(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2018-517211
(P2018-517211A)
(43)公表日　平成30年6月28日(2018.6.28)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 3/02	(2006.01)	G06F	3/02	530	5B020

審査請求 未請求　予備審査請求 未請求　（全 18 頁）

(21)出願番号　特願2017-561926 (P2017-561926)
(86)(22)出願日　平成28年4月28日 (2016.4.28)
(85)翻訳文提出日　平成30年1月29日 (2018.1.29)
(86)国際出願番号　PCT/CN2016/080440
(87)国際公開番号　WO2016/188297
(87)国際公開日　平成28年12月1日 (2016.12.1)
(31)優先権主張番号　201510282846.3
(32)優先日　平成27年5月28日 (2015.5.28)
(33)優先権主張国　中国(CN)

(71)出願人　505032849
アリババ　グループ　ホウルディング　リミテッド
英国領ケイマン諸島　グランド　ケイマン　ジョージ　タウン　ピーオーボックス　847　ワン　キャピタル　プレイス　フォース　フロア
(74)代理人　100097320
弁理士　宮川　貞二
(74)代理人　100155192
弁理士　金子　美代子
(74)代理人　100131820
弁理士　金井　俊幸
(74)代理人　100100398
弁理士　柴田　茂夫

最終頁に続く

(54)【発明の名称】情報入力方法及び装置

(57)【要約】
本願は、情報入力方法及び装置を提供する。情報入力方法は、予め格納された情報を取得するステップであって、前記予め格納された情報は、プレーンテキストである第１の情報又は暗号化された第１の情報を含み、前記第１の情報は、設定情報と、前記設定情報に応じて生成された関連情報とを含む、取得するステップと；照合すべき情報を受信するステップと；前記予め格納された情報に従い前記照合すべき情報を照合するステップと；前記照合すべき情報が前記関連情報に属する場合、再度照合を実行するステップと；を備える。本方法は、意図しないエラーと悪意のあるエラーとを効果的に判別し、結果として意図しない入力エラーに起因する情報照合の失敗を減らすことができる。
【選択図】図１

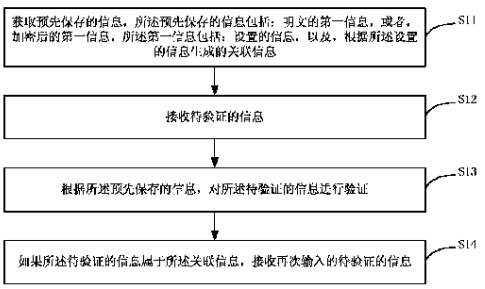

图１

S11　ACQUIRE PRE-SAVED INFORMATION, WHEREIN THE PRE-SAVED INFORMATION COMPRISES FIRST INFORMATION WHICH IS PROCLAIMED OR FIRST INFORMATION WHICH IS ENCRYPTED, AND THE FIRST INFORMATION COMPRISES SET INFORMATION AND ASSOCIATED INFORMATION GENERATED ACCORDING TO THE SET INFORMATION
S12　RECEIVE TO-BE-VERIFIED INFORMATION
S13　VERIFY, ACCORDING TO THE PRE-SAVED INFORMATION, THE TO-BE-VERIFIED INFORMATION
S14　IF THE TO-BE-VERIFIED INFORMATION BELONGS TO THE ASSOCIATED INFORMATION, RECEIVE THE TO-BE-VERIFIED INFORMATION WHICH IS INPUT AGAIN

【特許請求の範囲】
【請求項１】
情報入力方法であって：
予め格納された情報を取得するステップであって、前記予め格納された情報はプレーンテキストである第１の情報又は暗号化された第１の情報を含み、前記第１の情報は、設定情報と、前記設定情報に応じて生成された関連情報とを含む、取得するステップと；
照合すべき情報を受信するステップと；
前記予め格納された情報に従い前記照合すべき情報を照合するステップと；
前記照合すべき情報が前記関連情報に属する場合、再入力される照合すべき情報を受信するステップと；を備える、
情報入力方法。
【請求項２】
前記再入力される照合すべき情報を受信するステップの前に、ユーザに対し、前記ユーザがキーボードのキーに注意を向けるように促すために用いられるプロンプト情報を表示するステップ；又は、
前記再入力される照合すべき情報を受信するステップの後に、前記再入力される照合すべき情報のプレーンテキスト表示時間を延長するステップ；又は、
前記再入力される照合すべき情報を受信するステップの後に、前記再入力される照合すべき情報をプレーンテキストでそのまま表示するステップ；を更に備える、
請求項１に記載の方法。
【請求項３】
前記設定情報に応じて関連情報を生成するステップを更に備え、
前記設定情報に応じて関連情報を生成する前記ステップが：
前記設定情報から情報項目をランダムに選択し、前記選択された情報項目に対応する新しい情報項目を取得するステップであって、前記新しい情報項目の位置と前記選択された情報項目の位置との間のキーボード上での距離が予め設定された範囲内にある、取得するステップと；
前記設定情報の中の前記選択された情報項目を前記新しい情報項目に置き換えて前記関連情報を得るステップと；を備える、
請求項１に記載の方法。
【請求項４】
前記予め格納された情報が前記暗号化された第１の情報である場合、前記予め格納された情報に従い前記照合すべき情報を照合する前記ステップが：
前記第１の情報と同じ暗号化アルゴリズムを用いることにより前記照合すべき情報を暗号化して暗号化された照合すべき情報を得るステップと；
前記暗号化された照合すべき情報を前記予め格納された情報と比較するステップと；を備える、
請求項１に記載の方法。
【請求項５】
前記暗号化アルゴリズムがハッシュアルゴリズムである、
請求項４に記載の方法。
【請求項６】
前記予め格納された情報に従い前記照合すべき情報を照合する前記ステップの後に：
前記照合すべき情報が前記設定情報と同じである場合、前記照合が成功であると判定するステップ；又は、
前記照合すべき情報が前記設定情報と異なり、かつ前記関連情報に属していない場合、前記照合が失敗であると判定するステップ；を更に備える、
請求項１乃至５のいずれか一項に記載の方法。
【請求項７】
情報入力装置であって：

予め格納された情報を取得するように構成された取得モジュールであって、前記予め格納された情報は、プレーンテキストである第１の情報又は暗号化された第１の情報を含み、前記第１の情報は、設定情報と、前記設定情報に応じて生成された関連情報とを含む、取得モジュールと；
照合すべき情報を受信するように構成された第１の受信モジュールと；
前記予め格納された情報に従い前記照合すべき情報を照合するように構成された照合モジュールと；
前記照合すべき情報が前記関連情報に属する場合、再入力される照合すべき情報を受信するように構成された第２の受信モジュールと；を備える、
情報入力装置。
【請求項８】
前記第２の受信モジュールが：
前記再入力される照合すべき情報が受信される前に、ユーザに対し、前記ユーザがキーボードのキーに注意を向けるように促すために用いられるプロンプト情報を表示する；又は、
前記再入力される照合すべき情報が受信された後に、前記再入力される照合すべき情報のプレーンテキスト表示時間を延長する；又は、
前記再入力される照合すべき情報が受信された後に、前記再入力される照合すべき情報をプレーンテキストでそのまま表示する；ように更に構成された、
請求項７に記載の装置。
【請求項９】
前記設定情報から情報項目をランダムに選択し、前記選択された情報項目に対応する新しい情報項目を取得するように構成され、前記新しい情報項目の位置と前記選択された情報項目の位置との間のキーボード上での距離が予め設定された範囲内にあり；
前記設定情報の中の前記選択された情報項目を前記新しい情報項目に置き換えて前記関連情報を得る；ように構成された設定モジュールを更に備える、
請求項７に記載の装置。
【請求項１０】
前記予め格納された情報が前記暗号化された第１の情報である場合、前記照合モジュールは、具体的に：
前記第１の情報と同じ暗号化アルゴリズムを用いることにより前記照合すべき情報を暗号化して暗号化された照合すべき情報を取得し；
前記暗号化された照合すべき情報を前記予め格納された情報と比較する；ように構成された、
請求項７に記載の装置。
【請求項１１】
前記照合すべき情報が前記設定情報と同じである場合、前記照合が成功であると判定する；又は、
前記照合すべき情報が前記設定情報と異なり、かつ前記関連情報に属していない場合、前記照合が失敗であると判定する；ように構成された判定モジュールを更に備える、
請求項７乃至１０のいずれか一項に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本願は、データ処理技術の分野に関し、特に、情報入力方法及び装置に関する。
【背景技術】
【０００２】
モバイル通信技術の発展にともない、ユーザは、モバイルデバイスへ情報を入力することがしばしば必要となっている。とりわけ、情報を携帯電話に入力する場合、携帯電話のサイズが限られているため、物理的キーボード又は仮想キーボードのサイズは比較的小さ

く、ユーザは情報を不正確に入力してしまいがちである。例えば、ユーザが文字“ａ”を入力するつもりでいても、実際には文字“ａ”に隣接する文字、例えば“ｓ”を入力してしまう。

【発明の概要】

【発明が解決しようとする課題】

【０００３】

本願は、こうした技術的な課題の１つを少なくともある程度は解決することを目指している。

したがって、本願の一の目的は、小型キーボードに起因する入力エラーを減らし、入力効果を高めることができる情報入力方法を提案することである。

本願の別の目的は情報入力装置を提案することである。

【課題を解決するための手段】

【０００４】

上記目的を達成するために、本願の第１の態様による実施の形態で提案される情報入力方法は：予め格納された情報を取得するステップであって、前記予め格納された情報は、プレーンテキストである第１の情報又は暗号化された第１の情報を含み、前記第１の情報は、設定情報と、前記設定情報に応じて生成された関連情報とを含む、取得するステップと；照合すべき情報を受信するステップと；前記予め格納された情報に従い前記照合すべき情報を照合するステップと；前記照合すべき情報が前記関連情報に属する場合、再入力される照合すべき情報を受信するステップと；を備える。

【０００５】

本願の第１の態様による実施の形態によって提案される情報入力方法は、設定情報を生成できるだけでなく、設定情報に応じて得られる関連情報を生成でき、照合すべき情報（to-be-verified information）が関連情報に属する場合、再入力される照合すべき情報を受信できる。したがって、ユーザは、小型キーボード又は他の理由に起因して入力エラーが発生した後に、照合の機会をもう一度得ることができるため、小型キーボードに起因する入力エラーが減り、入力効果が高まる。

【０００６】

上記目的を達成するために、本願の第２の態様による実施の形態で提案される情報入力装置は：予め格納された情報を取得するように構成された取得モジュールであって、前記予め格納された情報は、プレーンテキストである第１の情報又は暗号化された第１の情報を含み、前記第１の情報は、設定情報と、前記設定情報に応じて生成された関連情報とを含む、取得モジュールと；照合すべき情報を受信するように構成された第１の受信モジュールと；前記予め格納された情報に従い前記照合すべき情報を照合するように構成された照合モジュールと；前記照合すべき情報が前記関連情報に属する場合、再入力される照合すべき情報を受信するように構成された第２の受信モジュールと；を備える。

【０００７】

本願の第２の態様による実施の形態によって提案される情報入力装置は、設定情報を生成できるだけでなく、設定情報に応じて得られる関連情報を生成でき、照合すべき情報が関連情報に属する場合、再入力される照合すべき情報を受信することができる。したがって、ユーザは、小型キーボード又は他の理由に起因して入力エラーが発生した後に、照合の機会をもう一度得ることができるため、小型キーボードに起因する入力エラーが減り、入力効果が高まる。

【０００８】

本願の更なる態様及び利点は以下の説明において部分的に提供され、以下の説明から部分的に明らかになろう、又は、本願の実施を通じて知ることになろう。

【図面の簡単な説明】

【０００９】

本願の上記及び／又は更なる態様及び利点は、添付の図面を参照する実施の形態に関する以下の説明から明らかになり、容易に理解される。

【００１０】
【図１】図１は、本願の実施の形態による情報入力方法の概略フローチャートである。
【図２】図２は、本願の別の実施の形態による情報入力方法の概略フローチャートである。
【図３】図３は、本願の別の実施の形態による情報入力方法の概略フローチャートである。
【図４】図４は、本願の別の実施の形態による情報入力方法の概略フローチャートである。
【図５】図５は、本願の別の実施の形態による情報入力装置の概略構造図である。
【図６】図６は、本願の別の実施の形態による情報入力装置の概略構造図である。
【発明を実施するための形態】
【００１１】
本願の実施の形態を以下で詳細に説明し、実施の形態の例を添付の図面に示すが、本文全体を通じ、同一又は類似の符号は、同一若しくは類似のモジュール、又は同一若しくは類似の機能を有するモジュールを表す。添付の図面を参照に以下で説明する実施の形態は例示であって、本願の説明を意図したものに過ぎず、本願を限定するものと解釈することはできない。対照的に、本発明の実施の形態は、付帯する請求項の精神及び言外の意味の範囲内に含まれる変更、変形、及び均等物を全て包含する。
【００１２】
図１は、本願の実施の形態による情報入力方法の概略フローチャートである。この方法は以下を含む。
【００１３】
Ｓ１１：予め格納された情報が取得され、前記予め格納された情報は、プレーンテキストである第１の情報又は暗号化された第１の情報を含み、前記第１の情報は、設定情報と、前記設定情報に応じて生成された関連情報とを含む。
【００１４】
この実施の形態の方法は、例えば、パスワード照合、ＩＤカード番号照合、銀行カード番号照合、携帯電話番号照合など、様々なシナリオにおける情報照合に用いることができる。この実施の形態では、パスワード照合を例に取り上げる。
【００１５】
パスワード照合の前に、ユーザは、パスワードを予め設定できる。例えば、パスワードがｘと設定される。当然ながら、ユーザが設定するパスワードｘは１つ以上の情報項目を含むことができ、各情報項目は数字や文字などであってもよい。
【００１６】
更に、パスワードが携帯電話端末に格納される場合を例に取り上げると、パスワードは、プレーンテキストの形で、例えばｘとして、そのまま携帯電話端末に格納されてもよい。或いは、セキュリティを強化するために、プレーンテキストのパスワードが格納前に暗号化される。例えば、暗号化されたｘが携帯電話端末に格納される。当然ながら、様々な暗号化アルゴリズムが存在するが、具体的には、例えばハッシュアルゴリズムである。この実施の形態では、携帯電話端末に格納されるハッシュ暗号化されたパスワードを例に取り上げる。ハッシュ暗号化後のｘはＨ（ｘ）と表すものとする。
【００１７】
従来技術において、予め格納される情報はせいぜいＨ（ｘ）であり、ユーザの入力がｘでなければ、照合は失敗となる。
【００１８】
この実施の形態では、単にＨ（ｘ）を格納できるだけでなく、ｘに応じて関連情報を得ることができ、関連情報に対してハッシュ暗号化を行った後に得られる情報が更に携帯電話端末に格納される。
【００１９】
具体的には、図２を参照すると、この実施の形態の方法は更に以下を含む。

【００２０】
Ｓ１０：設定情報に応じて関連情報を生成する。
任意ではあるが、設定情報に応じて関連情報を生成するステップは：
設定情報から情報項目をランダムに選択し、選択された情報項目に対応する新しい情報項目を取得するステップであって、新しい情報項目の位置と選択された情報項目の位置との間のキーボード上での距離が予め設定された範囲内にある、取得するステップと；
設定情報の中の選択された情報項目を新しい情報項目に置き換えて関連情報を得るステップと；を備える。
【００２１】
例えば、ユーザが設定したパスワードｘの１つの項目（要素）がａである場合、仮想キーボード又は物理的キーボード上でａから短い距離にあるキャラクタ（文字、記号）が、ａに対応する新しいキャラクタとして選択される。新しいキャラクタをａ’で表すとすると、ａ’は、ａと置き換わって新しいパスワードｘ’を構成するために用いられる。新しいパスワードｘ’は、ｘの関連情報である。ハッシュ暗号化後、暗号化された関連情報は、Ｈ（ｘ’）、Ｈ（ｘ”）、・・・と表すことができ、この配列がＨ’として記録される。具体的には、例えば、ｘがａｂｃｄであり、ａから短い距離にあるキャラクタがａ’を含むとすると、ｘの関連情報はａ’ｂｃｄを含む。更に、ａから短い距離にあるキャラクタがａ”を更に含むとすると、ｘの関連情報はａ”ｂｃｄを更に含む。更に、ｂから短い距離にあるキャラクタがｂ’を含むとすると、ｘの関連情報はａｂ’ｃｄを更に含み、残りについても同様に処理され、その結果全ての関連情報を得ることができる。
【００２２】
当然ながら、上記の短い距離の具体的な意味は、実際の要求に従って設定できる。例えば、４個の隣り合うキーに対応するキャラクタを短い距離にあるキャラクタとして決定する、キー２個以下の距離にあるキャラクタ全てを短い距離にあるキャラクタとして決定する、などとしてもよい。
【００２３】
Ｓ１２：照合すべき情報を受信する。
ユーザは、照合すべき情報を、キーボードを介して入力できる。
例えば、ユーザは携帯電話の仮想キーボードを使用してパスワードなどを入力する。
【００２４】
Ｓ１３：予め格納された情報に従い照合すべき情報を照合する。
携帯電話端末がプレーンテキストのパスワードをそのまま格納する場合、入力情報は予め格納された情報とそのまま比較することができ、それらが同じ場合、照合は成功である。そうでない場合、照合は失敗である。
【００２５】
この実施の形態では、暗号化された第１の情報を格納するステップを例に取り上げる。
予め格納された情報が暗号化された第１の情報である場合、予め格納された情報に従い照合すべき情報を照合するステップは：
第１の情報と同じ暗号化アルゴリズムを用いることにより照合すべき情報を暗号化して暗号化された照合すべき情報を得るステップと；
暗号化された照合すべき情報を予め格納された情報と比較するステップと；を備える。
【００２６】
ユーザが入力する照合すべき情報がｙであって、ハッシュ暗号化アルゴリズムが適用されるとすると、まずＨ（ｙ）を計算することができ、次いでＨ（ｙ）がＨ（ｘ）及びＨ’と比較される。
【００２７】
Ｓ１４：前記照合すべき情報が前記関連情報に属する場合、再入力される照合すべき情報が受信される。
例えば、Ｈ（ｙ）がＨ’に属する場合、再入力される照合すべき情報を受信できる。その後に再度、照合される。

【００２８】
図３を参照すると、この実施の形態では、照合すべき情報が関連情報に属する場合、具体的には以下のステップを実行してもよい。
【００２９】
Ｓ１４１：再入力される照合すべき情報を受信し、案内のステップが実行される、又は明確なプロンプトが与えられる。
具体的には、案内する又は明確なプロンプトを与えることを実行するステップは：
前記再入力される照合すべき情報を受信するステップの前に、ユーザに対し、前記ユーザがキーボードのキーに注意を向けるように促すために用いられるプロンプト情報を表示するステップ；又は、
前記再入力される照合すべき情報を受信するステップの後に、前記再入力される照合すべき情報のプレーンテキスト表示時間を延長するステップ；又は、
前記再入力される照合すべき情報を受信するステップの後に、前記再入力される照合すべき情報をプレーンテキストでそのまま表示するステップ；を備えてもよい。
【００３０】
例えば、ユーザが、関連情報に属するｙを入力した場合、これは、小さなキーサイズゆえの、ユーザの意図しない入力エラーが原因である可能性が極めて高い。このとき、ユーザはキーボードに注意を向けるよう促され、それによりキーボードのサイズが小さいことによる入力エラーを回避できる。或いは、記号＊などの非プレーンテキスト情報がパスワード照合の際に最終的に表示されるのが通常であり、記号＊が表示される前に、ユーザが入力したプレーンテキスト情報が短時間表示されてもよい。
【００３１】
この実施の形態において、プレーンテキスト表示時間を延長する場合、照合すべき情報の中の各情報項目のプレーンテキスト表示時間を延長してもよく、或いは、前回不正確に入力された情報項目のプレーンテキスト表示時間のみが延長される。例えば、照合すべき情報がａｂｃｄであって、ａの最初の検出時にエラーが発生した場合、ａのプレーンテキスト表示時間のみを延長してもよく、ａ、ｂ、ｃ、及びｄのプレーンテキスト表示時間を全て延長してもよい。加えて、プレーンテキストを表示する際にも、同様に実行してもよい。例えば、前回不正確に入力された情報項目のみをプレーンテキストで表示する、又は情報項目全てをプレーンテキストで表示する。
【００３２】
その後に、以下のステップを更に実行してもよい。
【００３３】
Ｓ１４２：再度、照合する。
例えば、ユーザは、プロンプト情報に従い再入力される照合すべき情報、又はプレーンテキストで表示された情報をチェックできる。ユーザが再入力した照合すべき情報が携帯電話端末で受信された後、情報を、予め格納された情報と比較して照合結果を得ることができる。
【００３４】
この実施の形態では、プレーンテキスト入力情報を表示する時間を延長することができ、その結果、ユーザは自ら入力した情報をよく見て情報が正しく入力されたか否かを照合できる。具体的な延長時間を設定してもよい。或いは、入力情報をプレーンテキストでそのまま表示することによりユーザのチェックを容易にする。
【００３５】
別の態様において、図４を参照すると、入力された照合すべき情報をユーザが照合した後、方法は以下を更に含んでもよい。
【００３６】
Ｓ１５：照合すべき情報が設定情報と同じである場合、照合が成功であると判定する。
例えば、ハッシュ暗号化後に得られた値が格納され、ユーザによって入力された照合すべき情報がｙである場合、ｙは、ハッシュ値に変換されてＨ（ｙ）が得られ、Ｈ（ｙ）が

Ｈ（ｘ）と同じ場合、照合は成功である。
【００３７】
Ｓ１６：照合すべき情報が設定情報と異なり、かつ関連情報に属していない場合、照合は失敗であると判定される。
例えば、Ｈ（ｙ）がＨ（ｘ）と異なり、かつＨ（ｙ）がＨ’に属していない場合、照合は失敗であると判定される。このとき、パスワードが不正確に入力されたことを示す情報がユーザに対して表示される。
【００３８】
この実施の形態では、設定情報だけでなく、設定情報に応じて得られる関連情報も生成でき、照合すべき情報が関連情報に属する場合、再度、照合される。キーボードのサイズが小さい、又は他の理由に起因するユーザの入力エラーの後に、照合のための機会をもう一度提供することにより、キーボードのサイズが小さいことに起因する入力エラーを減らし、入力効果を高めることができる。悪意のある入力エラーによる直接的な照合失敗とは異なるため、意図しないエラーと悪意のあるエラーとを効果的に判別し、意図しない入力エラーに起因する情報照合の失敗を減らすことができる。
【００３９】
図５は、本願の別の実施の形態による情報入力装置の概略構造図である。装置５０は、取得モジュール５１、第１の受信モジュール５２、照合モジュール５３、及び第２の受信モジュール５４を含む。
【００４０】
取得モジュール５１は、予め格納された情報を取得するように構成され、予め格納された情報は、プレーンテキストの第１の情報又は暗号化された第１の情報を含み、第１の情報は、設定情報及び設定情報に応じて生成された関連情報を含む。
この実施の形態の方法は、例えば、パスワード照合、ＩＤカード番号照合、銀行カード番号照合、携帯電話番号照合など、様々なシナリオにおける情報照合に用いることができる。この実施の形態では、パスワード照合を例に取り上げる。
【００４１】
パスワード照合の前に、ユーザは、パスワードを予め設定できる。例えば、パスワードがｘと設定される。当然ながら、ユーザによって設定されるパスワードｘは、１つ以上の情報項目を含むことができ、各情報項目は数字や文字などであってもよい。
【００４２】
更に、パスワードが携帯電話端末に格納される場合を例に取ると、パスワードは、携帯電話端末に、プレーンテキストの形で、例えば、ｘとしてそのまま格納されてもよい。或いは、セキュリティを強化するために、例えば、プレーンテキストのパスワードが格納前に暗号化され、暗号化されたｘが携帯電話端末に格納される。当然ながら、様々な暗号化アルゴリズムが存在するが、具体的には、例えばハッシュアルゴリズムである。この実施の形態では、携帯電話端末に格納されるハッシュ暗号化されたパスワードを例として取り上げる。ハッシュ暗号化後、ｘはＨ（ｘ）と表されるものとする。
【００４３】
従来技術では、予め格納される情報はせいぜいＨ（ｘ）であり、ユーザの入力がｘではない場合、照合は失敗である。
【００４４】
この実施の形態では、Ｈ（ｘ）を格納できるだけでなく、ｘに応じて関連情報を得ることができ、関連情報に対するハッシュ暗号化後に得られる情報が更に携帯電話端末に格納される。
【００４５】
図６を参照し、装置５０は：
前記設定情報から情報項目をランダムに選択し、前記選択された情報項目に対応する新しい情報項目を取得するように構成され、前記新しい情報項目の位置と前記選択された情報項目の位置との間のキーボード上での距離が予め設定された範囲内にあり；前記設定情

報の中の前記選択された情報項目を前記新しい情報項目に置き換えて前記関連情報を得る；ように構成された設定モジュール５５を更に備える。

【００４６】

例えば、ユーザが設定したパスワードｘの１つの項目（要素）がａである場合、仮想キーボード又は物理的キーボード上でａから短い距離にあるキャラクタが、ａに対応する新しいキャラクタとして選択される。新しいキャラクタをａ’で表すとすると、ａ’は、ａと置き換わって新しいパスワードｘ’を構成するために用いられる。新しいパスワードｘ’は、ｘの関連情報である。ハッシュ暗号化後、暗号化された関連情報は、Ｈ（ｘ’）、Ｈ（ｘ”）、・・・と表すことができ、この配列がＨ’として記録される。具体的には、例えば、ｘがａｂｃｄであり、ａから短い距離にあるキャラクタがａ’を含むとすると、ｘの関連情報はａ’ｂｃｄを含む。更に、ａから短い距離にあるキャラクタがａ”を更に含むとすると、ｘの関連情報はａ”ｂｃｄを更に含む。更に、ｂから短い距離にあるキャラクタがｂ’を含むとすると、ｘの関連情報はａｂ’ｃｄを更に含み、残りについても同様に処理され、その結果全ての関連情報を得ることができる。

【００４７】

当然ながら、上記の短い距離の具体的な意味は、実際の要求に従って設定できる。例えば、４個の隣り合うキーに対応するキャラクタを短い距離にあるキャラクタとして決定する、キー２個以下の距離にあるキャラクタ全てを短い距離にあるキャラクタとして決定する、などとしてもよい。

【００４８】

第１の受信モジュール５２は、照合すべき情報を受信するように構成され、ユーザは、照合すべき情報を、キーボードを介して入力できる。

例えば、ユーザは携帯電話の仮想キーボードを使用してパスワードなどを入力する。

【００４９】

照合モジュール５３は、予め格納された情報に従って、照合すべき情報を照合するように構成される。

携帯電話端末がプレーンテキストのパスワードをそのまま格納する場合、入力情報は予め格納された情報とそのまま比較することができ、それらが同じ場合、照合は成功となる。そうでない場合、照合は失敗となる。

【００５０】

この実施の形態では、暗号化された第１の情報を格納するステップを例に取り上げる。

前記予め格納された情報が前記暗号化された第１の情報である場合、前記照合モジュール５３は、具体的に：

前記第１の情報と同じ暗号化アルゴリズムを用いることにより前記照合すべき情報を暗号化して、暗号化された照合すべき情報を取得し；

前記暗号化された照合すべき情報を前記予め格納された情報と比較する；ように構成される。

【００５１】

ユーザが入力する照合すべき情報がｙであって、ハッシュ暗号化アルゴリズムが適用されるとすると、まずＨ（ｙ）を計算することができ、次いでＨ（ｙ）がＨ（ｘ）及びＨ’と比較される。

【００５２】

第２の受信モジュール５４は、前記照合すべき情報が前記関連情報に属する場合、再入力される照合すべき情報を受信するように構成される。

例えば、Ｈ（ｙ）がＨ’に属する場合、再入力される照合すべき情報を受信できる。その後に再度、照合される。

【００５３】

任意に、前記第２の受信モジュールは：

前記再入力される照合すべき情報が受信される前に、ユーザに対し、前記ユーザがキーボードのキーに注意を向けるように促すために用いられるプロンプト情報を表示する；又

は、
前記再入力される照合すべき情報が受信された後に、前記再入力される照合すべき情報のプレーンテキスト表示時間を延長する；又は、
前記再入力される照合すべき情報が受信された後に、前記再入力される照合すべき情報をプレーンテキストでそのまま表示する；ように更に構成される。
【００５４】
例えば、ユーザが、関連情報に属するｙを入力した場合、これは、小さなキーサイズゆえの、ユーザの意図しない入力エラーが原因である可能性が極めて高い。このとき、ユーザはキーボードに注意を向けるよう促され、それによりキーボードのサイズが小さいことによる入力エラーを回避できる。或いは、記号＊などの非プレーンテキスト情報がパスワード照合の際に最終的に表示されるのが通常であり、記号＊が表示される前に、ユーザが入力したプレーンテキスト情報が短時間表示されてもよい。
【００５５】
この実施の形態において、プレーンテキスト表示時間を延長する場合、照合すべき情報の中の各情報項目のプレーンテキスト表示時間を延長してもよく、或いは、前回不正確に入力された情報項目のプレーンテキスト表示時間のみが延長される。例えば、照合すべき情報がａｂｃｄであって、ａの最初の検出時にエラーが発生した場合、ａのプレーンテキスト表示時間のみを延長してもよく、ａ、ｂ、ｃ、及びｄのプレーンテキスト表示時間を全て延長してもよい。加えて、プレーンテキストを表示する際にも、同様に実行してもよい。例えば、前回不正確に入力された情報項目のみをプレーンテキストで表示する、又は情報項目全てをプレーンテキストで表示する。
【００５６】
この実施の形態では、プレーンテキスト入力情報を表示する時間を延長することができ、その結果、ユーザは自ら入力した情報をよく見て情報が正しく入力されたか否かを照合できる。具体的な延長時間を設定してもよい。或いは、入力情報をプレーンテキストでそのまま表示することによりユーザのチェックを容易にする。
【００５７】
図６を参照し、装置５０は：
前記照合すべき情報が前記設定情報と同じである場合、前記照合が成功であると判定する；又は、前記照合すべき情報が前記設定情報と異なり、かつ前記関連情報に属していない場合、前記照合が失敗であると判定する；ように構成された判定モジュール５６を更に備える。
【００５８】
例えば、ハッシュ暗号化後に得られた値が格納され、ユーザによって入力された照合すべき情報がｙである場合、ｙは、ハッシュ値に変換されてＨ（ｙ）が得られ、Ｈ（ｙ）がＨ（ｘ）と同じ場合、照合は成功である。
【００５９】
例えば、Ｈ（ｙ）がＨ（ｘ）と異なり、かつＨ（ｙ）がＨ’に属していない場合、照合は失敗であると判定される。このとき、パスワードが不正確に入力されたことを示す情報がユーザに対して表示される。
【００６０】
この実施の形態では、設定情報だけでなく、設定情報に応じて得られる関連情報も生成でき、照合すべき情報が関連情報に属する場合、再度、照合される。キーボードのサイズが小さい、又は他の理由に起因するユーザの入力エラーの後に、照合のための機会をもう一度提供することにより、キーボードのサイズが小さいことに起因する入力エラーを減らし、入力効果を高めることができる。悪意のある入力エラーによる直接的な照合失敗とは異なるため、意図しないエラーと悪意のあるエラーとを効果的に判別し、意図しない入力エラーに起因する情報照合の失敗を減らすことができる。
【００６１】
なお、本願の記載において、「第１の」及び「第２の」という用語は、単に説明目的に

用いるに過ぎず、相対的重要性を示したり、それを含意したりするものと解釈することはできない。加えて、本願の記載において、「多数の」とは、特別の定めがない限り、２以上を意味する。

【００６２】

本明細書において、フローチャートに記載する又は他の何らかの方法で記載する任意の工程又は方法は、特定の論理機能又は工程ステップを実現する実行可能な指令コードのための１つ以上のモジュール、セグメント、又は部分を含むものと理解できる。加えて、本願の好ましい実施の形態は、関連する機能に基づき、実質的に同時又は逆順も含め、図示又は検討したものとは異なる順序で機能を実行できる他の実施を含む。これは、本願の実施の形態が属する技術の当業者にとっては言うまでもない。

【００６３】

当然のことであるが、本願の各部分は、ハードウェア、ソフトウェア、ファームウェア、又はそれらの組合せによって実現できる。上記の実施の形態において、複数のステップ又は方法を、メモリに格納され、適切な指令実行システムにより実行されるソフトウェア又はファームウェアによって実施することができる。例えば、ハードウェアによって実施される場合、別の実施の形態と同様に、ステップ又は方法は、当技術分野で公知の以下の技法の１つ又は組合せによって実施できる：データ信号の論理機能を実現するための論理ゲート回路を有する離散ロジック回路、適切な論理ゲート回路の組合せを有する特定用途向け集積回路、プログラマブルゲートアレイ（ＰＧＡ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）など。

【００６４】

当業者は、上記の実施の形態の方法におけるステップの全て又は一部は、プログラムを具備する関連ハードウェアに命令することにより達成可能であることが分かる。プログラムは、コンピュータ読み取り可能な記録媒体に格納でき、プログラムは、実行時は、方法の実施の形態におけるステップの１つ又は組合せを含む。

【００６５】

加えて、本願の実施の形態における機能ユニットは、処理モジュールに統合されてもよく、ユニットが物理的に別々に提供されてもよく、２つ以上のユニットが１つのモジュールに統合されていてもよい。統合モジュールは、ハードウェアの形態で、またはソフトウェア機能モジュールの形態で実現されてもよい。統合モジュールがソフトウェア機能モジュールの形態で実現され、スタンドアロン製品として販売または用いられる場合、統合モジュールは、コンピュータ読み取り可能な記録媒体に格納されてもよい。

【００６６】

記憶媒体は、読み取り専用メモリ、磁気ディスク、ＣＤなどであってもよい。

【００６７】

本明細書を通じ、「実施の形態」、「一部の実施の形態」、「例」、「具体例」又は「一部の例」への言及は、かかる実施の形態又は例に関連し記載される特定の特徴、構造、材料、又は特性が、本願の少なくとも一の実施の形態又は例に含まれることを意味する。本明細書を通じ、これらの用語の例示的表現は、必ずしも同じ実施の形態又は例を指しているわけではない。更に、特定の特徴、構造、材料、又は特性を１つ以上の実施の形態又は例において任意適切な方法で組み合わせてもよい。

【００６８】

以上、本願の実施の形態を示し説明したが、上記の実施の形態は例示であって、本願を限定するものではなく、当業者であれば、本願の範囲内において実施の形態に変更、変形、代替、及び改変を行うことができる。

【図１】

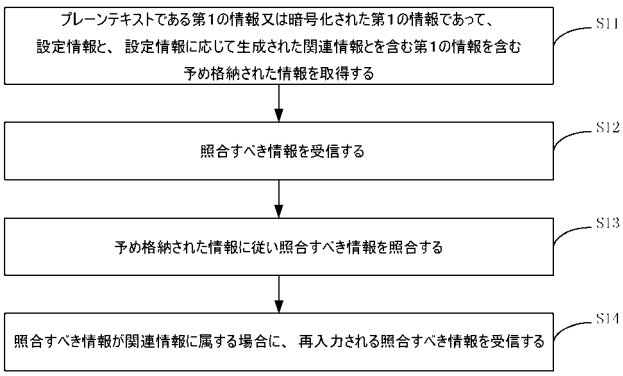

図1

【図２】

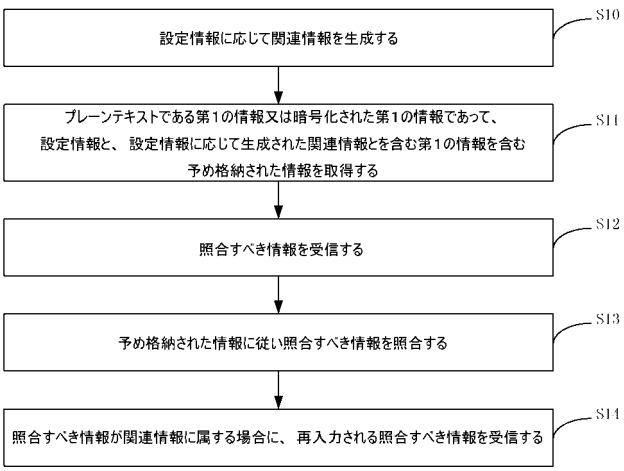

図2

【図３】

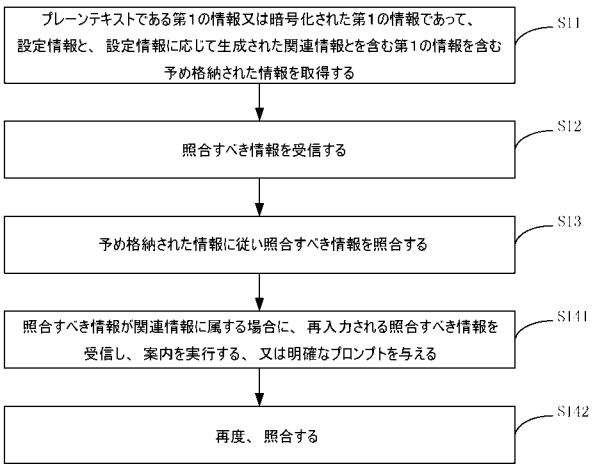

図3

【図４】

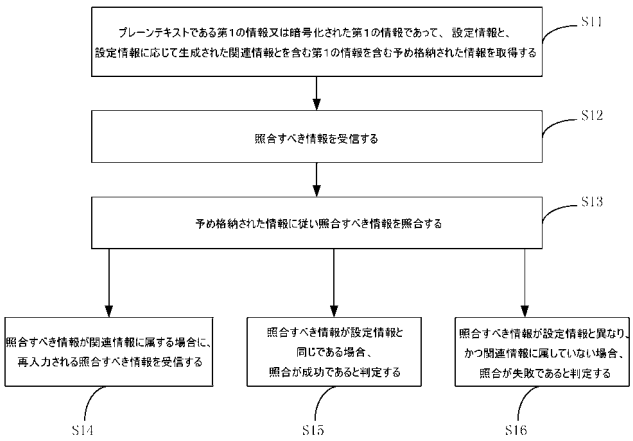

図4

【図５】

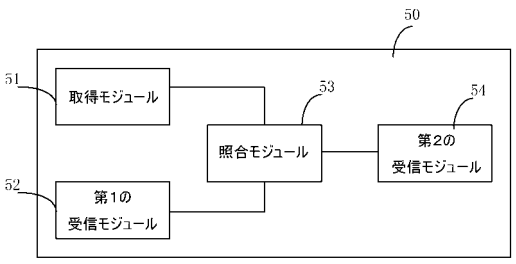

図5

【図６】

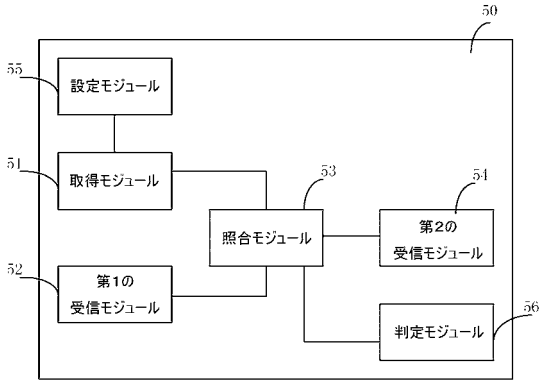
50
55
設定モジュール
51
取得モジュール
53
照合モジュール
54
第2の
受信モジュール
52
第1の
受信モジュール
56
判定モジュール

図6

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/080440

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/31 (2013.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

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

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

CNPAT; CNKI; WPI; EPODOC: second time, again, authenticat+, validat+, password, display, clew, hint, stor+, keyboard, character ??, second, error, incorrect

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104331668 A (XIAOMI TECHNOLOGY CO., LTD.), 04 February 2015 (04.02.2015), description, pages 9 and 10, and claims 1-3	1-2, 4-8, 10-11
A	US 8006096 B2 (KONICA MINOLTA BUSINESS TECH), 23 August 2011 (23.08.2011), the whole document	1-11
A	CN 103810414 A (INTERNATIONAL BUSINESS MACHINES CORPORATION), 21 May 2014 (21.05.2014), the whole document	1-11

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 June 2016 (13.06.2016)	**17 August 2016 (17.08.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **LIU, Huan** Telephone No.: (86-10) **62411853**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/080440

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104331668 A	04 February 2015	None	
US 8006096 B2	23 August 2011	US 2007101150 A1	03 May 2007
		JP 4332803 B2	16 September 2009
		JP 2007128201 A	24 May 2007
CN 103810414 A	21 May 2014	US 2014129974 A1	08 May 2014

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号
PCT/CN2016/080440

A. 主题的分类

G06F 21/31(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT；CNKI；WPI；EPODOC：验证，密码，显示，提示，存储，保存，键盘，字符，第二次，再次，错误，authenticat+，validat+，password，display，clew，hint，stor+，keyboard，character？？，second，error，incorrect

C. 相关文件

类型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 104331668 A (小米科技有限责任公司) 2015年 2月 4日 (2015-02-04) 说明书第9-10页、权利要求1-3	1-2，4-8，10-11
A	US 8006096 B2 (KONICA MINOLTA BUSINESS TECH) 2011年 8月 23日 (2011-08-23) 全文	1-11
A	CN 103810414 A (国际商业机器公司) 2014年 5月 21日 (2014-05-21) 全文	1-11

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 6月 13日	2016年 8月 17日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 刘欢 电话号码 (86-10)62411853

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/080440

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104331668	A	2015年2月4日	无			
US	8006096	B2	2011年8月23日	US	2007101150	A1	2007年5月3日
				JP	4332803	B2	2009年9月16日
				JP	2007128201	A	2007年5月24日
CN	103810414	A	2014年5月21日	US	2014129974	A1	2014年5月8日

表 PCT/ISA/210 (同族专利附件) (2009年7月)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(72)発明者 ファ，ヨン
中華人民共和国 ３１００９９，ハンヂョウ，ナンバー１８ ワンタン ロード，フアンロン タイムズ プラザ，ビルディング ビー １７エフ，アンツ パテント チーム内

Ｆターム(参考) 5B020 CC11 GG05 GG13 JJ03