

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6859513号
(P6859513)

(45) 発行日 令和3年4月14日 (2021.4.14)

(24) 登録日 令和3年3月30日 (2021.3.30)

(51) Int. Cl.	F I
H04L 9/32 (2006.01)	H04L 9/00 675B
G09C 1/00 (2006.01)	G09C 1/00 640D
G06F 21/64 (2013.01)	G06F 21/64

請求項の数 17 (全 25 頁)

(21) 出願番号 特願2019-543827 (P2019-543827)
 (86) (22) 出願日 平成30年2月14日 (2018.2.14)
 (65) 公表番号 特表2020-509674 (P2020-509674A)
 (43) 公表日 令和2年3月26日 (2020.3.26)
 (86) 国際出願番号 PCT/US2018/018157
 (87) 国際公開番号 W02018/152184
 (87) 国際公開日 平成30年8月23日 (2018.8.23)
 審査請求日 令和1年10月11日 (2019.10.11)
 (31) 優先権主張番号 201710078901.6
 (32) 優先日 平成29年2月14日 (2017.2.14)
 (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

早期審査対象出願

最終頁に続く

(54) 【発明の名称】 2次元コード生成の方法およびデバイス、ならびに2次元コード認識の方法およびデバイス

(57) 【特許請求の範囲】

【請求項1】

第2のサーバを認証および登録するために、第1のサーバによって、前記第2のサーバから登録情報を受信するステップと、

前記登録情報が認証されている場合、前記第1のサーバによって、前記第2のサーバを登録するステップと、

前記第1のサーバによって、前記登録情報を保存するステップと、

二次元(2D)コードを生成するために、前記第1のサーバによって、前記第2のサーバからの要求を受信するステップであって、前記要求が、2Dコードに符号化されるべき情報を含む、ステップと、

前記2Dコードを生成するために、前記第1のサーバによって、前記第2のサーバからの前記要求を受信したことに応答して、

前記第2のサーバが前記第1のサーバに登録されていることを、前記第1のサーバによって判定するステップと、

前記第1のサーバによって、非対称暗号化を使用してデジタル署名を生成することによって、前記2Dコードに符号化されるべき前記情報をデジタル署名するステップと、

前記第1のサーバによって、前記第2のサーバによって前記2Dコードに符号化されるべき前記デジタル署名された情報を前記第2のサーバに送信するステップと、

前記2Dコードがユーザコンピューティングデバイスによって走査された後に、前記2Dコードを解読するステップと、

10

20

前記2Dコードが走査されたことの記録を保存するステップであって、前記記録が、前記2Dコードを符号化する前記第2のサーバの識別情報を含み、前記2Dコードが前記デジタル署名された情報を悪用している別のサーバによって生成された場合には、前記記録が、前記別のサーバの識別情報を含む、ステップとを含む、
コンピュータで実行される方法。

【請求項2】

前記2Dコードが、前記デジタル署名を生成するサーバによって認証されたアプリケーションまたはソフトウェアを使用して走査される、
請求項1に記載のコンピュータで実行される方法。

【請求項3】

前記2Dコードに符号化されるべき前記情報をデジタル署名する前に、前記第2のサーバが登録されているかどうかを判定するステップをさらに含む、
請求項1に記載のコンピュータで実行される方法。

【請求項4】

前記デジタル署名が、前記非対称暗号化に基づいて秘密鍵を使用して生成される、
請求項1に記載のコンピュータで実行される方法。

【請求項5】

異なる秘密鍵が、前記2Dコードに符号化されるべき異なる情報に基づいて、異なるデジタル署名を生成するために使用される、
請求項4に記載のコンピュータで実行される方法。

【請求項6】

前記非対称暗号化が、リベスト-シャミア-エーデルマン(RSA)アルゴリズムを使用することによって実行される、
請求項4に記載のコンピュータで実行される方法。

【請求項7】

以下の動作を実行するために、コンピュータシステムによって実行可能な1つまたは複数の命令を記憶している非一時的コンピュータ可読媒体であって、前記動作が、
第1のサーバによって、第2のサーバを認証および登録するために、前記第2のサーバから登録情報を受信するステップと、
前記登録情報が認証されている場合、前記第1のサーバによって、前記第2のサーバを登録するステップと、
前記第1のサーバによって、前記登録情報を保存するステップと、
二次元(2D)コードを生成するために、前記第1のサーバによって、前記第2のサーバからの要求を受信するステップであって、前記要求が、2Dコードに符号化されるべき情報を含む、ステップと、
前記2Dコードを生成するために、前記第1のサーバによって、前記第2のサーバからの前記要求を受信したことに応答して、
前記第2のサーバが前記第1のサーバに登録されていることを、前記第1のサーバによって判定するステップと、
前記第1のサーバによって、非対称暗号化を使用してデジタル署名を生成することによって、前記2Dコードに符号化されるべき前記情報をデジタル署名するステップと、
前記第1のサーバによって、前記第2のサーバによって前記2Dコードに符号化されるべき前記デジタル署名された情報を前記第2のサーバに送信するステップと、
前記2Dコードがユーザコンピューティングデバイスによって走査された後に、前記2Dコードを解読するステップと、
前記2Dコードが走査されたことの記録を保存するステップであって、前記記録が、前記2Dコードを符号化する前記第2のサーバの識別情報を含み、前記2Dコードが前記デジタル署名された情報を悪用している別のサーバによって生成された場合には、前記記録が、前記別のサーバの識別情報を含む、ステップとを含む、
非一時的コンピュータ可読媒体。

10

20

30

40

50

【請求項 8】

前記2Dコードが、前記デジタル署名を生成するサーバによって認証されたアプリケーションまたはソフトウェアを使用して走査される、
請求項 7 に記載の非一時的コンピュータ可読媒体。

【請求項 9】

前記動作が、
前記2Dコードに符号化されるべき前記情報をデジタル署名する前に、前記第2のサーバが登録されているかどうかを判定するステップをさらに含む、
請求項 7 に記載の非一時的コンピュータ可読媒体。

【請求項 10】

前記デジタル署名が、前記非対称暗号化に基づいて秘密鍵を使用して生成される、
請求項 7 に記載の非一時的コンピュータ可読媒体。

【請求項 11】

異なる秘密鍵が、前記2Dコードに符号化されるべき異なる情報に基づいて、異なるデジタル署名を生成するために使用される、
請求項 10 に記載の非一時的コンピュータ可読媒体。

【請求項 12】

前記非対称暗号化が、リベスト-シャミア-エーデルマン(RSA)アルゴリズムを使用することによって実行される、
請求項 10 に記載の非一時的コンピュータ可読媒体。

【請求項 13】

1つまたは複数のコンピュータと、
前記1つまたは複数のコンピュータと相互動作可能に結合し、かつ以下の動作を実行するための1つまたは複数の命令を記憶している有形の非一時的マシン可読媒体を有する1つまたは複数のコンピュータメモリデバイスとを備える、

コンピュータで実装されるシステムであって、前記動作が、
第2のサーバを認証および登録するために、第1のサーバによって、前記第2のサーバから登録情報を受信するステップと、

前記登録情報が認証されている場合、前記第1のサーバによって、前記第2のサーバを登録するステップと、

前記第1のサーバによって、前記登録情報を保存するステップと、
二次元(2D)コードを生成するために、前記第1のサーバによって、前記第2のサーバからの要求を受信するステップであって、前記要求が、2Dコードに符号化されるべき情報を含む、ステップと、

前記2Dコードを生成するために、前記第1のサーバによって、前記第2のサーバからの前記要求を受信したことに応答して、

前記第2のサーバが前記第1のサーバに登録されていることを、前記第1のサーバによって判定するステップと、

前記第1のサーバによって、非対称暗号化を使用してデジタル署名を生成することによって、前記2Dコードに符号化されるべき前記情報をデジタル署名するステップと、

前記第1のサーバによって、前記第2のサーバによって前記2Dコードに符号化されるべき前記デジタル署名された情報を前記第2のサーバに送信するステップと、

前記2Dコードがユーザコンピューティングデバイスによって走査された後に、前記2Dコードを解読するステップと、

前記2Dコードが走査されたことの記録を保存するステップと、前記記録が、前記2Dコードを符号化する前記第2のサーバの識別情報を含み、前記2Dコードが前記デジタル署名された情報を悪用している別のサーバによって生成された場合には、前記記録が、前記別のサーバの識別情報を含む、ステップとを含む、

コンピュータで実装されるシステム。

【請求項 14】

前記2Dコードが、前記デジタル署名を生成するサーバによって認証されたアプリケーションまたはソフトウェアを使用して走査される、

請求項13に記載のコンピュータで実装されるシステム。

【請求項15】

前記動作が、

前記2Dコードに符号化されるべき前記情報をデジタル署名する前に、前記第2のサーバが登録されているかどうかを判定するステップをさらに含む、

請求項13に記載のコンピュータで実装されるシステム。

【請求項16】

前記デジタル署名が、前記非対称暗号化に基づいて秘密鍵を使用して生成される、

請求項13に記載のコンピュータで実装されるシステム。

【請求項17】

異なる秘密鍵が、前記2Dコードに符号化されるべき異なる情報に基づいて、異なるデジタル署名を生成するために使用される、

請求項16に記載のコンピュータで実装されるシステム。

【発明の詳細な説明】

【技術分野】

【0001】

優先権の主張

本出願は、その内容の全体が参照により本明細書に組み込まれている、2017年2月14日に
出願した中国特許出願第201710078901.6号の優先権を主張するものである。

【0002】

本出願は、グラフィック画像技術の分野に関し、より詳細には、2次元コード生成の方法
およびデバイス、ならびに2次元コード認識の方法およびデバイスに関する。

【背景技術】

【0003】

2次元バーコードとしても知られている2次元コードは、特定の規則に従って、(2次元方
向に)平面上に分散された特定のタイプの幾何グラフによって形成されたバー/空間交互グ
ラフ(bar/space alternating graph)を使用することによって、データシンボル情報を記
録する。2次元コードは、大きな情報容量、広いコーディング範囲、強いエラー耐性、お
よび高い復号信頼性などの特徴を有し、低コストおよび容易な製造などの利点をさらに有
する。したがって、2次元コードは、人々の生活において広く適用されている。

【0004】

インターネットの発展およびモバイル端末の普及に伴い、2次元コードは、日常生活に
おいてあらゆる場所で目にすることができる。たとえば、商人は、チェックアウト時に支
払い2次元コードを掲示することができ、ユーザは、アプリケーション内の2次元コード走
査機能を使用することによって、支払い2次元コードを走査することができる。または、
商品促進の場合、商人は、比較的混雑した場所(地下鉄またはショッピングモールなど)
において2次元コードをダウンロードするアプリを掲示して、2次元コードを走査してアプリ
ケーションをダウンロードするように通行人を引き付けることができる。したがって、商
人または第三者は、真正の、有効な2次元コードをユーザに提供する必要があり、ユーザ
は、これらの2次元コードを効果的に検証する必要がある。

【0005】

先行技術を研究および実施するとき、本発明の発明者は、人々が肉眼で2次元コードの
真正性を判断することは困難であり、2次元コード認識の間に、モバイルフォンアプリケ
ーション内の走査ユニットは、何の検証もなしに、様々な2次元コードを直接認識するこ
とになることを見出した。2次元コードの真正性および2次元コードの有効性を保証するよ
うに2次元コードを生成するための技術的解決策が現在要求されており、対応して、2次元
コードの認識の間に2次元コードの真正性を判断するための技術的解決策も要求されてい
ることが分かる。

10

20

30

40

50

【 0 0 0 6 】

上記の情報は、本開示の理解を促すための背景情報として単に提示されている。上記の情報のいずれも、本開示に対する先行技術として適用され得るかどうかはまだ決断または言明されていない。

【 発明の概要 】

【 課題を解決するための手段 】

【 0 0 0 7 】

本発明の主な目的は、前述の問題を解決するために、2次元コード生成の方法およびデバイス、ならびに2次元コード認識の方法およびデバイスを提供することである。

【 0 0 0 8 】

本発明の一態様は、第1のサーバが2次元コード生成要求を第2のサーバに送信するステップであって、要求が、2次元コードを生成するための情報を含む、ステップと、第2のサーバが、受信された2次元コード生成要求に従って、2次元コードを生成するための情報にデジタル署名するステップと、デジタル署名を含む2次元コード情報を第1のサーバに送信するステップと、第1のサーバが、2次元コード情報を使用することによって、2次元コードを生成するステップとを含む、2次元コード生成方法を提供する。

【 0 0 0 9 】

本発明の一態様は、2次元コード生成方法を提供し、この方法は、第1のサーバによって実行され、2次元コード生成要求を第2のサーバに送信するステップであって、要求が、2次元コードを生成するための情報を含む、ステップと、第2のサーバによって生成されたデジタル署名を含む2次元コード情報を第2のサーバから受信するステップと、2次元コード情報を使用することによって、2次元コードを生成するステップとを含む。

【 0 0 1 0 】

本発明の一態様は、2次元コード生成要求を第2のサーバに送信するように構成された送信ユニットであって、要求が、2次元コードを生成するための情報を含む、送信ユニットと、第2のサーバによって生成されたデジタル署名を含む2次元コード情報を第2のサーバから受信するように構成された受信ユニットと、2次元コード情報を使用することによって2次元コードを生成するように構成された生成ユニットとを含む、2次元コード生成デバイスを提供する。

【 0 0 1 1 】

本発明の一態様は、2次元コード生成方法を提供し、この方法は、第2のサーバによって実行され、2次元コード生成要求を第1のサーバから受信するステップであって、要求が、2次元コードを生成するための情報を含む、ステップと、2次元コードを生成するための情報にデジタル署名を行うステップと、デジタル署名を含む2次元コード情報を第1のサーバに送信するステップとを含む。

【 0 0 1 2 】

本発明の一態様は、2次元コード生成要求を第1のサーバから受信するように構成された受信ユニットであって、要求が、2次元コードを生成するための情報を含む、受信ユニットと、2次元コードを生成するための情報にデジタル署名を行うように構成された処理ユニットと、デジタル署名を含む2次元コード情報を第1のサーバに送信するように構成された送信ユニットを含む、2次元コード生成装置を提供する。

【 0 0 1 3 】

本発明の一態様は、2次元コード生成システムを提供する。このシステムは、第1のサーバと第2のサーバとを含む。第1のサーバは、2次元コード生成要求を第2のサーバに送信するように構成された送信ユニットであって、要求が、2次元コードを生成するための情報を含む、送信ユニットと、第1のサーバによって生成されたデジタル署名を含む2次元コード情報を第2のサーバから受信するように構成された受信ユニットと、2次元コード情報を使用することによって2次元コードを生成するように構成された生成ユニットとを含む。第2のサーバは、要求を第1のサーバから受信するように構成された受信ユニットと、2次元コードを生成するための情報にデジタル署名を行うように構成された処理ユニットと、

デジタル署名を含む2次元コード情報を第1のサーバに送信するように構成された送信ユニットを含む。

【0014】

本発明の別の態様は、2次元コードを生成するための情報にデジタル署名を行うサーバに対応するアプリケーションを開始するステップと、アプリケーション内の走査ユニットを使用することによって、2次元コードを走査するステップと、公開鍵を使用することによって、走査された2次元コードを検証するステップと、検証が成功した場合、走査された2次元コードに対応する情報を認識するステップとを含む、2次元コード認識方法を提供する。

【0015】

本発明の別の態様は、2次元コードを生成するための情報にデジタル署名を行うサーバに対応するアプリケーションを開始するように構成された開始ユニットと、アプリケーション内の走査ユニットを使用することによって、2次元コードを走査するように構成された走査ユニットと、公開鍵を使用することによって、走査された2次元コードを検証するように構成された検証ユニットと、検証ユニットによって実行された検証が成功した場合、走査された2次元コードに対応する情報を認識するように構成された認識ユニットとを含む、2次元コード認識デバイスを提供する。

【0016】

先行技術と比較して、本発明による実施形態では、2次元コードは、2次元コードのセキュリティおよび有効性が強化されるように、あるサーバと別のサーバとの間の相乗効果によって生成され、2次元コード認識プロセスにおいて、2次元コードが改ざんされているかどうかを認識することは好都合である。加えて、本発明の別の実施形態によれば、2次元コードに対応する情報は、公開鍵を使用することによって、真正性判断が2次元コード認識プロセスに追加され、2次元コードが改ざんされることを防ぐように、特定のアプリケーションを介して認識される。

【0017】

本明細書で説明する添付の図面は、本出願のさらなる理解を実現するために使用され、本出願の一部を構成する。本出願の概略実施形態およびその説明は、本出願を示すために使用され、本出願に対する不適切な限定を構成しない。添付の図面では、

【図面の簡単な説明】

【0018】

【図1】本発明の一実施形態による2次元コード生成方法が適用されるシナリオの図である。

【図2】図1に示したサーバ110とサーバ120との間の対話処理の概略図である。

【図3】本発明の一実施形態による、2次元コードの認識の概略図である。

【図4】本発明の一実施形態による、第1のサーバによって実行される2次元コード生成方法の流れ図である。

【図5】図4に示した2次元コード生成方法を実行する2次元コード生成デバイスのブロック図である。

【図6】本発明の一実施形態による、第2のサーバによって実行される2次元コード生成方法の流れ図である。

【図7】図6に示した2次元コード生成方法を実行する2次元コード生成デバイスのブロック図である。

【図8】本発明の一実施形態による2次元コード認識方法の流れ図である。

【図9】本発明の一実施形態による、図8に示した2次元コード認識方法を実行する2次元コード認識デバイスのブロック図である。

【図10】本発明の一実施形態による電子デバイスのブロック図である。

【図11】本開示の一実装形態による、2Dコードを生成するためのコンピュータ実装方法の一例を示す流れ図である。

【発明を実施するための形態】

【0019】

本出願の目的、技術的解決策、および利点をより分かりやすくするために、本出願の技術的解決策は、本出願の特定の実施形態および対応する図面を参照しながらさらに詳細に説明される。明らかに、説明する実施形態は、本出願の実施形態のすべてではなく、いくつかに過ぎない。創造的な取組みなしに当業者によって導出されるすべての他の実施形態は、本出願の保護範囲に属する。

【0020】

以下で、実施形態は、添付の図面を参照してさらに詳細に説明される。同一の参照番号は、同一要素を常に表す。本開示のより明瞭な理解のために、本開示に関する用語を以下で示す。

10

【0021】

端末/電子デバイスは、概して、ネットワークシステム内でユーザによって使用され、サーバと通信するように構成された装置を指す。本開示の一実施形態で提供される2次元コード生成方法は、2次元コード生成デバイスによって実行され得る。本開示の一実施形態で提供される2次元コード認識方法は、2次元コード認識デバイスによって実行され得る。2次元コード生成デバイスおよび2次元コード認識デバイスは、各々、端末/電子デバイスであってよい。本開示による端末/電子デバイスは、限定はしないが、ディスプレイユニットを有する以下のデバイス、すなわち、パーソナルコンピュータ(PC)、モバイル装置(セルラーフォン、携帯情報端末(PDA)、デジタルカメラ、ポータブルゲーム機、MP3プレーヤー、ポータブル/パーソナルマルチメディアプレーヤー(PMP)、ハンドヘルド電子ブック、タブレットPC、ポータブルラップトップPC、および全地球測位システム(GPS)ナビゲータなど)、スマートTVなどのうちのいずれかを含み得る。

20

【0022】

アプリケーション(アプリ)は、コンピュータオペレーティングシステム(OS)またはモバイルOS上でユーザによって直接実行され得るソフトウェアである。アプリケーションは、埋込み型アプリケーション、または端末の記憶ユニット内に記憶された第三者アプリケーションを含み得る。埋込み型アプリケーションは、端末内に事前にインストールされたアプリケーションを指す。たとえば、埋込み型アプリケーションは、ブラウザ、電子メール、またはインスタントメッセンジャーであってよい。第三者アプリケーションは、多様であり、オンラインマーケットからダウンロードされ、端末上にインストールされる以下のアプリケーション、たとえば、支払いアプリケーション、ショッピングアプリケーション、娯楽アプリケーションなどを指す。

30

【0023】

図1は、本発明の一実施形態による2次元コード生成方法が適用されるシナリオの図である。

【0024】

図1に示すように、サーバ110およびサーバ120は、ワイヤード様式またはワイヤレス様式で接続される。本開示の実施形態では、ワイヤレス接続は、Bluetooth(登録商標)および近距離通信(NFC)など、1対1ワイヤレス接続であってよく、セキュリティ保証されたシナリオでは、ワイヤレスローカルエリアネットワーク(WiFi)が使用されてもよいことを理解されたい。

40

【0025】

サーバ110は、2次元コードを生成するためのサーバである。たとえば、サーバ110は、アプリケーションサーバ、ウェブサイトサーバなどであってよい。たとえば、サーバ110が支払いアプリケーションサーバである場合、アプリケーションサーバ110は、ユーザ入力に応じて、商品に関する2次元コードを生成することができる。あるいは、サーバ110がウェブサイトサーバである場合、要件に従ってサーバ110によって生成される様々な2次元コードがディスプレイ上に表示され得る。サーバ120は、(Alipay(商標)サーバなど)許可証明を有する第三者サーバである。

【0026】

50

サーバ110とサーバ120は両方とも、コンピューティングサービスを提供する電子デバイスであり、サーバ要求に応答して、処理を実行することができることに留意されたい。その上、2つのサーバのアーキテクチャは、汎用コンピュータのアーキテクチャと同様である。本開示では、サーバ110およびサーバ120は、異なるサービスを提供する。

【0027】

図1を参照すると、サーバ110およびサーバ120は、対話処理を実行し、次いで、サーバ110は、サーバ120によって提供される情報に従って、2次元コードを生成する。これは、図2を参照しながら、下記でより詳細に説明され、したがって、ここでは説明しない。

【0028】

次に、サーバ110は、ディスプレイ上に2次元コードを表示するか、または出力デバイス(プリンタなど)を使用することによって、2次元コードを直接出力し得る。次いで、ユーザは、モバイル端末内の走査ユニットを使用することによって、2次元コードを走査することができる。

【0029】

サーバ110とサーバ120との間の対話処理は、図2を参照して下記で詳細に説明される。

【0030】

図2に示すように、ステップ210で、サーバ110は、2次元コード生成要求をサーバ120に送信する。この要求は、2次元コード(略して、2次元コード情報と呼ばれる)を生成するための情報を含み得る。たとえば、2次元コード情報は、支払先アカウント情報を含み得るか、または2次元コード情報は、ウェブサイト情報を含み得る。

【0031】

場合によっては、ステップ210を実行する前に、サーバ110は、登録要求をサーバ120に事前に送信する。登録要求は、現在の登録に関するすべての情報を含み得る。たとえば、サーバ110は、たとえば、営業証明、商品明細など、その様々な資格証明をサーバ120に提供し得る。次に、サーバ110によって提供された情報を首尾よく検証した後で、サーバ120は、サーバ110の登録を完了する。加えて、サーバ110によって提供された資格証明はサーバ120のメモリ内に記憶される。場合によっては、資格証明はリモートメモリ内に記憶されてもよい。このようにして、起動される必要があるとき、リモートメモリのアドレスを使用することによって、資格証明が起動される。

【0032】

このようにして、サーバ110が2次元コード生成要求をサーバ120に送信した後で、サーバ120は、サーバ110に対する検証を実行して、サーバ110がサーバ120内に登録されているかどうかを決定する。Noである場合、サーバ120は、後続のサービスを提供せず、登録を実行するようにサーバ110にリマインドする。具体的には、サーバ120は、サーバ110の2次元コード生成要求を拒否し、登録勧誘をサーバ110に送信する。サーバ110がサーバ120にすでに登録している場合、後続のステップが実行される。

【0033】

前述の登録ステップを通して、サーバ120は、検証を経たすべての装置に対してサービスを提供し、それによって、サーバ120によって相乗的に生成された2次元コードの有効性を保証し、サーバ110の商人との考えられる紛争において使用するための証拠を維持することができる。

【0034】

ステップ220で、サーバ120は、非対称暗号化アルゴリズムに基づいて、2次元コード情報にデジタル署名を行うことができる。具体的には、サーバ120は、非対称暗号化アルゴリズムに基づいて、事前に生成された秘密鍵(サーバ120内に記憶される)を使用することによって、ステップ210における2次元コード生成要求内の2次元コード情報にデジタル署名を行うことができる。このようにして、2次元コード認識プロセスにおいて、公開鍵を使用することによって2次元コードが首尾よく走査された場合、それは、2次元コードが、サーバ120を使用することによってサーバ110によって生成された2次元コードであることを示す。走査が失敗した場合、それは、2次元コードが、おそらく偽の2次元コードである

か、またはサーバ110によってのみ生成されたが、サーバ120を使用することによって処理されていない2次元コードであることを示す。

【0035】

サーバ120は、異なる2次元コード情報に従って、異なるデジタル署名を生成することに留意されたい。言い換えれば、サーバ120は、異なる2次元コード情報に従って異なる秘密鍵を提供することができ、次いで、それぞれの秘密鍵を使用することによって、異なる2次元コード情報にデジタル署名を行う。したがって、同じウェブサイトによって送信された異なる商品に関する異なるリンク情報に関してすら、異なる秘密鍵を使用することによって、異なるリンク情報に対してデジタル署名が行われる。

【0036】

前述の非対称暗号化アルゴリズムは、公開鍵暗号化アルゴリズムと呼ばれることがある。このアルゴリズムでは、データは、公開鍵を使用することによって暗号化され、対応する秘密鍵を使用することによってのみ解読され得る。あるいは、データは、秘密鍵を使用することによって暗号化され、対応する公開鍵を使用することによって解読される。例示的な実施形態によれば、非対称暗号化アルゴリズムは、RSA公開鍵暗号化アルゴリズム、Elgamal暗号化アルゴリズム、ナップサックアルゴリズム、および楕円曲線暗号(ECC:elliptic curve cryptography)暗号化アルゴリズムを含み得る。本開示の目的は、2次元コードの真正性および有効性を保証するためであることから、好ましくは、生成された取引データを暗号化するために、RSA公開鍵暗号化アルゴリズムが選択され得る。

【0037】

非対称暗号化アルゴリズムを使用することによってデータにデジタル署名を行うことは、本分野において一般的な技術的手段であるため、その詳細な説明は本明細書で省略される。非対称暗号化アルゴリズムの例が上記で提供されているが、デジタル署名を生成することができるすべての非対称暗号化アルゴリズムがここで適用可能であることを当業者は理解されたい。

【0038】

次に、ステップ230で、サーバ120は、デジタル署名を含む2次元コード情報をサーバ110に送信する。デジタル署名を含む2次元コード情報を受信した後で、ステップ240で、サーバ110は、デジタル署名を含む2次元コード情報を使用することによって、2次元コードを生成する。具体的には、2次元コードは、2次元コード生成アルゴリズムに基づいて、2次元コード情報ならびにデジタル署名を使用することによって、生成され得る。好ましくは、2次元コード生成アルゴリズムは、Quickresponseコード(QRコード(登録商標))アルゴリズムを含む。

【0039】

2次元コード生成アルゴリズムを使用することによって2次元コードを生成することは、本分野において一般的な技術的手段であるため、その詳細な説明は本明細書で省略される。2次元コードを生成することができるすべての2次元コード生成アルゴリズムがここで適用可能であることを当業者は理解されたい。

【0040】

次に、図3を参照して、2次元コードに対する検証の概略図について下記で詳細に説明する。

【0041】

図3に示すように、ユーザは、モバイル端末を使用することによって、ディスプレイ上に表示された電子2次元コード、または出力デバイスによって出力された2次元コードを検証することができる。

【0042】

ユーザは、サーバ120に対応するアプリケーションを開始することができる。たとえば、ユーザは、モバイル端末内で、Alipay(商標)サーバに対応するAlipay(商標)アプリケーションを開始することができる。その後、ユーザは、ディスプレイ上に表示された2次元コード、またはアプリケーション内の走査ユニットを使用することによって印刷された2

10

20

30

40

50

次元コードを走査する。

【0043】

2次元コード認識プロセスにおいて、サーバ120に対応するアプリケーションは、2次元コードに対応する公開鍵を含むか、またはその公開鍵を獲得することができるため、ユーザは、サーバ120に対応するアプリケーション内の走査ユニットを使用すべきであることに留意されたい。

【0044】

場合によっては、アプリケーション内の走査ユニットを使用することによって、2次元コードが走査された後で、公開鍵は、サーバ120、または公開鍵を記憶するリモート記憶デバイスから獲得され得る。その後、公開鍵を使用することによって、走査された2次元コードに対して検証が行われる。検証が成功した場合、次の動作を実行するために、2次元コードは首尾よく認識され得る。言い換えれば、2次元コードの認識結果に従って、2次元コードに対応する動作インターフェースがモバイル端末のディスプレイインターフェース上で表示され得る。たとえば、2次元コードの認識結果がAlipay(商標)に関するリンクである場合、モバイル端末は、Alipay(商標)アプリケーションを起動し、それによって、Alipay(商標)に関する動作インターフェースをディスプレイユニット上に表示する。2次元コードの認識結果がWeChatに関するリンクである場合、モバイル端末は、WeChatアプリケーションを起動し、それによって、WeChatに関する動作インターフェースをディスプレイユニット上に表示する。2次元コードの認識結果がウェブサイトに関するリンクである場合、モバイル端末は、ブラウザアプリケーションを起動し、それによって、ブラウザに関する動作インターフェースをディスプレイユニット上に表示する。

【0045】

検証が失敗した場合、それは、2次元コードが改ざんされていることを示す。加えて、このような事例も考えられる:2次元コードを改ざんしたオペレータもやはりサーバ120に登録しており、元の2次元コードを改ざんするための2次元コードもサーバ120によって相乗的に生成される。たとえば、商人Bが商人Aによって外に掲示された2次元コードを破棄し、その独自の2次元コードを掲示する。この場合、商人Bの2次元コードは、サーバ120に対応するアプリケーション内の走査ユニットを使用することによって首尾よく認識され得る。この問題を解決するために、前述の走査プロセスを記録することができる。このようにして、走査記録に従って、2次元コードを改ざんしたオペレータを判定することができ、登録の間にオペレータによって提供された情報に従って、オペレータの識別情報を判定することができる。

【0046】

図4は、本発明の一実施形態による、第1のサーバによって実行される2次元コード生成方法の流れ図である。

【0047】

ステップS410で、2次元コード生成要求を第2のサーバに送信し、要求は、2次元コードを生成するための情報を含む。

【0048】

ステップS420で、第2のサーバによって生成されたデジタル署名を含む2次元コード情報を第2のサーバから受信する。

【0049】

ステップS430で、2次元コード情報を使用することによって、2次元コードを生成する。

【0050】

代替実施形態では、2次元コード生成要求を第2のサーバに送信するステップの前に、この方法はさらに、登録要求を第2のサーバに送信するステップであって、登録要求が、現在の登録に関するすべての情報を含む、ステップを含む。

【0051】

図5は、図4に示した2次元コード生成方法を実行する2次元コード生成デバイス(すなわち、第1のサーバ)のブロック図である。

【 0 0 5 2 】

図5に示す2次元コード生成デバイスの構造は、本開示の電子デバイスを限定しないことを当業者は理解されよう。電子デバイスは、図に示す構成要素よりも多数のもしくは少数の構成要素を含んでよく、またはいくつかの構成要素が組み合わされてよく、または異なる構成要素レイアウトが採用されてもよい。

【 0 0 5 3 】

図5に示すように、2次元コード生成デバイスは、送信ユニット510と、受信ユニット520と、生成ユニット530とを含み得る。

【 0 0 5 4 】

送信ユニット510は、2次元コード生成要求を第2のサーバに送信するように構成可能であり、要求は、2次元コードを生成するための情報を含む。

10

【 0 0 5 5 】

受信ユニット520は、第2のサーバによって生成されたデジタル署名を含む2次元コード情報を第2のサーバから受信するように構成され得る。

【 0 0 5 6 】

生成ユニット530は、2次元コード情報を使用することによって、2次元コードを生成するように構成され得る。

【 0 0 5 7 】

代替実施形態では、送信ユニット510は、2次元コード生成要求を第1のサーバに送信する前に、登録要求を第1のサーバに送信するように構成され、登録要求は、現在の登録に関するすべての情報を含む。

20

【 0 0 5 8 】

図6は、本発明の一実施形態による、第2のサーバによって実行される2次元コード生成方法の流れ図である。

【 0 0 5 9 】

ステップS610で、2次元コード生成要求を第1のサーバから受信し、要求は、2次元コードを生成するための情報を含む。

【 0 0 6 0 】

ステップS620で、2次元コードを生成するための情報にデジタル署名を行う。

【 0 0 6 1 】

ステップS630で、デジタル署名を含む2次元コード情報を第1のサーバに送信する。

30

【 0 0 6 2 】

随意の実施形態では、2次元コード生成要求を第1のサーバから受信するステップの前に、この方法はさらに、登録要求を第1のサーバから受信するステップであって、登録要求が、現在の登録に関するすべての情報を含む、ステップを含む。その上、登録要求を第1のサーバから受信するステップの後で、2次元コード生成方法はさらに、登録要求に従って、第1のサーバの登録を完了するステップを含み得る。

【 0 0 6 3 】

図7は、図6に示した2次元コード生成方法を実行する2次元コード生成デバイス(すなわち、第2のサーバ)のブロック図である。

40

【 0 0 6 4 】

図7に示す2次元コード生成デバイスの構造は、本開示の電子デバイスを限定しないことを当業者は理解されよう。電子デバイスは、図に示す構成要素よりも多数のもしくは少数の構成要素を含んでよく、またはいくつかの構成要素が組み合わされてよく、または異なる構成要素レイアウトが採用されてもよい。

【 0 0 6 5 】

2次元コード生成デバイスは、受信ユニット710と、処理ユニット720と、送信ユニット730とを含み得る。

【 0 0 6 6 】

受信ユニット710は、2次元コード生成要求を第1のサーバから受信するように構成され

50

、要求は、2次元コードを生成するための情報を含む。代替実施形態では、受信ユニットは、登録要求を第1のサーバから受信するようにさらに構成され、登録要求は、現在の登録に関するすべての情報を含む。

【0067】

代替実施形態では、2次元コード生成デバイスは、登録ユニットを含むことができ、登録ユニットは、登録要求に従って、第1のサーバの登録を完了するように構成される。

【0068】

処理ユニット720は、2次元コードを生成するための情報にデジタル署名を行うように構成される。場合によっては、処理ユニット720は、非対称暗号化アルゴリズムに基づいて、秘密鍵を使用することによって、2次元コードを生成するための情報にデジタル署名を行うように構成され得る。

10

【0069】

送信ユニット730は、デジタル署名を含む2次元コード情報を第1のサーバに送信するように構成される。

【0070】

代替実施形態では、2次元コード生成デバイスは、判定ユニットをさらに含む。判定ユニットは、第1のサーバが第2のサーバに登録されているかどうかを判定するように構成される。Yesである場合、受信された2次元コード生成要求に従って、2次元コードを生成するための情報にデジタル署名を行う。Noである場合、2次元コードを生成するための情報に対してデジタル署名は行われず、登録勧誘が第1のサーバに送信される。

20

【0071】

代替実施形態では、2次元コードを生成するための異なる情報に従って、2次元コードを生成するための情報にデジタル署名を行うステップにおいて、異なる秘密鍵が使用される。

【0072】

別の例示的な実施形態では、2次元コード生成システムが提供され得る。このシステムは、図5に示したような2次元コード生成デバイスと、図7に示したような2次元コード生成デバイスとを含む。

【0073】

上記で説明したように、本開示の実施形態で提供される2次元コード生成の方法およびデバイスに従って、2次元コードのセキュリティおよび有効性が強化されるように、2次元コードは、あるサーバと別のサーバとの間の相乗効果によって生成され、2次元コード認識プロセスにおいて、2次元コードが改ざんされているかどうかを認識することは好都合である。

30

【0074】

図8は、本発明の一実施形態による2次元コード認識方法の流れ図である。

【0075】

ステップS810で、2次元コードを生成するための情報にデジタル署名を行うサーバに対応するアプリケーションを開始する。

【0076】

40

ステップS820で、アプリケーション内の走査ユニットを使用することによって、2次元コードを走査する。

【0077】

ステップS830で、公開鍵を使用することによって、走査された2次元コードを検証する。

【0078】

ステップS840で、検証が成功した場合、走査された2次元コードに対応する情報を認識する。

【0079】

代替実施形態では、公開鍵は、サーバまたはリモート記憶デバイスから取得される。加

50

えて、この方法は、検証ステップにおいて関連情報を記憶するステップをさらに含み得る。

【0080】

図9は、本発明の一実施形態による、図8に示した2次元コード認識方法を実行する2次元コード認識デバイスのブロック図である。

【0081】

図9に示す2次元コード認識デバイスの構造は、本開示の電子デバイスを限定しないことを当業者は理解されよう。電子デバイスは、図に示す構成要素よりも多数のもしくは少数の構成要素を含んでよく、またはいくつかの構成要素が組み合わされてよく、または異なる構成要素レイアウトが採用されてもよい。

10

【0082】

2次元コード認識デバイスは、開始ユニット910と、走査ユニット920と、検証ユニット930と、認識ユニット940とを含む。

【0083】

開始ユニット910は、2次元コードを生成するための情報にデジタル署名を行うサーバに対応するアプリケーションを開始するように構成され得る。

【0084】

走査ユニット920は、アプリケーション内の走査ユニットを使用することによって、2次元コードを走査するように構成され得る。

【0085】

20

検証ユニット930は、公開鍵を使用することによって、走査された2次元コードを検証するように構成され得る。

【0086】

認識ユニット940は、検証ユニットによって実行された検証が成功した場合、走査された2次元コードに対応する情報を認識するように構成され得る。

【0087】

代替実施形態では、公開鍵は、サーバまたはリモート記憶デバイスから取得される。

【0088】

代替実施形態では、2次元コード認識デバイスは、記憶ユニットをさらに含み、記憶ユニットは、検証ステップにおいて関連する情報を記憶するように構成される。

30

【0089】

図10は、本開示の実施形態による、2次元コード生成方法または2次元コード認識方法を実行する電子デバイスのブロック図である。図10を参照すると、ハードウェアレベルで、電子デバイスは、プロセッサと、内部バスと、ネットワークインターフェースと、メモリと、不揮発性記憶装置とを含む。明らかに、電子デバイスは、サービスが必要とする他のハードウェアをさらに含み得る。プロセッサは、対応するコンピュータプログラムを不揮発性記憶装置からメモリ内に読み取り、コンピュータプログラムを実行して、論理レベルでウェブページスクリーンショット装置を形成する。明らかに、ソフトウェア実装形態に加えて、本出願は、論理デバイスまたはソフトウェアとハードウェアとを組み合わせた様式など、他の実装形態を除外しない。言い換えれば、以下の処理手順は、様々な論理ユニットによって実行されると限定されず、ハードウェアデバイスまたは論理デバイスによって実行されてもよい。

40

【0090】

本開示の実施形態に従って提供される2次元コード認識の方法およびデバイスは、特定のアプリケーションを介して、公開鍵を使用することによって2次元コードに対応する情報を認識し、これにより、2次元コード認識プロセスにおいて真正性判断を加え、2次元コードが改ざんされるのを防ぐ。

【0091】

1990年代には、技術の改善は、ハードウェアに対する改善(たとえば、ダイオード、トランジスタ、およびスイッチなどの回路構造に対する改善)またはソフトウェアに対する

50

改善(方法手順に対する改善)としてはっきりと区別することが可能であった。しかしながら、技術の発展に伴い、現在、多くの方法手順の改善は、ハードウェア回路構造の直接的な改善と見なされ得る。ほぼすべての設計者は、対応するハードウェア回路構造を取得するために、改善された方法手順をハードウェア回路内にプログラムする。したがって、ハードウェアエンティティモジュールを使用することによって、方法手順の改善を実装することはできないと見なすことは適切でない。たとえば、プログラマブル論理デバイス(PLD)(たとえば、フィールドプログラマブルゲートアレイ(FPGA))は、その論理機能がユーザによってプログラムされたデバイスによって判定される、そのような集積回路である。設計者は、専用の集積回路チップを設計および製造することをチップ製造会社に要求する必要なしに、デジタルシステムを単一のPLD内に「統合する」ために自らプログラミングを実行する。その上、現在、集積回路チップを手動で製造する代わりに、プログラミングはほとんど、「論理コンパイラ」ソフトウェアを使用することによって実装される。論理コンパイラソフトウェアは、プログラムを開発および書き込むために使用されるソフトウェアコンパイラと同様であり、コンパイル前の元のコードも、ハードウェア記述言語(HDL)と呼ばれる特定のプログラミング言語によって書き込まれる。Advanced Boolean Expression Language(ABEL)、Altera Hardware Description Language(AHDL)、Confluence、Cornell University Programming Language(CUPL)、HDCal、Java(登録商標) Hardware Description Language(JHDL)、Lava、Lola、MyHDL、PALASM、およびRuby Hardware Description Language(RHDL)など、多くのタイプのHDLが存在し、その中で、現在、Very-High-Speed Integrated Circuit Hardware Description Language(VHDL)およびVerilogが最も一般的に使用されている。上記のいくつかのハードウェア記述言語を使用して方法手順を若干論理的にプログラムし、その方法手順を集積回路内にプログラムすることによって、論理方法手順を実装するためのハードウェア回路を容易に取得することができることを当業者はやはり理解されたい。

【0092】

コントローラは、任意の適切な方法で実装され得る。たとえば、コントローラは、たとえば、マイクロプロセッサもしくはプロセッサ、および(マイクロ)プロセッサ、論理ゲート、スイッチ、特定用途向け集積回路(ASIC)、プログラマブル論理コントローラ、および埋込み型マイクロコントローラによって実行可能なコンピュータ可読プログラムコード(たとえば、ソフトウェアまたはファームウェア)を記憶するコンピュータ可読媒体の形式であってよい。コントローラの例は、限定はしないが、以下のマイクロコントローラ:すなわち、ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20、およびSilicone Labs C8051F320を含む。メモリコントローラは、メモリの制御論理の一部として実装されてもよい。当業者はまた、コントローラは、純粋なコンピュータ可読プログラムコードを使用することによって実装可能であり、加えて、これらの方法ステップは、コントローラが、論理ゲート、スイッチ、特定用途向け集積回路、プログラマブル論理コントローラ、埋込み型マイクロコントローラなどの形式で同じ機能を実装することを可能にするように論理的にプログラムされ得ることを理解している。したがって、このタイプのコントローラは、ハードウェア構成要素と見なされてよく、様々な機能を実装するためにその中に含まれる装置は、ハードウェア構成要素内の構造と見なされてもよい。または、様々な機能を実装するために使用される装置はさらに、この方法を実装するためのソフトウェアモジュールと、ハードウェア構成要素内の構造の両方と見なされてもよい。

【0093】

上記の実施形態に示したシステム、装置、モジュール、またはユニットは、具体的には、コンピュータチップもしくはエンティティ、または一定の機能を有する製品を使用することによって実装され得る。典型的な実装デバイスはコンピュータである。具体的には、コンピュータは、たとえば、パーソナルコンピュータ、ラップトップコンピュータ、セルラーフォン、カメラフォン、スマートフォン、携帯情報端末、メディアプレーヤー、ナビゲーションデバイス、電子メールデバイス、ゲームコンソール、タブレットコンピュータ、装着可能デバイス、またはこれらのデバイスのうちのいずれかの組合せであってよい。

【0094】

説明を容易にするために、装置について説明するとき、装置は、それぞれの説明の機能の点で様々なユニットに分割される。当然、本出願が実装されるとき、ユニットの機能は、同じまたは複数のソフトウェアおよび/またはハードウェア内で実装され得る。

【0095】

本発明の実施形態は、方法、システム、または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当業者は理解されたい。したがって、本発明は、完全なハードウェア実施形態、完全なソフトウェア実施形態、またはソフトウェアとハードウェアを組み合わせた実施形態として実装され得る。その上、本発明は、(限定はしないが、磁気ディスクメモリ、CD-ROM、光メモなどを含む)コンピュータ使用可能プログラムコードを含む1つまたは複数のコンピュータ使用可能記憶媒体上で実装されるコンピュータプログラム製品であってよい。

10

【0096】

本出願は、本発明の実施形態による、方法、デバイス(システム)、およびコンピュータプログラム製品によるフローチャートおよび/またはブロック図を参照しながら説明される。コンピュータプログラム命令は、フローチャートおよび/またはブロック図の各プロセスおよび/またはブロック、ならびにフローチャートおよび/またはブロック図のプロセスおよび/またはブロックの組合せを実装するために使用され得ることを理解されたい。これらのコンピュータプログラム命令は、コンピュータまたは任意の他のプログラマブルデータ処理デバイスのプロセッサによって実行される命令が、フローチャートの1つまたは複数のプロセスおよび/またはブロック図の1つまたは複数のブロックの指定された機能を実装するための装置を生成するように、汎用コンピュータ、専用コンピュータ、埋込み型プロセッサ、または機械を生成するための任意の他のプログラマブルデータ処理デバイスのプロセッサに対して提供され得る。

20

【0097】

これらのコンピュータプログラム命令は、コンピュータ可読メモリ内に記憶された命令が命令装置を含むアーティファクトを生成するように、特定の方法で作業するようにコンピュータまたは任意の他のプログラマブルデータ処理デバイスに命令することができるコンピュータ可読メモリ内に記憶されてもよい。命令装置は、フローチャートの1つまたは複数のプロセスおよび/またはブロック図の1つまたは複数のブロックの指定された機能を実装する。

30

【0098】

これらのコンピュータプログラム命令は、一連の動作ステップがコンピュータまたは別のプログラマブルデバイス上で実行され、それにより、コンピュータ実装処理を生成するように、コンピュータまたは別のプログラマブルデータ処理デバイス上にロードされてもよい。したがって、コンピュータまたは別のプログラマブルデバイス上で実行される命令は、フローチャートの1つまたは複数のプロセスおよび/またはブロック図の1つまたは複数のブロックの指定された機能を実装するためのステップを提供する。

【0099】

典型的な構成では、計算デバイスは、1つまたは複数の中央処理装置(CPU)と、入出力インターフェースと、ネットワークインターフェースと、メモリとを含む。

40

【0100】

メモリは、揮発性メモリ、ランダムアクセスメモリ(RAM)、および/または不揮発性メモリ、たとえば、読取り専用メモリ(ROM)またはフラッシュRAMなど、コンピュータ可読媒体を含み得る。メモリは、コンピュータ可読媒体の一例である。

【0101】

コンピュータ可読媒体は、不揮発性媒体および揮発性媒体、ならびにムーバブル媒体および非ムーバブル媒体を含み、任意の方法または技術によって情報記憶を実装することができる。情報は、コンピュータ可読命令、データ構造、およびプログラムまたは他のデータのモジュールであってよい。コンピュータの記憶媒体は、たとえば、限定はしないが、

50

相変化メモリ(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)、他のタイプのRAM、ROM、電氣的消去可能プログラマブル読取り専用メモリ(EEPROM)、フラッシュメモリもしくは他のメモリ技術、コンパクトディスク読取り専用メモリ(CD-ROM)、デジタル多用途ディスク(DVD)もしくは他の光記憶装置、カセットテープ、磁気テープ/磁気ディスク記憶装置もしくは他の磁気記憶デバイス、または任意の他の非送信媒体を含み、コンピューティングデバイスによってアクセスされる情報を記憶するために使用され得る。このテキストの定義に従って、コンピュータ可読媒体は、変調データ信号およびキャリアなど、一時的媒体を含まない。

【0102】

「含む」、「備える」という用語、またはそれらの任意の他の変形は、非排他的な包含を対象とすることを意図し、その結果、一連の要素を含む、プロセス、方法、物品、またはデバイスは、これらの要素を含むのみならず、明示的に列挙されない他の要素をやはり含むか、またはそのプロセス、方法、物品、またはデバイスに固有の要素をさらに含むことにさらに留意されたい。それ以上の制約が存在しないとき、「を含む」によって定義される要素は、要素が他の同一要素をさらに有することを含めて、そのプロセス、方法、商品、またはデバイスを除外しない。

【0103】

本開示の実施形態は、方法、システム、または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当業者は理解されたい。したがって、本開示は、完全なハードウェア実施形態、完全なソフトウェア実施形態、またはソフトウェアとハードウェアとを組み合わせた実施形態として実装され得る。その上、本開示は、コンピュータ使用可能プログラムコードを含めて、1つまたは複数のコンピュータ使用可能記憶媒体(磁気ディスクメモリ、CD-ROM、光メモリなどを含むが、これらに限定されない)上で実装されるコンピュータプログラム製品の形態であってよい。

【0104】

本出願は、コンピュータ、たとえば、プログラムモジュールによって実行されるコンピュータ実行可能命令の一般的な文脈で説明されることがある。概して、プログラムモジュールは、特定のタスクを実行するため、または特定の抽象データタイプを実装するために使用される、ルーチン、プログラム、オブジェクト、アセンブリ、データ構造などを含む。本出願は、分散型コンピューティング環境で、かつ分散型コンピュータ環境で実装されてもよく、タスクは、通信ネットワークを介して接続された遠隔処理デバイスを使用することによって実行される。分散型コンピュータ環境において、プログラムモジュールは、記憶デバイスを含めて、ローカルコンピュータ記憶媒体およびリモートコンピュータ記憶媒体の中に配置され得る。

【0105】

本明細書における実施形態は、漸進的に説明され、本実施形態の同じまたは同様の部分は、互いに参照しながら取得され得、各実施形態は、他の実施形態と異なる部分を強調する。特に、システム実施形態は、方法実施形態と基本的に同様であり、したがって、簡単に説明され、関連する部分に関しては、方法実施形態の部分の説明を参照することがある。

【0106】

上記の説明は、本出願の単なる実施形態であり、本出願を限定することを意図しない。当業者にとっては、本出願は、様々な修正および変形を有し得る。本出願の趣旨および原理からの逸脱を伴わない、任意の修正、同等の置換、改善などはすべて、本出願の特許請求の範囲内に入るものとする。

【0107】

図11は、本開示の一実施形態による、2Dコードを生成するためのコンピュータ実装方法1100の一例を示す流れ図である。提示を明瞭にするために、続く説明は、概して、本明細書の他の図面の文脈で方法1100について説明する。しかしながら、方法1100は、適宜に、たとえば、いずれのシステム、環境、ソフトウェア、およびハードウェア、またはシステ

10

20

30

40

50

ム、環境、ソフトウェア、ハードウェアの組合せによって実行され得ることを理解されよう。いくつかの実装形態では、方法1100の様々なステップは、平行して、組み合わせて、ループで、または任意の順序で実行され得る。方法1100は、すでに論じた第2のサーバなど、デジタル署名を含む2Dコード暗号化情報を提供するサーバによって実行され得る。

【0108】

1102において、第1のサーバを認証して登録するための登録情報を第1のサーバから受信する。登録要求は、サーバを登録することに関する情報を含み得る。たとえば、サーバは、営業証明または商品詳細など、様々な資格認証を提供することができる。資格認証が検証された後で、サーバを登録することができる。1102から、方法1100は1104に進む。

【0109】

1104において、登録情報が認証された場合、第1のサーバを登録する。1104から、方法1100は1106に進む。

【0110】

1106において、登録情報を保存する。サーバによって提供される資格認証を含む登録情報は、ローカルメモリまたはリモートメモリ内に記憶され得る。したがって、資格認証は、将来の参照のために配置され得る。1106から、方法1100は1108に進む。

【0111】

1108において、2Dコードを生成する要求を第1のサーバから受信し、要求は、2Dコードに符号化されるべき情報を含む。2Dコードを使用して符号化されるべき情報は、支払いを受け取るためのアカウント情報、またはユーザに対応するウェブサイトのリダイレクトし得るウェブサイト情報を含み得る。1108から、方法1100は1110に進む。

【0112】

1110において、非対称暗号化を使用してデジタル署名を生成することによって、2Dコードに符号化されるべき情報にデジタル署名する。デジタル署名は、2Dコード生成要求内に含まれる2Dコード情報に対して生成され得る。場合によっては、2Dコード情報に対するデジタル署名は、非対称暗号化アルゴリズムおよび事前に生成された秘密鍵に基づいて生成され得る。たとえば、デジタル署名は、RSA暗号化アルゴリズムに基づいて生成され得る。2Dコードが対応する公開鍵を使用してユーザコンピューティングデバイスによって首尾よく走査された場合、それは、2Dコードがデジタル署名された2Dコード情報に基づいて第1のサーバによって生成されていることを示し得る。2Dコード走査が失敗した場合、それは、2Dコードが、改ざんされているか、またはデジタル署名された2Dコード情報に基づいて生成されていないことを示し得る。場合によっては、デジタル署名を提供するサーバは、2Dコード生成要求を送信するサーバが登録されたサーバであるかどうかを検査することができる。そうでない場合、サーバは、2Dコード生成要求を拒否することができる。1110から、方法1100は1112に進む。

【0113】

1112において、デジタル署名された情報を第1のサーバに送信する。第1のサーバは、受信された、デジタル署名された2Dコード情報を使用して、2Dコードを生成することができる。1112から、方法1100は1114に進む。

【0114】

1114において、2Dコードがユーザコンピューティングデバイスによって走査された後で、2Dコードを解読する。ユーザは、アプリケーション、ソフトウェア、または第2のサーバによって提供されたソフトウェア開発キット(SDK)を使用して、2Dコードを走査することができる。場合によっては、2Dコードが走査された後で、第2のサーバは、公開鍵を使用して、2Dコード内に含まれたデジタル署名を検証することができる。デジタル署名が認証されている場合、第2のサーバは、2Dコードを解読して、解読された情報をユーザに送信することができる。場合によっては、デジタル署名検証アルゴリズムを、アプリケーション、ソフトウェア、または第2のサーバによって提供され、ユーザコンピューティングデバイス上にインストールされたSDKの中に含めることができる。そのような場合、ユーザは、ユーザコンピューティングデバイス上で利用可能なデジタル署名検証アルゴリズム

10

20

30

40

50

を使用することによって、2Dコードを解読することができる。走査が失敗した場合、2Dコードは改ざんされている可能性がある。2Dコードは信用できないことをユーザに通知することができる。1114から、方法1100は1116に進む。

【0115】

1116において、2Dコードが走査されているという記録を第2のサーバに保存し、この記録は、2Dコードを符号化する第1のサーバを含む。第2のサーバは、2Dコードの走査活動を保存し得る。走査は成功したが、2Dコードがデジタル署名された情報を悪用している別のサーバによって生成された場合、2Dコードの走査活動は保存されているため、その悪用は第2のサーバによって識別され得る。1116の後で、方法1100は終了する。

【0116】

本明細書で説明した主題の実装形態および機能的動作は、デジタル電子回路内で、有形に実施されるコンピュータソフトウェアまたはコンピュータファームウェア内で、本明細書で開示する構造およびその構造的均等物を含めてコンピュータハードウェア内で、またはそれらのうちの1つまたは複数の組合せの中で実装され得る。説明した主題のソフトウェア実装形態は、1つまたは複数のコンピュータプログラム、すなわち、コンピュータシステムまたはコンピュータ実装システムによって実行するための、またはその動作を制御するための、有形の、非一時的コンピュータ可読媒体上で符号化されたコンピュータプログラム命令の1つまたは複数のモジュールとして実装され得る。代替または追加で、プログラム命令は、人工的に生成された伝搬信号、たとえば、コンピュータシステムまたはコンピュータ実装システムによって実行するために受信装置に送信するための情報を符号化するように生成された、機械生成された電子信号、光信号、または電磁信号内/上で符号化され得る。コンピュータ記憶媒体は、機械可読記憶デバイス、機械可読記憶基板、ランダムアクセスメモリデバイスもしくはシリアルアクセスメモリデバイス、またはコンピュータ記憶媒体の組合せであってよい。1つまたは複数のコンピュータを構成することは、ソフトウェアが1つまたは複数のコンピュータによって実行されるとき、特定のコンピューティング動作が実行されるように、1つまたは複数のコンピュータが、ハードウェア、ファームウェア、もしくはソフトウェア(または、ハードウェア、ファームウェア、およびソフトウェアの組合せ)をインストールしていることを意味する。

【0117】

「リアルタイム(real-time)」、「リアルタイム(real time)」、「リアルタイム(realtime)」、「リアル(ファスト)タイム(RFT:real (fast) time)」、「ほぼリアルタイム(NRT:near(ly)real-time)」、「準リアルタイム」、または(当業者が理解する)同様の用語は、個人が実質的に同時に生じる行為および応答を認知するように、行為および応答が時間的に近接していることを意味する。たとえば、データにアクセスするための個人の行為に続く、データを表示する応答のための(または、表示を開始するための)時差は、1ミリ秒(ms)未満、1秒(s)未満、または5s未満であり得る。依頼されたデータは瞬時に表示され(または、表示が開始され)なくてもよいが、説明したコンピューティングシステムの処理制限、および、たとえば、データを集め、正確に測定し、分析し、処理し、記憶し、または送信するために必要とされる時間を考慮に入れて、意図的な遅延を伴わずに表示される(または、表示が開始される)。

【0118】

「データ処理装置」、「コンピュータ」、または「電子コンピュータデバイス」(または、当業者が理解するような同等の用語)という用語は、データ処理ハードウェアを指し、例として、プログラマブルプロセッサ、コンピュータ、または複数のプロセッサもしくはコンピュータを含めて、データを処理するためのすべての種類の装置、デバイス、および機械を包含する。コンピュータは、専用論理回路、たとえば、中央処理装置(CPU)、FPGA(フィールドプログラマブルゲートアレイ)、またはASIC(特定用途向け集積回路)であってもよく、またはそれらをさらに含んでもよい。いくつかの実装形態では、コンピュータもしくはコンピュータ実装システム、または専用論理回路(あるいは、コンピュータシステムもしくはコンピュータ実装システムと専用論理回路の組合せ)は、ハードウェアペー

10

20

30

40

50

スもしくはソフトウェアベース(または、ハードウェアベースとソフトウェアベースの両方の組合せ)であってよい。コンピュータは、任意で、コンピュータプログラムのための実行環境を作り出すコード、たとえば、プロセッサファームウェア、プロトコルスタック、データベース管理システム、オペレーティングシステム、または実行環境の組合せを構成するコードを含み得る。本開示は、何らかのタイプのオペレーティングシステム、たとえば、LINUX(登録商標)、UNIX(登録商標)、WINDOWS(登録商標)、MAC OS、ANDROID(登録商標)、IOS、別のオペレーティングシステム、またはオペレーティングシステムの組合せを備えた、コンピュータシステムまたはコンピュータ実装システムの使用を企図する。

【0119】

プログラム、ソフトウェア、ソフトウェアアプリケーション、ユニット、モジュール、ソフトウェアモジュール、スクリプト、コード、または他の構成要素と呼ばれることがあるか、またはそれらとして説明されることもあるコンピュータプログラムは、コンパイル型言語もしくはインタープリタ型言語、または宣言型言語もしくは手続き型言語を含めて、任意の形式のプログラミング言語で書き込まれてよく、コンピュータプログラムは、コンピュータ環境で使用するために、たとえば、スタンドアロンプログラム、モジュール、構成要素、またはサブルーチンを含めて、任意の形式で展開されてよい。コンピュータプログラムは、ファイルシステム内のファイルに対応し得るが、そうでなくてもよい。プログラムは、他のプログラムまたはデータ、たとえば、マークアップ言語文書内、当該プログラム専用の単一ファイル内、または複数の協調ファイル、たとえば、1つまたは複数のモジュール、サブプログラム、またはコードの部分を記憶するファイル内に記憶された1つまたは複数のスクリプトを保有するファイルの部分の中に記憶され得る。コンピュータプログラムは、1つのコンピュータ上、または1つのサイト上に配置された、または複数のサイトにわたって分散され、通信ネットワークによって相互接続された、複数のコンピュータ上で実行されるように展開され得る。

【0120】

様々な図面で示したプログラムの部分は、様々なオブジェクト、方法、または他のプロセスを使用して、説明した特徴および機能性を実装する、ユニットまたはモジュールなど、個々の構成要素として示されることがあるが、プログラムは、代わりに、適宜に、いくつかのサブユニット、サブモジュール、第三者サーバ、構成要素、ライブラリ、および他の構成要素を含んでもよい。逆に、様々な構成要素の特徴および機能性は、適宜、単一の構成要素内に組み込まれてもよい。計算上の判定を行うために使用されるしきい値は、静的に、動的に、または静的と動的の両方で判定されてよい。

【0121】

説明した方法、プロセス、または論理フローは、本開示に整合する機能性の1つまたは複数の例を表し、本開示を説明したまたは示した実装形態に限定することを意図せず、説明した原理および特徴に整合する最大範囲が与えられるべきである。説明した方法、プロセス、または論理フローは、入力データに関して動作し、出力データを生成することによって機能を実行するために、1つまたは複数のコンピュータプログラムを実行する、1つまたは複数のプログラマブルコンピュータによって実行され得る。これらの方法、プロセス、または論理フローは、専用論理回路、たとえば、CPU、FPGA、またはASICによって実行されてもよく、コンピュータはそれらとして実装されてもよい。

【0122】

コンピュータプログラムの実行のためのコンピュータは、汎用マイクロプロセッサもしくは専用マイクロプロセッサ、両方、または別のタイプのCPUに基づいてよい。概して、CPUは、命令およびデータをメモリから受信し、命令およびデータをメモリに書き込むことになる。コンピュータの必須要素は、命令を実行(performing)または実行(executing)するためのCPU、および命令およびデータを記憶するための1つまたは複数のメモリデバイスである。概して、コンピュータはまた、データを記憶するための1つまたは複数の大容量記憶デバイス、たとえば、磁気ディスク、光磁気ディスク、または光ディスクを含むことになるか、またはそれらからデータを受信し、もしくはそれらにデータを転送し、または

その両方をするように動作可能に結合されるべき。しかしながら、コンピュータは、そのようなデバイスを有さなくてもよい。その上、コンピュータは、別のデバイス、たとえば、モバイル電話、携帯情報端末(PDA)、モバイルオーディオプレーヤーもしくはモバイルビデオプレーヤー、ゲームコンソール、全地球測位システム(GPS)受信機、またはポータブルメモリ記憶デバイス内に埋め込まれてもよい。

【0123】

コンピュータプログラム命令およびデータを記憶するための非一時的コンピュータ可読媒体は、例として、半導体メモリデバイス、たとえば、ランダムアクセスメモリ(RAM)、読取り専用メモリ(ROM)、相変化メモリ(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)、消去可能プログラマブル読取り専用メモリ(EPROM)、電氣的消去可能プログラマブル読取り専用メモリ(EEPROM)、およびフラッシュメモリデバイス;磁気デバイス、たとえば、テープ、カートリッジ、カセット、内蔵/リムーバブルディスク;光磁気ディスク;および光メモリデバイス、たとえば、デジタル多用途/ビデオディスク(DVD)、コンパクトディスク(CD)ROM、DVD+/-R、DVD-RAM、DVD-ROM、高解像度/密度(HD)-DVD、およびBLU-RAY/BLU-RAY DISC(BD)、ならびに他の光メモリ技術を含めて、すべての形式の永続的/非永続的または揮発性/不揮発性のメモリ、媒体、およびメモリデバイスを含み得る。メモリは、キャッシュ、クラス、フレームワーク、アプリケーション、モジュール、バックアップデータ、ジョブ、ウェブページ、ウェブページテンプレート、データ構造、データベース表、動的情報を記憶するリポジトリ、または、任意のパラメータ、変数、アルゴリズム、命令、規則、制約、または基準を含む他の適切な情報を含めて、様々なオブジェクトまたはデータを記憶することができる。加えて、メモリは、ログ、ポリシー、セキュリティデータもしくはアクセスデータ、または報告ファイルなど、他の適切なデータを含み得る。プロセッサおよびメモリは、専用論理回路によって補強されてよいが、または専用論理回路内に組み込まれてよい。

【0124】

ユーザとの対話を提供するために、本明細書で説明した主題の実装形態は、情報をユーザに表示するためのディスプレイデバイス、たとえば、CRT(陰極線管)、LCD(液晶ディスプレイ)、LED(発光ダイオード)、またはプラズマモニタ、ならびにキーボードおよびポインティングデバイス、たとえば、ユーザがコンピュータに入力を提供し得る、マウス、トラックボール、またはトラックパッドを有するコンピュータ上で実装され得る。入力は、感圧性を備えたタブレットコンピュータの表面、容量性感知または電気感知を使用したマルチタッチスクリーン、または別のタイプのタッチスクリーンなど、タッチスクリーンを使用してコンピュータに提供されてもよい。他のタイプのデバイスを使用して、ユーザと対話することもできる。たとえば、ユーザに提供されるフィードバックは、任意の形式の知覚フィードバック(視覚フィードバックタイプ、聴覚フィードバックタイプ、触覚フィードバックタイプ、またはフィードバックタイプの組合せなど)であってよい。ユーザからの入力は、音響入力、音声入力、または触覚入力を含めて、任意の形式で受信され得る。加えて、コンピュータは、ユーザによって使用されるクライアントコンピューティングデバイスに文書を送信すること、およびそこから文書を受信することによって(たとえば、ユーザのモバイルコンピューティングデバイス上のウェブブラウザから受信された依頼に回答して、ウェブページをそのウェブブラウザに送信することによって)ユーザと対話することができる。

【0125】

「グラフィカルユーザインターフェース」または「GUI」という用語は、1つまたは複数のグラフィカルユーザインターフェースおよび特定のグラフィカルユーザインターフェースのディスプレイの各々を説明するために単数形または複数形で使用されることがある。したがって、GUIは、限定はしないが、ウェブブラウザ、タッチスクリーン、または情報を処理し、情報結果をユーザに効率的に提示するコマンドラインインターフェース(CLI)を含めて、任意のグラフィカルユーザインターフェースを表し得る。概して、GUIは、双方向フィールド、プルダウンリスト、およびボタンなど、いくつかまたはすべてがウェブ

ブラウザに関連する、いくつかのユーザインターフェース(UI)要素を含み得る。これらのおよび他のUI要素は、ウェブブラウザの機能に関係し得るか、またはそれらの機能を表し得る。

【0126】

本明細書で説明した主題の実装形態は、たとえば、データサーバなど、バックエンド構成要素を含む、もしくはミドルウェア構成要素、たとえば、アプリケーションサーバを含む、またはフロントエンド構成要素、たとえば、それを介してユーザが本明細書で説明した主題の実装形態と対話することができるグラフィカルユーザインターフェースまたはウェブブラウザを有するクライアントコンピュータを含むか、あるいはそのようなバックエンド構成要素、ミドルウェア構成要素、またはフロントエンド構成要素のうちの1つまたは複数の任意の組合せを含む、コンピューティングシステム内で実装され得る。システムの構成要素は、任意の形式のまたは任意の媒体のワイヤラインまたはワイヤレスのデジタルデータ通信(または、データ通信の組合せ)、たとえば、通信ネットワークによって相互接続され得る。通信ネットワークの例は、ローカルエリアネットワーク(LAN)、無線アクセスネットワーク(RAN)、メトロポリタンエリアネットワーク(MAN)、広域ネットワーク(WAN)、ワールドワイドインターオペラビリティフォーマイクロウェーブアクセス(WIMAX)、たとえば、802.11a/b/g/nもしくは802.20(または、802.11xと802.20の組合せ、あるいは本開示に整合する他のプロトコル)を使用するワイヤレスローカルエリアネットワーク(WLAN)、インターネットのすべてまたは一部、別の通信ネットワーク、または通信ネットワークの組合せを含む。通信ネットワークは、たとえば、インターネットプロトコル(IP)パケット、フレームリレーフレーム、非同期転送モード(ATM)セル、ボイス、ビデオ、データ、またはネットワークノード同士の間での他の情報を通信し得る。

【0127】

コンピューティングシステムは、クライアントおよびサーバを含み得る。クライアントおよびサーバは、概して、互いと遠隔にあり、典型的に、通信ネットワークを介して通信する。クライアントおよびサーバの関係は、それぞれのコンピュータ上で実行し、互いとクライアント-サーバ関係を有するコンピュータプログラムにより生じる。

【0128】

本明細書は多くの特定の实装詳細を含むが、これらは、任意の発明的概念の範囲または特許請求され得る範囲に対する限定と解釈されるべきではなく、特定の発明的概念の特定の实装形態に特定であり得る特徴の説明と解釈されるべきである。別個の实装形態の文脈で本明細書において説明したいいくつかの特徴は、単一の实装形態で、組み合わせて実装されてもよい。逆に、単一の实装形態の文脈で説明した様々な特徴は、別個に複数の実装形態で、または任意の部分的な組合せで実装されてもよい。その上、すでに説明した特徴は、いくつかの組合せで作用するとして説明され、当初、そのように特許請求されている場合すらあるが、特許請求される組合せからの1つまたは複数の特徴は、場合によっては、その組合せから削除される場合があり、特許請求される組合せは、部分的な組合せまたは部分的な組合せの変形に関する場合もある。

【0129】

主題の特定の实装形態について説明してきた。説明した実装形態の他の実装形態、代替案、および置換は、当業者に明らかになるような、以下の特許請求の範囲内である。動作は図面または請求項において特定の順序で示されるが、これは、所望の結果を達成するために、そのような動作が、示した特定の順序で、または順番に実行される、またはすべての示した動作が実行されるべきである(いくつかの動作は、任意と見なされてよい)と理解するべきではない。状況によっては、マルチタスキングもしくは並行処理(または、マルチタスキングと並行処理の組合せ)は有利であり得、適切と見なされる場合、実行され得る。

【0130】

その上、すでに説明した実装形態内の様々なシステムモジュールおよび構成要素の分離または統合は、そのような分離または統合がすべての実装形態において要求されると理解

10

20

30

40

50

されるべきではなく、説明したプログラム構成要素およびシステムは、概して、単一のソフトウェア製品内に一緒に統合されてよいが、または複数のソフトウェア製品内に梱包されてもよいことを理解されたい。

【0131】

したがって、すでに説明した例示的な実装形態は、本開示を定義または制約しない。本開示の趣旨および範囲から逸脱せずに、他の変更、置換、および代替案も可能である。

【0132】

さらに、任意の特許請求される実装形態は、少なくともコンピュータ実装方法; コンピュータ実装方法を実行するためのコンピュータ可読命令を記憶した、非一時的コンピュータ可読媒体; およびコンピュータ実装方法または非一時的コンピュータ可読媒体上に記憶された命令を実行するように構成されたハードウェアプロセッサに相互作用可能に結合されたコンピュータメモリを含むコンピュータシステムに適用可能と見なされる。

10

【符号の説明】

【0133】

- 110 サーバ
- 120 サーバ
- 510 送信ユニット
- 520 受信ユニット
- 530 生成ユニット
- 710 受信ユニット
- 720 処理ユニット
- 730 送信ユニット
- 910 開始ユニット
- 920 走査ユニット
- 930 検証ユニット
- 940 認識ユニット

20

【図1】

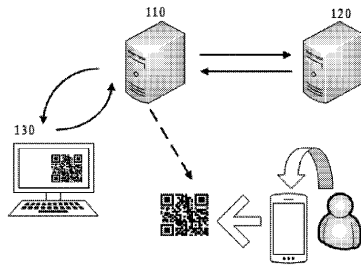
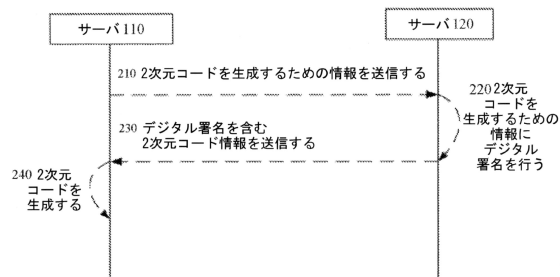


FIG. 1

【図2】



【図3】

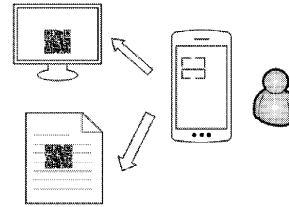
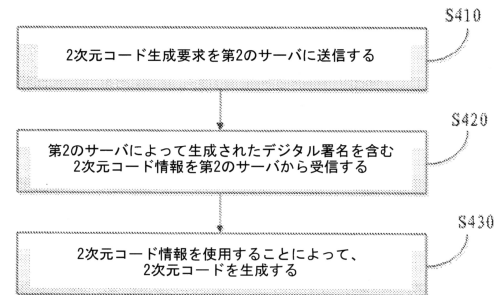
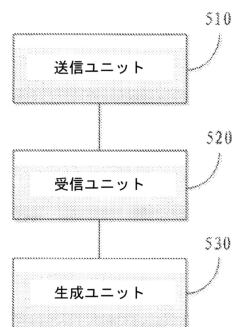


FIG. 3

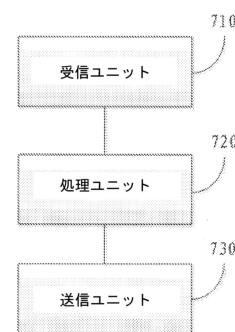
【図4】



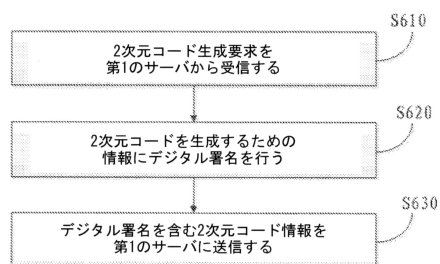
【図5】



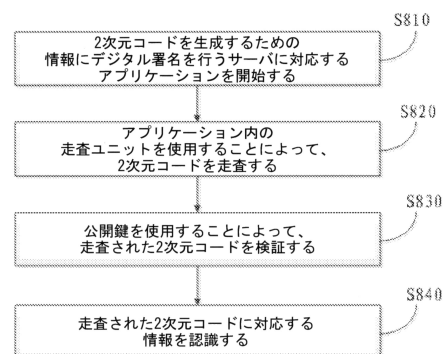
【図7】



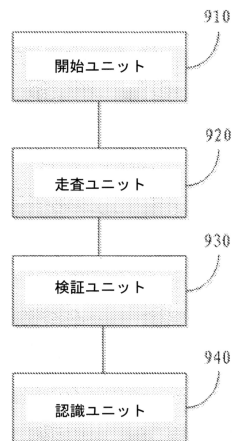
【図6】



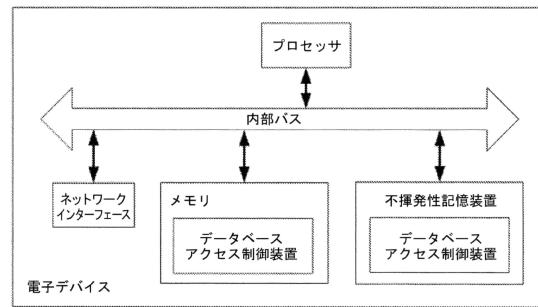
【図8】



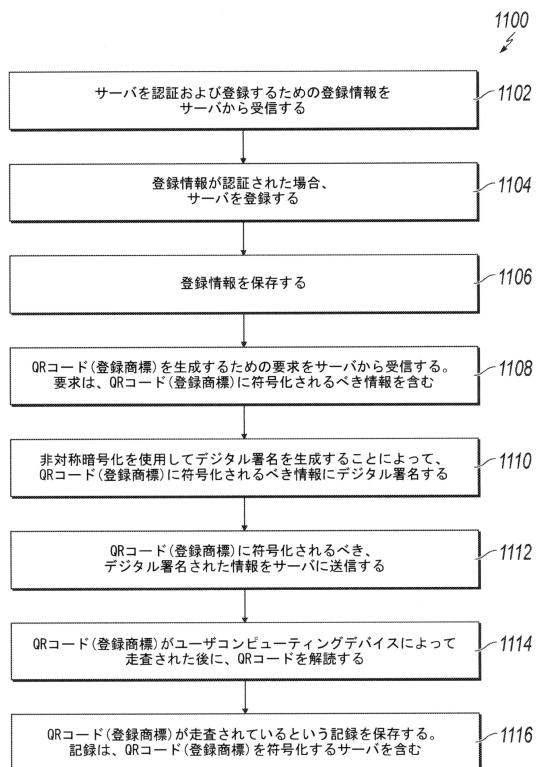
【図 9】



【図 10】



【図 11】



フロントページの続き

(72)発明者 ウエイ・グオ

中華人民共和国・311121・ゼジャン・ハンジョウ・ユ・ハン・ディストリクト・ウェスト・
ウェン・イ・ロード・ナンバー・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 平井 誠

(56)参考文献 特開2016-006945(JP, A)

Hatma Suryotrisongkoa et al., A Novel Mobile Payment Scheme Based on Secure Quick Response Payment with Minimal Infrastructure for Cooperative Enterprise in Developing Countries, International Congress on Interdisciplinary Business and Social Science 2012, 2012年12月3日, pp.906-912, (URL: <https://www.sciencedirect.com/science/article/pii/S1877042812052032>)

(58)調査した分野(Int.Cl., DB名)

H04L 9/00-38

G06F 21/00-88

G09C 1/00-5/00