(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7046006号
(P7046006)

(45)発行日　令和4年4月1日(2022.4.1)

(24)登録日　令和4年3月24日(2022.3.24)

(51)国際特許分類
Ｇ０６Ｆ　21/36　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/36

請求項の数　13　（全24頁）

(21)出願番号　特願2018-558116(P2018-558116)
(86)(22)出願日　平成29年4月10日(2017.4.10)
(65)公表番号　特表2019-515394(P2019-515394A)
(43)公表日　令和1年6月6日(2019.6.6)
(86)国際出願番号　PCT/CN2017/079862
(87)国際公開番号　WO2017/190577
(87)国際公開日　平成29年11月9日(2017.11.9)
審査請求日　令和2年3月19日(2020.3.19)
(31)優先権主張番号　201610292695.4
(32)優先日　平成28年5月5日(2016.5.5)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　520015461
アドバンスド ニュー テクノロジーズ カンパニー リミテッド
英国領ケイマン諸島 グランド ケイマン ケーワイ１－９００８ ジョージ タウン ホスピタル ロード ２７ ケイマン コーポレート センター
(74)代理人　100188558
弁理士　飯田 雅人
(74)代理人　100205785
弁理士　▲高▼橋 史生
(72)発明者　スン，シャオカイ
中華人民共和国，浙江省 ３１１１２１，ハンヂョウ，ユ ハンディストリクト，ウェスト ウェン イー ロード ナンバ

最終頁に続く

(54)【発明の名称】　認証方法及びデバイス並びに認証用情報を生成する方法及びデバイス

(57)【特許請求の範囲】
【請求項１】
デバイスによるユーザ認証のための方法であって、
第１のユーザにより事前に指定された画像を表示するステップであって、前記画像は前記第１のユーザによりカスタマイズされたジェスチャパスワード入力インターフェースを備える、ステップ（Ｓ２０１）と；
前記画像についての第２のユーザの対話型操作を検出するステップ（Ｓ２０２）と；
検出した前記第２のユーザの前記対話型操作に基づき、前記第２のユーザの対話型操作情報を生成するステップ（Ｓ２０３）と；
前記第２のユーザが前記第１のユーザであるかどうかを、第２のユーザの対話型操作情報を標準情報と照合することにより特定するために、認証を実行するステップ（Ｓ２０４）と；を備え、
前記標準情報は、前記画像上で前記第1のユーザにより実行される対話型操作に基づき、前もって生成された対話型操作情報であり、
前記標準情報は、前記画像における1つの特徴領域から他の特徴領域へのスライド操作に関する単一のスライド力を含み、前記単一のスライド力は、所定の複数のスライド力のうちの１つに対応する、方法。
【請求項２】
前記画像についての前記第１のユーザの対話型操作に基づいて前記標準情報を生成するステップとして：

前記第１のユーザにより指定された前記画像を取得するステップ（Ｓ３０１）と；
前記画像を表示し、前記画像上で１つ以上の特徴領域を特定するステップ（Ｓ３０２）と；
前記１つ以上の特徴領域への前記第１のユーザの対話型操作を検出するステップ（Ｓ３０３）と；
検出した前記第１のユーザの前記対話型操作に基づいて前記標準情報を生成するステップ（Ｓ３０４）と；を備える、
請求項１に記載の方法。
【請求項３】
前記画像上で前記１つ以上の特徴領域を特定するステップは：
前記画像上で特徴検出を実行し、特徴検出により前記画像上で前記１つ以上の特徴領域を特定するステップ；及び／又は
前記画像上の、前記第１のユーザにより指定された１つ以上の領域を特定し、前記第1のユーザにより指定された前記１つ以上の領域を、前記画像上の前記1つ以上の特徴領域として決定するステップを備える、
請求項２に記載の方法。
【請求項４】
前記第１のユーザにより事前に指定された前記画像を表示するステップの前に、
前記１つ以上の特徴領域に設定を実行するステップを更に備え、前記設定は、前記第１のユーザにより事前に指定された前記画像上で前記１つ以上の特徴領域をマーキングするかどうかを特定するために用いられる、
請求項２に記載の方法。
【請求項５】
前記画像上で１つ以上の特徴領域を特定するステップの後に、
各特徴領域についての対応する識別情報を生成するステップを更に備える、
請求項２に記載の方法。
【請求項６】
検出した前記第１のユーザの前記対話型操作に基づいて前記標準情報を生成する前記ステップは：
検出した前記第１のユーザの前記対話型操作に基づき、前記１つ以上の特徴領域についての前記第１のユーザの操作順序を特定するステップと；
前記操作順序を示すために用いられる特徴領域識別情報シーケンスを、前記１つ以上の特徴領域についての対応する前記操作順序及び識別情報に基づいて生成し、前記特徴領域識別情報シーケンスを前記標準情報として用いるステップと；を備える、
請求項５に記載の方法。
【請求項７】
検出した前記第２のユーザの前記対話型操作に基づいて、前記第２のユーザの前記対話型操作情報を生成するステップは：
前記第２のユーザの前記対話型操作が前記１つ以上の特徴領域についての前記第２のユーザの対話型操作を含む、と特定される場合に、前記１つ以上の特徴領域についての前記第２のユーザの操作順序を、検出された前記第２のユーザの前記対話型操作に基づいて特定するステップと；
前記操作順序を示すために用いられる特徴領域識別情報シーケンスを、前記１つ以上の特徴領域についての対応する前記操作順序及び前記識別情報に基づいて生成し、前記特徴領域識別情報シーケンスを前記第２のユーザの前記対話型操作情報として用いるステップと；を備える、
請求項６に記載の方法。
【請求項８】
前記第２のユーザが前記第１のユーザであるかどうかを前記第２のユーザの前記対話型操作情報を前記標準情報と照合することにより特定するために認証を実行するステップは：
前記第２のユーザの前記対話型操作情報と前記標準情報とが同一であるかどうかを、前記

第２のユーザの前記対話型操作情報を前記標準情報と照合することにより特定するステップと；
肯定である場合に、前記第２のユーザを前記第１のユーザである、と認証するステップと；を備える、
請求項７に記載の方法。
【請求項９】
前記第２のユーザが前記第１のユーザであるかどうかを、前記第２のユーザの前記対話型操作情報を前記標準情報と照合させることにより特定するために前記認証を実行するステップは：
前記第２のユーザの前記対話型操作情報に対応する対話型操作と、前記標準情報に対応する対話型操作とが同一であるかどうかを、前記第２のユーザの前記対話型操作情報を前記標準情報と照合することにより特定し、肯定の場合に、前記第２のユーザを前記第１のユーザとして認証するステップ；又は、
前記第２のユーザの前記対話型操作情報に対応する対話型操作と、前記標準情報に対応する対話型操作との間の類似性が所定の類似性閾値を下回らないかどうかを、前記第２のユーザの前記対話型操作情報を前記標準情報と照合することにより特定し、肯定の場合に、前記第２のユーザを前記第１のユーザとして認証するステップ；を備える、
請求項１乃至請求項８のいずれか１項に記載の方法。
【請求項１０】
前記画像についての前記対話型操作は：
前記画像上での１つ以上の特徴領域へのタップ操作をさらに備える、
請求項１乃至請求項９のいずれか１項に記載の方法。
【請求項１１】
前記タップ操作は、タップ力、タップ時間、タップ回数及びタップ頻度を備える、
請求項１０に記載の方法。
【請求項１２】
前記スライド操作は、スライド力、スライド時間、スライド距離及びスライドトラックを備える、
請求項１０に記載の方法。
【請求項１３】
請求項１乃至請求項１２のいずれか１項に記載の方法を実行するように構成された複数のモジュールを備える、
ユーザ認証のための認証デバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本願は情報セキュリティ技術の分野に関し、特に、認証方法及びデバイス並びに認証用情報を生成する方法及びデバイスに関する。
【背景技術】
【０００２】
情報技術の急速な発展に伴い、ユーザは情報セキュリティにますます注意を払うようになっている。認証は情報セキュリティを確保するための一般的な方法である。
【０００３】
例えば、第１のユーザの端末デバイスが認証を実行する。第１のユーザは認証用の標準情報（例えば、パスワード）を予め決めておくことができる。標準情報が設定された後に、端末デバイスは、標準情報に基づいて端末デバイス上で特定の操作を実行する任意ユーザ（第２のユーザと呼ぶ）に対して認証を実行できる。第２のユーザが標準情報を正確に入力できれば、端末デバイスは第２のユーザを第１のユーザとして認証できる。そうでない場合には、端末デバイスは、第２のユーザが第１のユーザではなく攻撃者であると特定でき、これにより、第２のユーザが特定の操作を実行することを阻止することができる。よ

って、端末デバイス上での第１のユーザの情報セキュリティを向上させることができる。特定の操作とは、画面ロック解除操作、ログイン操作、個人情報変更操作、決済操作等であってよい。

【０００４】

既存の技術において、標準情報はジェスチャパスワードであってよく、ジェスチャパスワードに基づいて認証を実行できる。具体的には、オペレーティングシステム又は端末デバイスのアプリケーションにより提供されるジェスチャパスワード入力インターフェース内には９個の主要ノード領域があり、９個の主要ノード領域は、９個のボックスグリッドの形式に配分されている。これは、図１のジェスチャパスワード入力インターフェースに示す通りである。第１のユーザは、少なくとも２個の主要ノード領域をジェスチャパスワードとして接続する２次元トラックを設定できる。ジェスチャパスワードの設定後、端末デバイスが第２のユーザに対して認証を実行する際に、第２のユーザがジェスチャパスワードに対応するジェスチャを再生するためにジェスチャパスワード入力インターフェース内の主要ノード領域を接続する場合にのみ、第２のユーザが認証され得る。

【０００５】

しかし、既存技術のジェスチャパスワード入力インターフェースは多様化されておらず、攻撃者は、通常は、ジェスチャパスワード入力インターフェースに熟知している。そのため、第１のユーザが入力したジェスチャパスワードを攻撃者が覗き見してこれを控えておく難度は低下する、及び／又は、第１のユーザが設定したジェスチャパスワードを、攻撃者による徹底的な攻撃によってクラッキングする難度が低下する。そのため、認証の信頼性は相対的に低くなる。

【発明の概要】

【０００６】

本願の実施は、既存技術における多様化されていないジェスチャパスワード入力インターフェースにより生じる、認証の信頼性が比較的に低いという問題を軽減する認証方法及びデバイスを提供する。

【０００７】

本願の実施は、認証のための情報を生成する方法及びデバイスを提供する。

【０００８】

以下の技術的解決策は本願の実施において用いられる。

【０００９】

本願の実施で提供される認証方法は：第１のユーザにより事前に指定された画像を表示するステップと；

前記画像についての第２のユーザの対話型操作を検出するステップと；検出した前記第２のユーザの前記対話型操作に基づき、前記第２のユーザの対話型操作情報を生成するステップと；前記第２のユーザが前記第１のユーザであるかどうかを、第２のユーザの対話型操作情報を標準情報と照合することにより特定するために、認証を実行するステップと；を含む。

【００１０】

本願の実施で提供される認証デバイスは：前記第１のユーザにより事前に指定された画像を表示するように構成された表示モジュールと；前記画像についての第２のユーザの対話型操作を検出するように構成された検出モジュールと；検出した前記第２のユーザの前記対話型操作に基づいて、前記第２のユーザの対話型操作情報を生成するように構成された生成モジュールと；前記第２のユーザの前記対話型操作情報を前記標準情報と照合することにより、前記第２のユーザが前記第１のユーザである、と特定するために、認証を実行するように構成された認証モジュールであって、前記標準情報は前記画像についての前記第１のユーザの対話型操作に基づいて生成される、認証モジュールと；を含む。

【００１１】

本願の実施で提供される認証のための情報を生成する方法は：第１のユーザにより指定された画像を取得するステップと；前記画像を表示し、前記画像上で１つ以上の特徴領域を

特定するステップと；前記１つ以上の特徴領域についての前記第１のユーザの対話型操作を検出するステップと；第２のユーザが前記第１のユーザであるかどうかを特定するために認証を実行するべく、検出された前記第１のユーザの前記対話型操作に基づいて標準情報を生成するステップと；を含む。

【００１２】

本願の実施で提供される認証のための情報を生成するデバイスは：第１のユーザにより指定された画像を取得するように構成された取得モジュールと；前記画像を表示し、前記画像上で１つ以上の特徴領域を特定するように構成された表示及び特定モジュールと；１つ以上の特徴領域についての前記第１のユーザの対話型操作を検出するように構成された検出モジュールと；前記第２のユーザが前記第１のユーザであるかどうかを特定するために認証を実行するべく、検出した前記第１のユーザの前記対話型操作に基づいて、標準情報を生成するように構成された生成モジュールと；を含む。

【００１３】

本願の実施で用いられる少なくとも１つの技術的解決策は、以下の有益な効果を奏する。第１のユーザにより指定された画像を、第１のユーザによりカスタマイズされたジェスチャパスワード入力インターフェースとして使用でき、対話型操作はジェスチャを含むことができ、ジェスチャパスワード入力インターフェースを多様化できる。異なる画像に対応するジェスチャパスワード入力インターフェースの特徴領域の位置は、通常は、異なっており、第１のユーザが指定した画像に対応するジェスチャパスワード入力インターフェースの特徴領域の位置も、既存技術のジェスチャパスワード入力インターフェースの特徴領域の位置とは異なる。そのため、攻撃者は画像に対応するジェスチャパスワード入力インターフェースに熟知していない可能性がある。よって、第１のユーザが入力したジェスチャパスワードを攻撃者が覗き見して控えておく難度を高めることができ、及び／又は、第１のユーザが設定したジェスチャパスワードを、攻撃者による徹底的な攻撃によってクラッキングする難度を高めることができ、よって、認証の信頼性を向上させることができる。したがって、本願は、既存技術における問題を部分的又は全面的に軽減することができる。

【図面の簡単な説明】

【００１４】

本明細書中では添付の図面は本願を更に理解するために用いられ、本願の一部を構成する。本願の実施の例及び実施の説明は本願を説明するために用いられ、本願を不適切に制限することはない。図面について以下説明する。

【００１５】

【図１】図１は、既存技術におけるジェスチャパスワード入力インターフェースを示す概略図である。

【００１６】

【図２】図２は、本願の実施に係る、認証方法を示す概略フローチャートである。

【００１７】

【図３】図３は、本願の実施に係る、図２における、標準情報を生成する工程の概略フローチャートである。

【００１８】

【図４】図４は、本願の実施に係る、指定画像の２つの例を示す図である。

【００１９】

【図５】図５は、本願の実施に係る、指定画像上で特定され、マーキングされた特徴領域の概略図である。

【００２０】

【図６】図６は、本願の実施に係る、特徴領域がマーキングされた、又はマーキングされていない場合の指定画像の概略図である。

【００２１】

【図７】図７は、本願の実施に係る、認証のための情報を生成する方法を示す概略フロー

チャートである。
【００２２】
【図８】図８は、本願の実施に係る、実際のアプリケーションシナリオにおける標準情報を生成する工程の詳細な概略フローチャートである。
【００２３】
【図９】図９は、別の既存技術における標準情報入力インターフェースの概略図である。
【００２４】
【図１０】図１０は、本願の実施に係る、認証デバイスを示す概略構造図である。
【００２５】
【図１１】図１１は、本願の実施に係る、認証のための情報を生成するデバイスを示す概略構造図である。
【発明を実施するための形態】
【００２６】
本願の目的、技術的解決策、及び利点を明瞭にするために、本願の特定の実施及び対応する添付の図面を参照しながら、本願の技術的解決策を明瞭且つ完全に以下説明する。記載された実施は本願の全ての実施ではなく、むしろその一例であることは明白である。当業者が創造的な努力なく本願の実施に基づいて得た全ての他の実施は、本願の保護範囲に含まれる。
【００２７】
本願の解決策は認証に用いることができる。例えば、第２のユーザが特定の操作を実行する場合に第２のユーザ（つまり、認証対象のユーザ）に対する認証を実行するために用いることができる。特定の操作とは、スクリーンロック解除操作、ログイン操作、個人情報変更操作、決済操作等であってよい。本願の解決策は既存技術における問題を部分的又は全面的に軽減することができ、この本願の解決策を以下説明する。
【００２８】
図２は、本願の実施に係る認証方法を示す概略フローチャートである。この手順は認証関連のデバイスにより実行できる。このデバイスとして、モバイルフォン、タブレット、スマートウォッチ、車両モバイルシステム、パーソナルコンピュータ、大型又は中型コンピュータ、コンピュータクラスタ等が挙げられるが、これらに限定されない。本願は、実行主体によって制限されることはない。
【００２９】
図２の手順は以下のステップを含んでよい。
【００３０】
Ｓ２０１：第１のユーザにより事前に指定された画像を表示する。
【００３１】
説明を容易にするために、ステップＳ２０１で第１のユーザにより事前に指定された画像は以下の特定の画像として参照できる。
【００３２】
本願のこの実施では、図２の手順を実行する前に、認証に用いる標準情報を、第１のユーザの操作に基づいて事前に生成できる。図２の手順では、この標準情報に基づいて第２のユーザに対して認証を実行する。実際には、第２のユーザは第１のユーザであってよく、第２のユーザは第１のユーザ以外のユーザ、例えば攻撃者、であってよい。図２の手順での認証により、第２のユーザが第１のユーザであるかどうかを特定できる。
【００３３】
本願のこの実施では、標準情報を指定画像に基づいて生成でき、この指定画像は第１のユーザによって指定される。例えば、第１のユーザは、事前にローカル又はクラウドに指定画像として格納された画像を指定画像として指定できる、又は、指定の方法で取得した新たな画像を指定画像として指定できる。例えば、カメラを有する実行主体が画像を撮影し、その画像を指定画像として指定できる。
【００３４】

Ｓ２０２：画像についての第２のユーザの対話型操作を検出する。
【００３５】
本願のこの実施では、ステップＳ２０２で、画像上の任意の領域についての第２のユーザの対話型（インタラクティブ）操作を検出できる、又は、画像上の１つ以上の特徴領域のみについての第２のユーザの対話型操作を検出できる。
【００３６】
Ｓ２０３：検出した第２のユーザの対話型操作に基づいて第２のユーザの対話型操作情報を生成する。
【００３７】
本願のこの実施において、対話型操作はタップ、スライド、プレスのような１つ以上の操作であってよく、対話型操作情報は対話型操作情報に対応する対話型操作内容を反映できる。
【００３８】
上に挙げた操作は対話型操作の単なる例に過ぎず、対話型操作はこれらの操作以外の操作であってよい点は特に留意すべきである。タップ、スライド、プレスのような操作を更に分割することで、対話型操作内容をより特定された特徴を用いて記述できる（対話型操作内容がより特異になる）。例えば、タップ操作はタップ力、タップ時刻、タップ回数、タップ頻度のような特徴に基づいて更に分割でき、スライド操作はスライドトラック、スライド時刻、スライド力、スライド距離のような特徴に基づいて更に分割でき、プレス操作はプレス時刻、プレス力のような特徴に基づいて更に分割できる。
【００３９】
本願では、対話型操作内容の特異性レベルは限定されない。概して、対話型操作内容がより特異であるほど、生成される対応の対話型操作情報もより特異となり、この対話型操作情報に基づいてより厳格な認証も実行できる。対話型操作内容の特異性レベルは、実際の必要性に応じて事前に指定できる。
【００４０】
例えば、対話型操作はタップ操作である。指定された特異性レベルが比較的低い場合にはタップ回数のみ検出できるが、タップ力やタップ時刻は検出されない。指定された特異性レベルが比較的高い場合には、タップ回数、タップ力、タップ時刻等を検出できる。
【００４１】
別の例として、対話型操作はスライド操作である。指定された特異性レベルが比較的低い場合には、スライドトラックのみ検出できるが、スライド時刻やスライド力は検出されない。指定された特異性レベルが比較的高い場合には、スライドトラック、スライド時刻、スライド力等を検出できる。
【００４２】
Ｓ２０４：第２のユーザの対話型操作情報を標準情報と照合することにより、第２のユーザが第１のユーザであるかどうかを特定するための認証を実行する。ここで、標準情報は画像についての第１ユーザの対話型操作に基づいて生成される。
【００４３】
本願のこの実施では、上で述べたように、認証に用いる標準情報を前もって生成した後、第２のユーザに認証を実行する必要があるときに（ステップＳ２０１に対応）、標準情報を生成するための画像（つまり指定画像）を表示できる。第２のユーザは、表示された指定画像についての標準情報に対応する対話型操作を再生するときに限って認証されることができる（ステップＳ２０２～Ｓ２０４に対応）。標準情報に対応する対話型操作は、標準情報を生成するために用いられる画像についての第１のユーザの対話型操作である。
【００４４】
例えば、第１のユーザによるジェスチャパスワード入力インターフェースとして指定画像を用いることができる。この場合、指定画像の１つ以上の特徴領域への第１のユーザの対話型操作をジェスチャとしてみなすことができ、指定された標準情報をジェスチャパスワードとしてみなすことができる。認証中、指定画像を表示でき、第１のユーザのジェスチ

ャを再生するために第２のユーザが指定画像上の１つ以上の特徴領域について対話型操作を実行する場合に限って、第２のユーザを認証できる。

【００４５】

本願のこの実施では、第２のユーザの対話型操作情報が指定画像についての第２のユーザの対話型操作内容を反映でき、また、標準情報が指定画像についての第１のユーザの対話型操作内容を反映できることが、先の記載から分かる。したがって、第２のユーザの対話型操作情報を標準情報と照合することにより、第２のユーザが第１のユーザの操作を再生したかどうかを特定して第２のユーザが第１のユーザであるかどうかを、認証を通じて更に特定できる。

【００４６】

第２のユーザの対話型操作を検出するために用いる具体的な検出方法は、通常、標準情報の生成中に第１のユーザの対話型操作を検出するために用いる具体的な検出方法と同一又は類似する点は特に留意すべきである（そうでなければ、第２のユーザの対話型操作情報と標準情報とを照合することは不適切である。これは、第２のユーザの対話型操作情報と標準情報との間の比較可能性が比較的低いためである）。よって、第２のユーザの対話型操作情報と標準情報とを照合することができ、対話型操作情報照合に基づいて認証を実行する方法の信頼性は、本願においてより高くなる。

【００４７】

先に述べた方法に基づけば、第１のユーザが指定した画像を、第１のユーザによりカスタマイズされたジェスチャパスワード入力インターフェースとして用いることができ、また、対話型操作はジェスチャを含むことで、ジェスチャパスワード入力インターフェースを多様化させることができる。異なる画像に対応するジェスチャパスワード入力インターフェースの特徴領域位置は、通常は、異なっており、また、第１のユーザが指定した画像に対応するジェスチャパスワード入力インターフェースの特徴領域位置は、既存技術におけるジェスチャパスワード入力インターフェースの特徴領域位置とも異なる。そのため、攻撃者は画像に対応するジェスチャパスワード入力インターフェースに熟知してはいない可能性がある。よって、第１のユーザが入力したジェスチャパスワードを攻撃者が覗き見して控えておく難度を高め、及び／又は、第１のユーザが設定したジェスチャパスワードを攻撃者が徹底的に攻撃してクラッキングする難度を高めることができるので、認証の信頼性は向上する。したがって、本願は既存技術の問題を部分的又は全面的に軽減できる。

【００４８】

加えて、本方法には既存技術と比べて多くの利点がある。具体的には、既存技術におけるジェスチャは対応する操作タイプの数が比較的少なく、特異性レベルも比較的低く、通常含まれる操作はスライド操作のみである。生成される対応のジェスチャ情報は、通常は、スライドトラックのみを記述するが、スライド時刻、スライド力、又はその他の特徴情報は記述しない。既存技術におけるジェスチャ（スライド操作）に加えて、本願の対話型操作はより多くの操作タイプ（例えば、タップ操作やプレス操作）を含むことができる。含まれる操作タイプについては、特異性レベルを、これらの操作を介して生成される対話型操作内容についてカスタマイズすることができるため、生成される対話型操作情報が（既存技術のジェスチャ情報と比較して）より特異なものとなる。したがって、認証がより厳格となり、第１のユーザの情報セキュリティが向上する。

【００４９】

加えて、先に述べた方法に基づくと、ユーザは既存技術の特異なジェスチャパスワード入力インターフェースを使用しないことを選択できるが、ユーザの好みの画像を自由に選択して、対応するジェスチャパスワード入力インターフェースを生成できる。そのため、ジェスチャパスワード入力インターフェースのより好ましいカスタマイズを行うことができ、ユーザエクスペリエンスを向上させることができる。

【００５０】

図２の手順におけるステップは１つのデバイスにより実行できる、又は、異なる複数のデバイスにより実行できることは特に留意すべき事項である。例えば、ステップ２０１をデ

バイス１によって実行し、ステップ２０２～２０４をデバイス２によって実行できる；又は、ステップ２０１～２０３をデバイス１によって実行し、ステップ２０４をデバイス２によって実行できる。

【００５１】

先に述べた方法に基づけば、本願のこの実施は、認証方法のいくつかの具体的な実施解決策及び拡張された解決策をさらに提供し、これらについて以下述べる。

【００５２】

本願のこの実施では、上で述べたように、図２の標準情報を、画像についての第１のユーザの対話型操作に基づいて生成できる。理解を容易にするために、図３に示すように、図２の標準情報を生成する手順について以下述べる。

【００５３】

図３は、本願の実施に係る、図２の標準情報を生成するステップの概略的なフローチャートである。図３の手順の実行主体と図２の手順の実行主体とは、同一のデバイスであっても別々のデバイスであってもよい。

【００５４】

図３の手順は以下のステップを含んでよい。

【００５５】

Ｓ３０１：第１のユーザにより指定された画像（つまり、指定画像）を取得する。

【００５６】

本願のこの実施では、指定画像の内容及び形式等の関連情報は限定されない。本願のこの実施では、図４に示す指定画像の２つの実施例を提供する。

【００５７】

図４は本願における指定画像の２つの例を示し、同図の左側は犬の画像、右側は猫の画像をそれぞれ示す。説明を容易にするために、以下の実施も図４の指定画像の実施例に基づいて述べる。

【００５８】

Ｓ３０２：画像を表示し、画像上の１つ以上の特徴領域を特定する。

【００５９】

本願のこの実施では、指定画像上の１つ以上の特徴領域を特定するために、指定画像特徴領域検出アルゴリズムに基づいて指定画像に対して特徴検出を実行できる。特徴領域は実行主体により又は第１のユーザにより指定され得る。この特徴領域の特定方法に基づけば、ユーザ操作やユーザの介入が減り、本願の解決策の自動化の程度が向上する。

【００６０】

本願において画像特徴領域検出アルゴリズムは限定されないが、ここでは、いくつかのアルゴリズムの例が挙げられる。画像特徴領域検出アルゴリズムは、スケール不変の特徴変換（ＳＩＦＴ）アルゴリズム、頑健な特徴量の高速化（ＳＵＲＦ）アルゴリズム、加速化断片試験による特徴抽出（ＦＡＳＴ）アルゴリズム、方向付きＦＡＳＴ及び回転ＢＲＩＥＦ（ＯＲＢ）アルゴリズム、ハリスアルゴリズム、二値特徴量不変スケール可能なキーポイント（ＢＲＩＳＫ）アルゴリズム等であってよい。種々の画像特徴領域検出アルゴリズムは種々の特徴に注目できるため、種々の画像特徴領域検出アルゴリズムを用いて検出できる特徴領域も多様であってよい。例えば、指定画像上の円形領域を、通常は、ＳＵＲＦアルゴリズムを用いて検出して、特徴領域として使用でき；指定画像上の角度領域を、通常は、ハリスアルゴリズムを用いて検出して、特徴領域として使用できる。本願の解決策の実施中に、実際の必要に応じて、１つ以上の画像特徴領域検出アルゴリズムを指定画像特徴領域検出アルゴリズムとして選択できる。

【００６１】

特定できる特徴領域の数は指定画像によって異なってもよい点は特に留意すべき事項である。過剰な数の特徴領域がある（例えば、１つの指定画像上に１ダース又は数ダースの特徴領域が特定される）場合には、以降の操作を容易に実行できない。特徴領域が少ない（例えば、指定画像上に特徴領域が１個か２個のみしか特定されない）場合には、認証を予

期したほど厳格に実行できない。この問題を軽減するために、特定される特徴領域の数、又は認証に用いられる特徴領域の数を限定できる。例えば、各指定画像上で第１のユーザにより特定される特徴領域の数を９個又は他の値に限定できる。限定された数を超えた場合にはいくつかの特徴領域を除去でき、限定された数に届かない場合にはいくつかの特徴領域を追加できる。こうして、特徴領域の数を適切な数にできる。

【００６２】

本願のこの実施では、特徴領域を指定画像特徴領域検出アルゴリズムに基づかずに第１のユーザが指定画像上で１つ以上の領域を特徴領域として特定することもできる。この特徴領域特定方法には以下の利点がある。すなわち、第１のユーザは特徴領域を比較的強くコントロールでき、また、特徴領域が第１のユーザによって指定されているので、第１のユーザは特徴領域をより容易に控えておくことができる。

【００６３】

先述の特徴領域を特定する方法の分析から分かることは、本願のこの実施において、ステップＳ３０２における画像上で１つ以上の特徴領域を特定するステップは：画像上で特徴検出を実行し、この特徴検出により指定画像上で１つ以上の特徴領域を特定するステップ；及び／又は、指定画像上で第１のユーザにより指定された１つ以上の領域を特定し、この１つ以上の領域を特徴領域として用いるステップと；を含むことができる。

【００６４】

本願のこの実施では、特徴領域が特定された後に、表示された指定画像上で、特定された特徴領域をマーキングすることもでき、これにより、第１のユーザは特定された特徴領域を知得でき、特徴領域についての対話型操作を実行できるようになる。マーキングはテキスト及び／又は図形及び／又は色等の形態で実行でき、マーキングを用いて、マーキングに対応する領域が特徴領域であることを示すことができる。

【００６５】

本願のこの実施は、図５に示すように、指定画像上で特定及びマーキングされた特徴領域の概略図を提供する。図４の指定画像を１つの実施例として用いる。

【００６６】

図５では、指定画像上で特定された各特徴領域は、円形の図形を用いてマーキングされている。図５の左側の指定画像上には５個の特徴領域がマーキングされており、図５右側の指定画像上には３個の特徴領域がマーキングされている。

【００６７】

Ｓ３０３：１つ以上の特徴領域についての第１のユーザの対話型操作を検出する。

【００６８】

Ｓ３０４：検出された第１のユーザの対話型操作に基づいて標準情報を生成する。

【００６９】

本願のこの実施では、標準情報を生成した後に、所定の条件が満たされると、認証手順がトリガされ得る。実際には、認証の厳格性を調整するために、認証前（例えば、ステップＳ２０１の実行前）に、１つ以上の特徴領域に設定を実行することができる。この設定を用いて、第１のユーザにより事前に指定された表示画像上の１つ以上の特徴領域をマーキングするかどうかを特定する。

【００７０】

この設定により、認証中に表示された指定画像上で特徴領域がマーキングされると、第２のユーザはマーキングによって指定画像上の特徴領域を直接知得できるため、特徴領域への第１のユーザの対話型操作を第２のユーザが再生する上での助けとなる。そのため、認証の厳格性は比較的低い。

【００７１】

設定により、認証中に表示される指定画像上で特徴領域がマーキングされていなければ、第２のユーザは指定画像上の特徴領域を直接知得することができない。第２のユーザが第１のユーザでない場合、第２のユーザが指定画像上の特徴領域を特定することはほぼできないため、特徴領域への対話型操作の再生はほぼ不可能である。よって、認証の厳格性は

比較的高くなり、第１のユーザの情報セキュリティが向上する。
【００７２】
本願のこの実施は、図６に示すように、特徴領域がマーキングされた場合とマーキングされない場合との指定画像の概略図を提供する。図４の左側の指定画像を実施例として用いる。
【００７３】
図６において、同図の左側は、マーキングされた特徴領域を有する指定画像の概略図であり、同図の右側は、マーキングされていない特徴領域を有する指定画像の概略図である。
【００７４】
本願のこの実施では、上述したように、対話型操作情報は対応する対話型操作内容を反映でき、この反映は複数の具体的な方法によって実施できる。以下に、２つの具体的な方法を実施例として挙げる。
【００７５】
具体的な方法１：指定画像上の特徴領域への操作順序は、対話型操作内容の一部であってよい。対話型操作情報は、対応する対話型操作内容のみを反映できる。
【００７６】
この場合、操作順序の表示を容易にするために、指定画像上で１つ以上の特徴領域が特定された後に、各特徴領域について対応する識別情報を更に生成できる。識別情報を用いて、指定画像上で識別情報に対応する特徴領域を一意に特定できる。例えば、識別情報は、識別情報に対応する特徴領域の座標情報であってもよく、識別情報に対応する特徴領域の座標情報に一意に対応する数字や文字（ｌｅｔｔｅｒｓ）等の文字（ｃｈａｒａｃｔｅｒｓ）又は文字列であってもよい。
【００７７】
標準情報の生成中に、ステップＳ３０４における検出された第１のユーザの対話型操作に基づいて標準情報を生成するステップは、検出された第１のユーザの対話型操作に基づいて１つ以上の特徴領域への第１のユーザの操作順序を特定するステップと；操作順序と、１つ以上の特徴領域に対応する識別情報とに基づいて操作順序を示すために用いられる特徴領域識別情報シーケンスを生成し、この特徴領域識別情報シーケンスを標準情報として使用するステップと；を含むことができる。
【００７８】
例えば、指定画像上で３個の特徴領域を特定し、３個の特徴領域に対応する識別情報（それぞれ「１」、「２」、「３」）を生成すると仮定する。３個の特徴領域へのユーザの対話型操作は、３個の特徴領域への連続したタップ操作の実行であると仮定する。この場合、３個の特徴領域への第１のユーザの操作順序は、第１の特徴領域、第２の特徴領域、第３の特徴領域である。操作シーケンスは特徴領域の識別情報を用いて表されるため、特徴領域識別情報シーケンス「１，２，３」又は「１２３」が生成され、標準情報として用いられる。この実施例での「１，２，３」と「１２３」は特徴領域識別情報シーケンスの例であり、限定にはならない点は特に留意すべき事項である。実際には、特徴領域識別情報シーケンスが特徴領域への第１のユーザの操作順序を示す場合には、特徴領域識別情報シーケンスはデジタルシーケンス以外の形態で表せる。
【００７９】
これに対応して、認証中に、具体的な方法１を用いて第２のユーザの対話型操作情報も生成できる。ステップ２０３における検出された第２のユーザの対話型操作に基づき第２のユーザの対話型操作情報を生成するステップは、第２のユーザの対話型操作が１つ以上の特徴領域への第２のユーザの対話型操作を含むと特定された場合に、１つ以上の特徴領域への第２のユーザの操作順序を検出した第２のユーザの対話型操作に基づいて特定するステップと；１つ以上の特徴領域に対応する操作順序と識別情報とに基づいて、操作順序を示すために用いられる特徴領域識別情報シーケンスを生成し、この特徴領域識別情報シーケンスを第２のユーザの対話型操作情報として用いるステップと；を含むことができる。
【００８０】

具体的な方法２：操作順序に加えて、対話型操作情報は更に具体的な対話型操作内容を反映できる。例えば、対話型操作がスライド操作である場合、操作順序（つまり、スライドトラック）を反映できるだけでなく、スライド力も反映させることができる。

【００８１】

標準情報の生成中に、ステップＳ３０４における検出された第１のユーザの対話情報に基づく標準情報を生成するステップは、１つ以上の特徴領域への第１のユーザの操作順序と、１つ以上の特徴領域の操作特徴表現値とを、検出された第１のユーザの対話型操作に基づいて特定するステップであって、ここで、操作特徴表現値は、操作特徴表現値に対応する特徴領域への対話型操作を第１のユーザが実行するときに操作特徴を表すために用いられる、１つ以上の特徴領域への第１のユーザの操作順序と、１つ以上の特徴領域の操作特徴表現値とを、検出された第１のユーザの対話型操作に基づいて特定するステップと；操作順序及び操作順序に基づく操作特徴と、１つ以上の特徴領域に対応する識別情報と、１つ以上の特徴領域の操作特徴表現値とを示すために用いられる特徴領域識別情報及び操作特徴表現値シーケンスを生成し、特徴領域識別情報及び操作特徴表現値シーケンスを標準情報として用いるステップと；を含むことができる。

【００８２】

例えば、指定画像上で３個の特徴領域を特定し、この３個の特徴領域に対応する識別情報（それぞれ、数字「１」、「２」、「３」）を生成する。３個の特徴領域へのユーザの対話型操作が、第１の特徴領域から第２の特徴領域へスライドを実行し、次に、第２の特徴領域から第３の特徴領域へスライドを実行する操作であると仮定する。この場合、３個の特徴領域への第１のユーザの操作順序は、第１の特徴領域、第２の特徴領域、第３の特徴領域である。さらに、操作特徴がスライド力であり、スライド力は力毎に「Ａ」と「Ｂ」に分類されると仮定する。この場合には、操作特徴表現値は「Ａ」又は「Ｂ」であってよい。

【００８３】

第１の特徴領域から第２の特徴領域へのスライドを実行する第１のユーザのスライド力は「Ａ」であり、第２の特徴領域から第３の特徴領域へのスライドを実行する第１のユーザのスライド力は「Ｂ」であると仮定する。この場合、特徴領域識別情報及び操作特徴表現値のシーケンスを生成し、標準情報「１，Ａ，２，Ｂ，３」又は「１Ａ２Ｂ３」として用いることができる。この実施例での「１，Ａ，２，Ｂ，３」と「１Ａ２Ｂ３」は、特徴領域識別情報及び操作特徴表現値のシーケンスの例であり、限定として解釈されない。実際には、特徴領域識別情報及び操作特徴表現値のシーケンスが特徴領域への第１のユーザの操作順序と操作特徴を示すことができる場合には、特徴領域識別情報及び操作特徴表現値のシーケンスはデジタル文字シーケンス以外で表せる。

【００８４】

これに対応して、認証中、具体的な方法２を、第２のユーザの対話型操作情報を生成するためにも用いることができる。ここでは簡略化のためにその詳細を省く。

【００８５】

本願のこの実施では、標準情報の生成中に、第１のユーザが誤操作をしてしまうことを防止するために、通常、第１のユーザは、生成された標準操作に対する操作を再確認できる（標準情報の二重確認と呼ばれる）。具体的には、標準情報を再生成して、過去に生成された標準情報と比較できる。その比較結果が、これらが同一である、という結果であった場合、生成された標準情報は認証に使用可能である、と特定される。

【００８６】

先に述べた標準情報の生成の説明に基づき、本願の実施は認証のための情報を生成する方法を提供する。標準情報は情報を生成する方法を実行することにより生成でき、図７に、この情報生成方法の手順を示す。

【００８７】

図７の手順は以下のステップを含むことができる。

【００８８】

Ｓ７０１：第１のユーザにより指定された画像を取得する。
【００８９】
Ｓ７０２：画像を表示し、画像上で１つ以上の特徴領域を特定する。
【００９０】
Ｓ７０３：１つ以上の特徴領域への第１のユーザの対話型操作を検出する。
【００９１】
Ｓ７０４：第２のユーザが第１のユーザであるかどうかを特定するために認証を実行するべく、検出された第１のユーザの対話型操作に基づいて標準情報を生成する。
【００９２】
本願のこの実施では、ステップＳ７０２における画像上で１つ以上の特徴領域を特定するステップは、画像上で特徴検出を実行し、この特徴検出により指定画像上で１つ以上の特徴領域を特定するステップと；及び／又は、指定画像上で第１のユーザにより指定された１つ以上の領域を特定し、この１つ以上の領域を特徴領域として用いるステップと；を含むことができる。
【００９３】
更に、図７の手順、及び先に説明した標準情報の生成に関連する拡張解決策に基づき、本願の実施は、図８に示す実際のアプリケーション（適用）シナリオにおいて標準情報を生成する詳細な概略フローチャートを更に提供する。実際のアプリケーションシナリオでは、対話型操作はタップ操作である。
【００９４】
図８の手順は以下のステップを含むことができる。
【００９５】
Ｓ８０１：第１のユーザによりアップロードされたカスタマイズ画像を受信する。
【００９６】
Ｓ８０２：第１のユーザにより指定された画像特徴検出アルゴリズムを特定し、この画像特徴検出アルゴリズムに基づき、受信した画像上で複数の特徴領域を特定する。
【００９７】
Ｓ８０３：画像を表示し、特徴領域をマーキングし、この特徴領域に対応する識別情報を生成する。
【００９８】
Ｓ８０４：特徴領域への第１のユーザのタップ操作を検出する。
【００９９】
Ｓ８０５：特徴領域の識別情報と、タップ順序とに基づいて、検出された特徴領域への第１のユーザのタップ順序を示すために用いられる特徴領域識別情報シーケンスを生成し、この特徴領域識別情報シーケンスを標準情報として用いる。
【０１００】
Ｓ８０６：標準情報についての第１のユーザの二重確認を受信する。
【０１０１】
Ｓ８０７：標準情報認証中に、表示された画像上の特徴領域をマーキングするかどうかを、第１のユーザの指示に基づいて特定する。
【０１０２】
本願のこの実施では、過去のシーケンス形式の標準情報と第２のユーザの対話型操作情報とが同一である場合、第２のユーザは第１のユーザの対話型操作を再生した、と通常は特定できる。この場合、ステップ２０４における、第２のユーザの対話型操作情報と標準情報とを照合することにより、第２のユーザが第１のユーザであるかどうかを特定するために認証を実行するステップは：第２のユーザの対話型操作情報と標準情報とが同一であるかどうかを、第２のユーザの対話型操作情報を標準情報と照合することにより特定し、肯定の場合には、第２のユーザを第１のユーザとして認証し；さもなければ、第２のユーザを第１のユーザとして認証しないステップを含む。
【０１０３】

本願のこの実施では、実際には、標準情報と第２のユーザの対話型操作情報とが同一であることを要することなく、第２のユーザを第１のユーザとして認証することもできる。代替的に、第２のユーザの対話型操作と第１のユーザの対話型操作とが同一である又は類似するかどうかを、標準情報を第２のユーザの対話型操作情報と照合することで特定し、次に、この特定結果に基づいて認証を実行できる。この場合、ステップ２０４における、第２のユーザが第１のユーザであるかどうかを特定するために、第２のユーザの対話型操作情報を標準情報と照合することにより認証を実行するステップは、第２のユーザの対話型操作情報に対応する対話型操作と、標準情報に対応する対話型操作とが同一であるかどうかを、第２のユーザの対話型操作情報を標準情報と照合することにより特定し；肯定である場合、第２のユーザを第１のユーザとして認証するステップ；又は、第２のユーザの対話型操作情報に対応する対話型操作と、標準情報に対応する対話型操作との間の類似性が所定の類似性閾値を下回らないかどうかを、第２のユーザの対話型操作情報を標準情報と照合することにより特定し；肯定である場合、第２のユーザを第１のユーザと認証し；さもなければ、第２のユーザを第１のユーザと認証しないステップ；を含むことができる。

【０１０４】

本願のこの実施では、画像の対話型操作は、画像上の１つ以上の特徴領域へのタップ操作；及び／又は、画像上に複数の特徴領域がある場合には、１つの特徴領域から別の特徴領域へのスライドを実行するためのスライド操作を含んでよい。加えて、対話型操作は、指定画像上の１つ以上の特徴領域へのプレス操作等を更に含んでよい。

【０１０５】

実際には、背景で述べた既存技術に加え、一般に使用されている別の認証技術がある。しかし、この別の既存技術も、背景で述べた既存技術に類似する問題を抱えている。

【０１０６】

図９は、別の既存技術におけるパスワード入力インターフェースの概略図である。この場合、パスワードは所定のデジタルシーケンスであり、第２のユーザは、第２のユーザがパスワードを入力するためにパスワード入力インターフェース内のデジタル領域をタップした場合に限って認証されることができる。

【０１０７】

しかし、図９のパスワード入力インターフェースは多様化されておらず、攻撃者は、通常、こうしたパスワード入力インターフェースに熟知しているため、認証信頼度は相対的に低下してしまう。

【０１０８】

先に述べた既存技術の問題を軽減するために、本願の解決策に基づけば、第１のユーザがパスワード入力インターフェースをカスタマイズでき、パスワードは先に述べた標準情報であってよく、これにより、パスワード入力インターフェースをカスタマイズ及び多様化できるようにしている。攻撃者は第１のユーザによりカスタマイズされたパスワード入力インターフェースに熟知していない可能性があるので、第１のユーザが入力したパスワードを攻撃者が覗き見して控えておく難度を高める、及び／又は、第１のユーザが設定したパスワードを攻撃者が徹底的に攻撃してクラッキングする難度を高めることができるため、認証の信頼性は向上する。したがって、本願は既存技術における他の問題も部分的又は全面的に軽減できる。

【０１０９】

本願の実施で提供される認証方法及び認証のための情報を生成する方法については上で述べている。これと同じ概念に基づき、本願の実施は、図１０及び図１１に示すように、対応する認証デバイスと、対応する認証のための情報を生成するためのデバイスとを更に提供する。

【０１１０】

図１０は、本願の実施に係る認証デバイスを示す概略構造図である。このデバイスは、第１のユーザが事前に指定した画像を表示するように構成された表示モジュール１００１と；画像についての第２のユーザの対話型操作を検出するように構成された検出モジュール

１００２と：検出された第２のユーザの対話型操作に基づき、第２のユーザの対話型操作情報を生成するように構成された生成モジュール１００３と：第２のユーザの対話型操作情報と標準情報とを照合することで、第２のユーザが第１のユーザかどうかを特定するために認証を実行するように構成された認証モジュール１００４であって、ここで、標準情報は、画像についての第１のユーザの対話型操作に基づいて生成される、認証モジュール１００４と；を含む。

【０１１１】

オプションで、本デバイスは、第１のユーザが指定した画像を取得し；画像を表示し、画像上の１つ以上の特徴領域を特定し；１つ以上の特徴領域への第１のユーザの対話型操作を検出し；検出した第１のユーザの対話型操作に基づいて、標準情報を生成するものであって、画像に対する第１のユーザの対話型操作に基づいて標準情報を生成するように構成された標準情報モジュール１００５を更に含む。

【０１１２】

オプションで、標準情報モジュール１００５は、画像上で特徴検出を実行し、この特徴検出により、指定画像上で１つ以上の特徴領域を特定し；及び／又は、第１のユーザが指定した１つ以上の領域を特定し、この１つ以上の領域を特徴領域として用いるように構成される。

【０１１３】

オプションで、標準情報モジュール１００５は、表示モジュール１００１が第１のユーザにより事前に指定された画像を表示する前に、１つ以上の特徴領域を設定するステップを実行するように構成され、ここで、設定するステップを用いて、第１のユーザが事前に指定した、表示された画像上で、１つ以上の特徴領域をマーキングするかどうかを特定する。

【０１１４】

オプションで、標準情報モジュール１００５は次のように構成される。画像上で１つ以上の特徴領域を特定した後に、対応する識別情報を各特徴領域に対して生成し；検出された第１のユーザの対話型操作に基づき、１つ以上の特徴領域への第１のユーザの操作順序を特定し；１つ以上の特徴領域に対応する操作順序及び識別情報に基づいて、操作順序を示すために用いられる特徴領域識別情報シーケンスを生成し、この特徴領域識別情報シーケンスを標準情報として使用し；第２のユーザの対話型操作が１つ以上の特徴領域についての第２のユーザの対話型操作を含む、と特定された場合に、検出された第２のユーザの対話型操作に基づいて１つ以上の特徴領域に第２のユーザの操作順序を特定し；１つ以上の特徴領域に対応する操作順序及び識別情報に基づいて、操作順序を示すために用いられる特徴領域識別情報シーケンスを生成し、この特徴領域識別情報シーケンスを第２のユーザの対話型操作情報として用いる。

【０１１５】

オプションで、認証モジュール１００４は、第２のユーザの対話型操作情報と標準情報とが同一であるかどうかを、第２のユーザの対話型操作情報を標準情報と照合することにより特定し；肯定の場合には、第２のユーザを第１のユーザとして認証するように構成される。

【０１１６】

オプションで、認証モジュール１００４は次のように構成される。第２のユーザの対話型操作情報に対応する対話型操作と、標準情報に対応する対話型操作とが同一であるかどうかを、第２のユーザの対話型操作情報を標準情報と照合することにより特定し、肯定の場合には、第２のユーザを第１のユーザとして認証し；又は、第２のユーザの対話型操作情報に対応する対話型操作と、標準情報に対応する対話型操作との間の類似性が所定の類似性閾値を下回らないかどうかを、第２のユーザの対話型操作情報を標準情報と照合することにより特定し、肯定の場合には、第２のユーザを第１のユーザとして認証する。

【０１１７】

オプションで、画像についての対話型操作は、画像上での１つ以上の特徴領域へのタップ操作；及び／又は、画像上に複数の特徴領域がある場合には、１つの特徴領域から別の特

徴領域へのスライドを実行するスライド操作を含む。
【０１１８】
図１０のデバイスを、認証関連デバイス内に配置できる。
【０１１９】
図１１は、本願の実施に係る認証のための情報を生成するデバイスを示す概略構造図である。このデバイスは、第１のユーザが指定した画像を取得するように構成された取得モジュール１１０１と；画像を表示し、画像上の１つ以上の特徴領域を特定するように構成された表示及び特定モジュール１１０２と；１つ以上の特徴領域についての第１のユーザの対話型操作を検出するように構成された検出モジュール１１０３と；検出した第１のユーザの対話型操作に基づいて標準情報を生成して、第２のユーザが第１のユーザかどうかを特定するために認証を実行するように構成された生成モジュール１１０４と；を含む。
【０１２０】
オプションで、表示及び特定モジュール１１０２は、画像上で特徴検出を実行し、この特徴検出により指定画像上で１つ以上の特徴領域を特定し；及び／又は、指定画像上で第１のユーザが指定した１つ以上の領域を特定し、１つ以上の領域を特徴領域として用いるように構成される。
【０１２１】
図１１のデバイスは、認証関連デバイス内に配置できる。
【０１２２】
本願にて提供されるデバイスは、本願で提供される方法との１対１のマッピング関係にある。したがって、デバイスはこれらの方法のものと類似する有益な技術的効果を奏する。方法の有益な技術的効果については詳細に説明しているので、ここでは簡略化のためにデバイスの有益な技術的効果についての説明を省く。
【０１２３】
当業者は、本願の実施は、方法、システム、又はコンピュータプログラム製品として提供できることを理解するはずである。そのため、本願は、ハードウェアのみの実施、ソフトウェアのみの実施、又は、ソフトウェアとハードウェアとの組み合わせによる実施の形式を用いることができる。さらに、本願は、コンピュータで使用可能なプログラムコードを含んだ１台以上のコンピュータで使用可能な記憶媒体（磁気ディスクストレージ、ＣＤ－ＲＯＭ、光学メモリ等を非限定的に含む）上で実施されるコンピュータプログラム製品の形式で使用できる。
【０１２４】
本願は、本願の実施に係る方法、デバイス（システム）、コンピュータプログラム製品のフローチャート及び／又はブロック図を参照して説明されている。コンピュータプログラム命令は、各工程、及び／又はフローチャート内の各ブロック、及び／又はブロック図を実施するために用いることができ、さらに、工程、及び／又はフローチャート内の１つのブロック、及び／又はブロック図、の組み合わせを実施するために用いることができる点が理解されるはずである。これらのコンピュータプログラム命令は、汎用コンピュータ、専用コンピュータ、組み込みプロセッサ、又はあらゆるその他のプログラム可能なデータ処理デバイスに、マシンを生成するために提供されることができ、これにより、コンピュータ、又は、あらゆるその他のプログラム可能なデータ処理デバイスのプロセッサが、フローチャートの１つ以上の工程において、及び／又は、ブロック図の１つ以上のブロックにおいて、特定の機能を実施するデバイスを生成できるようになる。
【０１２５】
これらのコンピュータプログラム命令を、コンピュータ又はあらゆるその他のプログラム可能なデータ処理デバイスに特定の態様で機能するように命令することができるコンピュータ読み取り可能なメモリに記憶して、これらのコンピュータ読み取り可能なメモリに記憶された命令が、命令デバイスを含む加工品を作り出すようにすることができる。この命令デバイスは、フローチャート内の１つ以上の工程における、及び／又は、ブロック図内の１つ以上のブロックにおける特定の機能を実施する。

【０１２６】
これらのコンピュータプログラム命令をコンピュータ又はその他のプログラム可能なデータ処理デバイスにロードして、コンピュータ又はその他のプログラム可能なデバイス上で一連の操作及びステップが実行されるようにし、コンピュータで実施される処理を生成することができる。これにより、コンピュータ又はその他のプログラム可能なデバイス上で実行される命令が、フローチャート内の１つ以上のステップ及び／又はブロック図内の１つ以上のブロックにおける特定の機能を実施するデバイスを提供することを可能とする。
【０１２７】
典型的な構成では、計算デバイスは１つ以上のプロセッサ（ＣＰＵ）、入出力インターフェース、ネットワークインターフェース、及びメモリを含む。
【０１２８】
メモリは非永続性メモリ、ランダムアクセスメモリ（ＲＡＭ）、不揮発性メモリ、及び／又は、例えば読み取り専用メモリ（ＲＯＭ）やフラッシュメモリ（フラッシュＲＡＭ）のようなコンピュータ読取可能な他の形式を含むことができる。メモリはコンピュータ読取可能な媒体の一例である。
【０１２９】
コンピュータ読取可能な媒体には、任意の方法又は技術を用いて情報を記憶できる、永続的、非永続的、移動可能な、移動不能な媒体が含まれる。この情報はコンピュータ読取可能な命令、データ構造、プログラムモジュール、又はその他のデータであってよい。コンピュータの記憶媒体の例として、計算デバイスによってアクセスできる情報を記憶するために用いることが可能な、相変化ランダムアクセスメモリ（ＰＲＡＭ）、スタティックランダムアクセスメモリ（ＳＲＡＭ）、ダイナミックランダムアクセスメモリ（ＤＲＡＭ）、別タイプのランダムアクセスメモリ、ＲＯＭ、電気的に消去可能でプログラム可能なＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリ、又は別のメモリ技術、コンパクトディスクＲＯＭ（ＣＤ－ＲＯＭ）、デジタル多用途ディスク（ＤＶＤ）、又は別の光学記憶装置、磁気カセットテープ、テープ及びディスク記憶装置、又は別の磁気記憶デバイス、若しくはその他任意の非一時的媒体があるが、それらに限定されない。本願で定義しているように、コンピュータ読取可能な媒体は、変調されたデータ信号及び搬送波のような一時的な媒体（ｔｒａｎｓｉｔｏｒｙ　ｍｅｄｉａ）を含まない。
【０１３０】
さらに、用語「含む」、「含有する」、又はこれらのその他任意の応用形は、非限定的な包含を網羅するものであるため、一連の要素を含んだ工程、方法、物品、デバイスはこれらの要素を含むだけでなく、ここで明確に挙げていないその他の要素をも含む、あるいは、このような工程、方法、物品、デバイスに固有の要素をさらに含むことができる点に留意することが重要である。「（一の）～を含む」との用語を付けて示された要素は、それ以上の制約がなければ、その要素を含んだ工程、方法、物品、デバイス内に別の同一の要素をさらに含むことを排除しない。
【０１３１】
当業者は、本願の実施が方法、システム、コンピュータプログラム製品として提供され得ることを理解するはずである。そのため、本願は、ハードウェアのみの実施、ソフトウェアのみの実施、又は、ソフトウェアとハードウェアの組み合わせによる実施を用いることができる。さらに、本願は、コンピュータで用いることができるプログラムコードを含んだ、１つ以上のコンピュータで使用可能な記憶媒体（磁気ディスクストレージ、ＣＤ－ＲＯＭ、光学ディスク等を非限定的に含む）上で実施されるコンピュータプログラム製品の形態を用いることが可能である。
【０１３２】
上述のものは本願の一実施形態であるが、本願を限定するものではない。当業者は、本願に様々な修正及び変更を加えることができる。本願の主旨及び原理から逸脱せずに為されるあらゆる修正、均等物による代替、改善は、本願の特許請求の範囲に含まれるものである。

以下、本発明の実施の態様の例を列挙する。
［第１の局面］
第１のユーザにより事前に指定された画像を表示するステップと；
前記画像についての第２のユーザの対話型操作を検出するステップと；
検出した前記第２のユーザの前記対話型操作に基づき、前記第２のユーザの対話型操作情報を生成するステップと；
前記第２のユーザが前記第１のユーザであるかどうかを、第２のユーザの対話型操作情報を標準情報と照合することにより特定するために、認証を実行するステップと；を備える、
認証方法。
［第２の局面］
前記標準情報は、前記画像についての前記第１のユーザの対話型操作に基づいて：
前記第１のユーザにより指定された前記画像を取得し；
前記画像を表示し、前記画像上で１つ以上の特徴領域を特定し；
前記１つ以上の特徴領域への前記第１のユーザの対話型操作を検出し；
検出した前記第１のユーザの前記対話型操作に基づいて前記標準情報を生成する；ようにして生成される、
第１の局面に記載の認証方法。
［第３の局面］
前記画像上の１つ以上の特徴領域を特定する前記ステップは、具体的に：
前記画像上で特徴検出を実行し、特徴検出により前記１つ以上の特徴領域を特定するステップ；及び／又は
前記指定画像上の、前記第１のユーザにより指定された１つ以上の領域を特定し、前記１つ以上の領域を前記特徴領域として用いるステップ；を備える、
第２の局面に記載の認証方法。
［第４の局面］
第１のユーザにより事前に指定された画像を表示する前記ステップの前に、
前記１つ以上の特徴領域に設定を実行するステップを更に備え、前記設定は、前記第１のユーザにより事前に指定された前記表示された画像上で前記１つ以上の特徴領域をマーキングするかどうかを特定するために用いられる、
第２の局面に記載の認証方法。
［第５の局面］
前記画像上で１つ以上の特徴領域を特定する前記ステップの後に、
各特徴領域についての対応する識別情報を生成するステップを更に備え、
検出した前記第１のユーザの前記対話型操作に基づいて前記標準情報を生成する前記ステップは、具体的に：
検出した前記第１のユーザの前記対話型操作に基づき、前記１つ以上の特徴領域についての前記第１のユーザの操作順序を特定するステップと；
前記操作順序を示すために用いられる特徴領域識別情報シーケンスを、前記１つ以上の特徴領域についての対応する前記操作順序及び識別情報に基づいて生成し、前記特徴領域識別情報シーケンスを前記標準情報として用いるステップと；を備え、
検出した前記第２のユーザの前記対話型操作に基づいて、前記第２のユーザの対話型操作情報を生成する前記ステップは、具体的に：
前記第２のユーザの前記対話型操作が前記１つ以上の特徴領域についての前記第２のユーザの対話型操作を含む、と特定される場合に、前記１つ以上の特徴領域についての前記第２のユーザの操作順序を、検出された前記第２のユーザの前記対話型操作に基づいて特定するステップと；
前記操作順序を示すために用いられる特徴領域識別情報シーケンスを、前記１つ以上の特徴領域についての対応する前記操作順序及び前記識別情報に基づいて生成し、前記特徴領域識別情報シーケンスを前記第２のユーザの前記対話型操作情報として用いるステップ

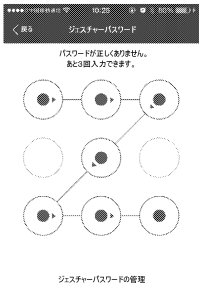
と；を備える、
第２の局面に記載の認証方法。
［第６の局面］
前記第２のユーザが前記第１のユーザであるかどうかを前記第２のユーザの前記対話型操作情報を前記標準情報と照合することにより特定するために認証を実行する前記ステップは、具体的に：
前記第２のユーザの前記対話型操作情報と前記標準情報とが同一であるかどうかを、前記第２のユーザの前記対話型操作情報を前記標準情報と照合することにより特定するステップと；
肯定である場合に、前記第２のユーザを前記第１のユーザである、と認証するステップと；を備える、
第５の局面に記載の認証方法。
［第７の局面］
前記第２のユーザが前記第１のユーザであるかどうかを、前記第２のユーザの前記対話型操作情報を前記標準情報と照合させることにより特定するために認証を実行する前記ステップは、具体的に：
前記第２のユーザの前記対話型操作情報に対応する対話型操作と、前記標準情報に対応する対話型操作とが同一であるかどうかを、前記第２のユーザの前記対話型操作情報を前記標準情報と照合することにより特定し、肯定の場合に、前記第２のユーザを前記第１のユーザとして認証するステップ；又は、
前記第２のユーザの前記対話型操作情報に対応する対話型操作と、前記標準情報に対応する対話型操作との間の類似性が所定の類似性閾値を下回らないかどうかを、前記第２のユーザの前記対話型操作情報を前記標準情報と照合することにより特定し、肯定の場合に、前記第２のユーザを前記第１のユーザとして認証するステップ；を備える、
第１の局面に記載の認証方法。
［第８の局面］
前記画像についての前記対話型操作は：
前記画像上での前記１つ以上の特徴領域へのタップ操作；及び／又は、
前記画像上に複数の特徴領域がある場合に、１つの特徴領域から別の特徴領域へのスライドを実行するスライド操作；を備える、
第１乃至７の局面に記載の認証方法。
［第９の局面］
第１のユーザにより指定された画像を取得するステップと；
前記画像を表示し、前記画像上で１つ以上の特徴領域を特定するステップと；
前記１つ以上の特徴領域についての前記第１のユーザの対話型操作を検出するステップと；
第２のユーザが前記第１のユーザであるかどうかを特定するために認証を実行するべく、検出された前記第１のユーザの前記対話型操作に基づいて標準情報を生成するステップと；を備える、
認証のための情報を生成する方法。
［第１０の局面］
前記画像上で１つ以上の特徴領域を特定する前記ステップは、具体的に：
前記画像に特徴検出を実行し、特徴検出により前記指定画像上で前記１つ以上の特徴領域を特定するステップ；及び／又は
前記指定画像上で前記第１のユーザが指定した１つ以上の領域を特定し、前記１つ以上の領域を前記特徴領域として用いるステップ；を備える、
第９の局面に記載の認証のための情報を生成する方法。
［第１１の局面］
前記第１のユーザにより事前に指定された画像を表示するように構成された表示モジュールと；

前記画像についての第２のユーザの対話型操作を検出するように構成された検出モジュールと；
検出した前記第２のユーザの前記対話型操作に基づいて、前記第２のユーザの対話型操作情報を生成するように構成された生成モジュールと；
前記第２のユーザの前記対話型操作情報を前記標準情報と照合することにより、前記第２のユーザが前記第１のユーザである、と特定するために、認証を実行するように構成された認証モジュールであって、前記標準情報は前記画像についての前記第１のユーザの対話型操作に基づいて生成される、認証モジュールと；を備える、
認証デバイス。
［第１２の局面］
前記標準情報を前記画像についての前記第１のユーザの前記対話型操作に基づいて：
前記第１のユーザにより指定された前記画像を取得し；
前記画像を表示し、前記画像上で１つ以上の特徴領域を特定し；
前記１つ以上の特徴領域への前記第１のユーザの対話型操作を検出し；
検出した前記第１のユーザの前記対話型操作に基づいて前記標準情報を生成する；ように構成された標準情報モジュールを更に備える、
第１１の局面に記載の認証デバイス。
［第１３の局面］
前記標準情報モジュールは：
前記画像上で特徴検出を実行し、特徴検出により前記指定画像上で前記１つ以上の特徴領域を特定し；及び／又は、
前記指定画像上で前記第１のユーザにより指定された１つ以上の領域を特定し、前記１つ以上の領域を前記特定領域として用いる；ように構成される、
第１２の局面に記載の認証デバイス。
［第１４の局面］
前記標準情報モジュールは、前記表示モジュールが、前記第１のユーザにより事前に指定された前記画像を表示する前に、前記１つ以上の特徴領域についての設定を実行するように構成されており、前記設定は、前記第１のユーザにより事前に指定された前記表示された画像上の前記１つ以上の特徴領域をマーキングするかどうかを特定するために使用される、
第１２の局面に記載の認証デバイス。
［第１５の局面］
前記標準情報モジュールは：
前記１つ以上の特徴領域を特定した後に、対応する識別情報を各特徴領域について生成し；検出した前記第１のユーザの前記対話型操作に基づいて、前記１つ以上の特徴領域についての前記第１のユーザの操作順序を特定し；前記１つ以上の特徴領域についての対応する前記操作順序と、識別情報とに基づいて、前記操作順序を示すために用いられる特徴領域識別情報シーケンスを生成し、前記特徴領域識別情報シーケンスを前記標準情報として用い；
前記第２のユーザの前記対話型操作が前記１つ以上の特徴領域についての前記第２のユーザの対話型操作を含む、と特定される場合に、検出した前記第２ユーザの前記対話型操作に基づいて、前記１つ以上の特徴領域についての前記第２のユーザの操作順序を特定し；
前記１つ以上の特徴領域についての対応する前記操作順序及び前記識別情報に基づいて、前記操作順序を示すために用いられる特徴領域識別情報シーケンスを生成し、前記特徴領域識別情報シーケンスを前記第２のユーザの前記対話型操作情報として用いる；ように構成される、
第１２の局面に記載の認証デバイス。
［第１６の局面］
前記認証モジュールは、前記第２のユーザの前記対話型操作情報と前記標準情報とが同一であるかどうかを、前記第２のユーザの前記対話型操作情報を前記標準情報と照合する

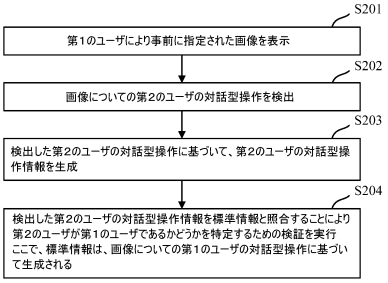
ことにより特定し；肯定の場合には、前記第２のユーザを前記第１のユーザとして認証するように構成される、
　第１５の局面に記載の認証デバイス。
［第１７の局面］
　前記認証モジュールは、前記第２のユーザの前記対話型操作情報と前記標準情報に対応する対話型操作とが同一であるかどうかを、前記第２のユーザの前記対話型操作情報を前記標準情報と照合することにより特定し、肯定の場合に、前記第２のユーザを前記第１のユーザとして認証する；又は、前記第２のユーザの前記対話型操作情報に対応する対話型操作と、前記標準情報に対応する対話型操作との間の類似性が所定の類似性閾値を下回らないかどうかを、前記第２のユーザの前記対話型操作情報を前記標準情報と照合することにより特定し、肯定の場合に、前記第２のユーザを前記第１のユーザとして認証する；ように構成される、
　第１１の局面に記載の認証デバイス。
［第１８の局面］
　前記画像についての前記対話型操作は：
　前記画像上の前記１つ以上の特徴領域についてのタップ操作と；及び／又は、
　前記画像上に複数の特徴領域がある場合には１つの特徴領域から別の特徴領域へのスライド操作を実行するスライド操作と；を備える、
　第１１乃至１７の局面に記載の認証デバイス。
［第１９の局面］
　第１のユーザにより指定された画像を取得するように構成された取得モジュールと；
　前記画像を表示し、前記画像上で１つ以上の特徴領域を特定するように構成された表示及び特定モジュールと；
　１つ以上の特徴領域についての前記第１のユーザの対話型操作を検出するように構成された検出モジュールと；
　前記第２のユーザが前記第１のユーザであるかどうかを特定するために認証を実行するべく、検出した前記第１のユーザの前記対話型操作に基づいて、標準情報を生成するように構成された生成モジュールと；を備える、
　認証のための情報を生成するデバイス。
［第２０の局面］
　前記表示及び特定モジュールは、前記画像に特徴検出を実行して、特徴検出により前記指定画面上の前記１つ以上の特徴領域を特定する；及び／又は、前記第１のユーザが指定した１つ以上の領域を特定し、前記１つ以上の領域を前記特徴領域として用いる；ように構成される、
　第１９の局面に記載の認証のための情報を生成するデバイス。
【符号の説明】
【０１３３】
１００１　表示モジュール
１００２、１１０３　検出モジュール
１００３、１１０４　生成モジュール
１００４　認証モジュール
１００５　標準情報モジュール
１１０１　取得モジュール
１１０２　表示及び特定モジュール

【図面】

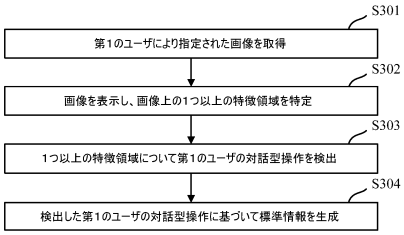
【図１】



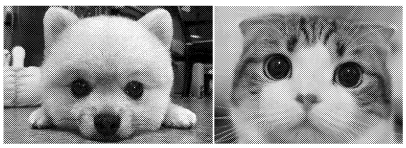
【図２】



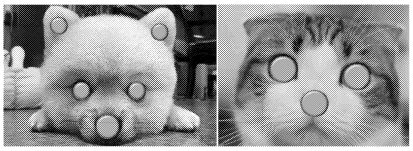
【図３】



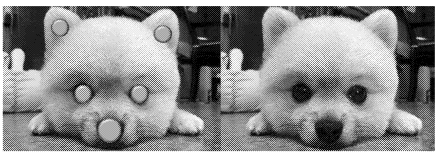
【図４】



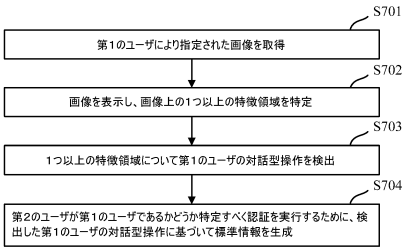
【図５】



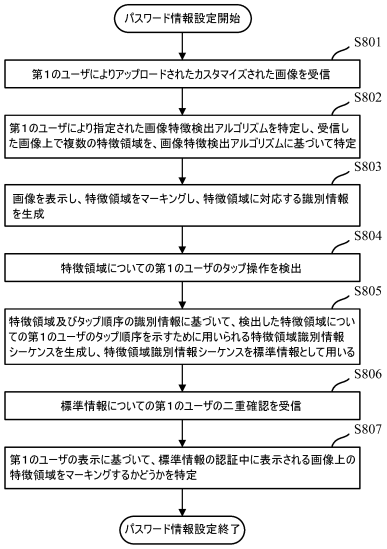
【図６】



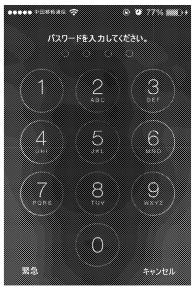
【図７】



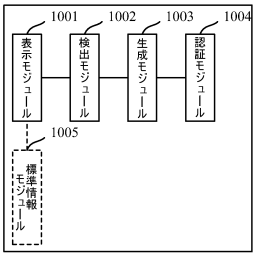
【図８】



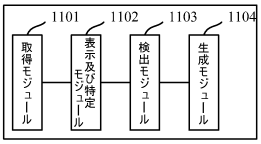
【図９】



【図１０】



【図１１】



フロントページの続き

ー ９６９，ビルディング ３，５／エフ，アリババ グループ リーガル デパートメント

審査官　今城 朋彬

(56)参考文献

特開２０１３－１９０９９２（ＪＰ，Ａ）
米国特許出願公開第２０１０／０３２５７２１（ＵＳ，Ａ１）
米国特許出願公開第２０１４／０１８１９５７（ＵＳ，Ａ１）
特表２０１４－５２０３１３（ＪＰ，Ａ）
再公表特許第２０１１／１５８７６８（ＪＰ，Ａ１）
特開２０１２－２１２３００（ＪＰ，Ａ）
特表２０１３－５１５３１８（ＪＰ，Ａ）
特開２０１５－０４９６０８（ＪＰ，Ａ）
特開２００５－０８２０８６（ＪＰ，Ａ）
特表２０１１－５２４５９２（ＪＰ，Ａ）
Muhammad Shahzad et al.，Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures - You can see it but you can not do it，MobiCom '13: Proceedings of the 19th annual international conference on Mobile computing & networking [online]，ACM，2013年09月30日，p.39-50，https://dl.acm.org/doi/10.1145/2500423.2500434

(58)調査した分野　(Int.Cl.，ＤＢ名)

Ｇ０６Ｆ　２１／００
Ｇ０６Ｆ　２１／３０－２１／４６