(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7632294号
(P7632294)

(45)発行日　令和7年2月19日(2025.2.19)

(24)登録日　令和7年2月10日(2025.2.10)

(51)国際特許分類		FI		
H04L 9/32 (2006.01)		H04L	9/32	200B
G06F 21/32 (2013.01)		G06F	21/32	
G06F 21/64 (2013.01)		G06F	21/64	
G06T 7/00 (2017.01)		G06T	7/00	510A

請求項の数　16　（全46頁）

(21)出願番号　特願2021-552276(P2021-552276)
(86)(22)出願日　令和2年9月16日(2020.9.16)
(86)国際出願番号　PCT/JP2020/035057
(87)国際公開番号　WO2021/075198
(87)国際公開日　令和3年4月22日(2021.4.22)
審査請求日　令和5年7月24日(2023.7.24)
(31)優先権主張番号　特願2019-190350(P2019-190350)
(32)優先日　令和1年10月17日(2019.10.17)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　000002185
ソニーグループ株式会社
東京都港区港南１丁目７番１号
(74)代理人　110003410
弁理士法人テクノピア国際特許事務所
(74)代理人　100116942
弁理士　岩田 雅信
(74)代理人　100167704
弁理士　中川 裕人
(72)発明者　高塚 進
東京都港区港南１丁目７番１号 ソニー株式会社内
(72)発明者　鉄川 弘樹
東京都港区港南１丁目７番１号 ソニー株式会社内

最終頁に続く

(54)【発明の名称】　情報処理システム、情報処理方法、プログラム、ユーザインタフェース

(57)【特許請求の範囲】

【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画素アレイと、前記画素アレイにおける光電変換に基づいて得た撮像画像データからハッシュ値を生成するハッシュ値生成部と、前記ハッシュ値に対する暗号化処理を実行する暗号化処理部と、を有するアレイセンサと、

前記撮像画像データと暗号化された前記ハッシュ値を取得する取得部と、

前記取得した暗号化されたハッシュ値の復号化を行う復号化処理部と、

前記取得した撮像画像データからハッシュ値を算出するハッシュ値算出部と、

前記復号化されたハッシュ値と前記算出されたハッシュ値を比較するハッシュ値比較部と、

前記ハッシュ値の比較結果に基づいて前記取得した撮像画像データの改竄の有無を判定する改竄判定部と、

前記改竄判定部の判定結果を通知するための出力制御を行う出力制御部と、を備え、

前記出力制御部は、チャット画面を提示する制御を行い、

前記チャット画面においては、チャット参加者が使用する他の撮像装置であって前記アレイセンサを有する撮像装置から出力されたチャット参加者の撮像画像データが表示出力されずに撮像画像データに係る前記改竄判定部の判定結果がチャット参加者ごとに表示出力される

情報処理システム。

【請求項２】
前記取得した撮像画像データに基づいて被写体の生体情報を抽出するための解析を行う生体解析処理部と、
前記生体解析処理部の解析結果に基づいて前記被写体が生体であるか否かを判定する生体判定部と、を備えた
請求項１に記載の情報処理システム。
【請求項３】
前記取得した撮像画像データに含まれる被写体の個体特徴量を解析するための個体解析処理部と、
前記個体解析処理部の解析結果に基づいて前記被写体についての個体認識可否を判定する個体判定部と、を備えた
請求項１に記載の情報処理システム。
【請求項４】
前記出力制御部は、前記生体判定部の判定結果を通知するための出力制御を行う
請求項２に記載の情報処理システム。
【請求項５】
前記出力制御部は、前記個体判定部の判定結果を通知するための出力制御を行う
請求項３に記載の情報処理システム。
【請求項６】
撮像装置と情報処理装置とを含んで構成され、
前記撮像装置は、前記アレイセンサを有し、
前記情報処理装置は、前記取得部と、前記復号化処理部と、前記ハッシュ値算出部と、前記ハッシュ値比較部と、前記改竄判定部と、前記出力制御部と、を有する
請求項１に記載の情報処理システム。
【請求項７】
前記出力制御部は、前記取得した撮像画像データを表示出力する制御と、前記取得した撮像画像データについての前記改竄判定部の判定結果を表示出力する制御と、を実行する
請求項６に記載の情報処理システム。
【請求項８】
撮像装置と情報処理装置とを含んで構成され、
前記撮像装置は、前記アレイセンサと、前記出力制御部と、を有し、
前記情報処理装置は、認証処理を行う認証処理部と、前記取得部と、前記復号化処理部と、前記ハッシュ値算出部と、前記ハッシュ値比較部と、前記改竄判定部と、を有する
請求項１に記載の情報処理システム。
【請求項９】
前記出力制御部は、前記情報処理装置から取得した前記改竄判定部の判定結果を表示出力する制御を行い、
前記認証処理部は、前記改竄判定部の判定結果に基づいて前記認証処理を行う
請求項８に記載の情報処理システム。
【請求項１０】
前記情報処理装置は、
前記取得した撮像画像データに基づいて被写体の生体情報を抽出するための解析を行う生体解析処理部と、
前記生体解析処理部の解析結果に基づいて前記被写体が生体であるか否かを判定する生体判定部と、を備え、
前記出力制御部は、前記生体判定部の判定結果を表示出力する制御を行い、
前記認証処理部は、前記生体判定部の判定結果に基づいて前記認証処理を行う
請求項９に記載の情報処理システム。
【請求項１１】
前記取得した撮像画像データに含まれる被写体の個体特徴量を解析するための個体解析

処理部と、
前記個体解析処理部の解析結果に基づいて前記被写体についての個体認識可否を判定する個体判定部と、
前記改竄の有無についての判定結果と前記生体であるか否かについての判定結果と前記個体認識可否についての判定結果に基づいて、前記取得した撮像画像データが改竄されていないことが担保されていない非担保状態と、前記取得した撮像画像データが改竄されていないことが担保された状態である第１担保状態と、前記取得した撮像画像データが改竄されていないことが担保され且つ前記被写体が生体であるとされた状態である第２担保状態と、前記取得した撮像画像データが改竄されていないことが担保され前記被写体が生体であるとされ且つ前記個体認識が可とされた状態である第３担保状態と、を判定する状態判定部と、を備えた
請求項２に記載の情報処理システム。
【請求項１２】
前記出力制御部は、前記非担保状態、前記第１担保状態、前記第２担保状態及び前記第３担保状態に応じた表示出力を行う
請求項１１に記載の情報処理システム。
【請求項１３】
前記生体判定部は、前記解析の結果得られた前記被写体の生体信号の変化の有無を判定することにより生体であるか否かを判定する
請求項２に記載の情報処理システム。
【請求項１４】
前記撮像画像データにおける被写体は生体情報を抽出不可能な被写体とされた
請求項１に記載の情報処理システム。
【請求項１５】
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画素アレイと、光電変換して得た撮像画像データからハッシュ値を生成するハッシュ値生成部と、前記ハッシュ値に対する暗号化処理を実行する暗号化処理部と、を有するアレイセンサから、前記撮像画像データと暗号化された前記ハッシュ値を取得する処理と、
前記取得した暗号化されたハッシュ値の復号化を行う処理と、
前記取得した撮像画像データからハッシュ値を算出する処理と、
前記復号化されたハッシュ値と前記算出されたハッシュ値を比較する処理と、
前記ハッシュ値の比較結果に基づいて前記取得した撮像画像データの改竄の有無を判定する処理と、
前記改竄の有無の判定結果を通知する処理と、
チャット参加者が使用する他の撮像装置であって前記アレイセンサを有する撮像装置から出力されたチャット参加者の撮像画像データが表示されずに撮像画像データに係る前記改竄の有無の判定結果がチャット参加者ごとに表示されたチャット画面を提示する処理と、を
情報処理装置が実行する情報処理方法。
【請求項１６】
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画素アレイと、光電変換して得た撮像画像データからハッシュ値を生成するハッシュ値生成部と、前記ハッシュ値に対する暗号化処理を実行する暗号化処理部と、を有するアレイセンサから、前記撮像画像データと暗号化された前記ハッシュ値を取得する処理と、
前記取得した暗号化されたハッシュ値の復号化を行う処理と、
前記取得した撮像画像データからハッシュ値を算出する処理と、
前記復号化されたハッシュ値と前記算出されたハッシュ値を比較する処理と、
前記ハッシュ値の比較結果に基づいて前記取得した撮像画像データの改竄の有無を判定する処理と、
前記改竄の有無の判定結果を通知する処理と、

チャット参加者が使用する他の撮像装置であって前記アレイセンサを有する撮像装置から出力されたチャット参加者の撮像画像データが表示されずに撮像画像データに係る前記改竄の有無の判定結果がチャット参加者ごとに表示されたチャット画面を提示する処理と、を

情報処理装置に実行させるプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本技術は情報処理システム、情報処理方法、プログラム、ユーザインタフェースに関し、特にデータの改竄の有無を検出する技術に関する。

【背景技術】

【０００２】

画像処理の技術が発展してきており、その結果、撮像された人物の顔や身体の画像を改竄することにより別人になりすますことが可能になってきている。

また、人工的な人物画像と音声を作成して機械にインタラクティブなコミュニケーションを取らせることにより、通信の相手が機械であることを認識できないまま実在の人物と誤認してコミュニケーションを取ってしまうという問題が発生し得る。

このような問題に対して、例えば下記特許文献１では、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いて行うことが記載されている。

【先行技術文献】

【特許文献】

【０００３】

【文献】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】

【０００４】

ところで、撮像画像データの改竄を防止するためには、撮像画像データが伝送される伝送路をセキュリティの高いものとすることが考えられるが、全ての伝送路のセキュリティを高めることはコストの面で不利である。

具体的には、イメージセンサからの出力に基づいてハッシュ値を生成するが、ハッシュ値を生成する前の段階でイメージセンサからの出力が漏洩してしまうと撮像画像データが改竄されていないものであることを保証することができない。

【０００５】

そこで本技術では、コストを増大させることなく撮像画像データが改竄されていないことを保証することを目的とする。

【課題を解決するための手段】

【０００６】

本技術に係る情報処理システムは、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画素アレイと、前記画素アレイにおける光電変換に基づいて得た撮像画像データからハッシュ値を生成するハッシュ値生成部と、前記ハッシュ値に対する暗号化処理を実行する暗号化処理部と、を有するアレイセンサと、前記撮像画像データと暗号化された前記ハッシュ値を取得する取得部と、前記取得した暗号化されたハッシュ値の復号化を行う復号化処理部と、前記取得した撮像画像データからハッシュ値を算出するハッシュ値算出部と、前記復号化されたハッシュ値と前記算出されたハッシュ値を比較するハッシュ値比較部と、前記ハッシュ値の比較結果に基づいて前記取得した撮像画像データの改竄の有無を判定する改竄判定部と、を備えたものである。

即ち、アレイセンサ内でハッシュ値の生成と暗号化処理が実行される。

【０００７】

上記した情報処理システムにおいては、前記取得した撮像画像データに基づいて被写体の生体情報を抽出するための解析を行う生体解析処理部と、前記生体解析処理部の解析結

果に基づいて前記被写体が生体であるか否かを判定する生体判定部と、を備えていてもよい。
これにより、被写体が生きているか否かを判定することができる。
【０００８】
上記した情報処理システムにおいては、前記取得した撮像画像データに含まれる被写体の個体特徴量を解析するための個体解析処理部と、前記個体解析処理部の解析結果に基づいて前記被写体についての個体認識可否を判定する個体判定部と、を備えていてもよい。
これにより、被写体を個人特定するための情報を得ることができる。
【０００９】
上記した情報処理システムにおいては、前記改竄判定部の判定結果を通知するための出力制御を行う出力制御部を備えていてもよい。
これにより、ユーザは改竄判定結果を認識することができる。
また、上記した情報処理システムでは、前記撮像画像データにおける被写体は生体情報を抽出不可能な被写体とされてもよい。
【００１０】
上記した情報処理システムにおいては、前記生体判定部の判定結果を通知するための出力制御を行う出力制御部を備えていてもよい。
これにより、ユーザは生体判定結果を認識することができる。
【００１１】
上記した情報処理システムにおいては、前記個体判定部の判定結果を通知するための出力制御を行う出力制御部を備えていてもよい。
これにより、ユーザは個体判定の結果を認識することができる。
【００１２】
上記した情報処理システムにおいては、撮像装置と情報処理装置とを含んで構成され、前記撮像装置は、前記アレイセンサを有し、前記情報処理装置は、前記取得部と、前記復号化処理部と、前記ハッシュ値算出部と、前記ハッシュ値比較部と、前記改竄判定部と、前記出力制御部と、を有していてもよい。
例えば、撮像装置と情報処理装置から成る監視カメラシステムなどに適用可能である。
【００１３】
上記した情報処理システムにおいては、前記出力制御部は、前記取得した撮像画像データを表示出力する制御と、前記取得した撮像画像データについての前記改竄判定部の判定結果を表示出力する制御と、を実行してもよい。
このような情報処理システムとしては、例えば、受信した撮像画像を表示しつつその画像についての改竄の有無を表示するユーザインタフェース制御を行うものが考えられる。
【００１４】
上記した情報処理システムにおける前記出力制御部は、前記取得した撮像画像データについての表示出力を行わずに前記改竄判定部の判定結果を表示出力する制御を行ってもよい。
このような情報処理システムとしては、例えば、撮像画像が表示されないようなテキストチャットシステムなどが考えられる。
【００１５】
上記した情報処理システムにおける前記出力制御部は、チャット画面を提示する制御と、チャット参加者が使用する前記撮像装置から受信した参加者の撮像画像データについての前記改竄判定部の判定結果を前記チャット画面においてチャット参加者ごとに表示出力する制御と、を行ってもよい。
撮像画像が表示されないようなテキストチャットシステムなどにおいて、参加者ごとに信用できるか否かの指標が表示される。
【００１６】
上記した情報処理システムにおいては、撮像装置と情報処理装置とを含んで構成され、前記撮像装置は、前記アレイセンサと、前記出力制御部と、を有し、前記情報処理装置は

、認証処理を行う認証処理部と、前記取得部と、前記復号化処理部と、前記ハッシュ値算出部と、前記ハッシュ値比較部と、前記改竄判定部と、を有していてもよい。
　このような情報処理システムとしては、例えば、撮像画像データを送信した側の情報処理装置（撮像装置）において認証結果等を通知するものが考えられる。
【００１７】
　上記した情報処理システムにおける前記出力制御部は、前記情報処理装置から取得した前記改竄判定部の判定結果を表示出力する制御を行い、前記認証処理部は、前記改竄判定部の判定結果に基づいて前記認証処理を行ってもよい。
　即ち、撮像画像データを送信した装置（撮像装置）において、送信した撮像画像データが改竄されずに受信側装置であるサーバ装置（情報処理装置）まで届いたか否かをユーザが認識することができる。
【００１８】
　上記した情報処理システムにおける前記情報処理装置は、前記取得した撮像画像データに基づいて被写体の生体情報を抽出するための解析を行う生体解析処理部と、前記生体解析処理部の解析結果に基づいて前記被写体が生体であるか否かを判定する生体判定部と、を備え、前記出力制御部は、前記生体判定部の判定結果を表示出力する制御を行い、前記認証処理部は、前記生体判定部の判定結果に基づいて前記認証処理を行ってもよい。
　即ち、改竄判定処理だけでなく、受信した撮像画像データから生体情報の抽出を行い、その抽出結果に基づいて被写体が生体であるか否かの判定処理を行う。
【００１９】
　上記した情報処理システムにおいては、前記取得した撮像画像データに含まれる被写体の個体特徴量を解析するための個体解析処理部と、前記個体解析処理部の解析結果に基づいて前記被写体についての個体認識可否を判定する個体判定部と、前記改竄の有無についての判定結果と前記生体であるか否かについての判定結果と前記個体認識可否についての判定結果に基づいて、前記取得した撮像画像データが改竄されていないことが担保されていない非担保状態と、前記取得した撮像画像データが改竄されていないことが担保された状態である第１担保状態と、前記取得した撮像画像データが改竄されていないことが担保され且つ前記被写体が生体であるとされた状態である第２担保状態と、前記取得した撮像画像データが改竄されていないことが担保され前記被写体が生体であるとされ且つ前記個体認識が可とされた状態である第３担保状態と、を判定する状態判定部と、を備えていてもよい。
　これにより、セキュリティの保証度合いに応じた処理を行うことが可能とされる。
【００２０】
　上記した情報処理システムにおいては、前記非担保状態、前記第１担保状態、前記第２担保状態及び前記第３担保状態に応じた表示出力を行う出力制御部を備えていてもよい。
　これにより、ユーザは保証度合いを確認することが可能となる。
【００２１】
　上記した情報処理システムにおける前記生体判定部は、前記解析の結果得られた前記被写体の生体信号の変化の有無を判定することにより生体であるか否かを判定してもよい。
　例えば、複数枚の撮像画像データの解析を行うことにより、生体信号の変化を抽出する。
【００２２】
　本技術の情報処理方法は、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画素アレイと、光電変換して得た撮像画像データからハッシュ値を生成するハッシュ値生成部と、前記ハッシュ値に対する暗号化処理を実行する暗号化処理部と、を有するアレイセンサから、前記撮像画像データと暗号化された前記ハッシュ値を取得する処理と、前記取得した暗号化されたハッシュ値の復号化を行う処理と、前記取得した撮像画像データからハッシュ値を算出する処理と、前記復号化されたハッシュ値と前記算出されたハッシュ値を比較する処理と、前記ハッシュ値の比較結果に基づいて前記取得した撮像画像データの改竄の有無を判定する処理と、を情報処理装置が実行するものである。

【００２３】
本技術のプログラムは、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画素アレイと、光電変換して得た撮像画像データからハッシュ値を生成するハッシュ値生成部と、前記ハッシュ値に対する暗号化処理を実行する暗号化処理部と、を有するアレイセンサから、前記撮像画像データと暗号化された前記ハッシュ値を取得する処理と、前記取得した暗号化されたハッシュ値の復号化を行う処理と、前記取得した撮像画像データからハッシュ値を算出する処理と、前記復号化されたハッシュ値と前記算出されたハッシュ値を比較する処理と、前記ハッシュ値の比較結果に基づいて前記取得した撮像画像データの改竄の有無を判定する処理と、を情報処理装置に実行させるものである。
これにより、アレイセンサ内でハッシュ値の生成と暗号化処理が実行される。
【００２４】
本技術のユーザインタフェースは、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画素アレイと光電変換して得た撮像画像データからハッシュ値を生成するハッシュ値生成部と前記ハッシュ値に対する暗号化処理を実行する暗号化処理部とを有するアレイセンサから取得した暗号化された前記ハッシュ値を復号化して得られるハッシュ値と、前記アレイセンサから取得した撮像画像データから算出したハッシュ値と、の比較結果に基づいて行われる前記撮像画像データの改竄の有無についての判定処理の結果を通知するものである。
【図面の簡単な説明】
【００２５】
【図１】第１の実施の形態としての情報処理システムの構成例を示した概略説明図である。
【図２】第１の実施の形態としてのユーザ端末の内部構成例を示したブロック図である。
【図３】第１の実施の形態としてのビデオチャットシステムを利用する際の流れを説明するための概略説明図である。
【図４】第１の実施の形態としてのビデオチャットシステムにおける着信画面の例を示す図である。
【図５】第１の実施の形態としてのビデオチャットシステムにおける通話画面の例を示す図である。
【図６】実施の形態の第２保証アイコンの例を示す図である。
【図７】実施の形態の第３保証アイコンの例を示す図である。
【図８】実施の形態の非保証アイコンの例を示す図である。
【図９】第１の実施の形態としてのビデオチャットシステムにおいて送信者側のユーザ端末が実行する処理を示すフローチャートである。
【図１０】第１の実施の形態としてのビデオチャットシステムにおいて受信者側のユーザ端末が実行する処理を示すフローチャートである。
【図１１】第２の実施の形態としてのユーザ端末の内部構成例を示したブロック図である。
【図１２】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１３】第２の実施の形態における振幅制御による読み出し信号の暗号化を説明するためのイメージ図である。
【図１４】第２の実施の形態としてのビデオチャットシステムにおいて送信者側のユーザ端末が実行する処理を示すフローチャートである。
【図１５】第２の実施の形態における撮像画像データの暗号化処理についてのフローチャートである。
【図１６】第２の実施の形態としてのビデオチャットシステムにおいて受信者側のユーザ端末が実行する処理を示すフローチャートである。
【図１７】第３の実施の形態としてのビデオチャットシステムにおいて受信側のユーザ端末が実行する処理を示すフローチャートである。
【図１８】第３の実施の形態としてのビデオチャットシステムにおいて受信側のユーザ端

末が実行する処理を示すフローチャートである。
【図１９】第３の実施の形態の応用例を示す図でありテキストチャット画面の一例を示す図である。
【図２０】第４の実施の形態における情報処理システムの構成例を示した概略説明図である。
【図２１】第４の実施の形態におけ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２２】第４の実施の形態におけるサーバ装置の内部構成例を示したブロック図である。
【図２３】第４の実施の形態としての情報処理システムにおけるログイン画面の例を示す図である。
【図２４】第４の実施の形態としての情報処理システムにおいてユーザ端末が実行する処理を示すフローチャートである。
【図２５】第４の実施の形態としての情報処理システムにおいてサーバ装置が実行する処理を示すフローチャートである。
【図２６】第４の実施の形態としての情報処理システムにおけるサインアップ画面の一例である。
【図２７】変形例としての情報処理システムにおいてユーザ端末が実行する処理を示すフローチャートである。
【図２８】オークションサイトにおいて改竄されていない画像が表示されていることを示す図である。
【図２９】宿泊検索サイトにおいて改竄されていない画像が表示されていることを示す図である。
【発明を実施するための形態】
【００２６】
以下、実施の形態を次の順序で説明する。

【００２７】
＜１．第１の実施の形態＞
＜１－１．システム構成＞

図１は、第１の実施の形態における情報処理システム１の概略構成例を示したブロック図である。
なお、第１の実施の形態においては、ビデオチャットシステムとしての情報処理システム１を例示する。
【００２８】
情報処理システム１は、ユーザがビデオチャットシステムを利用するために使用するユーザ端末２と、ネットワーク３と、サーバ装置４とを備えている。
ユーザ端末２は、本技術に係る撮像装置であり且つ情報処理装置でもある。具体的には、ユーザ端末２は、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）を得る撮像装置の一形態とされる。また、ユーザ端末２は、ネットワーク３を介して他のユーザ端末２から取得した撮像画像データが改竄されていないことを証明するための処理を実行する情報処理装置の一形態とされる。
【００２９】
以降の説明においては、イメージセンサによる撮像を行い撮像画像データを送信する側のユーザ端末２をユーザ端末２Ａと記載する。また、ユーザ端末２Ａから撮像画像データを受信する側のユーザ端末２をユーザ端末２Ｂと記載する。
なお、ビデオチャットシステムとしての情報処理システム１においては、撮像した撮像画像データの送受信は双方向で行われる。従って、一台のユーザ端末２はユーザ端末２Ａとして捉えることもユーザ端末２Ｂとして捉えることも可能である。
【００３０】
本実施の形態では、電子署名の対象データは、このユーザ端末２Ａによる撮像画像データとされる。
【００３１】
ユーザ端末２Ａは、ユーザ端末２Ｂに対して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、ユーザ端末２Ａ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、公開鍵とをユーザ端末２Ｂに送信する。
ユーザ端末２Ｂは、ユーザ端末２Ａ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の有無を判定する処理（改竄判定処理）を行う。
なお、改竄判定処理については後に改めて説明する。
【００３２】
ネットワーク３は、例えばインターネット、ホームネットワーク、ＬＡＮ（Local Area Network）、衛星通信網、その他の各種のネットワークが想定される。
サーバ装置４は、ビデオチャットシステムを管理する情報処理装置であり、利用者であるユーザの個人情報を管理する機能やユーザ同士の通話記録や履歴を記憶する機能などを備えている。
【００３３】
＜１－２．ユーザ端末の構成＞
図２は、ユーザ端末２の内部構成例を示したブロック図である。
ユーザ端末２は、ユーザ端末２Ａとしての機能を実行するために、アレイセンサ１０、画像プロセッサ１１、制御部１２、メモリ部１３、入力部１４、通信部１５及び出力部１６を備えている。
【００３４】
アレイセンサ１０は、画素アレイ２１と、ハッシュ値生成部２２と、暗号化処理部２３とを備えている。
画素アレイ２１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おり、ユーザ端末２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。
【００３５】

ハッシュ値生成部２２は、画素アレイ２１から出力された撮像画像データからハッシュ値を生成（算出）する。生成したハッシュ値は後段の暗号化処理部２３に出力される。

【００３６】

暗号化処理部２３は、入力されたハッシュ値の暗号化処理を行う。暗号化処理には秘密鍵が用いられる。即ち、暗号化処理部２３は、署名生成鍵としての秘密鍵の生成と、署名検証鍵としての公開鍵の生成を行う。

【００３７】

アレイセンサ１０は、暗号化されたハッシュ値と生成した公開鍵を制御部１２に出力する。また、画素アレイ２１において生成された撮像画像データを画像プロセッサ１１に出力する。

【００３８】

図示は省略するが、アレイセンサ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、プロセッサとしての構成部位を有している。そして、これらの構成部位が平置き構成とされたり、或いは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。

本例のアレイセンサ１０は、ハッシュ値の生成を行う機能や暗号化を行う機能を備えるものとされ、所謂インテリジェントアレイセンサと呼ぶことのできるデバイスとされる。

【００３９】

画像プロセッサ１１は、光電変換信号に対してデジタル化する処理を施す。更に、画像プロセッサ１１は、デジタル化された信号をバッファに一時記憶する処理や、バッファに記憶された信号を読み出し必要な各種の信号処理（画像処理）などを行う。

【００４０】

各種の信号処理としては、例えば、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など、画質調整のための処理が想定される。また画像プロセッサ１１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。

これら画像プロセッサ１１で行われる各処理においては、各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。画像プロセッサ１１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。

【００４１】

制御部１２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、ユーザ端末２の全体制御を行う。

例えば、制御部１２は、アレイセンサ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。また、制御部１２は、画像プロセッサ１１についても各種処理の実行制御を行う。

【００４２】

また、制御部１２は、メモリ部１３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１３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、例えばアレイセンサ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。

【００４３】

更にまた、制御部１２は、入力部１４からの入力信号を取得し、入力信号に応じた制御を行う。入力部１４は、例えば、ビデオチャットを利用するユーザが使用するキーボードやマウス、或いはタッチパネルなどを含んでいる。更に、スマートフォンやカメラなどが備える速度センサや加速度センサ、或いは角速度センサなども入力部１４の一例とされる。

制御部１２は、それらの操作情報やセンサ情報を取得し、各種の処理を実行する。

【００４４】
さらに、制御部１２は、通信部１５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１５は、図１に示したネットワーク３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１２は、図１に示した他のユーザ端末２Ｂからの求めに応じ、例えばアレイセンサ１０で得られメモリ部１３に保存された撮像画像データ等の各種データを通信部１５を介してユーザ端末２Ｂに送信することが可能とされる。
【００４５】
また、制御部１２は、出力部１６に対して出力信号を出力する。出力部１６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。
【００４６】
制御部１２は、電子署名に係る各種の機能を備えている。具体的に、制御部１２は、取得部３１、復号化処理部３２、ハッシュ値算出部３３、ハッシュ値比較部３４、改竄判定部３５、生体解析処理部３６、生体判定部３７、個体解析処理部３８、個体判定部３９、出力制御部４０、状態判定部４１を備えている。
これらの各部は、ユーザ端末２Ｂとしての機能である。即ち、ユーザ端末２Ａから受信した撮像画像データの改竄の有無を判定するための機能を実現するための各部である。
なお、本実施の形態及び以下に示す他の実施の形態において、ユーザ端末２が全ての機能を備えている必要はなく、上述した各部の一部のみを備えた構成であってもよい。
【００４７】
取得部３１は、ユーザ端末２Ａで生成された撮像画像データと暗号化されたハッシュ値を取得する処理を実行する。また、取得部３１は、暗号化されたハッシュ値を復号化するための公開鍵の取得を行う。
【００４８】
復号化処理部３２は、暗号化されたハッシュ値を復号化する処理を行う。復号化には公開鍵が用いられる。
【００４９】
ハッシュ値算出部３３は、受信した撮像画像データからハッシュ値を算出する処理を行う。
【００５０】
ハッシュ値比較部３４は、復号化処理部３２が復号化したハッシュ値とハッシュ値算出部３３が算出したハッシュ値を比較する処理を実行する。
【００５１】
改竄判定部３５は、ハッシュ値の比較結果に基づいて撮像画像データが改竄されているものであるか否かを判定する改竄判定処理を実行する。改竄判定の判定結果としては、改竄されていないことが保証できる判定結果（非改竄判定）と、改竄されていないことが保証できない判定結果（改竄判定）とが設けられている。即ち、改竄されていないからといって必ず非改竄判定となるわけではない。改竄されていないことが保証されていない場合は、実際に改竄が行われていなくても改竄判定となる。
【００５２】
生体解析処理部３６は、受信した撮像画像データを解析し生体情報を抽出する処理を行う。例えば、受信した複数枚の撮像画像データを比較解析することにより、生体情報の抽出を行う。
【００５３】
生体判定部３７は、生体解析処理部３６の解析結果に基づいて被写体が生体であるか否かを判定する処理を行う。例えば、撮像画像データが実際に生きている人間を撮像したことによって得られたものであるか否か、即ち、生きた人間が被写体であるか否かを判定する。また、被写体として何人の人間が映っているかを判定してもよい。
【００５４】

個体解析処理部３８は、受信した撮像画像データを解析し被写体の個体特徴量を抽出する処理を行う。個体特徴量とは、個人を特定可能な情報であり、例えば、肌の色、目の位置、眉間の長さと顔の横幅の比率、鼻の位置や形、唇の位置や形や形状や色、その他ほくろの位置や数などである。また、髪型や色などは普遍的なものではないが個体の特徴量として抽出してもよい。更に、被写体の全身が写っている場合には、肩幅や手足の長さなど各部の比率や長さや大きさなどを抽出してもよい。

なお、犬や猫など人間以外の生物の個体を特定するための特徴量を個体特徴量として抽出してもよい。

【００５５】

個体判定部３９は、個体解析処理部３８の解析結果に基づいて個体を判定する処理を行う。この処理は、例えば、他の情報処理装置に解析結果を送信することにより個体を特定してもよいし、ユーザ端末２Ｂにおいて個体を特定してもよい。他の情報処理装置に個体の特定を依頼する例としては、例えば、サーバ装置４にユーザごとの個体特徴量が記憶されており、サーバ装置４に抽出した個体特徴量を送信することにより個体の特定を依頼する。この場合には、サーバ装置４において、記憶されている個体特徴量と受信した抽出した個体特徴量を比較する処理が実行され個体が特定されることとなる。

【００５６】

出力制御部４０は、改竄判定部３５の判定結果や生体判定部３７の判定結果や個体判定部３９の判定結果に応じてユーザに対する通知を行うための出力制御を行う。例えば、表示部に対する表示制御を行うユーザインタフェース制御を行う。また、音声等の出力制御を行ってもよい。

【００５７】

状態判定部４１は、ユーザ端末２Ａから受信した撮像画像データに対する各種判定処理の結果に応じて該撮像画像データの状態（保証状態）を判定する処理を行う。撮像画像データの状態としては、例えば、撮像画像データが改竄されていないことが担保されていない状態である非担保状態ＳＴ０、撮像画像データが改竄されていないことのみが担保された状態である第１担保状態ＳＴ１、撮像画像データが改竄されていないことが担保されると共に被写体が生体であると判定された状態である第２担保状態ＳＴ２、撮像画像データが改竄されていないことが担保され被写体が生体であると判定された状態であり且つ被写体の個体認識がされた状態である第３担保状態ＳＴ３などが設けられている。

【００５８】

なお、図２に示す例では、アレイセンサ１０と制御部１２が別体として設けられている例を説明したが、アレイセンサ１０の一部として制御部１２が設けられていてもよい。これは、後述する他の実施の形態においても同様である。

【００５９】

＜１－３．全体の流れ＞

ユーザ端末２Ａを利用するユーザＡがユーザ端末２Ｂを利用する他のユーザＢに対してビデオチャットによる通話要求を行う際の全体の流れについて、一例を図３，図４及び図５に示す。

【００６０】

先ず、ユーザＡがビデオチャットシステムを利用するためのプログラム（以降、「ビデオチャットプログラム」と記載）を起動させると、ユーザ端末２Ａはアプリケーションのプログラムに従ってユーザ端末２Ａのカメラ機能を起動し撮像動作を行う（図３Ａ参照）。このとき、ユーザ端末２Ａは光電変換により得た撮像画像データからハッシュ値を生成して暗号化処理を施す。

【００６１】

続いて、ユーザＡがビデオチャットプログラムを操作することにより通話相手を選択して発信を開始させると、ユーザ端末２Ｂの表示部にはユーザＡから着信していることを示す着信画面５０が表示される。図４に示す着信画面５０の例は、ユーザ端末２Ｂがスマートフォンなどの携帯端末とされた例である。

【００６２】
図４に示すように、着信画面５０には、発信者についてのアイコン画像及び発信者であるユーザＡの登録名が表示される発信者表示欄６１と、ユーザ端末２Ａから受信した撮像画像データが改竄されていないことを示す保証アイコン６２と、撮像画像データが改竄されていないことが文章で説明された説明文６３と、通話開始ボタン６４と、通話拒否ボタン６５とが配置されている。
【００６３】
発信者表示欄６１には、発信者であるユーザＡが登録したアイコン画像が表示されてもよいし、今回の通話要求の際にユーザ端末２Ａで撮像された撮像画像データに基づく画像が表示されてもよい。
【００６４】
保証アイコン６２としては、例えば、上述した撮像画像データの状態（ＳＴ０～ＳＴ３）に応じたアイコン画像が表示されるようにしてもよい。図４に示す例では、ユーザ端末２Ａから今回受信した撮像画像データが改竄されていないことが担保された第１担保状態ＳＴ１に応じた第１保証アイコンＭＫ１が表示された状態である。
【００６５】
第１保証アイコンＭＫ１が保証アイコン６２に表示される状態は、ユーザ端末２Ｂが改竄判定処理を実行しそれ以外の判定処理（生体判定処理及び個体判定処理）を実行していないために撮像画像データが改竄されていないことのみが保証されている状態であってもよいし、改竄判定処理に加えて生体判定処理や個体判定処理を実行したが被写体が生体であると判定できなかった状態や被写体の個体認識ができなかったために撮像画像データが改竄されていないことのみが保証されている状態であってもよい。
【００６６】
通話を開始する前に発信者から受信した撮像画像データが改竄されていないこと、即ち、実際にユーザ端末２Ａで撮像された画像が送信されてきており、不正に取得した画像データを悪用して発信者になりすまして通話要求を行っているものではないことを保証アイコン６２を視認することによりユーザＢは確認することができる。
これにより、ユーザＢは詐欺のような不正な通話要求を見分けることができ、被害を未然に防止することができる。
【００６７】
ユーザＢが通話開始ボタン６４を操作すると、ユーザ端末２Ｂの表示部に通話画面５１が表示される。通話画面５１の一例を図５に示す。
【００６８】
通話画面５１には、相手画像表示欄６６と、自画像表示欄６７と、各種の機能アイコン６８が表示されている。
相手画像表示欄６６には、通話相手が使用するユーザ端末２Ａで撮像している動画像データが表示される。
自画像表示欄６７には、通話相手のユーザ端末２Ａに表示される自分（即ちユーザＢ）の動画像データが縮小されて表示される。
【００６９】
相手画像表示欄６６上には保証アイコン６２が重畳表示される。図５に示す例では、保証アイコン６２として、撮像画像データが改竄されていないことのみが保証されている状態を示す第１保証アイコンＭＫ１が重畳表示されている。
【００７０】
機能アイコン６８は、各種の機能を実行するための操作子として画面上に設けられている。各種の機能としては、例えば、通話を終了させる機能、自分の音声をＯＦＦにする機能、通話を一時停止する機能、音量変更機能、自分の動画像の送信を停止する機能、テキストによるチャットを行う機能などである。これらの機能はあくまで一例であり、その他の機能を実行するための機能アイコン６８が通話画面５１上に表示されていてもよい。また、上述した機能アイコン６８の一部が表示されていなくてもよい。更に、それらのアイ

コンの表示及び非表示の状態をユーザが設定可能とされていてもよい。
【００７１】
通話画面５１においても保証アイコン６２が表示され続けていることで、通話相手（ユーザＡ）から送信されてくる動画像データが実際にユーザ端末２Ａで撮像された画像であることをユーザＢは確認することができ、通話途中で不正な人物による通話の乗っ取りなどが発生した場合に認識することができる。
【００７２】
なお、そのためには、例えば数秒などの一定時間ごとに、ユーザ端末２Ａにおいて撮像画像データのハッシュ値生成処理と暗号化処理と送信処理が実行されると共に、それに応じてユーザ端末２Ｂにおいて受信したハッシュ値の復号化処理と比較処理と改竄判定処理が実行されることが望ましい。
【００７３】
図４及び図５においては保証アイコン６２として第１保証アイコンＭＫ１が表示される例を挙げたが、受信した撮像画像データの保証状態によっては他のアイコン画像が表意されてもよい。
【００７４】
例えば、撮像画像データが改竄されていないことが担保されると共に被写体が生体であると判定された状態である第２担保状態ＳＴ２である場合は、図６に示す第２保証アイコンＭＫ２が各画面における保証アイコン６２として表示されてもよい。また、図５の着信画面５０における説明文６３の代わりに図６に示す説明文６３が表示される。
【００７５】
また、撮像画像データが改竄されていないことが担保され被写体が生体であると判定された状態であり且つ被写体の個体認識がされた状態である第３担保状態ＳＴ３である場合は、図７に示す第３保証アイコンＭＫ３が各画面における保証アイコン６２として表示されてもよい。また、図５の着信画面５０における説明文６３の代わりに図７に示す説明文６３が表示される。
【００７６】
更に、撮像画像データが改竄されていないことが担保されていない状態である非担保状態ＳＴ０である場合には、図８に示す非保証アイコンＭＫ０が各画面における保証アイコン６２として表示されてもよい。また、図５の着信画面５０における説明文６３の代わりに図８に示す説明文６３が表示される。
【００７７】
なお、各アイコン画像はあくまで一例である。各アイコン画像は、受信した撮像画像データの保証状態が識別できるように構成されていればよい。
【００７８】
＜１－４．送信側の処理＞
上述したビデオチャットシステムを実現するために、送信側であるユーザ端末２Ａが実行する処理の一例を示したものが図９である。なお、図９に示す一連の処理は、例えば、ユーザＡがユーザ端末２Ａを操作してビデオチャットプログラムを立ち上げた際に実行される処理である。
【００７９】
ユーザ端末２Ａの制御部１２は、先ずステップＳ１０１において、カメラ機能を起動し、アレイセンサによる撮像動作を行う。
【００８０】
次に、ユーザ端末２Ａの制御部１２は、ステップＳ１０２において、撮像動作により得られた撮像画像データからハッシュ値を生成する処理を実行する。
【００８１】
続いて、ユーザ端末２Ａの制御部１２は、ステップＳ１０３において、生成したハッシュ値に対して秘密鍵を用いた暗号化処理を施す。
【００８２】

ユーザＡが通話相手を選択し通話開始要求を送信するための操作を行うと、ユーザ端末２Ａの制御部１２は、ステップＳ１０４において、通話開始要求の送信処理を行う。通話開始要求は、例えばサーバ装置４を介してユーザＢが利用するユーザ端末２Ｂへと送信される。

なお、ステップＳ１０４の通話開始要求の送信処理では、ステップＳ１０１で取得した撮像画像データと、ステップＳ１０３で暗号化されたハッシュ値と生成された公開鍵がユーザ端末２Ｂに送信される。

【００８３】

＜１－５．受信側の処理＞

上述したビデオチャットシステムを実現するために、受信側であるユーザ端末２Ｂが実行する処理の一例を示したものが図１０である。

【００８４】

ユーザ端末２Ｂが撮像画像データと暗号化されたハッシュ値と公開鍵を受信しビデオチャットプログラムが起動されると、ユーザ端末２Ｂの制御部１２は、ステップＳ２０１において、受信した各データの取得処理を行う。

【００８５】

続いて、ユーザ端末２Ｂの制御部１２は、ステップＳ２０２において、暗号化されたハッシュ値の復号化処理を実行する。

更に、ユーザ端末２Ｂの制御部１２は、ステップＳ２０３において、受信した撮像画像からハッシュ値の算出処理を実行する。

【００８６】

ユーザ端末２Ｂの制御部１２は、ステップＳ２０４において、算出したハッシュ値と復号化したハッシュ値の比較処理を行う。

【００８７】

ユーザ端末２Ｂの制御部１２は、ステップＳ２０５において、改竄判定処理を行う。この処理は、ハッシュ値の比較結果に応じて改竄の有無を判定する処理である。なお、実際に改竄がされているか否かによらず、改竄されている可能性がある場合には改竄されていない保証がないとして判定する。

具体的には、二つのハッシュ値が一致した場合には判定結果を非改竄判定とする。一方、二つのハッシュ値が一致しなかった場合には判定結果を改竄判定とする。

【００８８】

ユーザ端末２Ｂの制御部１２は、ステップＳ２０６において、改竄判定処理の判定結果に応じた分岐処理を実行する。

改竄されていないことが保証できる場合（非改竄判定）、ユーザ端末２Ｂの制御部１２は、ステップＳ２０７において、第１担保状態ＳＴ１に基づく出力制御を行う。

第１担保状態ＳＴ１に基づく出力制御とは、例えば、図４の着信画面５０において第１保証アイコンＭＫ１と説明文６３を表示させる処理である。

【００８９】

出力制御の他の態様としては、例えば、第１担保状態ＳＴ１に応じた音声出力を行う処理とされてもよい。

【００９０】

一方、改竄されていないことが保証できない場合（改竄判定）、即ち、非担保状態ＳＴ０とされている場合、ユーザ端末２Ｂの制御部１２は、ステップＳ２０８において、非担保状態ＳＴ０に基づく出力制御を行う。

非担保状態ＳＴ０に基づく出力制御とは、例えば、図４の着信画面５０において非保証アイコンＭＫ０と説明文６３（図８参照）を表示させる処理である。また、この処理において音声出力などが実行されてもよい。

【００９１】

前述したように、一定時間ごとに改竄されていないことの保証を行う場合には、図９及び図１０の各処理をユーザ端末２Ａ及びユーザ端末２Ｂが一定時間ごとに実行する。これ

により、通話中に不正な人物による乗っ取りなどが発生した場合にユーザＢは認識することができる。

【００９２】

＜２．第２の実施の形態＞

第２の実施の形態では、通話の秘匿性を高めるためにユーザ端末２Ａからユーザ端末２Ｂに送信する撮像画像データが暗号化される。

以降の説明においては、第１の実施の形態と同様の部分については同じ符号を付し適宜説明を省略する。

【００９３】

＜２－１．システム構成＞

第２の実施の形態における情報処理システム１のユーザ端末２（２Ａ，２Ｂ）は、アレイセンサ１０が画像暗号化処理部２４を備えている。

従って、ここでは、主に画像暗号化処理部２４の構成について説明する。

【００９４】

画像暗号化処理部２４は、画素アレイ２１から出力された撮像画像データを暗号化する処理を施す。暗号化処理は各種の例が考えられるが、ここでは、光電乱数を用いた暗号化処理を施す例について説明する。

【００９５】

画像暗号化処理部２４が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際に用いる光電乱数は、アレイセンサ１０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１０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。

【００９６】

図１２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１０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１０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。

以下の説明においては、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。

【００９７】

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。

【００９８】

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。

【００９９】
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。
【０１００】
なお、上述したハッシュ値の暗号化について光電乱数を用いてもよい。具体的には、暗号化に用いられる秘密鍵の生成を光電乱数に基づいて行ってもよい。これにより、秘密鍵の解読を困難化することが可能となり、セキュリティの向上を図ることができる。
【０１０１】
＜２－２．暗号化対象の信号について＞
従来、アレイセンサ１０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１０から読み出された画像信号を一旦平文の状態でメモリに保存し、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。
【０１０２】
そこで本実施の形態では、アレイセンサ１０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１１に示した画像暗号化処理部２４により、アレイセンサ１０の画素からの読み出し信号に対し図１２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。
【０１０３】
図１３は、画像暗号化処理部２４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１０の画素アレイ２１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、画像暗号化処理部２４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１１に示したユーザ端末２の画像暗号化処理部２４では、このように画素ごとの読み出し信号に対してアナログ信号の段階で振幅制御を施した後、フレーム単位の画像データをバッファに一時記憶する。バッファに一時記憶された画像データは、適切なタイミングで読み出され画像プロセッサ１１等に供される。
【０１０４】
即ち、画像暗号化処理部２４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１０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。
【０１０５】
なお、図１３はあくまでもイメージ図であり、画像暗号化処理部２４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、画像暗号化処理部２４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。
【０１０６】
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。
【０１０７】
なお、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、アナログの

読み出し信号に対する暗号化を施す構成を採用することにより、セキュリティの向上が図られる。

【０１０８】

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に映った被写体が生体であるか否か等の解析に用いられる場合には、画像の再現性としては生体解析処理に耐えうる程度であればよく、実用上の問題は生じないと考えられる。対象とする画像に映った被写体の個体解析処理行う場合についても同様である。

【０１０９】

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。

【０１１０】

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。

【０１１１】

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無い。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、撮像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。

【０１１２】

＜２－３．送信側の処理＞

第２の実施の形態において送信側のユーザ端末２Ａが実行する処理例を図１４に示す。なお、図９に示す第１の実施の形態における送信側の処理と同様の処理については、同じ符号を付し適宜説明を省略する。

【０１１３】

ユーザ端末２Ａの制御部１２は、ステップＳ１０１において、カメラ機能を用いてアレイセンサによる撮像動作を行う。

【０１１４】

ユーザ端末２Ａは、ステップＳ１１１において、撮像画像データの暗号化処理を行う。撮像画像データの暗号化処理は、アレイセンサ１０の画像暗号化処理部２４によって実行される。

【０１１５】

撮像画像データの暗号化処理について具体的に図１５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。

【０１１６】

画像暗号化処理部２４は、ステップＳ３０１で、静止画の撮像動作で生成された撮像画像データを取得する。この撮像画像データは、暗号鍵の生成の元となる静止画データであり、制御部１２の指示によりアレイセンサ１０が１フレーム分の画像の撮像（画素ごとの電荷の読み出し）を実行することにより得る。

ステップＳ３０１で静止画データを取得することで、アレイセンサ１０が備えるメモリ等にシードフレームとしての画像データが保存される。

【０１１７】

ステップＳ３０１に続くステップＳ３０２で画像暗号化処理部２４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する処理であり、具体的に画像暗号化処理部２４は、輝度値がゼロとなっている画素の数や飽和値（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。
【０１１８】
ステップＳ３０２に続くステップＳ３０３で画像暗号化処理部２４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Ｓ３０２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Ｓ３０２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、画像暗号化処理部２４はステップＳ３０４に進んでシードフレームを消去する処理、すなわちメモリ等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Ｓ３０１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。
【０１１９】
一方、ステップＳ３０３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、画像暗号化処理部２４はステップＳ３０５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、画像暗号化処理部２４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。
【０１２０】
ここで、本例おいて、ステップＳ３０５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。
【０１２１】
ステップＳ３０５に続くステップＳ３０６で画像暗号化処理部２４は、シードフレームを消去する処理、すなわち、ステップＳ３０１の取得処理によりメモリ等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。
【０１２２】
なお、例えば画像暗号化処理部２４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、シードフレームをメモリ等に一旦保存させることは必須ではない。この場合には、ステップＳ３０６の消去処理やステップＳ３０４の消去処理が不要とされる。
【０１２３】
続くステップＳ３０７で画像暗号化処理部２４は、既存鍵があれば消去する。例えば、図１５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Ｓ３０８の処理により、画像暗号化処理部２４は暗号鍵を保持している。ステップＳ３０７の処理は、このように保持している既存の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を防止することができる。
【０１２４】
続くステップＳ３０８で画像暗号化処理部２４は、暗号鍵の保存処理を実行する。すな

わち、ステップＳ３０５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。
なお、新規の暗号鍵を既存の暗号鍵に上書き保存することによりステップＳ３０７とステップＳ３０８の処理を同時に行ってもよい。
ステップＳ３０８の保存処理を実行したことに応じ、画像暗号化処理部２４は図１５に示す一連の処理を終える。

【０１２５】

ユーザ端末２Ａにおいては、ステップＳ３０８で保存された暗号鍵を用いて、アレイセンサ１０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、画像暗号化処理部２４は、図１５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各アンプに設定して、アレイセンサ１０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１０は動画像の撮像を行うものとされ、画像暗号化処理部２４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。

【０１２６】

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１２の制御に基づき、メモリ部１３に保存される。制御部１２は、このようにメモリ部１３に保存された撮像画像データを、通信部１５を介してユーザ端末２Ｂに送信することが可能とされる。

【０１２７】

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。

【０１２８】

なお、画像暗号化処理部２４は、図１５に示す処理を、不正アクセスを検出した際に実行することも可能である。
不正アクセスの検知に応じて図１５に示す処理を開始させることで、光電乱数の取得（ステップＳ３０１）や暗号鍵の生成（ステップＳ３０５）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。

【０１２９】

図１４の説明に戻る。
ユーザ端末２Ａの制御部１２は、ステップＳ１０２においてハッシュ値を生成し、ステップＳ１０３において秘密鍵を用いたハッシュ値の暗号化処理を行い、ステップＳ１０４において通話開始要求をユーザ端末２Ｂ（或いはサーバ装置４）に対して送信する。
これにより、ユーザ端末２Ａからユーザ端末２Ｂに対して撮像画像データと、暗号化されたハッシュ値と、公開鍵が送信される。

【０１３０】

＜２－４．受信側の処理＞

第２の実施の形態において受信側のユーザ端末２Ｂが実行する処理例を図１６に示す。
なお、図１０に示す第１の実施の形態における受信側の処理と同様の処理については、同じ符号を付し適宜説明を省略する。

【０１３１】

ユーザ端末２Ａから各データを受信しユーザ端末２Ｂにおいてビデオチャットプログラムが起動されると、ユーザ端末２Ｂの制御部１２は、ステップＳ２０１Ａにおいて、暗号化された撮像画像データと、暗号化されたハッシュ値と公開鍵を取得する。

【０１３２】

次に、ユーザ端末２Ｂの制御部１２はステップＳ２０２において、暗号化されたハッシュ値の復号化処理を実行する。

【０１３３】

続いて、ユーザ端末２Ｂの制御部１２はステップＳ２０３Ａにおいて、暗号化された状態の撮像画像からハッシュ値を算出する。

【０１３４】

ユーザ端末２Ｂの制御部１２は、ステップＳ２０４で算出したハッシュ値と復号化したハッシュ値の比較処理を行い、ステップＳ２０５で改竄判定処理を行い、ステップＳ２０６において改竄判定結果に応じた分岐処理を行う。

【０１３５】

ユーザ端末２Ｂの制御部１２は、改竄されていないことが保証できると判定した場合にステップＳ２０７の第１担保状態ＳＴ１に基づく出力制御を行い、保証できないと判定した場合にステップＳ２０８の非担保状態ＳＴ０に基づく出力制御を行う。

【０１３６】

これにより、ユーザＢに提示される着信画面５０において第１保証アイコンＭＫ１や非保証アイコンＭＫ０が表示される。

【０１３７】

＜３．第３の実施の形態＞

第３の実施の形態における情報処理システム１では、受信側のユーザ端末２Ｂにおいて受信した撮像画像データの保証状態に応じた表示を行う。具体的には、ユーザ端末２Ａから受信した撮像画像データに対する状態判定部４１の判定結果（非担保状態ＳＴ０、第１担保状態ＳＴ１、第２担保状態ＳＴ２、第３担保状態ＳＴ３）に応じた画面表示を行う。

【０１３８】

システム構成やユーザ端末２の構成や構成等については第１の実施の形態で説明したものと同様の構成であるため説明を省略する。従って、以降においては、送信側であるユーザ端末２Ａの処理と受信側であるユーザ端末２Ｂの処理の流れについて説明する。

【０１３９】

＜３－１．送信側の処理＞

送信側であるユーザ端末２Ａは、例えば、図９に示す各処理を実行する。但し、第３の実施の形態においては、生体解析を行う。生体解析は、複数枚の静止画像から生体情報を抽出する処理である。従って、ステップＳ１０１の撮像動作は複数枚の静止画像を取得するために行われる。

また、ステップＳ１０２のハッシュ値の生成処理では、複数枚の静止画像データそれぞれにおいてハッシュ値を生成する。更に、ステップＳ１０３の暗号化処理は、生成した複数のハッシュ値それぞれを暗号化するものである。

【０１４０】

ステップＳ１０４の通話開始要求送信処理では、複数枚の撮像画像データとそれぞれに対応する暗号化されたハッシュ値と公開鍵をユーザ端末２Ｂへ送信する。

【０１４１】

＜３－２．受信側の処理＞

第３の実施の形態において、受信側であるユーザ端末２Ｂは、ユーザ端末２Ａから撮像画像データと暗号化されたハッシュ値と公開鍵を受信したことによって、例えば図１７及び図１８に示す各処理を実行する。

なお、図１０に示す各処理と同様の処理については同じ符号を付し適宜説明を省略する。

【０１４２】

ユーザ端末２Ｂの制御部１２は、ステップＳ２０１からステップＳ２０５の各処理を実行することにより、受信した各撮像画像データが改竄されていないことを保証できるか否かを判定する。

【０１４３】

ユーザ端末２Ｂの制御部１２は、ステップＳ２０６において、改竄判定処理の結果に応

じた分岐処理を行う。具体的には、改竄されていないことが保証できない場合、ユーザ端末２Ｂの制御部１２はステップＳ２０８で非担保状態ＳＴ０に基づく出力制御を行う。これにより、ユーザ端末２Ｂにおいてユーザに提示される着信画面５０上に図８に示すような非保証アイコンＭＫ０や説明文６３が表示される。

【０１４４】

一方、改竄されていないことを保証できると判定した場合、ユーザ端末２Ｂの制御部１２は図１８に示す各処理を実行する。

具体的には、ユーザ端末２Ｂの制御部１２は、ステップＳ２１１において、生体解析処理を実行する。生体解析処理は、複数枚の静止画像から生体情報を抽出する処理であり、生体ならではの情報を抽出する処理である。

【０１４５】

例えば、生体である人間からは眼振を検出することができる。眼振は、１枚の撮像画像データから抽出することはできないが、複数枚の撮像画像データにおける眼球付近の差分情報を抽出することにより検出可能である。

【０１４６】

或いは、生体である人間からは心拍を検出することができる。人間の肌の色は心拍に合わせて微少に変化している。このような変化を複数枚の撮像画像データから抽出する。

【０１４７】

更には、明るさによる瞳孔反応やリップシンクを複数枚の撮像画像データから抽出することもできる。

【０１４８】

ステップＳ２１１の生体解析処理では、このような生体情報の抽出を行う。

【０１４９】

続いて、ユーザ端末２Ｂの制御部１２は、ステップＳ２１２において、生体判定処理を実行する。この処理は、抽出した生体情報に基づいて被写体が生体であるか否かを判定する処理である。例えば、複数枚の撮像画像データから生体情報として眼振が検出された場合には、被写体は生体であると判定する。

【０１５０】

ユーザ端末２Ｂの制御部１２は、ステップＳ２１３において、生体であるか否かの判定結果に基づいた分岐処理を行う。

被写体が生体であると判定できなかった場合（或いは生体でないと判定した場合）は、撮像画像データが改竄されていないことは保証できるが生体であるという保証はできない状態とされる。この場合、ユーザ端末２Ｂの制御部１２はステップＳ２０７において第１担保状態ＳＴ１に基づく出力制御を行う。これにより、ユーザ端末２Ｂにおいてユーザに提示される着信画面５０上に図４に示すような第１保証アイコンＭＫ１や説明文６３が表示される。

【０１５１】

一方、被写体が生体であると判定した場合、ユーザ端末２Ｂの制御部１２はステップＳ２１４において、個体解析処理を行う。

個体解析処理は、受信した撮像画像データから個体を識別するための個体情報を抽出する処理である。

【０１５２】

個体解析処理を終えた後、ユーザ端末２Ｂの制御部１２はステップＳ２１５において、個体判定処理を行う。個体判定処理は、抽出した個体情報に基づいて個体を判定する処理を行う。個体判定処理は、被写体を個人特定してもよいし、個人特定可能な情報が抽出できたか否かを判定してもよい。

【０１５３】

ユーザ端末２Ｂの制御部１２はステップＳ２１６において、個体判定処理の判定結果に基づく分岐処理を実行する。

個体が特定できなかった場合、或いは、個体を特定可能な情報を抽出できなかった場合

は、撮像画像データが改竄されていないこと及び被写体が生体であることは保証できるが個体までは特定できなかった場合である。この場合には、ユーザ端末２Ｂの制御部１２はステップＳ２１７において第２担保状態ＳＴ２に基づく出力制御を行う。

これにより、ユーザ端末２Ｂにおいてユーザに提示される着信画面５０上に図６に示すような第２保証アイコンＭＫ２や説明文６３が表示される。

【０１５４】

一方、個体が特定できた場合、或いは、個体を特定可能な情報を抽出できた場合、ユーザ端末２Ｂの制御部１２はステップＳ２１８において第３担保状態ＳＴ３に基づく出力制御を行う。

これにより、ユーザ端末２Ｂにおいてユーザに提示される着信画面５０上に図７に示すような第３保証アイコンＭＫ３や説明文６３が表示される。

【０１５５】

以上説明してきたように、ユーザ端末２Ｂは受信した撮像画像データについての改竄可能性の有無や抽出できる情報に応じて、着信画面５０上に保証アイコン６２や説明文６３を表示させる。これにより、ユーザＢは着信に応じるか否かを適切に判断することができ、詐欺などの被害にあってしまうことを未然に防止することができる。

【０１５６】

なお、改竄判定処理や生体解析処理や個体解析処理に用いる撮像画像データは、実際にユーザＢに提示される送信者の動画像データを利用してもよい。これにより、改竄判定処理や各解析処理に用いるための専用の撮像画像データを取得する必要がなく、処理負担の軽減や通信容量の削減を図ることができる。

【０１５７】

＜３－３．適用例＞

なお、第１の実施の形態、第２の実施の形態及び第３の実施の形態に記載した構成は、音声を伴わないテキストチャットシステムにも適用することができる。

具体的に、テキストチャットシステムを利用するユーザに提示されるテキストチャット画面５２を示した図１９を参照して説明する。

【０１５８】

テキストチャット画面５２は、チャットに参加しているユーザごとに設定された参加者アイコン７０と、参加者ごとの保証状態を示す保証アイコン７１と、発言内容が表示される吹き出し７２と、発言内容を入力するための入力欄７３と、各種の機能を実行させるための機能アイコン７４が配置されている。

【０１５９】

参加者アイコン７０には、自分（ユーザＢ）以外の参加者についての参加者アイコン７０Ａと自分の参加者アイコン７０Ｂが設けられている。

また、保証アイコン７１には、自分（ユーザＢ）以外の参加者についての保証アイコン７１Ａと自分の保証アイコン７１Ｂが設けられている。

【０１６０】

図１９の例では、他ユーザについての保証アイコン７１Ａは第２保証アイコンＭＫ２とされ、自身についての保証アイコン７１Ｂは第３保証アイコンＭＫ３とされている。

このように、参加者ごとの保証状態に合わせた保証アイコン７１が表示されている。

【０１６１】

なお、自身についての保証アイコン７１Ｂは少なくとも他の参加者に提示されているテキストチャット画面５２において表示されていればよい。即ち、ユーザＢに提示されるテキストチャット画面５２においてユーザＢ自身の保証アイコン７１は表示されなくてもよい。但し、自身の保証アイコン７１が表示されることで、他の参加者に対して自身の保証状態がどのように表示されているかを把握することができる。これにより、意図した保証状態になっていない場合に、上述した各種の判定処理や解析処理を再度実行させるなどの操作を行うことが可能となる。

【０１６２】

テキストチャットシステムは、上述したビデオチャットシステムと異なり、本来撮像画像データの送信を必要としないものである。しかし、本適用例においては、改竄判定処理や各種の解析処理のために撮像画像データを送信する。従って、送信する撮像画像データは、改竄判定や解析処理の実行が可能な程度であればよく、解像度等を落としてもよい。また、生体解析処理や個体解析処理を行わずに改竄判定処理のみを実行する場合には、被写体を人が認識できないほどに解像度を落としたような撮像画像データを送信してもよい。これにより、撮像画像データの漏洩リスクを低減させることができる。

【０１６３】

＜４．第４の実施の形態＞

＜４－１．システム構成＞

第４の実施の形態における情報処理システム１Ａでは、各種のサービスを利用するためのログインや新規登録を行う際に改竄判定処理や生体解析処理や個体解析処理を行うものである。

情報処理システム１Ａの概略構成例を示したブロック図を図２０に示す。

【０１６４】

情報処理システム１Ａは、ユーザ端末２とネットワーク３とサーバ装置４とを備えている。

ユーザ端末２は、各種サービス（例えばソーシャルネットワーキングサービス）を利用するユーザが使用する情報処理装置である。

【０１６５】

ネットワーク３は、第１の実施の形態と同様に、インターネットなど各種の例が考えられる。

【０１６６】

サーバ装置４は、各種サービスを提供するための情報処理装置で、例えば、ユーザ情報の管理やＡＰＩ（Application Programming Interface）機能などを備えている。

なお、本実施の形態においては、サーバ装置４が改竄判定処理や各種の解析処理を実行する。

【０１６７】

ユーザ端末２の構成について図２１に一例を示す。

ユーザ端末２は、電子署名の対象とされた撮像画像データを取得するためのアレイセンサ１０と、画像プロセッサ１１と制御部１２とメモリ部１３と入力部１４と通信部１５と出力部１６とを備えている。制御部１２は、取得部３１など図２に示す各部を備えていない。アレイセンサ１０や画像プロセッサ１１やメモリ部１３や入力部１４や通信部１５や出力部１６については第１の実施の形態で説明したものと同様のため、詳述を省く。

【０１６８】

サーバ装置４の構成について図２２に一例を示す。

サーバ装置４は、制御部１２とメモリ部１３と入力部１４と通信部１５と出力部１６とを備えている。

制御部１２は、各種機能を備えており、具体的には、取得部３１、復号化処理部３２、ハッシュ値算出部３３、ハッシュ値比較部３４、改竄判定部３５、生体解析処理部３６、生体判定部３７、個体解析処理部３８、個体判定部３９、出力制御部４０、状態判定部４１、認証処理部４２を備えている。

【０１６９】

取得部３１、復号化処理部３２、ハッシュ値算出部３３、ハッシュ値比較部３４、改竄判定部３５、生体解析処理部３６、生体判定部３７、個体解析処理部３８、個体判定部３９、出力制御部４０、状態判定部４１の各部については、第１の実施の形態のユーザ端末２が備えているものと同様のため、詳述を省く。

【０１７０】

認証処理部４２は、サーバ装置４が提供するサービスをユーザに利用させるか否かを判定する認証処理を実行する。具体的には、ユーザ端末２を利用する人物が登録されたユー

ザと一致するか否かを判定する処理を実行する。これにより、例えば、ログインについての可否の判定が行われる。

【０１７１】

メモリ部１３，入力部１４，通信部１５及び出力部１６については、第１の実施の形態と同様のため、詳述を省く。

【０１７２】

＜４－２．ログイン画面＞

サーバ装置４が提供するサービスを利用するためにユーザがユーザ端末２を用いてログイン画面を表示させる操作を行うと、例えば、図２３に示すログイン画面５３が表示される。

なお、図２３に示す例は、元々表示されていた画面上にログイン画面５３としてのモーダルウィンドウが重畳表示された例である。

【０１７３】

ログイン画面５３には、例えば、アカウント名（或いはユーザＩＤ（Identification）やメールアドレスなどでもよい）を入力するためのＩＤ入力欄８０と、パスワードを入力するためのパスワード入力欄８１と、保証アイコン８２と、認証処理をサーバ装置４に依頼するためのログインボタン８３と、ログイン操作を取りやめるためのキャンセルボタン８４が設けられている。

【０１７４】

ユーザは、ＩＤ入力欄８０とパスワード入力欄８１に所定の文字列を入力した後ログインボタン８３を押下することで、サーバ装置４に認証処理を実行させることができる。

【０１７５】

保証アイコン８２は、ログイン画面５３が表示される際にユーザ端末２で撮像動作が行われると共に撮像画像データ、ハッシュ値及び公開鍵がサーバ装置４に送信されることによりサーバ装置４おいて実行される改竄判定処理の判定結果に応じて表示されるものである。

即ち、保証アイコン８２は、ユーザ端末２において撮像された撮像画像データに関してサーバ装置４がどのような保証を行ったか（保証の度合いなど）をユーザに提示するために表示されるものである。

【０１７６】

保証アイコン８２は、サーバ装置４が実行する処理内容に応じて表示されるものであり、サーバ装置４が改竄判定処理のみを実行する場合には非保証アイコンＭＫ０か第１保証アイコンＭＫ１の何れかが表示される。

また、サーバ装置４が改竄判定処理だけでなく生体判定処理や個体判定処理を実行する場合には、非保証アイコンＭＫ０、第１保証アイコンＭＫ１、第２保証アイコンＭＫ２、第３保証アイコンＭＫ３のいずれかが表示される。

【０１７７】

＜４－３．ユーザ端末の処理＞

第４の実施の形態においてユーザ端末２の制御部１２が実行する処理の一例について、図２４を参照して説明する。

なお、図９に示したユーザ端末２が実行する処理と同等の処理については、同じ符号を付し適宜説明を省略する。

【０１７８】

ログイン画面５３を表示させるための操作がユーザによって実行されると、ユーザ端末２の制御部１２は、ステップＳ１０１でカメラ機能を起動しアレイセンサによる撮像動作を行う。

続いて、ユーザ端末２の制御部１２は、ステップＳ１０２において撮像画像データからハッシュ値の生成を行い、ステップＳ１０３においてハッシュ値の暗号化処理を施す。

【０１７９】

ユーザ端末２の制御部１２はステップＳ１２１で、撮像画像データと暗号化されたハッ

シュ値と公開鍵をサーバ装置４に送信する。なお、送信する撮像画像データは暗号化されたものとしてもよい。その場合には、撮像画像データをサーバ装置４に送信する前に図１４のステップＳ１１１の処理を実行すればよい。

【０１８０】

ユーザ端末２の制御部１２はステップＳ１２２で文字入力操作を検出したか否かを判定する。文字入力操作を検出した場合、ユーザ端末２の制御部１２はステップＳ１２３において対応する入力欄（ＩＤ入力欄８０、パスワード入力欄８１）に入力文字を表示させる処理を行う。なお、パスワード入力欄８１に関しては、入力された文字列が分からないように所定の文字（例えば「＊」）で表示を代用してもよい。

【０１８１】

ステップＳ１２３の処理を実行した後、ユーザ端末２の制御部１２は再度ステップＳ１２２の処理へと戻る。

【０１８２】

文字入力操作を検出していない場合、ユーザ端末２の制御部１２はステップＳ１２４でサーバ装置４から判定結果情報を受信したか否かを判定する。

改竄判定処理の結果など、判定処理を受信した場合、ユーザ端末２の制御部１２はステップＳ１２５で保証アイコン８２をログイン画面５３上に表示させる処理を行う。なお、保証アイコン８２が既に表示されている状態で新たに判定結果を受信した場合、ステップＳ１２５の処理は、保証アイコン８２を更新する処理とされてもよい。

【０１８３】

サーバ装置４から判定結果情報を受信していない場合、ユーザ端末２の制御部１２はステップＳ１２６において、ログインボタン８３の押下を検出したか否かを判定する。

ログインボタン８３の押下を検出した場合、ユーザ端末２の制御部１２はステップＳ１２７の認証処理要求をサーバ装置４に送信する処理を実行した後、図２４に示す一連の処理を終了させる。なお、終了させる際に、ログイン画面５３の表示を終了させてもよい。

【０１８４】

ログインボタン８３の押下を検出していない場合、ユーザ端末２の制御部１２はステップＳ１２８でキャンセルボタン８４の押下を検出したか否かを判定する。

キャンセルボタン８４の押下を検出した場合、ユーザ端末２の制御部１２は図２４に示す一連の処理を終了させる。

【０１８５】

一方、キャンセルボタン８４の押下を検出していない場合、ユーザ端末２の制御部１２は再びステップＳ１２２の処理へと戻る。

即ち、ユーザ端末２の制御部１２は、ステップＳ１２２、Ｓ１２４、Ｓ１２６及びＳ１２８の各処理を順に実行することにより、文字入力操作や各ボタンに対する押下操作や判定結果の受信を検出していないかを確認し、各操作を検出した場合には対応する処理（ステップＳ１２３，Ｓ１２５，Ｓ１２７の処理）を実行するものである。

【０１８６】

＜４－４．サーバ装置の処理＞

第４の実施の形態においてサーバ装置４が実行する処理の一例について説明する。

なお、図１０に示す処理と同様の処理については、同じ符号を付し適宜説明を省略する。

【０１８７】

ユーザ端末２から撮像画像データと、暗号化されたハッシュ値と公開鍵を受信したことに応じて、サーバ装置４の制御部１２は、図２５に示す一連の処理を開始させる。

具体的には、サーバ装置４の制御部１２は、ステップＳ２０１において撮像画像データと暗号化されたハッシュ値と公開鍵を取得し、ステップＳ２０２において暗号化されたハッシュ値の復号化処理を行い、ステップＳ２０３において受信した撮像画像データからハッシュ値を算出し、ステップＳ２０４においてハッシュ値の比較処理を行い、ステップＳ２０５において改竄判定処理を行う。

【０１８８】

続いて、サーバ装置４の制御部１２は、ステップＳ２２１において、改竄判定処理の判定結果をユーザ端末２に通知する処理を行う。
これにより、撮像画像データの改竄がされていないことの保証がされたか否かについての通知がユーザ端末２に対してなされる。ユーザ端末２では、この通知に応じた保証アイコン６２がログイン画面５３上に表示される（図２４のステップＳ１２５の処理）。
【０１８９】
なお、サーバ装置４の制御部１２は、ステップＳ２０５の改竄判定処理に加えて、生体解析処理及び生体判定処理や、個体解析処理及び個体判定処理などを実行してもよい。この場合には、改竄判定処理の結果と生体判定処理の結果と個体判定処理の結果に応じた通知処理がなされ、ユーザ端末２では非保証アイコンＭＫ０，第１保証アイコンＭＫ１、第２保証アイコンＭＫ２、第３保証アイコンＭＫ３のいずれかがログイン画面５３上に表示される。
【０１９０】
図２５の説明に戻る。
サーバ装置４の制御部１２は、ステップＳ２２１で判定結果の通知処理を行った後、ステップＳ２２２で認証処理要求をユーザ端末２から受信したか否かを判定する。
承認要求を受信していない場合、サーバ装置４の制御部１２は、ステップＳ２２３で判定結果通知処理から一定時間が経過したか否かを判定する。一定時間経過していた場合、サーバ装置４の制御部１２は図２５に示す一連の処理を終了させる。
【０１９１】
一方、一定時間経過していない場合、サーバ装置４の制御部１２は、ステップＳ２２２の処理へと戻る。
【０１９２】
改竄判定処理の結果を通知した後、長時間が経過してしまうと、ユーザ端末２を操作している人物が変わっている虞が高くなる。そこで、本例においては、判定結果を通知した後、認証処理要求を受信するまで所定時間が経過してしまった場合には、図２５に示す一連の処理を終了させることにより後述するステップＳ２２５の認証処理を実行しないように構成されている。これにより、ステップＳ２０１で受信した撮像画像データに映っている被写体と実際に認証処理を要求した人物が異なってしまうことを防止している。即ち、本構成によれば、不正にログインされてしまう可能性を低減させることができる。
【０１９３】
ステップＳ２２２において認証処理要求を受信したと判定した場合、サーバ装置４の制御部１２は、ステップＳ２２４で照合処理を実行する。照合処理は、例えば、ユーザ端末２から受信した認証処理要求に含まれているアカウント名（ユーザＩＤ）とパスワードを取得し、データベースに記憶されている情報と照合する処理である。ユーザ端末２から受信した情報とデータベースに記憶された情報が一致した場合には、照合成功と判定される。また、一致しなかった場合には照合失敗と判定される。
【０１９４】
サーバ装置４の制御部１２は、ステップＳ２２５において、認証処理を実行する。認証処理は、改竄判定処理の結果と照合処理の結果に基づいてユーザに特定の機能を利用させるか否かを判定する処理である。即ち、認証成功と判定した場合は、ユーザは特定の機能を利用することができる。一方、認証失敗と判定した場合は、ユーザは特定の機能を利用することができない。
【０１９５】
サーバ装置４の制御部１２は、ステップＳ２２６において、認証処理の結果を通知する処理を実行する。これにより、ユーザ端末２の画面上に認証（ログイン）が成功したか否かを示す情報が表示される。例えば、認証が成功した場合にはマイページが表示され、認証が失敗した場合には認証が失敗したことを通知するためのページが表示されるように構成されている。
【０１９６】

なお、改竄判定処理の結果と認証結果の組み合わせは各種考えられる。その中で認証成功と判定される可能性があるのは、例えば、改竄判定結果が「非改竄判定」とされ認証処理結果が認証成功とされた場合（ケース１）や、改竄判定結果が「改竄判定」とされ認証処理結果が認証成功とされた場合（ケース２）が考えられる。

【０１９７】

ケース１については、問題無くサーバ装置４が提供する各種の機能を利用させることができる。

ケース２については、改竄判定結果が「改竄判定」とされていることから、様々な態様が考えられる。例えば、サーバ装置４が提供する各種の機能のうち、一部の機能を制限した状態で提供してもよい。

【０１９８】

また、ケース２については、特定の条件下でのみ全機能を利用できるように構成してもよい。具体的には、ユーザが使用しているユーザ端末２のＭＡＣアドレスを取得し、これまでに使用履歴があるか否かを判定する処理を更に実行する。ユーザ端末２がこれまでに使用されたことのある端末であると判定した場合には、認証成功と判定する。

或いは、ユーザ端末２や他の端末を用いて二次認証を実行してもよい。具体的には、登録したメールアドレスに認証コードを送信し、認証コードを入力させる処理や、秘密の質問に対する回答を入力させる処理を実行してもよい。ユーザがこれらの処理に対する正しい入力操作を実行できた場合には、認証成功と判定し全ての機能の利用を許可してもよい。

【０１９９】

サーバ装置４が改竄判定処理だけでなく生体判定処理の結果及び個体判定処理を実行する場合には、これらの判定処理の結果の組み合わせに基づいて、全機能の提供や一部機能の提供や二次認証処理の実行を決定すればよい。

このような構成により、サーバ装置４が提供する機能の不正利用や不適切な利用などを防止することができる。

【０２００】

第４の実施の形態に係る情報処理システム１は、直筆のサインを入力可能なタブレット端末などを備えたサインアップシステムにも適用することができる。具体的には、来社した来客用に設置された操作端末と認証を行うサーバ装置４を備えた情報処理システム１である。

タブレット端末上に表示される具体的なサインアップ画面５４の例を図２６に示す。サインアップ画面５４には、サインを入力するためのサイン入力欄９０とサイン入力欄９０に表示される保証アイコン９１が表示されている。保証アイコン９１は、サーバ装置４が実行する処理内容に応じて表示されるものであり、サーバ装置４が改竄判定処理のみを実行する場合には非保証アイコンＭＫ０か第１保証アイコンＭＫ１の何れかが表示される。

また、サーバ装置４が改竄判定処理だけでなく生体判定処理や個体判定処理を実行する場合には、非保証アイコンＭＫ０、第１保証アイコンＭＫ１、第２保証アイコンＭＫ２、第３保証アイコンＭＫ３のいずれかが表示される。

【０２０１】

その場合には、各図で説明したユーザ端末２が実行する処理を来客用に設置された操作端末が実行すればよい。即ち、上述した説明におけるユーザ端末２を操作端末に読み替えればよい。これにより、操作端末は図２１に示すアレイセンサ１０を備えた情報処理装置とされる。また、サーバ装置４は、アレイセンサ１０で撮像した来客の撮像画像データと来客者によって入力された直筆のサインに関する各種の判定処理を実行する。

【０２０２】

＜５．変形例＞

上述した各実施の形態においては、受信側の情報処理装置でのみ改竄判定処理や生体判定処理や個体判定処理を実行する例を説明した。

本変形例においては、送信側の情報処理装置においてもそれらの処理を実行するものである。具体的には、送信側の情報処理装置において、生体判定処理を実行する。この場合

の送信側の情報処理装置としてのユーザ端末２が実行する処理例について、図２７を参照して説明する。
なお、本変形例においてはビデオチャットシステムとしての情報処理システム１を例に挙げる。
【０２０３】
図９に示す処理と同様の処理については、同じ符号を付し適宜説明を省略する。
ユーザ端末２は、ステップＳ１０１で撮像動作を行い、ステップＳ１０２でハッシュ値を生成し、ステップＳ１０３でハッシュ値の暗号化を行う。なお、本例においては、複数枚の撮像画像データを取得する。
【０２０４】
次に、ユーザ端末２はステップＳ１３１において、複数枚の撮像画像データを解析し生体情報を抽出する処理を行う。この処理は、第３の実施の形態において受信側のユーザ端末２Ｂで実行したステップＳ２１１（図１８）の処理と同様の処理である。
【０２０５】
続いて、ユーザ端末２はステップＳ１３２において、抽出した生体情報に基づいて被写体が生体であるか否かを判定する。この処理は、図１８のステップＳ２１２の処理と同様の処理である。
【０２０６】
ユーザ端末２は、ステップＳ１３３において、生体であるか否かの判定結果に基づいた分岐処理を行う。
被写体が生体であると判定した場合、ユーザ端末２はステップＳ１０４において、通話開始要求をサーバ装置４に対して送信する。
【０２０７】
一方、被写体が生体であると判定できなかった場合（或いは生体でないと判定した場合）、ユーザ端末２は図２７に示す一連の処理を終了させる。即ち、サーバ装置４に対する通話開始要求を行わない。
【０２０８】
これにより、サーバ装置４が通話開始要求を受信するという状況は、ユーザ端末２において被写体が生体であることが担保された場合に限られる。従って、サーバ装置４で被写体が生体であると判定できなかった場合は、不正者による不正な通話開始要求がなされた可能性が高い。この場合には、通話開始要求を受信しても通話を開始させないことにより、詐欺などの不正行為を未然に防止することが可能となる。
【０２０９】
なお、ユーザ端末２において個体解析処理及び個体判定処理を行い、個人を特定可能な情報が抽出できた場合に限りステップＳ１０４の通話開始要求を送信するように構成してもよい。
これにより、不正な通話開始要求の防止を更に図ることができる。
【０２１０】
上述した例では、保証アイコン６２によってユーザに通知する例を説明したが、それ以外の方法であってもよい。例えば、音声による通知を行ってもよい。更に、保証アイコン６２による通知と音声による通知の双方を同時に或いは時分割で実行してもよい。
例えば、ビデオチャットシステムとしての情報処理システム１であれば、保証状態に応じて着信音を変えることが考えられる。
また、保証状態に応じて着信画面５０の背景色を変えるなど、画面の態様やデザインを変更するように構成してもよい。
【０２１１】
なお、上述したユーザ端末２は少なくとも一方が店舗端末であってもよい。例えば、店舗端末でユーザ（顧客或いは店舗にいるオペレータ）が実際に端末の前で操作していることを保証するために、店舗端末で撮像動作とハッシュ値の生成とハッシュ値の暗号化を行い、サーバ装置で復号化処理とハッシュ値算出処理とハッシュ値比較処理と改竄判定処理

を実行することにより、ハッキングが行われていないことを検出してもよい。また、この場合には、サーバ装置が更に生体解析処理と生体判定処理を実行することにより、機械による自動的な不正行為が行われていないことを保証してもよい。更に、サーバ装置が個体解析処理と個体判定処理を実行し、取得したオペレータの個体特徴量と事前に保存しておいた該オペレータについてのデータとを比較することにより、確かに登録されているオペレータによる操作であることを保証してもよい。これにより、不正行為を行い難くすることができ、セキュリティの向上を図ることができる。

【０２１２】

＜６．まとめ＞

上述した各実施の形態や変形例で説明したように、情報処理システム１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画素アレイ２１と、画素アレイにおける光電変換に基づいて得た撮像画像データからハッシュ値を生成するハッシュ値生成部２２と、ハッシュ値に対する暗号化処理を実行する暗号化処理部２３と、を有するアレイセンサ１０と、撮像画像データと暗号化されたハッシュ値を取得する取得部３１と、取得した暗号化されたハッシュ値の復号化を行う復号化処理部３２と、取得した撮像画像データからハッシュ値を算出するハッシュ値算出部３３と、復号化されたハッシュ値と算出されたハッシュ値を比較するハッシュ値比較部３４と、ハッシュ値の比較結果に基づいて取得した撮像画像データの改竄の有無を判定する改竄判定部３５と、を備えている。

即ち、アレイセンサ１０内でハッシュ値の生成と暗号化処理が実行される。

これにより、撮像されてからハッシュ値の生成に供されるまでの間に撮像画像データが改竄されてしまう可能性を著しく低減させることができ、改竄の困難性を向上させることができる。また、改竄の検出性能の向上を図ることができる。

【０２１３】

第１及び第３の実施の形態で説明したように、取得した撮像画像データに基づいて被写体の生体情報を抽出するための解析を行う生体解析処理部３６と、生体解析処理部３６の解析結果に基づいて被写体が生体であるか否かを判定する生体判定部３７と、を備えていてもよい。

これにより、被写体が生きている生体であるか否かを判定することができる。

従って、例えば、生きている人間が端末の前にいる状況で通話開始要求や認証処理要求が送信されたか否かを判定することができ、ユーザによる正規のログイン操作と機械による不正ログイン処理等を見分けることができ、詐欺行為等を未然に防ぐことが可能となる。

即ち、例えば３Ｄプリンターで製作された顔の模型をカメラの前に置くことにより本人による手続きであると誤認させることが困難とされる。

また、例えば、お問い合わせ用のチャット機能が設けられたウェブサイト等において、該チャット機能が利用された際に、実際にオペレータが対応している場合には、人間が対応していることを保証する保証マークを問い合わせユーザの利用しているユーザ端末上に表示させることで、機械的な対応でないことを訴求することができユーザの信用度を高めることができる。この場合には、オペレータが利用しているユーザ端末はハッシュ値生成処理とハッシュ値の暗号化処理を行う第３の実施の形態におけるユーザ端末２Ａとされ、問い合わせユーザが利用するユーザ端末は復号化処理とハッシュ値算出処理とハッシュ値比較処理と改竄判定処理と生体解析処理と生体判定処理を行う第３の実施の形態におけるユーザ端末２Ｂとされる。

【０２１４】

第１及び第３の実施の形態で説明したように、取得した撮像画像データに含まれる被写体の個体特徴量を解析するための個体解析処理部３８と、個体解析処理部３８の解析結果に基づいて被写体についての個体認識可否を判定する個体判定部３９と、を備えていてもよい。

これにより、被写体を個人特定するための情報を得ることができる。

従って、例えば、特定のユーザに対して機能を提供することや、特定のユーザであるこ

とを通信相手に通知することなどが可能となり、改竄やなりすまし等を防止することができ、詐欺行為等を未然に防ぐことが可能となる。
　また、例えば、営業活動を行うユーザが本技術のハッシュ値生成処理と暗号化処理を実行可能なアレイセンサ１０を有する撮像装置を利用して他のユーザに対する通話要求を行うことにより、他のユーザの警戒感を薄れさせ自身への信用度を高めることができる。これにより、営業活動をし易くすることができる。
【０２１５】
　第１の実施の形態などで説明したように、改竄判定部３５の判定結果を通知するための出力制御を行う出力制御部４０を備えていてもよい。
　これにより、改竄判定結果をユーザが認識することができる。
　従って、判定結果に応じた操作をユーザが選択することができる。例えば、ビデオチャットシステムであれば、相手からの着信に応えるか否かについて改竄判定の結果に基づいた選択を行うことができる。
【０２１６】
　第３の実施の形態などで説明したように、生体判定部３７の判定結果を通知するための出力制御を行う出力制御部４０を備えていてもよい。
　これにより、生体判定結果をユーザに通知することができる。
　従って、生体判定の結果に応じた操作をユーザが選択することができる。例えば、機械による自動的な通話要求を判別することができるようになり、そのような通話要求を拒否することが可能となる。
【０２１７】
　第３の実施の形態で説明したように、個体判定部３９の判定結果を通知するための出力制御を行う出力制御部４０を備えていてもよい。
　これにより、個体判定の結果をユーザに通知することができる。
　従って、個体判定の結果に応じた操作をユーザが選択することができる。例えば、個人認証されていない不審なユーザからの通話要求を拒絶することなどが可能となる。
【０２１８】
　各実施の形態で説明したように、撮像装置（ユーザ端末２Ａ）と情報処理装置（ユーザ端末２Ｂ）とを含んで構成され、撮像装置は、アレイセンサ１０を有し、情報処理装置は、取得部３１と、復号化処理部３２と、ハッシュ値算出部３３と、ハッシュ値比較部３４と、改竄判定部３５と、出力制御部４０と、を有していてもよい。
　例えば、撮像装置と情報処理装置から成る監視カメラシステムなどに適用可能である。
　具体的には、監視カメラで撮像された撮像画像データが確かに監視カメラで撮像されたデータであり、且つ、改竄されていないことを情報処理装置とされたサーバ装置で確認することができる。
　また、二者間の通話を行う場合において、一方のユーザが使用するユーザ端末２（２Ａ）を撮像装置として捉え、他方のユーザが使用するユーザ端末２（２Ｂ）を情報処理装置として捉えることもできる。
【０２１９】
　各実施の形態で説明したように、出力制御部４０は、取得した撮像画像データを表示出力する制御と、取得した撮像画像データについての改竄判定部３５の判定結果を表示出力する制御と、を実行してもよい。
　このような情報処理システムとしては、例えば、受信した撮像画像を表示しつつその画像についての改竄の有無を表示するユーザインタフェース制御を行うものが考えられる。
　例えば、ビデオチャットシステムや防犯カメラの管理システムなどが考えられる。また、オークションシステムについても、ユーザが利用するアプリケーション（オークションアプリ）において出品された商品の画像を表示する際に、サーバ装置にアップロードされた撮像画像データ（商品画像のデータ）や暗号化されたハッシュ値を取得し、非改竄性の判定処理を行い、判定結果を画像と共に表示することが考えられる。これにより、商品に付いている傷などを画像加工アプリケーションなどで消去した改竄画像でないことをユー

ザは確認することができ、利便性の向上を図ることができる。また、商品を不当に高品質に見せかけるなどの詐欺行為を見分けることも可能となる。

具体的に、オークションシステムにおけるオークションサイトや宿泊検索システムにおける検索サイトにおいては、撮像された出品物（図２８参照）や部屋の画像（図２９参照）が掲載される。そして、これらの撮像画像の上部には、改竄が行われていないことを示す実写保証アイコンが重畳されている。このような実写保証アイコンが重畳されることにより、画像加工アプリケーションなどで被写体（出品物や部屋）の見栄えを改善した改竄画像でないことをユーザが確認することができる。

このような被写体は、上述したような生体情報を抽出可能な被写体ではなく、生体情報を抽出できない無機物の被写体などである。即ち、本技術は、生体情報を抽出可能な人物などの被写体だけでなく、無機物などの被写体に対しても適用することができる。

【０２２０】

第３の実施の形態における適用例で説明したように、出力制御部４０は、取得した撮像画像データについての表示出力を行わずに改竄判定部３５の判定結果を表示出力する制御を行ってもよい。

このような情報処理システムとしては、例えば、撮像画像が表示されないようなテキストチャットシステムなどが考えられる。

画像表示を行わない場合であっても、通信相手が信用に足る人物であるのか否かなどの判断指標を提示することができる。従って、詐欺行為等を未然に防ぐことが可能となる。

【０２２１】

第３の実施の形態における適用例で説明したように、出力制御部４０は、チャット画面を提示する制御と、チャット参加者が使用する撮像装置（ユーザ端末２Ａ）から受信した参加者の撮像画像データについての改竄判定部３５の判定結果をチャット画面においてチャット参加者ごとに表示出力する制御と、を行ってもよい。

撮像画像が表示されないようなテキストチャットシステムなどにおいては、どのような人物がチャットを利用しているかを知ることは困難である。本構成によれば、参加者ごとに信用できるか否かの指標が表示される。

従って、ユーザは適切なコミュニケーションを図ることが可能となる。

【０２２２】

第４の実施の形態で説明したように、撮像装置（ユーザ端末２）と情報処理装置（サーバ装置４）とを含んで構成され、撮像装置は、アレイセンサ１０と、出力制御部４０と、を有し、情報処理装置は、認証処理を行う認証処理部４２と、取得部３１と、復号化処理部３２と、ハッシュ値算出部３３と、ハッシュ値比較部３４と、改竄判定部３５と、を有していてもよい。

このような情報処理システムとしては、例えば、撮像画像データを送信した側の情報処理装置（撮像装置）において認証結果等を通知するものが考えられる。

具体的には、撮像装置とされた認証対象端末（スマートフォンなど）と認証処理を行うサーバ装置などによって構成された認証システムがある。

これにより、サーバ装置において不正な認証要求を見分けることができ、不正な認証要求に対して認証をしてしまうことが防止される。

【０２２３】

第４の実施の形態で説明したように、出力制御部４０は、情報処理装置（サーバ装置４）から取得した改竄判定部３５の判定結果を表示出力する制御を行い、認証処理部４２は、改竄判定部３５の判定結果に基づいて認証処理を行ってもよい。

即ち、撮像画像データを送信した装置（撮像装置：ユーザ端末２）において、送信した撮像画像データが改竄されずに受信側装置であるサーバ装置４（情報処理装置）まで届いたか否かをユーザが認識することができる。

これにより、今まさにハッキングを受けている状態であるか否かをユーザが認識できる。

また、サーバ装置４において不正な認証要求（ログイン要求など）を更に見分けやすくすることができ、認証の厳格化を図ることができる。

【０２２４】
第４の実施の形態で説明したように、情報処理装置（サーバ装置４）は、取得した撮像画像データに基づいて被写体の生体情報を抽出するための解析を行う生体解析処理部３６と、生体解析処理部３６の解析結果に基づいて被写体が生体であるか否かを判定する生体判定部３７と、を備え、出力制御部４０は、生体判定部３７の判定結果を表示出力する制御を行い、認証処理部４２は、生体判定部３７の判定結果に基づいて認証処理を行ってもよい。
即ち、改竄判定処理だけでなく、受信した撮像画像データから生体情報の抽出を行い、その抽出結果に基づいて被写体が生体であるか否かの判定処理を行う。
これにより、認証の厳格化が図られ、セキュリティの向上を図ることができる。
【０２２５】
第１及び第３の実施の形態で説明したように、取得した撮像画像データに含まれる被写体の個体特徴量を解析するための個体解析処理部３８と、個体解析処理部３８の解析結果に基づいて被写体についての個体認識可否を判定する個体判定部３９と、改竄の有無についての判定結果と生体であるか否かについての判定結果と個体認識可否についての判定結果に基づいて、取得した撮像画像データが改竄されていないことが担保されていない非担保状態ＳＴ０と、取得した撮像画像データが改竄されていないことが担保された状態である第１担保状態ＳＴ１と、取得した撮像画像データが改竄されていないことが担保され且つ被写体が生体であるとされた状態である第２担保状態ＳＴ２と、取得した撮像画像データが改竄されていないことが担保され被写体が生体であるとされ且つ個体認識が可とされた状態である第３担保状態ＳＴ３と、を判定する状態判定部４１と、を備えていてもよい。
これにより、セキュリティの保証度合いに応じた処理を行うことが可能とされる。
例えば、保証度合いに応じた画像出力を行ってもよいし、保証度合いに応じて機能を制限して利用させることも可能となる。例えば、認証処理を行うサーバ装置においては、第３担保状態ＳＴ３において全機能の利用を許可する処理を行い、第２担保状態ＳＴ２においては一部機能を制限した利用を許可する処理を行うことなどが可能となる。
【０２２６】
第１及び第３の実施の形態で説明したように、非担保状態ＳＴ０、第１担保状態ＳＴ１、第２担保状態ＳＴ２及び第３担保状態ＳＴ３に応じた表示出力を行う出力制御部４０を備えていてもよい。
これにより、ユーザは保証度合いを確認することが可能となる。
例えば、チャットシステムや通話システムなどのようにユーザ間のやりとりが行われるシステムにおいては、保証度合いに応じた操作をユーザが選択することが可能となる。
また、サーバ装置４において表示出力がなされる場合には、管理者等が表示出力に応じた措置を施すことが可能となる。
【０２２７】
第３の実施の形態で説明したように、生体判定部３７は、前記解析の結果得られた前記被写体の生体信号の変化の有無を判定することにより生体であるか否かを判定してもよい。
例えば、複数枚の撮像画像データの解析を行うことにより、生体信号の変化を抽出する。
生体信号の例としては、例えば、眼振の有無、リップシンク、瞳孔反応、スペクトラム分析による心拍検知などである。このような定量的な解析を行うことにより、例えば、人による操作が行われたか否かを判定することができ、詐欺行為や機械による不正アクセス等の防止を図ることができる。
【０２２８】
実施の形態のプログラムは、図９，図１０，図１４から図１８，図２４から図２７の各図に示す処理を、例えば、ＣＰＵ、ＤＳＰ等、或いはこれらを含むデバイスに実行させるプログラムである。
即ち、実施の形態のプログラムは、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画素アレイと、光電変換して得た撮像画像データからハッシュ値を生成するハッシュ値生成部と、ハッシュ値に対する暗号化処理を実行する暗号化

処理部と、を有するアレイセンサから、撮像画像データと暗号化されたハッシュ値を取得する処理を制御部１２に実行させる。
　また、取得した暗号化されたハッシュ値の復号化を行う処理を制御部１２に実行させる。
　更に、取得した撮像画像データからハッシュ値を算出する処理を制御部１２に実行させる。
　更にまた、復号化されたハッシュ値と算出されたハッシュ値を比較する処理を制御部１２に実行させる。
　加えて、ハッシュ値の比較結果に基づいて取得した撮像画像データの改竄の有無を判定する処理を制御部１２に実行させる。
　このようなプログラムにより、上述した情報処理システム１を実現できる。
【０２２９】
　このような情報処理システム１を実現するプログラムはコンピュータ装置等の機器に内蔵されている記録媒体としてのＨＤＤや、ＣＰＵを有するマイクロコンピュータ内のＲＯＭ等に予め記録しておくことができる。
　或いはまた、フレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)、ＭＯ(Magneto Optical)ディスク、ＤＶＤ(Digital Versatile Disc)、ブルーレイディスク（Blu-ray Disc（登録商標））、磁気ディスク、半導体メモリ、メモリカードなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。
　また、このようなプログラムは、リムーバブル記録媒体からパーソナルコンピュータ等にインストールする他、ダウンロードサイトから、ＬＡＮ(Local Area Network)、インターネットなどのネットワークを介してダウンロードすることもできる。
【０２３０】
　またこのようなプログラムによれば、実施の形態の情報処理システム１（或いはそのうちのユーザ端末２）の広範な提供に適している。例えばスマートフォンやタブレット等の携帯端末装置、携帯電話機、パーソナルコンピュータ、ゲーム機器、ビデオ機器、ＰＤＡ（Personal Digital Assistant）等のカメラ機能を備えた機器にプログラムをダウンロードすることで、当該スマートフォン等を、本開示の情報処理システム１（或いはユーザ端末２）として機能させることができる。
【０２３１】
　また、このようなプログラムにより、例えばスマートフォンやタブレット等の携帯端末装置、携帯電話機、パーソナルコンピュータ、ゲーム機器、ビデオ機器、ＰＤＡ等のカメラ機能を備えた機器におけるユーザインタフェース制御を行うことができる。
【０２３２】
　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。
【０２３３】
＜７．本技術＞
　（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画素アレイと、光電変換して得た撮像画像データからハッシュ値を生成するハッシュ値生成部と、前記ハッシュ値に対する暗号化処理を実行する暗号化処理部と、を有するアレイセンサと、
　前記撮像画像データと暗号化された前記ハッシュ値を取得する取得部と、
　前記取得した暗号化されたハッシュ値の復号化を行う復号化処理部と、
　前記取得した撮像画像データからハッシュ値を算出するハッシュ値算出部と、
　前記復号化されたハッシュ値と前記算出されたハッシュ値を比較するハッシュ値比較部と、
　前記ハッシュ値の比較結果に基づいて前記取得した撮像画像データの改竄の有無を判定

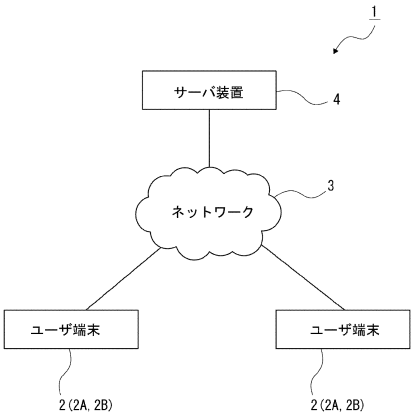
する改竄判定部と、を備えた
情報処理システム。
（２）
前記取得した撮像画像データに基づいて被写体の生体情報を抽出するための解析を行う生体解析処理部と、
前記生体解析処理部の解析結果に基づいて前記被写体が生体であるか否かを判定する生体判定部と、を備えた
上記（１）に記載の情報処理システム。
（３）
前記取得した撮像画像データに含まれる被写体の個体特徴量を解析するための個体解析処理部と、
前記個体解析処理部の解析結果に基づいて前記被写体についての個体認識可否を判定する個体判定部と、を備えた
上記（１）から上記（２）の何れかに記載の情報処理システム。
（４）
前記改竄判定部の判定結果を通知するための出力制御を行う出力制御部を備えた
上記（１）から上記（３）の何れかに記載の情報処理システム。
（５）
前記生体判定部の判定結果を通知するための出力制御を行う出力制御部を備えた
上記（２）に記載の情報処理システム。
（６）
前記個体判定部の判定結果を通知するための出力制御を行う出力制御部を備えた
上記（３）に記載の情報処理システム。
（７）
撮像装置と情報処理装置とを含んで構成され、
前記撮像装置は、前記アレイセンサを有し、
前記情報処理装置は、前記取得部と、前記復号化処理部と、前記ハッシュ値算出部と、前記ハッシュ値比較部と、前記改竄判定部と、前記出力制御部と、を有する
上記（４）に記載の情報処理システム。
（８）
前記出力制御部は、前記取得した撮像画像データを表示出力する制御と、前記取得した撮像画像データについての前記改竄判定部の判定結果を表示出力する制御と、を実行する
上記（７）に記載の情報処理システム。
（９）
前記出力制御部は、前記取得した撮像画像データについての前記改竄判定部の判定結果を表示出力する制御を行う
上記（７）に記載の情報処理システム。
（１０）
前記出力制御部は、
チャット画面を提示する制御と、
チャット参加者が使用する前記撮像装置から受信した参加者の撮像画像データについての前記改竄判定部の判定結果を前記チャット画面においてチャット参加者ごとに表示出力する制御と、を行う
上記（９）に記載の情報処理システム。
（１１）
撮像装置と情報処理装置とを含んで構成され、
前記撮像装置は、前記アレイセンサと、前記出力制御部と、を有し、
前記情報処理装置は、認証処理を行う認証処理部と、前記取得部と、前記復号化処理部と、前記ハッシュ値算出部と、前記ハッシュ値比較部と、前記改竄判定部と、を有する
上記（４）に記載の情報処理システム。

（１２）
前記出力制御部は、前記情報処理装置から取得した前記改竄判定部の判定結果を表示出力する制御を行い、
前記認証処理部は、前記改竄判定部の判定結果に基づいて前記認証処理を行う
上記（１１）に記載の情報処理システム。
（１３）
前記情報処理装置は、
前記取得した撮像画像データに基づいて被写体の生体情報を抽出するための解析を行う生体解析処理部と、
前記生体解析処理部の解析結果に基づいて前記被写体が生体であるか否かを判定する生体判定部と、を備え、
前記出力制御部は、前記生体判定部の判定結果を表示出力する制御を行い、
前記認証処理部は、前記生体判定部の判定結果に基づいて前記認証処理を行う
上記（１２）に記載の情報処理システム。
（１４）
前記取得した撮像画像データに含まれる被写体の個体特徴量を解析するための個体解析処理部と、
前記個体解析処理部の解析結果に基づいて前記被写体についての個体認識可否を判定する個体判定部と、
前記改竄の有無についての判定結果と前記生体であるか否かについての判定結果と前記個体認識可否についての判定結果に基づいて、前記取得した撮像画像データが改竄されていないことが担保されていない非担保状態と、前記取得した撮像画像データが改竄されていないことが担保された状態である第１担保状態と、前記取得した撮像画像データが改竄されていないことが担保され且つ前記被写体が生体であるとされた状態である第２担保状態と、前記取得した撮像画像データが改竄されていないことが担保され前記被写体が生体であるとされ且つ前記個体認識が可とされた状態である第３担保状態と、を判定する状態判定部と、を備えた
上記（２）に記載の情報処理システム。
（１５）
前記非担保状態、前記第１担保状態、前記第２担保状態及び前記第３担保状態に応じた表示出力を行う出力制御部を備えた
上記（１４）に記載の情報処理システム。
（１６）
前記生体判定部は、解析の結果得られた生体信号の変化の有無を判定することにより生体であるか否かを判定する
上記（２）に記載の情報処理システム。
（１７）
前記撮像画像データにおける被写体は生体情報を抽出不可能な被写体とされた
上記（１）に記載の情報処理システム。
（１８）
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画素アレイと、光電変換して得た撮像画像データからハッシュ値を生成するハッシュ値生成部と、前記ハッシュ値に対する暗号化処理を実行する暗号化処理部と、を有するアレイセンサから、前記撮像画像データと暗号化された前記ハッシュ値を取得する処理と、
前記取得した暗号化されたハッシュ値の復号化を行う処理と、
前記取得した撮像画像データからハッシュ値を算出する処理と、
前記復号化されたハッシュ値と前記算出されたハッシュ値を比較する処理と、
前記ハッシュ値の比較結果に基づいて前記取得した撮像画像データの改竄の有無を判定する処理と、を
情報処理装置が実行する情報処理方法。

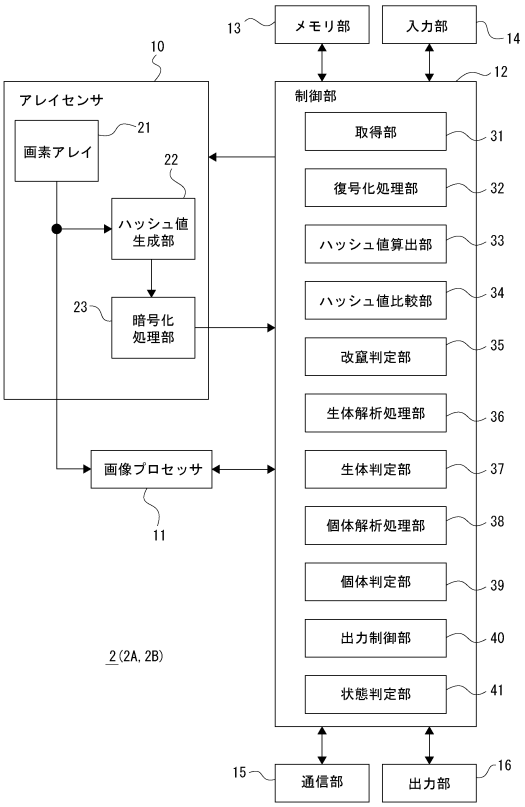
（１９）
可視光又は非可視光の受光素子を有する画素が一次元又は二次元に複数配列された画素アレイと、光電変換して得た撮像画像データからハッシュ値を生成するハッシュ値生成部と、前記ハッシュ値に対する暗号化処理を実行する暗号化処理部と、を有するアレイセンサから、前記撮像画像データと暗号化された前記ハッシュ値を取得する処理と、
前記取得した暗号化されたハッシュ値の復号化を行う処理と、
前記取得した撮像画像データからハッシュ値を算出する処理と、
前記復号化されたハッシュ値と前記算出されたハッシュ値を比較する処理と、
前記ハッシュ値の比較結果に基づいて前記取得した撮像画像データの改竄の有無を判定する処理と、を
情報処理装置に実行させるプログラム。
（２０）
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画素アレイと光電変換して得た撮像画像データからハッシュ値を生成するハッシュ値生成部と前記ハッシュ値に対する暗号化処理を実行する暗号化処理部とを有するアレイセンサから取得した暗号化された前記ハッシュ値を復号化して得られるハッシュ値と、前記アレイセンサから取得した撮像画像データから算出したハッシュ値と、の比較結果に基づいて行われる前記撮像画像データの改竄の有無についての判定処理の結果を通知する
ユーザインタフェース。
【符号の説明】
【０２３４】
１，１Ａ　情報処理システム
２，２Ａ，２Ｂ　ユーザ端末
４　サーバ装置
１０　アレイセンサ
１２　制御部
２１　画素アレイ
２２　ハッシュ値生成部
２３　暗号化処理部
２４　画像暗号化処理部
３１　取得部
３２　復号化処理部
３３　ハッシュ値算出部
３４　ハッシュ値比較部
３５　改竄判定部
３６　生体解析処理部
３７　生体判定部
３８　個体解析処理部
３９　個体判定部
４０　出力制御部
４１　状態判定部
４２　認証処理部

【図面】

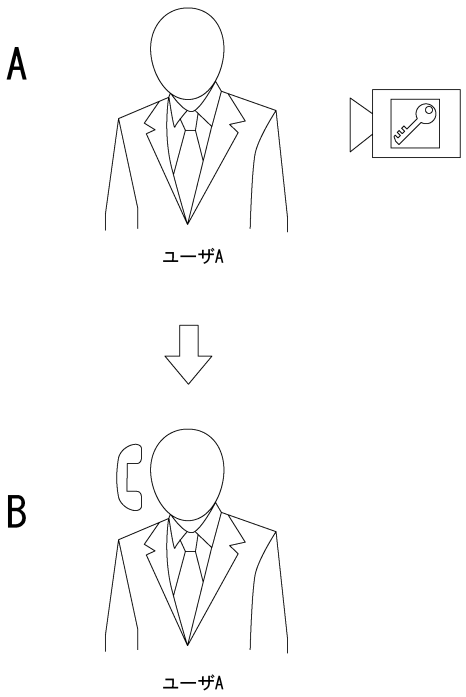
【図１】


1
サーバ装置
4
ネットワーク
3
ユーザ端末
ユーザ端末
2(2A, 2B)
2(2A, 2B)

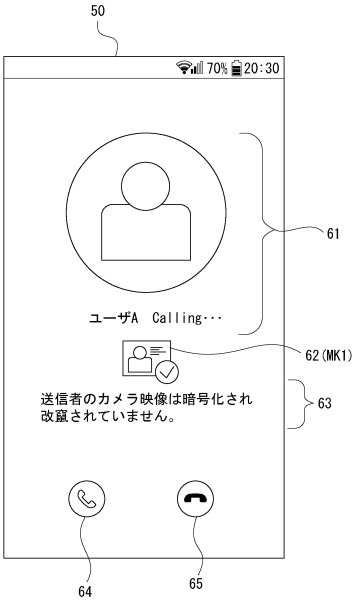
【図２】


13
メモリ部
入力部
14
10
12
アレイセンサ
制御部
21
画素アレイ
取得部
31
22
復号化処理部
32
ハッシュ値
生成部
ハッシュ値算出部
33
ハッシュ値比較部
34
23
暗号化
処理部
改竄判定部
35
生体解析処理部
36
画像プロセッサ
生体判定部
37
11
個体解析処理部
38
個体判定部
39
出力制御部
40
2(2A, 2B)
状態判定部
41
15
通信部
出力部
16

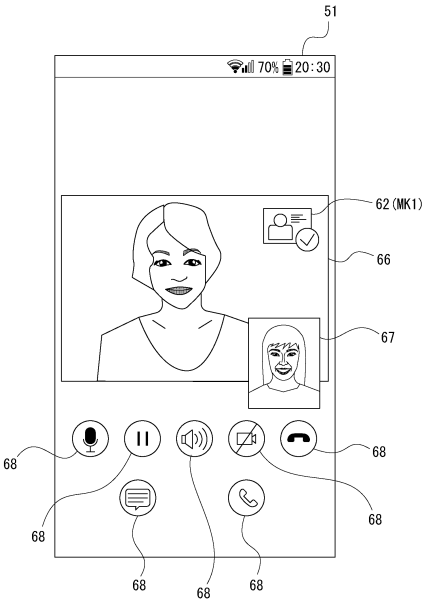
【図３】


A
ユーザA
B
ユーザA

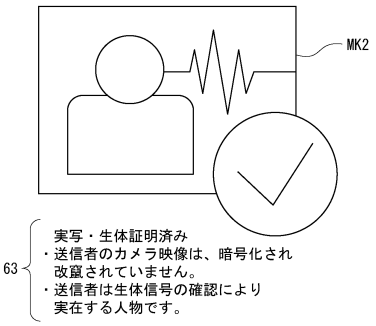
【図４】


50
70% 20:30
61
ユーザA Calling･･･
62(MK1)
送信者のカメラ映像は暗号化され
改竄されていません。
63
64
65

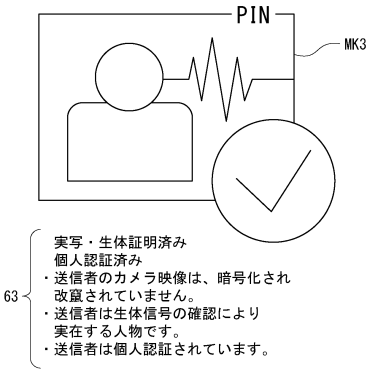
【図５】


51
70%
20:30
62(MK1)
66
67
68
68
68
68
68
68

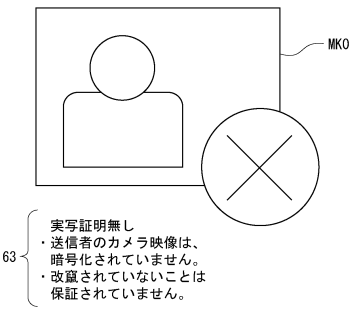
【図６】


MK2
63
実写・生体証明済み
・送信者のカメラ映像は、暗号化され
改竄されていません。
・送信者は生体信号の確認により
実在する人物です。

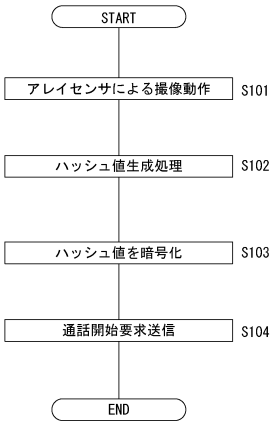
【図７】


PIN
MK3
63
実写・生体証明済み
個人認証済み
・送信者のカメラ映像は、暗号化され
改竄されていません。
・送信者は生体信号の確認により
実在する人物です。
・送信者は個人認証されています。

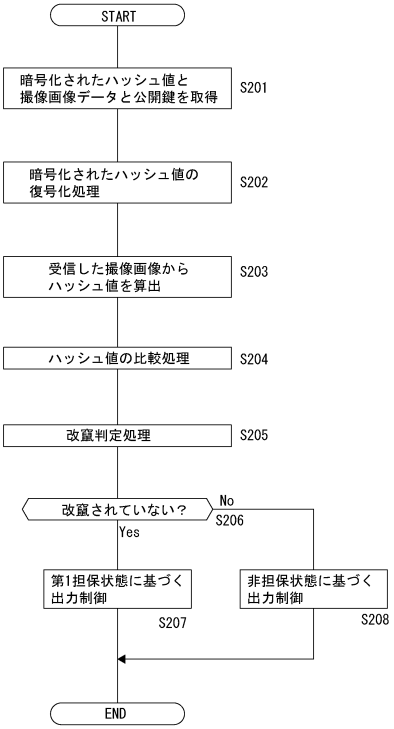
【図８】


MK0
63
実写証明無し
・送信者のカメラ映像は、
暗号化されていません。
・改竄されていないことは
保証されていません。

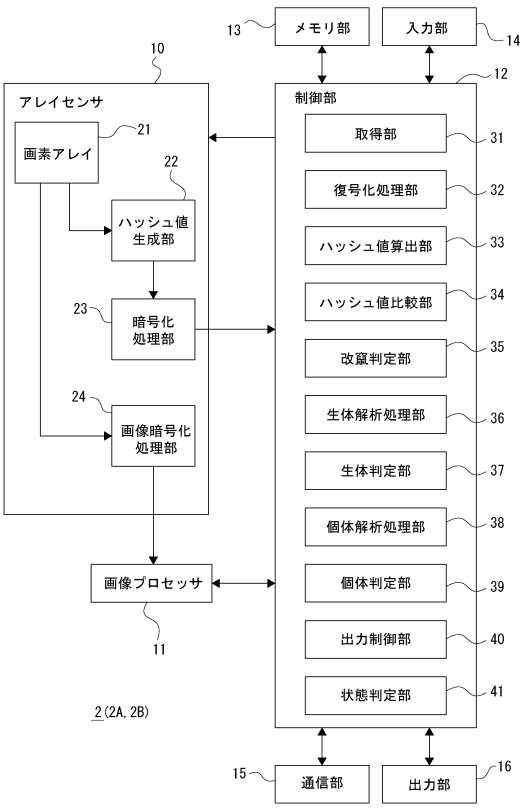
【図９】



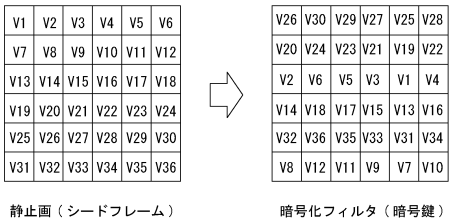
【図１０】



【図１１】



【図１２】



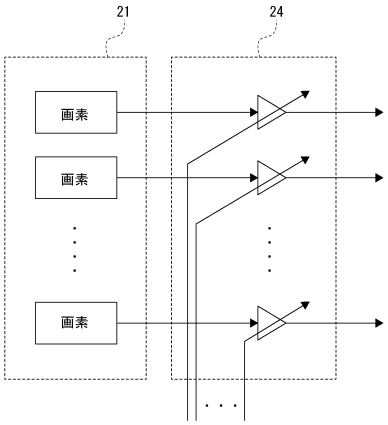
V1	V2	V3	V4	V5	V6
V7	V8	V9	V10	V11	V12
V13	V14	V15	V16	V17	V18
V19	V20	V21	V22	V23	V24
V25	V26	V27	V28	V29	V30
V31	V32	V33	V34	V35	V36

静止画（シードフレーム）

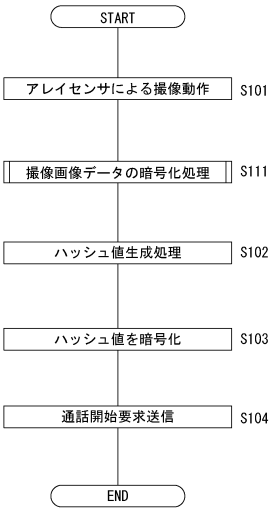
V26	V30	V29	V27	V25	V28
V20	V24	V23	V21	V19	V22
V2	V6	V5	V3	V1	V4
V14	V18	V17	V15	V13	V16
V32	V36	V35	V33	V31	V34
V8	V12	V11	V9	V7	V10

暗号化フィルタ（暗号鍵）

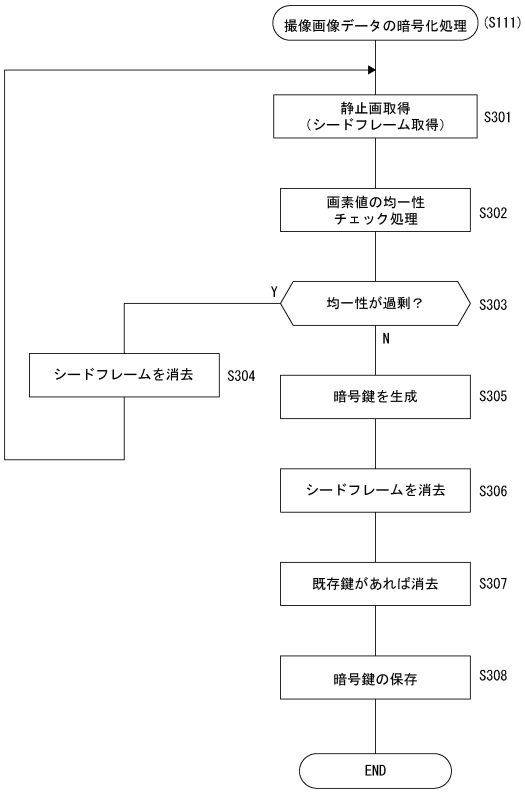
【図１３】



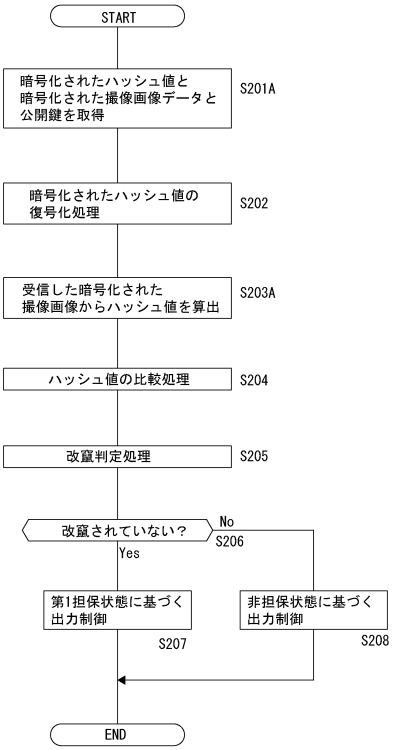
【図１４】



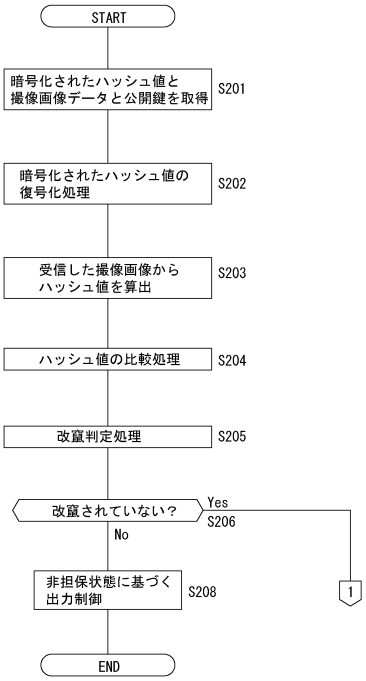
【図１５】



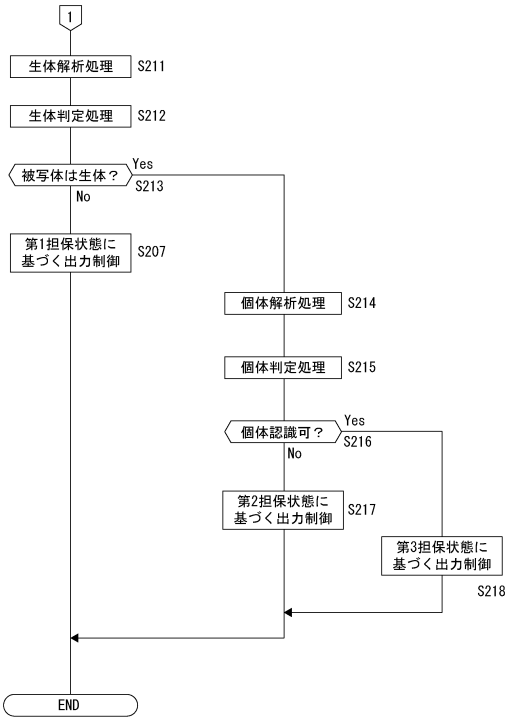
【図１６】



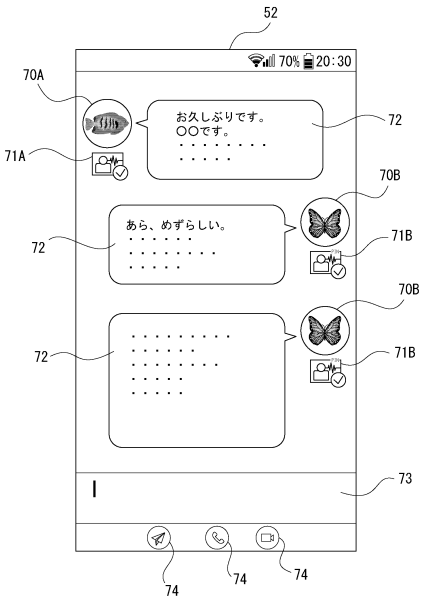
【図１７】



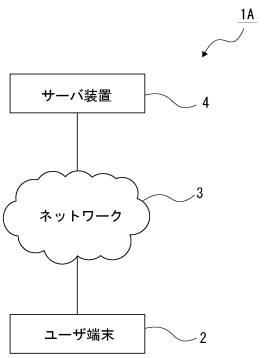
【図１８】



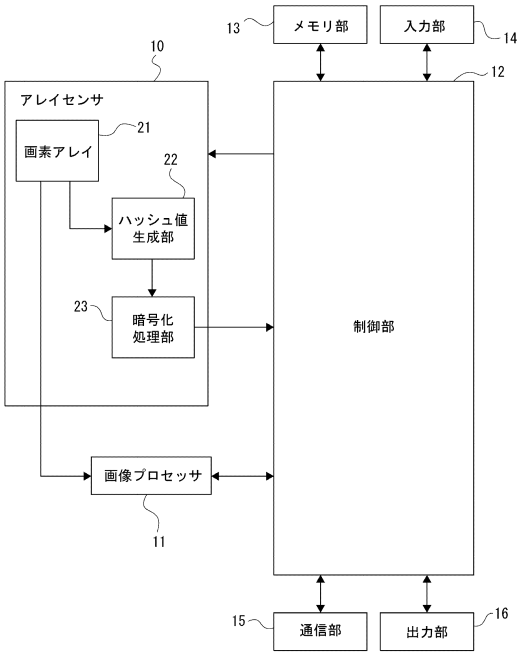
【図１９】



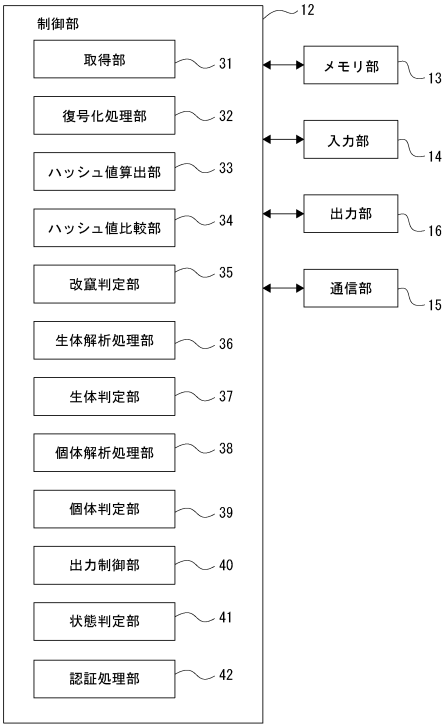
【図２０】



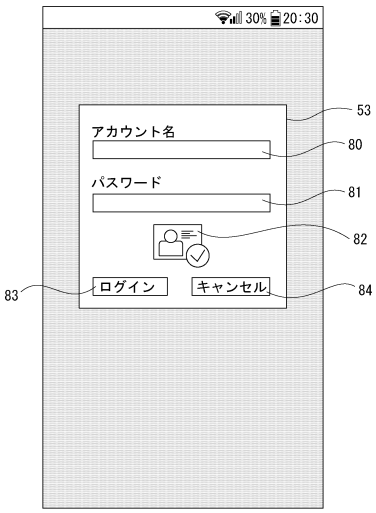
【図２１】



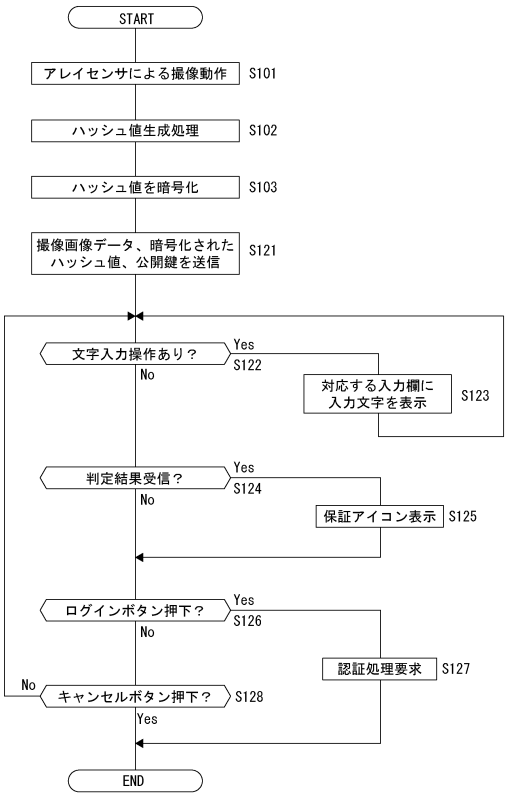
【図２２】



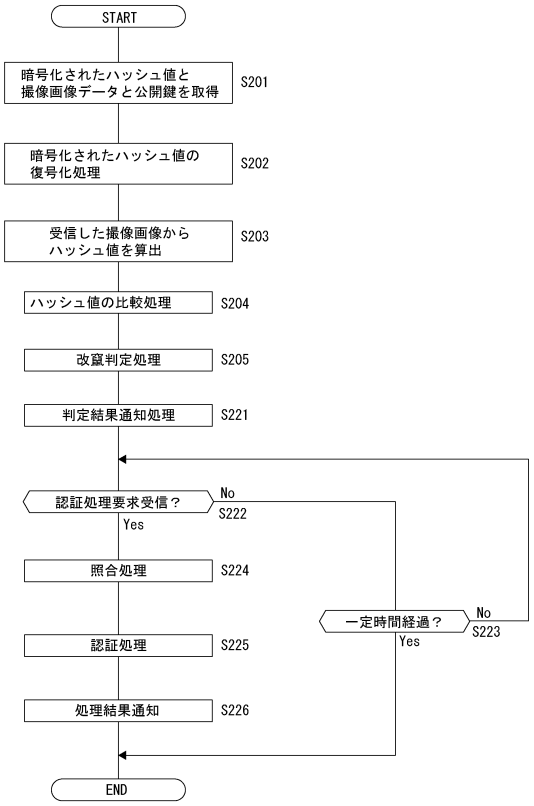
【図２３】



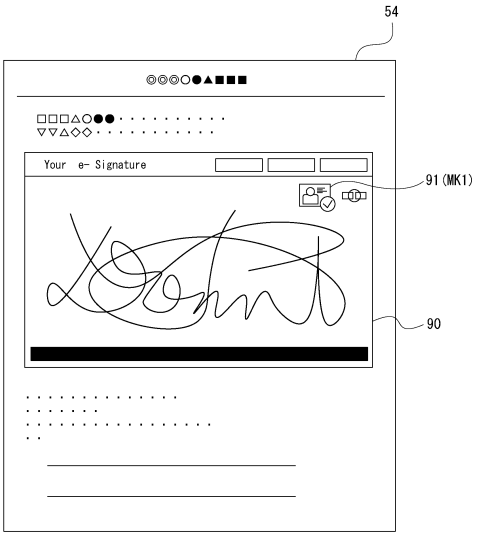
【図２４】



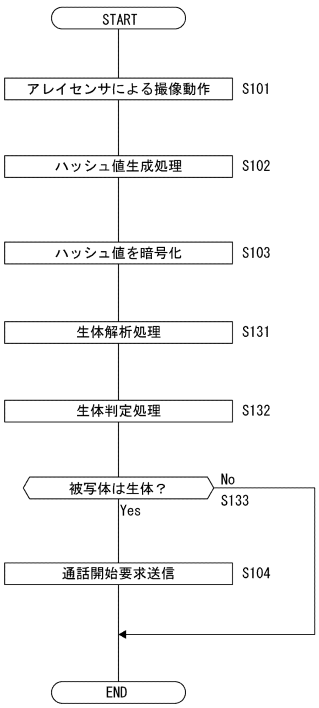
【図２５】



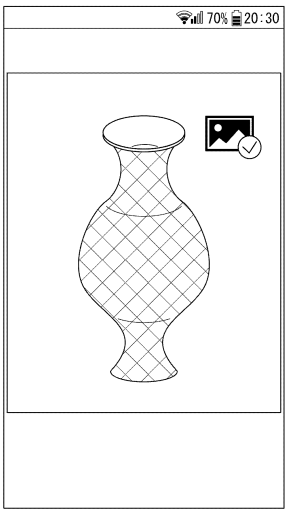
【図２６】



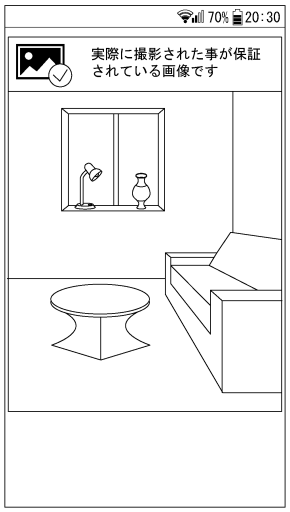
【図２７】



【図２８】



【図２９】



フロントページの続き

審査官　金沢 史明

(56)参考文献　特開２０１７－０８４４３１（ＪＰ，Ａ）
特表２０１５－５２４１１９（ＪＰ，Ａ）
米国特許出願公開第２０１８／００４８４７４（ＵＳ，Ａ１）
特開２０１７－１８４１９８（ＪＰ，Ａ）
特開２０１５－０８２１９５（ＪＰ，Ａ）
国際公開第２０１９／１５１３６８（ＷＯ，Ａ１）
米国特許出願公開第２０１１／０２６７４２２（ＵＳ，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)

Ｈ０４Ｌ　９／３２
Ｇ０６Ｆ　２１／３２
Ｇ０６Ｆ　２１／６４
Ｇ０６Ｔ　７／００