

(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
2024年6月13日(13.06.2024)



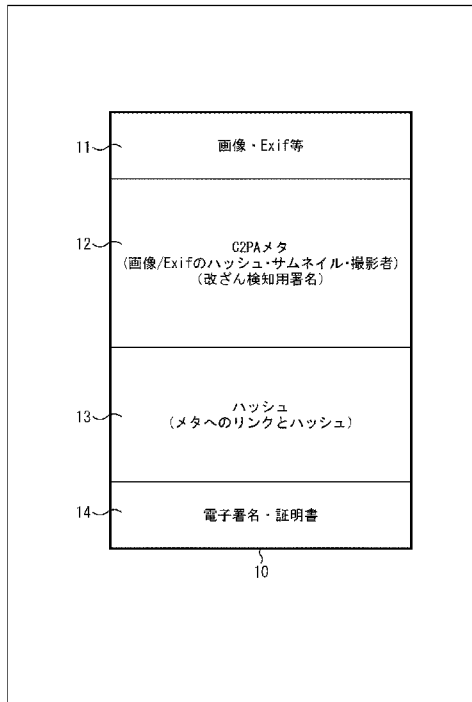
(10) 国際公開番号
WO 2024/122601 A1

- (51) 国際特許分類:
G06F 21/64 (2013.01) *H04L 9/30* (2006.01)
- (21) 国際出願番号: PCT/JP2023/043767
- (22) 国際出願日: 2023年12月7日(07.12.2023)
- (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:
63/430,788 2022年12月7日(07.12.2022) US
- (71) 出願人: ソニーグループ株式会社(SONY GROUP CORPORATION) [JP/JP]; 〒1080075 東京都港区港南1丁目7番1号 Tokyo (JP).
- (72) 発明者: 平塚 陽介 (HIRATSUKA Yosuke); 〒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: 西川 孝, 外 (NISHIKAWA Takashi et al.); 〒1700013 東京都豊島区東池袋3丁目9番10号 池袋F Nビル4階 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, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY,

(54) Title: IMAGE PROCESSING DEVICE AND METHOD

(54) 発明の名称: 画像処理装置および方法

FIG. 2



- 11 Image, Exif, and like
12 C2PA meta (Hash, thumbnail, and taker of image/Exif) (signature for detecting tampering)
13 Hash (link to meta and hash)
14 Electronic signature/certificate

(57) Abstract: The present disclosure relates to an image processing device and method that make it possible to suppress a decrease in usability of a captured image. A captured image and metadata are used to generate a first hash corresponding to a first signature, and a second hash corresponding to a second signature. The first signature is generated using a first private key and the first hash. The second signature is generated using a second private key and the second hash. A file for storing the captured image, the metadata, the first signature, and the second signature is generated. The first private

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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))

key corresponds to a limited public key that is only made public to a first presence that has a specific right other than a user right. The second private key corresponds to a user public key that is also made public to a second presence that has a user right. The present disclosure is applicable, for example, to image processing devices or image processing methods.

(57) 要約: 本開示は、撮像画像のユーザビリティの低減を抑制することができるようにする画像処理装置および方法に関する。撮像画像およびメタデータを用いて、第1の署名に対応する第1のハッシュと第2の署名に対応する第2のハッシュとを生成し、第1の秘密鍵と第1のハッシュとを用いて第1の署名を生成し、第2の秘密鍵と第2のハッシュとを用いて第2の署名を生成し、撮像画像、メタデータ、第1の署名、および第2の署名を格納するファイルを生成する。第1の秘密鍵は、ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵に対応し、第2の秘密鍵は、ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する。本開示は、例えば、画像処理装置、または画像処理方法等に適用することができる。

明 細 書

発明の名称：画像処理装置および方法

技術分野

[0001] 本開示は、画像処理装置および方法に関し、特に、撮像画像のユーザビリティの低減を抑制することができるようにした画像処理装置および方法に関する。

背景技術

[0002] 従来、撮影時に画像に電子署名を付与することで、改竄検知を可能にする方法があった（例えば、特許文献1参照）。また、画像生成時や編集時に、履歴を電子署名付きで残し、履歴をたどれるようにする方法があった（例えば、非特許文献1参照）。これらの手法では、秘密鍵で署名し、その秘密鍵に対応する公開鍵を用いて検証が行われた。そのため秘密鍵が漏洩すると、電子署名を用いて画像の改ざんを検知することが困難になるおそれがあった。

[0003] これに対して、公開鍵の配布を一部に限定し、さらに追加の改ざん検知を実施する方法が考えられた。追加の改ざん検知を実施することにより、より強力な改ざん検知を行うことができる。そして、公開鍵の配布を一部に限定することにより、改ざん検知の実施者を制限することができ、改ざん検知の手法を非公開とする（または公開範囲を制限する）ことができる。これにより、改ざん検知の正当性の低減を抑制することができる。

先行技術文献

特許文献

[0004] 特許文献1：国際公開第2022／137798号

非特許文献

[0005] 非特許文献1：<https://c2pa.org/>

発明の概要

発明が解決しようとする課題

[0006] しかしながら、このように公開鍵の配布先を一部に制限すると、C2PAのように、他社のツールなどと連携して改ざんできない編集履歴をつけていくようなケースに対応できなくなるおそれがあった。すなわち、撮像画像のユーザビリティ（使いやすさ）が低減するおそれがあった。

[0007] 本開示は、このような状況に鑑みてなされたものであり、撮像画像のユーザビリティの低減を抑制することができるようにするものである。

課題を解決するための手段

[0008] 本技術の一側面の画像処理装置は、撮像画像およびメタデータを用いて、第1の署名に対応する第1のハッシュと第2の署名に対応する第2のハッシュとを生成するハッシュ処理部と、第1の秘密鍵と前記第1のハッシュとを用いて前記第1の署名を生成し、第2の秘密鍵と前記第2のハッシュとを用いて前記第2の署名を生成する署名生成部と、前記撮像画像、前記メタデータ、前記第1の署名、および前記第2の署名を格納するファイルを生成するファイル生成部とを備え、前記第1の秘密鍵は、ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵に対応し、前記第2の秘密鍵は、前記ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する画像処理装置である。

[0009] 本技術の一側面の画像処理方法は、撮像画像およびメタデータを用いて、第1の署名に対応する第1のハッシュと第2の署名に対応する第2のハッシュとを生成し、第1の秘密鍵と前記第1のハッシュとを用いて前記第1の署名を生成し、第2の秘密鍵と前記第2のハッシュとを用いて前記第2の署名を生成し、前記撮像画像、前記メタデータ、前記第1の署名、および前記第2の署名を格納するファイルを生成し、前記第1の秘密鍵は、ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵に対応し、前記第2の秘密鍵は、前記ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する画像処理方法である。

[0010] 本技術の他の側面の画像処理装置は、画像、メタデータ、第1の署名、および第2の署名が格納されたファイルを取得するファイル取得部と、ユーザ

権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵、前記画像、前記メタデータ、および前記第1の署名を用いて、前記画像の真贋を検証する検証部とを備え、前記第1の署名は、前記限定公開鍵に対応する第1の秘密鍵、前記画像に対応する撮像画像、および前記撮像画像のメタデータを用いて生成された署名であり、前記第2の署名は、前記ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する第2の秘密鍵、前記画像、および前記メタデータを用いて生成された署名である画像処理装置である。

[0011] 本技術の他の側面の画像処理方法は、画像、メタデータ、第1の署名、および第2の署名が格納されたファイルを取得し、ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵、前記画像、前記メタデータ、および前記第1の署名を用いて、前記画像の真贋を検証し、前記第1の署名は、前記限定公開鍵に対応する第1の秘密鍵、前記画像に対応する撮像画像、および前記撮像画像のメタデータを用いて生成された署名であり、前記第2の署名は、前記ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する第2の秘密鍵、前記画像、および前記メタデータを用いて生成された署名である画像処理方法である。

[0012] 本技術の一側面の画像処理装置および方法においては、撮像画像およびメタデータを用いて、第1の署名に対応する第1のハッシュと第2の署名に対応する第2のハッシュとが生成され、第1の秘密鍵と第1のハッシュとを用いて第1の署名が生成され、第2の秘密鍵と第2のハッシュとを用いて第2の署名が生成され、撮像画像、メタデータ、第1の署名、および第2の署名を格納するファイルが生成される。第1の秘密鍵が、ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵に対応し、第2の秘密鍵が、前記ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する。

[0013] 本技術の他の側面の画像処理装置および方法においては、画像、メタデータ、第1の署名、および第2の署名が格納されたファイルが取得され、ユー

ザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵、画像、メタデータ、および第1の署名を用いて、その画像の真贋が検証される。第1の署名が、限定公開鍵に対応する第1の秘密鍵、画像に対応する撮像画像、およびその撮像画像のメタデータを用いて生成された署名であり、第2の署名が、ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する第2の秘密鍵、画像、およびメタデータを用いて生成された署名である。

図面の簡単な説明

- [0014] [図1]画像ファイルの生成方法の例を示す図である。
- [図2]画像ファイルの主な構成例を示す図である。
- [図3]画像ファイルの主な構成例を示す図である。
- [図4]ハッシュの対象範囲の例を示す図である。
- [図5]署名の格納場所の例を示す図である。
- [図6]画像処理システムの主な構成例を示す図である。
- [図7]撮像装置の主な構成例を示すブロック図である。
- [図8]検証装置の主な構成例を示すブロック図である。
- [図9]サーバの主な構成例を示すブロック図である。
- [図10]撮像処理の流れの例を説明するフローチャートである。
- [図11]ユーザレベル画像検証処理の流れの例を説明するフローチャートである。
- [図12]高レベル画像検証処理の流れの例を説明するフローチャートである。
- [図13]高レベル画像検証処理の流れの例を説明するフローチャートである。
- [図14]高レベル画像検証処理の流れの例を説明するフローチャートである。
- [図15]高レベル画像検証処理の流れの例を説明するフローチャートである。
- [図16]限定公開鍵供給処理の流れの例を説明するフローチャートである。
- [図17]コンピュータの主な構成例を示すブロック図である。

発明を実施するための形態

- [0015] 以下、本開示を実施するための形態（以下実施の形態とする）について説

明する。なお、説明は以下の順序で行う。

1. 技術内容・技術用語をサポートする文献等
2. 改ざんの検知
3. 複数の署名の格納
4. 第1の実施の形態（画像処理システム）
5. 付記

[0016] <1. 技術内容・技術用語をサポートする文献等>

本技術で開示される範囲は、実施の形態に記載されている内容だけではなく、出願当時において公知となっている以下の特許文献および非特許文献等に記載されている内容や以下の特許文献および非特許文献において参照されている他の文献の内容等も含まれる。

[0017] 特許文献1：（上述）

非特許文献1：（上述）

[0018] つまり、上述の特許文献および非特許文献に記載されている内容や、上述の特許文献および非特許文献において参照されている他の文献の内容等も、サポート要件を判断する際の根拠となる。

[0019] <2. 改ざんの検知>

<電子署名を用いた改ざんの検知>

従来、例えば、特許文献1に記載のように、撮影時に画像に電子署名を付与することで、改竄検知を可能にする方法があった。また、非特許文献1に開示されているように、画像生成時や編集時に、履歴を電子署名付きで残し、履歴を辿ることができるようにする方法があった。編集時、編集を担当したソフトやサーバは、画像の過去の履歴を画像内の公開鍵で確認後、過去のツールの署名や署名対象のデータの一部を新しい画像のメタデータとして引き継ぎ、加えて秘密鍵で署名し、対応する公開鍵を付与する。

[0020] これらの手法では、秘密鍵で署名し、その秘密鍵に対応する公開鍵を用いて検証が行われた。公開鍵を画像とともに配布すれば、だれでも改ざんを検知することができた。そのため秘密鍵が漏洩すると、不正なユーザが画像を

改ざんし、その秘密鍵を用いて電子署名を不正に生成することができるので、現実的に、電子署名を用いて画像の改ざんを検知することが困難になるおそれがあった。

[0021] これに対して、公開鍵の配布を一部に限定し、さらに追加の改ざん検知を実施する方法が考えられた。追加の改ざん検知を実施することにより、より強力な改ざん検知を行うことができる。そして、公開鍵の配布を一部に限定することにより、改ざん検知の実施者を制限することができ、改ざん検知の手法を非公開とする（または公開範囲を制限する）ことができる。これにより、改ざん検知の正当性の低減を抑制することができる。

[0022] しかしながら、このように公開鍵の配布先を一部に制限すると、C2PAのように、他社のツールなどと連携して改ざんできない編集履歴をつけていくようなケースに対応できなくなるおそれがあった。

[0023] 例えば、第三者による加工が改ざんに該当するとして厳格運用にしたいようなケースにおいては、署名検証を自社サーバで限定したいというニーズがある。これに対して、ある程度、第三者による加工を許容できるケースにおいては、他社による署名検証を可能にして他社ツールとの連携で来歴の証明を行いたいといったニーズがある。しかしながら、現状のC2PA規格では、上述の2つのケースを同じ機材・同じフォーマットを用いて併存させることができない。つまり、従来の方法では、署名検証を限定し、強力な改ざん検出を実現するユースケースと、他社に署名検証を許し編集来歴の維持を実現するユースケースの両方に対応することが困難であった。すなわち、撮像画像のユーザビリティ（使いやすさ）が低減するおそれがあった。

[0024] <3. 複数の署名の格納>

<方法1>

そこで、図1の表の最上段に記載のように、公開範囲が互いに異なる公開鍵に対応する複数の署名をファイルに格納する（方法1）。より具体的には、公開範囲が制限された公開鍵に対応する署名と公開範囲が制限されていない公開鍵に対応する署名とをファイルに格納する。

- [0025] 例えば、画像の改ざんを検知するための検証を実行するとする。その際、ユーザ権限以外の特定の権限を有する存在のみが、より強力に改ざんを検知することができる検証手法を適用することが許可されるものとする。
- [0026] ここで、「より強力に改ざんを検知することができる検証手法」とは、例えば、ユーザ権限を有する存在が実行可能な検証手法よりも確実に画像の改ざんを検知することができる検証手法である。その検証手法は、どのような手法であってもよい。例えば、署名を用いる検証だけでなく、ファイルに格納される情報（例えば画像やそのメタデータ等）を利用した検証も適用される手法であってもよい。このファイルに格納される情報を利用した検証はどのような手法であってもよい。例えば、画像とメタデータとの間の矛盾の有無により改ざんを検知する手法であってもよいし、その他の手法であってもよい。また、ファイルに格納される情報以外の情報を利用する手法が適用されてもよい。
- [0027] また、「ユーザ権限以外の特定の権限を有する存在」とは、例えば、システムやサービスの提供者や管理者、または、それらと同等の権限を有するコンピュータやアプリケーション等のような、ユーザ権限には与えられない権限が与えられる存在を示す。つまり、「特定の権限」は、例えば、ユーザ権限よりも高レベルの権限であってもよい。したがって、本明細書においては、「より強力に改ざんを検知することができる検証手法」を高レベル画像検証（処理）とも称する。
- [0028] この高レベル画像検証を実行する権限は、上述したように、「ユーザ権限以外の特定の権限を有する存在」に制限される。つまり、高レベル画像検証に含まれる「署名を用いる検証」には、「ユーザ権限以外の特定の権限を有する存在」にのみ公開される公開鍵が用いられる。本明細書において、この公開鍵を限定公開鍵とも称する。この高レベル画像検証において利用される署名は、画像やメタデータ等のハッシュと、この限定公開鍵に対応する秘密鍵とを用いて生成される。本明細書において、この署名を第1の署名とも称する。また、この第1の署名の生成に用いられるハッシュ（つまり、第1の

署名に対応するハッシュ)を第1のハッシュとも称する。また、限定公開鍵に対応する秘密鍵(つまり、第1の署名の生成に用いられる秘密鍵)を第1の秘密鍵とも称する。また、第1の署名は、上述のように画像の改ざんを検知するための検証に利用されるので、改ざん検知用署名とも称する。

[0029] これに対して、ユーザ権限を有する存在は、上述の「より強力に改ざんを検知することができる検証手法」を適用することが許可されないが、一般的な検証手法を適用することが許可されるものとする。

[0030] ここで、「一般的な検証手法」とは、例えば、ユーザ権限を有する存在が実行可能な検証手法である。その検証手法は、どのような手法であってもよい。例えば、署名を用いて画像の改ざんを検知する手法であってもよい。

[0031] また、「ユーザ権限を有する存在」とは、例えば、システムやサービスのユーザ、または、そのユーザと同等の権限を有するコンピュータやアプリケーション等である。したがって、本明細書においては、「一般的な検証手法」をユーザレベル画像検証(処理)とも称する。

[0032] ユーザ権限を有する存在には、公開範囲が制限されない公開鍵が提供される。本明細書において、この公開範囲が制限されない公開鍵をユーザ公開鍵とも称する。このユーザレベル画像検証において利用される署名は、画像やメタデータ等のハッシュと、このユーザ公開鍵に対応する秘密鍵とを用いて生成される。本明細書において、この署名を第2の署名とも称する。また、この第2の署名の生成に用いられるハッシュ(つまり、第2の署名に対応するハッシュ)を第2のハッシュとも称する。また、ユーザ公開鍵に対応する秘密鍵(つまり、第2の署名の生成に用いられる秘密鍵)を第2の秘密鍵とも称する。

[0033] 例えば、第2の署名がC2PA規格に準拠した方法で生成されることにより、ユーザ権限を有する存在は、ユーザレベル画像検証によって画像の編集の来歴を確認することができる。したがって、本明細書において、第2の署名を来歴確認用署名とも称する。

[0034] 第1の署名(改ざん検知用署名)は、改ざん検知のための検証処理に利用

されるので、最初の画像（例えば、撮像画像）に対して生成される。第2の署名（来歴確認用署名）は、来歴確認のための検証処理に利用されるので、最初の画像（例えば、撮像画像）に対して生成され、その画像に対して編集が行われる度に更新される（新たな署名が生成される）。例えば、編集時、編集を担当したソフトやサーバは、画像の過去の履歴を画像内の公開鍵で確認後、過去のツールの署名や署名対象のデータの一部を新しい画像のメタデータとして引き継ぎ、加えて第2の秘密鍵で署名し、対応するユーザ公開鍵を付与する。

[0035] このような、第1の署名（改ざん検知用署名）と第2の署名（来歴確認用署名）とを、画像やメタデータ等を格納するファイル（画像ファイルとも称する）に格納する。

[0036] 例えば、第1の画像処理装置（例えば撮像装置）が、撮像画像およびメタデータを用いて、第1の署名（改ざん検知用署名）に対応する第1のハッシュと第2の署名（来歴確認用署名）に対応する第2のハッシュとを生成するハッシュ処理部と、第1の秘密鍵と第1のハッシュとを用いて第1の署名を生成し、第2の秘密鍵と第2のハッシュとを用いて第2の署名を生成する署名生成部と、撮像画像、メタデータ、第1の署名、および第2の署名を格納するファイル（画像ファイル）を生成するファイル生成部とを備える。なお、第1の秘密鍵は、ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵に対応する。また、第2の秘密鍵は、ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する。

[0037] また、第1の画像処理装置（例えば撮像装置）において、撮像画像およびメタデータを用いて、第1の署名（改ざん検知用署名）に対応する第1のハッシュと第2の署名（来歴確認用署名）に対応する第2のハッシュとを生成し、第1の秘密鍵と第1のハッシュとを用いて第1の署名を生成し、第2の秘密鍵と第2のハッシュとを用いて第2の署名を生成し、撮像画像、メタデータ、第1の署名、および第2の署名を格納するファイル（画像ファイル）を生成する。なお、第1の秘密鍵は、ユーザ権限以外の特定の権限を有する

第1の存在にのみ公開される限定公開鍵に対応する。また、第2の秘密鍵は、ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する。

[0038] このようにすることにより、画像検証時にそれらの署名を適用することができる。つまり、高レベル画像検証やユーザレベル画像検証を実現することができる。

[0039] したがって、「ユーザ権限を有する存在」が画像を編集したり、ユーザレベル画像検証を実行したりすることができる。つまり、より多様な存在が、画像を編集したり、画像の編集の来歴を確認したりすることができる。また、「特定の権限を有する存在」のみが、高レベル画像検証を実行することができる。つまり、より強力な画像検証を実行することができるだけでなく、その手法の公開範囲が制限されることにより、より安全な画像検証システムを実現することができる。つまり、情報漏洩等による画像検証システムの破綻を抑制することができる。

[0040] 換言するに、上述の方法1を適用することにより、例えば、署名検証を限定し、強力な改ざん検出を実現するユースケースと、他社に署名検証を許し編集来歴の維持を実現するユースケースの両方に対応することができる。すなわち、撮像画像のユーザビリティ（使いやすさ）の低減を抑制することができる。

[0041] なお、高レベル画像検証の際に使用される限定公開鍵は、漏洩のおそれにより少ない方法で提供されることが望ましい。例えば、限定公開鍵が所定の方法で暗号化されて供給されてもよい。つまり、高レベル画像検証において、暗号化された限定公開鍵を復号して利用するようにしてもよい。また、この限定公開鍵は、何処から提供されてもよい。例えば、限定公開鍵を管理するサーバから提供されてもよいし、暗号化された状態で画像ファイルに格納されてもよい。例えば、撮像装置が暗号化された限定公開鍵を予め有し、その限定公開鍵を画像ファイルに格納してもよい。

[0042] また、ユーザ公開鍵は、何処から提供されてもよい。例えば、画像ファイルに格納されてもよい。例えば、撮像装置が予めユーザ公開鍵を有し、その

ユーザ公開鍵を画像ファイルに格納してもよい。

[0043] また、限定公開鍵に対応する第1の秘密鍵、および、ユーザ公開鍵に対応する第2の秘密鍵は、撮像装置が予め有してもよい。例えば、第1の画像処理装置において、署名生成部が、第1の秘密鍵および第2の秘密鍵を予め保持してもよい。

[0044] なお、改ざん検出用署名および来歴確認用署名を生成する際、改ざん検出用署名を生成してから来歴確認用署名を生成してもよい。例えば、第1の画像処理装置において、ハッシュ処理部が、撮像画像およびメタデータを用いて第1のハッシュを生成し、署名生成部が、第1の秘密鍵とその第1のハッシュとを用いて第1の署名を生成し、ハッシュ処理部が、撮像画像、メタデータ、およびその第1の署名を用いて第2のハッシュを生成し、署名生成部が、第2の秘密鍵とその第2のハッシュとを用いて第2の署名を生成してもよい。

[0045] このようにすることにより、高レベル画像検証を実行せずに、ユーザレベル画像検証を実行することができる。つまり、ユーザ公開鍵を用いた（限定公開鍵を必要とせずに）来歴の確認が実行可能である。つまり、ユーザ権限を有する存在が画像編集の来歴を確認することができる。

[0046] 上述のように、改ざん検知用署名および来歴確認用署名は、最初の画像に対して生成される。例えば、撮像装置において、改ざん検知用署名および来歴確認用署名は、被写体を撮像して得られた撮像画像に対して生成されてもよい。換言するに、撮像装置が、被写体を撮像し、得られた撮像画像とそのメタデータ等を用いて、第1のハッシュおよび第2のハッシュを生成してもよい。例えば、第1の画像処理装置が、被写体を撮像し、撮像画像を生成する撮像部をさらに備えてもよい。そして、ハッシュ処理部が、その生成された撮像画像およびメタデータを用いて、第1のハッシュおよび第2のハッシュを生成してもよい。このようにすることにより、撮像画像についてのより強力な改ざん検出や、その撮像画像に対する編集の来歴の確認が可能になる。

[0047] また、改ざん検出用署名は、画像ファイルの何処に格納されてもよい。例えば、改ざん検出用署名が、画像ファイルの、メタデータを格納する領域に格納されてもよい。例えば、第１の画像処理装置において、ファイル生成部が、ファイルの、メタデータを格納するメタデータ領域に、第１の署名（改ざん検出用署名）を格納してもよい。

[0048] 図２は、画像ファイルの主な構成例を示す図である。図２に示される画像ファイル１０には、画像領域１１、メタデータ領域１２、ハッシュ領域１３、および署名領域１４が形成される。画像領域１１には、例えば、撮像画像（画像、Exif (Exchangeable Image File Format) 等）が格納される。メタデータ領域１２には、例えば、画像/Exifのハッシュ、縮小画像（サムネイルやスクリーンネイル等）、撮影者等といった、メタデータ等が格納される。このメタデータは、例えば、C2PA規格で定義されるメタデータ（C2PAメタ）であってもよい。ハッシュ領域１３には、例えば、メタデータへのリンクとハッシュ等が格納される。署名領域１４には、例えば、電子署名や証明書等が格納される。

[0049] このような構成の画像ファイル１０の、メタデータ領域１２内には、さらに、改ざん検出用署名が格納されている。このように、改ざん検出用署名をメタデータとして画像ファイルに格納することにより、画像に対して編集が行われる場合も、改ざん検出用署名をメタデータとして残すことができる。これにより、編集された画像を格納する画像ファイルについても、高レベル画像検証を実行することができる。

[0050] なお、来歴確認用署名は、署名領域１４に格納される。この来歴確認用署名は、編集の度に生成される。画像が編集される場合の画像ファイルの主な構成例を図３に示す。図３に示される画像ファイル２０は、画像領域２１、メタデータ領域２２－１、ハッシュ領域２３－１、署名領域２４－１、メタデータ領域２２－２、ハッシュ領域２３－２、署名領域２４－２、メタデータ領域２２－３、ハッシュ領域２３－３、および署名領域２４－３を有する。以下の説明において、メタデータ領域２２－１、メタデータ領域２２－２

、およびメタデータ領域 22-3 を互いに区別しない場合、メタデータ領域 22 とともに称する。同様に、ハッシュ領域 23-1、ハッシュ領域 23-2、およびハッシュ領域 23-3 を互いに区別しない場合、ハッシュ領域 23 とともに称する。また、署名領域 24-1、署名領域 24-2、および署名領域 24-3 を互いに区別しない場合、署名領域 24 とともに称する。

[0051] 画像領域には、最新の画像が格納される。つまり、画像領域 21 には、撮像画像から 2 回編集が行われた 2 次編集画像（画像・Exif 等）が格納される。

[0052] メタデータ領域 22-3、ハッシュ領域 23-3、および署名領域 24-3 には、撮像画像からの情報が格納される。つまり、メタデータ領域 22-3 には、撮像画像のメタデータ（例えば、画像/Exif のハッシュ、縮小画像、撮影者等）が格納される。また、このメタデータ領域 22-3 には、画像およびメタデータのハッシュと第 1 の秘密鍵とを用いて生成された改ざん検知用署名も格納される。ハッシュ領域 23-3 には、メタデータ領域 22-3 に格納されるメタデータへのリンクとハッシュが格納される。署名領域 24-3 には、ハッシュ領域 23-3 の情報（画像およびメタデータのハッシュ等）と第 2 の秘密鍵を用いて生成された来歴確認用署名（撮像画像に対応する来歴確認用署名）やユーザ公開鍵等が格納される。

[0053] メタデータ領域 22-2、ハッシュ領域 23-2、および署名領域 24-2 には、撮像画像が編集された 1 次編集画像からの情報が格納される。つまり、メタデータ領域 22-2 には、1 次編集画像のメタデータ（例えば、画像/Exif のハッシュ、縮小画像、編集情報等）が格納される。ハッシュ領域 23-2 には、メタデータ領域 22-2 に格納されるメタデータへのリンクとハッシュが格納される。署名領域 24-2 には、ハッシュ領域 23-2 の情報（画像およびメタデータのハッシュ等）と第 2 の秘密鍵を用いて生成された来歴確認用署名（1 次編集画像に対応する来歴確認用署名）やユーザ公開鍵等が格納される。

[0054] メタデータ領域 22-1、ハッシュ領域 23-1、および署名領域 24-

1 には、1 次編集画像が編集された 2 次編集画像からの情報が格納される。つまり、メタデータ領域 2 2 - 1 には、2 次編集画像のメタデータ（例えば、画像/Exif のハッシュ、縮小画像、編集情報等）が格納される。ハッシュ領域 2 3 - 1 には、メタデータ領域 2 2 - 1 に格納されるメタデータへのリンクとハッシュが格納される。署名領域 2 4 - 1 には、ハッシュ領域 2 3 - 1 の情報（画像およびメタデータのハッシュ等）と第 2 の秘密鍵を用いて生成された来歴確認用署名（2 次編集画像に対応する来歴確認用署名）やユーザ公開鍵等が格納される。

[0055] つまり、1 回編集が追加されると、画像領域 2 1 の画像が更新され、その最新の画像に対応するメタデータ領域 2 2、ハッシュ領域 2 3、および署名領域 2 4 が画像ファイル 2 0 に追加される。元画像（編集前の画像）の情報は、ハッシュ領域 2 3 の情報から参照される。このように、画像ファイル 2 0 には、編集毎に情報が履歴として格納される。そして、各編集についての来歴確認用署名が格納される。したがって、ユーザは、このような構成の画像ファイル 2 0 に対してユーザレベル画像検証を実行することにより、画像編集の来歴を確認することができる。

[0056] このような画像ファイルに格納される撮像画像の真贋の検証を行う検証装置は、限定公開鍵と改ざん検出用署名とを用いてその検証を実行する。

[0057] 例えば、第 2 の画像処理装置（検証装置）が、画像、メタデータ、第 1 の署名（改ざん検知用署名）、および第 2 の署名（来歴確認用署名）が格納されたファイル（画像ファイル）を取得するファイル取得部と、ユーザ権限以外の特定の権限を有する第 1 の存在にのみ公開される限定公開鍵、画像、メタデータ、および第 1 の署名を用いて、画像の真贋を検証する検証部とを備える。

[0058] また、第 2 の画像処理装置（検証装置）において、画像、メタデータ、第 1 の署名（改ざん検知用署名）、および第 2 の署名（来歴確認用署名）が格納されたファイル（画像ファイル）を取得し、ユーザ権限以外の特定の権限を有する第 1 の存在にのみ公開される限定公開鍵、画像、メタデータ、およ

び第1の署名を用いて、画像の真贋を検証する。

[0059] なお、第1の署名は、限定公開鍵に対応する第1の秘密鍵、画像に対応する撮像画像、および撮像画像のメタデータを用いて生成された署名である。第2の署名は、ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する第2の秘密鍵、画像、およびメタデータを用いて生成された署名である。

[0060] 例えば、図3に示される画像ファイル20に対して高レベル画像検証を行う場合、検証装置は、画像ファイル20から必要な部分（撮像画像に関する情報）を抽出して検証を行う。

[0061] このようにすることにより、検証装置は、高レベル画像検証（より強力に改ざんを検知することができる検証）を行うことができる。

[0062] なお、上述したように、この高レベル画像検証において使用される限定公開鍵は、漏洩のおそれがより少ない方法で提供されることが望ましい。例えば、限定公開鍵が所定の方法で暗号化されて供給されてもよい。つまり、高レベル画像検証において、暗号化された限定公開鍵を復号して利用するようにしてもよい。例えば、第2の画像処理装置（検証装置）が、暗号化された限定公開鍵を復号する復号部をさらに備えてもよい。そして、検証部が、その復号された限定公開鍵、画像、メタデータ、および第1の署名を用いて、画像の真贋を検証してもよい。このようにすることにより、限定公開鍵が漏洩することを抑制することができる。

[0063] また、この限定公開鍵は、何処から提供されてもよい。例えば、限定公開鍵を管理するサーバから提供されてもよい。また、暗号化された状態で画像ファイルに格納されてもよい。また、縮小画像やメタデータを用いて高レベル画像検証が行われてもよい。

[0064] 例えば、第2の画像処理装置（検証装置）が、他の装置から供給される「暗号化された限定公開鍵」を取得する限定公開鍵取得部をさらに備えてもよい。そして、復号部が、その取得された「暗号化された限定公開鍵」を復号し、検証部が、その復号された限定公開鍵、画像、メタデータ、および第1

の署名を用いて、画像の真贋を検証してもよい。例えば、専用のサーバにおいて限定公開鍵を管理することにより、限定公開鍵が漏洩することを抑制することができる。また、サーバから限定公開鍵を取得する際に、検証装置がサーバに対して認証処理を行ってもよい。この認証処理の方法はどのような方法であってもよい。認証処理を行うことにより、不正な装置へ限定公開鍵を提供してしまうことを抑制することができる。また、復号部が、暗号化された限定公開鍵をファイルから抽出して復号してもよい。

[0065] <方法 1-1>

上述の方法 1 が適用される場合において、図 1 の表の上から 2 段目に示されるように、各署名の対象を互いに異なる範囲にしてもよい（方法 1-1）。例えば、来歴確認用署名が対象とするデータの範囲を、改ざん検知用署名が対象とするデータの範囲よりも広くしてもよい。例えば、第 1 の画像処理装置（例えば撮像装置）において、ハッシュ処理部が、撮像画像およびメタデータの内の、第 1 の範囲を対象として第 1 のハッシュを生成し、その第 1 の範囲よりも広い第 2 の範囲を対象として第 2 のハッシュを生成してもよい。

[0066] 例えば、来歴確認用署名は撮像画像およびメタデータの全体を対象とし、改ざん検知用署名は、撮像画像およびメタデータの内の、一部のデータを対象外としてもよい。つまり、上述の第 1 の範囲が、撮像画像およびメタデータの内の一部のデータを除く範囲であってもよい。また、上述の第 2 の範囲が、撮像画像およびメタデータの全体であってもよい。

[0067] また、この一部のデータが、撮像画像に対する所定の加工に関するデータであってもよい。例えば、この「所定の加工に関するデータ」が、画像のローテーションに関するデータ、画像のレーティング（星評価）に関するデータ、IPTC（International Press Telecommunications Council）メタデータ等の内の少なくとも 1 つを含むものであってもよい。なお、IPTCメタデータは、IPTCによって策定された、デジタル画像に含まれるメタデータの標準規格に準拠するメタデータである。例えば、IPTCメタデータは、画像の詳細や

、所有権、撮影場所などの情報を含み得る。より具体的には、IPTCメタデータは、画像の説明、記事の見出し、撮影者の名前、画像の著作権を有する法人名、撮影イベント名、撮影場所、画像への編集指示、ステータス、画像の取扱い時の連絡先、画像のライセンス情報、モデルの追加情報等の情報を含み得る。

[0068] 図4は、ハッシュの対象範囲の例を示す図である。図4において、図中右側の太線で示される四角がJPEG (Joint Photographic Experts Group) データ30である。JPEGデータ30は、撮像画像のデータの一例である。図4に示されるように、JPEGデータ30は、S0I31、APP1_32、APP2_33、APP11_34、DQT35、DHT36、S0F37、S0S38、実画像39、EOI40、およびスクリンネイル41を有する。

[0069] S0I (Start Of Image) 31は、JPEGファイルの起点を表すスタートマーカである。APP1_32、APP2_33、APP11_34は、アプリケーションが設定するアプリケーションデータである。例えば、APP1_32にはExifの情報が格納される。APP2_33にはICC (International Color Consortium) プロファイルの情報が格納される。DQT (Define Quantization Table) 35は、量子化テーブルを定義するセグメントである。DHT (Define Huffman Table) 36は、ハフマンテーブルを定義するセグメントである。S0F (Start of Frame) 37は、JPEGファイルの種類や画像サイズ等といった画像の主要な情報が格納されるセグメントである。S0S (Start of Scan) 38は、イメージデータの先頭に設けられ、そのイメージデータの成分などの内容が格納されるセグメントである。実画像39は、イメージデータが格納されるセグメントである。EOI (End Of Image) 40は、JPEGファイルの終わりを表すエンドマーカである。スクリンネイル41は、実画像39に格納される画像の縮小画像 (スクリンネイル) を格納するセグメントである。

[0070] 図中左側のグレーの各四角がそのJPEGデータ30を用いて生成される、改ざん検知用署名 (第1の署名) に対応する第1のハッシュの例 (ハッシュ51からハッシュ57まで) を示す。JPEGデータ30の、各グレー地の四角に

隣接する部分（各四角の右側に位置する部分）が、ハッシュの対象となる部分である。例えば、ハッシュ 5 1 は主に S0I 3 1 に対応する。つまり、ハッシュ 5 1 は S0I 3 1 等を用いて生成される。ハッシュ 5 2 は主に APP1_3 2 に対応する。つまり、ハッシュ 5 2 は APP1_3 2 等を用いて生成される。ハッシュ 5 3 およびハッシュ 5 4 は主に APP2_3 3 に対応する。つまり、ハッシュ 5 3 およびハッシュ 5 4 は APP2_3 3 等を用いて生成される。ハッシュ 5 5 は主に DQT 3 5 から EOI 4 0 までに対応する。つまり、ハッシュ 5 5 は DQT 3 5 から EOI 4 0 まで等を用いて生成される。ハッシュ 5 6 およびハッシュ 5 7 は主に スクリンネイル 4 1 に対応する。つまり、ハッシュ 5 6 およびハッシュ 5 7 は スクリンネイル 4 1 等を用いて生成される。

[0071] つまり、図 4 の例の場合、改ざん検知用署名（第 1 の署名）に対応する第 1 のハッシュは、撮像画像およびメタデータの内、画像のローテーションに関するデータ、画像のレーティング（星評価）に関するデータ、および IPTC メタデータ（IPTC/XML）等を除く範囲（第 1 の範囲）を対象として生成される。このようにすることにより、高レベル画像検証において、撮像画像の回転、撮像画像のレーティング、IPTC メタデータの更新等の編集（加工）が許容される。すなわち、この場合、撮像画像を回転させても撮像画像の改ざんとはみなされない。また、撮像画像に付与するレーティングを更新しても撮像画像の改ざんとはみなされない。また、IPTC メタデータが更新されても撮像画像の改ざんとはみなされない。

[0072] 画像の回転、レーティング、IPTC メタデータの更新等は、比較的一般的に行われる処理であり、現実的には、これらの簡易な加工処理（編集）は改ざんとみなさなくてもよいとする運用方法が考えられる。そのようなケースにおいて、上述のように、第 1 のハッシュの対象から一部のデータを除外することにより、所定の加工（編集）を改ざん検知の対象外とすることができる。例えば、上述のような簡易な加工を改ざん検知の対象外とすることができる。つまり、このように画像およびメタデータの内、一部のデータを改ざん検知用署名の対象外とすることにより、高レベル画像検証において、現実の

運用に対してより適切な改ざん検知を行うことができる。また、その際に、第2のハッシュの対象を画像およびメタデータの全体としてもよい。このようにすることにより、画像およびメタデータのどの部分に対する編集についても来歴を確認することができる。換言するに、第1のハッシュの対象と第2のハッシュの対象とを互いに独立に設定してもよい。

[0073] <方法1-2>

上述の方法1が適用される場合において、図1の表の上から3段目に示されるように、改ざん検知用署名のハッシュをマルチハッシュとしてもよい（方法1-2）。つまり、改ざん検知用署名のハッシュが、互いに異なるデータに対応する複数のハッシュにより構成されてもよい。例えば、第1の画像処理装置（例えば撮像装置）において、ハッシュ処理部が、第1のハッシュを、互いに独立した複数のハッシュにより構成されるマルチハッシュとして生成してもよい。

[0074] マルチハッシュとすることにより、複数のハッシュのそれぞれについて、検証を実行することができる。例えば、第1のハッシュが単一のハッシュにより構成されている場合、第1のハッシュの対象全体についての検証を実行することができるが、その対象の一部についての検証を実行することができない。これに対して、第1のハッシュが互いに独立した複数のハッシュにより構成される場合、仮にその複数のハッシュの内の一部の対象が削除されても、残った（削除されなかった）ハッシュの対象についての検証が可能である。つまり、第1のハッシュの対象の一部についての検証を実行することができる。

[0075] 例えば図4の場合、ハッシュ51からハッシュ57までが互いに独立したハッシュであるとする、仮にハッシュ51の対象が削除されても、ハッシュ52からハッシュ57までの対象についての検証は実行することができる。したがって、より確実に（よりロバストに）高レベル画像検証（すなわち、撮像画像のより強力な検証）を実行することができる。

[0076] なお、来歴確認用署名に対応する第2のハッシュをマルチハッシュにして

もよい。例えば、第1の画像処理装置（例えば撮像装置）において、ハッシュ処理部が、第2のハッシュをマルチハッシュとして生成してもよい。このようにすることにより、第1のハッシュの場合と同様に、第2のハッシュの対象の一部についての検証を実行することができる。つまり、より確実に（よりロバストに）ユーザレベル画像検証（すなわち、来歴の確認）を実行することができる。

[0077] <方法1-2-1>

上述の方法1-2が適用される場合において、図1の表の上から4段目に示されるように、改ざん検知用署名のハッシュの分け方を来歴用署名用のハッシュの分け方よりも細かくしてもよい（方法1-2-1）。つまり、改ざん検知用署名に対応する第1のハッシュが第2のハッシュよりも多くのハッシュにより構成されてもよい。例えば、第1の画像処理装置（例えば撮像装置）において、ハッシュ処理部が、第1のハッシュを、第2のハッシュよりも多くのハッシュにより構成されるマルチハッシュとして生成してもよい。

[0078] ハッシュの分け方（粒度）が細かい程、削除されていない部分をより多く検証することができる。つまり、上述のようにすることにより、高レベル画像検証の方が、ユーザレベル画像検証の場合よりも、削除されていない部分をより多く検証することができる。なお、第2のハッシュはマルチハッシュであってもよいし、マルチハッシュでなくてもよい。

[0079] <方法1-3>

上述の方法1が適用される場合において、図1の表の上から5段目に示されるように、改ざん検知用署名を来歴で伝搬される領域に格納してもよい（方法1-3）。例えば、第1の画像処理装置（例えば撮像装置）において、ファイル生成部が、メタデータ領域内の、来歴で伝搬される領域に第1の署名（改ざん検知用署名）を格納してもよい。

[0080] ここで「来歴で伝搬される領域」とは、画像ファイルの、画像編集が行われても消去されない領域を示す。このような領域に第1の署名を格納することにより、画像に対して編集が行われても、より確実に高レベル画像検証を

実行することができる。

[0081] この「来歴で伝搬される領域」はどのような領域であってもよいが、例えば、ベンダーが拡張することができるベンダーエクステンション領域 (Vendor Extension) であってもよい。例えば、第1の画像処理装置 (例えば撮像装置) において、ファイル生成部が、メタデータ領域内の、ベンダー拡張領域に第1の署名 (改ざん検知用署名) を格納してもよい。例えば、図5に示される画像ファイル70には、画像領域 (Main image) 71、メタデータ (C2PA meta) 領域72、ベンダー拡張領域 (Vendor Extension) 73が形成される。そして、ベンダー拡張領域73には、SOI 81、APP1_82、APP11_83、およびスクリンネイル84等のセグメントが形成される。例えば、このAPP11_83に改ざん検知用署名 (Multi hash for each area and Signature) が格納されてもよい。

[0082] なお、画像ファイルに、来歴で伝搬されるように改ざん検知用署名を格納するための専用領域を新たに設けてもよい。

[0083] <方法1-3-1>

上述の方法1-3が適用される場合において、図1の表の最下段に示されるように、改ざん検知用署名のハッシュをマルチハッシュとし、かつ、来歴で落とされ得る領域 (若しくは落とされる領域) を他と独立にハッシュにしてもよい (方法1-3-1)。つまり、編集により、除去される領域若しくは除去される可能性のある領域については、他の領域とは独立にハッシュを生成するようにしてもよい。例えば、第1の画像処理装置 (例えば撮像装置) において、ハッシュ処理部が、撮像画像およびメタデータの、来歴において除去される領域に対応する除去ハッシュを他と独立に生成し、第1のハッシュを、その除去ハッシュを含む互いに独立した複数のハッシュにより構成されるマルチハッシュとして生成してもよい。

[0084] このようにすることにより、編集によりその領域が除去された場合に、より多くの他の領域について検証を行うことができる。つまり、高レベル画像検証において、より多くの情報を検証することができる。

[0085] ＜組み合わせ＞

＜３．複数の署名の格納＞において上述した各方法は、矛盾が生じない限り、任意の他の方法と組み合わせて適用してもよい。３以上の方法を組み合わせて適用してもよい。例えば、方法１－１から方法１－３－１までの内のいずれか２つ以上を組み合わせて適用してもよい。また、組み合わせ可能な手法は、「方法」として図１の表に示したものだけでなく、＜３．複数の署名の格納＞において上述した全ての要素を含み得る。また、上述した各方法は、上述した以外の他の方法と組み合わせて適用してもよい。

[0086] なお、本明細書において、上位の方法について行った説明は、矛盾が生じない限り、その方法に属する下位の方法にも適用される。例えば、「方法１を適用してもよい」と説明した場合、方法１－１から方法１－３までの各方法を適用することができる。同様に、方法１－２－１を適用することもできるし、方法１－３－１を適用することもできる。

[0087] ＜４．第１の実施の形態＞

 ＜画像処理システム＞

本技術は、撮像画像を処理する画像処理システム（またはシステムを構成する各装置）に適用することができる。図６は、本技術を適用した画像処理システムの構成の一例を示すシステム図である。図６に示される画像処理システム１００は、撮像画像を処理するシステムである。

[0088] 図６においては、装置構成やデータの流れ等の主なものを示しており、図６に示されるものが全てとは限らない。つまり、画像処理システム１００において、図６に示されていない装置が存在したり、図６において矢印等として示されていない処理やデータの流れが存在したりしてもよい。

[0089] 図６に示されるように、画像処理システム１００は、ネットワーク１１０を介して互いに通信可能に接続される撮像装置１１１、検証装置１１２、およびサーバ１１３を有する。なお、図６においては、撮像装置１１１、検証装置１１２、およびサーバ１１３が１台ずつ示されているが、それぞれの数はいくつであってもよい。つまり、撮像装置１１１、検証装置１１２、およ

びサーバ 113 は、それぞれ 2 台以上であってもよい。また、撮像装置 111、検証装置 112、およびサーバ 113 のそれぞれの数は、互いに同一でなくてもよい。また、図 6 においては、ネットワーク 110 として 1 つのネットワークが示されているが、画像処理システム 100 が、複数のネットワークを有してもよい。

[0090] ネットワーク 110 は、各装置間の通信媒体となる通信網である。ネットワーク 110 は、有線通信の通信網であってもよいし、無線通信の通信網であってもよいし、それらの両方を含んでもよい。例えば、有線 LAN (Local Area Network)、無線 LAN、公衆電話回線網、所謂 4G 回線や 5G 回線等の無線移動体用の広域通信網、またはインターネット等であってもよいし、それらの組み合わせであってもよい。また、ネットワーク 110 は、単数の通信網であってもよいし、複数の通信網であってもよい。また、例えば、ネットワーク 110 は、その一部若しくは全部が、例えば USB (Universal Serial Bus) (登録商標) ケーブルや HDMI (High-Definition Multimedia Interface) (登録商標) ケーブル等のような、所定の規格の通信ケーブルにより構成されるようにしてもよい。

[0091] 撮像装置 111 は、被写体の撮像、すなわち、撮像画像 (画像ファイル) の生成に関する処理を行う。例えば、撮像装置 111 は、被写体を撮像し、撮像画像を生成してもよい。撮像装置 111 は、その撮像画像等を格納する画像ファイルを生成してもよい。撮像装置 111 は、改ざん検知用署名を生成し、その画像ファイルに格納してもよい。撮像装置 111 は、来歴確認用署名を生成し、その画像ファイルに格納してもよい。撮像装置 111 は、ネットワーク 110 または記録媒体を介してその画像ファイルを供給してもよい。

[0092] 検証装置 112 は、画像等の検証に関する処理を行う。例えば、検証装置 112 は、ネットワーク 110 または記録媒体を介して画像ファイルを取得してもよい。検証装置 112 は、画像ファイルに格納される画像等の改ざんを検知する検証処理を行ってもよい。また、検証装置 112 は、その検証結

果を表示してもよい。なお、検証装置 112 は、ネットワーク 110 を介して「暗号化された限定公開鍵」を取得し、それを復号し、得られた限定公開鍵を検証処理に利用してもよい。

[0093] サーバ 113 は、限定公開鍵の管理に関する処理を行う。例えば、サーバ 113 は、暗号化された限定公開鍵を管理してもよい。また、サーバ 113 は、ネットワーク 110 を介してその暗号化された限定公開鍵を供給してもよい。

[0094] また、撮像装置 111、検証装置 112、およびサーバ 113 は、ネットワーク 110 を介して通信を行い、情報を授受してもよい。例えば、点線両矢印 121 に示されるように、撮像装置 111 は、画像ファイルを検証装置 112 へ供給してもよい。検証装置 112 は、その画像ファイルを取得してもよい。例えば、この画像ファイルには、撮像画像が格納されてもよい。また、この画像ファイルには、改ざん検知用署名が格納されてもよい。また、この画像ファイルには、来歴確認用署名が格納されてもよい。

[0095] また、点線両矢印 122 に示されるように、サーバ 113 は、自身が管理する限定公開鍵を検証装置 112 へ供給してもよい。検証装置 112 は、その限定公開鍵を取得してもよい。この限定公開鍵は暗号化されていてもよい。

[0096] <撮像装置>

撮像装置 111 は、例えば、デジタルカメラ、スマートフォン、タブレット端末、ノート型パーソナルコンピュータといった、撮像機能を有する情報処理端末装置により構成される。撮像装置 111 が 1 つの装置（電子機器）により構成されてもよいし、複数の装置（電子機器）により構成されてもよい。例えば、撮像装置 111 がデジタルカメラおよびスマートフォンにより構成されてもよい。その場合、例えば、デジタルカメラが撮像画像を生成し、スマートフォンがそれらの署名の生成や、検証装置 112 への供給を行ってもよい。以下においては、撮像装置 111 が 1 つの装置（電子機器）により構成されるものとして説明する。

[0097] 図7は、本技術を適用した画像処理装置の一態様である撮像装置111の構成の一例を示すブロック図である。

[0098] なお、図7においては、処理部やデータの流れ等の主なものを示しており、図7に示されるものが全てとは限らない。つまり、撮像装置111において、図7においてブロックとして示されていない処理部が存在したり、図7において矢印等として示されていない処理やデータの流れが存在したりしてもよい。

[0099] 図7に示されるように撮像装置111は、制御部201、撮像処理部202、入力部203、および出力部204を有する。制御部201は、撮像処理部202内の各処理部を制御する。撮像処理部202は、制御部201により制御されて、撮像に関する処理を行う。入力部203は、例えばボタンやスイッチ等の入力デバイスを有する。入力部203は、その入力デバイスを介してユーザ等の指示入力等を受け付ける。入力部203は、その受け付けた指示等を制御部201へ供給する。制御部201は、その受け付けられた指示等に基づいて撮像処理部202を制御してもよい。出力部204は、例えばモニタやスピーカ等の出力デバイスを有する。出力部204は、その出力デバイスを介して制御部201から供給される情報を、例えば画像や音声等として出力する。制御部201は、例えば制御結果等、任意の情報を出力部204へ供給し、出力させてもよい。

[0100] 撮像処理部202は、光学系221、センサ部222、RAW処理部223、YUV処理部224、縮小画像生成部225、画像情報付加部226、3D情報処理部227、ハッシュ処理部228、署名制御部229、署名生成部230、画像ファイル生成部231、画像ファイル記録部232、および画像ファイル供給部233を有する。

[0101] 光学系221は、例えばレンズ、ミラー、フィルタ、絞り等の光学素子により構成され、被写体からの光線に対して所定の影響を及ぼし、その光線をセンサ部222へ誘導する。つまり、被写体からの光線は、この光学系221を介してセンサ部222に入射する。

- [0102] センサ部222は、光電変換に関する処理を行う。センサ部222は、イメージセンサ241および3D情報センサ242を有する。例えば、センサ部222は、光学系221を介して入射される被写体からの光線を用いて撮像画像や3D情報を生成してもよい。
- [0103] イメージセンサ241は、撮像画像の生成に関する処理を行う。イメージセンサ241は、光電変換素子を有する画素が行列状に配置される画素アレイを有する。例えば、イメージセンサ241は、その画素アレイにおいて、光学系221を介して入射する被写体からの光線を受光し、光電変換して撮像画像（RAW画像またはそのRAW画像から生成されたJPEG（Joint Photographic Experts Group）画像）を生成してもよい。つまり、イメージセンサ241は、被写体を撮像し、その被写体の撮像画像を生成するので、撮像画像生成部とも言える。また、イメージセンサ241は、生成した撮像画像をRAW処理部223へ供給してもよい。
- [0104] 3D情報センサ242は、イメージセンサ241において得られる撮像画像内の複数個所についての距離関連情報をその撮像画像と同一の光軸で検出し、3D情報を生成する。つまり、3D情報センサ242は、3D情報生成部とも言える。例えば、3D情報センサ242は、距離関連情報を検出する所定のセンサデバイスを有する。3D情報センサ242は、そのセンサデバイスにおいて、光学系221を介して入射する被写体からの光線を受光し、距離関連情報を検出して3D情報を生成する。
- [0105] ここで、「同一の光軸」とは、3D情報センサ242へ入射する被写体からの光線が、イメージセンサ241へ入射する被写体からの光線が通過する光学系221を通過することを示す。つまり、イメージセンサ241へ入射する光線と3D情報センサ242へ入射する光線の、少なくとも被写体からセンサ部222までの経路が互いに同一であることを示す。このように、撮像画像および距離関連情報が互いに同一の光軸において検出されることにより、例えば、顔写真等を撮像し、その顔写真の被写体とは別の人物までの距離を検出するといったトリック撮影を行うことが困難になる。つまり、撮像画像

の被写体と3D情報の被写体とが互いに同一である可能性が高くなる。

[0106] また、「距離関連情報」は、撮像装置 1 1 1 (3D情報センサ 2 4 2) から被写体までの距離を示す情報であってもよいし、その距離を導出するための情報であってもよい。例えば、距離関連情報は、デプスマップ、位相差データ、ToF (Time of Flight) データ、または、視差画像の集合等を含み得る。

[0107] 3D情報センサ 2 4 2 は、生成した3D情報を3D情報処理部 2 2 7 へ供給する。

[0108] なお、図 7 においては、イメージセンサ 2 4 1 および3D情報センサ 2 4 2 が別体として構成されているが、イメージセンサ 2 4 1 および3D情報センサ 2 4 2 が一体化されてもよいし、イメージセンサ 2 4 1 が3D情報センサ 2 4 2 を兼ねてもよい。例えば、距離関連情報がToFデータである場合、3D情報センサ 2 4 2 は、イメージセンサ 2 4 1 とは別体の、ToF方式で距離を計測するToFセンサにより構成されてもよい。また、距離関連情報が位相差データである場合、3D情報センサ 2 4 2 は、イメージセンサ 2 4 1 の画素アレイの有効画素領域に形成される像面位相差検出画素により構成されてもよい。像面位相差検出画素は、位相差方式の合焦（オートフォーカス）機能に用いられる画素であり、位相差データを検出し得る。この場合、イメージセンサ 2 4 1 および3D情報センサ 2 4 2 が一体として形成される。また、3D情報センサ 2 4 2 は、イメージセンサ 2 4 1 とは別体の、位相差データを検出する位相差センサにより構成されてもよい。また、距離関連情報が3Dスイングパノラマ撮影等により生成される視差画像の集合である場合、イメージセンサ 2 4 1 が3D情報センサ 2 4 2 を兼ねる。換言するに、この場合、イメージセンサ 2 4 1 が撮像画像および3D情報を生成し、3D情報センサ 2 4 2 は省略し得る。

[0109] 以下においては、特に説明しない限り、3D情報センサ 2 4 2 が、像面位相差検出画素により構成される場合を例に説明する。つまり、3D情報センサ 2 4 2 により、距離関連情報として位相差データが検出される場合を例に説明する。

[0110] RAW処理部 2 2 3 は、RAW画像に関する処理を行う。例えば、RAW処理部 2 2

3は、イメージセンサ241から供給される撮像画像（RAW画像）を取得してもよい。RAW処理部223は、そのRAW画像に対して所定の処理を行ってもよい。この処理の内容は任意である。例えば、ホワイトバランス等の補正であってもよい。RAW処理部223は、処理後のRAW画像をYUV処理部224に供給してもよい。

[0111] YUV処理部224は、YUV画像の生成に関する処理を行う。例えば、YUV処理部224は、RAW処理部223から供給されるRAW画像を取得してもよい。YUV処理部224は、そのRAW画像をYUV画像に変換してもよい。YUV処理部224は、そのYUV画像を符号化し、JPEG画像に変換してもよい。YUV処理部224は、その生成したJPEG画像を縮小画像生成部225へ供給してもよい。なお、イメージセンサ241が撮像画像としてJPEG画像を出力する場合、RAW処理部223およびYUV処理部224を省略し、イメージセンサ241がそのJPEG画像を縮小画像生成部225へ供給するようにしてもよい。

[0112] 縮小画像生成部225は、縮小画像の生成に関する処理を行う。例えば、縮小画像生成部225は、YUV処理部224から供給されるJPEG画像を取得してもよい。縮小画像生成部225は、そのJPEG画像の縮小画像を生成してもよい。なお、以下において、この縮小画像に対して元のJPEG画像を「本画像」とも称する。この縮小画像の生成方法は任意である。例えば、縮小画像生成部225は、本画像の一部の画素値を間引くことにより縮小画像を生成してもよい。縮小画像生成部225は、本画像の所定の部分領域毎に画素値を合成して画素数を低減させることにより、縮小画像を生成してもよい。縮小画像生成部225は、本画像の全画素を見て作るようにしてもよい。タップ数が足りない場合、縮小画像生成部225は、タップ数の足りる倍率の縮小を複数回繰り返し、所望の縮小倍率の縮小画像を生成してもよい。縮小画像生成部225は、生成した縮小画像を、本画像（JPEG画像）とともに画像情報付加部226へ供給する。

[0113] 画像情報付加部226は、画像情報の付加に関する処理を行う。例えば、画像情報付加部226は、縮小画像生成部225から供給される本画像およ

び縮小画像を取得してもよい。画像情報付加部 226 は、その取得した本画像に関する情報である画像情報を生成してもよい。画像情報付加部 226 は、その生成した画像情報を本画像に関連付けてもよい。つまり、画像情報付加部 226 は、画像情報を本画像のメタデータとして生成してもよい。画像情報付加部 226 は、その生成した画像情報を、本画像および縮小画像とともにハッシュ処理部 228 へ供給してもよい。

[0114] 3D情報処理部 227 は、3D情報に対する処理を行う。例えば、3D情報処理部 227 は、3D情報センサ 242 から供給される3D情報を取得してもよい。3D情報処理部 227 は、その取得した3D情報に対する所定の処理を行ってもよい。例えば、3D情報処理部 227 は、その取得した3D情報をハッシュ処理部 228 へ供給してもよい。また、3D情報処理部 227 は、署名制御部 229 の制御に基づいて、署名が生成されない場合、その取得した3D情報を低解像度化し、その低解像度の3D情報をハッシュ処理部 228 へ供給してもよい。また、3D情報処理部 227 は、署名制御部 229 の制御に基づいて、署名が生成される場合、3D情報の低解像度化を省略し、その取得した3D情報をハッシュ処理部 228 へ供給してもよい。3D情報処理部 227 は、3D情報解像度設定部とも言える。また、3D情報処理部 227 は、その取得した3D情報の被写体（測距対象）が平面であるか否かを判定し、その判定結果を署名制御部 229 へ供給してもよい。3D情報処理部 227 は、平面判定部とも言える。

[0115] ハッシュ処理部 228 は、ハッシュの生成に関する処理を行う。例えば、ハッシュ処理部 228 は、画像情報付加部 226 から供給される本画像、縮小画像、および画像情報を取得してもよい。ハッシュ処理部 228 は、3D情報処理部 227 から供給される3D情報を取得してもよい。ハッシュ処理部 228 は、その本画像、画像情報、および3D情報を用いてハッシュ（hash）を生成してもよい。ハッシュ処理部 228 は、生成したハッシュを、本画像、縮小画像、画像情報、および3D情報とともに署名生成部 230 へ供給してもよい。

[0116] なお、ハッシュ処理部 228 は、署名制御部 229 により制御されて駆動

してもよい。つまり、ハッシュ処理部228は、署名制御部229によりハッシュ生成が指示された場合、上述のようにハッシュを生成し、署名制御部229によりハッシュ生成が指示されなかった場合、そのハッシュの生成を省略してもよい。ハッシュの生成が省略される場合、ハッシュ処理部228は、取得した情報（例えば、本画像、縮小画像、画像情報、および3D情報等）を署名生成部230へ供給してもよい。

[0117] 署名制御部229は、署名の制御に関する処理を行う。例えば、署名制御部229は、制御部201を介して入力されるユーザやアプリケーション等からの指示に基づいて、署名を生成するか否かを制御してもよい。署名制御部229は、3D情報処理部227から供給される、3D情報の被写体（測距対象）が平面であるか否かの判定結果に基づいて、署名を生成するか否かを制御してもよい。例えば、署名制御部229は、3D情報の被写体（測距対象）が平面であると判定された場合、署名の生成を省略するように制御してもよい。署名制御部229は、3D情報の被写体（測距対象）が平面でないと判定された場合、署名を生成するように制御してもよい。その制御の際、署名制御部229は、ハッシュ処理部228および署名生成部230を制御することにより、署名を生成するか否かを制御してもよい。例えば、署名制御部229は、署名を生成しないように制御する場合、ハッシュ処理部228に対してハッシュの生成を省略させ、署名生成部230に対して署名の生成を省略させてもよい。署名制御部229は、署名を生成するように制御する場合、ハッシュ処理部228に対してハッシュを生成させ、署名生成部230に対して署名を生成させてもよい。署名制御部229は、署名を生成するか否かを示す制御情報を3D情報処理部227へ供給してもよい。

[0118] 署名生成部230は、署名の生成に関する処理を行う。例えば、署名生成部230は、ハッシュ処理部228から供給されるハッシュやそのハッシュの生成に用いた情報（例えば、本画像、縮小画像、画像情報、および3D情報等）を取得してもよい。署名生成部230は、秘密鍵を用いて、その取得したハッシュを暗号化し、署名（電子署名）を生成してもよい。つまり、署名

生成部 230 は、少なくとも本画像および 3D 情報を含む情報の署名を生成してもよい。したがって、署名生成部 230 は、署名生成部とも言える。署名生成部 230 は、生成した署名を、その署名に対応する情報（例えば、本画像、縮小画像、画像情報、および 3D 情報等）とともに画像ファイル生成部 231 へ供給してもよい。

[0119] なお、署名生成部 230 は、署名制御部 229 により制御されて駆動してもよい。例えば、署名制御部 229 により署名生成が指示された場合、署名生成部 230 は、上述のように署名を生成してもよい。また、署名制御部 229 により署名生成が指示されなかった場合、署名生成部 230 は、その署名の生成を省略してもよい。署名の生成が省略される場合、署名生成部 230 は、ハッシュ処理部 228 から供給された情報（例えば、本画像、縮小画像、画像情報、および 3D 情報等）を画像ファイル生成部 231 へ供給してもよい。

[0120] 画像ファイル生成部 231 は、画像ファイルの生成に関する処理を行う。例えば、画像ファイル生成部 231 は、署名生成部 230 から供給される情報（例えば、本画像、縮小画像、画像情報、3D 情報、および署名等）を取得してもよい。画像ファイル生成部 231 は、所定のフォーマットで画像ファイルを生成し、その取得した情報（例えば、本画像、縮小画像、画像情報、3D 情報、および署名等）をその画像ファイルに格納してもよい。また、画像ファイル生成部 231 は、暗号化された限定公開鍵をその画像ファイルに格納してもよい。画像ファイル生成部 231 は、その画像ファイルを画像ファイル記録部 232 へ供給してもよい。また、画像ファイル生成部 231 は、その画像ファイルを画像ファイル供給部 233 へ供給してもよい。

[0121] 画像ファイル記録部 232 は、画像ファイルの記録に関する処理を行う。画像ファイル記録部 232 は、例えば、磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリなどのリムーバブル記録媒体を駆動し、書き込みや読み出しを行うドライブを有する。例えば、画像ファイル記録部 232 は、画像ファイル生成部 231 から供給される画像ファイルを取得しても

よい。画像ファイル記録部 2 3 2 は、その取得した画像ファイルを、そのドライブを介してリムーバブル記録媒体に記録してもよい。

[0122] 画像ファイル供給部 2 3 3 は、画像ファイルの供給に関する処理を行う。画像ファイル供給部 2 3 3 は、ネットワーク 1 1 0 を介して検証装置 1 1 2 と通信を行う通信機能を有する。例えば、画像ファイル供給部 2 3 3 は、画像ファイル生成部 2 3 1 から供給される画像ファイルを取得してもよい。画像ファイル供給部 2 3 3 は、その通信機能を利用して、取得した画像ファイルを検証装置 1 1 2 へ供給してもよい。

[0123] <検証装置>

検証装置 1 1 2 は、例えば、スマートフォン、タブレット端末、ノート型パーソナルコンピュータ、デスクトップ型パーソナルコンピュータ、専用のコンピュータ、サーバといった、画像表示機能を有する情報処理装置により構成される。検証装置 1 1 2 が 1 つの装置（電子機器）により構成されてもよいし、複数の装置（電子機器）により構成されてもよい。以下においては、検証装置 1 1 2 が 1 つの装置（電子機器）により構成されるものとして説明する。

[0124] 図 8 は、本技術を適用した画像処理装置の一態様である検証装置 1 1 2 の構成の一例を示すブロック図である。

[0125] なお、図 8 においては、処理部やデータの流れ等の主なものを示しており、図 8 に示されるものが全てとは限らない。つまり、検証装置 1 1 2 において、図 8 においてブロックとして示されていない処理部が存在したり、図 8 において矢印等として示されていない処理やデータの流れが存在したりしてもよい。

[0126] 図 8 に示されるように検証装置 1 1 2 は、画像ファイル取得部 3 1 1、ユーザレベル画像検証部 3 1 2、限定公開鍵取得部 3 1 3、限定公開鍵復号部 3 1 4、高レベル画像検証部 3 1 5、および表示部 3 1 6 を有する。

[0127] 画像ファイル取得部 3 1 1 は、画像ファイルの取得に関する処理を行う。画像ファイル取得部 3 1 1 は、ネットワーク 1 1 0 を介して撮像装置 1 1 1

と通信を行う通信機能を有する。例えば、画像ファイル取得部 311 は、その通信機能を利用して、撮像装置 111 から供給される画像ファイルを取得してもよい。画像ファイル取得部 311 は、その取得した画像ファイルをユーザレベル画像検証部 312 へ供給してもよい。画像ファイル取得部 311 は、その画像ファイルを限定公開鍵復号部 314 へ供給してもよい。

[0128] ユーザレベル画像検証部 312 は、ユーザレベル画像検証に関する処理を実行する。例えば、ユーザレベル画像検証部 312 は、画像ファイル取得部 311 から供給される画像ファイルを取得してもよい。ユーザレベル画像検証部 312 は、その取得した画像ファイルに格納される来歴確認用署名やユーザ公開鍵等を用いて、ユーザレベル画像検証処理を実行してもよい。このユーザレベル画像検証処理は、その画像ファイルに格納される画像に対する編集の来歴を確認するための検証処理である。ユーザレベル画像検証部 312 は、そのユーザレベル画像検証の結果（来歴の確認結果）を示す情報を表示部 316 へ供給してもよい。

[0129] 限定公開鍵取得部 313 は、限定公開鍵の取得に関する処理を実行する。例えば、限定公開鍵取得部 313 は、ネットワーク 110 を介してサーバ 113 と通信を行う通信機能を有する。例えば、限定公開鍵取得部 313 は、その通信機能を利用して、サーバ 113 に対して限定公開鍵を要求してもよい。その際、限定公開鍵取得部 313 は、サーバ 113 と通信を行い、検証装置 112 をサーバ 113 へ認証させる認証処理を行ってもよい。限定公開鍵取得部 313 は、その通信機能を利用して、その要求に対応してサーバ 113 から供給される限定公開鍵を取得してもよい。この限定公開鍵は暗号化されていてもよい。限定公開鍵取得部 313 は、その取得した限定公開鍵（暗号化された限定公開鍵）を限定公開鍵復号部 314 へ供給してもよい。

[0130] 限定公開鍵復号部 314 は、暗号化された限定公開鍵の復号に関する処理を行う。例えば、限定公開鍵復号部 314 は、限定公開鍵取得部 313 から限定公開鍵が供給される場合、その限定公開鍵を取得してもよい。限定公開鍵復号部 314 は、画像ファイル取得部 311 から画像ファイルを取得して

もよい。限定公開鍵復号部 314 は、限定公開鍵取得部 313 から取得した限定公開鍵が暗号化されている場合、その暗号化された限定公開鍵を復号してもよい。限定公開鍵復号部 314 は、その復号により得られた限定公開鍵を画像ファイルとともに高レベル画像検証部 315 へ供給してもよい。

[0131] また、限定公開鍵復号部 314 は、画像ファイル取得部 311 から取得した画像ファイルに「暗号化された限定公開鍵」が格納されている場合、その暗号化された限定公開鍵を抽出してもよい。そして、限定公開鍵復号部 314 は、その抽出した「暗号化された限定公開鍵」を復号してもよい。限定公開鍵復号部 314 は、その復号により得られた限定公開鍵を画像ファイルとともに高レベル画像検証部 315 へ供給してもよい。

[0132] 高レベル画像検証部 315 は、高レベル画像検証に関する処理を実行する。例えば、高レベル画像検証部 315 は、限定公開鍵復号部 314 から供給される限定公開鍵および画像ファイルを取得してもよい。高レベル画像検証部 315 は、その取得した限定公開鍵や、画像ファイルに格納される改ざん検知用署名等を用いて、高レベル画像検証処理を実行してもよい。この高レベル画像検証処理は、その画像ファイルに格納される撮像画像の改ざんを検知するための検証処理である。高レベル画像検証部 315 は、その高レベル画像検証の結果（改ざん検知の結果）を示す情報を表示部 316 へ供給してもよい。

[0133] 表示部 316 は、情報の表示に関する処理を行う。表示部 316 は、例えば液晶モニタ等の画像表示デバイスを有する。この画像表示デバイスは画像を表示できるものであればどのようなデバイスであってもよい。例えば、表示部 316 は、ユーザレベル画像検証部 312 から供給されるユーザレベル画像検証の結果を示す情報を取得してもよい。表示部 316 は、その取得した情報を表示するための画像情報を生成し、その画像表示デバイスを用いて、その画像情報を表示してもよい。また、表示部 316 は、高レベル画像検証部 315 から供給される高レベル画像検証の結果を示す情報を取得してもよい。表示部 316 は、その取得した情報を表示するための画像情報を生成

し、その画像表示デバイスを用いて、その画像情報を表示してもよい。

[0134] <サーバ>

サーバ113は、例えば、単数の情報処理装置により構成されてもよいし、複数の情報処理装置に構成されてもよい。また、サーバ113は、ネットワークを介して複数の装置で分担、共同して処理するクラウドコンピューティング（つまり、クラウドサーバ）として実施するようにしてもよい。

[0135] 図9は、本技術を適用した画像処理装置の一態様であるサーバ113の構成の一例を示すブロック図である。

[0136] なお、図9においては、処理部やデータの流れ等の主なものを示しており、図9に示されるものが全てとは限らない。つまり、サーバ113において、図9においてブロックとして示されていない処理部が存在したり、図9において矢印等として示されていない処理やデータの流れが存在したりしてもよい。

[0137] 図9に示されるようにサーバ113は、限定公開鍵管理部411、限定公開鍵提供部412、および認証部413を有する。

[0138] 限定公開鍵管理部411は、限定公開鍵の管理に関する処理を実行する。例えば、限定公開鍵管理部411は、任意の記憶媒体を有し、撮像装置111が使用する第1の秘密鍵に対応する限定公開鍵をその記憶媒体に保持し、管理してもよい。限定公開鍵管理部411は、限定公開鍵提供部412から限定公開鍵を要求されると、その要求された限定公開鍵を記憶媒体から読み出し、要求元である限定公開鍵提供部412へ供給してもよい。

[0139] 限定公開鍵提供部412は、限定公開鍵の提供に関する処理を行う。例えば、限定公開鍵提供部412は、ネットワーク110を介して検証装置112と通信を行う通信機能を有する。例えば、限定公開鍵提供部412は、その通信により、検証装置112から供給される限定公開鍵の要求を受け付けてもよい。限定公開鍵提供部412は、その要求において指定される限定公開鍵を限定公開鍵管理部411に対して要求してもよい。

[0140] なお、限定公開鍵提供部412は、認証部413により認証された検証装

置 1 1 2 からの要求を受け付けてもよい。つまり、限定公開鍵提供部 4 1 2 は、認証部 4 1 3 から供給される検証装置 1 1 2 の認証結果を示す情報を取得してもよい。限定公開鍵提供部 4 1 2 は、その認証結果において検証装置 1 1 2 が認証された場合、その検証装置 1 1 2 から供給される限定公開鍵の要求を受け付けてもよい。そして、限定公開鍵提供部 4 1 2 は、その要求において指定される限定公開鍵を限定公開鍵管理部 4 1 1 に対して要求してもよい。

[0141] また、限定公開鍵提供部 4 1 2 は、限定公開鍵管理部 4 1 1 から供給される限定公開鍵を取得してもよい。限定公開鍵提供部 4 1 2 は、その取得した限定公開鍵を、ネットワーク 1 1 0 を介して検証装置 1 1 2 へ供給してもよい。

[0142] なお、この検証装置 1 1 2 へ供給する限定公開鍵は暗号化されていてもよい。つまり、限定公開鍵提供部 4 1 2 が、取得した限定公開鍵を暗号化し、その暗号化された限定公開鍵を検証装置 1 1 2 へ供給してもよい。また、限定公開鍵管理部 4 1 1 が暗号化された限定公開鍵を管理し、限定公開鍵提供部 4 1 2 へ供給してもよい。その場合、限定公開鍵提供部 4 1 2 は、その暗号化された限定公開鍵を取得し、検証装置 1 1 2 へ供給してもよい。

[0143] 認証部 4 1 3 は、検証装置 1 1 2 の認証に関する処理を実行する。例えば、認証部 4 1 3 は、ネットワーク 1 1 0 を介して検証装置 1 1 2 と通信を行う通信機能を有する。例えば、認証部 4 1 3 は、検証装置 1 1 2 と通信を行い、その検証装置 1 1 2 の認証処理を行ってもよい。認証部 4 1 3 は、その認証結果を示す情報を限定公開鍵提供部 4 1 2 へ供給してもよい。

[0144] <本技術の適用>

このような構成の画像処理システム 1 0 0（の各装置）において、<3. 複数の署名の格納>において上述した各種方法（本技術）を適用してもよい。例えば、上述した方法 1 を適用してもよい。つまり、公開範囲が互いに異なる公開鍵に対応する複数の署名をファイルに格納してもよい。

[0145] 例えば、撮像装置 1 1 1 において、ハッシュ処理部 2 2 8 が、撮像画像お

よびメタデータを用いて、第1の署名（改ざん検知用署名）に対応する第1のハッシュと第2の署名（来歴確認用署名）に対応する第2のハッシュとを生成してもよい。署名生成部230が、第1の秘密鍵と第1のハッシュとを用いて第1の署名を生成してもよい。署名生成部230が、第2の秘密鍵と第2のハッシュとを用いて第2の署名を生成してもよい。画像ファイル生成部231が、撮像画像、メタデータ、第1の署名、および第2の署名を格納するファイル（画像ファイル）を生成してもよい。なお、第1の秘密鍵は、ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵に対応してもよい。また、第2の秘密鍵は、ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応してもよい。

[0146] また、署名生成部230が、第1の秘密鍵および第2の秘密鍵を予め保持してもよい。ハッシュ処理部228が、撮像画像およびメタデータを用いて第1のハッシュを生成し、署名生成部230が、第1の秘密鍵とその第1のハッシュとを用いて第1の署名（改ざん検知用署名）を生成してもよい。そして、ハッシュ処理部228が、撮像画像、メタデータ、およびその第1の署名を用いて第2のハッシュを生成し、署名生成部230が、第2の秘密鍵とその第2のハッシュとを用いて第2の署名を生成してもよい。

[0147] また、イメージセンサ241が、被写体を撮像し、撮像画像を生成してもよい。そして、ハッシュ処理部228が、その生成された撮像画像およびメタデータを用いて、第1のハッシュおよび第2のハッシュを生成してもよい。

[0148] また、画像ファイル生成部231が、ファイルの、メタデータを格納するメタデータ領域に、第1の署名（改ざん検出用署名）を格納してもよい。また、画像ファイル生成部231が、その暗号化された限定公開鍵をファイルに格納してもよい。

[0149] 例えば、検証装置112において、画像ファイル取得部311が、画像、メタデータ、第1の署名（改ざん検知用署名）、および第2の署名（来歴確認用署名）が格納されたファイル（画像ファイル）を取得してもよい。高レ

ベル画像検証部 315 が、ユーザ権限以外の特定の権限を有する第 1 の存在にのみ公開される限定公開鍵、画像、メタデータ、および第 1 の署名を用いて、画像の真贋を検証してもよい。

[0150] また、検証装置 112 において、限定公開鍵復号部 314 が、暗号化された限定公開鍵を復号してもよい。高レベル画像検証部 315 が、その復号された限定公開鍵、画像、メタデータ、および第 1 の署名を用いて、画像の真贋を検証してもよい。

[0151] 例えば、検証装置 112 において、限定公開鍵取得部 313 が、他の装置から供給される「暗号化された限定公開鍵」を取得してもよい。限定公開鍵復号部 314 が、その取得された「暗号化された限定公開鍵」を復号してもよい。また、限定公開鍵復号部 314 が、「暗号化された限定公開鍵」を画像ファイルから抽出して復号してもよい。高レベル画像検証部 315 が、その復号された限定公開鍵、画像、メタデータ、および第 1 の署名を用いて、画像の真贋を検証してもよい。

[0152] また、上述した方法 1-1 を適用してもよい。つまり、各署名の対象を互いに異なる範囲にしてもよい。例えば、撮像装置 111 において、ハッシュ処理部 228 が、撮像画像およびメタデータの内の、第 1 の範囲を対象として第 1 のハッシュを生成してもよい。ハッシュ処理部 228 が、その第 1 の範囲よりも広い第 2 の範囲を対象として第 2 のハッシュを生成してもよい。この第 1 の範囲が、撮像画像およびメタデータの内の一部のデータを除く範囲であってもよい。また、上述の第 2 の範囲が、撮像画像およびメタデータの全体であってもよい。また、この一部のデータが、撮像画像に対する所定の加工に関するデータであってもよい。例えば、この「所定の加工に関するデータ」が、画像のローテーションに関するデータ、画像のレーティング（星評価）に関するデータ、IPTCメタデータ等の内の少なくとも 1 つを含むものであってもよい。

[0153] また、上述した方法 1-2 を適用してもよい。つまり、改ざん検知用署名のハッシュをマルチハッシュとしてもよい。例えば、撮像装置 111 におい

て、ハッシュ処理部 228 が、第 1 のハッシュを、互いに独立した複数のハッシュにより構成されるマルチハッシュとして生成してもよい。また、ハッシュ処理部 228 が、第 2 のハッシュをマルチハッシュとして生成してもよい。

[0154] また、上述した方法 1-2-1 を適用してもよい。つまり、改ざん検知用署名のハッシュの分け方を来歴用署名用のハッシュの分け方よりも細かくしてもよい。つまり、改ざん検知用署名に対応する第 1 のハッシュが第 2 のハッシュよりも多くのハッシュにより構成されてもよい。例えば、撮像装置 111 において、ハッシュ処理部 228 が、第 1 のハッシュを、第 2 のハッシュよりも多くのハッシュにより構成されるマルチハッシュとして生成してもよい。

[0155] また、上述した方法 1-3 を適用してもよい。つまり、改ざん検知用署名を来歴で伝搬される領域に格納してもよい。例えば、撮像装置 111 において、画像ファイル生成部 231 が、メタデータ領域内の、来歴で伝搬される領域に第 1 の署名（改ざん検知用署名）を格納してもよい。画像ファイル生成部 231 が、メタデータ領域内の、ベンダー拡張領域に第 1 の署名（改ざん検知用署名）を格納してもよい。

[0156] また、上述した方法 1-3-1 を適用してもよい。つまり、改ざん検知用署名のハッシュをマルチハッシュとし、かつ、来歴で落とされ得る領域（若しくは落とされる領域）を他と独立にハッシュにしてもよい。つまり、編集により、除去される領域若しくは除去される可能性のある領域については、他の領域とは独立にハッシュを生成するようにしてもよい。例えば、撮像装置 111 において、ハッシュ処理部 228 が、撮像画像およびメタデータの、来歴において除去される領域に対応する除去ハッシュを他と独立に生成し、第 1 のハッシュを、その除去ハッシュを含む互いに独立した複数のハッシュにより構成されるマルチハッシュとして生成してもよい。

[0157] このように各装置を構成することにより、高レベル画像検証やユーザレベル画像検証を実現することができる。例えば、署名検証を限定し、強力な改

ざん検出を実現するユースケースと、他社に署名検証を許し編集来歴の維持を実現するユースケースの両方に対応することができる。すなわち、撮像画像のユーザビリティ（使いやすさ）の低減を抑制することができる。

[0158] <撮像処理の流れ>

図10のフローチャートを参照して、このような撮像装置111により実行される撮像処理の流れの例を説明する。

[0159] 撮像処理が開始されると、制御部201は、ステップS101において、撮像処理部202の電源をオンにし、プレビューを開始する。

[0160] ステップS102において、制御部201は、撮像処理部202の動作モードとして、電子署名モードをオンにする。つまり、制御部201は、撮像処理部202の動作モードを、電子署名を画像ファイルに格納するモードに設定する。

[0161] ステップS103において、センサ部222（イメージセンサ241および3D情報センサ242）は、被写体を撮像し、RAW画像と3D情報を同一光軸で取得する。

[0162] ステップS104において、RAW処理部223は、そのRAW画像に対し、ホワイトバランスの調整等の補正処理を行う。YUV処理部224は、その補正されたRAW画像をYUV画像に変換する。また、YUV処理部224は、そのYUV画像を符号化し、JPEG画像を生成する。縮小画像生成部225は、そのJPEG画像（本画像）を縮小した縮小画像を生成する。この縮小画像の生成方法は任意である。また、縮小画像のサイズは任意である。例えば、縮小画像は、所謂サムネイルであってもよいし、所謂スクリーンネイルであってもよい。画像情報付加部226は、本画像や縮小画像に関する画像情報をメタデータとして生成する。3D情報処理部227は、例えばその3D情報を低解像度化する等、その3D情報に対する所定の処理を行う。

[0163] ステップS105において、ハッシュ処理部228は、撮像画像やメタデータ等を用いて第1のハッシュを生成する。

[0164] ステップS106において、署名生成部230は、第1の秘密鍵を用いて

、その生成した第１のハッシュを暗号化することにより、改ざん検知用署名を生成する。

[0165] ステップＳ１０７において、ハッシュ処理部２２８は、撮像画像やメタデータ等を用いて第２のハッシュを生成する。

[0166] ステップＳ１０８において、署名生成部２３０は、第２の秘密鍵を用いて、その生成した第２のハッシュを暗号化することにより、来歴確認用署名を生成する。

[0167] ステップＳ１０９において、画像ファイル生成部２３１は、撮像画像と改ざん検知用署名と来歴確認用署名等を格納する画像ファイルを生成する。その際、画像ファイル生成部２３１は、その画像ファイルに、撮像画像のメタデータや証明書等を格納してもよい。また、画像ファイル生成部２３１は、その画像ファイルに、暗号化された限定公開鍵を格納してもよい。

[0168] ステップＳ１１０において、画像ファイル記録部２３２は、その画像ファイルを記録する。

[0169] ステップＳ１１１において、画像ファイル供給部２３３は、その画像ファイルを検証装置１１２へ供給する。

[0170] ステップＳ１１１が終了すると撮像処理が終了する。

[0171] このように各処理を実行することにより、撮像装置１１１は、高レベル画像検証やユーザレベル画像検証を実現することができる。例えば、撮像装置１１１は、署名検証を限定し、強力な改ざん検出を実現するユースケースと、他社に署名検証を許し編集来歴の維持を実現するユースケースの両方に対応することができる。すなわち、撮像装置１１１は、撮像画像のユーザビリティ（使いやすさ）の低減を抑制することができる。

[0172] <ユーザレベル画像検証処理の流れ>

検証装置１１２により実行されるユーザレベル画像検証処理の流れの例を、図１１のフローチャートを参照して説明する。

[0173] ユーザレベル画像検証処理が開始されると、画像ファイル取得部３１１は、ステップＳ２０１において、画像ファイルを取得する。この画像ファイル

には、撮像装置（第１の画像処理装置）により生成された撮像画像、その撮像画像のメタデータ、第１の署名（改ざん検知用署名）、および第２の署名（来歴確認用署名）が格納されている。

[0174] ステップＳ２０２において、ユーザレベル画像検証部３１２は、その画像ファイルからユーザ公開鍵を抽出する。

[0175] ステップＳ２０３において、ユーザレベル画像検証部３１２は、その抽出したユーザ公開鍵を用いて、画像ファイルに格納される来歴確認用署名を検証する。

[0176] ステップＳ２０４において、ユーザレベル画像検証部３１２は、その検証の結果、来歴確認用署名が正しいか否かを判定する。来歴確認用署名が正当であると判定された場合、処理はステップＳ２０５へ進む。

[0177] ステップＳ２０５において、表示部３１６は、検証結果を示す画像情報を表示することにより、改ざんが検知されなかった旨を通知する。ステップＳ２０５の処理が終了すると、ユーザレベル画像検証処理が終了する。

[0178] また、ステップＳ２０４において、来歴確認用署名が不正であると判定された場合、処理はステップＳ２０６へ進む。

[0179] ステップＳ２０６において、表示部３１６は、検証結果を示す画像情報を表示することにより、改ざんが検知された旨を通知する。ステップＳ２０６の処理が終了すると、ユーザレベル画像検証処理が終了する。

[0180] <高レベル画像検証処理の流れ>

また、検証装置１１２により実行される高レベル画像検証処理の流れの例を、図１２のフローチャートを参照して説明する。

[0181] 高レベル画像検証処理が開始されると、画像ファイル取得部３１１は、ステップＳ２２１において、画像ファイルを取得する。この画像ファイルには、撮像装置（第１の画像処理装置）により生成された撮像画像、その撮像画像のメタデータ、第１の署名（改ざん検知用署名）、および第２の署名（来歴確認用署名）が格納されている。

[0182] ステップＳ２２２において、限定公開鍵取得部３１３は、暗号化された限

定公開鍵をサーバ 113 から取得する。

[0183] ステップ S 223 において、限定公開鍵復号部 314 は、その暗号化された限定公開鍵を復号する。

[0184] ステップ S 224 において、高レベル画像検証部 315 は、その限定公開鍵を用いて、画像ファイルに格納される改ざん検知用署名を検証する。

[0185] ステップ S 225 において、高レベル画像検証部 315 は、その検証の結果、改ざん検知用署名が正しいか否かを判定する。改ざん検知用署名が正当であると判定された場合、処理はステップ S 226 へ進む。

[0186] ステップ S 226 において、表示部 316 は、検証結果を示す画像情報を表示することにより、改ざんが検知されなかった旨を通知する。ステップ S 226 の処理が終了すると、高レベル画像検証処理が終了する。

[0187] また、ステップ S 225 において、改ざん検知用署名が不正であると判定された場合、処理はステップ S 227 へ進む。

[0188] ステップ S 227 において、表示部 316 は、検証結果を示す画像情報を表示することにより、改ざんが検知された旨を通知する。ステップ S 227 の処理が終了すると、高レベル画像検証処理が終了する。

[0189] <高レベル画像検証処理の流れ>

なお、撮像画像に対して編集が行われ、その履歴が画像ファイルに格納されている場合、高レベル画像検証処理は、図 13 のフローチャートのような流れで実行される。

[0190] 高レベル画像検証処理が開始されると、画像ファイル取得部 311 は、ステップ S 241 において、画像ファイルを取得する。この画像ファイルには、撮像装置（第 1 の画像処理装置）により生成された撮像画像、その撮像画像のメタデータ、第 1 の署名（改ざん検知用署名）、および第 2 の署名（来歴確認用署名）が格納されている。

[0191] ステップ S 242 において、画像ファイル取得部 311 は、画像ファイルから撮像画像部分を抽出する。

[0192] ステップ S 243 において、限定公開鍵取得部 313 は、暗号化された限

定公開鍵をサーバ 1 1 3 から取得する。

[0193] ステップ S 2 4 4 において、限定公開鍵復号部 3 1 4 は、その暗号化された限定公開鍵を復号する。

[0194] ステップ S 2 4 5 において、高レベル画像検証部 3 1 5 は、画像ファイルから抽出した撮像画像部分と、その限定公開鍵を用いて、改ざん検知用署名を検証する。

[0195] ステップ S 2 4 6 において、高レベル画像検証部 3 1 5 は、その検証の結果、改ざん検知用署名が正しいか否かを判定する。改ざん検知用署名が正当であると判定された場合、処理はステップ S 2 4 7 へ進む。

[0196] ステップ S 2 4 7 において、表示部 3 1 6 は、検証結果を示す画像情報を表示することにより、改ざんが検知されなかった旨を通知する。ステップ S 2 4 7 の処理が終了すると、高レベル画像検証処理が終了する。

[0197] また、ステップ S 2 4 6 において、改ざん検知用署名が不正であると判定された場合、処理はステップ S 2 4 8 へ進む。

[0198] ステップ S 2 4 8 において、表示部 3 1 6 は、検証結果を示す画像情報を表示することにより、改ざんが検知された旨を通知する。ステップ S 2 4 8 の処理が終了すると、高レベル画像検証処理が終了する。

[0199] このように各処理を実行することにより、検証装置 1 1 2 は、高レベル画像検証やユーザレベル画像検証を実現することができる。例えば、検証装置 1 1 2 は、署名検証を限定し、強力な改ざん検出を実現するユースケースと、他社に署名検証を許し編集来歴の維持を実現するユースケースの両方に対応することができる。すなわち、検証装置 1 1 2 は、撮像画像のユーザビリティ（使いやすさ）の低減を抑制することができる。

[0200] <高レベル画像検証処理の流れ>

なお、図 1 2 の高レベル画像検証処理において、暗号化された限定公開鍵は、画像ファイルに格納されて検証装置 1 1 2 へ提供されてもよい。その場合の、高レベル画像検証処理の流れを、図 1 4 のフローチャートを参照して説明する。

[0201] 高レベル画像検証処理が開始されると、画像ファイル取得部 311 は、ステップ S 261 において、画像ファイルを取得する。この画像ファイルには、撮像装置（第 1 の画像処理装置）により生成された撮像画像、その撮像画像のメタデータ、第 1 の署名（改ざん検知用署名）、および第 2 の署名（来歴確認用署名）が格納されている。

[0202] ステップ S 262 において、限定公開鍵復号部 314 は、その画像ファイルから、暗号化された限定公開鍵を抽出する。

[0203] ステップ S 263 乃至ステップ S 267 の各処理は、ステップ S 223 乃至ステップ S 227 の各処理（図 12）と同様に実行される。ステップ S 266 またはステップ S 267 の処理が終了すると、高レベル画像検証処理が終了する。

[0204] <高レベル画像検証処理の流れ>

なお、図 13 の高レベル画像検証処理においても同様に、暗号化された限定公開鍵は、画像ファイルに格納されて検証装置 112 へ提供されてもよい。その場合の、高レベル画像検証処理の流れを、図 15 のフローチャートを参照して説明する。

[0205] 高レベル画像検証処理が開始されると、画像ファイル取得部 311 は、ステップ S 281 において、画像ファイルを取得する。この画像ファイルには、撮像装置（第 1 の画像処理装置）により生成された撮像画像、その撮像画像のメタデータ、第 1 の署名（改ざん検知用署名）、および第 2 の署名（来歴確認用署名）が格納されている。

[0206] ステップ S 282 において、画像ファイル取得部 311 は、その画像ファイルから、撮像画像部分を抽出する。

[0207] ステップ S 283 において、限定公開鍵復号部 314 は、その画像ファイルから、暗号化された限定公開鍵を抽出する。

[0208] ステップ S 284 乃至ステップ S 288 の各処理は、ステップ S 244 乃至ステップ S 248 の各処理（図 13）と同様に実行される。ステップ S 287 またはステップ S 288 の処理が終了すると、高レベル画像検証処理が

終了する。

[0209] <限定公開鍵供給処理>

サーバ 113 により実行される限定公開鍵供給処理の流れの例を図 16 のフローチャートを参照して説明する。

[0210] 限定公開鍵供給処理が開始されると、認証部 413 は、ステップ S301 において、認証処理を行う。

[0211] 認証処理が正常に終了し、検証装置 112 が認証されると、ステップ S302 において、限定公開鍵提供部 412 は、その認証された検証装置 112 から限定公開鍵の要求を受け付ける。

[0212] ステップ S303 において、限定公開鍵提供部 412 は、要求された限定公開鍵を限定公開鍵管理部 411 から取得する。

[0213] ステップ S304 において、限定公開鍵提供部 412 は、その取得した限定公開鍵を暗号化し、その暗号化された限定公開鍵を、要求元である検証装置 112 へ供給する。

[0214] ステップ S304 の処理が終了すると、限定公開鍵供給処理が終了する。

[0215] このように各処理を実行することにより、サーバ 113 は、限定公開鍵を検証装置 112 に提供することができる。したがって、サーバ 113 は、撮像画像のユーザビリティ（使いやすさ）の低減を抑制することができる。

[0216] <5. 付記>

 <その他>

上述した本技術の各例（各方法）は、矛盾が生じない限り、他の例（他の方法）と適宜組み合わせて適用してもよい。また、上述した本技術の各例を、上述した以外の他の技術と組み合わせて適用してもよい。

[0217] <コンピュータ>

上述した一連の処理は、ハードウェアにより実行させることもできるし、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行する場合には、そのソフトウェアを構成するプログラムが、コンピュータにインストールされる。ここでコンピュータには、専用のハードウェア

アに組み込まれているコンピュータや、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータ等が含まれる。

[0218] 図17は、上述した一連の処理をプログラムにより実行するコンピュータのハードウェアの構成例を示すブロック図である。

[0219] 図17に示されるコンピュータ900において、CPU (Central Processing Unit) 901、ROM (Read Only Memory) 902、RAM (Random Access Memory) 903は、バス904を介して相互に接続されている。

[0220] バス904にはまた、入出力インタフェース910も接続されている。入出力インタフェース910には、入力部911、出力部912、記憶部913、通信部914、およびドライブ915が接続されている。

[0221] 入力部911は、例えば、キーボード、マウス、マイクロホン、タッチパネル、入力端子などよりなる。出力部912は、例えば、ディスプレイ、スピーカ、出力端子などよりなる。記憶部913は、例えば、ハードディスク、RAMディスク、不揮発性のメモリなどよりなる。通信部914は、例えば、ネットワークインタフェースよりなる。ドライブ915は、磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリなどのリムーバブルメディア921を駆動する。

[0222] 以上のように構成されるコンピュータでは、CPU901が、例えば、記憶部913に記憶されているプログラムを、入出力インタフェース910およびバス904を介して、RAM903にロードして実行することにより、上述した一連の処理が行われる。RAM903にはまた、CPU901が各種の処理を実行する上において必要なデータなども適宜記憶される。

[0223] コンピュータが実行するプログラムは、例えば、パッケージメディア等としてのリムーバブルメディア921に記録して適用することができる。その場合、プログラムは、リムーバブルメディア921をドライブ915に装着することにより、入出力インタフェース910を介して、記憶部913にインストールすることができる。

[0224] また、このプログラムは、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の伝送媒体を介して提供することもできる。その場合、プログラムは、通信部 914 で受信し、記憶部 913 にインストールすることができる。

[0225] その他、このプログラムは、ROM 902 や記憶部 913 に、あらかじめインストールしておくこともできる。

[0226] <本技術の適用可能な対象>

本技術は、任意の符号化・復号方式に適用することができる。

[0227] また、本技術は、任意の構成に適用することができる。例えば、本技術は、様々な電子機器に応用され得る。

[0228] また、例えば、本技術は、システムLSI (Large Scale Integration) 等としてのプロセッサ（例えばビデオプロセッサ）、複数のプロセッサ等を用いるモジュール（例えばビデオモジュール）、複数のモジュール等を用いるユニット（例えばビデオユニット）、または、ユニットにさらにその他の機能を付加したセット（例えばビデオセット）等、装置の一部の構成として実施することもできる。

[0229] また、例えば、本技術は、複数の装置により構成されるネットワークシステムにも適用することもできる。例えば、本技術を、ネットワークを介して複数の装置で分担、共同して処理するクラウドコンピューティングとして実施するようにしてもよい。例えば、コンピュータ、AV (Audio Visual) 機器、携帯型情報処理端末、IoT (Internet of Things) デバイス等の任意の端末に対して、画像（動画画像）に関するサービスを提供するクラウドサービスにおいて本技術を実施するようにしてもよい。

[0230] なお、本明細書において、システムとは、複数の構成要素（装置、モジュール（部品）等）の集合を意味し、全ての構成要素が同一筐体中にあるか否かは問わない。したがって、別個の筐体に収納され、ネットワークを介して接続されている複数の装置、および、1つの筐体の中に複数のモジュールが収納されている1つの装置は、いずれも、システムである。

[0231] <本技術を適用可能な分野・用途>

本技術を適用したシステム、装置、処理部等は、例えば、交通、医療、防犯、農業、畜産業、鉱業、美容、工場、家電、気象、自然監視等、任意の分野に利用することができる。また、その用途も任意である。

[0232] 例えば、本技術は、観賞用コンテンツ等の提供の用に供されるシステムやデバイスに適用することができる。また、例えば、本技術は、交通状況の監視や自動運転制御等、交通の用に供されるシステムやデバイスにも適用することができる。さらに、例えば、本技術は、セキュリティの用に供されるシステムやデバイスにも適用することができる。また、例えば、本技術は、機械等の自動制御の用に供されるシステムやデバイスに適用することができる。さらに、例えば、本技術は、農業や畜産業の用に供されるシステムやデバイスにも適用することができる。また、本技術は、例えば火山、森林、海洋等の自然の状態や野生生物等を監視するシステムやデバイスにも適用することができる。さらに、例えば、本技術は、スポーツの用に供されるシステムやデバイスにも適用することができる。

[0233] <その他>

なお、本明細書において「フラグ」とは、複数の状態を識別するための情報であり、真(1)または偽(0)の2状態を識別する際に用いる情報だけでなく、3以上の状態を識別することが可能な情報も含まれる。したがって、この「フラグ」が取り得る値は、例えば1/0の2値であってもよいし、3値以上であってもよい。すなわち、この「フラグ」を構成するbit数は任意であり、1bitでも複数bitでもよい。また、識別情報（フラグも含む）は、その識別情報をビットストリームに含める形だけでなく、ある基準となる情報に対する識別情報の差分情報をビットストリームに含める形も想定されるため、本明細書においては、「フラグ」や「識別情報」は、その情報だけではなく、基準となる情報に対する差分情報も包含する。

[0234] また、撮像画像に関する各種情報（メタデータ等）は、撮像画像に関連づけられていれば、どのような形態で伝送または記録されるようにしてもよい

。ここで、「関連付ける」という用語は、例えば、一方のデータを処理する際に他方のデータを利用し得る（リンクさせ得る）ようにすることを意味する。つまり、互いに関連付けられたデータは、1つのデータとしてまとめられてもよいし、それぞれ個別のデータとしてもよい。例えば、符号化データ（画像）に関連付けられた情報は、その符号化データ（画像）とは別の伝送路上で伝送されるようにしてもよい。また、例えば、符号化データ（画像）に関連付けられた情報は、その符号化データ（画像）とは別の記録媒体（または同一の記録媒体の別の記録エリア）に記録されるようにしてもよい。なお、この「関連付け」は、データ全体でなく、データの一部であってもよい。例えば、画像とその画像に対応する情報とが、複数フレーム、1フレーム、またはフレーム内の一部分などの任意の単位で互いに関連付けられるようにしてもよい。

[0235] なお、本明細書において、「合成する」、「多重化する」、「付加する」、「一体化する」、「含める」、「格納する」、「入れ込む」、「差し込む」、「挿入する」等の用語は、例えば符号化データとメタデータとを1つのデータにまとめるといった、複数の物を1つにまとめることを意味し、上述の「関連付ける」の1つの方法を意味する。

[0236] また、本技術の実施の形態は、上述した実施の形態に限定されるものではなく、本技術の要旨を逸脱しない範囲において種々の変更が可能である。

[0237] 例えば、1つの装置（または処理部）として説明した構成を分割し、複数の装置（または処理部）として構成するようにしてもよい。逆に、以上において複数の装置（または処理部）として説明した構成をまとめて1つの装置（または処理部）として構成されるようにしてもよい。また、各装置（または各処理部）の構成に上述した以外の構成を付加するようにしてももちろんよい。さらに、システム全体としての構成や動作が実質的に同じであれば、ある装置（または処理部）の構成の一部を他の装置（または他の処理部）の構成に含めるようにしてもよい。

[0238] また、例えば、上述したプログラムは、任意の装置において実行されるよ

うにしてもよい。その場合、その装置が、必要な機能（機能ブロック等）を有し、必要な情報を得ることができるようにすればよい。

[0239] また、例えば、1つのフローチャートの各ステップを、1つの装置が実行するようにしてもよいし、複数の装置が分担して実行するようにしてもよい。さらに、1つのステップに複数の処理が含まれる場合、その複数の処理を、1つの装置が実行するようにしてもよいし、複数の装置が分担して実行するようにしてもよい。換言するに、1つのステップに含まれる複数の処理を、複数のステップの処理として実行することもできる。逆に、複数のステップとして説明した処理を1つのステップとしてまとめて実行することもできる。

[0240] また、例えば、コンピュータが実行するプログラムは、プログラムを記述するステップの処理が、本明細書で説明する順序に沿って時系列に実行されるようにしても良いし、並列に、あるいは呼び出しが行われたとき等の必要なタイミングで個別に実行されるようにしても良い。つまり、矛盾が生じない限り、各ステップの処理が上述した順序と異なる順序で実行されるようにしてもよい。さらに、このプログラムを記述するステップの処理が、他のプログラムの処理と並列に実行されるようにしても良いし、他のプログラムの処理と組み合わせて実行されるようにしても良い。

[0241] また、例えば、本技術に関する複数の技術は、矛盾が生じない限り、それぞれ独立に単体で実施することができる。もちろん、任意の複数の本技術を併用して実施することもできる。例えば、いずれかの実施の形態において説明した本技術の一部または全部を、他の実施の形態において説明した本技術の一部または全部と組み合わせて実施することもできる。また、上述した任意の本技術の一部または全部を、上述していない他の技術と併用して実施することもできる。

[0242] なお、本技術は以下のような構成も取ることができる。

(1) 撮像画像およびメタデータを用いて、第1の署名に対応する第1のハッシュと第2の署名に対応する第2のハッシュとを生成するハッシュ処

理部と、

第 1 の秘密鍵と前記第 1 のハッシュとを用いて前記第 1 の署名を生成し、
第 2 の秘密鍵と前記第 2 のハッシュとを用いて前記第 2 の署名を生成する署名生成部と、

前記撮像画像、前記メタデータ、前記第 1 の署名、および前記第 2 の署名を格納するファイルを生成するファイル生成部と

を備え、

前記第 1 の秘密鍵は、ユーザ権限以外の特定の権限を有する第 1 の存在にのみ公開される限定公開鍵に対応し、

前記第 2 の秘密鍵は、前記ユーザ権限を有する第 2 の存在にも公開されるユーザ公開鍵に対応する

画像処理装置。

(2) 被写体を撮像し、前記撮像画像を生成する撮像部をさらに備え、
前記ハッシュ処理部は、生成された前記撮像画像および前記メタデータを用いて、前記第 1 のハッシュおよび前記第 2 のハッシュを生成するように構成される

(1) に記載の画像処理装置。

(3) 前記署名生成部は、前記第 1 の秘密鍵および前記第 2 の秘密鍵を予め保持するように構成される

(1) または (2) に記載の画像処理装置。

(4) 前記ハッシュ処理部が、前記撮像画像および前記メタデータを用いて前記第 1 のハッシュを生成し、

前記署名生成部が、前記第 1 の秘密鍵と前記第 1 のハッシュとを用いて前記第 1 の署名を生成し、

前記ハッシュ処理部が、前記撮像画像、前記メタデータ、および前記第 1 の署名を用いて前記第 2 のハッシュを生成し、

前記署名生成部が、前記第 2 の秘密鍵と前記第 2 のハッシュとを用いて前記第 2 の署名を生成する

ように構成される（１）から（３）までのいずれかに記載の画像処理装置。

（５） 前記ハッシュ処理部は、前記撮像画像および前記メタデータの内の、第１の範囲を対象として前記第１のハッシュを生成し、前記第１の範囲よりも広い第２の範囲を対象として前記第２のハッシュを生成するように構成される

（１）から（４）までのいずれかに記載の画像処理装置。

（６） 前記第１の範囲は、前記撮像画像および前記メタデータの内の一部のデータを除く範囲であり、

前記第２の範囲は、前記撮像画像および前記メタデータの全体である

（５）に記載の画像処理装置。

（７） 前記一部のデータは、前記撮像画像に対する所定の加工に関するデータである

（６）に記載の画像処理装置。

（８） 前記所定の加工に関するデータは、ローテーションに関するデータ、レーティングに関するデータ、およびIPTC（International Press Telecommunications Council）メタデータの内の少なくとも１つを含む

（７）に記載の画像処理装置。

（９） 前記ハッシュ処理部は、前記第１のハッシュを、互いに独立した複数のハッシュにより構成されるマルチハッシュとして生成するように構成される

（１）から（８）までのいずれかに記載の画像処理装置。

（１０） 前記ハッシュ処理部は、前記第２のハッシュを前記マルチハッシュとして生成するように構成される

（９）に記載の画像処理装置。

（１１） 前記ハッシュ処理部は、前記第１のハッシュを、前記第２のハッシュよりも多くのハッシュにより構成される前記マルチハッシュとして生成するように構成される

(9) または (10) に記載の画像処理装置。

(12) 前記ファイル生成部は、前記ファイルの、前記メタデータを格納するメタデータ領域に前記第1の署名を格納するように構成される

(1) から (11) までのいずれかに記載の画像処理装置。

(13) 前記ファイル生成部は、前記メタデータ領域内の、来歴で伝搬される領域に前記第1の署名を格納するように構成される

(12) に記載の画像処理装置。

(14) 前記ファイル生成部は、前記メタデータ領域内の、ベンダー拡張領域に前記第1の署名を格納するように構成される

(13) に記載の画像処理装置。

(15) 前記ハッシュ処理部は、前記撮像画像および前記メタデータの、前記来歴において除去される領域に対応する除去ハッシュを他と独立に生成し、前記第1のハッシュを、前記除去ハッシュを含む互いに独立した複数のハッシュにより構成されるマルチハッシュとして生成する

(14) に記載の画像処理装置。

(16) 前記ファイル生成部は、暗号化された前記限定公開鍵を前記ファイルに格納するように構成される

(1) から (15) までに記載の画像処理装置。

(17) 撮像画像およびメタデータを用いて、第1の署名に対応する第1のハッシュと第2の署名に対応する第2のハッシュとを生成し、

第1の秘密鍵と前記第1のハッシュとを用いて前記第1の署名を生成し、
第2の秘密鍵と前記第2のハッシュとを用いて前記第2の署名を生成し、

前記撮像画像、前記メタデータ、前記第1の署名、および前記第2の署名を格納するファイルを生成し、

前記第1の秘密鍵は、ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵に対応し、

前記第2の秘密鍵は、前記ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する

画像処理方法。

[0243] (18) 画像、メタデータ、第1の署名、および第2の署名が格納されたファイルを取得するファイル取得部と、

ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵、前記画像、前記メタデータ、および前記第1の署名を用いて、前記画像の真贋を検証する検証部と

を備え、

前記第1の署名は、前記限定公開鍵に対応する第1の秘密鍵、前記画像に対応する撮像画像、および前記撮像画像のメタデータを用いて生成された署名であり、

前記第2の署名は、前記ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する第2の秘密鍵、前記画像、および前記メタデータを用いて生成された署名である

画像処理装置。

(19) 暗号化された前記限定公開鍵を復号する復号部をさらに備え、前記検証部は、復号された前記限定公開鍵、前記画像、前記メタデータ、および前記第1の署名を用いて、前記画像の真贋を検証するように構成される

(18)に記載の画像処理装置。

(20) 他の装置から供給される、暗号化された前記限定公開鍵を取得する限定公開鍵取得部をさらに備え、

前記復号部は、取得された、暗号化された前記限定公開鍵を復号するように構成される

(19)に記載の画像処理装置。

(21) 前記復号部は、暗号化された前記限定公開鍵を前記ファイルから抽出して復号するように構成される

(19)に記載の画像処理装置。

(22) 画像、メタデータ、第1の署名、および第2の署名が格納され

たファイルを取得し、

ユーザ権限以外の特定の権限を有する第１の存在にのみ公開される限定公開鍵、前記画像、前記メタデータ、および前記第１の署名を用いて、前記画像の真贋を検証し、

前記第１の署名は、前記限定公開鍵に対応する第１の秘密鍵、前記画像に対応する撮像画像、および前記撮像画像のメタデータを用いて生成された署名であり、

前記第２の署名は、前記ユーザ権限を有する第２の存在にも公開されるユーザ公開鍵に対応する第２の秘密鍵、前記画像、および前記メタデータを用いて生成された署名である

画像処理方法。

符号の説明

[0244] １００ 画像処理システム, １１０ ネットワーク, １１１ 撮像装置, １１２ 検証装置, １１３ サーバ, ２０１ 制御部, ２０２ 撮像処理部, ２２１ 光学系, ２２２ センサ部, ２２８ ハッシュ処理部, ２２９ 署名制御部, ２３０ 署名生成部, ２３１ 画像ファイル生成部, ２３２ 画像ファイル記録部, ２３３ 画像ファイル供給部, ３１１ 画像ファイル取得部, ３１２ ユーザレベル画像検証部, ３１３ 限定公開鍵取得部, ３１４ 限定公開鍵復号部, ３１５ 高レベル画像検証部, ３１６ 表示部, ４１１ 限定公開鍵管理部, ４１２ 限定公開鍵提供部, ４１３ 認証部, ９００ コンピュータ

請求の範囲

- [請求項1] 撮像画像およびメタデータを用いて、第1の署名に対応する第1のハッシュと第2の署名に対応する第2のハッシュとを生成するハッシュ処理部と、
- 第1の秘密鍵と前記第1のハッシュとを用いて前記第1の署名を生成し、第2の秘密鍵と前記第2のハッシュとを用いて前記第2の署名を生成する署名生成部と、
- 前記撮像画像、前記メタデータ、前記第1の署名、および前記第2の署名を格納するファイルを生成するファイル生成部と
- を備え、
- 前記第1の秘密鍵は、ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵に対応し、
- 前記第2の秘密鍵は、前記ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する
- 画像処理装置。
- [請求項2] 被写体を撮像し、前記撮像画像を生成する撮像部をさらに備え、
- 前記ハッシュ処理部は、生成された前記撮像画像および前記メタデータを用いて、前記第1のハッシュおよび前記第2のハッシュを生成するように構成される
- 請求項1に記載の画像処理装置。
- [請求項3] 前記署名生成部は、前記第1の秘密鍵および前記第2の秘密鍵を予め保持するように構成される
- 請求項1に記載の画像処理装置。
- [請求項4] 前記ハッシュ処理部が、前記撮像画像および前記メタデータを用いて前記第1のハッシュを生成し、
- 前記署名生成部が、前記第1の秘密鍵と前記第1のハッシュとを用いて前記第1の署名を生成し、
- 前記ハッシュ処理部が、前記撮像画像、前記メタデータ、および前

記第 1 の署名を用いて前記第 2 のハッシュを生成し、

前記署名生成部が、前記第 2 の秘密鍵と前記第 2 のハッシュとを用いて前記第 2 の署名を生成する

ように構成される請求項 1 に記載の画像処理装置。

[請求項5] 前記ハッシュ処理部は、前記撮像画像および前記メタデータの内の、第 1 の範囲を対象として前記第 1 のハッシュを生成し、前記第 1 の範囲よりも広い第 2 の範囲を対象として前記第 2 のハッシュを生成するように構成される

請求項 1 に記載の画像処理装置。

[請求項6] 前記第 1 の範囲は、前記撮像画像および前記メタデータの内の一部のデータを除く範囲であり、

前記第 2 の範囲は、前記撮像画像および前記メタデータの全体である

請求項 5 に記載の画像処理装置。

[請求項7] 前記一部のデータは、前記撮像画像に対する所定の加工に関するデータである

請求項 6 に記載の画像処理装置。

[請求項8] 前記所定の加工に関するデータは、ローテーションに関するデータ、レーティングに関するデータ、およびIPTC (International Press Telecommunications Council) メタデータの内の少なくとも 1 つを含む

請求項 7 に記載の画像処理装置。

[請求項9] 前記ハッシュ処理部は、前記第 1 のハッシュを、互いに独立した複数のハッシュにより構成されるマルチハッシュとして生成するように構成される

請求項 1 に記載の画像処理装置。

[請求項10] 前記ハッシュ処理部は、前記第 2 のハッシュを前記マルチハッシュとして生成するように構成される

請求項 9 に記載の画像処理装置。

[請求項11] 前記ハッシュ処理部は、前記第 1 のハッシュを、前記第 2 のハッシュよりも多くのハッシュにより構成される前記マルチハッシュとして生成するように構成される

請求項 9 に記載の画像処理装置。

[請求項12] 前記ファイル生成部は、前記ファイルの、前記メタデータを格納するメタデータ領域に前記第 1 の署名を格納するように構成される

請求項 1 に記載の画像処理装置。

[請求項13] 前記ファイル生成部は、前記メタデータ領域内の、来歴で伝搬される領域に前記第 1 の署名を格納するように構成される

請求項 1 2 に記載の画像処理装置。

[請求項14] 前記ファイル生成部は、前記メタデータ領域内の、ベンダー拡張領域に前記第 1 の署名を格納するように構成される

請求項 1 3 に記載の画像処理装置。

[請求項15] 前記ハッシュ処理部は、前記撮像画像および前記メタデータの、前記来歴において除去される領域に対応する除去ハッシュを他と独立に生成し、前記第 1 のハッシュを、前記除去ハッシュを含む互いに独立した複数のハッシュにより構成されるマルチハッシュとして生成する

請求項 1 4 に記載の画像処理装置。

[請求項16] 前記ファイル生成部は、暗号化された前記限定公開鍵を前記ファイルに格納するように構成される

請求項 1 に記載の画像処理装置。

[請求項17] 撮像画像およびメタデータを用いて、第 1 の署名に対応する第 1 のハッシュと第 2 の署名に対応する第 2 のハッシュとを生成し、

第 1 の秘密鍵と前記第 1 のハッシュとを用いて前記第 1 の署名を生成し、第 2 の秘密鍵と前記第 2 のハッシュとを用いて前記第 2 の署名を生成し、

前記撮像画像、前記メタデータ、前記第 1 の署名、および前記第 2

の署名を格納するファイルを生成し、

前記第1の秘密鍵は、ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵に対応し、

前記第2の秘密鍵は、前記ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する

画像処理方法。

[請求項18]

画像、メタデータ、第1の署名、および第2の署名が格納されたファイルを取得するファイル取得部と、

ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵、前記画像、前記メタデータ、および前記第1の署名を用いて、前記画像の真贋を検証する検証部と

を備え、

前記第1の署名は、前記限定公開鍵に対応する第1の秘密鍵、前記画像に対応する撮像画像、および前記撮像画像のメタデータを用いて生成された署名であり、

前記第2の署名は、前記ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する第2の秘密鍵、前記画像、および前記メタデータを用いて生成された署名である

画像処理装置。

[請求項19]

暗号化された前記限定公開鍵を復号する復号部をさらに備え、

前記検証部は、復号された前記限定公開鍵、前記画像、前記メタデータ、および前記第1の署名を用いて、前記画像の真贋を検証するように構成される

請求項18に記載の画像処理装置。

[請求項20]

他の装置から供給される、暗号化された前記限定公開鍵を取得する限定公開鍵取得部をさらに備え、

前記復号部は、取得された、暗号化された前記限定公開鍵を復号するように構成される

請求項 19 に記載の画像処理装置。

[請求項21] 前記復号部は、暗号化された前記限定公開鍵を前記ファイルから抽出して復号するように構成される

請求項 19 に記載の画像処理装置。

[請求項22] 画像、メタデータ、第1の署名、および第2の署名が格納されたファイルを取得し、

ユーザ権限以外の特定の権限を有する第1の存在にのみ公開される限定公開鍵、前記画像、前記メタデータ、および前記第1の署名を用いて、前記画像の真贋を検証し、

前記第1の署名は、前記限定公開鍵に対応する第1の秘密鍵、前記画像に対応する撮像画像、および前記撮像画像のメタデータを用いて生成された署名であり、

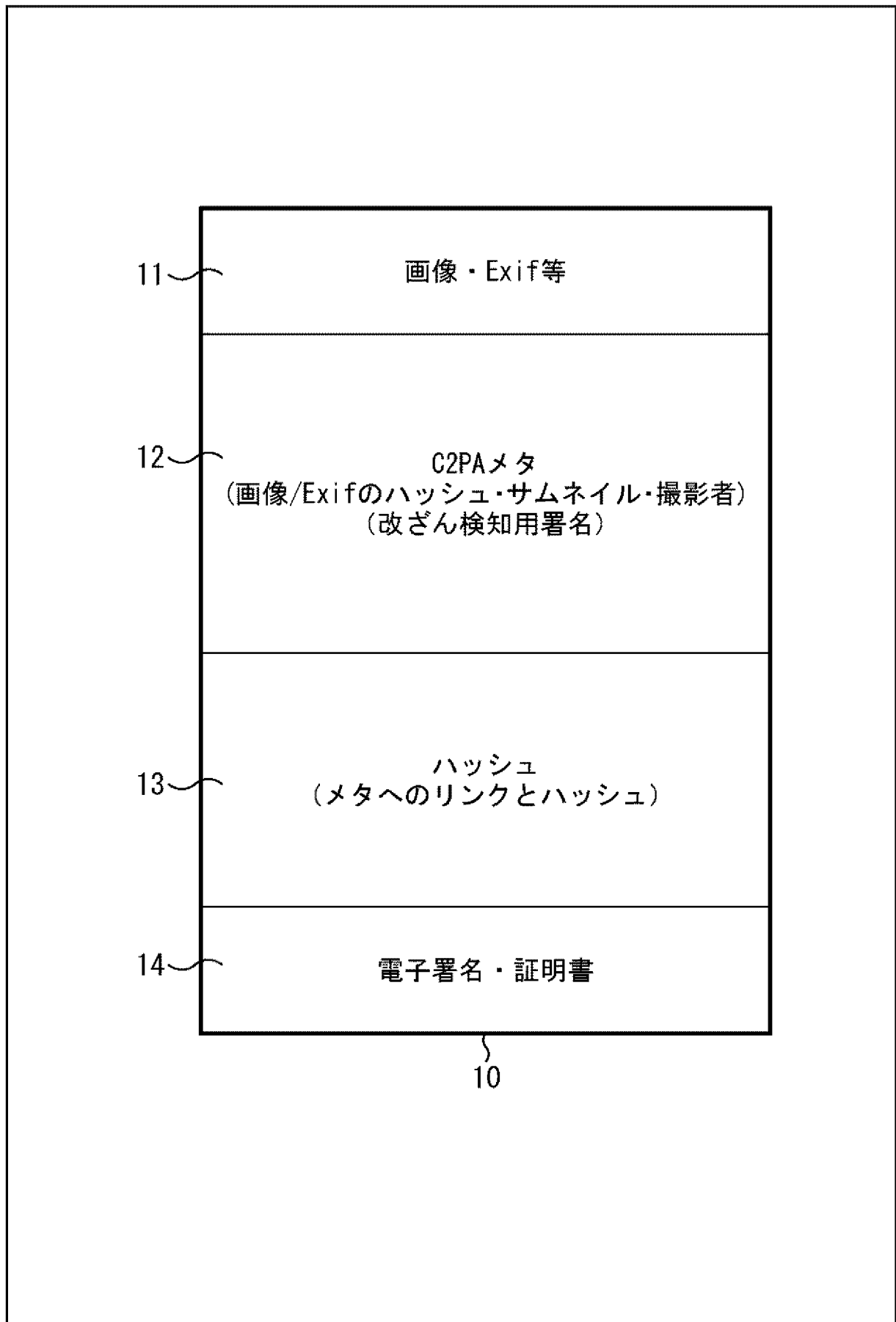
前記第2の署名は、前記ユーザ権限を有する第2の存在にも公開されるユーザ公開鍵に対応する第2の秘密鍵、前記画像、および前記メタデータを用いて生成された署名である

画像処理方法。

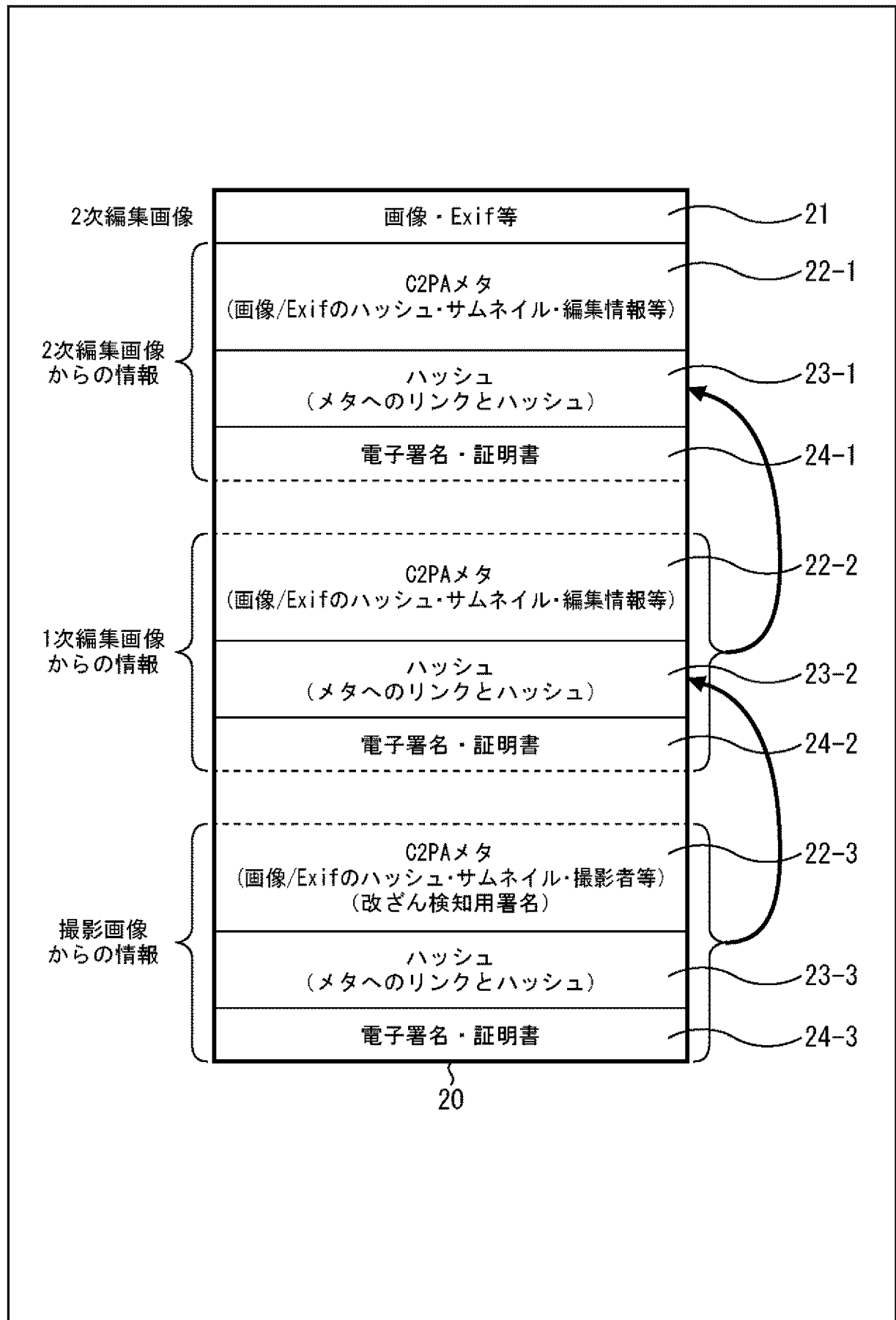
[図1]
FIG. 1

方法1	公開範囲が互いに異なる公開鍵に対応する複数の署名をファイルに格納する	
方法1-1	各署名の対象を互いに異なる範囲にする	
方法1-2	改ざん検知用署名のハッシュをマルチハッシュとする	
方法1-2-1	改ざん検知用署名のハッシュの分け方を来歴用署名用のハッシュの分け方よりも細かくする	
方法1-3	改ざん検知用署名を来歴で伝搬される領域に格納する	
方法1-3-1	改ざん検知用署名のハッシュをマルチハッシュとし、かつ、来歴で落とされ得る領域を他と独立にハッシュにする	

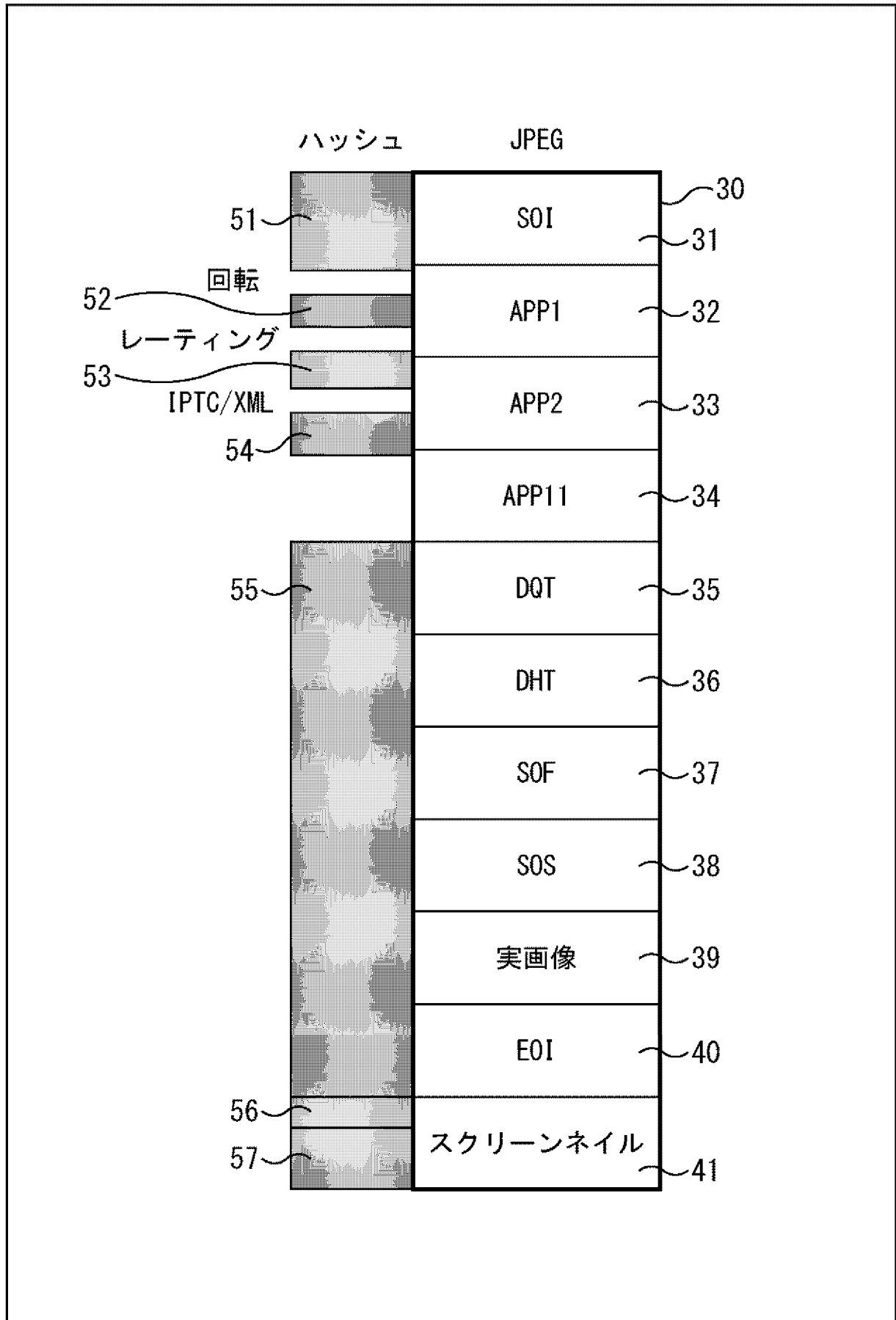
[図2]
FIG. 2



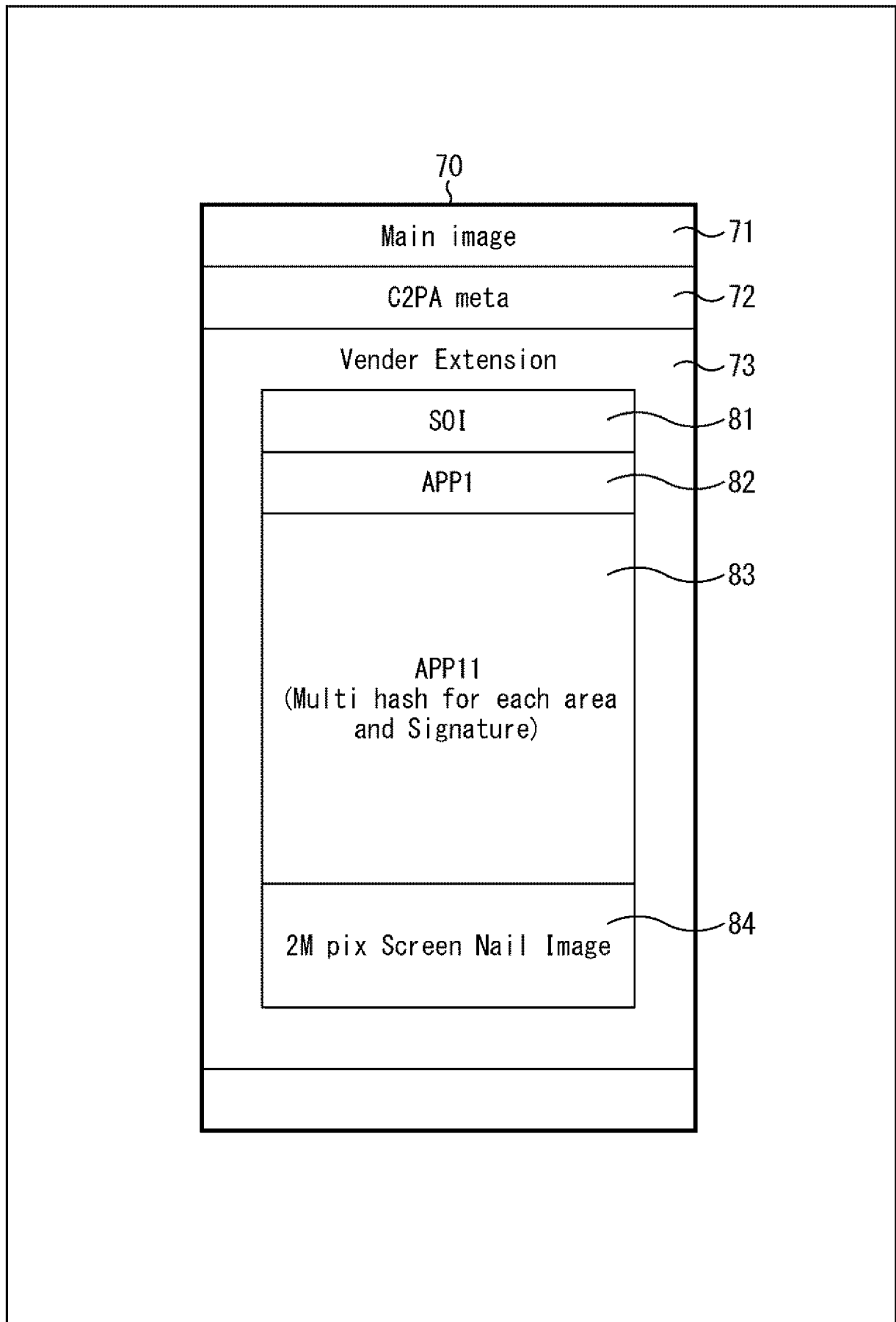
[図3]
FIG. 3

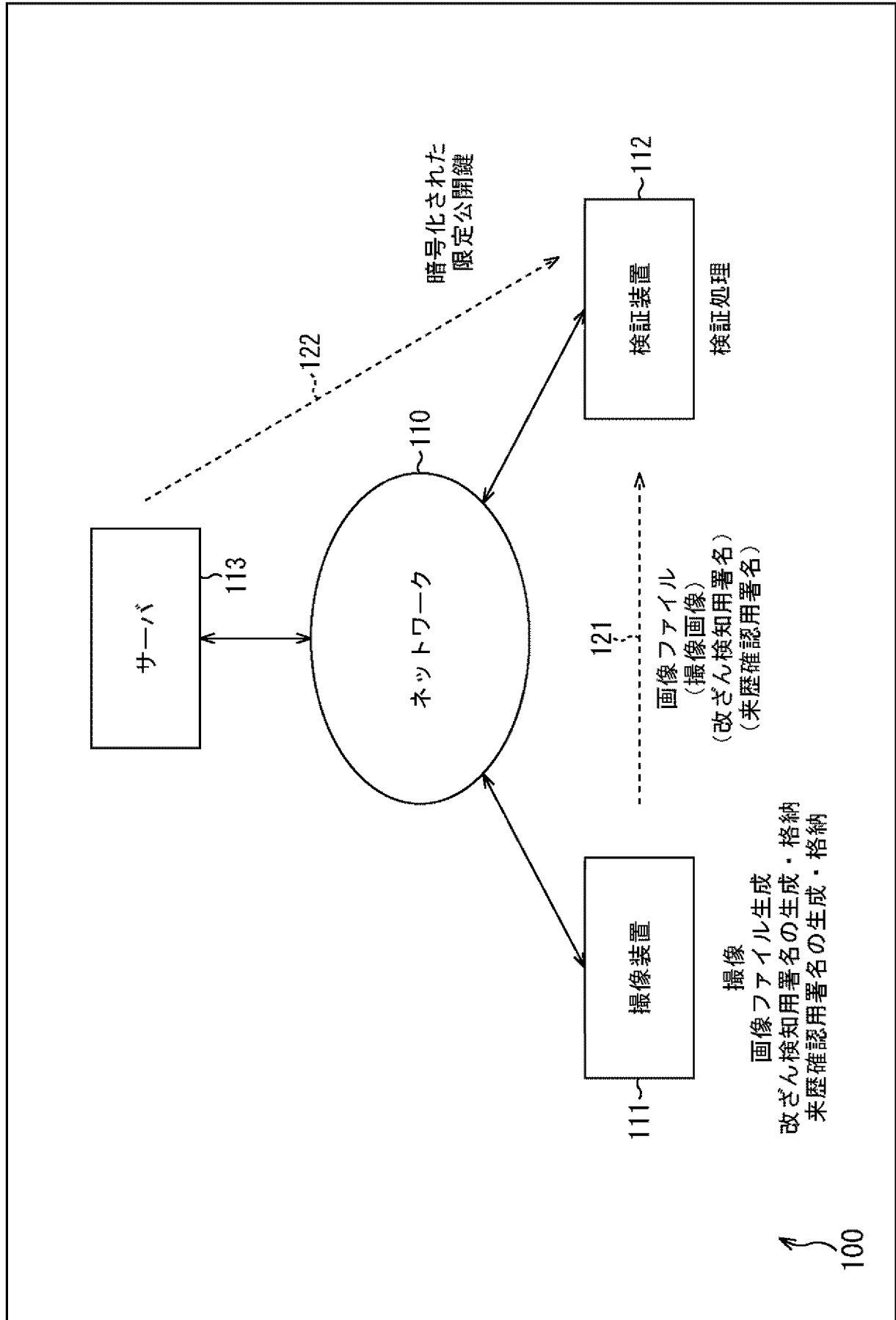


[図4]
FIG. 4

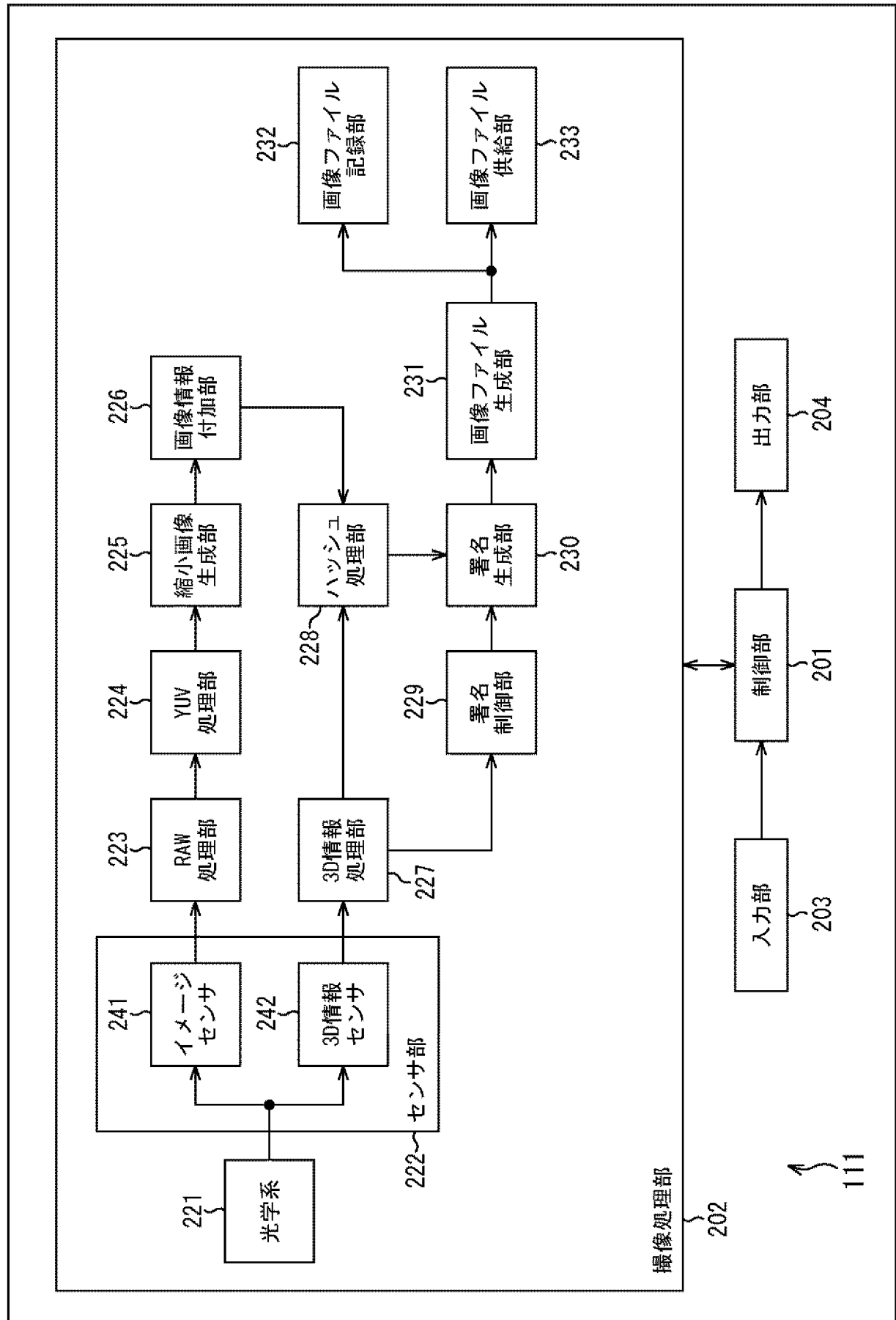


[図5]
FIG. 5

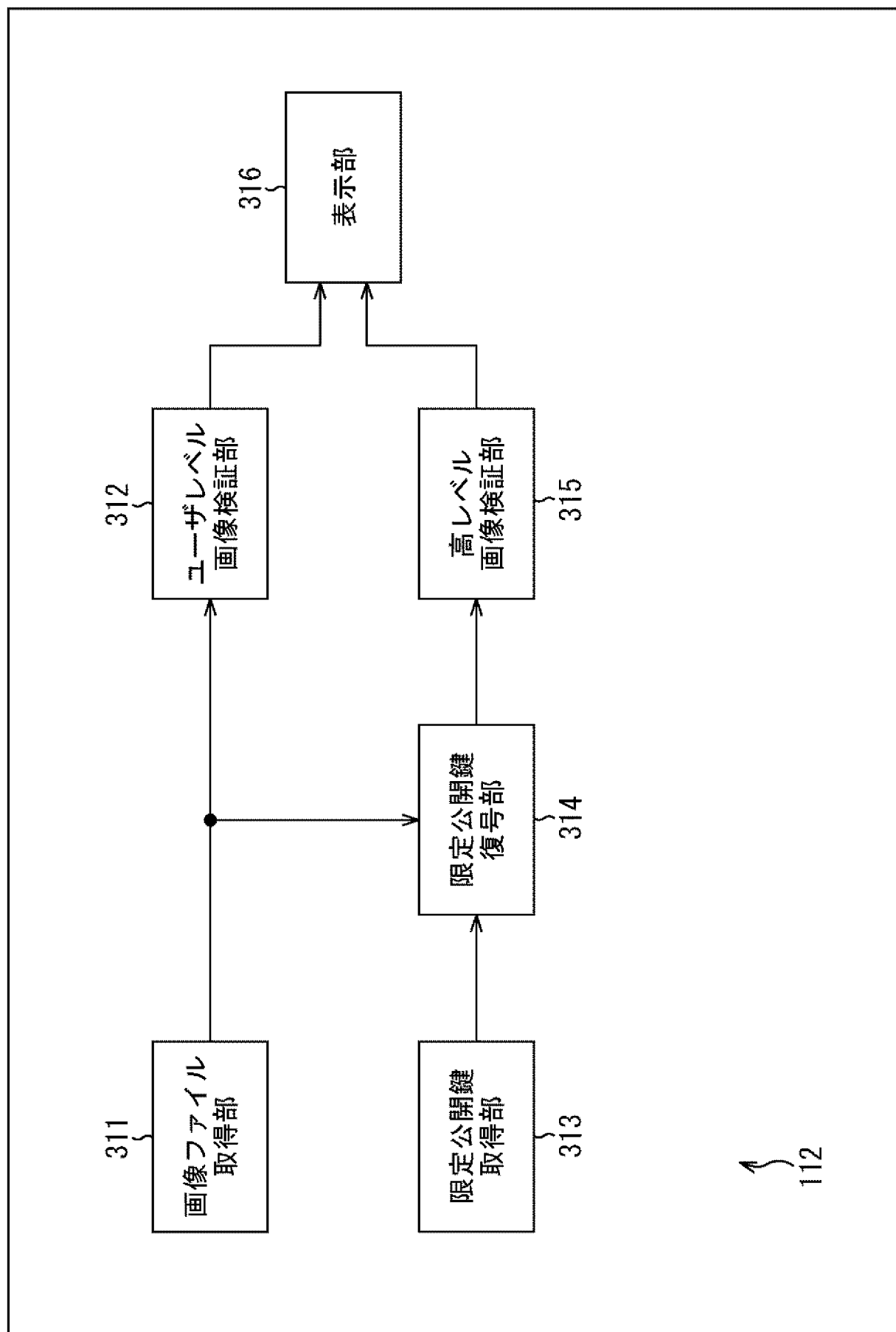


[図6]
FIG. 6

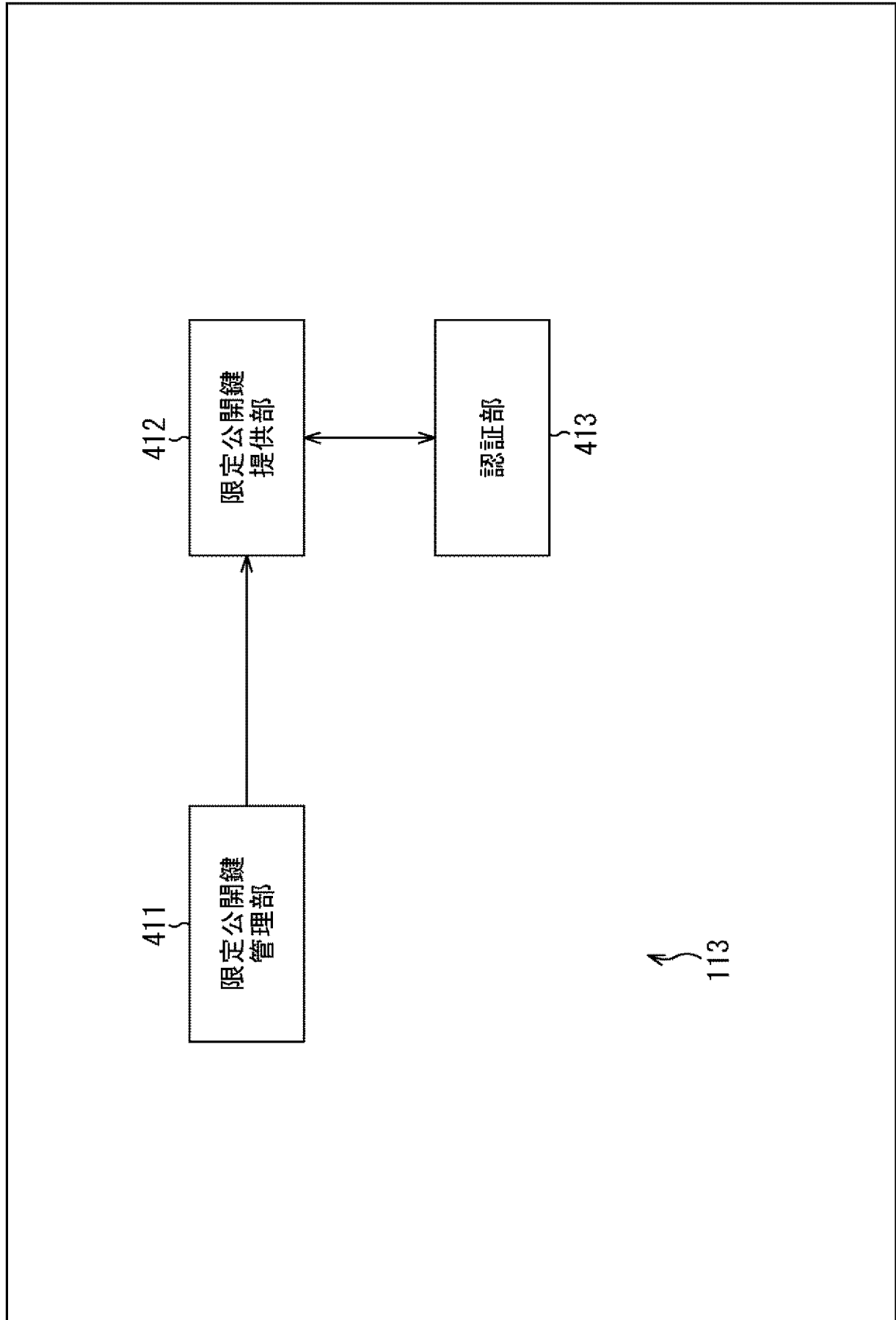
[図7]
FIG. 7



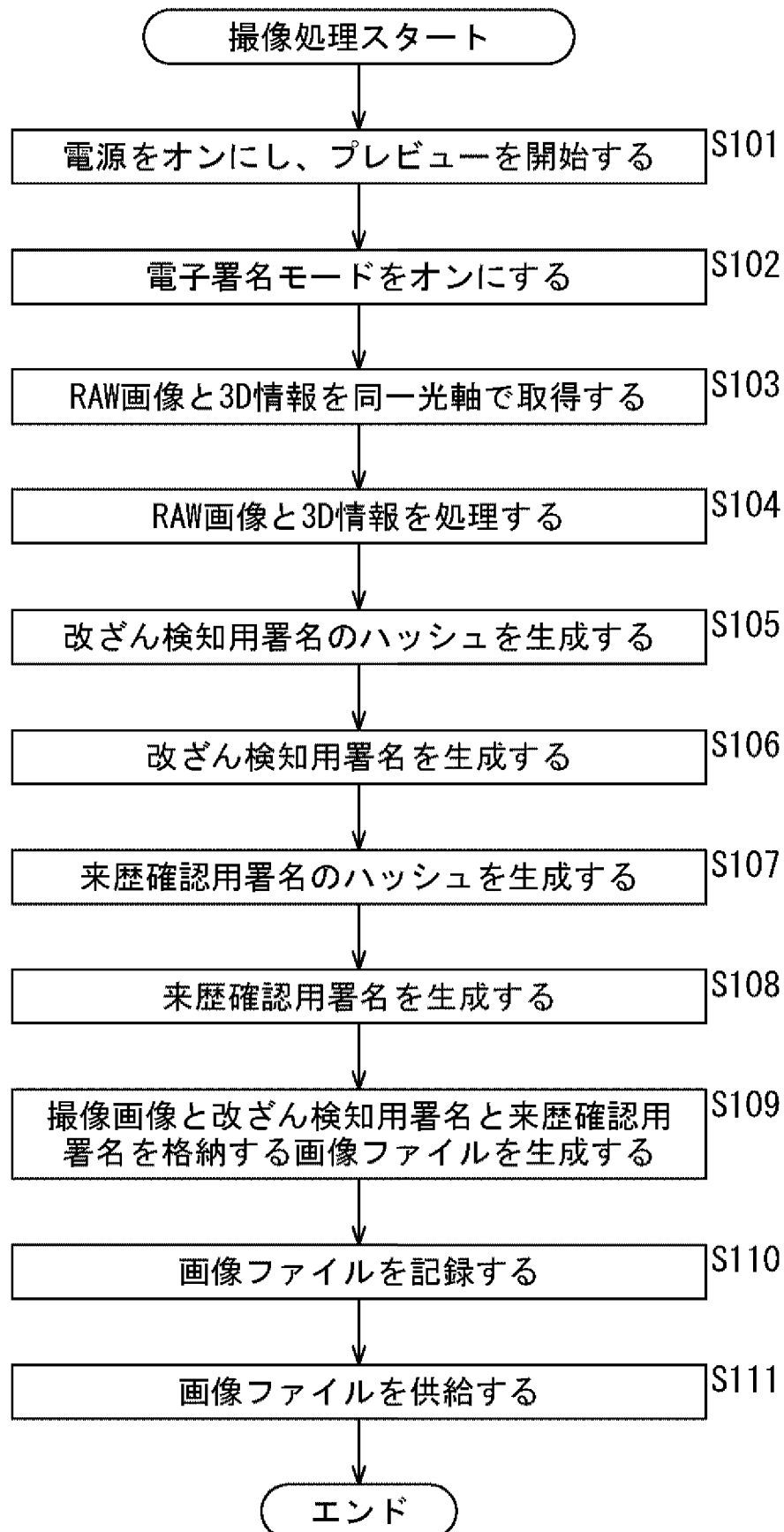
[図8]
FIG. 8



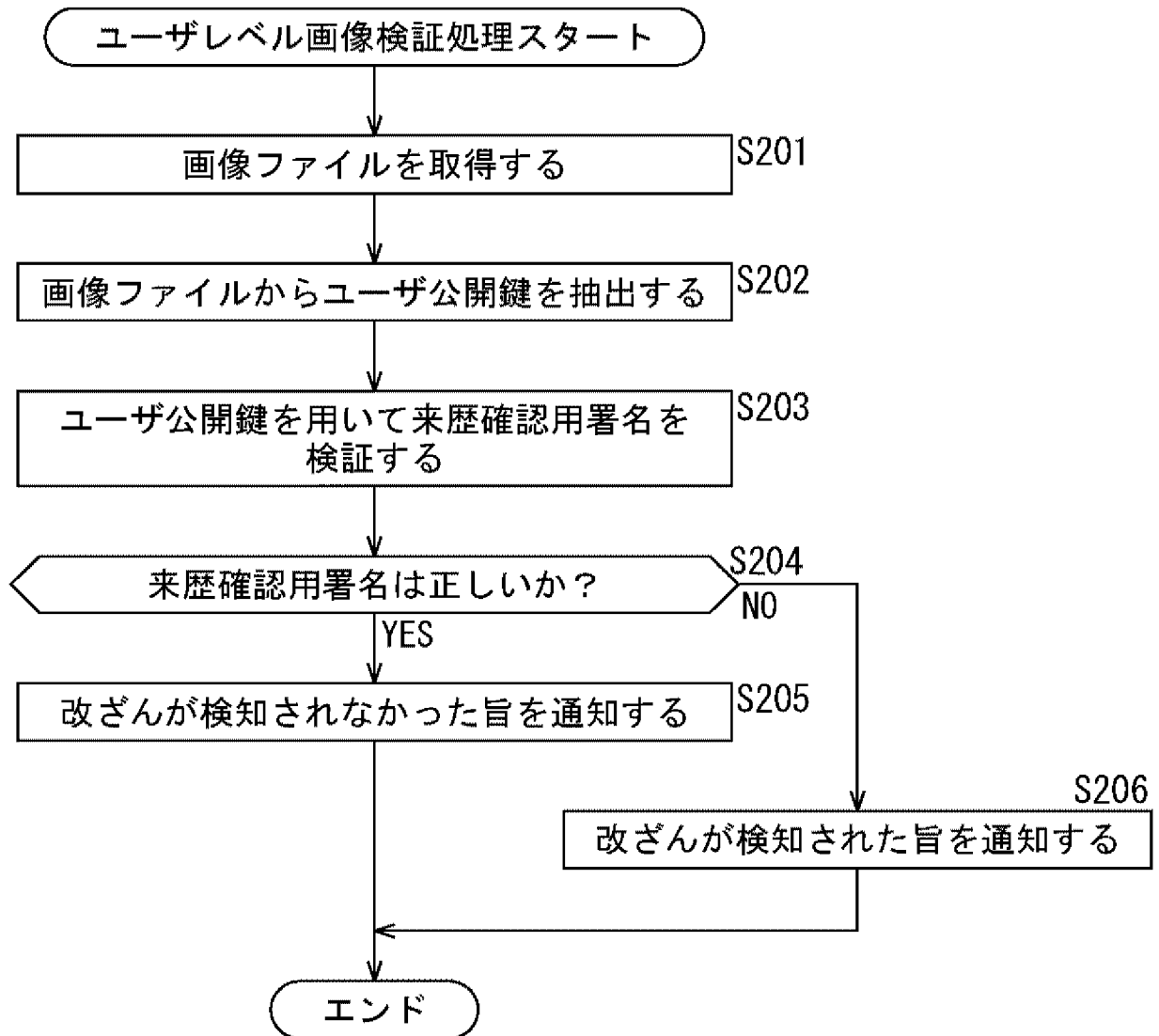
[図9]
FIG. 9



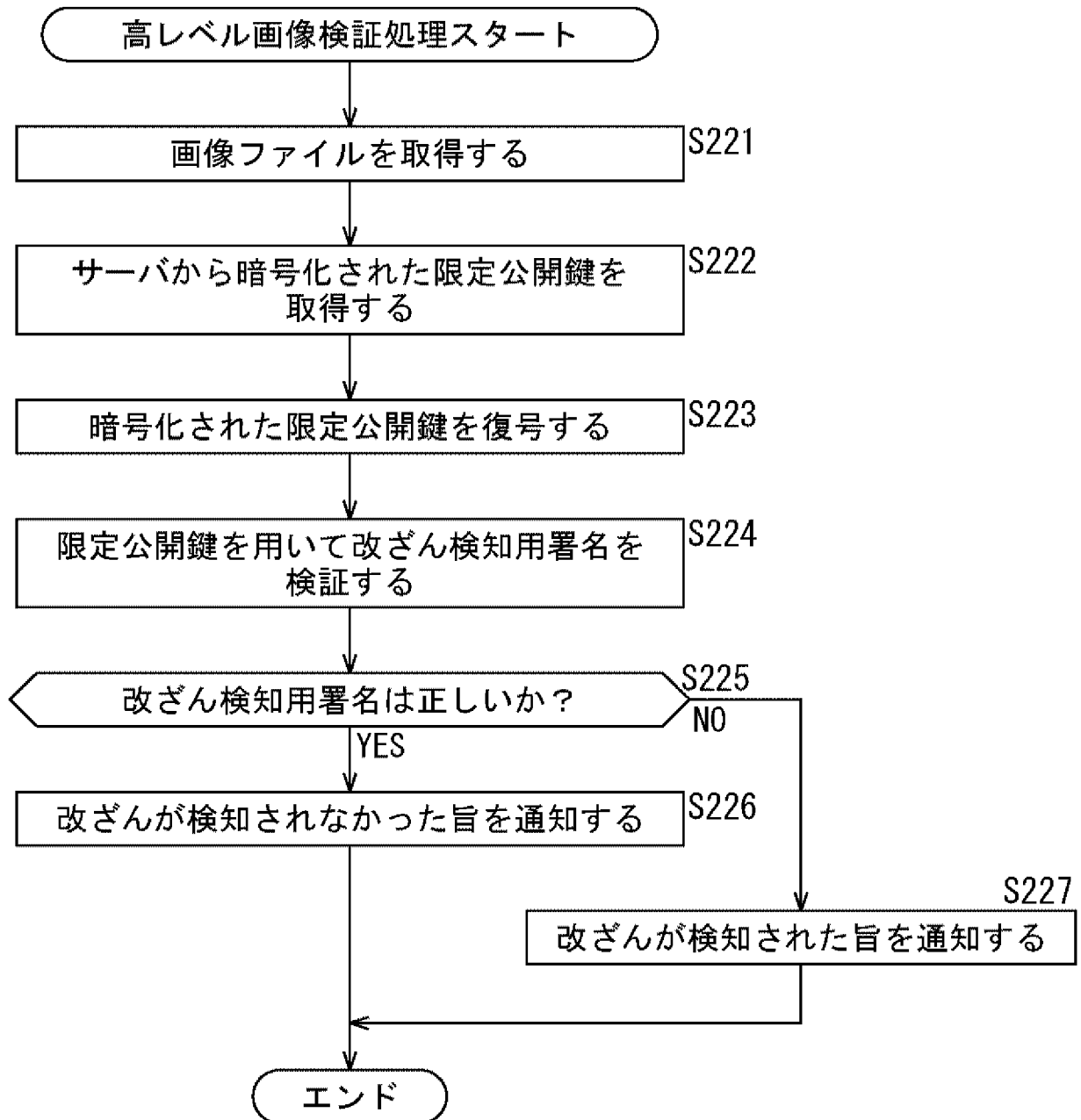
[図10]
FIG. 10



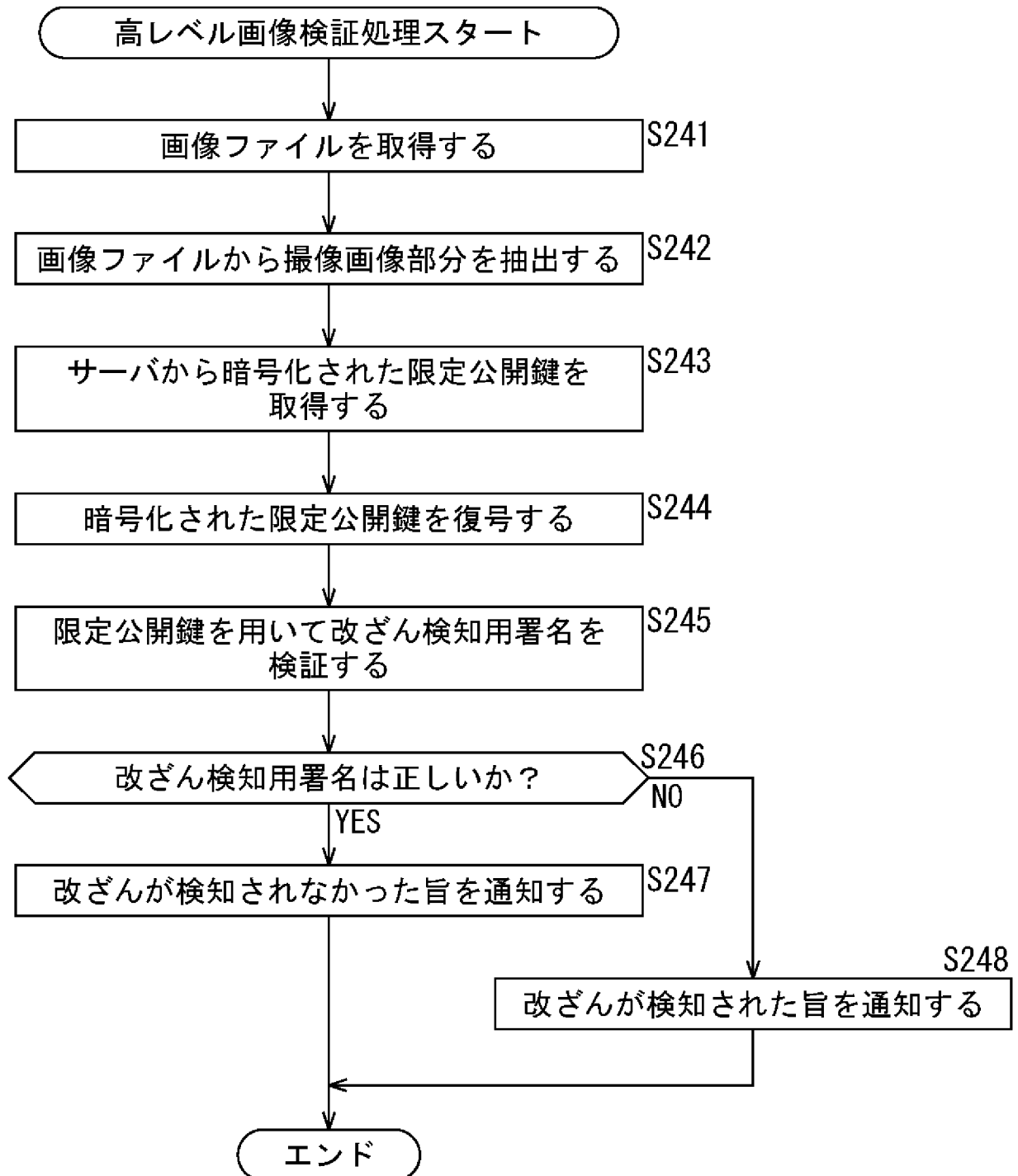
[図11]
FIG. 11



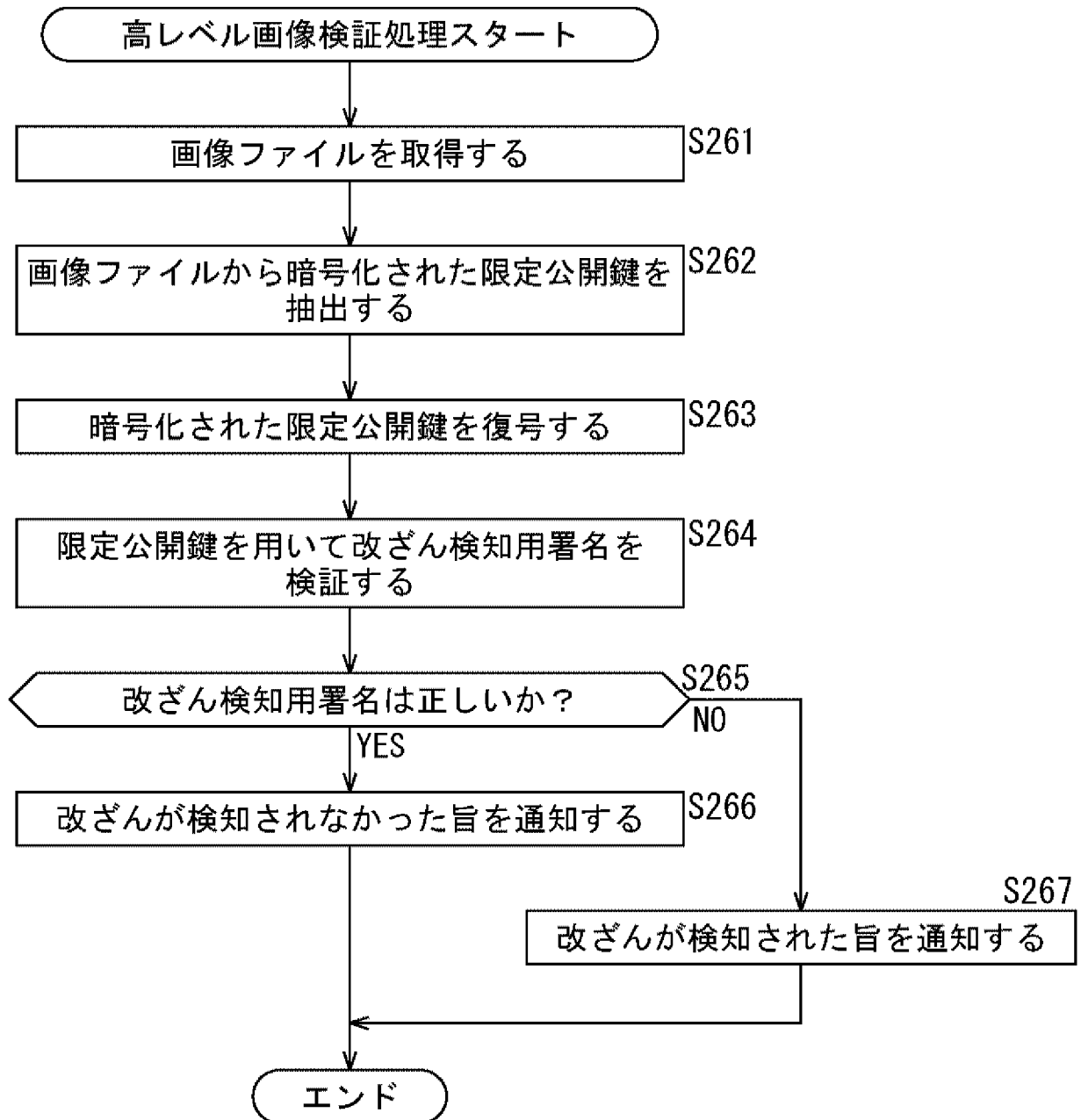
[図12]
FIG. 12



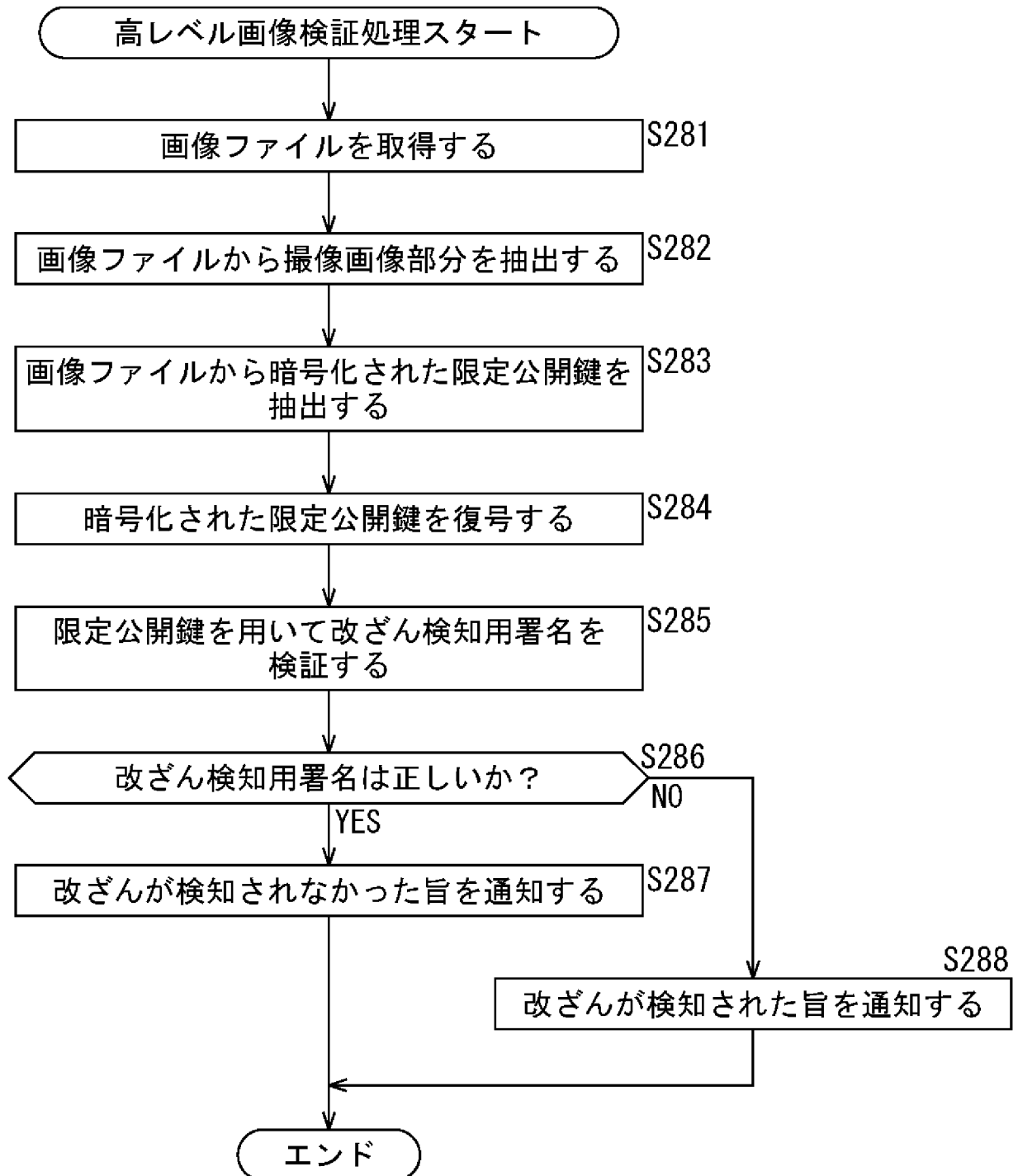
[図13]
FIG. 13



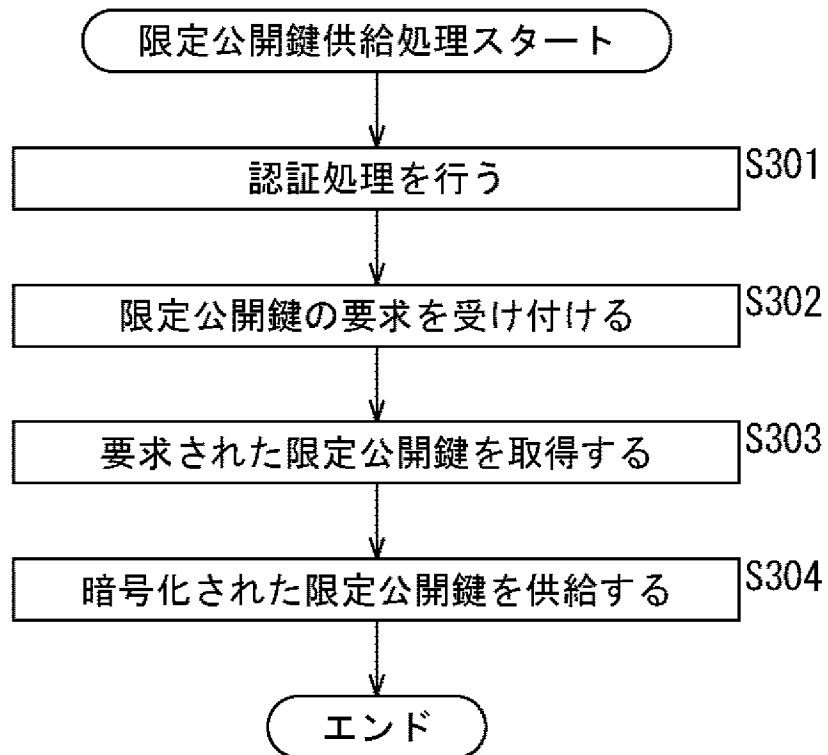
[図14]
FIG. 14



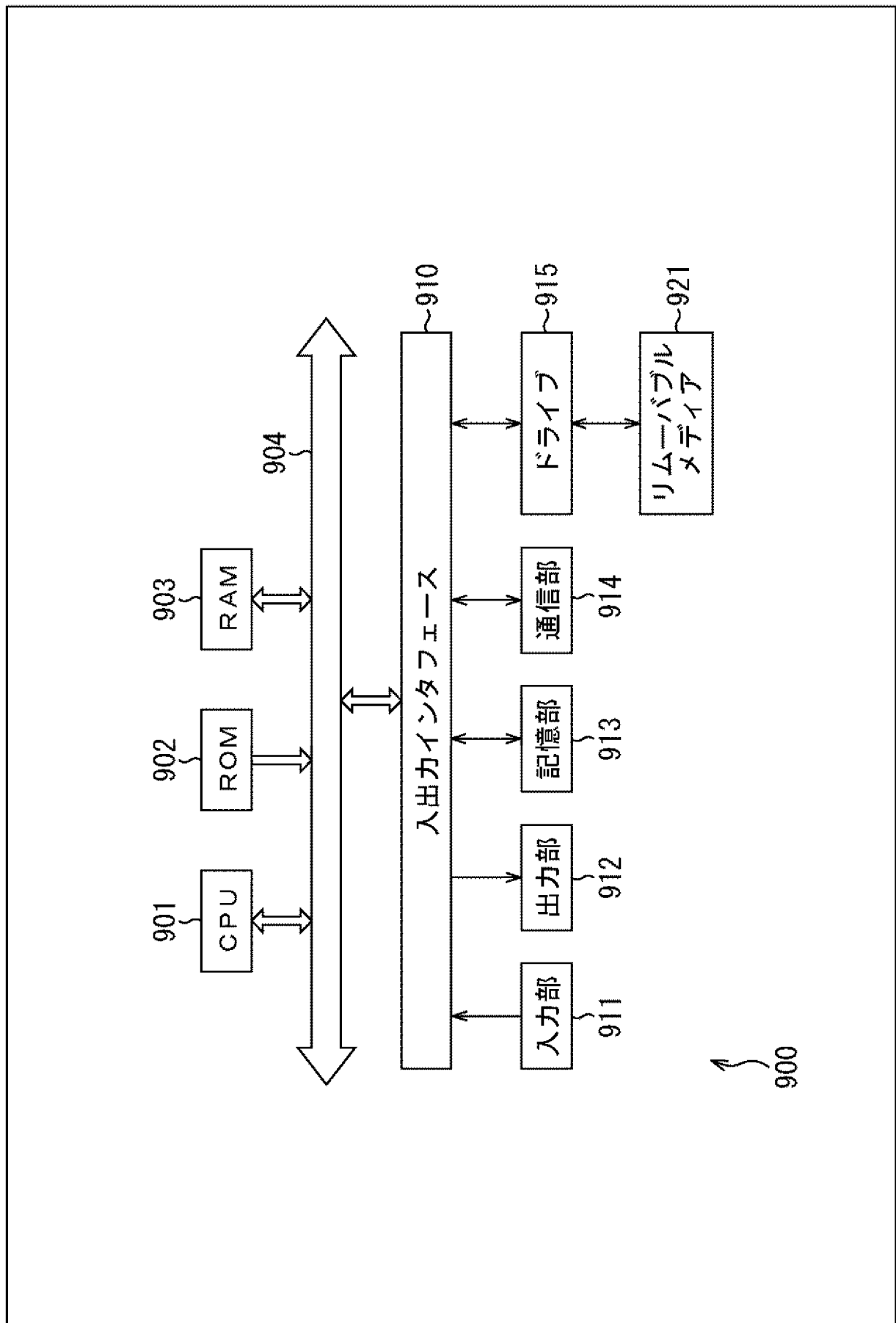
[図15]
FIG. 15



[図16]
FIG. 16



[図17]
FIG. 17



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2023/043767

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/64**(2013.01)i; **H04L 9/30**(2006.01)i

FI: G06F21/64; H04L9/30

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)

G06F21/64; H04L9/30

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 1971-2024
 Registered utility model specifications of Japan 1996-2024
 Published registered utility model applications of Japan 1994-2024

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2021/039055 A1 (SONY CORP.) 04 March 2021 (2021-03-04) paragraphs [0057]-[0059]	1-22
A	JP 2003-242139 A (MITSUBISHI ELECTRIC INFORMATION SYSTEMS CORP.) 29 August 2003 (2003-08-29) abstract	1-22
A	JP 2005-45486 A (CASIO COMPUTER CO., LTD.) 17 February 2005 (2005-02-17) paragraphs [0062]-[0064]	1-22



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
 “D” document cited by the applicant in the international application
 “E” earlier application or patent but published on or after the international filing date
 “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 “O” document referring to an oral disclosure, use, exhibition or other means
 “P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 “&” document member of the same patent family

Date of the actual completion of the international search

05 February 2024

Date of mailing of the international search report

20 February 2024

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)
 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/JP2023/043767

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO	2021/039055	A1	04 March 2021	US 2022/0279120 A1 paragraphs [0132]-[0139] EP 4013032 A1 CN 114270776 A	
JP	2003-242139	A	29 August 2003	(Family: none)	
JP	2005-45486	A	17 February 2005	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/64(2013.01)i; H04L 9/30(2006.01)i FI: G06F21/64; H04L9/30		
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）） G06F21/64; H04L9/30 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 - 2024年 日本国実用新案登録公報 1996 - 2024年 日本国登録実用新案公報 1994 - 2024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
A	WO 2021/039055 A1（ソニー株式会社）04.03.2021（2021 - 03 - 04） 段落[0057]-[0059]	1-22
A	JP 2003-242139 A（三菱電機インフォメーションシステムズ株式会社）29.08.2003 （2003 - 08 - 29） 要約	1-22
A	JP 2005-45486 A（カシオ計算機株式会社）17.02.2005（2005 - 02 - 17） 段落[0062]-[0064]	1-22
☐ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技术水準を示すもの “D” 国際出願で出願人が先行技術文献として記載した文献 “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 05.02.2024	国際調査報告の発送日 20.02.2024	
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） 宮司 卓佳 5S 9555 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/JP2023/043767

引用文献			公表日	パテントファミリー文献			公表日
WO	2021/039055	A1	04.03.2021	US	2022/0279120	A1	
				段落[0132]-[0139]			
				EP	4013032	A1	
				CN	114270776	A	

JP	2003-242139	A	29.08.2003	(ファミリーなし)			

JP	2005-45486	A	17.02.2005	(ファミリーなし)			
