【0029】

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。

40

【0030】

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。

50

【0031】

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チャン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。

【0032】

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ンネル（格納用チャンネルといい、例えば、Bチャンネル）以外のチャンネル（算出用チャンネルといい、例えば、Rチャンネル及びノ
10
又はGチャンネル）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。

【0033】

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、 $d = e^{-1} \pmod{\text{lcm}(p-1)(q-1)}$ によって求められる。
20

【0034】

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。

【0035】

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。

【0036】

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。
30

(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ン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。
40

【0037】

(2) 算出した複数の画素の各格納用チャン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、各格納用チャン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ン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ンネルの所定のビット（例えば、
50

ビット3)にビットの重み「 2^n 」を対応付ける。

【0038】

(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ンネルのビット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ンネルのビット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ンネルのビット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。

10

【0039】

格納用チャン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。

【0040】

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。

20

【0041】

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、格納チャン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。

【0042】

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。

30

【0043】

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。

【0044】

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。

40

【0045】

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。

【0046】

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

50

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。

【0047】

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。

【0048】

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。

【0049】

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。

【0050】

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。

【0051】

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、格納用チャンネルのビット1）。

【0052】

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。

【0053】

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を収集できなかつたり、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。

10

【0054】

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。

【0055】

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。

【0056】

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。

20

【0057】

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ンネルのうち、格納用チャンネルは、Bチャンネルとし、算出用チャンネルは、Rチャンネル及びGチャンネルとする。各チャンネルは、例えば、8ビット構成とする。

30

【0058】

例えば、全体画像コード（例えば、1024ビット）は、Rチャンネル及びGチャンネルの階調値を加算することにより得られる。加算は、チャンネル単位（8ビットずつ）でなくてもよい。例えば、9ビットずつ（Rチャンネルの8ビット及びGチャンネルのLSBと、Gチャンネルの残り7ビット及び次の画素のRチャンネルの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。

【0059】

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。

40

【0060】

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

50

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。

【 0 0 6 1 】

図 4 は、本発明の一実施形態に係る分割画像データ 5 1 1 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。

【 0 0 6 2 】

図 4 (1) は、分割画像データ 5 1 1 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 チャンネルと、緑色の階調値を記憶する G チャンネルと、青色の階調値を記憶する B チャン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、X Y 平面上の位置で表わした場合を示す例である。

10

【 0 0 6 3 】

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 1 0 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。

【 0 0 6 4 】

ここで、1 番目の画素の R チャンネルのそれぞれのビットの値を P 0 R 0 から P 0 R 7 で表わし、n 番目の画素の R チャンネルのそれぞれのビットの値を P n R 0 から P n R 7 で表わす。同様に、1 番目の画素の G チャンネルのそれぞれのビットの値を P 0 G 0 から P 0 G 7 で表わし、n 番目の画素の G チャンネルのそれぞれのビットの値を P n G 0 から P n G 7 で表わす。すなわち、R チャンネル及び G チャンネルのビット値は次の様な並びで表わせる。

20

【 0 0 6 5 】

1 番目の R チャンネルのビット値 = P 0 R 0、P 0 R 1、P 0 R 2、P 0 R 3、P 0 R 4、P 0 R 5、P 0 R 6、P 0 R 7

1 番目の G チャンネルのビット値 = P 0 G 0、P 0 G 1、P 0 G 2、P 0 G 3、P 0 G 4、P 0 G 5、P 0 G 6、P 0 G 7

・
・

n 番目の R チャンネルのビット値 = P n R 0、P n R 1、P n R 2、P n R 3、P n R 4、P n R 5、P n R 6、P n R 7

n 番目の G チャンネルのビット値 = P n G 0、P n G 1、P n G 2、P n G 3、P n G 4、P n G 5、P n G 6、P n G 7

30

・
・

【 0 0 6 6 】

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、1 0 2 4 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 チャンネル又は G チャンネルの階調値の 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变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。

40

【 0 0 6 7 】

例えば、1 0 2 4 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

$Dat[0] = Dat[0] + P0R0 * 2^0$

$Dat[1] = Dat[1] + P0G0 * 2^0$

・
・

$Dat[1022] = Dat[1022] + P63R7 * 2^7$

$Dat[1023] = Dat[1023] + P63G7 * 2^7$

$Dat[1023+1] = Dat[1023+1] + P64R0 * 2^0$

50

2 巡目

$$\text{Dat}[0] = \text{Dat}[0] + P64G0 * 2^0$$

$$\text{Dat}[1] = \text{Dat}[1] + P64R1 * 2^1$$

.

.

$$\text{Dat}[1022] = \text{Dat}[1022] + P127G7 * 2^7$$

$$\text{Dat}[1023] = \text{Dat}[1023] + P128R0 * 2^0$$

$$\text{Dat}[1023+1] = \text{Dat}[1023+1] + P128G0 * 2^0$$

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。

【0068】

次に、生成された所定の個数（例えば、1024個）の疑似乱数に基づいて、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、生成した疑似乱数（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。

【0069】

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。

【0070】

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。

【0071】

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。

【0072】

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。

【0073】

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ン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、各格納用チャン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、疑似乱数Dat[0]に基づいて位置を算出し、算出した画素P1の格納用チャンネルの所定のビット（例えば、ビット3）にビットの重み「2⁰」を対応付ける。同様にして、電子投票システム10は、疑似乱数Dat[n - 1]に基づいて位置を算出し、算出した画素Pnの格納用チャン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。

【0074】

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「2⁰」が対応付けられた画素P1の格納用チャ

10

20

30

40

50

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。

【0075】

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。

10

【0076】

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。

【0077】

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。

【0078】

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。

20

【0079】

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。

【0080】

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

30

40

【0081】

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。

【0082】

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

50

票データ作成装置 100 は、B チャンネルのビット 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 チャンネルのビット 3 から公開鍵を復元する。そして、電子投票装置 200 は、B チャンネルのビット 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 チャンネルのビット 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 チャンネルのビット 1 から復元した投票内容及び確認コードを復号する。

【0083】

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 チャンネルのビット 2 に、暗号化され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 チャンネルのビット 1 に、受け付けた投票内容及び確認コードを埋め込む。

【0084】

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 チャンネルのビット 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。

【0085】

[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。

【0086】

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

10

20

30

40

50

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。

【0087】

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。

10

【0088】

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。

20

【0089】

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。

30

【0090】

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。

【0091】

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。

40

【0092】

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。

【0093】

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

50

素について、その画素の算出用チャンネルのビット0を反転する。

【0094】

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ンネルの各階調値を、加算やビット演算等することによって算出される。

【0095】

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。

10

【0096】

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。

【0097】

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。

【0098】

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。

20

【0099】

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。

【0100】

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。

30

【0101】

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ンネルの階調値を、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。

【0102】

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。

40

【0103】

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ン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。

50

【 0 1 0 4 】

電子投票データ作成部 1 1 3 は、公開鍵位置算出部 1 0 9 によって算出された公開鍵位置に、暗号鍵作成部 1 0 5 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 5 2 1 を固有に作成する。すなわち、電子投票データ作成部 1 1 3 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。

【 0 1 0 5 】

電子投票データ出力部 1 1 4 は、電子投票データ作成部 1 1 3 によって作成された電子投票データ 5 2 1 を電子投票装置 2 0 0 に出力する。例えば、電子投票データ出力部 1 1 4 は、コンピュータネットワークを介して電子投票データ 5 2 1 を電子投票装置 2 0 0 に出力する。そして、電子投票データ出力部 1 1 4 は、電子投票データ 5 2 1 の投票状態を投票済み状態にする。

10

【 0 1 0 6 】

図 1 0 は、本発明の一実施形態に係る電子投票装置 2 0 0 の機能を示す機能ブロック図である。電子投票装置 2 0 0 は、投票入力部 2 0 1 と、投票領域設定部 2 0 2 と、投票公開鍵位置算出部 2 0 3 と、公開鍵取得部 2 0 4 と、投票受付部 2 0 5 と、パスワード受付部 2 0 6 と、投票内容領域設定部 2 0 7 と、投票内容位置算出部 2 0 8 と、パスワード暗号化部 2 0 9 と、パスワード位置算出部 2 1 0 と、投票書込部 2 1 1 と、再投票受付部 2 1 2 と、投票出力部 2 1 3 と、投票パラメータ記憶部 2 3 1 とを備えている。このような電子投票装置 2 0 0 について各部ごとに説明する。

20

【 0 1 0 7 】

投票入力部 2 0 1 は、電子投票データ 5 2 1 を入力する。投票入力部 2 0 1 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 1 0 0 から電子投票データ 5 2 1 を入力する。

【 0 1 0 8 】

投票パラメータ記憶部 2 3 1 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 1 0 0 によって電子投票データ 5 2 1 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 1 3 1 の値) と同じである。

【 0 1 0 9 】

投票領域設定部 2 0 2 は、投票パラメータ記憶部 2 3 1 に記憶された所定のパラメータに基づいて、投票入力部 2 0 1 によって入力された電子投票データ 5 2 1 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 $p a r = 0$ である場合、投票領域設定部 2 0 2 は、電子投票データ作成装置 1 0 0 と同様に、図 7 (3) の領域 6 0 1 を設定する。

30

【 0 1 1 0 】

投票公開鍵位置算出部 2 0 3 は、投票領域設定部 2 0 2 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 2 0 3 は、電子投票データ作成装置 1 0 0 と同様に、公開鍵位置を算出する。

【 0 1 1 1 】

公開鍵取得部 2 0 4 は、投票公開鍵位置算出部 2 0 3 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 1 0 0 によって埋め込まれた公開鍵を取得する。

40

【 0 1 1 2 】

投票受付部 2 0 5 は、投票内容と、確認コードとの入力を受け付ける。

【 0 1 1 3 】

パスワード受付部 2 0 6 は、パスワードの入力を受け付ける。

【 0 1 1 4 】

投票内容領域設定部 2 0 7 は、パスワード受付部 2 0 6 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 5 2 1 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 2 0 7 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 (C i) を算出し、算出したパラメータによって、図 7 (3) の領域 6

50

02を設定する。

【0115】

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。

【0116】

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。

【0117】

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。

10

【0118】

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。

【0119】

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。

20

【0120】

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。

【0121】

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。

30

【0122】

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。

40

【0123】

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。

【0124】

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。

【0125】

50

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。

【0126】

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。

10

【0127】

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 (MD5) 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。

【0128】

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。

【0129】

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。

20

30

【0130】

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。

40

【0131】

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。

【0132】

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。

50

【 0 1 3 3 】

開票パラメータ記憶部 3 3 1 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 1 0 0 によって電子投票データ 5 2 1 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 1 3 1 の値）と同じである。

【 0 1 3 4 】

開票領域設定部 3 1 1 は、開票パラメータ記憶部 3 3 1 に記憶された所定のパラメータに基づいて、開票入力部 3 0 1 によって入力された電子投票データ 5 2 1 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 3 1 1 は、電子投票データ作成装置 1 0 0 と同様に、図 7 (3) の領域 6 0 1 を設定する。

10

【 0 1 3 5 】

開票パスワード位置算出部 3 1 2 は、開票領域設定部 3 1 1 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。

【 0 1 3 6 】

暗号パスワード取得部 3 1 3 は、開票パスワード位置算出部 3 1 2 によって算出されたパスワード位置から、電子投票装置 2 0 0 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。

【 0 1 3 7 】

暗号パスワード復号部 3 1 4 は、秘密鍵作成部 3 1 0 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 3 1 3 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。

20

【 0 1 3 8 】

開票投票内容領域設定部 3 1 5 は、暗号パスワード復号部 3 1 4 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 5 2 1 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 5 2 1 内の位置）である場合、開票投票内容領域設定部 3 1 5 は、図 7 (3) の領域 6 0 2 を設定する。

【 0 1 3 9 】

開票投票位置算出部 3 1 6 は、開票投票内容領域設定部 3 1 5 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。

30

【 0 1 4 0 】

投票データ取得部 3 1 7 は、開票投票位置算出部 3 1 6 によって算出された投票内容位置から、電子投票装置 2 0 0 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 3 1 7 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。

【 0 1 4 1 】

開票公表部 3 1 8 は、投票データ取得部 3 1 7 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。

【 0 1 4 2 】

図 1 2 は、本発明の一実施形態に係る電子投票データ作成装置 1 0 0 の処理内容を示すフローチャートである。

40

【 0 1 4 3 】

ステップ S 1 0 1 において、電子投票データ作成装置 1 0 0 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 1 5 0（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 5 0 1 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ンネルのビット 0 を反転する）。その後、作成 CPU は、処理をステップ S 1 0 2 に移す。

【 0 1 4 4 】

ステップ S 1 0 2 において、作成 CPU は、全体画像データ 5 0 1 に基づいて全体画像

50

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ンネルの各階調値を、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。

【0145】

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。

【0146】

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。

【0147】

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。

【0148】

ステップS106において、作成CPUは、暗号化处理(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ンネルのビット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

【0149】

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ンネルのビット5に埋め込む。その後、作成CPUは、処理をステップS108に移す。

【0150】

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ンネルのビット4に埋め込む。その後、作成CPUは、処理をステップS109に移す。

【0151】

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ンネルのビット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。

【0152】

図13は、本発明の一実施形態に係る暗号化处理の内容を示すフローチャートである。なお、暗号化处理は、電子投票データ作成装置100だけでなく、電子投票装置200、

10

20

30

40

50

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。

【0153】

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。

【0154】

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 、 \dots 、 $2^{10^{2^3}}$) を対応付ける。その後、CPU は、処理をステップ S123 に移す。

10

【0155】

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。

【0156】

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。

20

【0157】

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。

30

【0158】

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。

【0159】

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 $x = \text{擬似乱数} \bmod (w - 2)$ 、格納位置 $y = \text{擬似乱数} \bmod (h - 1)$ 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。

40

【0160】

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 $x = (\text{格納位置} x + 23) \bmod (w)$ 、新格納位置 $y = (\text{格納位置} y + 11) \bmod (h)$ 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。

【0161】

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

50

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。

【0162】

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。

【0163】

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。

【0164】

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。

【0165】

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。

【0166】

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。

【0167】

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。

【0168】

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。

【0169】

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。

【0170】

10

20

30

40

50

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。

【0171】

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。

【0172】

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。

10

【0173】

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。

20

【0174】

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。

【0175】

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。

30

【0176】

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。

40

【0177】

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。

【0178】

50

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。

【0179】

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ンネルのビット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。

10

【0180】

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ンネルのビット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。

20

【0181】

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。

【0182】

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。

30

【0183】

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。

【0184】

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。

【0185】

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。

40

【0186】

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。

【0187】

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

50

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。

【0188】

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。

【0189】

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。

10

【0190】

[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。

【0191】

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。

20

【0192】

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。

【0193】

領域設定部 402 は、画像内に領域を設定する。

【0194】

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。

30

【0195】

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。

【0196】

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。

40

【0197】

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。

【0198】

50

[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。

【 0199 】

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。

10

【 0200 】

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。

【 0201 】

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。

【 0202 】

時刻取得部 701 は、現在の時刻を取得する。

20

【 0203 】

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 P Q R S 0 1 2 3 4 とすると、投票 ID として、P Q R S 0 1 2 3 4 - 2 0 0 9 0 1 2 3 1 6 5 9 - 0 0 0 1 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。

【 0204 】

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。

30

【 0205 】

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。

【 0206 】

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。

【 0207 】

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。

【 0208 】

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、Get Pos 処理 (図 14 参照) へのパラメータ (p a r = C i) 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。

40

【 0209 】

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。

50

【0210】

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。

【0211】

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。 10

【0212】

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。

【0213】

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。

【0214】

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。 20

【0215】

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。 30

(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。

【0216】

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。 40

【0217】

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 50

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。

【0218】

10

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。

【0219】

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。

20

【0220】

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。

【0221】

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。

【0222】

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。

30

【0223】

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。

【0224】

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。

【0225】

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。

40

【0226】

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。

【0227】

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。

【0228】

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。

50

【 0 2 2 9 】

ステップ S 5 0 2 において、媒体 C P U は、投票内容と電子投票データ 5 2 1 とを記憶部に記憶する。その後、媒体 C P U は、処理をステップ S 5 0 1 に移す。

【 0 2 3 0 】

ステップ S 5 0 3 において、媒体 C P U は、ID 作成ボタン 7 2 1 押下か否かを判断する。この判断が Y E S の場合、媒体 C P U は、処理をステップ S 5 0 4 に移し、N O の場合、媒体 C P U は、処理をステップ S 5 0 5 に移す。

【 0 2 3 1 】

ステップ S 5 0 4 において、媒体 C P U は、投票 ID を作成する。より具体的には、媒体 C P U 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 7 3 3 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 C P U 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 C P U は、処理をステップ S 5 0 1 に移す。

10

【 0 2 3 2 】

ステップ S 5 0 5 において、媒体 C P U は、確認コード作成ボタン 7 2 2 押下か否かを判断する。この判断が Y E S の場合、媒体 C P U は、処理をステップ S 5 0 6 に移し、N O の場合、媒体 C P U は、処理をステップ S 5 0 7 に移す。

【 0 2 3 3 】

ステップ S 5 0 6 において、媒体 C P U 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 C P U は、確認コード作成ボタン 7 2 2 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 7 2 2 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 C P U 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 C P U は、処理をステップ S 5 0 1 に移す。

20

【 0 2 3 4 】

ステップ S 5 0 7 において、媒体 C P U は、表示ボタン 7 2 3 押下か否かを判断する。この判断が Y E S の場合、媒体 C P U は、処理をステップ S 5 0 8 に移し、N O の場合、媒体 C P U は、処理をステップ S 5 0 9 に移す。

【 0 2 3 5 】

ステップ S 5 0 8 において、媒体 C P U 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 C P U は、検出した表示ボタン 7 2 3 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 7 3 5 に表示する。そして、媒体 C P U は、検出した表示ボタン 7 2 3 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 7 3 5 に表示する。その後、媒体 C P U は、処理をステップ S 5 0 1 に移す。

30

【 0 2 3 6 】

ステップ S 5 0 9 において、媒体 C P U は、投票ボタン 7 2 4 押下か否かを判断する。この判断が Y E S の場合、媒体 C P U は、処理をステップ S 5 1 0 に移し、N O の場合、媒体 C P U は、処理をステップ S 5 0 1 に移す。

40

【 0 2 3 7 】

ステップ S 5 1 0 において、媒体 C P U は、電子投票データ 5 2 1 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 C P U は、パスワードに基づいて G e t P o s 処理 (図 1 4 参照) へのパラメータ (p a r = C i) を算出し、算出したパラメータによって電子投票データ 5 2 1 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 C P U は、電子投票データ 5 2 1 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 C P U は、G e t P o s 処理 (図 1 4 参照、p a r = 0) によって算出された電子投票データ 5 2 1 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 C P U は、処理をステップ S 5 0 1 に移す。

50

【 0 2 3 8 】

図 2 7 は、本発明の一実施形態に係る電子投票媒体 7 0 0 を利用する場合の電子投票データ作成装置 1 0 0 の処理内容を示すフローチャートである。

【 0 2 3 9 】

ステップ S 1 5 1 において、作成 CPU は、電子投票データ 5 2 1 を作成する。作成 CPU は、図 1 2 のステップ S 1 0 1 からステップ S 1 0 8 と同様に電子投票データ 5 2 1 を作成する。その後、作成 CPU は、処理をステップ S 1 5 2 に移す。

【 0 2 4 0 】

ステップ S 1 5 2 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 7 9 0 から投票 ID を受信したか否かを判断する。この判断が Y E S の場合、作成 CPU は、処理をステップ S 1 5 3 に移し、N O の場合、作成 CPU は、処理を終了する。

10

【 0 2 4 1 】

ステップ S 1 5 3 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 Y E S の場合、作成 CPU は、処理をステップ S 1 5 4 に移し、N O の場合、作成 CPU は、処理をステップ S 1 5 6 に移す。

【 0 2 4 2 】

ステップ S 1 5 4 において、作成 CPU は、電子投票データ 5 2 1 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 S 1 5 5 に移す。

20

【 0 2 4 3 】

ステップ S 1 5 5 において、作成 CPU は、電子投票データ 5 2 1 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 7 9 0 に電子投票データ 5 2 1 を送信する。その後、作成 CPU は、処理を終了する。

【 0 2 4 4 】

ステップ S 1 5 6 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 5 2 1 を取得する。すなわち、作成 CPU は、電子投票データ 5 2 1 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 5 2 1 を取得する。その後、作成 CPU は、処理をステップ S 1 5 5 に移す。

30

【 0 2 4 5 】

図 2 8 は、本発明の一実施形態に係る電子投票媒体 7 0 0 を利用する場合の電子開票装置 3 0 0 の処理内容を示すフローチャートである。

【 0 2 4 6 】

ステップ S 3 5 1 において、開票 CPU は、電子投票データ 5 2 1 を入力する。すなわち、開票 CPU は、図 1 6 のステップ S 3 0 1 と同様に、電子投票データ 5 2 1 を入力する。その後、開票 CPU は、処理をステップ S 3 5 2 に移す。

【 0 2 4 7 】

ステップ S 3 5 2 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 7 9 0 から投票 ID を受信したか否かを判断する。この判断が Y E S の場合、開票 CPU は、処理をステップ S 3 5 3 に移し、N O の場合、開票 CPU は、処理をステップ S 3 5 5 に移す。

40

【 0 2 4 8 】

ステップ S 3 5 3 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 3 3 2 に記憶されているか否かを判断する。この判断が Y E S の場合、開票 CPU は、処理をステップ S 3 5 4 に移し、N O の場合、開票 CPU は、処理をステップ S 3 5 7 に移す。

【 0 2 4 9 】

ステップ S 3 5 4 において、開票 CPU は、電子投票データ 5 2 1 に投票 ID を対応付けて電子投票データ記憶部 3 3 2 に記憶する。その後、開票 CPU は、処理をステップ S

50

355に移す。

【0250】

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。

【0251】

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。

10

【0252】

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。

【0253】

本実施形態によれば、電子投票媒体700は、電子投票媒体700を識別するための媒体識別情報を記憶する媒体識別情報記憶部733を有している。そして、電子投票媒体700は、現在の時刻を取得し、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と、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IDを作成し、最新の投票IDを出力する。そして、電子投票媒体700は、公開鍵が所定の方法によって書き込まれた電子投票データ521と、受け付けられた候補者を示す投票内容とを入力し、投票内容に対応付けて確認コードを作成し、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。次に、電子投票媒体700は、電子投票データ521に、作成し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み、入力された電子投票データ521から公開鍵を取得し、取得された公開鍵に基づいてパスワードを暗号化して電子投票データ521に埋め込み、出力する。したがって、電子投票媒体700は、電子投票

20

30

【0254】

さらに、電子投票媒体700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し、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。したがって、電子投票媒体700は、投票後の集計が正しく行われたことを確認し、投票内容を検証することができる情報を提供することができる。

40

【0255】

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】

【0256】

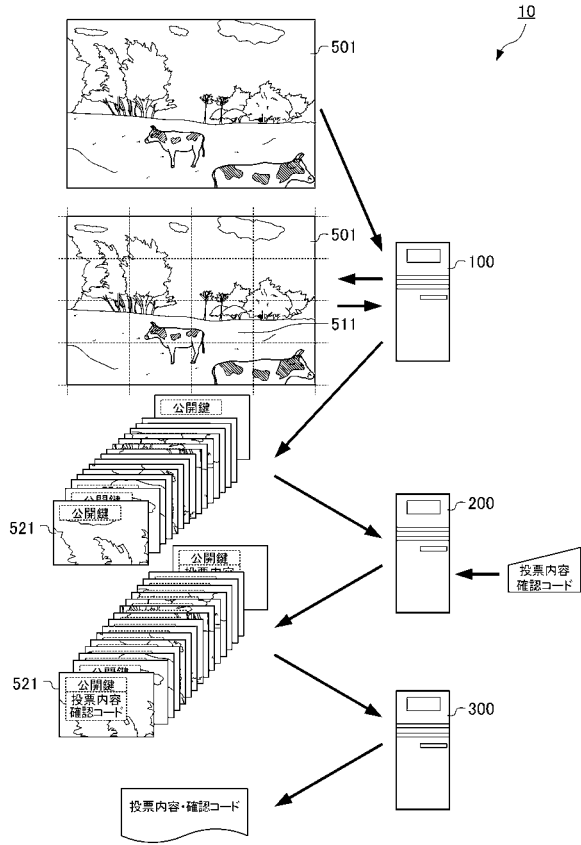
- 10 電子投票システム
- 100 電子投票データ作成装置
- 101 秘密コード受付部

50

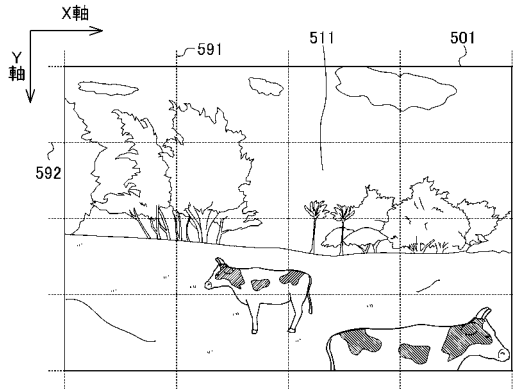
| | | |
|-------|--------------|----|
| 1 0 2 | 全体画像データ変更部 | |
| 1 0 3 | 全体画像コード算出部 | |
| 1 0 4 | 暗号秘密コード算出部 | |
| 1 0 5 | 暗号鍵作成部 | |
| 1 0 6 | 分割数設定部 | |
| 1 0 7 | 全体画像分割部 | |
| 1 0 8 | 作成領域設定部 | |
| 1 0 9 | 公開鍵位置算出部 | |
| 1 1 0 | 固有コード作成部 | |
| 1 1 1 | 固有コード位置算出部 | 10 |
| 1 1 2 | 冗長情報書込部 | |
| 1 1 3 | 電子投票データ作成部 | |
| 1 1 4 | 電子投票データ出力部 | |
| 1 3 1 | 作成パラメータ記憶部 | |
| 2 0 0 | 電子投票装置 | |
| 2 0 1 | 投票入力部 | |
| 2 0 2 | 投票領域設定部 | |
| 2 0 3 | 投票公開鍵位置算出部 | |
| 2 0 4 | 公開鍵取得部 | |
| 2 0 5 | 投票受付部 | 20 |
| 2 0 6 | パスワード受付部 | |
| 2 0 7 | 投票内容領域設定部 | |
| 2 0 8 | 投票内容位置算出部 | |
| 2 0 9 | パスワード暗号化部 | |
| 2 1 0 | パスワード位置算出部 | |
| 2 1 1 | 投票書込部 | |
| 2 1 2 | 再投票受付部 | |
| 2 1 3 | 投票出力部 | |
| 2 3 1 | 投票パラメータ記憶部 | |
| 3 0 0 | 電子開票装置 | 30 |
| 3 0 1 | 開票入力部 | |
| 3 0 2 | 開票判断部 | |
| 3 0 3 | 開票秘密コード受付部 | |
| 3 0 4 | 開票固有コード位置算出部 | |
| 3 0 5 | 固有コード取得部 | |
| 3 0 6 | 電子投票データ検索部 | |
| 3 0 7 | 電子投票データ決定部 | |
| 3 0 8 | 開票全体画像コード算出部 | |
| 3 0 9 | 開票暗号秘密コード算出部 | |
| 3 1 0 | 秘密鍵作成部 | 40 |
| 3 1 1 | 開票領域設定部 | |
| 3 1 2 | 開票パスワード位置算出部 | |
| 3 1 3 | 暗号パスワード取得部 | |
| 3 1 4 | 暗号パスワード復号部 | |
| 3 1 5 | 開票投票内容領域設定部 | |
| 3 1 6 | 開票投票位置算出部 | |
| 3 1 7 | 投票データ取得部 | |
| 3 1 8 | 開票公表部 | |
| 3 3 1 | 開票パラメータ記憶部 | |
| 3 3 2 | 電子投票データ記憶部 | 50 |

| | | |
|-------|------------|----|
| 4 0 0 | 暗号化装置 | |
| 4 0 1 | 画像読込部 | |
| 4 0 2 | 領域設定部 | |
| 4 0 3 | 擬似乱数生成部 | |
| 4 0 4 | 位置算出部 | |
| 4 0 5 | ハッシュ値算出部 | |
| 4 0 6 | 重み対応付部 | |
| 4 0 7 | 埋込部 | |
| 7 0 0 | 電子投票媒体 | |
| 7 0 1 | 時刻取得部 | 10 |
| 7 0 2 | 投票識別コード作成部 | |
| 7 0 3 | 投票識別コード出力部 | |
| 7 0 4 | 投票データ入力部 | |
| 7 0 5 | 確認コード作成部 | |
| 7 0 6 | パスワード作成部 | |
| 7 0 7 | 投票内容書込部 | |
| 7 0 8 | 公開鍵取得部 | |
| 7 0 9 | 暗号化書込部 | |
| 7 1 0 | 電子投票データ出力部 | |
| 7 1 1 | 表示部 | 20 |
| 7 2 1 | ID作成ボタン | |
| 7 2 2 | 確認コード作成ボタン | |
| 7 2 3 | 表示ボタン | |
| 7 2 4 | 投票ボタン | |
| 7 3 1 | 媒体パラメータ記憶部 | |
| 7 3 2 | 投票データ記憶部 | |
| 7 3 3 | 媒体識別情報記憶部 | |
| 7 3 4 | 接続部 | |
| 7 3 5 | 表示装置 | 30 |

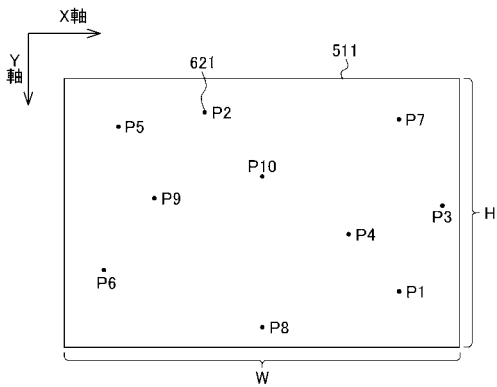
【図1】



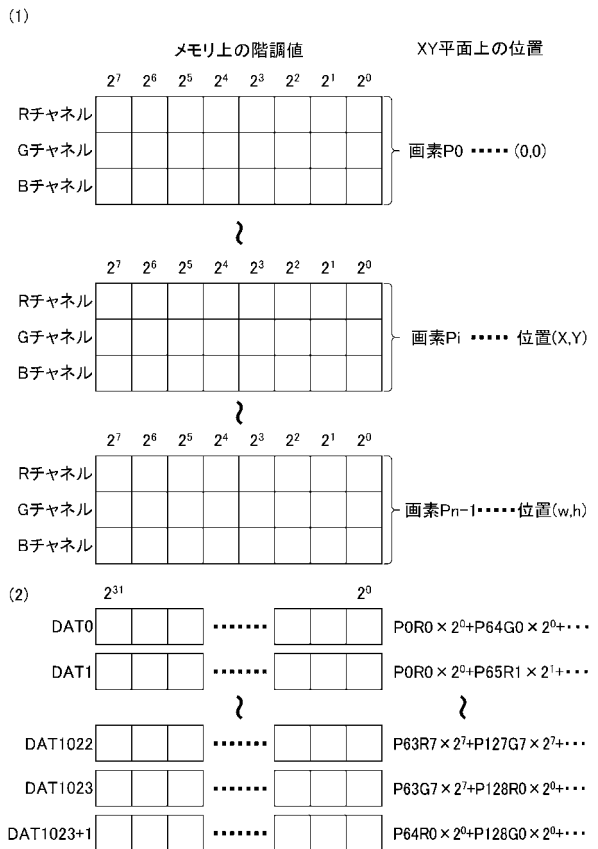
【図2】



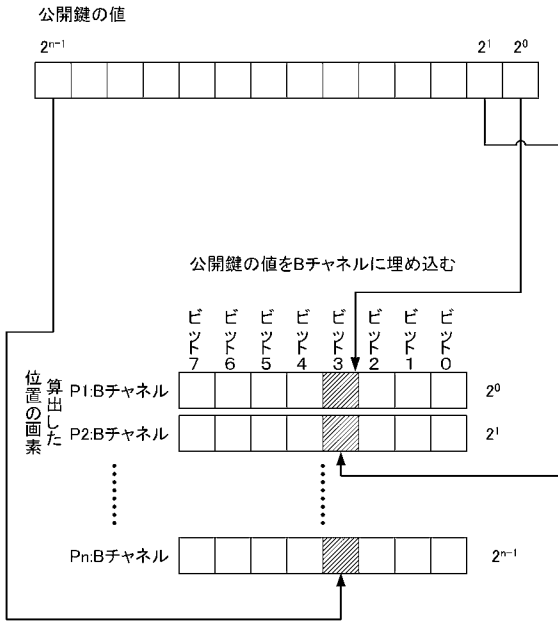
【図3】



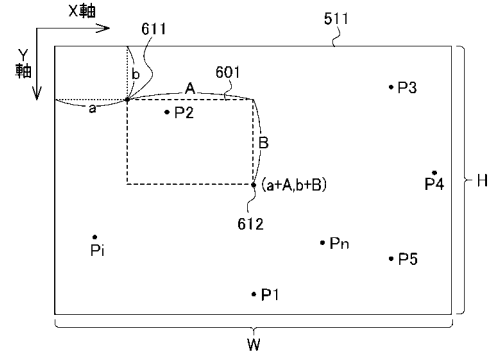
【図4】



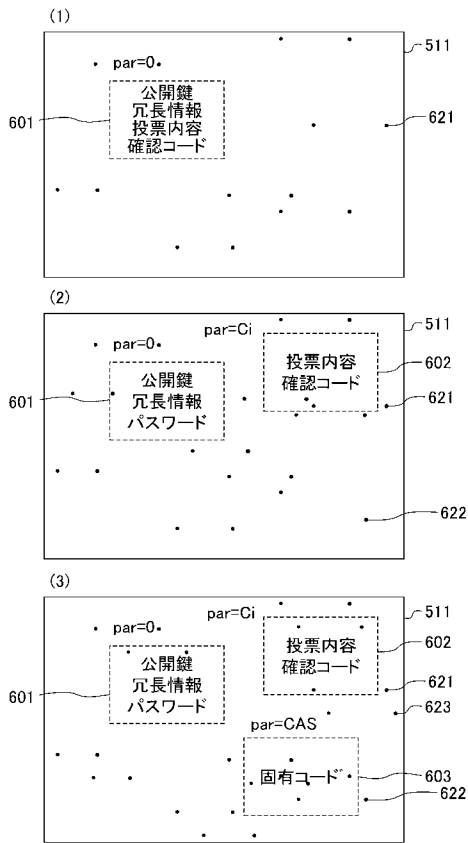
【図5】



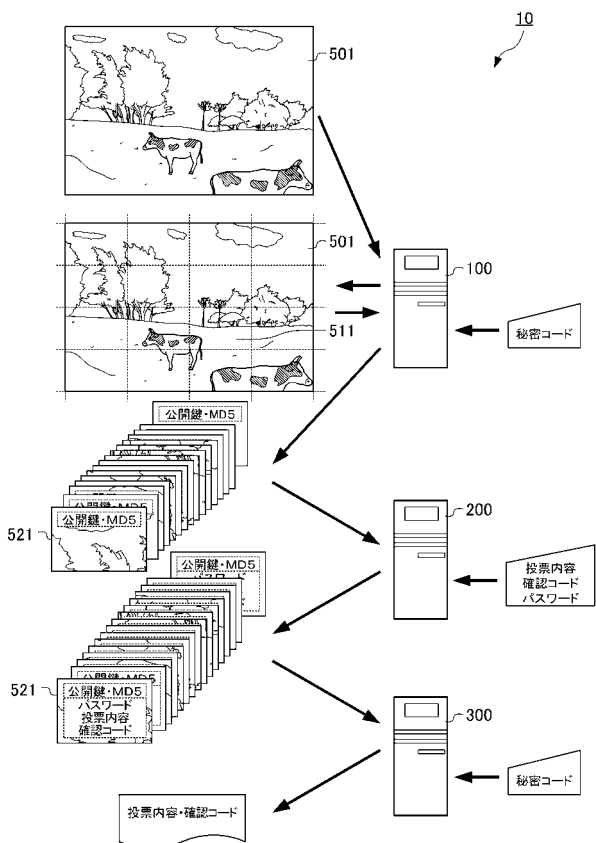
【図6】



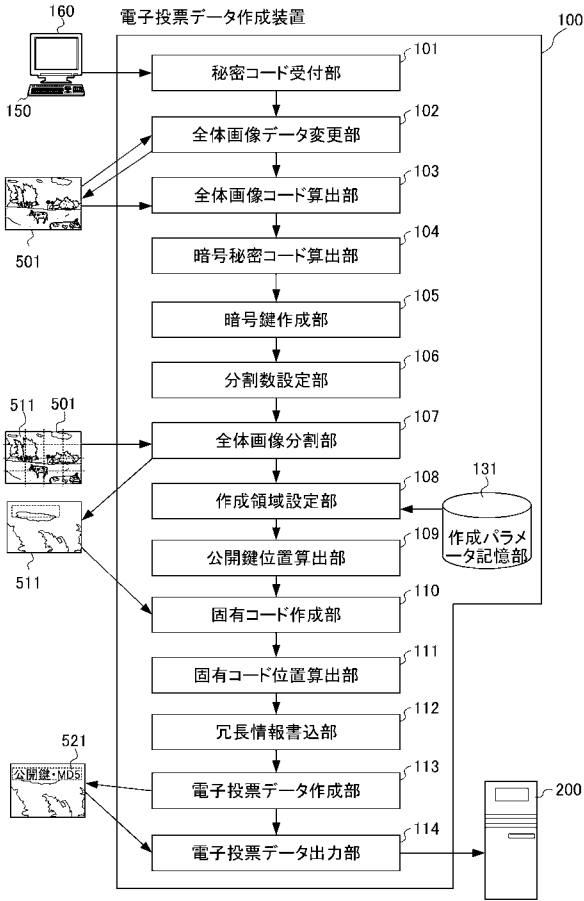
【図7】



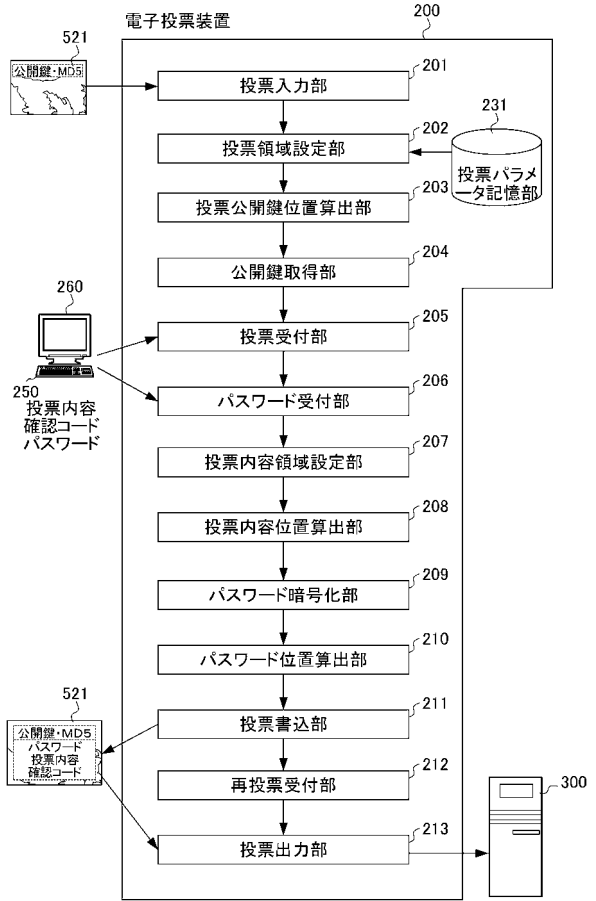
【図8】



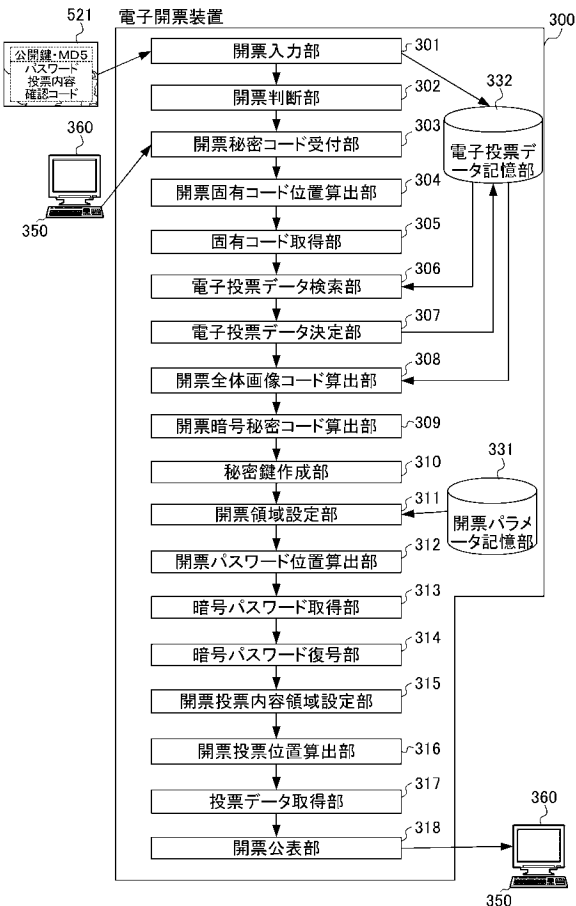
【図 9】



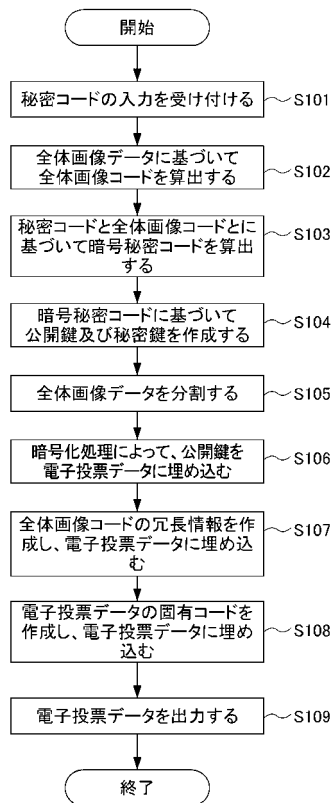
【図 10】



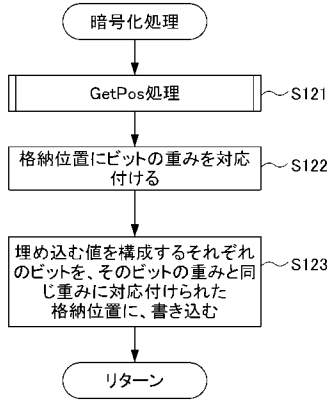
【図 11】



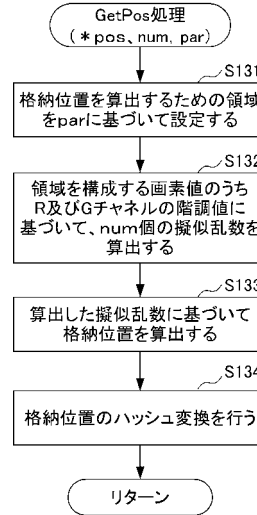
【図 12】



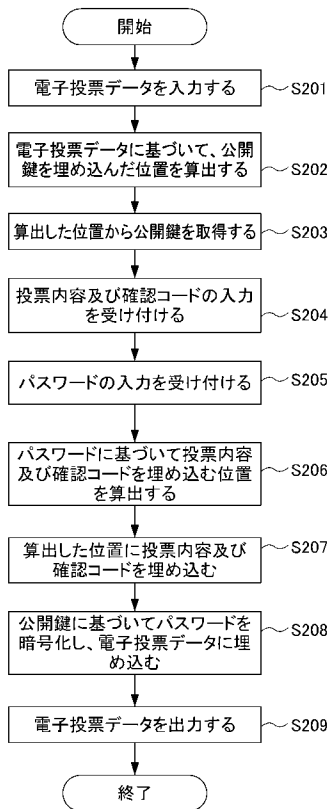
【図13】



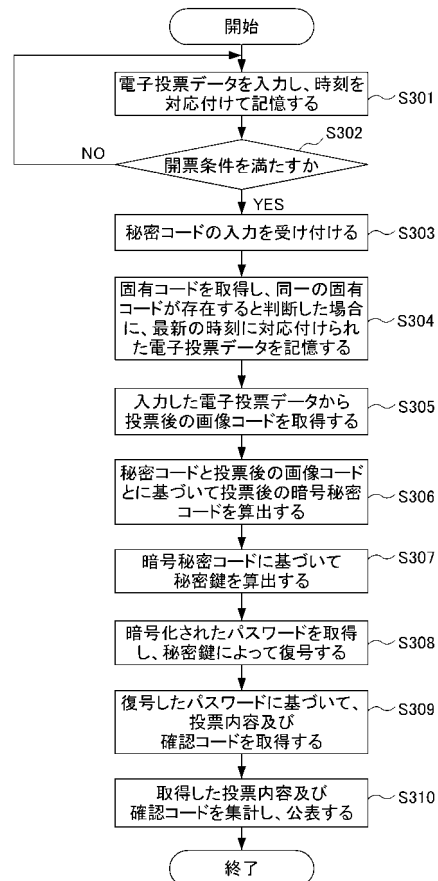
【図14】



【図15】



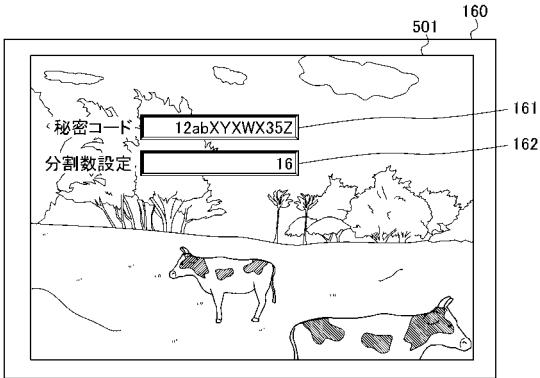
【図16】



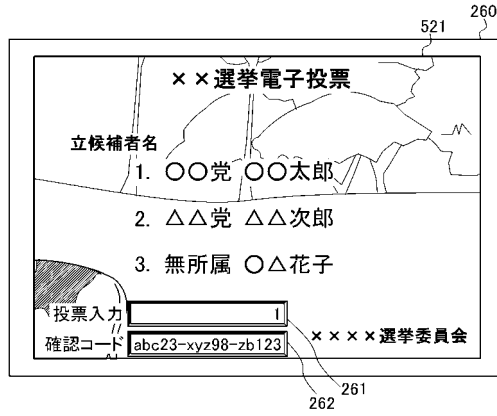
【図17】

| 番号 | 画素の位置 | | 階調値(2進) | | | ビットの重み |
|-------|-------|-----|----------|----------|----------|--------|
| | X | Y | R値 | G値 | B値 | |
| 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 |

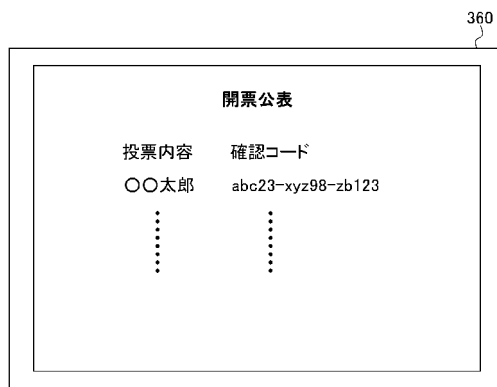
【図18】



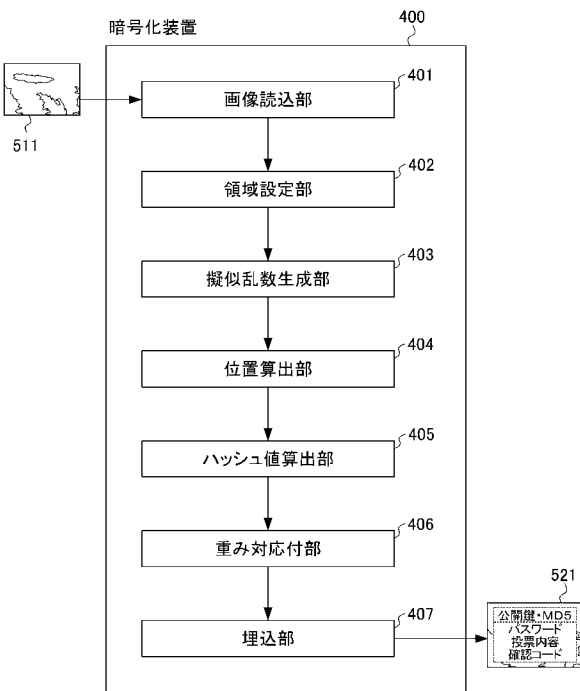
【図19】



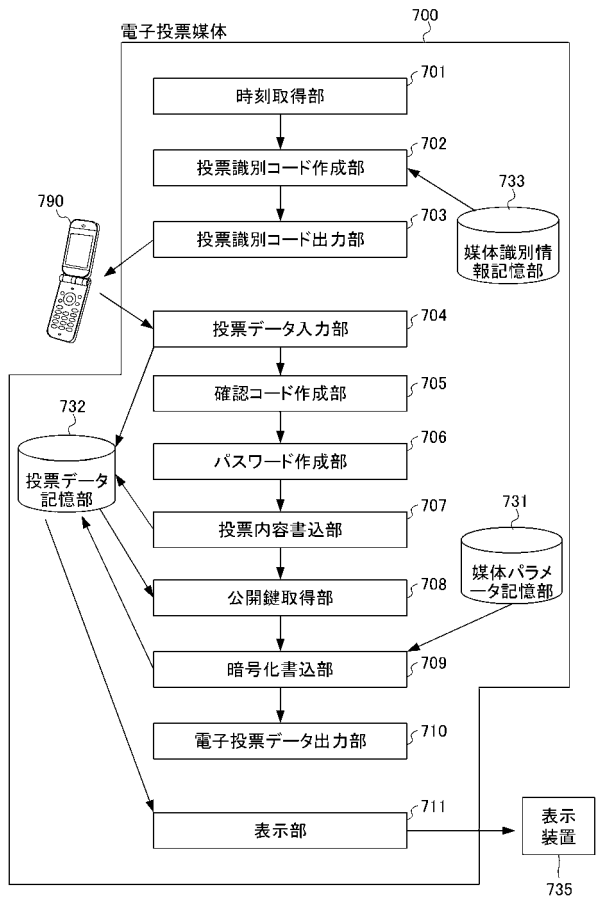
【図20】



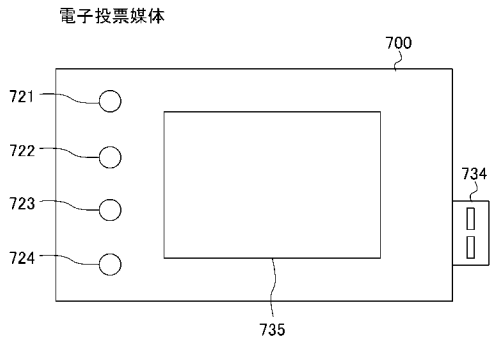
【図21】



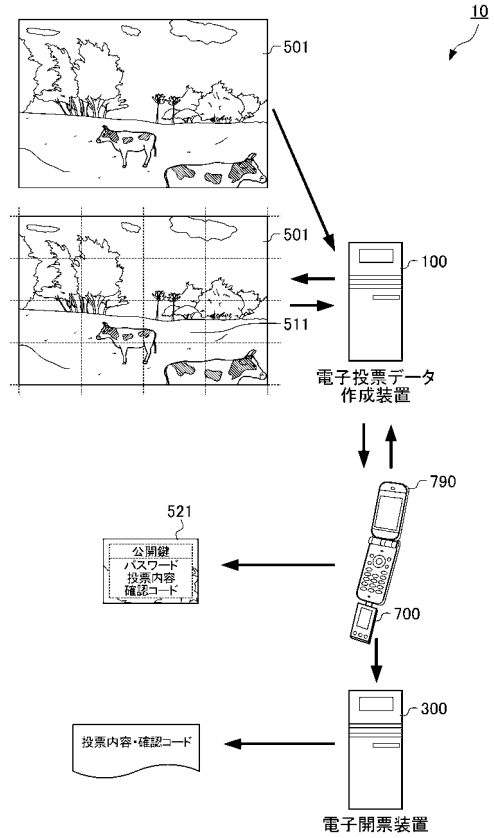
【図22】



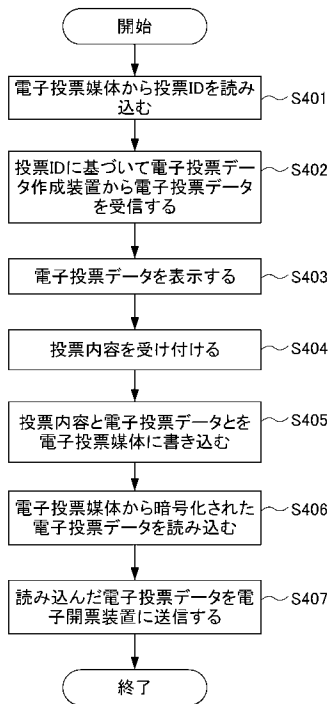
【図 2 3】



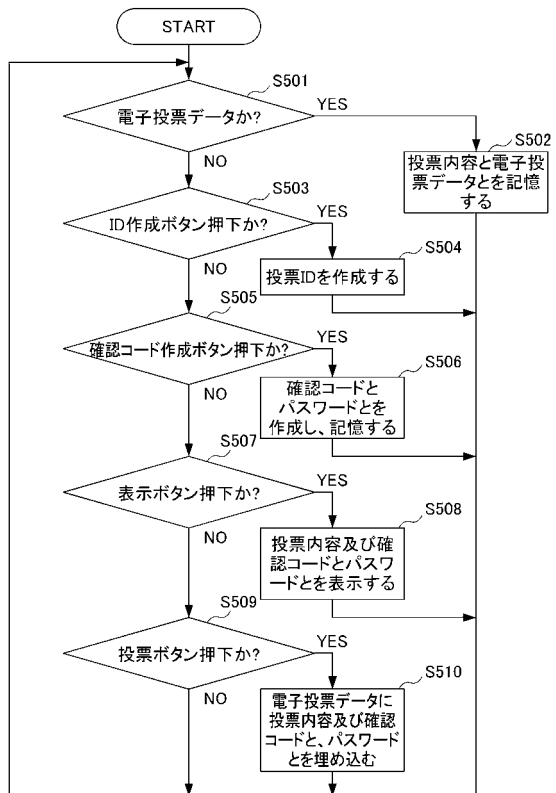
【図 2 4】



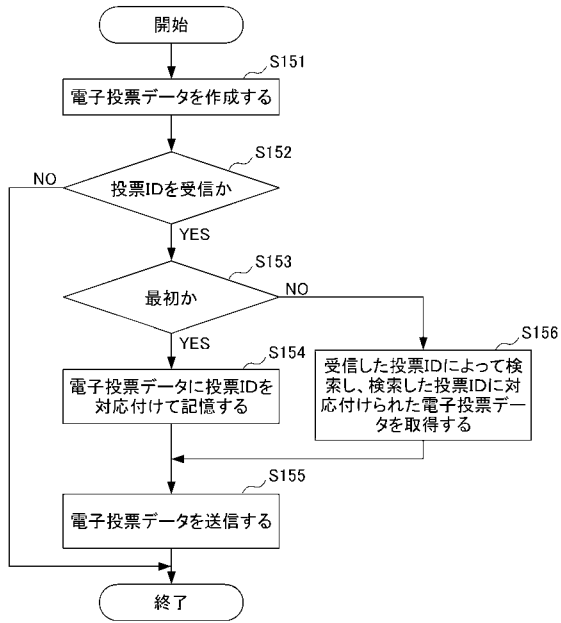
【図 2 5】



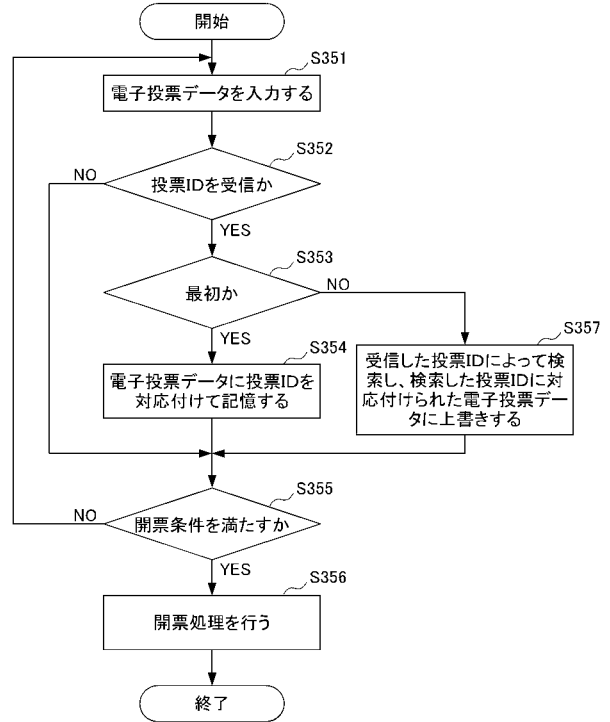
【図 2 6】



【図 27】



【図 28】



フロントページの続き

- (56)参考文献 特開2005-70892(JP,A)
特開2007-183707(JP,A)
特開2008-250810(JP,A)
特開2006-139620(JP,A)

- (58)調査した分野(Int.Cl., DB名)
G06Q 30/08
H04L 9/08