

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年12月24日(24.12.2020)



(10) 国際公開番号

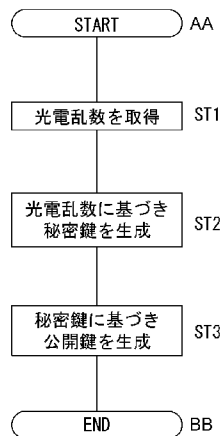
WO 2020/255793 A1

- (51) 国際特許分類:
G09C 1/00 (2006.01) *G06F 7/58* (2006.01)
H04L 9/32 (2006.01)
- (21) 国際出願番号: PCT/JP2020/022668
- (22) 国際出願日: 2020年6月9日(09.06.2020)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2019-113731 2019年6月19日(19.06.2019) JP
- (71) 出願人: ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1080075 東京都港区港南1丁目7番1号 Tokyo (JP).
- (72) 発明者: 高塚 進 (TAKATSUKA, Susumu); 〒1080075 東京都港区港南1丁目7番1号 ソニー株式会社内 Tokyo (JP). 河本 献太 (KAWAMOTO, Kenta); 〒1080075 東京都港区港南1丁目7番1号 ソニー株式会社内 Tokyo (JP). 鉄川 弘樹 (TETSUKAWA Hiroki); 〒1080075 東京都港区港南1丁目7番1号 ソニー株式会社内 Tokyo (JP).
- (74) 代理人: 岩田 雅信, 外 (IWATA, Masanobu et al.); 〒1010032 東京都千代田区岩本町1丁目3番9号 ハクセイビル8階 テクノピア国際特許事務所 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ,

(54) Title: CRYPTOGRAPHY KEY GENERATION DEVICE AND CRYPTOGRAPHY KEY GENERATION METHOD

(54) 発明の名称: 暗号鍵生成装置、暗号鍵生成方法

[図13]



ST1 Acquire photoelectric random number
ST2 Generate private key on basis of photoelectric random number
ST3 Generate public key on basis of private key
AA START
BB END

(57) Abstract: The present invention makes it difficult to decrypt a private key for an electronic signature, and achieves an improvement in tampering detection performance. A cryptography key generation device according to the present technology comprises a key generation unit that generates a private key for an electronic signature, on the basis of a photoelectric random number that is a random number obtained on the basis of photoelectric conversion by an array sensor in which a plurality of pixels having visible or invisible light receiving elements are arranged one-dimensionally

BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 一 国際調査報告(条約第21条(3))

or two-dimensionally.

(57) 要約: 電子署名用の秘密鍵について解読を困難化し、改竄検知性能の向上を図る。本技術に係る暗号鍵生成装置は、可視光又は非可視光の受光素子を有する画素が一次元又は二次元に複数配列されたアレイセンサによる光電変換に基づき得られる乱数である光電乱数に基づき、電子署名用の秘密鍵を生成する鍵生成部を備える。

明 細 書

発明の名称： 暗号鍵生成装置、暗号鍵生成方法

技術分野

[0001] 本技術は暗号鍵生成装置及び暗号鍵生成方法に関し、特に、電子署名用の暗号鍵生成についての技術分野に関する。

背景技術

[0002] データの改竄検知のために電子署名の手法が広く用いられている。電子署名の手法では、データの送信者がハッシュ値の暗号化に用いる秘密鍵と公開鍵を生成する。送信者は、改竄検知の対象データと、秘密鍵により暗号化した該対象データのハッシュ値と、公開鍵とを受信者に送信する。受信者は、受信した対象データのハッシュ値を計算すると共に、受信した公開鍵により秘密鍵で暗号化されたハッシュ値を復号化し、それらハッシュ値が一致するか否かによりデータの改竄有無を判定することができる。

[0003] なお、関連する従来技術として、下記特許文献1には、撮像画像データについての改竄検知を電子署名情報に基づき行う技術が開示されている。

先行技術文献

特許文献

[0004] 特許文献1：特開2017-184198号公報

発明の概要

発明が解決しようとする課題

[0005] しかしながら、従来の電子署名の手法では、ハッシュ値の暗号化に用いる秘密鍵がソフトウェアで生成した疑似乱数を元に生成されており、該秘密鍵が解読されて複製されるリスクがあった。秘密鍵が複製されると、改竄データを受信者に改竄が無いものと誤判定させることが可能となってしまう。すなわち、電子署名用の秘密鍵について解読のリスクが高まることは、改竄検知性能の低下を招くものとなる。

[0006] 本技術は上記事情に鑑み為されたものであり、電子署名用の秘密鍵につい

て解読を困難化し、改竄検知性能の向上を図ることを目的とする。

課題を解決するための手段

[0007] 本技術に係る暗号鍵生成装置は、可視光又は非可視光の受光素子を有する画素が一次元又は二次元に複数配列されたアレイセンサによる光電変換に基づき得られる乱数である光電乱数に基づき、電子署名用の秘密鍵を生成する鍵生成部を備えたものである。

これにより、電子署名用の秘密鍵について、疑似乱数を用いる場合よりも解読を困難化することが可能とされる。

[0008] 上記した本技術に係る暗号鍵生成装置においては、前記鍵生成部は、画像データについての電子署名用の秘密鍵を生成する構成とすることが考えられる。

これにより、電子署名の対象データが画像データとされる場合に対応して、電子署名用の秘密鍵について、疑似乱数を用いる場合よりも解読を困難化することが可能とされる。

[0009] 上記した本技術に係る暗号鍵生成装置においては、前記鍵生成部は、前記アレイセンサでの撮像により得られる画像データについての電子署名用の秘密鍵を生成する構成とすることが考えられる。

これにより、画像データを得るためのアレイセンサが、光電乱数を得るためのアレイセンサと共通化される。

[0010] 上記した本技術に係る暗号鍵生成装置においては、前記アレイセンサでの撮像により得られる画像データの暗号化を行う暗号化部と、前記暗号化部により暗号化された前記画像データを外部装置に送信する処理を行う送信処理部を備えた構成とすることが考えられる。

これにより、電子署名の対象データとしての画像データをセキュアに送信することが可能とされる。

[0011] 上記した本技術に係る暗号鍵生成装置においては、前記暗号化部は、前記光電乱数に基づき生成した暗号鍵により前記画像データの暗号化を行う構成とすることが考えられる。

これにより、画像データの暗号化についても、疑似乱数を用いる場合より暗号鍵の解読を困難化することが可能とされる。

[0012] 上記した本技術に係る暗号鍵生成装置においては、前記暗号化部は、前記画像データの復号に用いる復号鍵のレベルによって復号化可能な画像範囲が異なるように前記画像データを暗号化し、前記送信処理部は、前記外部装置が前記暗号化部により暗号化された前記画像データの送信要求を行ったことに応じて、該外部装置が有する前記復号鍵と同レベルの復号鍵により前記暗号化された前記画像データを復号化し、復号化した画像データのハッシュ値を生成し、前記秘密鍵により暗号化した該ハッシュ値と前記暗号化された前記画像データとを前記外部装置に送信する構成とすることが考えられる。

これにより、画像データの受信装置に対して該受信装置が有する復号鍵のレベルに応じたハッシュ値を送信すべき場合において、ハッシュ値の生成は、送信要求が行われた際に、該送信要求を行った受信装置の復号鍵のレベルについてのみに行えば済み、画像データ（撮像画像データ）の記録時に各レベルのハッシュ値を一度に生成する必要がなくなる。

[0013] 上記した本技術に係る暗号鍵生成装置においては、前記鍵生成部は、前記光電乱数に基づき、ブロックチェーンシステムにおける電子署名用の秘密鍵を生成する構成とすることが考えられる。

これにより、ブロックチェーンシステムにおける電子署名用の秘密鍵について、疑似乱数を用いる場合より解読を困難化することが可能とされる。

[0014] 上記した本技術に係る暗号鍵生成装置においては、前記光電乱数に基づき、スマートコントラクトシステムにおけるコントラクト検証作業者の選出を行う検証者選出部を備える構成とすることが考えられる。

これにより、コントラクト検証作業者の選出に用いる乱数について、疑似乱数を用いる場合より解読を困難化することが可能とされる。

[0015] 上記した本技術に係る暗号鍵生成装置においては、前記光電乱数に基づき、DAppsによるサービスの享受者からの代表者の選出を行う代表者選出部を備える構成とすることが考えられる。

これにより、D A p p s のサービス享受者からの代表者選出に用いる乱数について、疑似乱数を用いる場合より解読を困難化することが可能とされる。

[0016] 上記した本技術に係る暗号鍵生成装置においては、前記鍵生成部は、前記光電変換により得られる前記画素ごとの電気信号の値を前記光電乱数として取得して前記秘密鍵を生成する構成とすることが考えられる。

これにより、解読が困難な電子署名秘密鍵を生成することが可能とされる。

[0017] 上記した本技術に係る暗号鍵生成装置においては、前記鍵生成部は、前記画素ごとの電気信号の値のうち少なくとも一部を、該電気信号の値が得られた画素位置とは異なる画素位置に割り当てた形式による前記光電乱数に基づき、前記秘密鍵を生成する構成とすることが考えられる。

これにより、画素ごとの電気信号の値をそれら電気信号の値が得られた画素位置にそのまま割り当てた光電乱数を用いる場合と比較して、電子署名秘密鍵の解読が困難とされる。

[0018] 上記した本技術に係る暗号鍵生成装置においては、前記光電乱数の生成後、前記光電乱数の元となった画像データをメモリ上から消去するための処理を行う消去処理部を備えた構成とすることが考えられる。

これにより、光電乱数の元となった画像が流出して光電乱数が推定されてしまうことの防止を図ることが可能とされる。

[0019] 上記した本技術に係る暗号鍵生成装置においては、暗号鍵生成装置外部からの不正アクセスが検知されたことに応じて前記光電乱数を再生成するための処理を行う再生成処理部を備えた構成とすることが考えられる。

これにより、外部からの不正アクセスが検知された場合は、再生成した光電乱数に基づき電子署名秘密鍵を更新することが可能とされる。

[0020] 本技術に係る暗号鍵生成方法は、情報処理装置が、可視光又は非可視光の受光素子を有する画素が一次元又は二次元に複数配列されたアレイセンサによる光電変換に基づき得られる乱数である光電乱数に基づき、電子署名用の

秘密鍵を生成する暗号鍵生成方法である。

[0021] このような暗号鍵生成方法によっても、上記した本技術に係る暗号鍵生成装置と同様の作用が得られる。

図面の簡単な説明

[0022] [図1]第一実施形態としての電子署名システムの概略構成例を示したブロック図である。

[図2]第一実施形態としての暗号鍵生成装置（撮像装置）の内部構成例を示したブロック図である。

[図3]第一実施形態における受信装置の内部構成例を示したブロック図である。

[図4]光電乱数に基づき暗号化フィルタ（暗号鍵）を生成する手法の例を示した図である。

[図5]実施形態における振幅制御回路による読み出し信号の暗号化のイメージを示した図である。

[図6]デジタル信号による読み出し信号に対して暗号化を施す場合の撮像装置の構成例を示した図である。

[図7]実施形態としての撮像用センサ部の構造例を示した図である。

[図8]実施形態としての撮像用センサ部の構造の別例を示した図である。

[図9]実施形態としての撮像用センサ部の構造のさらに別例を示した図である。

[図10]第一実施形態としての画像暗号化を実現するために実行すべき処理の手順を示したフローチャートである。

[図11]受信装置に画像復号化のための復号鍵をセキュアに受け渡すための手法の例を説明するための図である。

[図12]電子署名を用いた電子文書の改竄検知手法を説明するための模式図である。

[図13]第一実施形態としての電子署名用暗号鍵の生成処理の例を示したフローチャートである。

[図14]第一実施形態における改竄検知のための処理手順の例を示したフローチャートである。

[図15]ターゲットのクラスが人物である場合における段階的な画像暗号化のイメージを示した図である。

[図16]ターゲットのクラスが車両である場合における段階的な画像暗号化のイメージを示した図である。

[図17]段階的な画像暗号化の具体的手法の例を説明するための図である。

[図18]秘匿レベルの変化例についての説明図である。

[図19]第二実施形態としての画像暗号化の具体的な手法の例を説明するための図である。

[図20]第二実施形態におけるROIの変形例について説明するための図である。

[図21]第二実施形態におけるシードフレームの撮像から暗号鍵の元となる乱数の保存までに対応した処理を示しフローチャートである。

[図22]第二実施形態において生成した暗号鍵に基づき対象画像を暗号化するための処理を示したフローチャートである。

[図23]第二実施形態としての改竄検知手法について説明するための図である。

[図24]同じく、第二実施形態としての改竄検知手法について説明するための図である。

[図25]第二実施形態としての改竄検知手法を実現するための処理手順の例を示したフローチャートである。

[図26]各レベルの受信装置が自身の公開鍵を撮像装置に保有させることの説明図である。

[図27]受信者側が有する公開鍵の確認プロセスの例を説明するための図である。

[図28]同じく、受信者側が有する公開鍵の確認プロセスの例を説明するための図である。

[図29]送信者側が有する電子署名公開鍵の確認プロセスの例を説明するための図である。

[図30]同じく、送信者側が有する電子署名公開鍵の確認プロセスの例を説明するための図である。

[図31]ブロックチェーンシステムのハードウェア構成を例示したブロック図である。

[図32]ブロックチェーンシステムを構成するユーザ端末の内部構成例を示したブロック図である。

[図33]スマートコントラクトシステムの構成を概念的に表した図である。

発明を実施するための形態

[0023] 以下、実施の形態を次の順序で説明する。

< 1. 第一実施形態 >

[1-1. 電子署名システムの構成]

[1-2. 撮像装置の構成]

[1-3. 受信装置の構成]

[1-4. 暗号化に用いる乱数について]

[1-5. 暗号化対象とする信号について]

[1-6. 耐タンパー化について]

[1-7. 画像暗号化のための処理手順]

[1-8. 画像復号化のための鍵の受け渡しについて]

[1-9. 第一実施形態としての改竄検知手法]

< 2. 第二実施形態 >

[2-1. 第二実施形態の画像暗号化手法]

[2-2. 画像暗号化のための処理手順]

[2-3. 第二実施形態としての改竄検知手法]

[2-4. 受信者側が有する公開鍵の確認プロセス]

[2-5. 送信者側が有する電子署名公開鍵の確認プロセス]

< 3. 第三実施形態 >

<4. 変形例>

<5. 実施形態のまとめ>

<6. 本技術>

[0024] <1. 第一実施形態>

[1-1. 電子署名システムの構成]

図1は、第一実施形態における電子署名システムの概略構成例を示したブロック図である。

図示のように電子署名システムは、撮像装置1、ネットワーク2、及び複数の受信装置3を備えている。

撮像装置1は、本技術に係る暗号鍵生成装置の一実施形態であり、イメージセンサによる撮像を行ってデジタルデータとしての画像データ（撮像画像データ）を得る。本実施形態では、電子署名の対象データは、この撮像装置1による撮像画像データとされる。

[0025] 各受信装置3は、電子署名の対象データ、つまり本例では撮像装置1による撮像画像データを受信する装置とされ、例えばインターネットとされたネットワーク2を介して撮像装置1とデータ通信を行うことが可能に構成されている。

[0026] 後述もするように撮像装置1は、受信装置3に対し撮像画像データを送信するにあたり、電子署名用の秘密鍵、及び該秘密鍵に基づく公開鍵を生成すると共に、送信対象の撮像画像データについてのハッシュ値を計算し、該ハッシュ値を秘密鍵により暗号化する。そして、撮像装置1は、該暗号化したハッシュ値と、送信対象の撮像画像データと、公開鍵とを受信装置3に送信する。

受信装置3は、撮像装置1から送信されるこれらのデータに基づいて、受信した撮像画像データについての改竄検知処理を行う。

なお、本実施形態における改竄検知のための処理については後に改めて説明する。

[0027] 本実施形態において、撮像装置1が撮像画像データを受信装置3に送信す

る際には、秘匿性を高めるため、該撮像画像データを暗号化する。以降で説明するように、本実施形態の撮像装置 1 は、このように撮像画像データを暗号化するための各種処理を実行する。

[0028] [1-2. 撮像装置の構成]

図 2 は、撮像装置 1 の内部構成例を示したブロック図である。

撮像装置 1 は、撮像用センサ部 10、画像プロセッサ 21、センサ部 22、制御部 23、メモリ部 24、及び通信部 25 を備えている。

[0029] 撮像用センサ部 10 は、撮像装置 1 に設けられた不図示のカメラ光学系を介して入射する光を画素ごとに受光し、光電変換を行って撮像画像データを得る。

ここでの図示は省略するが、撮像用センサ部 10 は、ハードウェアとしては、イメージセンサデバイス、DRAM (Dynamic Random Access Memory) 等のメモリデバイス、AI (artificial intelligence) 機能プロセッサとしての構成部位を有している。そして、これら三つが 3 レイヤ積層構造とされたり、1 レイヤでいわゆる平置き構成とされたり、或いは 2 レイヤ（例えばメモリデバイスと AI 機能プロセッサが同一レイヤ）積層構造とされたりするなどして一体型のデバイスとされている。

本例の撮像用センサ部 10 は、画像解析による物体検出機能を備えるものとし、インテリジェントアレイセンサと呼ぶことのできる装置とされる。

[0030] 図示のように撮像用センサ部 10 は、アレイセンサ 12、振幅制御回路 19、ADC (Analog to Digital Converter) / ピクセルセクタ 13、バッファ 14、ロジック部 15、メモリ 16、インタフェース部 17、及び演算部 18 を有している。

[0031] アレイセンサ 12 は、可視光又は非可視光の受光素子を有する画素が 1 次元又は 2 次元に複数配列されて構成されている。例えば、行方向及び列方向の 2 次元に多数の画素が配列され、各画素の受光素子における光電変換により二次元画像信号を出力する構成とされる。

[0032] 振幅制御回路 19 は、アレイセンサ 12 によって光電変換された電気信号

（アナログ信号）の振幅制御を行う。本例では、振幅制御回路 19 は、演算部 18 からの指示に基づき増幅率を変更可能に構成されているが、この点については後に改めて説明する。

[0033] ADC／ピクセルセクタ 13 には、アレイセンサ 12 によって光電変換された電気信号が振幅制御回路 19 を介して入力される。ADC／ピクセルセクタ 13 は、入力したアナログ信号としての電気信号をデジタルデータ化し、デジタルデータとしての画像信号（画像データ）を出力する。

また、ADC／ピクセルセクタ 13 は、アレイセンサ 12 の画素（受光素子）に対するピクセル選択の機能を持つ。これにより、アレイセンサ 12 における選択した画素のみについて、光電変換信号を取得してデジタルデータ化して出力することが可能とされている。つまり ADC／ピクセルセクタ 13 は、通常は 1 フレームの画像を構成する有効な画素の全てについて光電変換信号のデジタルデータ化出力を行うが、選択した画素のみについての光電変換信号のデジタルデータ化出力を行うことも可能とされている。

[0034] ADC／ピクセルセクタ 13 によって、フレーム単位で画像データが取得されるが、この各フレームの画像データはバッファ 14 に一時記憶され、適切なタイミングで読み出されてロジック部 15 の処理に供される。

[0035] ロジック部 15 では、入力される各フレーム画像信号に対して各種必要な信号処理（画像処理）を行う。

例えばロジック部 15 では、色補正、ガンマ補正、色階調処理、ゲイン処理、輪郭強調処理等の処理により画質調整を行うことが想定される。またロジック部 15 ではデータ圧縮処理、解像度変換、フレームレート変換など、データサイズを変更する処理を行うことも想定される。

これらロジック部 15 で行われる各処理については、それぞれの処理に用いるパラメータが設定される。例えば色や輝度の補正係数、ゲイン値、圧縮率、フレームレートなどの設定値がある。ロジック部 15 では、それぞれの処理について設定されたパラメータを用いて必要な処理を行う。本実施形態では、これらのパラメータを演算部 18 が設定する場合がある。

[0036] ロジック部 15 で処理された画像データは例えば D R A M 等で構成されたメモリ 16 に記憶される。

メモリ 16 に記憶された画像データは、必要なタイミングでインタフェース部 17 により画像プロセッサ 21 等に送信出力される。

[0037] 画像プロセッサ 21 では、撮像用センサ部 10 から送信されてきた画像データについて、画像解析、画像認識処理を行って、必要な物体検出等を実行する。

画像プロセッサ 21 は、センサ部 22 の検出情報を参照することもできる。

[0038] また、撮像用センサ部 10 において、演算部 18 は、例えば一つの A I プロセッサとして構成される。そして、実行可能な演算機能として図示のようにキーフレーム選択部 81、物体領域認識部 82、クラス識別部 83、パラメータ選択部 84、暗号化制御部 85、及び不正アクセス検知部 86 を備える。なおこれらの演算機能が複数のプロセッサにより構成されてもよい。

[0039] キーフレーム選択部 81 は、所定のアルゴリズム又は指示に応じて、動画としての画像データのフレームの内からキーフレームを選択する処理を行う。

[0040] 物体領域認識部 82 は、アレイセンサ 12 で光電変換され、A D C / ピクセルセレクタ 13 によって取得される画像データのフレームに対して、検出の候補となる物体の領域の検出や、検出対象の物体について画像（フレーム）内での当該物体を囲う領域（バウンディングボックス）の認識処理を行う。

画像信号から検出される物体とは、画像からの認識を目的として検出対象となり得る物体のことをいう。撮像用センサ部 10 や画像プロセッサ 21 の検出の目的、処理能力、アプリケーション種別などに応じて、どのような物体が検出対象とされるかは異なるが、あらゆる物体が、ここでいう検出対象の物体とされる可能性がある。あくまで一部であるが例示すると、動物、移動体（自動車、自転車、航空機等）、自然物（野菜、植物等）、工業製品／

部品、建造物、施設、山、海、川、星、太陽、雲など、あらゆる物体が該当する可能性がある。

また、本例における物体領域認識部 8 2 は、バウンディングボックスに基づいて、処理の対象とすべき領域（関心領域）を示す領域情報である R O I（Region of Interest）を算出する処理を実行する。

[0041] クラス識別部 8 3 は、物体領域認識部 8 2 が検出した物体についてクラス分類を行う。

クラスとは、物体のカテゴリを表す情報であり、例えば「人」「自動車」「飛行機」「船」「トラック」「鳥」「猫」「犬」「鹿」「蛙」「馬」などのように、検出すべき物体をクラス分けしたものである。

[0042] パラメータ選択部 8 4 は、各クラスに応じた信号処理用のパラメータを記憶しており、クラス識別部 8 3 が識別した検出物体のクラスやバウンディングボックス等を用いて、対応する 1 又は複数のパラメータを選択する。そしてその 1 又は複数のパラメータをロジック部 1 5 に設定する。

[0043] ここで、上記した演算部 1 8 による各種機能の処理は、通常イメージセンサ内では行わなかった処理であり、本実施形態では、物体検出やクラス認識、及びこれらに基づく制御をイメージセンサ内で実行する。これにより、画像プロセッサ 2 1 へ供給する画像データを、検出目的に沿った適切なものとしたり、検出性能の低下を招かないようにデータ量を適切に削減したりするといったことが可能とされる。

[0044] 暗号化制御部 8 5 は、アレイセンサ 1 2 での撮像により得られる画像信号について暗号化が行われるように制御する。なお、このような画像信号の暗号化のために暗号化制御部 8 5 が行う処理の具体例については改めて説明する。

[0045] 不正アクセス検知部 8 6 は、撮像装置 1 外部からの不正アクセスを検知する。具体的に、本例における不正アクセス検知部 8 6 は、メモリ 1 6 に保存されたデータに対する外部からの不正アクセスを検知する。

不正アクセス検知部 8 6 は、不正アクセスを検知した場合には、そのログ

情報（例えば検知日時や不正アクセスの種別を表す情報等）をメモリ 16 の所定領域に記録する。

[0046] 制御部 23 は、例えば CPU (Central Processing Unit)、ROM (Read Only Memory)、及び RAM (Random Access Memory) を備えたマイクロコンピュータを有して構成され、CPU が ROM に記憶されているプログラム、又は RAM (Random Access Memory) にロードされたプログラムに従って各種の処理を実行することで、撮像装置 1 の全体制御を行う。

例えば、制御部 23 は、撮像用センサ部 10 に対する指示を行って撮像画像データの取得処理等の各種処理の実行制御を行う。同様に、画像プロセッサ 21 についても各種処理の実行制御を行う。

また、制御部 23 は、メモリ部 24 に対する各種データの書き込みや読み出しについての制御を行う。メモリ部 24 は、例えば HDD (Hard Disk Drive) やフラッシュメモリ装置等の不揮発性の記憶デバイスとされ、例えば撮像用センサ部 10 により得られた撮像画像データ等の各種のデータの保存先（記録先）として用いられる。

さらに、制御部 23 は、通信部 25 を介して外部装置との間で各種データ通信を行う。通信部 25 は、図 1 に示したネットワーク 2 を介した外部装置との間でのデータ通信を行うことが可能に構成されている。

制御部 23 は、図 1 に示した受信装置 3 からの求めに応じ、例えば撮像用センサ部 10 で得られメモリ部 24 に保存された撮像画像データ等の各種データを通信部 25 経由で該受信装置 3 に送信することが可能とされる。

[0047] ここで、制御部 23 は、電子署名に係る各種の処理を実行するが、該処理については後に改めて説明する。

[0048] [1-3. 受信装置の構成]

図 3 は、受信装置 3 の内部構成例を示したブロック図である。

図示のように受信装置 3 は、CPU 31、ROM 32、RAM 33、バス 34、入出力インタフェース 35、入力部 36、出力部 37、記憶部 38、通信部 39 を備えている。

CPU 31、ROM 32、及びRAM 33は、バス34を介して相互に接続されている。このバス34には、入出力インタフェース35も接続されている。CPU 31は、ROM 32に記憶されているプログラム、又は記憶部38からRAM 33にロードされたプログラムに従って各種の処理を実行する。RAM 33にはまた、CPU 31が各種の処理を実行する上において必要なデータ等も適宜記憶される。

[0049] 入出力インタフェース35には、入力部36、出力部37、記憶部38、及び通信部39が接続されている。

入力部36は、ユーザからの操作入力情報を検出する例えばキーボード、マウス、タッチパネル等の操作入力検出デバイスを包括的に表している。

出力部37は、例えばLCD (Liquid Crystal Display)、有機EL (Electroluminescence) パネル等よりなるディスプレイ、並びにスピーカ等により構成される。

記憶部38はHDD (Hard Disk Drive) やフラッシュメモリ装置等により構成される。

通信部39は、ネットワーク2を介しての通信処理や機器間通信を行う。

[0050] 受信装置3において、CPU 31は、撮像装置1より送信された暗号化状態の撮像画像データの復号化や、電子署名データに基づく撮像画像データについての改竄検知処理等を行うが、これらの処理の具体例については後に改めて説明する。

[0051] [1-4. 暗号化に用いる乱数について]

ここで、本実施形態の撮像装置1では、電子署名の対象データである撮像画像データについて暗号化を施すものとするが、本例では、このような撮像画像データの暗号化に光電乱数を用いる。すなわち、撮像画像データの暗号化に用いる暗号鍵を光電乱数に基づき生成するものである。

ここで、光電乱数とは、アレイセンサ12による光電変換に基づき得られる乱数を意味する。具体的に、本例では、アレイセンサ12の光電変換により得られる画素ごとの電気信号の値を光電乱数として取得し、暗号鍵を生成

する。

[0052] 図4は、光電乱数に基づき、画像データについての暗号化フィルタ(暗号鍵)を生成する手法の例を示している。

先ず、図中左側は、アレイセンサ12の光電変換により得られる画素ごとの電気信号の値を例示している。本例において、光電乱数としては、アレイセンサ12での撮像により得られる画像(静止画)の各画素値(輝度値)を用いる。

ここで以下、光電乱数を得るために撮像されたフレーム画像、換言すれば、光電乱数の元となったフレーム画像のことを「シードフレーム」と表記する。

[0053] 本例では、このような画素ごとの電気信号の値そのものを光電乱数とするのではなく、図中の右側に例示するように、画素ごとの電気信号の値の少なくとも一部を、該電気信号の値が得られた画素位置とは異なる画素位置に割り当てた形式による光電乱数を生成する。換言すれば、画素ごとの電気信号の値について、画素位置をシャッフルさせて光電乱数を生成する。そして、本例では、このように生成した光電乱数を、撮像画像データについての暗号鍵(暗号化フィルタ)として用いる

上記のように画素位置をシャッフルさせた形式による光電乱数とすることで、画素ごとの電気信号の値をそれら電気信号の値が得られた画素位置にそのまま割り当てた光電乱数を用いる場合と比較して、暗号鍵の解読が困難とされ、セキュリティを高めることができる。

[0054] ここで、暗号鍵の生成にあたっては、画素ごとの電気信号の値を所定のアルゴリズムにより変調して用いることもできる。例えば、画素ごとの電気信号の値に所定の係数を乗じて得た値をその画素に割り当てた形式による光電乱数とすることが挙げられる。或いは、画素ごとの電気信号の値が小数点以下の値を含む場合において、小数下数桁の値を整数化して光電乱数とするなどの手法を採ることもできる。

なお、暗号鍵の生成にあたっては、上記のような画素位置のシャッフルを

行うことは必須でなく、画素ごとの電気信号の値そのものを暗号鍵として用いることもできる。

[0055] ここで、従来、暗号化に用いる乱数としては多くの場合、ソフトウェアで生成した疑似乱数が用いられている。しかしながら、疑似乱数は数値を計算するアルゴリズムで生成されるものであり、真の乱数を生成することはできないため、暗号鍵が解読され複製されるリスクがあった。

これに対し、上記の光電乱数は真の乱数となり得るものであり、光電乱数に基づき暗号鍵を生成することで暗号鍵の解読を困難化することが可能となる。

[0056] [1-5. 暗号化対象とする信号について]

従来、アレイセンサ 1 2 での撮像により得られる画像信号について暗号化を行う場合には、アレイセンサ 1 2 から読み出された画像信号を一旦平文の状態メモリに保存し、該保存した画像信号に対し暗号化を施すことが通常とされている。

しかしながら、このような暗号化手法を採った場合には、マルウェアなどを使って暗号化のタイミングで意図的にエラーを起こし、メモリ内容をダンプファイルで出力させ、メモリに置かれた平文をコピーするというハッキングが可能となってしまう。

[0057] そこで本実施形態では、アレイセンサ 1 2 の画素からの読み出し信号に対して暗号化を行うことで、メモリに平文による画像信号が保存されないようにする。

具体的に、本例では、図 2 に示した振幅制御回路 1 9 により、アレイセンサ 1 2 の画素からの読み出し信号に対し図 4 に示した暗号鍵（暗号化フィルタ）に応じた係数による振幅制御を実行させることで、読み出し信号に対する暗号化を実現する。

[0058] 図 5 は、振幅制御回路 1 9 による読み出し信号の暗号化のイメージを示した図である。

図示のようにアレイセンサ 1 2 における各画素からの読み出し信号（この

場合は電荷信号) に対し、振幅制御回路 19 が備えるアンプによって暗号鍵に応じた係数を乗じる。図 2 に示した撮像装置 1 では、このように画素ごとの読み出し信号がアナログ信号の段階で振幅制御された上で、ADC/ピクセルセクタ 13 により A/D 変換され、バッファ 14 及びロジック部 15 を介してメモリ 16 に保存(記録)される。

[0059] 暗号化制御部 85 は、暗号鍵に応じた係数を上記のアンプに設定することで、アレイセンサ 12 における各画素からの読み出し信号に対する暗号化が行われるようにする。

[0060] なお、図 5 はあくまでもイメージ図であり、振幅制御回路 19 において、アンプが画素ごとに設けられることは必須ではない。例えば、CCD (Charged-coupled devices) イメージセンサのように一括読み出しが行われる場合、振幅制御回路 19 が備えるアンプは各画素に共通の一つとされる場合もある。なおその場合、画素ごとの振幅制御は時分割により行う。

[0061] 上記では、読み出し信号に対する暗号化の例として、アナログ信号による読み出し信号に暗号化を施す例を挙げたが、A/D 変換後のデジタル信号による読み出し信号に対して暗号化を施すこともできる。

[0062] 図 6 は、デジタル信号による読み出し信号に対して暗号化を施す場合の撮像装置 1 の構成例を示している。

この場合の撮像装置 1 では、撮像用センサ部 10 内において、振幅制御回路 19 に代えて、ADC/ピクセルセクタ 13 によりデジタル信号に変換された読み出し信号について振幅制御を行う振幅制御回路 19A が設けられる。

[0063] なお、この場合における暗号化制御部 85 による処理は、暗号鍵に応じた画素ごとの係数の設定対象が振幅制御回路 19 から振幅制御回路 19A に変更される以外は同様となるため、重複説明は避ける。

[0064] ここで、上述のようにアナログの読み出し信号に対する暗号化を施すものとするれば、アナログ信号を外部から不正取得することは非常に困難であるため、セキュリティの向上が図られる。

[0065] なお、アナログ読み出し信号に対する暗号化を施す場合には、暗号化画像を復号化して得た画像について、画像の再現性が低下することが懸念される。

しかしながら、例えば対象とする画像が人物等のターゲットの属性や行動の分析に用いられる場合には、画像の再現性としてはターゲットの検出や分析が可能な程度であればよく、実用上の問題は生じないと考えられる。

[0066] 一方で、デジタル読み出し信号に対する暗号化を施す場合には、暗号化処理の正確性が向上し、画像の再現性の向上を図ることができる。

[0067] ここで、上記のように読み出し信号に対して行う暗号化は、ストリーム暗号方式による暗号化の一種である。ストリーム暗号方式は、平文をビット単位やバイト単位等の所定のデータ単位で暗号化する暗号方式である。

ストリーム暗号方式では、暗号化の対象信号についてデータの長さを揃える必要がなく、そのため、対象信号に対する暗号化の前処理が不要とされる。従って、ストリーム暗号方式の採用により、暗号化処理の高速化を図ることができる。

[0068] ここで、アナログの読み出し信号に対して暗号化を施した場合であっても、結果的には、電子署名の対象データとして、暗号化された撮像画像データが得られることに変わりはない。この点より、本明細書においてアナログ信号の段階で暗号化を施すことは、画像データの暗号化を行うことの範疇に含まれるとする。

[0069] [1-6. 耐タンパー化について]

本例の撮像用センサ部10は、ハードウェア面での耐タンパー化を図るべく、図7に例示するようにアレイセンサ12、メモリ16、演算部18の各チップが1パッケージ化されている。図7の例では、演算部18としてのチップ上にメモリ16としてのチップが積層され、さらにメモリ16としてのチップ上にアレイセンサ12としてのチップが積層されている。

本例において、読み出し信号に対する暗号化を施す暗号化部は、例えばアレイセンサ12としてのチップ内に形成されている。

また、光電乱数に基づく暗号鍵を生成し、上記の暗号化部に該暗号鍵に基づく暗号化を実行させる暗号化制御部 85 は、演算部 18 としてのチップに含まれている。

[0070] 本例では、各チップの電氣的な接続が Cu（銅）製のパッド同士を接続する Cu-Cu 接続により行われており、撮像用センサ部 10 の分解を試みるとこれらの電氣的接続部分が破壊される。つまりこれにより、ハードウェア面での耐タンパー化が図られている。

[0071] 図 8 は、撮像用センサ部 10 の構造の別例を示しており、図 7 との差は演算部 18 とメモリ 16 との上下関係が入れ替わった点である。

図 9 は、撮像用センサ部 10 の構造のさらに別例を示しており、図 7 との差はメモリ 16 としてのチップが複数積層された点（図の例では 2 層）である。

なお、図示は省略したが、撮像用センサ部 10 としては、メモリ 16 を演算部 18 と同レイヤに形成して 2 レイヤの構造としたり、アレイセンサ 12、メモリ 16、及び演算部 18 を同レイヤに形成した 1 レイヤの構造とすることもできる。

[0072] 図 7 から図 9 で例示したような 1 パッケージ化の構成を採ることで、上記した Cu-Cu 接続など、分解によるメモリ 16 からの不正な情報取得に対する耐性を高めるための対策を施すことが可能となり、ハードウェア面での耐タンパー化を図ることが可能とされる。

[0073] [1-7. 画像暗号化のための処理手順]

続いて、上記により説明した第一実施形態としての画像暗号化を実現するために演算部 18 が実行する処理の手順について、図 10 のフローチャートを参照して説明する。

なお、以下で説明する処理のうち少なくとも一部についてはハードウェアによる処理として実現することもできる。

[0074] 先ず前提として、本例の演算部 18 は、図 10 に示す処理を、起動時、及び不正アクセス検知部 86 により不正アクセスが検知されたことに応じて開

始する。

不正アクセスの検知に応じて図10に示す処理を開始することで、光電乱数の取得（S101）や暗号鍵の生成（S105）が不正アクセスの検知に応じて実行される。すなわち、不正アクセスの検知に応じて光電乱数が再取得され、再取得された光電乱数に基づき暗号鍵が再生成される。これにより、ソフトウェア面での耐タンパー化が図られる。

なお、図10に示す処理は、外部からの指示（例えば操作入力に応じた指示）に応じて開始する、或いは、一定時間おきに開始する等、他の条件に基づき開始することもできる。

[0075] 図10において、演算部18はステップS101で、静止画撮像処理を実行する。この静止画撮像処理は、暗号鍵の生成の元となる静止画を撮像するための処理であり、演算部18はアレイセンサ12を制御して1フレーム分の画像の撮像（画素ごとの電荷の読み出し）を実行させる。

ステップS101の静止画撮像処理が実行されることで、メモリ16にシードフレームとしての画像データが保存される。

[0076] ステップS101に続くステップS102で演算部18は、画素値の均一性チェック処理を実行する。この均一性チェック処理は、シードフレームについて画素ごとの輝度値の均一性をチェック処理であり、具体的に演算部18は、輝度値がゼロや飽和値（最大値）となっている画素の数をカウントする。

なお、画素値の均一性チェック処理としては、読み出し信号の値を対象とした均一性のチェック処理として実行することもできる。

[0077] ステップS102に続くステップS103で演算部18は、均一性が過剰であるか否かを判定する。具体的には、ステップS102でカウントした画素の数が所定閾値（例えば、有効画素数の30%～50%に対応した値）以上であるか否かを判定する。

ステップS102でカウントした画素の数が上記閾値以上であり、均一性が過剰であるとの判定結果を得た場合、演算部18はステップS104に進

んでシードフレームを消去する処理、すなわちメモリ 16 に保存されたシードフレームとしての画像データを消去する処理を実行した上で、ステップ S 101 に戻る。

これにより、シードフレームの画素値のランダム性が低い場合に対応して、シードフレームを撮像し直すことができる。すなわち、光電乱数のランダム性が低い場合に対応して、光電乱数を取得し直すことができる。

従って、ランダム性の低い乱数に基づく暗号鍵により暗号化が行われてしまうことの防止を図ることが可能とされ、セキュリティの向上を図ることができる。

[0078] 一方、ステップ S 103 において、カウントした画素の数が上記閾値以上ではなく、均一性が過剰ではないとの判定結果を得た場合、演算部 18 はステップ S 105 に進んで暗号鍵を生成する。具体的に本例では、シードフレームにおける各画素の輝度値に基づき、振幅制御回路 19（又は 19A）における各アンプに設定すべき係数を表す暗号鍵を生成する。

[0079] ここで、本例において、ステップ S 105 の処理では、画素ごとの輝度値をそれら輝度値が得られた画素位置にそのまま割り当てた形式の光電乱数に基づき暗号鍵を生成するものとはせず、画素ごとの輝度値の少なくとも一部を、該輝度値が得られた画素位置とは異なる画素位置に割り当てた形式による光電乱数に基づき、暗号鍵を生成する。

これにより、暗号鍵の解読が困難とされ、セキュリティの向上を図ることができる。

[0080] ステップ S 105 に続くステップ S 106 で演算部 18 は、シードフレームを消去する処理、すなわち、ステップ S 101 の撮像処理によりメモリ 16 に保存されたシードフレームとしての画像データを消去する処理を実行する。

このシードフレームの消去処理を行うことで、光電乱数の元となった画像が流出して光電乱数が推定されてしまうことの防止を図ることができる。

[0081] なお、例えば演算部 18 の処理能力が高い場合やシードフレームの画像サ

イズが小さい場合等には、シードフレームを一旦メモリ 16 に保存させることは必須ではない。その場合、演算部 18（暗号化制御部 85）は、例えば振幅制御回路 19（又は 19A）から光電乱数を受け取り、ステップ S 102 及び S 103 の処理を経由してステップ S 105 で暗号鍵の生成を行う。この場合には、ステップ S 106 の消去処理は不要である（勿論、ステップ S 104 の消去処理も不要である）。

[0082] 続くステップ S 107 で演算部 18 は、既存鍵があれば消去する。例えば、図 10 に示す処理が一定時間ごとに開始される等の場合には、過去に行われたステップ S 108 の処理により、メモリ 16 には暗号鍵が保存されている。ステップ S 107 の処理は、このようにメモリ 16 に既存の暗号鍵が保存されている場合に、該暗号鍵を消去する処理となる。

このような既存鍵の消去処理を行うことで、過去に暗号化に用いた暗号鍵の流出防止を図ることが可能とされ、過去に暗号化した信号が不正に復号化されてしまうことの防止を図ることができる。

[0083] 続くステップ S 108 で演算部 18 は、暗号鍵の保存処理を実行する。すなわち、ステップ S 105 で生成した暗号鍵をメモリ 16 に保存する処理を実行する。

ステップ S 108 の保存処理を実行したことに応じ、演算部 18 は図 10 に示す一連の処理を終える。

[0084] 撮像装置 1 においては、ステップ S 108 で保存された暗号鍵を用いて、アレイセンサ 12 での撮像により得られる画像データ（撮像画像データ）の暗号化が行われる。具体的に、演算部 18（暗号化制御部 85）は、図 10 に示した処理の終了後、保存された暗号鍵に基づく画素ごとの係数を振幅制御回路 19（又は 19A）における各アンプに設定して、アレイセンサ 12 での撮像により得られる画像信号に該保存された暗号鍵に基づく暗号化が施されるようにする。

本例では、アレイセンサ 12 は動画像の撮像を行うものとされ、振幅制御回路 19（又は 19A）による暗号化は動画像を構成する各フレーム画像に

対して行われる。

[0085] 本例において、上記のように暗号化が施された動画像としての撮像画像データは、制御部23の制御に基づき、メモリ部24に保存される。制御部23は、このようにメモリ部24に保存された撮像画像データを、通信部25を介して受信装置3に送信することが可能とされる。

[0086] ここで、上記説明から理解されるように、本例では、画像データの暗号化は、暗号化対象の画像データとは異なるフレーム期間に得た光電乱数に基づき行うものとしている。

これにより、暗号化画像から暗号鍵が推定されることの困難性が高められ、セキュリティの向上を図ることができる。

なお、暗号化対象の画像データと同一フレーム期間に得た光電乱数に基づき画像データの暗号化を行うことも可能である。

[0087] [1-8. 画像復号化のための鍵の受け渡しについて]

受信装置3は、上記のように光電乱数に基づき生成した暗号鍵（暗号化フィルタ）で暗号化された撮像画像データを撮像装置1より受信し、受信した撮像画像データを復号化するが、この際、復号化に用いる鍵（復号鍵）は、暗号化に用いた鍵と同一鍵とされる。つまり本例では、共通鍵暗号方式を採用している。周知のように共通鍵暗号方式では、共通鍵の受け渡しをセキュアに行うことが重要とされる。

[0088] 図11を参照し、受信装置3に復号化のための鍵（共通鍵）をセキュアに受け渡すための手法の例について説明しておく。該手法の概要としては、公開鍵暗号を使用して共通鍵を受け渡す手法となる。

先ず、受信装置3は、公開鍵と秘密鍵を作成し、公開鍵を撮像装置1に受け渡す（図11A）。

[0089] 公開鍵を取得した撮像装置1では、前述のように光電乱数に基づき生成した暗号鍵を共通鍵として、該共通鍵を公開鍵により暗号化し、受信装置3に送信する（図11B）。

そして、受信装置3においては、送信された共通鍵（復号鍵）を、図11

Aにおいて作成した秘密鍵を用いて復号化する（図11C）。

これにより以降、受信装置3においては、撮像装置1から受信される暗号化された撮像画像データを、上記のように復号化した共通鍵を用いて高速に復号化することができる。図11Dでは、撮像装置1側において共通鍵を用いて画像暗号化が行われることを模式的に表し、図11Eでは、共通鍵により暗号化された画像データを、受信装置3が共通鍵を用いて復号化することを模式的に表している。

[0090] なお、図11Bの公開鍵による共通鍵の暗号化、及び図11Cの共通鍵の秘密鍵による復号化にはそれぞれ数秒程度の時間を要するが、これらの暗号化、復号化を要するのは一つの鍵の受け渡しにつき1度のみである。

[0091] [1-9. 第一実施形態としての改竄検知手法]

前述のように、本実施形態では、撮像装置1が受信装置3に対して送信する撮像画像データは、電子署名の対象データとされる。

ここで、確認のため、図12の模式図を参照し、電子署名を用いた電子文書の改竄検知手法について説明しておく。

実施形態との対応では、図中の「送信者側」が撮像装置1に相当し、「受信者側」が受信装置3に相当する。また、「電子文書」は、撮像装置1による撮像画像データ（本例では光電乱数に基づき暗号化されている）に相当する。

[0092] 送信者側では、電子文書についてのハッシュ値を計算すると共に、署名生成鍵としての秘密鍵を生成し、生成した秘密鍵によりハッシュ値を暗号化する。さらに送信者側は、秘密鍵に基づき、署名検証鍵としての公開鍵を生成する。

送信者側では、電子文書を受信者側に送信する際、送信データに、秘密鍵により暗号化したハッシュ値を電子署名データとして含ませる。また送信者側は、該送信データに秘密鍵から生成した公開鍵を含む電子証明書データを含ませる。

[0093] 受信者側では、送信者側から受信した電子文書のハッシュ値を計算する。

また、受信者側では、図中に「署名検証」と示す処理として、電子署名データにおける暗号化されたハッシュ値を、電子証明書に含まれる公開鍵により復号化する。その上で受信者側は、双方のハッシュ値が一致するか否かの一致判定を行う。

このとき、受信者側で受信した電子文書が、送信時の内容から改竄されていなければ、二つのハッシュ値は一致することになる。このため、上記のような一致判定により、電子文書の改竄有無を検知（判定）することができる。

[0094] 本実施形態では、このような電子署名を用いた改竄検知手法を採る場合において、署名生成鍵としての秘密鍵を、前述した光電乱数に基づき生成することで、該秘密鍵の解読を困難化して改竄検知性能の向上を図る。

[0095] 図13のフローチャートを参照し、第一実施形態としての電子署名用暗号鍵の生成処理について説明する。

本例において、図13に示す処理は、制御部23が実行する。

まず、制御部23はステップST1で、光電乱数を取得する処理を行う。この光電乱数としては、撮像用センサ部10に新たに生成させたものを取得することが考えられる。

或いは、撮像用センサ部10が撮像画像データの暗号化のために既に生成していた光電乱数を取得することもできる。例えば、本例では、前述したステップS105の暗号鍵生成処理において、画素ごとの電気信号値に基づき生成した光電乱数がメモリ16に保存される。ステップST1の処理は、このようにメモリ16に保存された光電乱数を撮像用センサ部10から取得する処理とすることもできる。

ここで、ステップST1の処理として、撮像用センサ部10に新たに生成させた光電乱数を取得する処理を行う場合、図13に示す処理は、不正アクセス検知部86により不正アクセスが検知されたことに応じて開始することができる。この場合、電子署名秘密鍵についても、外部からの不正アクセスが検知された場合は、再生成した光電乱数に基づき更新されることになる。

或いは、図 1 3 に示す処理は、一定時間おきに開始する等、他の条件に基づき開始することもできる。

また、秘密鍵生成のために撮像用センサ部 1 0 に新たに光電乱数を生成させる場合、制御部 2 3 は、該新たな光電乱数の生成後、該光電乱数の元となった画像データ（シードフレーム）の消去を撮像用センサ部 1 0 に指示することもできる。

[0096] ステップ S T 1 に続くステップ S T 2 で制御部 2 3 は、光電乱数に基づき秘密鍵を生成する。ここで、光電乱数から秘密鍵を生成する手法については、例えば R S A 暗号（R S A : Rivest Shamir Adleman）の手法を挙げることができるが、特定の手法に限定されるものではない。

[0097] さらに、ステップ S T 2 に続くステップ S T 3 で制御部 2 3 は、秘密鍵に基づき公開鍵を生成する。すなわち、署名生成鍵としての秘密鍵に基づき、署名検証鍵としての公開鍵を生成するものである。

[0098] 図 1 4 のフローチャートは、上記のように生成した秘密鍵と公開鍵とに基づき撮像画像データの改竄検知を行うために実行されるべき処理手順の例を示している。

図中、撮像装置 1 として示す処理は制御部 2 3 が、受信装置 3 として示す処理は C P U 3 1 が実行する。

[0099] 先ず、受信装置 3 側において、C P U 3 1 はステップ S 3 0 1 で、暗号化画像データの送信要求を撮像装置 1 側に対して行う。

[0100] 撮像装置 1 側において、制御部 2 3 は上記の送信要求をステップ S 2 0 1 で待機しており、送信要求があった場合は、ステップ S 2 0 2 に進んで要求された画像データのハッシュ値を計算する。すなわち、メモリ部 2 4 に記憶され、送信要求により要求された撮像画像データについてのハッシュ値を計算する。このとき、ハッシュ値の計算に用いるハッシュ関数については、受信装置 3 側が後述するステップ S 3 0 4 のハッシュ値計算で用いるハッシュ関数と同一のものをを用いる。ハッシュ関数の例としては、例えば S H A - 1 や S H A - 2 等を挙げることができるが、特定のハッシュ関数に限定される

ものではない。

[0101] ステップS202に続くステップS203で制御部23は、ハッシュ値を秘密鍵により暗号化する。すなわち、図13の処理で光電乱数に基づき生成した秘密鍵により、ステップS202で計算したハッシュ値を暗号化する。

さらに、続くステップS204で制御部23は、要求された暗号化画像データ、暗号化ハッシュ値、及び公開鍵を要求元の受信装置3に送信する。すなわち、送信要求された暗号化状態の撮像画像データ、ステップS203で暗号化したハッシュ値、及び図13の処理で生成した公開鍵を送信要求元の受信装置3に送信する。

[0102] 受信装置3側において、CPU31は、ステップS204で送信されるデータの受信をステップS302で待機しており、該データが受信された場合は、先ずステップS303で暗号化画像データを復号化する。すなわち、光電乱数に基づく暗号鍵（暗号化フィルタ）により暗号化された状態の撮像画像データを、撮像装置1より予め取得された同暗号鍵（復号鍵）により復号化する。本例では、暗号化フィルタとしての暗号鍵は、図11に例示した手法等により受信装置3が予め撮像装置1よりセキュアに取得している。

ステップS303に続くステップS304でCPU31は、ハッシュ値を計算する処理として、ステップS303で復号化した撮像画像データについてのハッシュ値を計算する。

[0103] 次いで、CPU31はステップS305で、暗号化ハッシュ値を公開鍵により復号化する。すなわち、撮像装置1側より受信した暗号化ハッシュ値を同じく撮像装置1側より受信した公開鍵により復号化する。

そして、CPU31はステップS306で、両ハッシュ値の一致判定、すなわちステップS304で計算したハッシュ値とステップS305で復号化したハッシュ値との一致判定を行う。この一致判定により、撮像画像データの改竄有無が判定される。

[0104] <2. 第二実施形態>

[2-1. 第二実施形態の画像暗号化手法]

続いて、第二実施形態について説明する。

なお、第二実施形態においても、撮像装置 1 や受信装置 3 の構成については第一実施形態で説明したものと同様となるため重複説明は避ける。以下の説明において、既に説明済みとなった部分と同様となる部分については同一符号を付して説明を省略する。

[0105] 第二実施形態では、画像データにおけるターゲット領域を対象とした暗号化を行う。具体的に、第二実施形態では、画像全体とターゲット領域とで異なる暗号鍵に基づく暗号化を行うと共に、ターゲット領域については、特定部位の領域とそれ以外の領域とで異なる暗号鍵に基づく暗号化を行うことで、画像の受け手側に保有させる復号鍵の別によって情報の秘匿レベルを段階的に変化させる。

[0106] 図 1 5、図 1 6 は、第二実施形態における段階的な画像暗号化のイメージを説明するための図である。

図 1 5 は、ターゲットのクラスが人物である場合における段階的な画像暗号化のイメージを示している。

図 1 5 A は暗号化前の画像を示している。この場合、ターゲット領域 A T は、画像内で人物が映し出されている部分の全域とされる。またこの場合、特定部位の領域である特定領域 A S は、人物の顔の領域とされる。

図 1 5 B は、特定領域 A S のみが暗号化された画像、図 1 5 C は特定領域 A S を含むターゲット領域 A T のみが暗号化された画像、図 1 5 D は画像全域が暗号化された画像を示している。

[0107] 図 1 6 は、ターゲットのクラスが車両である場合における段階的な暗号化のイメージを示しており、図 1 6 A は、暗号化前の画像を示している。

この場合、ターゲット領域 A T は、画像内で車両が映し出されている部分の全域とされ、特定領域 A S は、車両の搭乗者、及びナンバープレートの領域とされる。

図 1 6 B は、特定領域 A S のみが暗号化された画像、図 1 6 C は特定領域 A S を含むターゲット領域 A T のみが暗号化された画像、図 1 6 D は画像全

域が暗号化された画像である。

[0108] これら図 1 5、図 1 6 の例の場合、暗号鍵としては、画像全域の暗号化に対応した第一暗号鍵と、ターゲット領域 A T のみの暗号化に対応した第二暗号鍵と、特定領域 A S のみの暗号化に対応した第三暗号鍵の 3 種を少なくとも生成する。

[0109] 図 1 7 は、段階的な暗号化の具体的手法の例を説明するための図である。

本例では、対象の画像に対し第一、第二、第三暗号鍵に基づく暗号化をそれぞれ個別に施すことはせず、これら複数の暗号鍵を合成した合成鍵に基づき対象の画像に対する暗号化を行う。

[0110] 先ず、特定領域 A T を暗号化するための第三暗号鍵、ターゲット領域 A T 全域を暗号化するための第二暗号鍵、画像全域を暗号化するための第一暗号鍵をそれぞれ用意する。これら 3 種の暗号鍵を生成するにあたっては、3 種の光電乱数を得る（つまりシードフレームを 3 種撮像する）ようにしてもよいが、本例では、暗号鍵生成に要する時間の短縮化のため、共通の光電乱数から 3 種の暗号鍵を生成する。具体的に、本例では、3 種の暗号鍵の生成にあたっては、先ず、共通の光電乱数における画素ごとの数値の配置をそれぞれ異ならせた 3 種の乱数（以下、それぞれ第一乱数、第二乱数、第三乱数と表記する）を生成する。

そして、第三暗号鍵については、第三乱数の数値のうち、特定領域 A S の各画素の数値を抽出した暗号鍵として生成する。

また、第二暗号鍵については、第二乱数の数値のうち、ターゲット領域 A T の各画素の数値を抽出した暗号鍵として生成する。

第一暗号鍵については、第一乱数をそのまま適用した暗号鍵として生成する。

[0111] その上で、合成鍵として、図示のようにこれら第一、第二、及び第三暗号鍵を合成した暗号鍵を生成する。

そして、該合成鍵に基づき、対象の画像の暗号化が行われるようにする。

[0112] 上記のような段階的な暗号化を行うことで、画像の受け手側（受信装置 3

側) が保有する復号鍵の別によって、情報の秘匿レベルを変化させることが可能とされる。

図 18 は、秘匿レベルの変化例についての説明図である。

ここでは、鍵の保有に関するレベルとして、レベル 0 からレベル 3 までの 4 レベルを定義する。図示のようにレベル 0 は鍵なし、レベル 1 は第一暗号鍵のみ保有、レベル 2 は第一、第二暗号鍵の合成鍵を保有、レベル 3 は第一、第二、及び第三暗号鍵の合成鍵を保有、をそれぞれ意味する。

[0113] レベル 0 の場合には、画像の受け手側において暗号化画像を復号化できず、全域が暗号化された画像が得られる。

レベル 1 の場合、画像の受け手側では第一暗号鍵を用いてターゲット領域 A T 以外の領域を復号化することができ、従ってターゲット領域 A T のみが暗号化された画像が得られる。

[0114] レベル 2 の場合、画像の受け手側では第一、第二暗号鍵の合成鍵を用いて特定領域 A S 以外の領域を復号化することができ、ターゲットにおける特定領域 A S のみが暗号化された画像が得られる。

レベル 3 の場合、画像の受け手側では第一、第二、及び第三暗号鍵の合成鍵を用いて画像全域を復号化することができ、この場合には情報の秘匿のない画像を得ることができる。

[0115] ここで、本例では、暗号化対象の画像は動画像とされるため、画像内に映し出されるターゲットとしての物体は時間経過と共に画像内で変位する可能性がある。このため、上記のようなターゲット領域 A T を対象とした暗号化を行う場合には、ターゲットの追尾を行うことを要する。

[0116] 以下、このようなターゲットの追尾を含む、第二実施形態としての画像暗号化の具体的な手法の例について、図 19 を参照して説明する。

なお、図 19 において、ターゲットのクラスは「人物」とする。また、図 19 では説明の便宜上、ターゲット領域 A T において特定領域 A C とそれ以外の領域とを区別せず、画像内のターゲット領域 A T とそれ以外の領域とについてのみ暗号化し分ける例を挙げる。

[0117] 先ず、図 19 A に示すフレーム F 1 は、ターゲットクラスである人物がまだフレームインしていない状態を示している。なお、ここでは、画像内にターゲットクラスではない「木」としての物体が識別されている例としている。

[0118] ここで、画像全域に対する暗号化は、ターゲットの有無に拘わらず行われるものである。つまり、本例では、各フレーム F の画像は、画像全域に対応した第一暗号鍵に基づき振幅制御回路 19（又は 19 A）において暗号化された後、メモリ 16 に保存される。図 19 の各分図に示す白抜きの鍵マークは、出力画像として、このような画像全域を対象とした暗号化が施されていることを表している。

[0119] ターゲットの追尾のためには、演算部 18 は、画像内における物体の領域の検出やクラス識別を行うことになる（前述した物体領域認識部 82 やクラス識別部 83 の処理）。これらの処理を行うために、演算部 18 は、上記のように暗号化されて保存されたフレーム画像を復号化する。すなわち、演算部 18 は、ターゲット追尾のための処理を、第一暗号鍵に基づき暗号化されたフレーム画像を復号化しながら実行する。

演算部 18 は、この際の復号化をオンザフライ方式により行う。これにより、ターゲットの追尾を行う際に平文状態の画像信号が流出してしまう可能性を低減することが可能とされ、セキュリティの向上を図ることができる。

[0120] 図 19 B に示すフレーム F 2 は、ターゲットクラスである「人物」がフレームインした状態を示している。この状態では、既に識別されている「木」と共に、ターゲットクラスである「人物」が識別される。

このようにターゲットクラスとしての物体を識別した場合、演算部 18（物体領域認識部 82）は、当該物体のエリアを囲う正確な位置座標のバウンディングボックス 40 の算出を行う。

例えば図 19 C にターゲットクラスである人物の画像についてのバウンディングボックス 40 の例を示している。すなわちバウンディングボックス 40 はターゲットクラスに該当する物体のより正確な領域として計算される。

さらに演算部 18（物体領域認識部 82）は、バウンディングボックス 40 を元に、関心領域である RO I 41 を算出する。

[0121] 図 19D に、RO I 41 とバウンディングボックス 40 を示している。RO I 41 は、例えばバウンディングボックス 40 の縦横サイズ（ $x \times y$ ）を拡大（ $a \times b$ ）して計算される。拡大の縮尺 a 、 b は縦横別に設定でき、拡大率は固定でもよいが、撮像用センサ部 10 の外部（例えば画像プロセッサ 21 など）より指定されるようにすることも考えられる。

[0122] 本例では、この RO I 41 をターゲット領域 AT として、画像全域とは異なる暗号鍵を用いた暗号化を行う。

[0123] ここで、フレーム F 2 は、画像内にターゲットクラスが新たに識別されたフレームであり、ターゲットクラス発見フレームと換言することができる。

本例では、画素からの読み出し信号に対して暗号化を施す手法を採るため、ターゲットクラス発見フレームについては、RO I 41 に対し第二暗号鍵に基づく暗号化を施すことができない。ターゲットクラス発見フレームについては、既に第一暗号鍵のみに基づく暗号化が施されてメモリ 16 に保存されている。このように第一暗号鍵のみに基づく暗号化が施されたターゲットクラス発見フレームがそのまま出力されてしまうと、第一暗号鍵のみの保有者に対し、RO I 41 の画像領域が秘匿されずに開示されてしまうことになる。

[0124] そこで、本例では、ターゲットクラス発見フレームについてはメモリ 16 から消去するものとし、画像の受け手側が保有する復号鍵の別に応じた適切な情報秘匿レベルが実現されるようにする。

[0125] 図 19E は、フレーム F 2 の次のフレームであるフレーム F 3 を表している。

ターゲットクラス発見フレームの次のフレーム F より、RO I 41 を対象とした第二暗号鍵に基づく暗号化を施す。ここでの RO I 41 は、ターゲットクラス発見フレームであるフレーム F 2 の時点で算出された RO I 41 である。

ターゲットクラスとしての「人物」が移動している場合には、フレームF 3では、フレームF 2よりも人物が移動方向側に進むことになるが、R O I 4 1がバウンディングボックス4 0よりも大きな範囲とされることで、フレームF 3においてR O I 4 1内にターゲットクラスとしての人物が収まることになる。すなわち、ターゲットクラスとしての人物が第二暗号鍵に基づく暗号化の対象範囲内に収まる。

[0126] フレームF 3以降においても、同様にターゲットクラスについてのバウンディングボックス4 0及びR O I 4 1の算出を行い、これによりターゲットクラスが追尾されるようにする（図1 9 F参照）。

そして、フレームF 4以降では、フレームF 3と同様に、一つ前のフレームFで算出されたR O I 4 1を対象として、第二暗号鍵に基づく暗号化が施されるようにする（図1 9 G参照）。

[0127] 図1 9 Hは、ターゲットクラスとしての「人物」がフレームアウトした後のフレームF nを表している。ターゲットクラスがフレームアウトしたことで、R O I 4 1は算出されなくなる。このため、フレームF nの画像については、第一暗号鍵のみに基づく暗号化が行われる。

[0128] なお、上記説明では、バウンディングボックス4 0を拡大した矩形の領域をR O I 4 1とする例を述べたが、R O I 4 1は矩形の領域に限られるものではない。

例えばセマンティックセグメンテーション、すなわち画素レベルでの物体エリア検出を用いて、そのターゲットクラスの物体のエリアからR O I 4 1を計算してもよい。

[0129] 図2 0は、セマンティックセグメンテーションに基づくR O I 4 1を示している。これは物体（例えば人物）としての画素領域を広げて、非矩形のR O I 4 1を設定した例である。

例えば突起物のあるトラック、自転車に乗っている人など、矩形のR O I 4 1では一部が含まれなかったり、或いは大きすぎる状態になってしまうことがある。画素レベルの物体位置に応じて非矩形のR O I 4 1を生成すれば

、ターゲットに係る秘匿領域を過不足なく適切に設定することが可能となる。

[0130] [2-2. 画像暗号化のための処理手順]

上記により説明した第二実施形態としての画像暗号化を実現するために演算部 18 が実行する処理の手順について、図 21 及び図 22 のフローチャートを参照して説明する。

図 21 は、シードフレームの撮像から暗号鍵の元となる乱数の保存までに対応した処理を示している。なお、図 21 において、既に図 10 で説明した処理と同様となる処理については同一ステップ番号を付して説明を省略する。

図 10 の処理と同様、図 21 の処理は、起動時、及び不正アクセス検知部 86 により不正アクセスが検知されたことに応じて開始する。或いは、一定時間おきに開始する等、他の条件に基づき開始することもできる。

なお、図 21 及び図 22 で説明する処理のうち少なくとも一部についてはハードウェアによる処理として実現することもできる。

[0131] 図 21 において、この場合の演算部 18 は、ステップ S103 で均一性が過剰と判定した場合に、ステップ S151 に進んで各レベルの乱数を生成する。ここでは、ターゲット領域 AT において特定領域 AS を区別しないため、乱数としては前述した第一乱数と第二乱数の 2 種を生成する。

なお、シードフレームの光電乱数に基づき各種の乱数を生成する手法については既に説明したため重複説明は避ける。

[0132] この場合の演算部 18 は、ステップ S151 の乱数生成処理を実行したことに応じ、ステップ S106 でシードフレームの消去処理を実行する。

そして、ステップ S106 の消去処理を実行したことに応じ、演算部 18 はステップ S152 で既存乱数があれば消去する処理を実行する。すなわち、過去に実行されたステップ S153 の処理でメモリ 16 に保存された各レベルの乱数（第一乱数と第二乱数）があれば、それらの乱数を消去する処理である。

ステップS 1 5 2に続くステップS 1 5 3で演算部 1 8は、ステップS 1 5 1で生成した各レベルの乱数をメモリ 1 6に保存する処理を行い、図 2 1に示す一連の処理を終える。

[0133] 図 2 2は、生成した暗号鍵に基づき対象画像を暗号化するための処理を示している。

先ず、演算部 1 8はステップS 4 0 1で、暗号化対象とする画像の撮像開始を待機しており、撮像開始となったら、ステップS 4 0 2で第一暗号鍵による暗号化処理を実行する。すなわち、振幅制御回路 1 9（又は 1 9 A）に第一暗号鍵に基づく画素ごとの係数を指示してアレイセンサ 1 2の読み出し信号に対する暗号化を実行させる。先の説明から理解されるように、本例では、第一暗号鍵は、第一乱数をそのまま適用した暗号鍵とされる。

[0134] ステップS 4 0 2に続くステップS 4 0 3で演算部 1 8は、物体領域認識処理を実行し、さらに続くステップS 4 0 4でクラス識別処理を実行する。ステップS 4 0 3の物体領域認識処理は、前述した物体領域認識部 8 2の処理であり、現フレームの画像から候補となる物体の検出及びその物体領域の認識処理を行う。また、ステップS 4 0 4のクラス識別処理は、前述したクラス識別部 8 3の処理であり、上記の物体領域認識処理で検出された物体についてクラス識別を行う。複数の物体や複数種類の物体が検出された場合、それぞれについてクラス識別が行われ、各クラスに分類される。例えば、先の図 1 9 Bの場合、「木」というクラスの物体が 1 つ、「人物」というクラスの物体が 1 つというようにクラス識別及び分類が行われる。

なお、演算部 1 8は、ステップS 4 0 3及びS 4 0 4の処理については、ステップS 4 0 2や後述するステップS 4 1 3で暗号化されたフレーム画像をオンザフライ方式で復号化しながら実行する。

[0135] ステップS 4 0 4に続くステップS 4 0 5で演算部 1 8は、ターゲットクラスが存在するか否かを判定する。すなわち、ステップS 4 0 4で識別されたクラスのうちにターゲットクラスが存在したか否かを判定する。

ターゲットクラスが存在しなければ、演算部 1 8はステップS 4 0 6で次

のフレームを待機（次のフレーム期間の到来を待機）した上で、ステップS 4 0 2に戻る。すなわち、ターゲットクラスが検出されるまで、ステップS 4 0 2による画像全域の暗号化処理、ステップS 4 0 3の物体領域認識処理、及びステップS 4 0 4のクラス識別処理がフレームごとに繰り返し実行される。

[0136] ステップS 4 0 5でターゲットクラスが存在すると判定した場合、演算部 1 8はステップS 4 0 7に進んでバウンディングボックス4 0の算出を行い、続くステップS 4 0 8でR O I 4 1の算出を行う。

さらに、続くステップS 4 0 9で演算部 1 8は、R O I 4 1のみに第二乱数の数値を適用した第二暗号鍵と、第一暗号鍵とを合成した合成鍵を生成する。

[0137] ステップS 4 0 9で合成鍵を生成したことに応じ、演算部 1 8はステップS 4 1 0でターゲットクラス発見フレームであるか否かを判定する。現フレームがターゲットクラス発見フレームであれば、演算部 1 8はステップS 4 1 1でターゲットクラス発見フレームを消去する処理を実行する。これにより、ターゲットクラス発見フレームについて、鍵の保有レベルがレベル1であるにも拘わらずターゲットの画像部分が秘匿されなくなってしまうことの防止が図られる。

[0138] ステップS 4 1 0において、現フレームがターゲットクラス発見フレームでなければ、演算部 1 8はステップS 4 1 1の消去処理をパスして、ステップS 4 1 2で次のフレームを待機する処理を行う。また、演算部 1 8は、ステップS 4 1 1の消去処理を実行した場合も、ステップS 4 1 2で次のフレームを待機する処理を行う。

[0139] ステップS 4 1 2の待機処理を実行したことに応じ、演算部 1 8はステップS 4 1 3で一つ前のフレームで生成した合成鍵による暗号化処理を実行する。すなわち、振幅制御回路 1 9（又は1 9 A）に当該合成鍵に基づく画素ごとの係数を指示してアレイセンサ 1 2の読み出し信号に対する暗号化を実行させる。

[0140] ステップS 4 1 3に続くステップS 4 1 4で演算部 1 8は、撮像終了か否か、すなわち、例えば外部からの撮像終了指示が行われる等、暗号化対象の画像の撮像を終了すべき状態となったか否かを判定する。

撮像終了でなければ、演算部 1 8はステップS 4 0 3に戻る。これにより、撮像終了となるまで、これまで説明した処理が繰り返される。すなわち、引き続きターゲットクラスが存在すれば、該ターゲットクラスについてのR O I 4 1の算出、及び算出したR O I 4 1に基づく合成鍵の生成、及び一つ前のフレームで生成した合成鍵に基づく暗号化処理が行われ、ターゲットクラスが存在しなくなった場合は、合成鍵による暗号化処理が行われず、第一暗号鍵による暗号化処理が実行される。

[0141] 撮像終了であれば、演算部 1 8は図 2 2に示す一連の処理を終える。

[0142] なお、本例では、R O I 4 1については、次のフレームにおいてターゲットとしての物体を包含できるようにバウンディングボックス4 0を広げた領域として設定しているが、縦横サイズ($x \times y$)を拡大($a \times b$)するときの拡大の縮尺 a 、 b は、フレームレートに応じたものとするとも考えられる。

例えば、フレームレートが低いと、フレーム間隔の時間が長くなり人物などの物体の移動量も大きくなるため、フレームレートが高い場合よりもR O I 4 1を広くすることが考えられる。

[0143] なお、ターゲット領域A Tについて、特定部位とそれ以外の領域とを区別して暗号化を行う場合には、特定部位について、上記で説明した手法と同様の手法によりバウンディングボックス4 0及びR O I 4 1を算出し、算出したR O I 4 1に第三乱数の数値を適用した第三暗号鍵を生成する。その上で、第一、第二、第三暗号鍵を合成した合成鍵を生成し、次のフレームの画像の暗号化に用いるようにすればよい。

[0144] [2-3. 第二実施形態としての改竄検知手法]

続いて、上記のように受信装置3側が有する鍵のレベルごとに復号化可能な画像範囲が異なるように撮像画像データが暗号化される場合に対応して、

電子署名を用いた改竄検知を行うための手法について説明する。

この際、ポイントとなるのは、受信装置 3 側では自身が保有する鍵のレベルに応じた画像範囲しか暗号化画像を復号化できない点であり、保有する鍵のレベルが異なる受信装置 3 間では、復号化した画像から計算されるハッシュ値がそれぞれ異なる値になる。このため、撮像装置 1 側では、鍵のレベルが何れのレベルであっても各受信装置 3 が適正に改竄検知処理を実行可能となるように、それぞれの鍵のレベルに応じたハッシュ値を計算する。

[0145] 図 2 3 及び図 2 4 を参照し、このような受信装置 3 側の鍵の保有レベルの差を考慮した第二実施形態としての改竄検知手法について説明する。

ここでは説明上の一例として、鍵の保有レベルがそれぞれレベル 1 とレベル 2 の受信装置 3 に暗号化画像データと電子署名データとを送信する例を挙げる。先の図 1 8 を参照して説明したように、鍵の保有レベルとして、レベル 1 は、ターゲット領域 A T 全域のみが暗号化された画像が得られるレベルであり、レベル 2 は、ターゲット領域 A T における特定領域 A S のみが暗号化された画像が得られるレベルである。

[0146] 図 2 3 は、撮像装置 1 が受信装置 3 への画像送信時に行う処理を模式的に表している。

まず、送信対象の撮像画像データは、本例では、第一、第二、及び第三暗号鍵の合成鍵により暗号化された画像データとされる。以下では説明上、該合成鍵で暗号化された撮像画像データを「暗号化画像データ G c」と表記する。

撮像装置 1 は、レベル 1 の受信装置 3 に送信すべきハッシュ値として、この暗号化画像データ G c を第一暗号鍵で復号化して得た画像データのハッシュ値（以下「ハッシュ値 H 1」と表記する）を計算する。レベル 1 の受信装置 3 に対しては、このように計算したハッシュ値 H 1 を署名生成鍵としての秘密鍵（第一実施形態と同様、光電乱数に基づき生成される）により暗号化した値と、該秘密鍵に基づき生成した署名検証鍵としての公開鍵とを暗号化画像データ G c と共に送信する。

[0147] 一方、撮像装置 1 は、レベル 2 の受信装置 3 に送信すべきハッシュ値として、暗号化画像データ G_c を第一及び第二暗号鍵の合成鍵で復号化して得た画像データのハッシュ値（以下「ハッシュ値 H_2 」と表記する）を計算する。そして、レベル 2 の受信装置 3 に対しては、このように計算したハッシュ値 H_2 を署名生成鍵としての秘密鍵により暗号化した値と、署名検証鍵としての公開鍵とを暗号化画像データ G_c と共に送信する。

[0148] 図 24 は、受信装置 3 側の処理を模式的に表している。

レベル 1 の受信装置 3 では、撮像装置 1 から受信した暗号化画像データ G_c を、自身が保有する第一暗号鍵により復号化し、該復号化した画像データについてのハッシュ値（以下「ハッシュ値 H_{1a} 」と表記する）を計算する。また、レベル 1 の受信装置 3 では、撮像装置 1 から受信した、秘密鍵により暗号化されたハッシュ値 H_1 を公開鍵により復号化する。この復号化により得られた値をハッシュ値 H_{1b} と表記する。そして、レベル 1 の受信装置 3 は、ハッシュ値 H_{1a} とハッシュ値 H_{1b} の一致判定を行う。

[0149] レベル 2 の受信装置 3 では、撮像装置 1 から受信した暗号化画像データ G_c を自身が保有する第一及び第二暗号鍵の合成鍵により復号化し、該復号化した画像データについてのハッシュ値（以下「ハッシュ値 H_{2a} 」と表記する）を計算する。さらに、レベル 2 の受信装置 3 では、撮像装置 1 から受信した、秘密鍵により暗号化されたハッシュ値 H_2 を公開鍵により復号化する。この復号化により得られた値をハッシュ値 H_{2b} とすると、レベル 2 の受信装置 3 は、ハッシュ値 H_{2a} とハッシュ値 H_{2b} の一致判定を行う。

[0150] ここで、電子署名の手法において、ハッシュ値は、改竄検知の対象データの記録時において生成されることが一般的である。しかしながら、本例のように受信装置 3 側の鍵のレベルに応じて復号化可能な画像範囲を異ならせる手法を採る場合においては、各レベルのハッシュ値（上記例では H_1 、 H_2 ）を生成する必要がある、これらのハッシュ値を撮像画像データの記録時に一度に生成しようとする処理が重くなり、処理遅延を招く虞がある。

[0151] このため、本例では、各レベルのハッシュ値の生成は、受信装置 3 からの

送信要求に応じた暗号化画像データ G c の送信時に行う。これにより、ハッシュ値の生成は、送信要求が行われた際に、該送信要求を行った受信装置 3 の鍵のレベルについてのみ行えば済み、撮像画像データの記録時に各レベルのハッシュ値を一度に生成する必要がなくなる。

従って、ハッシュ値の生成に伴う処理遅延の抑制を図ることができる。

[0152] 図 25 のフローチャートを参照し、上記により説明した第二実施形態としての改竄検知手法を実現するための撮像装置 1 側の処理手順の例を説明する。

なお本例において、図 25 に示す処理は、制御部 23 が実行する。

[0153] 先ず、制御部 23 は、ステップ S 501 で受信装置 3 側からの送信要求を待機する。すなわち、暗号化画像データ G c の送信要求を待機する。

続くステップ S 502 で制御部 23 は、受信装置 3 のレベル情報を取得する。すなわち、送信要求を行った受信装置 3 が保有する復号鍵のレベルを表す情報を取得する。本例では、該レベルの情報は、受信装置 3 が送信要求と共に撮像装置 1 に送信するものとする。

[0154] ステップ S 502 に続くステップ S 503 で制御部 23 は、暗号化画像データ G c を受信装置 3 のレベルに応じた復号レベルで復号化する。すなわち、メモリ部 24 に記憶されている暗号化画像データ G c を、ステップ S 402 で取得したレベル情報に応じた復号鍵により復号化する。具体的には、レベル 1 であれば、第一暗号鍵による復号化を行い、レベル 2 であれば第一及び第二暗号鍵の合成鍵による復号化を行うといったように、受信装置 3 の鍵の保有レベルに応じた復号鍵による復号化を行う。

[0155] ステップ S 503 に続くステップ S 504 で制御部 23 は、復号化された画像データのハッシュ値を計算し、さらに続くステップ S 505 で、該ハッシュ値を秘密鍵により暗号化する。

さらに、制御部 23 は続くステップ S 506 で、暗号化画像データ G c 、暗号化したハッシュ値、及び公開鍵を要求元の受信装置 3 に対して送信し、図 25 に示す一連の処理を終える。

確認のため述べておくと、ステップS506で送信する公開鍵は、光電乱数に基づき生成した署名生成鍵としての秘密鍵に基づき生成した署名検証鍵としての公開鍵である。

上記では、該公開鍵とその対となる秘密鍵について、各レベルで共通の鍵を使用する例を挙げたが、これら公開鍵及び秘密鍵はレベルごとに異なる鍵を用いることもできる。

[0156] [2-4. 受信者側が有する公開鍵の確認プロセス]

ここでは、受信装置3側の鍵のレベルに応じて復号化可能な画像範囲を異ならせる手法を採る場合において、受信装置3が有する公開鍵が適正な公開鍵であるかの確認プロセスの例を説明する。なお、ここで言う公開鍵は、電子署名用の公開鍵ではなく、共通鍵としての画像暗号鍵（暗号化フィルタ）を受信装置3側にセキュアに受け渡すために用いる公開鍵（図11の説明を参照）を指す。

なお、以下の図26から図30の説明においても、鍵の保有レベルがそれぞれレベル1とレベル2の受信装置3を例に挙げるが、他の保有レベルの受信装置3についても同様の処理を行えばよい。

[0157] 先ず、図26に示すように、各レベルの受信装置3は、秘密鍵と公開鍵を保有しており、それぞれ自身が保有する公開鍵を撮像装置1に対して送信する。

[0158] そして、図27に示すように、撮像装置1は、光電乱数をハッシュ化したハッシュ値Hdを生成する。

その後、撮像装置1は、受信装置3のレベルごとに、光電乱数を対応するレベルの公開鍵で暗号化する。そして、レベル1の受信装置3に対しては、レベル1の公開鍵により暗号化した光電乱数を送信し、レベル2の受信装置3に対してはレベル2の公開鍵により暗号化した光電乱数を送信する。

[0159] 各レベルの受信装置3側では、図28に示すように、自身が保有するレベルの秘密鍵により、公開鍵で暗号化された光電乱数を復号化する。そして、各レベルの受信装置3は、復号化した光電乱数からハッシュ値を計算し、そ

れぞれ撮像装置 1 に送信する。

[0160] 撮像装置 1 では、各レベルの受信装置 3 から受信したハッシュ値について、図 27 で計算した元々のハッシュ値 H_d との一致判定を行う。

撮像装置 1 は、受信したハッシュ値がハッシュ値 H_d と一致する場合には、該ハッシュ値を送信した受信装置 3 を正式な受信者として登録する。

[0161] [2-5. 送信者側が有する電子署名公開鍵の確認プロセス]

続いて、撮像装置 1 が有する電子署名公開鍵が適正な公開鍵であるかの確認プロセスの例を説明する。具体的に、ここで説明する確認プロセスは、撮像装置 1 が保有している電子署名公開鍵（署名検証鍵としての公開鍵）が適正な公開鍵であるか否かを各レベルの受信装置 3 側で確認するプロセスとなる。

[0162] 先ず、撮像装置 1 は、図 29 に示すように、自身が保有しているレベル 1 向けの電子署名公開鍵、レベル 2 向けの電子署名公開鍵をそれぞれのレベルの公開鍵で暗号化する。この暗号化に用いる各レベルの公開鍵は、先の図 26 で説明したように各レベルの受信装置 3 が送信して撮像装置 1 が保有するに至った公開鍵である。

撮像装置 1 は、レベル 1 の受信装置 3 に対しては、レベル 1 公開鍵で暗号化したレベル 1 向け電子署名公開鍵を送信し、レベル 2 の受信装置 3 に対してはレベル 2 公開鍵で暗号化したレベル 2 向け電子署名公開鍵を送信する。

[0163] 各レベルの受信装置 3 は、図 30 に示すように、撮像装置 1 から受信した暗号化された電子署名公開鍵を、自身の保有するレベルの秘密鍵で復号化する。

この一方で、各レベルの受信装置 3 は、ネットワーク上の認証局サーバ等の所定のサーバ装置から、撮像装置 1 に対応づけられて管理されている電子署名公開鍵を参照し、該参照した電子署名公開鍵と、上記のように復号化した電子署名公開鍵との一致判定を行う。各レベルの受信装置 3 は、双方の電子署名公開鍵が一致する場合には、撮像装置 1 を想定している適正な送信者として登録する。

[0164] ここで、電子署名公開鍵の持ち主の情報は公開情報としてネットワーク上で管理されており、確認が可能とされている。この確認のためのシステムについては特に限定はされないが、例えばPGP (Pretty Good Privacy) 方式やPKI (Public Key Infrastructure) 方式のシステムを挙げることができる。

[0165] <3. 第三実施形態>

続いて、第三実施形態について説明する。

第三実施形態は、ブロックチェーンシステムにおける電子署名用の秘密鍵を光電乱数に基づき生成するものである。

ここで、ブロックチェーンは、複数の取引データを含むブロックを時系列に沿って繋げたものを意味する。ブロックチェーンシステムとは、このようなブロックチェーンを扱うシステムであって、P2P (Peer to Peer) ネットワークを利用して取引データ(トランザクション)を分散して管理し合うシステムを意味する。

[0166] 図31は、ブロックチェーンシステムのハードウェア構成を例示したブロック図である。

図示のようにブロックチェーンシステムにおいては、複数のユーザ端末50のそれぞれが、例えばインターネットとしてのネットワーク2に接続され、それぞれのユーザ端末50は、ネットワーク2を介して相互にデータ通信を行うことが可能とされている。

[0167] 図32は、ユーザ端末50の内部構成例を示したブロック図である。

図示のようにユーザ端末50は、図3に示した受信装置3と同様の構成を有した上で、入出力インタフェース35にカメラ部51が接続されている。カメラ部51は、少なくとも図2に示したアレイセンサ12を有し、前述したシードフレームとしての画像データを生成可能に構成されている。

[0168] ブロックチェーンシステムでは、ネットワーク2に接続されたユーザ端末50が、電子署名用の秘密鍵を生成する。

ブロックチェーンシステムでは、この秘密鍵から公開鍵が生成され、該公

公開鍵に基づいてブロックチェーンアドレスが生成される。ブロックチェーンアドレスは、銀行口座に例えると口座番号に相当する情報であり、ブロックチェーンシステムにおける仮想通貨の取引は、ブロックチェーンアドレス間で通貨をやりとりすることにより行われる。

また、ブロックチェーンシステムにおいて秘密鍵から生成された公開鍵は、秘密鍵により暗号化されP2Pネットワークにブロードキャストされたトランザクションの改竄検知に用いられる。すなわちこの場合における秘密鍵や公開鍵は、取引が正当に行われたか否かをチェックするために使用される。

[0169] ブロックチェーンシステムにおいても、秘密鍵の生成には乱数が用いられるが、この乱数の予測が容易であると秘密鍵を解読され易くなる、すなわち不正取引が成立し易くなる。このため、該乱数はブロックチェーンシステムのセキュリティを高める上で重要な役割を担う。

[0170] そこで、第三実施形態では、ブロックチェーンシステムにおける電子署名用の秘密鍵を光電乱数に基づき生成する。

具体的に、ユーザ端末50におけるCPU31は、電子署名用の秘密鍵を生成するにあたり、カメラ部51にシードフレームとしての画像データを生成させる。そして、該画像データの各画素の電気信号値を光電乱数として取得し、該光電乱数に基づいて秘密鍵の生成を行う。

これにより、ブロックチェーンシステムにおける電子署名用の秘密鍵について、疑似乱数を用いる場合より解読を困難化することが可能とされる。

[0171] ここで、ブロックチェーンシステムをベースに、取引の契約（コントラクト）を人の手を介さず自動で実行させる仕組みとしてスマートコントラクトシステム（以下「SCシステム」と表記する）が知られている。

SCシステムでは、特定の条件を満たした場合に自動で契約内容が実行されるよう、予めプログラムされており、そのためトラストレスな取引が可能とされる。なお、トラストレスな取引とは、第三者の仲介を必要とせず、当事者間のみでデジタル取引を行うことを意味する。

[0172] SCシステムでは、ブロックチェーンシステム上でコントラクトの検証作業者の選出を行う際に、その選出を公正に行う目的で乱数が活用されているが、この乱数の予測が容易であると意図的な検証作業者の選出が可能となつて、検証作業者の選出の公正性が失われる虞がある。

[0173] そこで、本実施形態では、SCシステムにおけるコントラクト検証作業者の選出を、光電乱数に基づき行う。

図33は、SCシステムの構成を概念的に表した図である。

SCシステムにおいては、ブロックチェーンシステム上に各種のユーザ端末50が存在する。図中のスマートコントラクトアプリケーションは、スマートコントラクトのサービスを享受するユーザ端末50やスマートコントラクトの運用を管理するユーザ端末50の集合を表している。また、図中の検証者グループは、コントラクト検証作業者としてのユーザ端末50の集合を表している。

[0174] 図33に例示するようにスマートコントラクトの検証作業者は複数のグループ（検証者グループ）に分かれていて、各グループ内で検証作業者同士がデータを同期し合っている場合がある。

このような場合においては、複数の検証者グループのうちから所定数の検証者グループを選出するということが行われ得る。そのような場合、スマートコントラクトアプリケーションにおける選出者としてのユーザ端末50が、検証者グループの選出を光電乱数に基づいて行う。

また、グループ内で検証作業者のリーダー（図中、検証者リーダー）を選出する場合もあり、その場合には、上記選出者としてのユーザ端末50が、該リーダーの選出を光電乱数に基づいて行う。

なお、上記のような検証者グループの選出は、複数の検証作業者を選出するものと換言することができる。

[0175] 選出者としてのユーザ端末50において、上記のような検証者グループの選出やリーダーの選出は、CPU31がカメラ部51に生成させたシードフレームとしての画像データの各画素の電気信号値を光電乱数として取得し、

該光電乱数に基づいて行う。

[0176] また、第三実施形態の他の例として、D A p p s (Decentralized Applications: 自律分散型アプリケーション) における代表者選出に光電乱数を用いることも可能である。

ここで、D A p p s は、ブロックチェーン技術を利用したアプリケーションである。

[0177] D A p p s には、ゲームを中心にアプリケーションが多く開発されている。例えば、D A p p s としては、所要の仮想通貨システムをベースとして、サービス享受者にランダムに報酬が得られるようなアプリケーションが想定される。この際、報酬の得られる代表者を選出するために、D A p p s では、R N G (Random Number Generator) が用いられる。

しかしながら、R N G により生成される乱数が予測可能な場合には、特定のサービス享受者が不正に報酬を得ることが可能となってしまう、サービスの公正性を欠くものとなる。

[0178] そこで、D A p p s によるサービス享受者からの代表者選出に光電乱数を用い、公正性を高めることが考えられる。

この場合は、ブロックチェーンシステムにおける上記代表者の選出を行うユーザ端末50において、C P U 31が、カメラ部51に生成させたシードフレームとしての画像データの各画素の電気信号値を光電乱数として取得し、該光電乱数に基づいて上記代表者の選出を行う。

[0179] なお、第三実施形態においても、光電乱数としては、図4で説明したような画素位置をシャッフルさせたものを用いることもできる。

また、第三実施形態においても、光電乱数の元となった画像データをメモリ上から消去することもでき、また、外部からの不正アクセスが検知されたことに応じて光電乱数を再生成することもできる。第三実施形態において、上記の消去や光電乱数の再生成の指示は例えばC P U 31が行うようにする。

[0180] <4. 変形例>

なお、実施形態としては、これまでに説明した具体例に限定されるものではなく多様な変形例が考えられる。

例えば、第一、第二実施形態では、電子署名の対象データが画像データとされる場合を例示したが、本技術は、例えばテキストデータや音声データ等、各種データについて電子署名を用いた改竄検知を行う場合に広く好適に適用することができる。

また、上記では光電乱数に基づく秘密鍵の生成を撮像用センサ部10の外部で行う例を挙げたが、光電乱数に基づく秘密鍵の生成は撮像用センサ部10内部にて行う（例えば、演算部18において生成する）こともできる。

[0181] また、光電乱数に基づく暗号化については、以下のような変形例としての手法を採ることもできる。

一つは、通常のイメージセンサでは低減させている暗電流ノイズや読み出しノイズを高いランダム性の生成に応用するものである。具体的には、乱数のシードフレーム撮像時において、露光時間（蓄積時間）を減らす一方でアンプの増幅率を上げることで、熱雑音による暗電流ノイズを増やす手法を挙げることができる。或いは、読み出しノイズを減らす回路（例：適応ゲイン型の増幅器などのノイズ低減の為の回路）をオフにして読み出しを行った結果得られる撮像画像をシードフレームとして用いる手法も挙げることができる。

また、別手法として、ベイヤー配列などカラーフィルタ（波長フィルタ）が規則的に配列されたイメージセンサを用いる場合に、何れか一色のフィルタ（一つの波長帯のフィルタ）の画素のみを参照して乱数生成のシードフレームとして利用することも考えられる。例えば、ベイヤー配列であれば、赤色の画素のみを参照する等である。

これらの手法を採ることで、よりランダム性の高い乱数生成を行うことが可能となる。

[0182] また、上記では、電子署名の対象データの暗号化に関して、光電乱数に基づく暗号化を行う例を挙げたが、該対象データの暗号化に用いる乱数は光電

乱数に限定されない。例えば、疑似乱数を用いることもできる。或いは、真の乱数を用いるのであれば、例えば熱や音の変化など、予測や再現が実質的に不可能な自然現象を対応するセンサで検知して、その値を基に乱数を生成する手法を挙げることができる。

また、電子署名の対象データを暗号化することは必須ではない。

[0183] <5. 実施形態のまとめ>

上記のように実施形態の暗号鍵生成装置（撮像装置 1 又はユーザ端末 5 0）は、可視光又は非可視光の受光素子を有する画素が一次元又は二次元に複数配列されたアレイセンサ（同 1 2）による光電変換に基づき得られる乱数である光電乱数に基づき、電子署名用の秘密鍵を生成する鍵生成部（制御部 2 3 又は CPU 3 1：ステップ S T 2 参照）を備えたものである。

これにより、電子署名用の秘密鍵について、疑似乱数を用いる場合よりも解読を困難化することが可能とされる。

従って、改竄検知性能の向上を図ることができる。

[0184] また、実施形態としての暗号鍵生成装置においては、鍵生成部は、画像データについての電子署名用の秘密鍵を生成している。

これにより、電子署名の対象データが画像データとされる場合に対応して、電子署名用の秘密鍵について、疑似乱数を用いる場合よりも解読を困難化することが可能とされる。

従って、画像データについての改竄検知性能向上を図ることができる。

[0185] さらに、実施形態としての暗号鍵生成装置においては、鍵生成部は、アレイセンサでの撮像により得られる画像データについての電子署名用の秘密鍵を生成している。

これにより、画像データを得るためのアレイセンサが、光電乱数を得るためのアレイセンサと共通化される。

従って、画像データを生成するアレイセンサとは別途に光電乱数生成用のアレイセンサを設ける必要がなくなり、部品点数の削減、及びコスト削減を図ることができる。

[0186] さらにまた、実施形態としての暗号鍵生成装置においては、アレイセンサでの撮像により得られる画像データの暗号化を行う暗号化部（振幅制御回路19又は19A、演算部18）と、暗号化部により暗号化された画像データを外部装置に送信する処理を行う送信処理部（制御部23：ステップS204、S506参照）を備えている。

これにより、電子署名の対象データとしての画像データをセキュアに送信することが可能とされる。

従って、画像内容の漏洩防止の面でのセキュリティ向上を図ることができる。

[0187] また、実施形態としての暗号鍵生成装置においては、暗号化部は、光電乱数に基づき生成した暗号鍵により画像データの暗号化を行っている。

これにより、画像データの暗号化についても、疑似乱数を用いる場合より暗号鍵の解読を困難化することが可能とされる。

従って、セキュリティのさらなる向上を図ることができる。

[0188] さらに、実施形態としての暗号鍵生成装置においては、暗号化部は、画像データの復号に用いる復号鍵のレベルによって復号化可能な画像範囲が異なるように画像データを暗号化し、送信処理部は、外部装置が暗号化部により暗号化された画像データの送信要求を行ったことに応じて、該外部装置が有する復号鍵と同レベルの復号鍵により暗号化された画像データを復号化し、復号化した画像データのハッシュ値を生成し、秘密鍵により暗号化した該ハッシュ値と暗号化された画像データとを外部装置に送信している（図23、図25参照）。

これにより、画像データの受信装置に対して該受信装置が有する復号鍵のレベルに応じたハッシュ値を送信すべき場合において、ハッシュ値の生成は、送信要求が行われた際に、該送信要求を行った受信装置の復号鍵のレベルについてのみ行えば済み、画像データ（撮像画像データ）の記録時に各レベルのハッシュ値を一度に生成する必要がなくなる。

従って、ハッシュ値の生成に伴う処理遅延の抑制を図ることができる。

[0189] さらにまた、実施形態としての暗号鍵生成装置においては、鍵生成部（CPU 31）は、光電乱数に基づき、ブロックチェーンシステムにおける電子署名用の秘密鍵を生成している。

これにより、ブロックチェーンシステムにおける電子署名用の秘密鍵について、疑似乱数を用いる場合より解読を困難化することが可能とされる。

従って、ブロックチェーンシステムにおける電子署名の対象データについて、改竄検知性能の向上を図ることができる。

[0190] また、実施形態としての暗号鍵生成装置においては、光電乱数に基づき、スマートコントラクトシステムにおけるコントラクト検証作業者の選出を行う検証者選出部（CPU 31：図33参照）を備えている。

これにより、コントラクト検証作業者の選出に用いる乱数について、疑似乱数を用いる場合より解読を困難化することが可能とされる。

従って、コントラクト検証作業者の選出について、公正性を高めることができる。

[0191] さらに、実施形態としての暗号鍵生成装置においては、光電乱数に基づき、DAppsによるサービスの享受者からの代表者の選出を行う代表者選出部（CPU 31）を備えている。

これにより、DAppsのサービス享受者からの代表者選出に用いる乱数について、疑似乱数を用いる場合より解読を困難化することが可能とされる。

従って、DAppsのサービス享受者からの代表者選出について、公正性を高めることができる。

[0192] さらにまた、実施形態としての暗号鍵生成装置においては、鍵生成部は、光電変換により得られる画素ごとの電気信号の値を光電乱数として取得して秘密鍵を生成している。

これにより、解読が困難な電子署名秘密鍵を生成することが可能とされる。

従って、改竄検知性能の向上を図ることができる。

[0193] また、実施形態としての暗号鍵生成装置においては、鍵生成部は、画素ごとの電気信号の値のうち少なくとも一部を、該電気信号の値が得られた画素位置とは異なる画素位置に割り当てた形式による光電乱数に基づき、秘密鍵を生成している。

これにより、画素ごとの電気信号の値をそれら電気信号の値が得られた画素位置にそのまま割り当てた光電乱数を用いる場合と比較して、電子署名秘密鍵の解読が困難とされる。

従って、改竄検知性能の向上を図ることができる。

[0194] さらに、実施形態としての暗号鍵生成装置においては、光電乱数の生成後、光電乱数の元となった画像データをメモリ上から消去するための処理を行う消去処理部（演算部 18 又は制御部 23 又は CPU 31：ステップ S106、ST1 等参照）を備えている。

これにより、光電乱数の元となった画像が流出して光電乱数が推定されてしまうことの防止を図ることが可能とされる。

従って、改竄検知性能の向上を図ることができる。

[0195] さらにまた、実施形態としての暗号鍵生成装置においては、暗号鍵生成装置外部からの不正アクセスが検知されたことに応じて光電乱数を再生成するための処理を行う再生成処理部（演算部 18 又は制御部 23 又は CPU 31：図 10、ステップ ST1 等参照）を備えている。

これにより、外部からの不正アクセスが検知された場合は、再生成した光電乱数に基づき電子署名秘密鍵を更新することが可能とされる。

従って、不正アクセスにより秘密鍵が外部流出したとしても、該流出した秘密鍵では改竄検知処理が適正に行われないように図ることができ、データ改竄の抑止効果向上を図ることができる。

[0196] また、実施形態の暗号鍵生成方法は、情報処理装置が、可視光又は非可視光の受光素子を有する画素が一次元又は二次元に複数配列されたアレイセンサによる光電変換に基づき得られる乱数である光電乱数に基づき、電子署名用の秘密鍵を生成する暗号鍵生成方法である。

このような暗号鍵生成方法によっても、上記した実施形態としての暗号鍵生成装置と同様の作用及び効果を得ることができる。

[0197] なお、本明細書に記載された効果はあくまでも例示であって限定されるものではなく、また他の効果があってもよい。

[0198] <6. 本技術>

本技術は以下のような構成も採ることができる。

(1)

可視光又は非可視光の受光素子を有する画素が一次元又は二次元に複数配列されたアレイセンサによる光電変換に基づき得られる乱数である光電乱数に基づき、電子署名用の秘密鍵を生成する鍵生成部を備えた暗号鍵生成装置。

(2)

前記鍵生成部は、
画像データについての電子署名用の秘密鍵を生成する
前記(1)に記載の暗号鍵生成装置。

(3)

前記鍵生成部は、
前記アレイセンサでの撮像により得られる画像データについての電子署名用の秘密鍵を生成する
前記(2)に記載の暗号鍵生成装置。

(4)

前記アレイセンサでの撮像により得られる画像データの暗号化を行う暗号化部と、
前記暗号化部により暗号化された前記画像データを外部装置に送信する処理を行う送信処理部を備えた
前記(3)に記載の暗号鍵生成装置。

(5)

前記暗号化部は、

前記光電乱数に基づき生成した暗号鍵により前記画像データの暗号化を行う

前記（４）に記載の暗号鍵生成装置。

（６）

前記暗号化部は、

前記画像データの復号に用いる復号鍵のレベルによって復号化可能な画像範囲が異なるように前記画像データを暗号化し、

前記送信処理部は、

前記外部装置が前記暗号化部により暗号化された前記画像データの送信要求を行ったことに応じて、該外部装置が有する前記復号鍵と同レベルの復号鍵により前記暗号化された前記画像データを復号化し、復号化した画像データのハッシュ値を生成し、前記秘密鍵により暗号化した該ハッシュ値と前記暗号化された前記画像データとを前記外部装置に送信する

前記（４）又は（５）に記載の暗号鍵生成装置。

（７）

前記鍵生成部は、

前記光電乱数に基づき、ブロックチェーンシステムにおける電子署名用の秘密鍵を生成する

前記（１）に記載の暗号鍵生成装置。

（８）

前記光電乱数に基づき、スマートコントラクトシステムにおけるコントラクト検証作業者の選出を行う検証者選出部を備える

前記（７）に記載の暗号鍵生成装置。

（９）

前記光電乱数に基づき、D A p p sによるサービスの享受者からの代表者の選出を行う代表者選出部を備える

前記（７）又は（８）に記載の暗号鍵生成装置。

（１０）

前記鍵生成部は、

前記光電変換により得られる前記画素ごとの電気信号の値を前記光電乱数として取得して前記秘密鍵を生成する

前記（１）から（９）の何れかに記載の暗号鍵生成装置。

（１１）

前記鍵生成部は、

前記画素ごとの電気信号の値のうち少なくとも一部を、該電気信号の値が得られた画素位置とは異なる画素位置に割り当てた形式による前記光電乱数に基づき、前記秘密鍵を生成する

前記（１０）に記載の暗号鍵生成装置。

（１２）

前記光電乱数の生成後、前記光電乱数の元となった画像データをメモリ上から消去するための処理を行う消去処理部を備えた

前記（１）から（１１）の何れかに記載の暗号鍵生成装置。

（１３）

暗号鍵生成装置外部からの不正アクセスが検知されたことに応じて前記光電乱数を再生成するための処理を行う再生成処理部を備えた

前記（１）から（１２）の何れかに記載の暗号鍵生成装置。

符号の説明

[0199] １ 撮像装置、２ ネットワーク、３ 受信装置、１０ 撮像用センサ部、１２ アレイセンサ、１３ ADC／ピクセルセクタ、１４ バッファ、１５ ロジック部、１６ メモリ、１７ インタフェース部、１８ 演算部、１９、１９Ａ 振幅制御回路、８１ キーフレーム選択部、８２ 物体領域認識部、８３ クラス識別部、８４ パラメータ選択部、８５ 暗号化制御部、８６ 不正アクセス検知部、２１ 画像プロセッサ、２２ センサ部、２３ 制御部、２４ メモリ部、２５ 通信部、３１ CPU、３２ ROM、３３ RAM、３４ バス、３５ 入出力インタフェース、３６ 入力部、３７ 出力部、３８ 記憶部、３９ 通信部、４０ バウンディング

グボックス、41 ROI

請求の範囲

- [請求項1] 可視光又は非可視光の受光素子を有する画素が一次元又は二次元に複数配列されたアレイセンサによる光電変換に基づき得られる乱数である光電乱数に基づき、電子署名用の秘密鍵を生成する鍵生成部を備えた
暗号鍵生成装置。
- [請求項2] 前記鍵生成部は、
画像データについての電子署名用の秘密鍵を生成する
請求項1に記載の暗号鍵生成装置。
- [請求項3] 前記鍵生成部は、
前記アレイセンサでの撮像により得られる画像データについての電子署名用の秘密鍵を生成する
請求項2に記載の暗号鍵生成装置。
- [請求項4] 前記アレイセンサでの撮像により得られる画像データの暗号化を行う暗号化部と、
前記暗号化部により暗号化された前記画像データを外部装置に送信する処理を行う送信処理部を備えた
請求項3に記載の暗号鍵生成装置。
- [請求項5] 前記暗号化部は、
前記光電乱数に基づき生成した暗号鍵により前記画像データの暗号化を行う
請求項4に記載の暗号鍵生成装置。
- [請求項6] 前記暗号化部は、
前記画像データの復号に用いる復号鍵のレベルによって復号化可能な画像範囲が異なるように前記画像データを暗号化し、
前記送信処理部は、
前記外部装置が前記暗号化部により暗号化された前記画像データの送信要求を行ったことに応じて、該外部装置が有する前記復号鍵と同

レベルの復号鍵により前記暗号化された前記画像データを復号化し、復号化した画像データのハッシュ値を生成し、前記秘密鍵により暗号化した該ハッシュ値と前記暗号化された前記画像データとを前記外部装置に送信する

請求項 4 に記載の暗号鍵生成装置。

[請求項7]

前記鍵生成部は、

前記光電乱数に基づき、ブロックチェーンシステムにおける電子署名用の秘密鍵を生成する

請求項 1 に記載の暗号鍵生成装置。

[請求項8]

前記光電乱数に基づき、スマートコントラクトシステムにおけるコントラクト検証作業者の選出を行う検証者選出部を備える

請求項 7 に記載の暗号鍵生成装置。

[請求項9]

前記光電乱数に基づき、D A p p s によるサービスの享受者からの代表者の選出を行う代表者選出部を備える

請求項 7 に記載の暗号鍵生成装置。

[請求項10]

前記鍵生成部は、

前記光電変換により得られる前記画素ごとの電気信号の値を前記光電乱数として取得して前記秘密鍵を生成する

請求項 1 に記載の暗号鍵生成装置。

[請求項11]

前記鍵生成部は、

前記画素ごとの電気信号の値のうち少なくとも一部を、該電気信号の値が得られた画素位置とは異なる画素位置に割り当てた形式による前記光電乱数に基づき、前記秘密鍵を生成する

請求項 1 0 に記載の暗号鍵生成装置。

[請求項12]

前記光電乱数の生成後、前記光電乱数の元となった画像データをメモリ上から消去するための処理を行う消去処理部を備えた

請求項 1 に記載の暗号鍵生成装置。

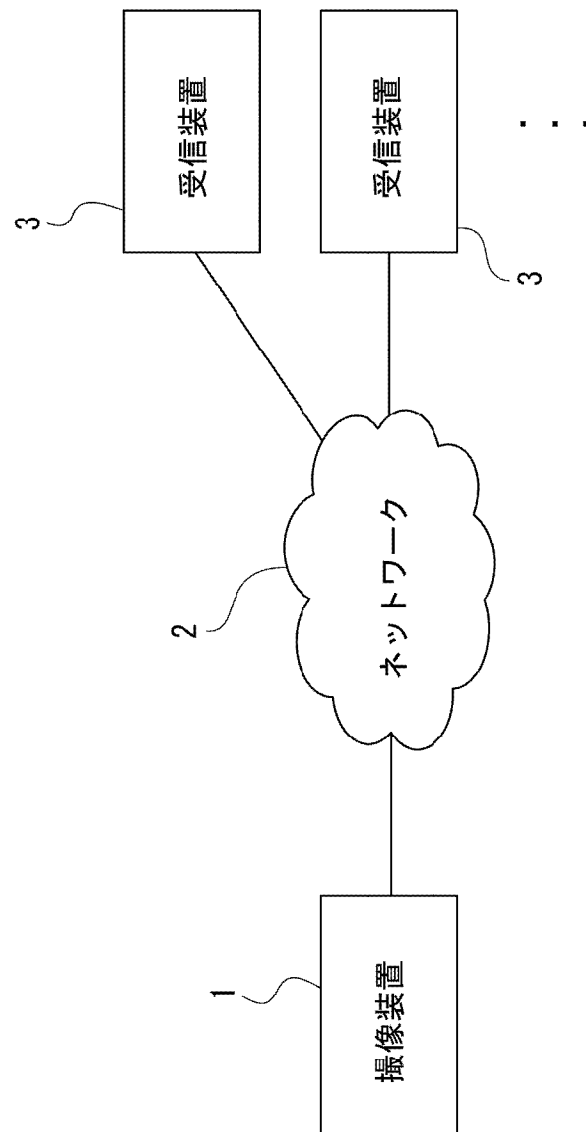
[請求項13]

暗号鍵生成装置外部からの不正アクセスが検知されたことに応じて

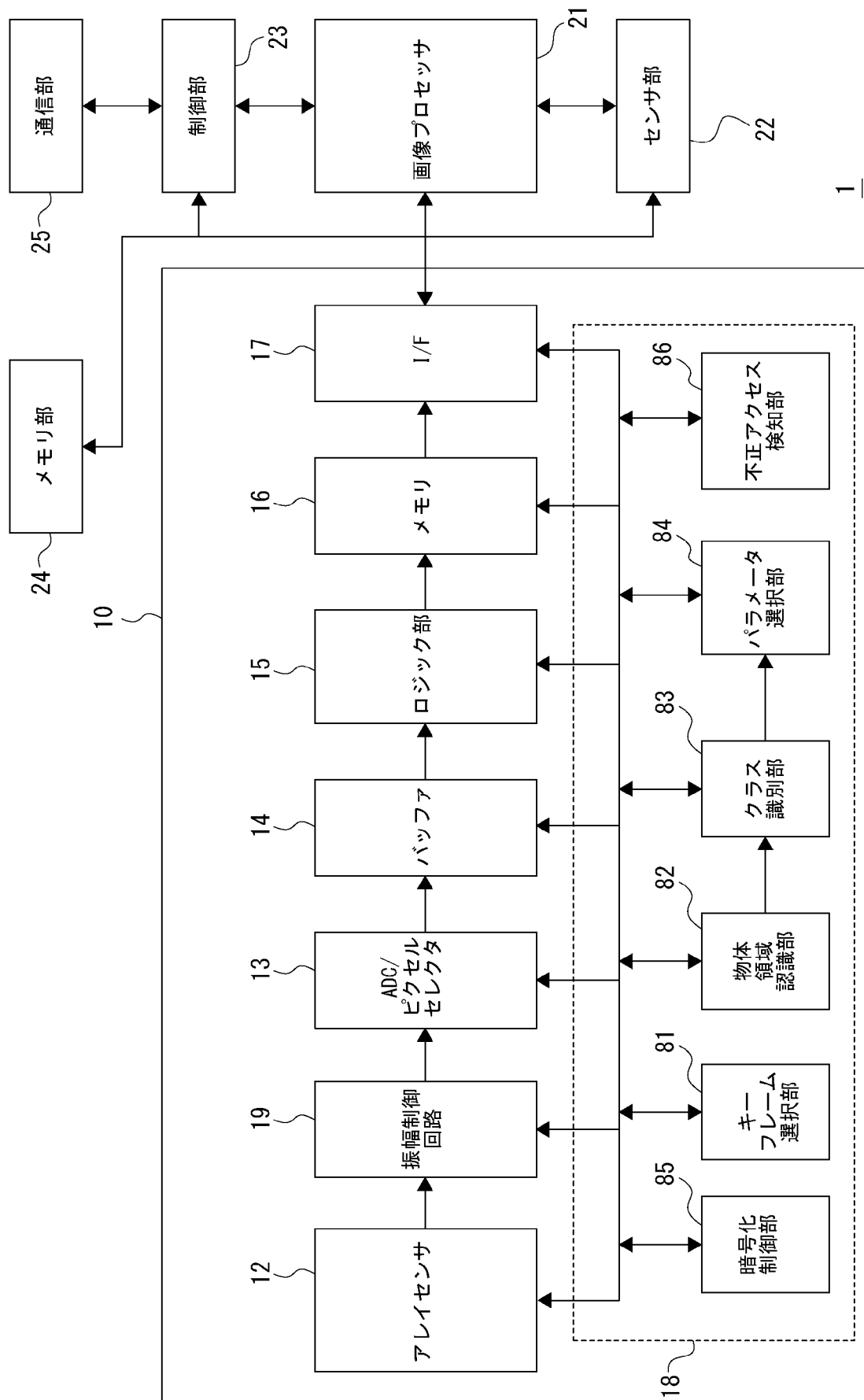
前記光電乱数を再生成するための処理を行う再生成処理部を備えた
請求項 1 に記載の暗号鍵生成装置。

[請求項14] 情報処理装置が、可視光又は非可視光の受光素子を有する画素が一次元又は二次元に複数配列されたアレイセンサによる光電変換に基づき得られる乱数である光電乱数に基づき、電子署名用の秘密鍵を生成する
暗号鍵生成方法。

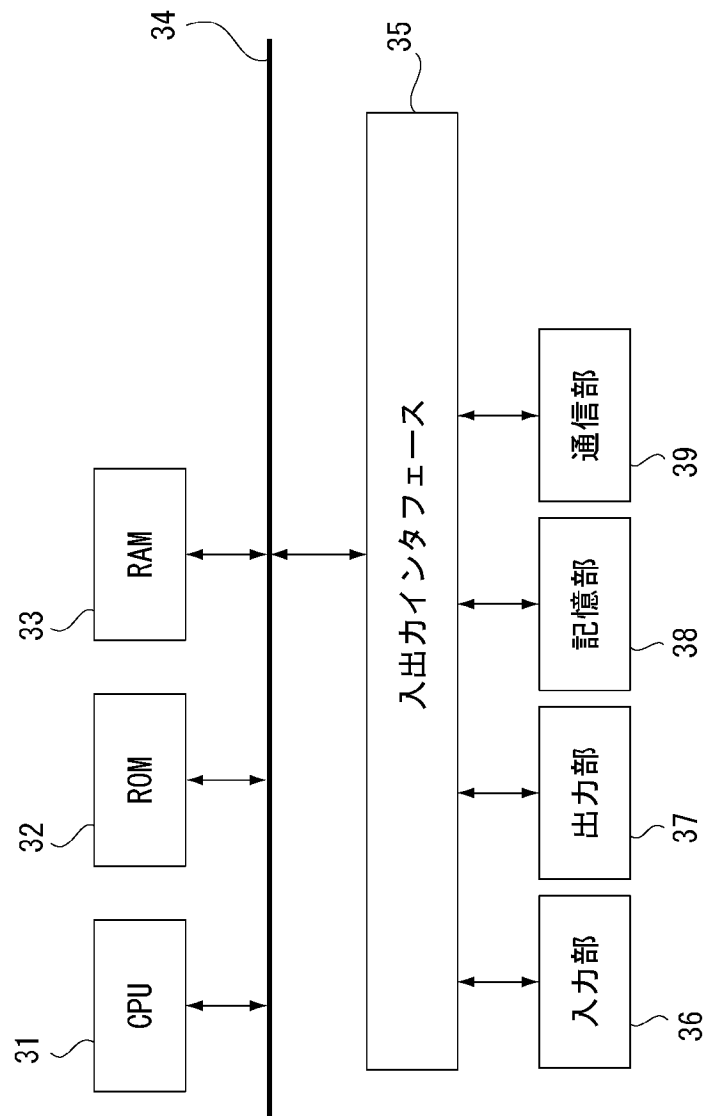
[図1]



[図2]



[図3]



[図4]

V1	V2	V3	V4	V5	V6
V7	V8	V9	V10	V11	V12
V13	V14	V15	V16	V17	V18
V19	V20	V21	V22	V23	V24
V25	V26	V27	V28	V29	V30
V31	V32	V33	V34	V35	V36

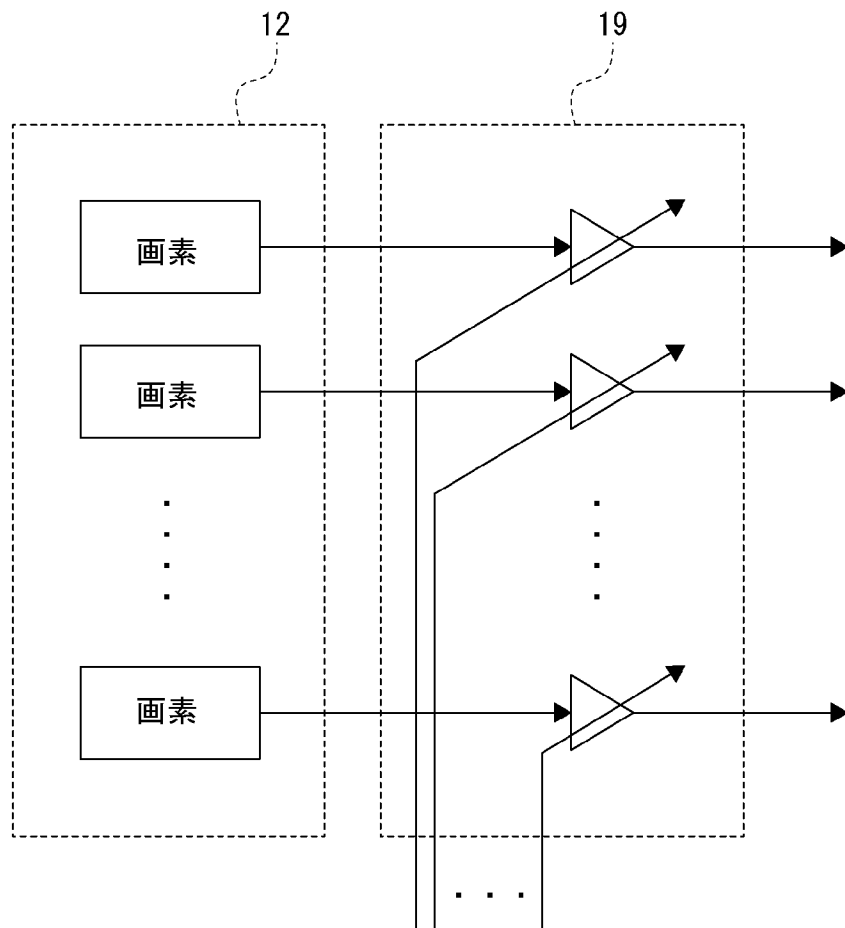
静止画（シードフレーム）



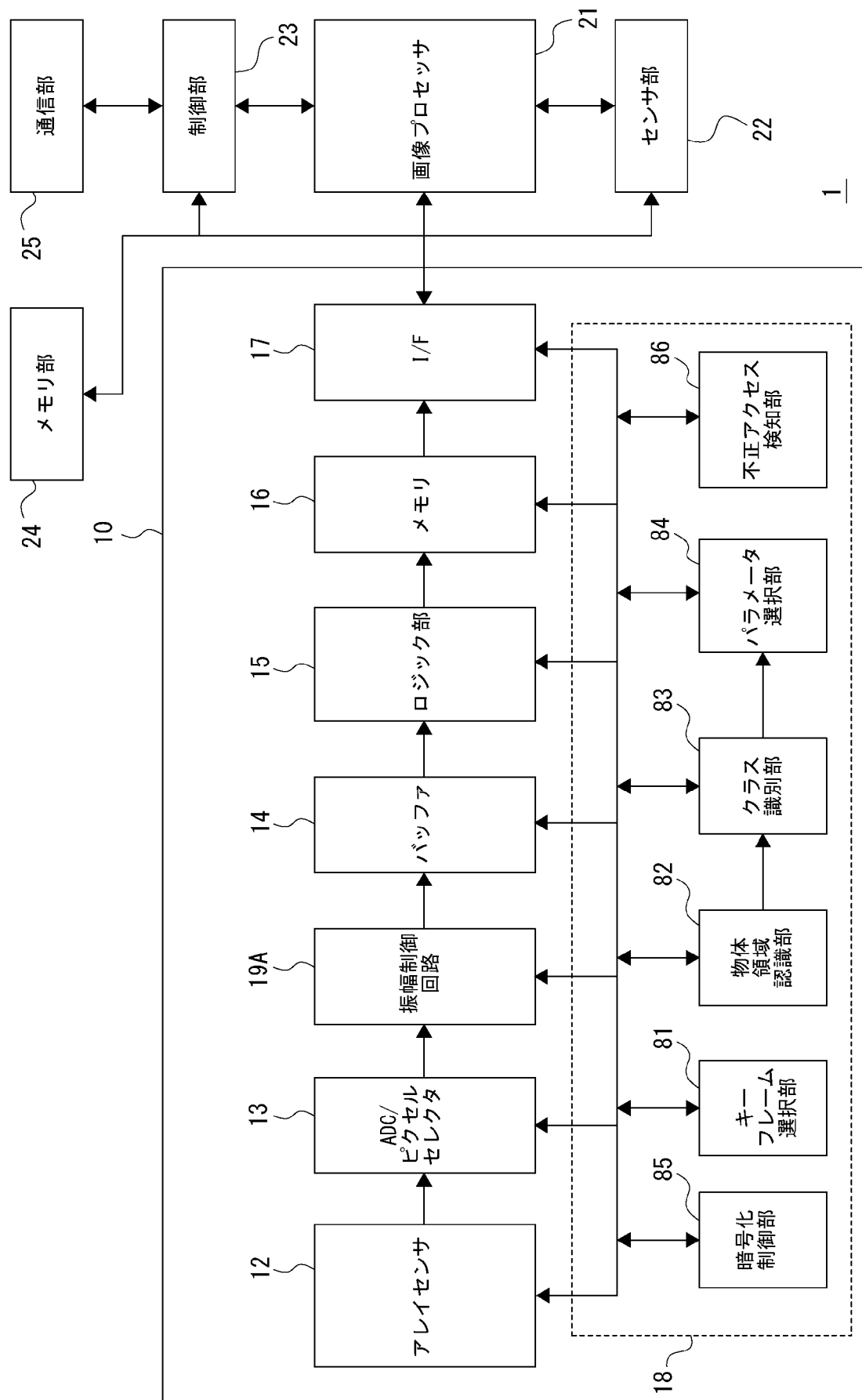
V26	V30	V29	V27	V25	V28
V20	V24	V23	V21	V19	V22
V2	V6	V5	V3	V1	V4
V14	V18	V17	V15	V13	V16
V32	V36	V35	V33	V31	V34
V8	V12	V11	V9	V7	V10

暗号化フィルタ（暗号鍵）

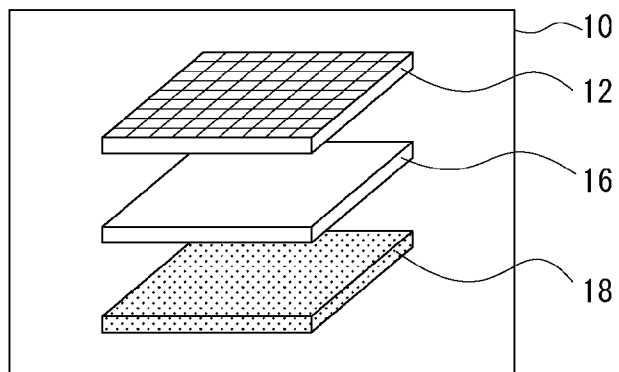
[図5]



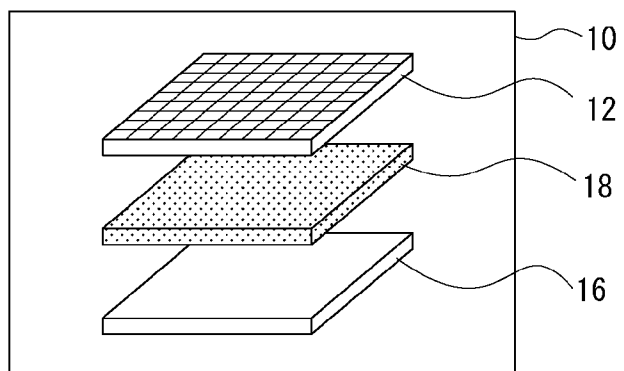
[図6]



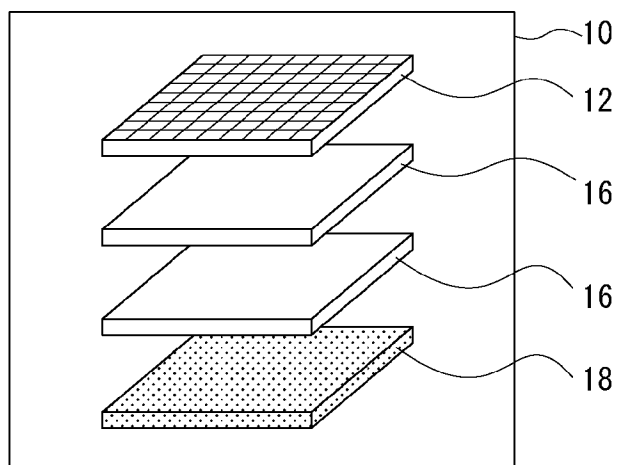
[図7]



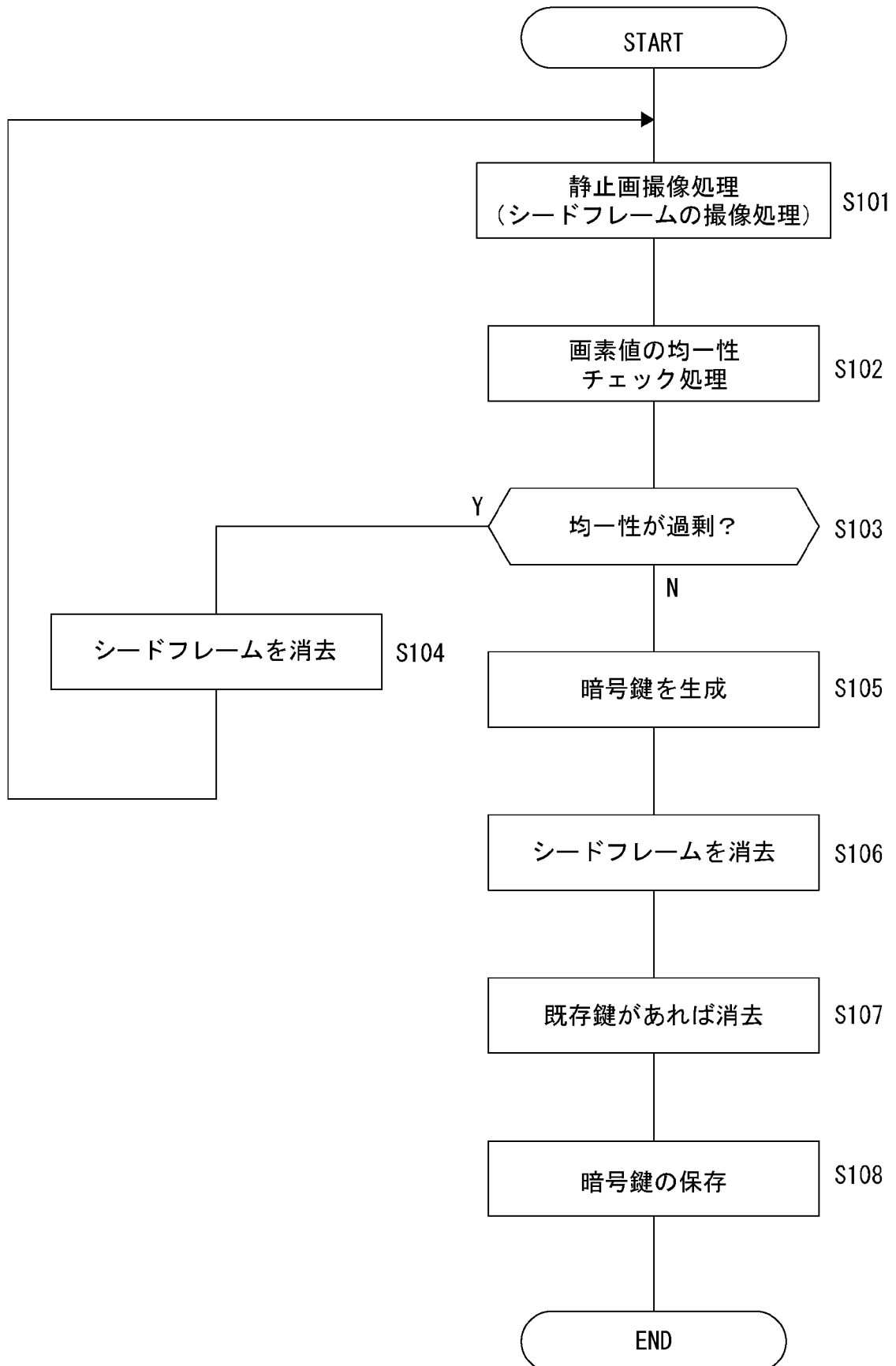
[図8]



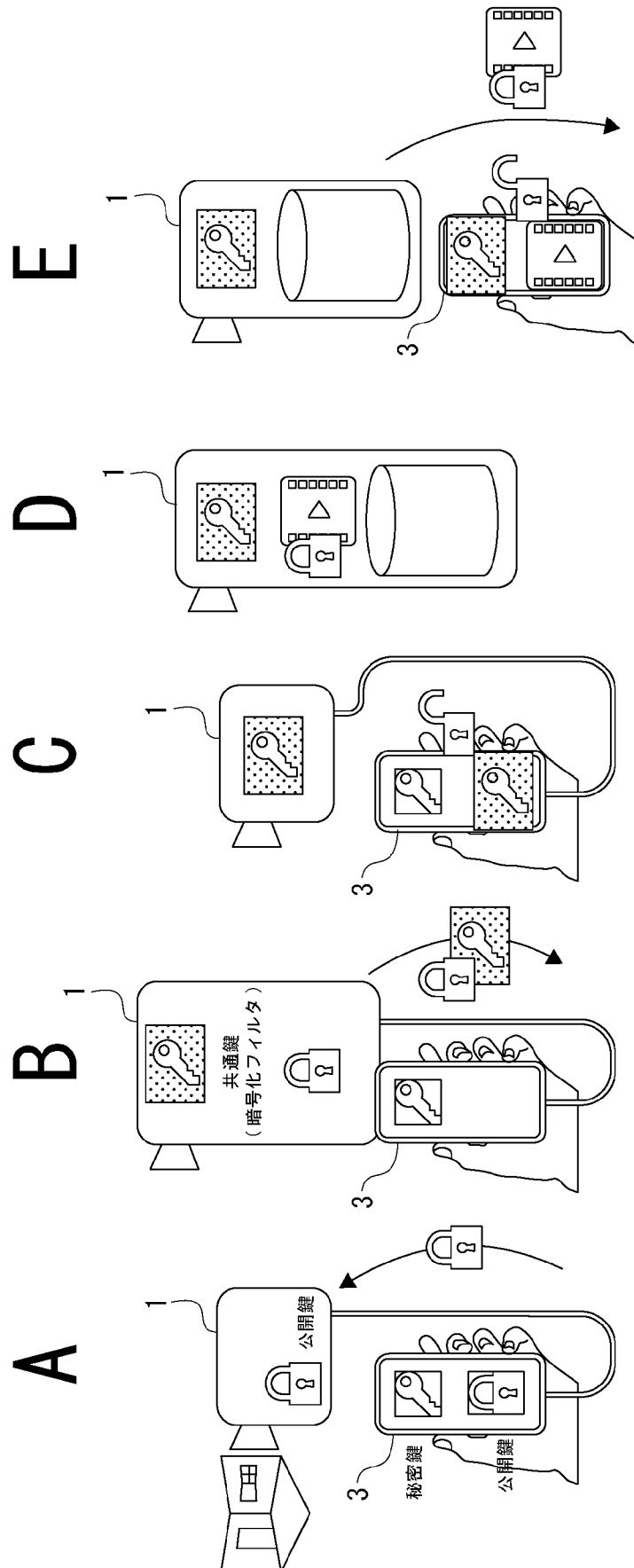
[図9]



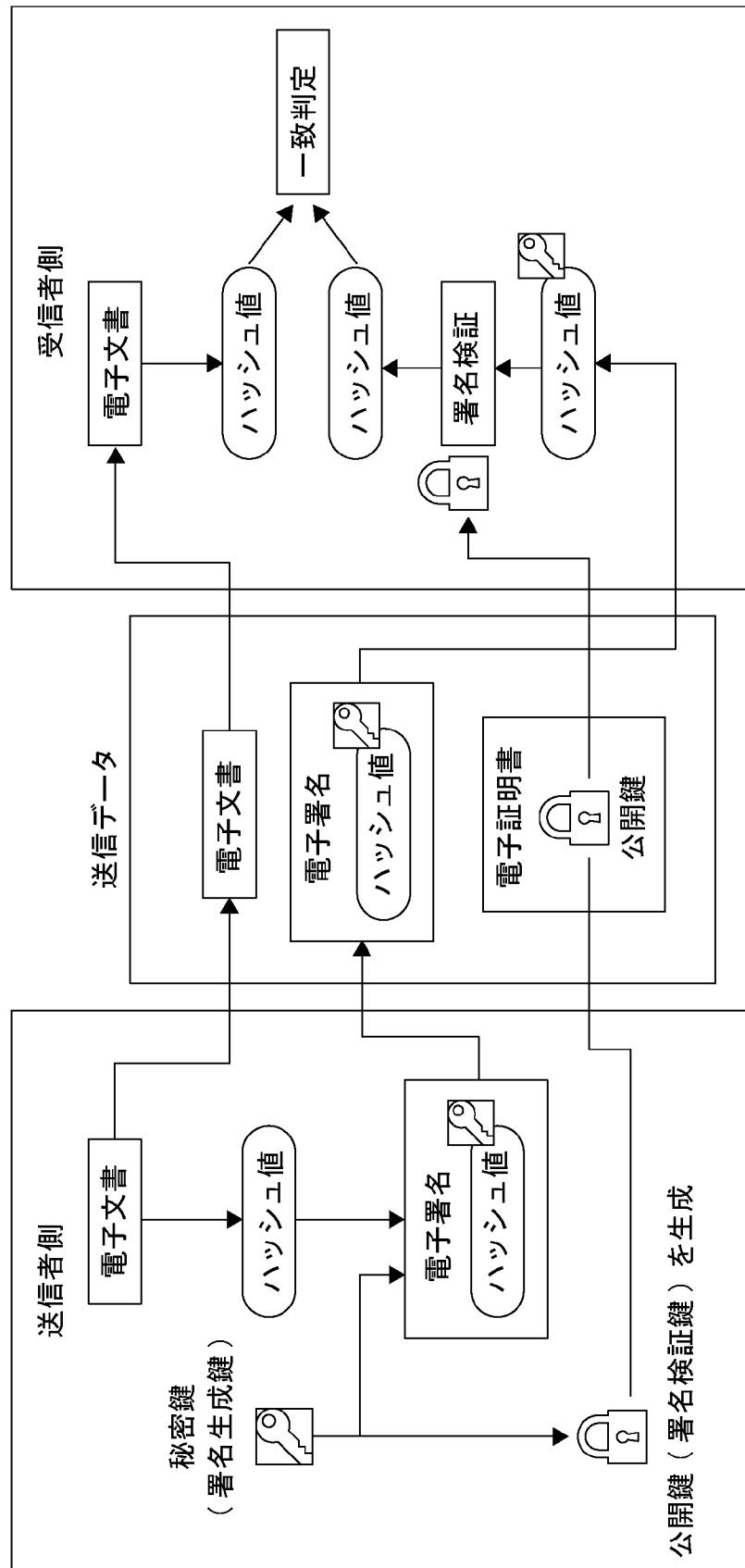
[図10]



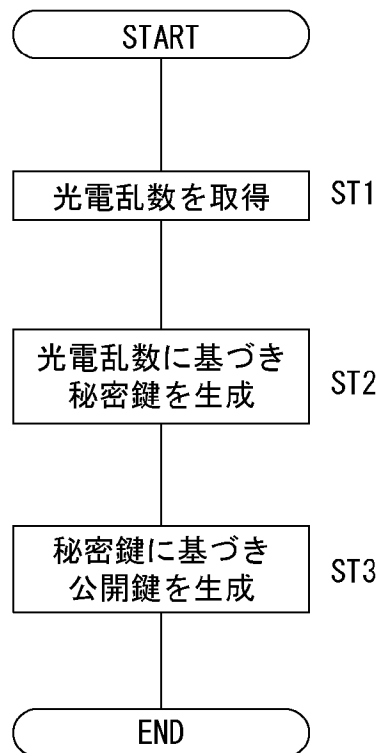
[図11]



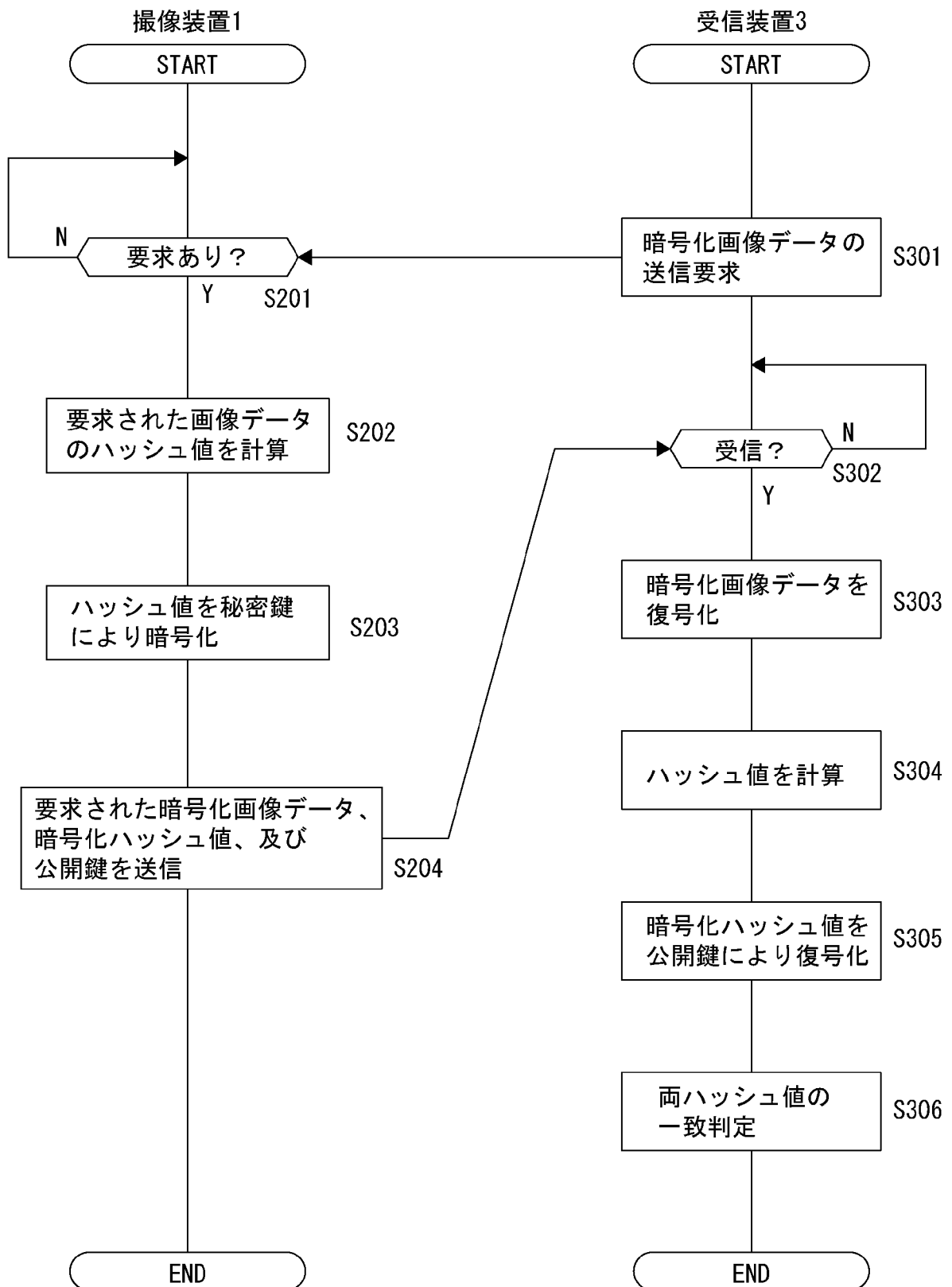
[図12]



[図13]



[図14]



[図15]

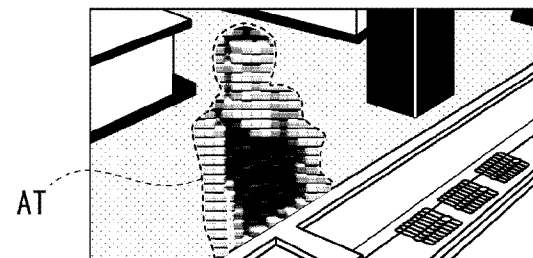
A



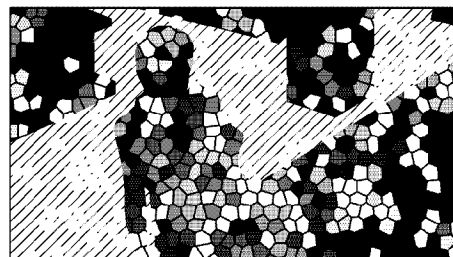
B



C

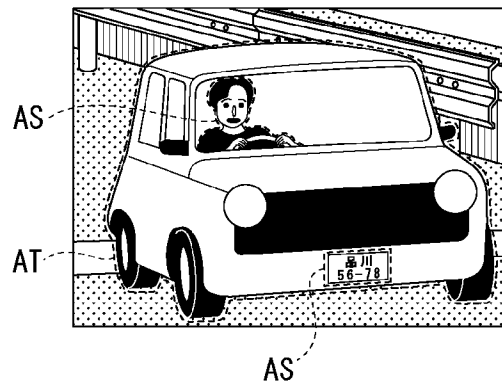


D

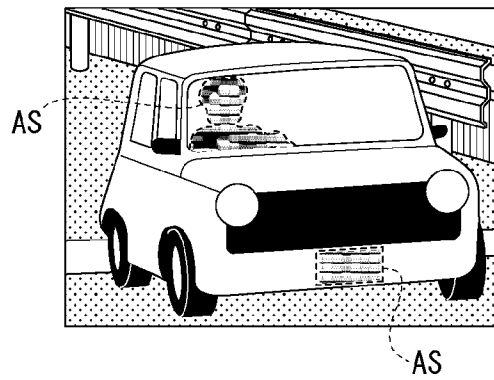


[図16]

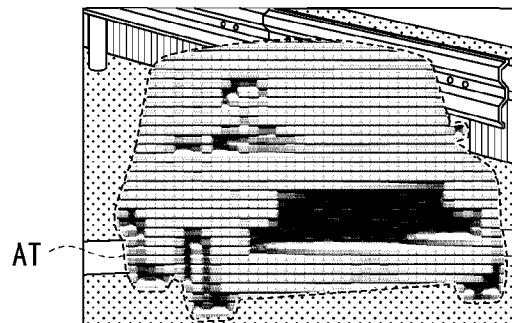
A



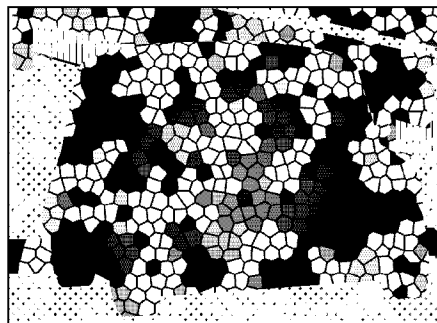
B



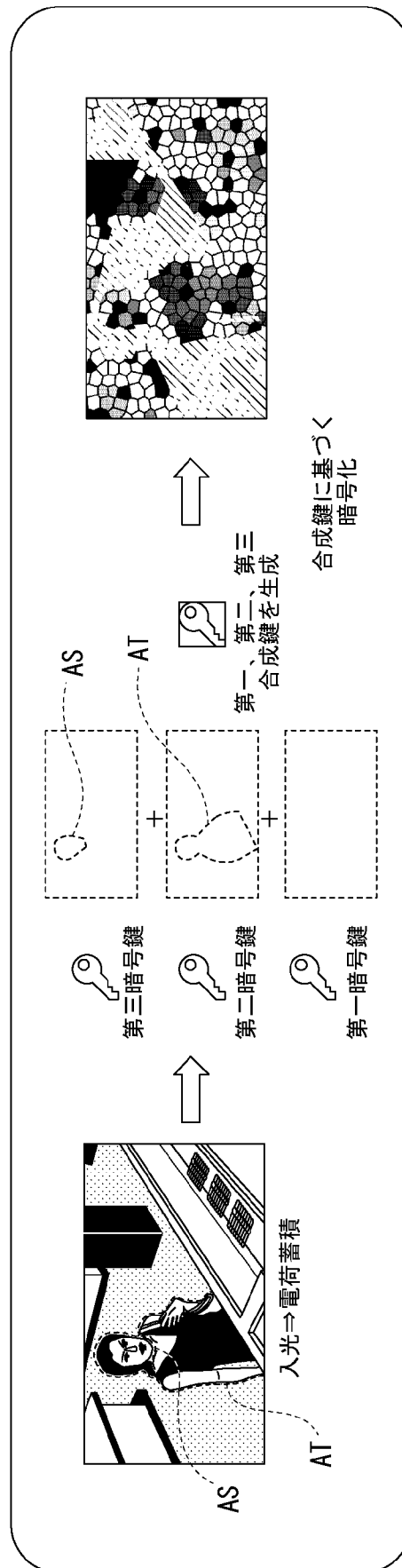
C



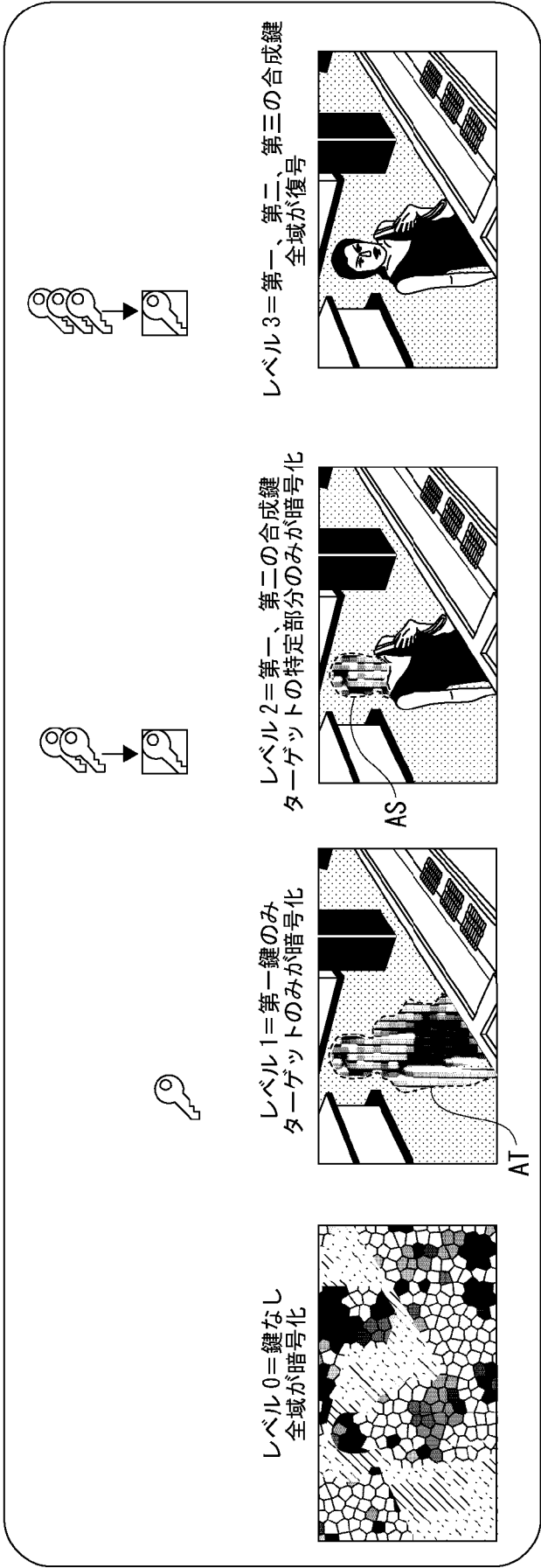
D



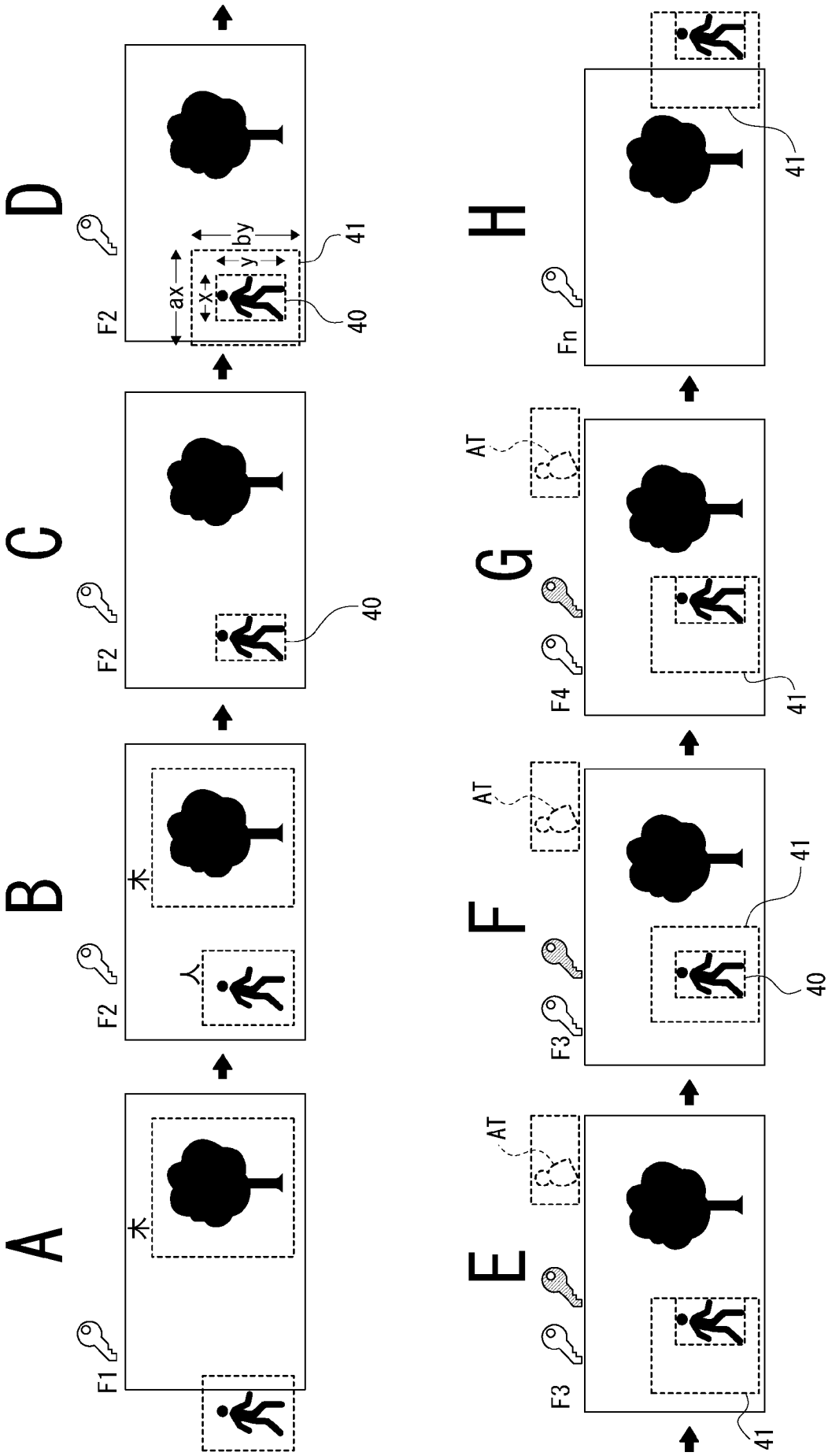
[図17]



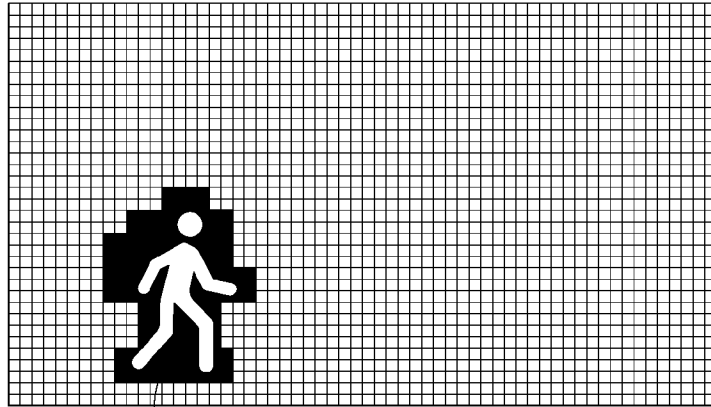
[図18]



[図19]

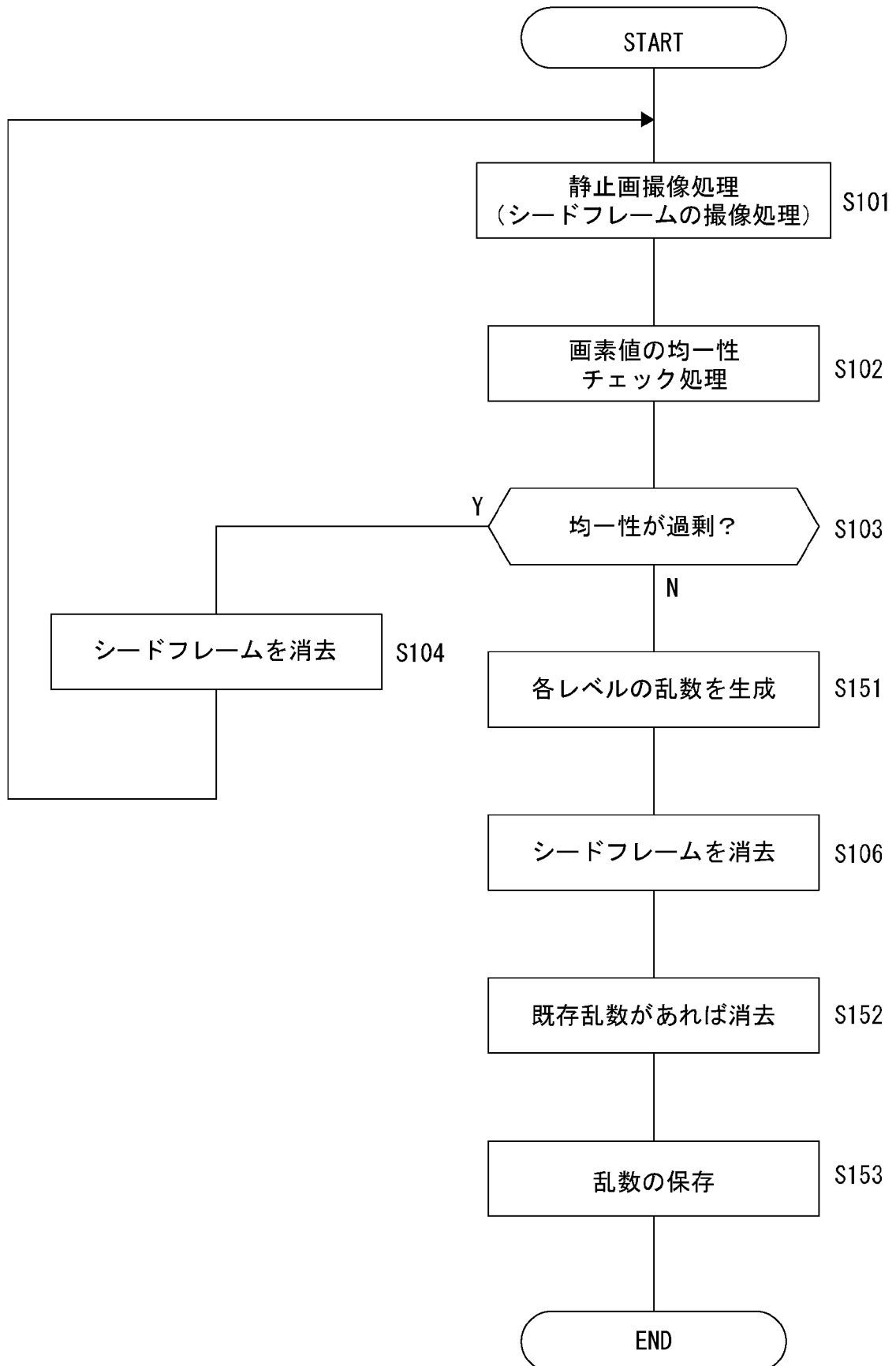


[図20]

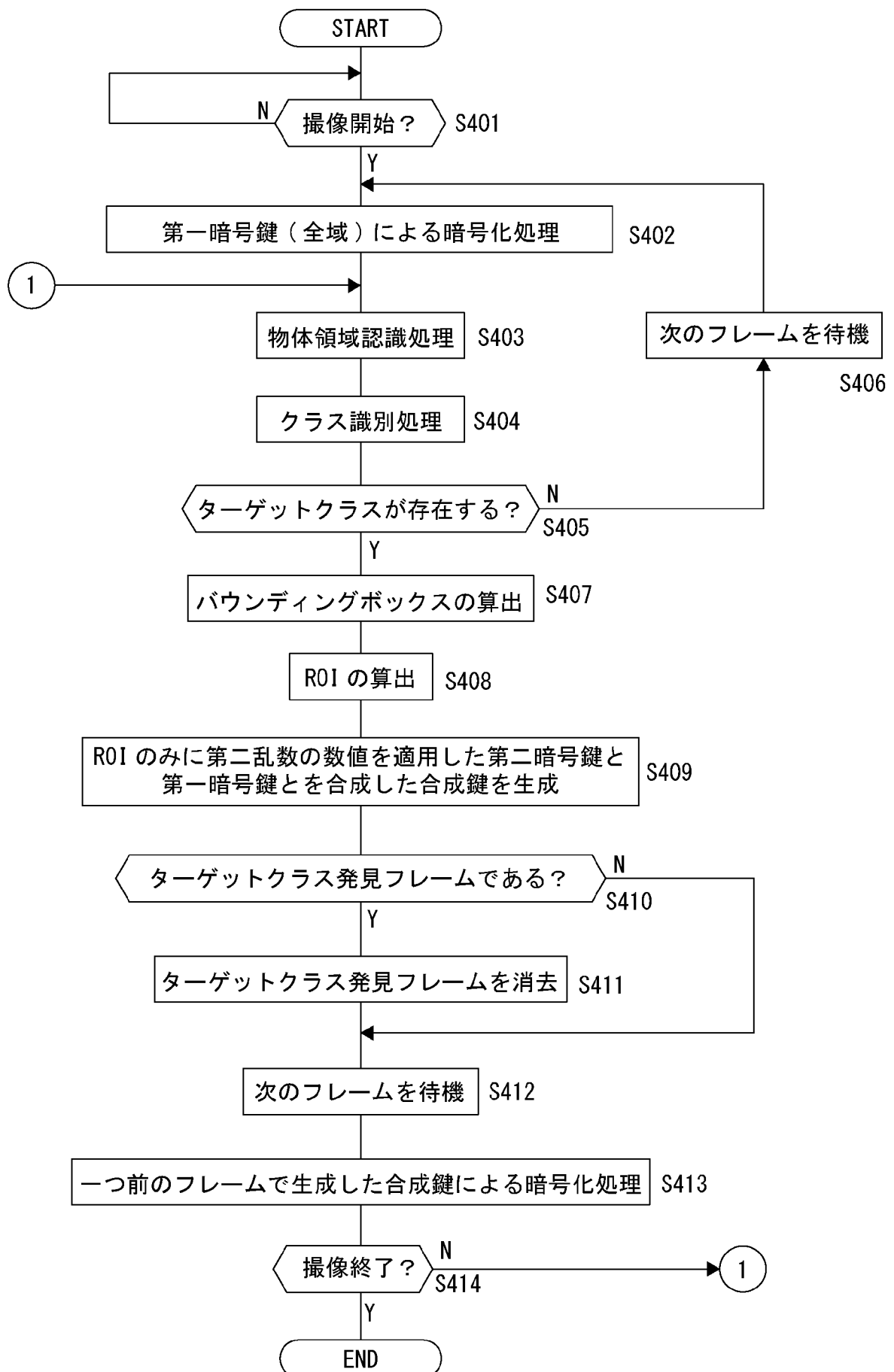


41

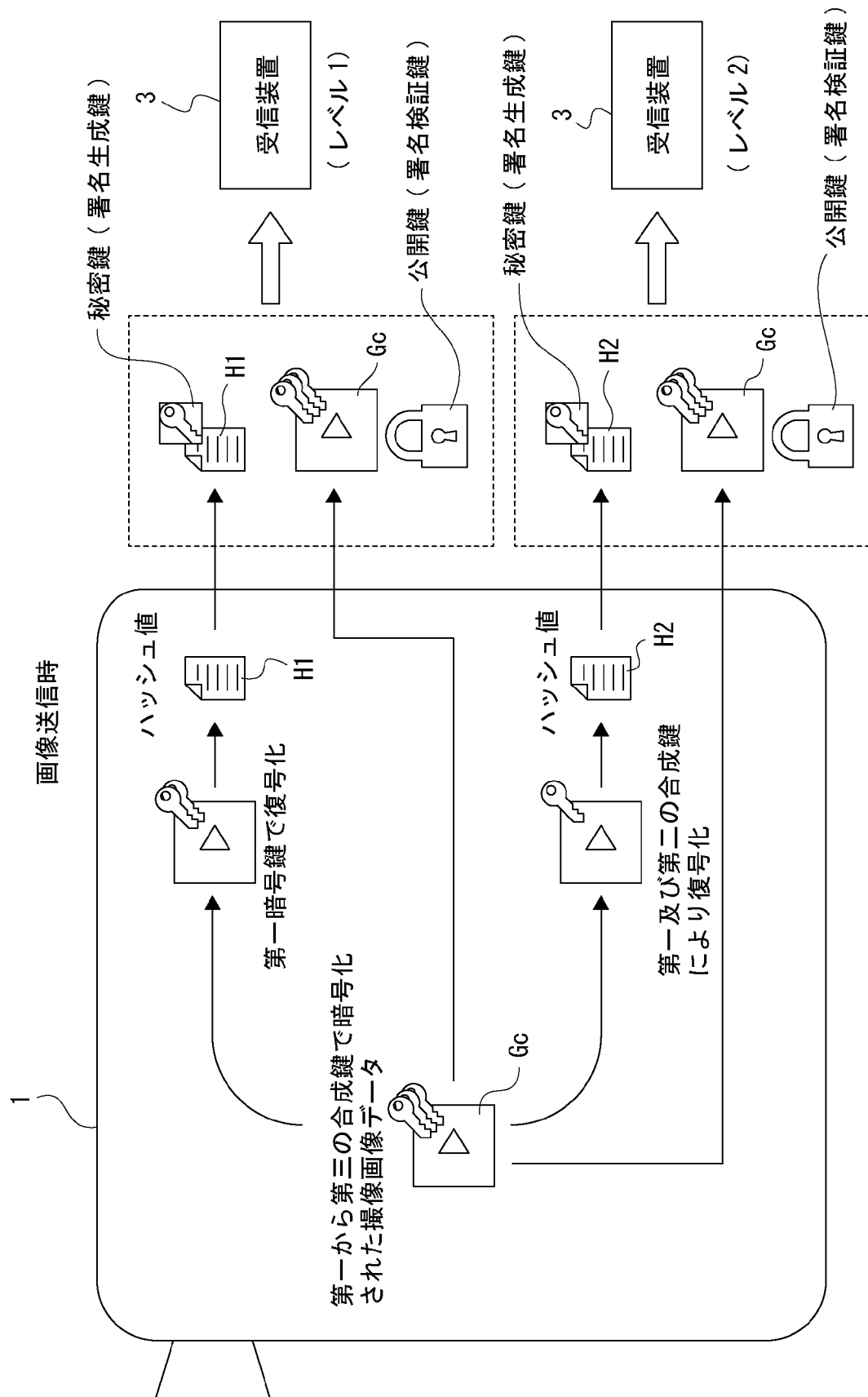
[図21]



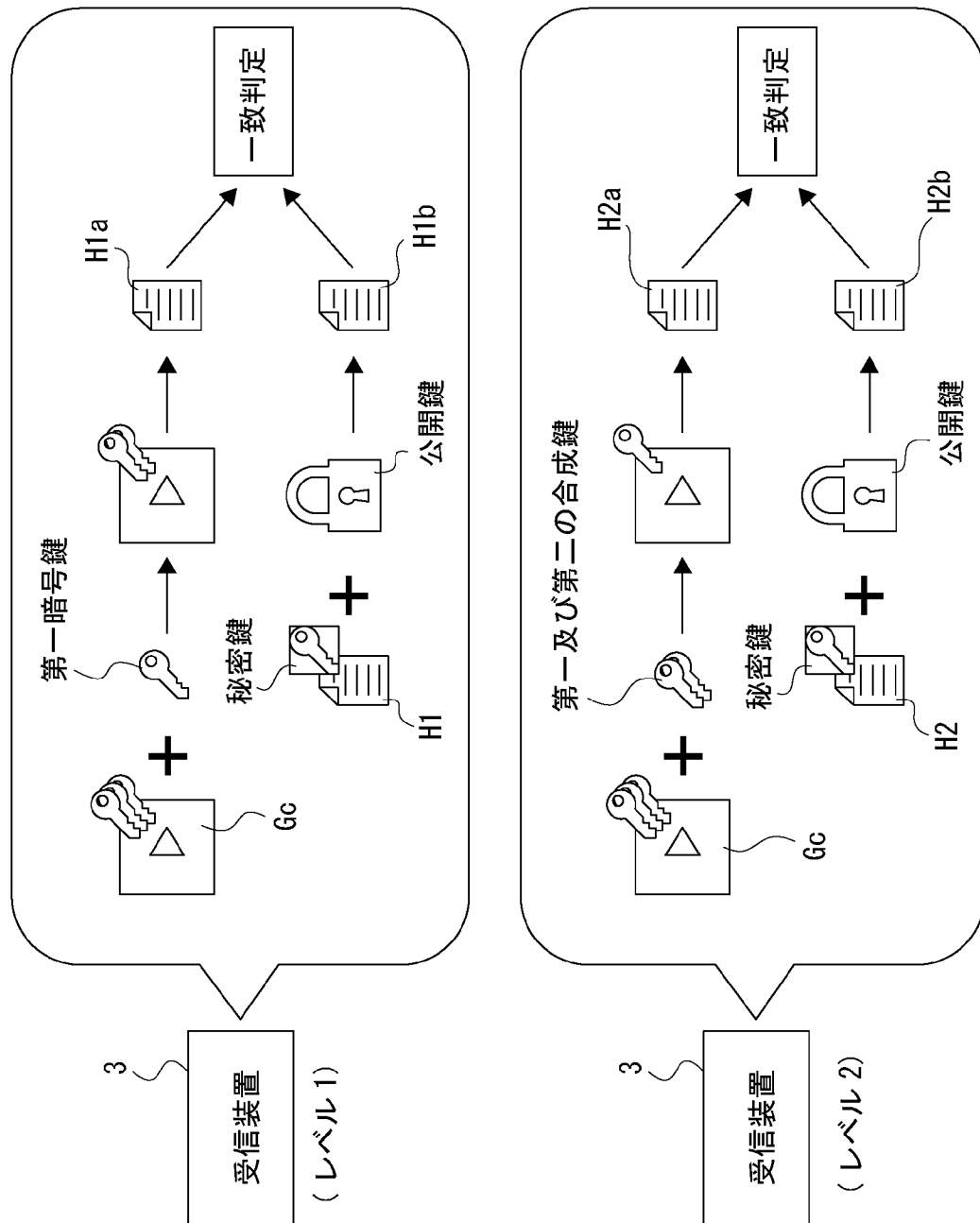
[図22]



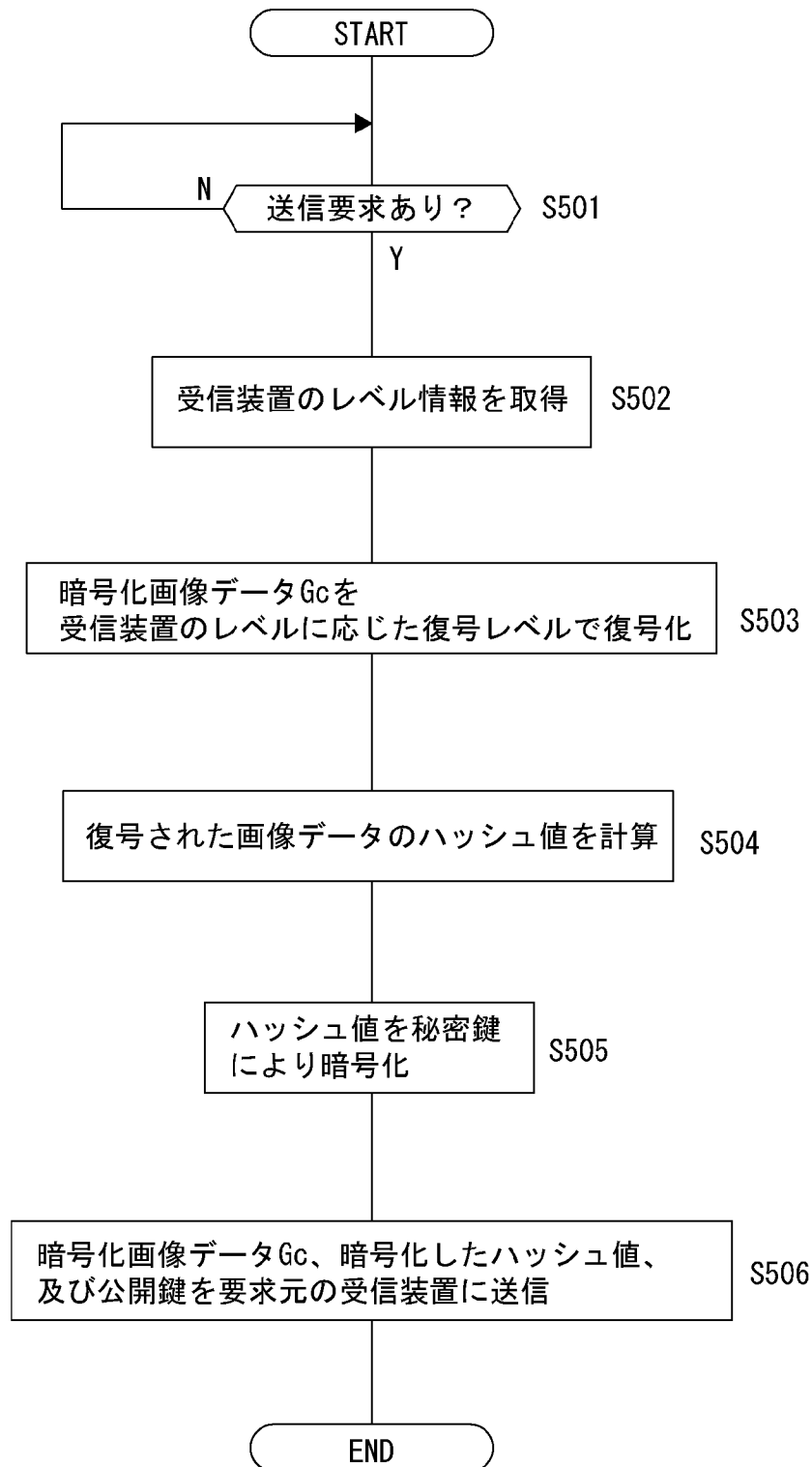
[図23]



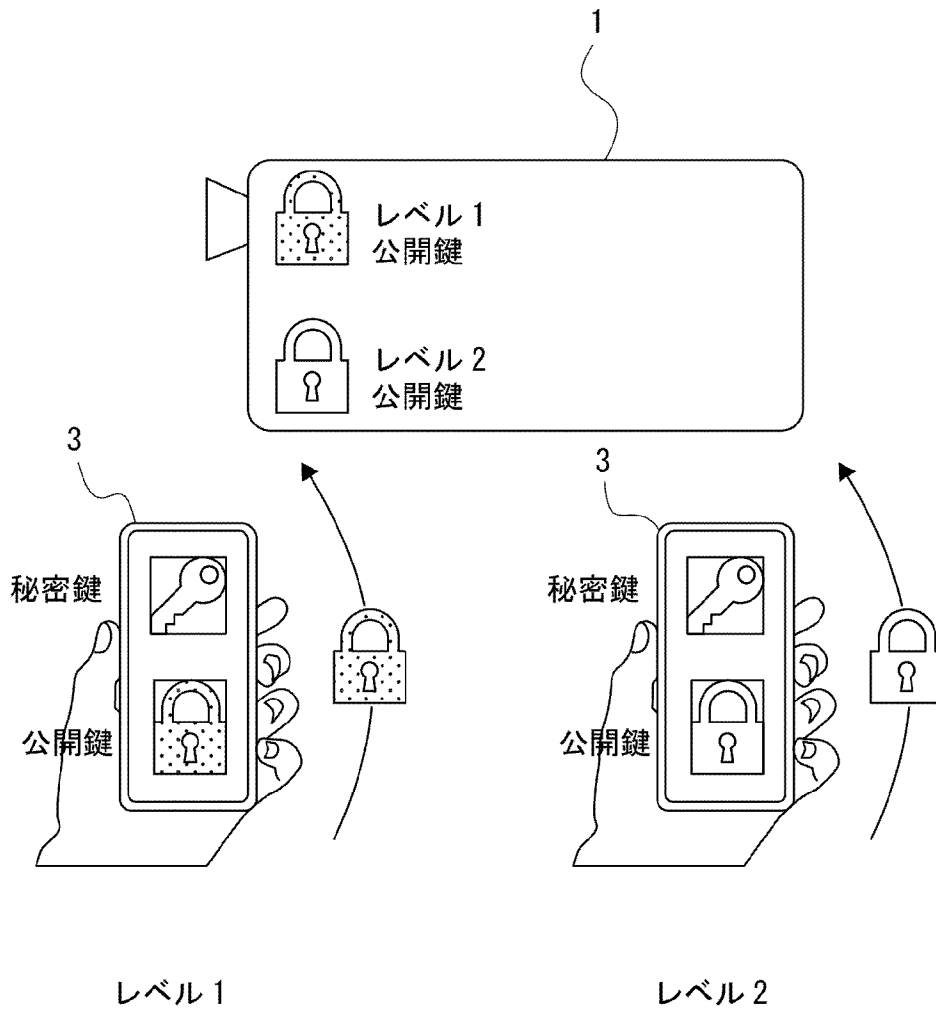
[図24]



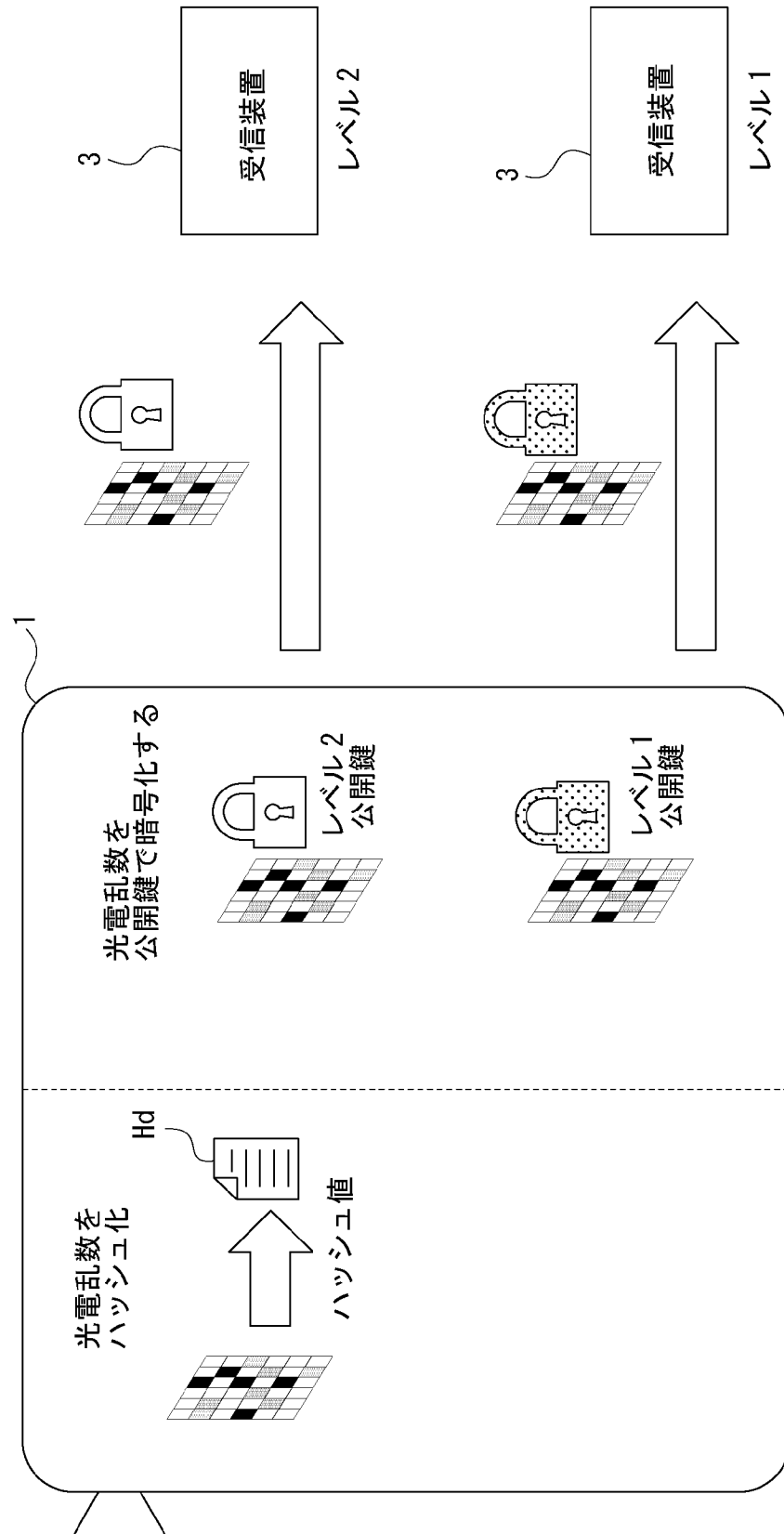
[図25]



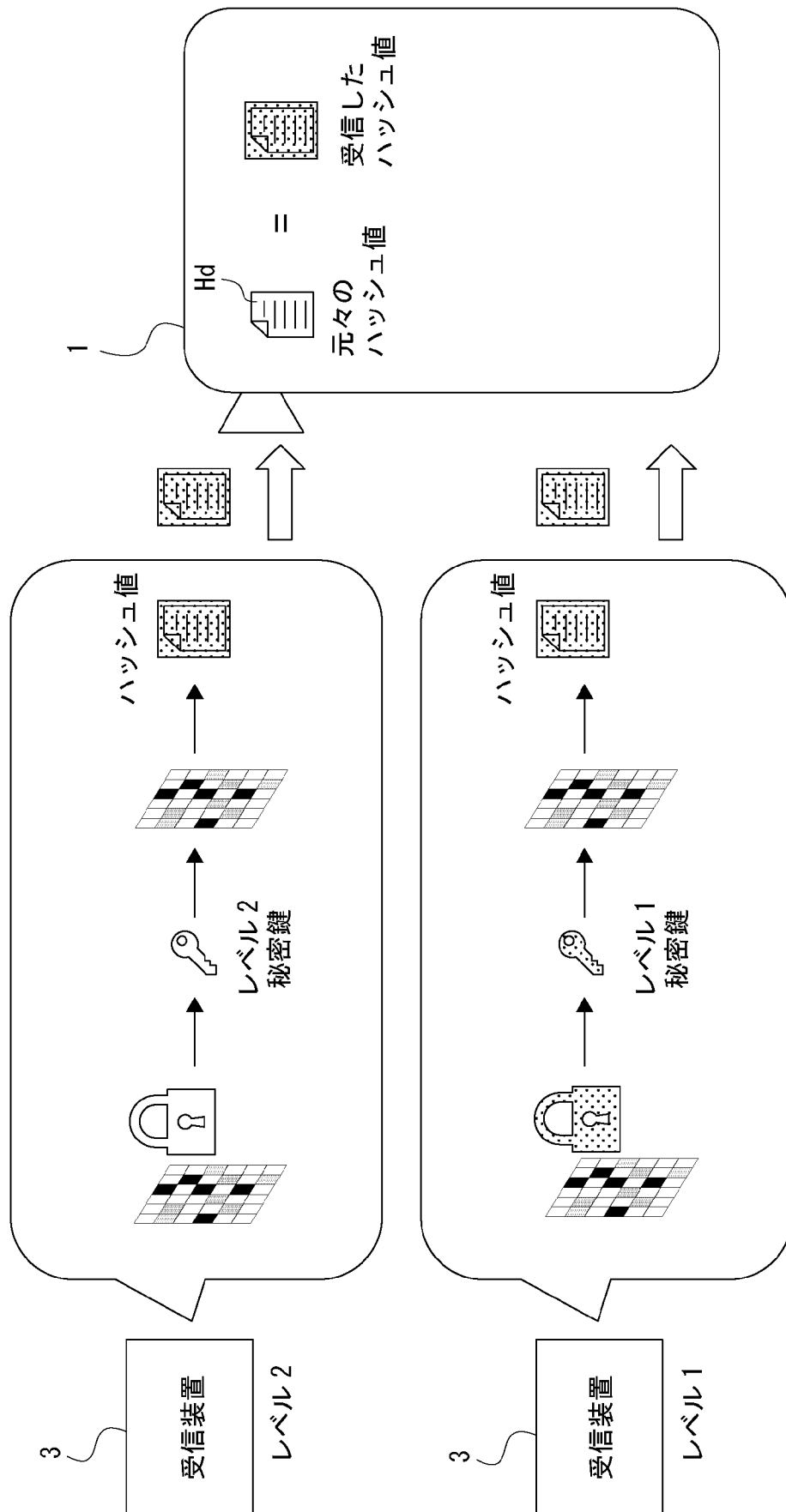
[図26]



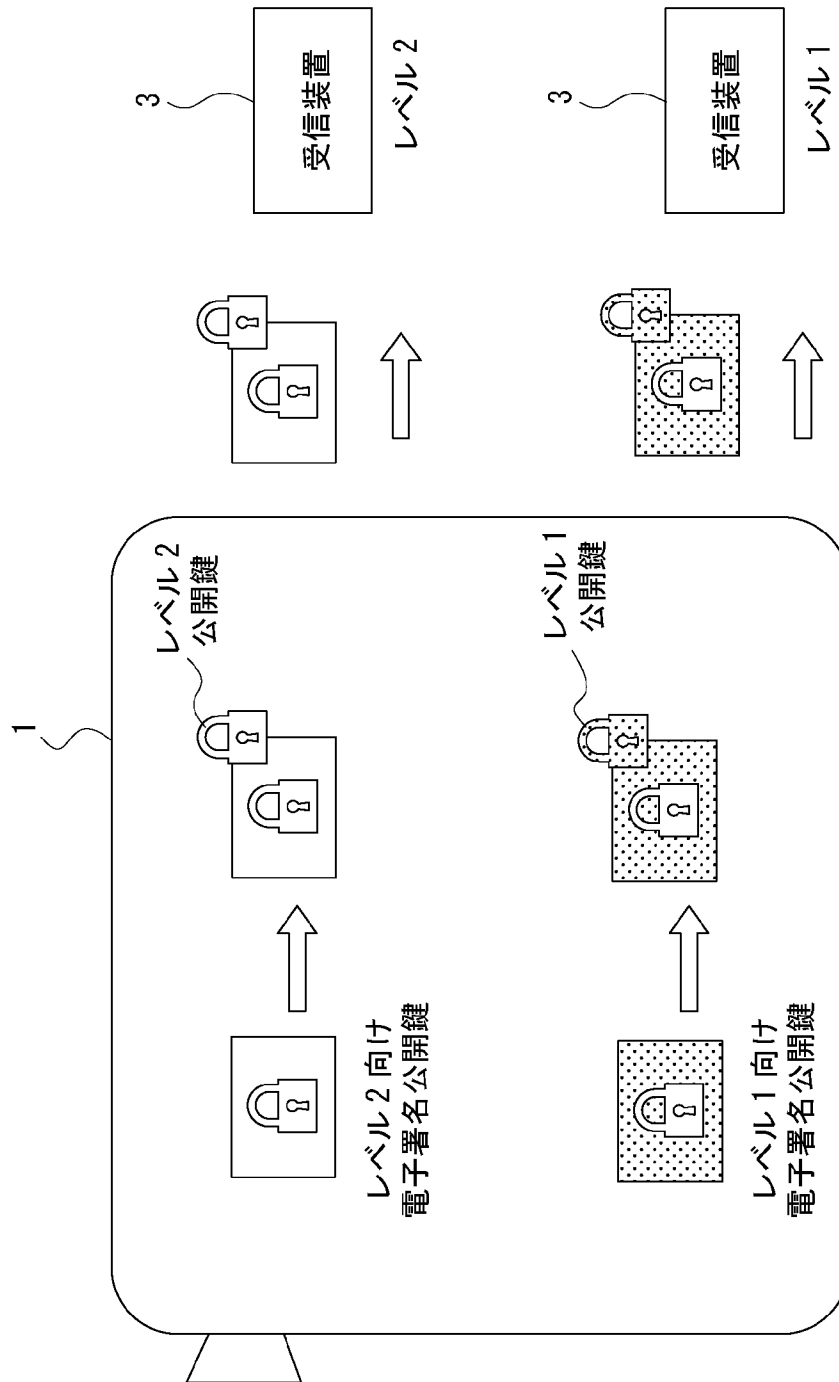
[図27]



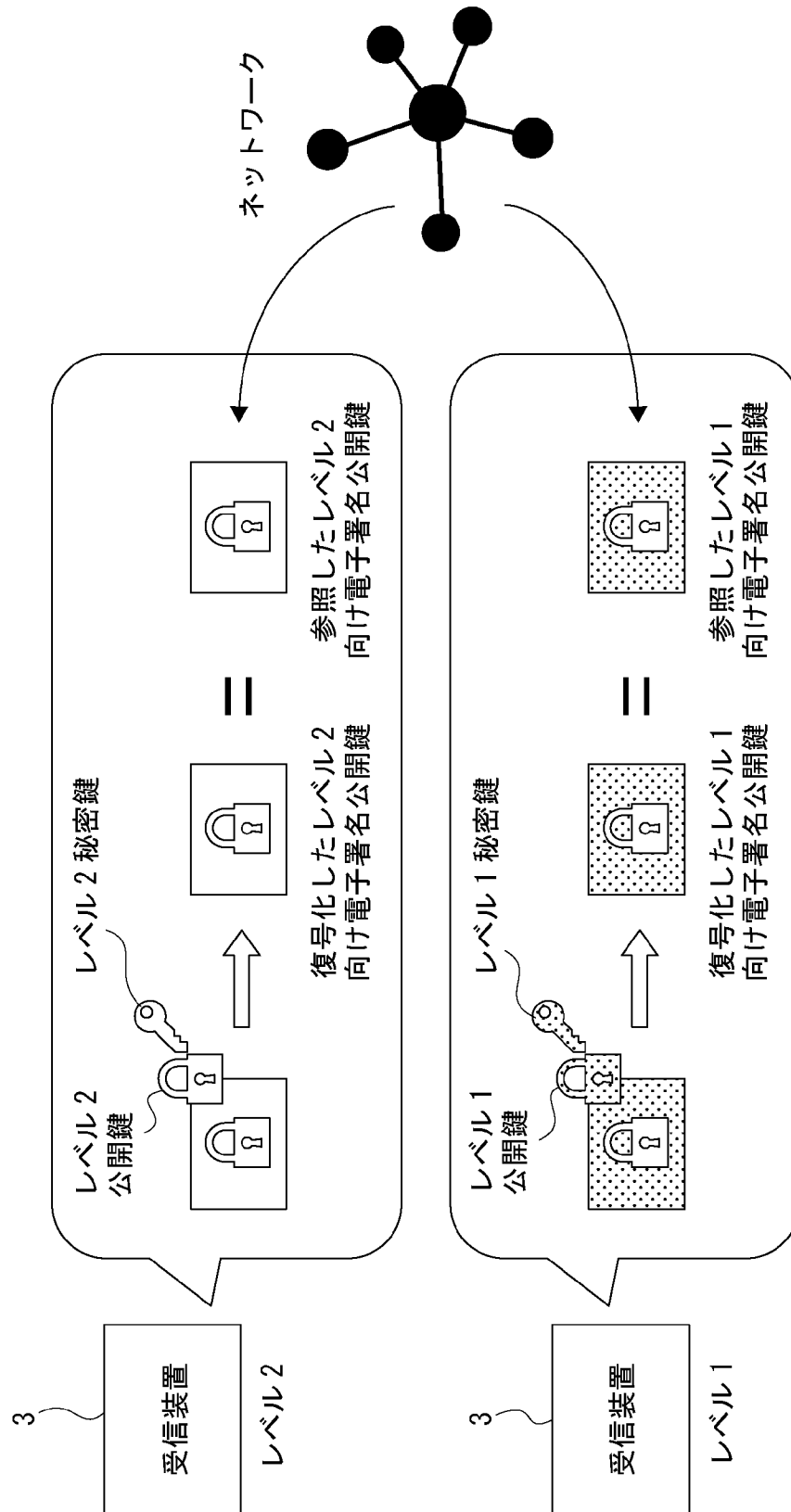
[図28]



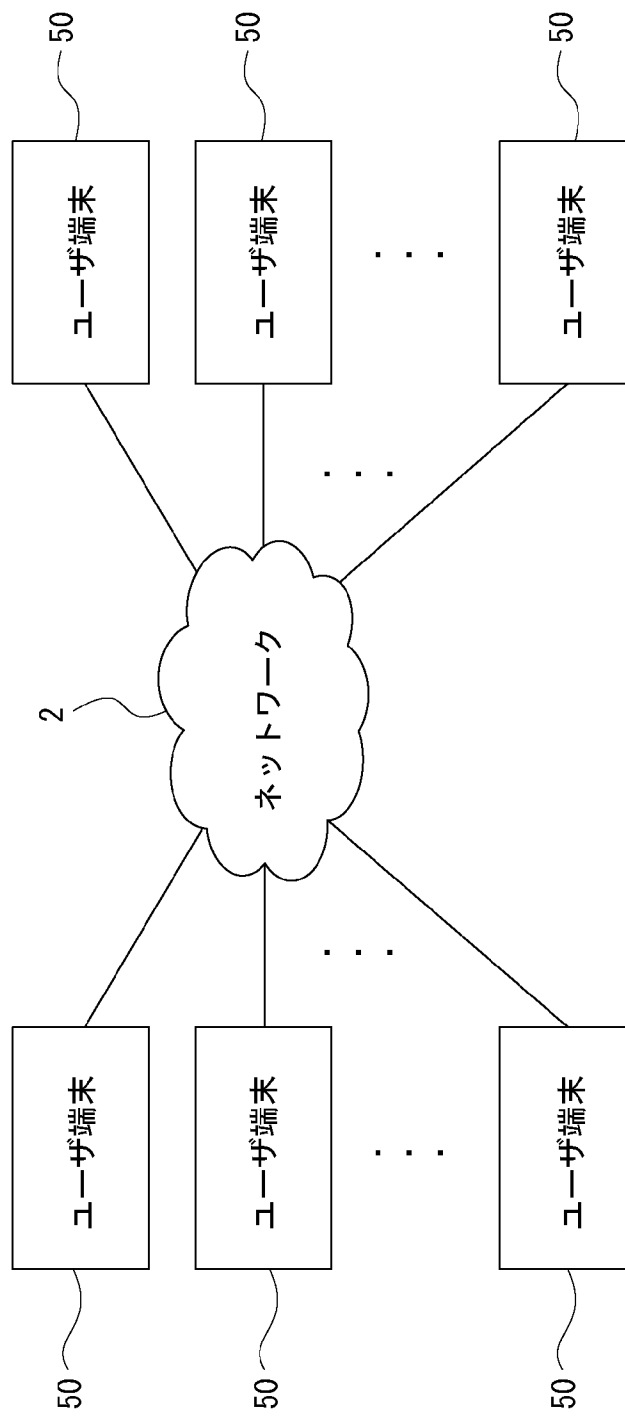
[図29]



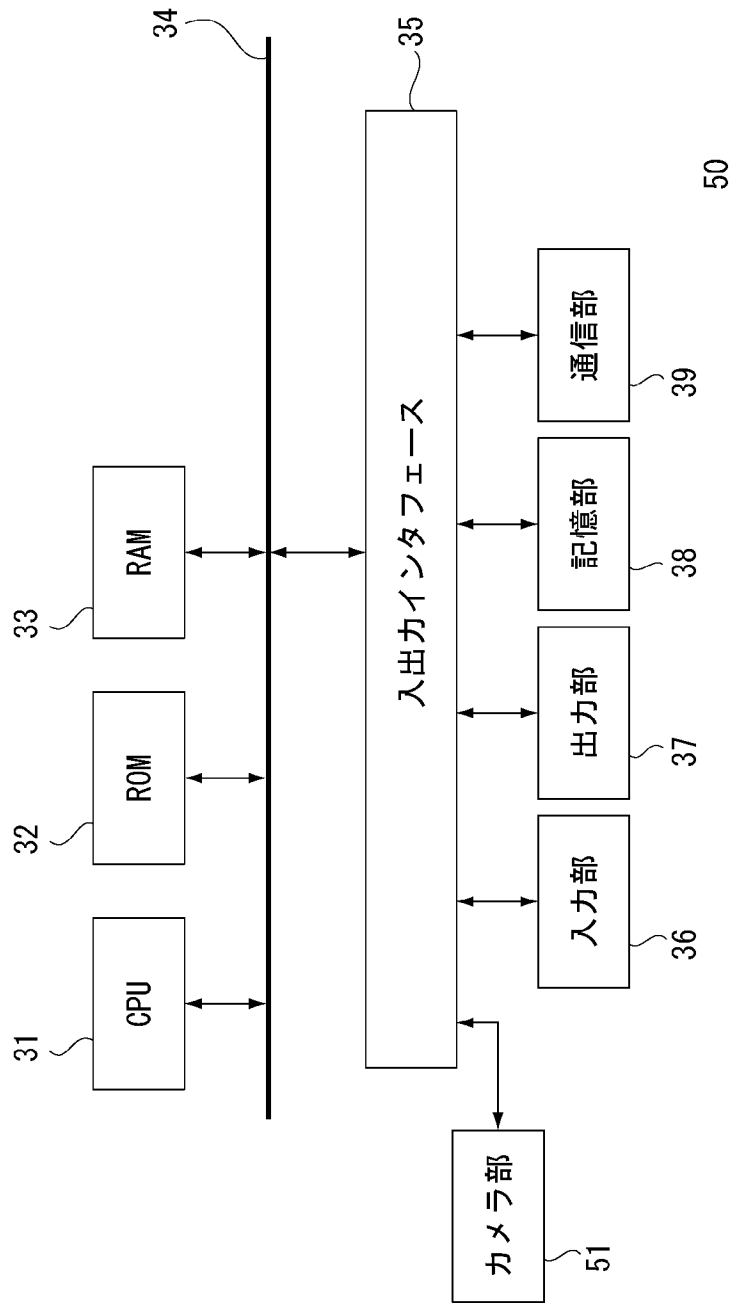
[図30]



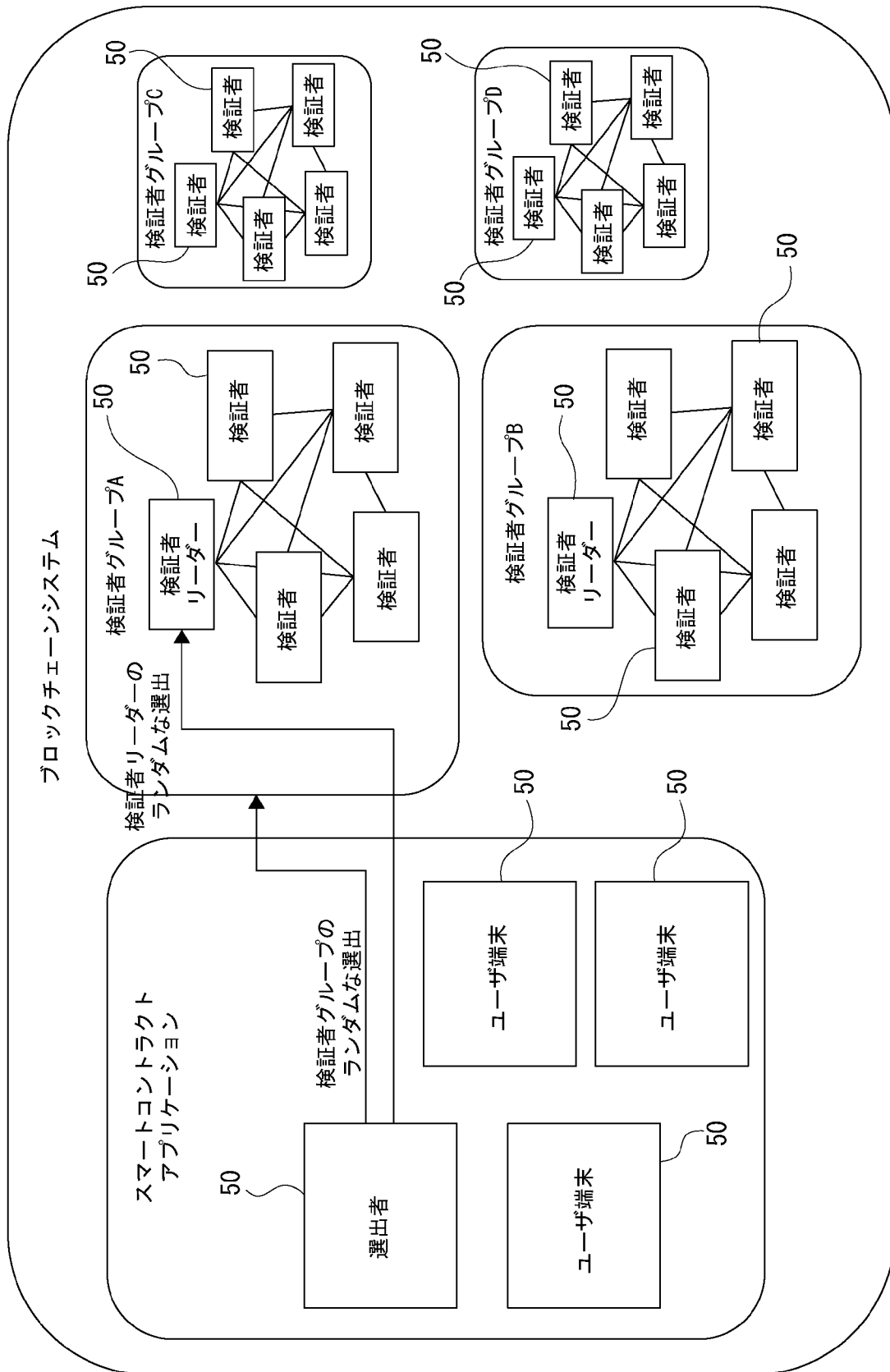
[図31]



[図32]



[図33]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/022668

A. CLASSIFICATION OF SUBJECT MATTER

G09C 1/00 (2006.01) i; H04L 9/32 (2006.01) i; G06F 7/58 (2006.01) i
FI: G09C1/00 650B; H04L9/00 675B; G06F7/58 680

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G09C1/00; H04L9/32; G06F7/58

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2019-20431 A (SONY SEMICONDUCTOR SOLUTIONS CORPORATION) 07.02.2019 (2019-02-07) paragraphs [0055]-[0104]	1-5, 7, 10-14 6, 8-9
Y A	US 2019/0121955 A1 (SECURE-IC SAS) 25.04.2019 (2019-04-25) paragraphs [0006]-[0015]	1-5, 10-14 6
Y A	JP 2017-157926 A (FUJI XEROX CO., LTD.) 07.09.2017 (2017-09-07) paragraphs [0042]-[0044], [0071]-[0073]	1, 7, 14 8-9
A	JP 2006-80658 A (MITSUBISHI ELECTRIC INFORMATION SYSTEMS CORP.) 23.03.2006 (2006-03-23) paragraphs [0002]-[0003]	6

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

☒ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search
26 August 2020 (26.08.2020)

Date of mailing of the international search report
08 September 2020 (08.09.2020)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/022668

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2019-20431 A	07 Feb. 2019	WO 2019/012779 A1 CN 110546916 A	
US 2019/0121955 A1	25 Apr. 2019	EP 3474485 A1 CN 109698742 A	
JP 2017-157926 A	07 Sep. 2017	US 2017/0249482 A1 paragraphs [0031]- [0033], [0062]-[0064]	
JP 2006-80658 A	23 Mar. 2006	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G09C 1/00(2006.01)i; H04L 9/32(2006.01)i; G06F 7/58(2006.01)i FI: G09C1/00 650B; H04L9/00 675B; G06F7/58 680		
B. 調査を行った分野		
調査を行った最小限資料（国際特許分類（IPC）） G09C1/00; H04L9/32; G06F7/58		
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2020年 日本国実用新案登録公報 1996-2020年 日本国登録実用新案公報 1994-2020年		
国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y A	JP 2019-20431 A（ソニーセミコンダクタソリューションズ株式会社）07.02.2019 （2019 - 02 - 07） 段落0055-0104	1-5, 7, 10-14 6, 8-9
Y A	US 2019/0121955 A1（SECURE-IC SAS）25.04.2019（2019 - 04 - 25） 段落0006-0015	1-5, 10-14 6
Y A	JP 2017-157926 A（富士ゼロックス株式会社）07.09.2017（2017 - 09 - 07） 段落0042-0044, 0071-0073	1, 7, 14 8-9
A	JP 2006-80658 A（三菱電機インフォメーションシステムズ株式会社）23.03.2006 （2006 - 03 - 23） 段落0002-0003	6
☐ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的な技術水準を示すもの “E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの “L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す） “O” 口頭による開示、使用、展示等に言及する文献 “P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献 “T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの “X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの “Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの “&” 同一パテントファミリー文献		
国際調査を完了した日 26.08.2020		国際調査報告の発送日 08.09.2020
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号		権限のある職員（特許庁審査官） 金沢 史明 5S 4538 電話番号 03-3581-1101 内線 3546

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2020/022668

引用文献			公表日	パテントファミリー文献			公表日
JP	2019-20431	A	07.02.2019	WO	2019/012779	A1	
				CN	110546916	A	
US	2019/0121955	A1	25.04.2019	EP	3474485	A1	
				CN	109698742	A	
JP	2017-157926	A	07.09.2017	US	2017/0249482	A1	
				段落0031-0033, 0062-0064			
JP	2006-80658	A	23.03.2006	(ファミリーなし)			