(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2025-503398
(P2025-503398A)
(43)公表日　令和7年2月4日(2025.2.4)

(51)国際特許分類　FI
G06F 11/08 (2006.01)　G06F 11/08
G06K 1/12 (2006.01)　G06K 1/12　A
G06K 19/06 (2006.01)　G06K 19/06　037
G06K 7/14 (2006.01)　G06K 19/06　075
G06K 7/14　017
審査請求　未請求　予備審査請求　未請求　（全39頁）　最終頁に続く

(21)出願番号　特願2024-534143(P2024-534143)
(86)(22)出願日　令和4年12月22日(2022.12.22)
(85)翻訳文提出日　令和6年6月7日(2024.6.7)
(86)国際出願番号　PCT/EP2022/087384
(87)国際公開番号　WO2023/126287
(87)国際公開日　令和5年7月6日(2023.7.6)
(31)優先権主張番号　22150029.1
(32)優先日　令和4年1月3日(2022.1.3)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)
(81)指定国・地域　AP(BW,CV,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
最終頁に続く

(71)出願人　590000248
コーニンクレッカ フィリップス エヌヴェ
Koninklijke Philips N.V.
オランダ国 5656 アーヘー アインドーフェン ハイテック キャンパス 52
High Tech Campus 52, 5656 AG Eindhoven, Netherlands
(74)代理人　100122769
弁理士　笛田 秀仙
(74)代理人　100163809
弁理士　五十嵐 貴裕
(74)代理人　100145654
最終頁に続く

(54)【発明の名称】　複数アプリケーションＱＲコード

(57)【要約】
本発明は、複数のアプリケーションの情報を、信頼性があり時間効率的な態様でアプリケーションごとにそれぞれの情報を取り出すことができるように格納することができる複数アプリケーションQRコードに関する。情報は、少なくともヘッダとアプリケーションごとのそれぞれのデータコンテナとを含む符号化データに符号化される。ヘッダは、複数のアプリケーションの存在を示す少なくとも1つの識別子と、アプリケーションごとのそれぞれのアプリケーション識別子とを含むことができる。符号化データは、割り当て規則に従って、QRコード化領域に分散された複数のデータピクセルに分散して格納される。QRコードリーダは、それぞれの関心アプリケーションに関連するデータピクセルにアクセスして処理するだけで、このそれぞれのアプリケーションに特有の誤り訂正を使用することによって、QRコードに格納された情報を取り出すことができる。

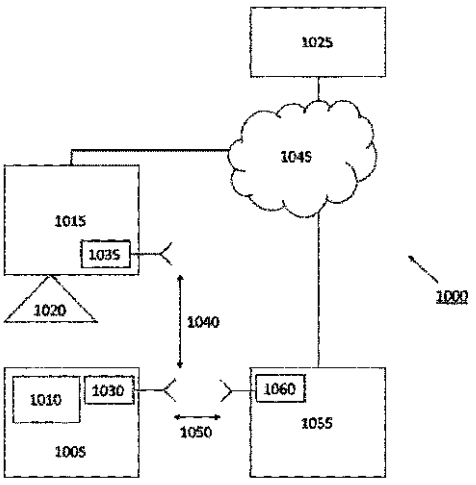

Fig. 10

【特許請求の範囲】
【請求項１】
ＱＲコードへの格納のために複数のアプリケーションの情報を符号化する方法であって、前記複数のアプリケーションの前記情報を収集するステップと、前記情報を符号化データに符号化するステップであって、前記符号化データは、少なくともヘッダとアプリケーションごとのそれぞれのデータコンテナとを含む、ステップとを有し、前記ヘッダは、前記複数のアプリケーションの存在を示す少なくとも単一の識別子と、アプリケーションごとのそれぞれのアプリケーション識別子とを含む、方法。
【請求項２】
アプリケーションごとの前記それぞれのデータコンテナの前記符号化データ中のアプリケーションごとの各々のデータコンテナのために、それぞれの誤り訂正機構および／または誤り検出機構が使用される、請求項１に記載の方法。
【請求項３】
情報を符号化データに符号化する前記ステップが、前記情報の入力データストリームをアプリケーションごとのそれぞれの入力ビット列に変換するステップと、アプリケーションごとの前記ぞれぞれの入力ビット列を１つまたは複数のデータコードワードのシーケンスに分割するステップと、１つまたは複数のコードワードの前記シーケンスを所定の数のブロックに分割するステップと、各ブロックのための１つまたは複数の誤り訂正コードワードを生成するステップと、前記誤り訂正コードワードをデータコードワードの前記シーケンスに含めるステップと、を少なくとも有する、請求項１または２に記載の方法。
【請求項４】
情報を符号化データに符号化する前記ステップが、各アプリケーションのために前記ヘッダからそれぞれのデータストリームを取得するステップと、前記それぞれのデータストリームを組み合わされたそれぞれのデータストリームに組み合わせるステップと、前記組み合わされたそれぞれのデータストリームをそれぞれの入力ビット列に変換するステップと、アプリケーションごとの前記ぞれぞれの入力ビット列を１つまたは複数のデータコードワードのシーケンスに分割するステップと、１つまたは複数のコードワードの前記シーケンスを所定の数のブロックに分割するステップと、各ブロックのための１つまたは複数の誤り訂正コードワードを生成するステップと、前記誤り訂正コードワードをデータコードワードの前記シーケンスに含めるステップと、を少なくとも有する、請求項１または２に記載の方法。
【請求項５】
前記符号化データの一部または全体を、前記ＱＲコードの符号化領域にわたって分布する複数のデータピクセルに分散的に格納するステップをさらに有する、請求項１から４のいずれか一項に記載の方法。
【請求項６】
アプリケーションごとのそれぞれの誤り訂正機構に用いるように構成されるデータが、アプリケーションごとの各データコンテナに含まれる、請求項１から５のいずれか一項に記載の方法。
【請求項７】
前記符号化データが、他のデータコンテナ中のコードワードに基づいて前記それぞれのデータコンテナ中に誤りが存在するかを検出するために前記複数のアプリケーションのうちの全てのアプリケーションによって共有される全体的な誤り検出機構により用いられるように構成されたデータ、および／または他のデータコンテナ中のコードワードに基づいて前記それぞれのデータコンテナ中の誤りを訂正するために前記複数のアプリケーションのうちの全てのアプリケーションによって共有される全体的な誤り訂正機構により用いられるように構成されたデータ、を含む、請求項１から６のいずれか一項に記載の方法。
【請求項８】
前記ＱＲコードに物理的に重畳されたグラフィカル表現から画像データを収集するステップと、前記符号化データの前記ヘッダに、前記グラフィカル表現の存在の指標および前記

QRコード上の前記グラフィカル表現により占められる領域の指標を含めるステップと、をさらに有し、前記グラフィカル表現により占められる領域と一致する前記QRコード中の領域を占める前記QRコードの前記符号化領域の前記データピクセルが、前記符号化データの一部または全体の格納から除外される、請求項５に記載の方法。

【請求項９】

前記QRコードが、少なくとも公開鍵の情報を格納するためのDPPブートストラップ情報を含む、請求項１から８のいずれか一項に記載の方法。

【請求項１０】

QRコード中の複数のアプリケーションのうちのそれぞれのアプリケーションの情報を復号する方法であって、前記情報は前記QRコード中に符号化データとして格納され、前記符号化データは、少なくともヘッダと、アプリケーションごとのそれぞれのデータコンテナとを含み、当該方法は、前記QRコードのヘッダを読み取るステップであって、前記ヘッダは、前記複数のアプリケーションの存在を示す少なくとも単一の識別子と、アプリケーションごとのそれぞれのアプリケーション識別子と含む、ステップと、前記ヘッダから、前記複数のアプリケーションの存在を示す前記単一の識別子を用いることにより、前記QRコードを識別するステップと、前記ヘッダから、前記それぞれのアプリケーションを特定するステップと、前記それぞれのアプリケーションに関連付けられたそれぞれのデータコンテナを特定するステップと、を有する方法。

【請求項１１】

前記それぞれのアプリケーションに関連する少なくとも１つのデータコードワード、および、前記複数のアプリケーションの全てのためのパリティビット、誤り検出ビットまたは誤り訂正ビットを読み出すために前記それぞれのアプリケーションの前記データコンテナに関連する全てのピクセルを読み取るステップと、前記それぞれのアプリケーションのエラーフリーアプリケーションデータを取得するステップと、をさらに有する、請求項１０に記載の方法。

【請求項１２】

前記情報が、通信プロトコルのためのコミッショニング情報を符号化し、前記方法は、事前設定された値、ポリシー、コンテキスト及び前記QRコード中のデータの一部のうちの少なくとも１つに基づいて第１のコミッショニングプロトコルを選択する、請求項１０または１１に記載の方法。

【請求項１３】

QRコードにおける格納のために複数のアプリケーションの情報を符号化する機器であって、請求項１から９のいずれか一項に記載の方法を実行するように適応された機器。

【請求項１４】

QRコード中の複数のアプリケーションのうちのそれぞれのアプリケーションの情報を復号する機器であって、前記情報は、前記QRコードに符号化データとして格納され、前記符号化データは、少なくとのヘッダと、アプリケーションごとのそれぞれのデータコンテナとを含み、前記装置は、請求項１０から１２のいずれか一項に記載の方法を実行するように適応される、機器。

【請求項１５】

関連するQRコードを有する装置であって、前記QRコードは２つの異なるコミッショニングプロトコルのためのコミッショニング情報を含み、前記装置は、コミッショナ装置から第１のコミッショニングプロトコルの初期コミッショニングメッセージを受信すると、前記第１のコミッショニングプロトコルが終了するまで、第２のコミッショニングプロトコルの初期コミッショニングメッセージを受け入れない、装置。

【請求項１６】

カメラと第１の通信インタフェイスを有する請求項１４に記載の機器、関連するQRコードと第２の通信インタフェイスを有する第１の装置、第３の通信インタフェイスを有する第２の装置、および第３の装置、を含むシステムであって、前記機器は、前記第３の装置とインタフェイスし、前記第１の装置との第１のコミッショニングプロトコルを開始して

実行するように適応され、および／または前記第３の装置は、前記第２の装置から前記第１の装置との、前記第１のコミッショニングプロトコルと同一または異なる第２のコミッショニングプロトコルを鳥がするように適応される、システム。
【請求項１７】
コンピュータ上で実行され、前記コンピュータに請求項１から９のいずれか一項に記載の方法を実行させる、コンピュータプログラム。
【請求項１８】
コンピュータ上で実行され、前記コンピュータに請求項１０から１２のいずれか一項に記載の方法を実行させる、コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はQRコードの分野に関し、より具体的には、複数アプリケーションQRコードに関する。
【背景技術】
【０００２】
クイックレスポンス（QR）コード（［ISO 18004］参照）は、二次元バーコードとも呼ばれ、情報を符号化する機械可読光学ラベルであり、QRコードリーダまたはスキャンデバイスによって復号することができる。例えば、スマートフォンなどのハンドヘルドデバイスは、QRコードリーダと、QRコードの画像をキャプチャし、それを復号して符号化された情報を識別することができる光学カメラとを装備することができる。QRコードは多くのアプリケーションに使用することができる。例えば、QRコードは、ポスター上に印刷されることができ、ユーザがQRコードをスキャンすると、例えば、QRコードリーダ上のブラウザが、ポスターの主題に関するより多くの情報を有するウェブサイトを開く。別の例では、会社が、例えばシリアル番号を使用して製品を登録するために、または製品と通信するためにその会社のアプリケーションによって使用され得る製品のシリアル番号を含むQRコードを、自身の製品上に印刷することができる。
【０００３】
Wi-Fi（すなわち、IEEE 802.11ベース）を使用する無線ネットワークなどの無線ネットワークにデバイスを接続することは一般的である。接続されるべきデバイスが、ユーザインタフェイスを欠いているか、または非常に基本的なユーザインタフェイスしか有していない場合、接続のセットアップを支援するために別のデバイスを使用することが一般的である。セットアップ、すなわち設定プロセスの一部は、ブートストラップを含む。一例はWi-Fi Easy Connectであり、デバイスプロビジョニングプロトコル（Device Provisioning Protocol：DPP）スキームをサポートし（Wi-Fi Allianceによって確立された［DPP］を参照）、QRコードを使用してWi-Fiデバイス間のセキュアなWi-Fi接続をブートストラップする。そのようなセットアッププロトコルは、通常、「コミッショニング」と呼ばれる。
【０００４】
製品は、いくつかの異なるアプリケーション用にいくつかのQRコードを含むことができる。例えば、ワイヤレス製品（例えばWi-Fi製品）は、Bluetooth Low Energy(BLE)製品、またはIEEE 802.15.4ベースの製品などである場合がある。そのような製品は、第1のコミッショニングプロトコル、例えばWi-Fi Easy ConnectによってWi-Fiネットワークに接続するための第1のQRコードと、Wi-Fiフレーム上のMatterのようなスマートホームネットワーク（SHS）のような別のネットワークにおいて第2のコミッショニングプロトコルによって登録するための第1のQRコード以外の第2のQRコードとを必要とする場合がある。しかしながら、ユーザは、どのQRコードがどのアプリケーションのために使用されるべきかを理解しなければならないので、ユーザが特定のアプリケーション、例えばコミッショニングプロトコルのために正しいQRコードをスキャンすることは問題となる可能性がある。さらに、Wi-Fi Easy ConnectおよびSHSの両方をサポート

するワイヤレス製品の場合、この製品は、Wi-Fi Easy ConnectおよびSHSの両方のコミッショニングプロトコルも実装する。両方のコミッショニングプロトコルは、Wi-Fiフレームに依存するか、またはWi-Fiフレーム上で交換されるので、製品は、コミッショニングツールによってトリガされる初期のインタラクションに基づいて、どのコミッショニングプロトコルを使用する必要があるかを選択する必要がある。しかしながら、この挙動は定義されていない。同様の問題は、同じ無線インタフェイス上で2つ以上のコミッショニングプロトコルを実装する他のワイヤレス製品にも現れる。

【０００５】

さらに、そのような状況では、複数のQRコードに含まれる情報がアプリケーションのうちの1つによって必要とされる場合があり、その結果、単一のQRコードのスキャンでは十分ではない。実際、関連する情報をそれぞれが含むいくつかのQRコードをスキャンする必要がある事例がますます増えている。各QRコードをスキャンすることは非効率的で時間がかかり、単一のスキャン動作は遥かに迅速である。そのような例の1つは、グループで旅行する乗客のためのドキュメンテーションチェックである。個々人についてのQRコードのスキャンは、行列の著しい延長および関与する全ての人にとってのフラストレーションにつながるだろう。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

本発明の目的は、各アプリケーションのそれぞれの情報を信頼性が高く時間効率の良い方法で個別に読み出すことができるような態様で、複数のアプリケーションの情報を１つのQRコードに格納することである。本発明のさらなる目的は、QRコードから読み出された情報に基づいて、同じ通信インタフェイス上で動作するコミッショニングプロトコルの動作を調整することである。

【課題を解決するための手段】

【０００７】

この目的は、請求項1～9のいずれかに記載の符号化方法によって、請求項10～12のいずれかに記載の復号方法によって、請求項13に記載の符号化装置によって、請求項14に記載の復号装置によって、請求項15に記載の装置によって、請求項16に記載のシステムによって、および請求項17および18に記載のそれぞれのコンピュータプログラム製品によって達成される。

【０００８】

第1の態様によれば、第1のQRコードに記憶するための複数のアプリケーションの情報を符号化することに向けられた方法は、複数のアプリケーションの情報を少なくとも収集するステップと、情報を符号化データに符号化するステップとを有し、符号化データは、少なくともヘッダと、アプリケーションごとのそれぞれのデータコンテナとを含む。ヘッダは、少なくとも、複数のアプリケーションの存在を示す単一の識別子と、アプリケーションごとのそれぞれのアプリケーション識別子とを含む。したがって、それぞれのアプリケーションおよびデータコンテナのためのヘッダによって示される識別情報は、同じ（第1の)QRコード上で複数のアプリケーションをサポートすることを可能にする。以下の開示では、第1のQRコード、すなわち、複数のアプリケーションを処理することが可能なQRコードは、マスタコードとしても互換的に表されることができる。

【０００９】

第1の態様の例では、それぞれの誤り訂正機構（ECM）および/または誤り検出機構（EDM）が、アプリケーションごとのそれぞれのデータコンテナの符号化データにおいて、アプリケーションごとのそれぞれのデータコンテナに対して使用される。それによって、データコンテナごとにECMおよび/またはEDMを提供することで、第1のQRコード内のそれぞれのアプリケーションのデータを確実に高速に読み取ることが可能になる。

【００１０】

第1の態様の例では、情報を符号化データに符号化するステップは、情報の入力データス

トリームを、アプリケーションごとのそれぞれの入力ビット列に少なくとも変換するステップと、アプリケーションごとのそれぞれの入力ビット列を1つまたは複数のデータコードワードのシーケンスに分割するステップと、1つまたは複数のデータコードワードの前記シーケンスを事前定義された数のブロックに分割するステップと、ブロックごとに1つまたは複数の誤り訂正コードワードを生成するステップと、データコードワードシーケンス中に誤り訂正コードワードを含めるステップとを有する。例えば、誤り訂正コードワードは、データコードワードシーケンス内の任意の適切な場所または複数の場所に挿入されることができる。これにより、アプリケーションごとに誤り訂正能力が存在する。一例では、データおよび誤り訂正コードワードは、8ビット長、または別の長さのビットを有することができる。

【００１１】

第1の態様の例では、情報を符号化データに符号化するステップは、少なくとも、各アプリケーションのヘッダからそれぞれのデータストリームを取り出すステップと、それぞれのデータストリームをそれぞれの結合データストリームに結合するステップと、それぞれの結合データストリームをそれぞれの入力ビット列に変換するステップと、それぞれの入力ビット列を1つまたは複数のデータコードワードのシーケンスに分割するステップと、1つまたは複数のデータコードワードのシーケンスを予め定義された数のブロックに分割するステップと、各ブロックに対して1つまたは複数の誤り訂正コードワードを生成するステップと、誤り訂正コードワードをデータコードワードシーケンスに含めるステップとを含む。例えば、誤り訂正コードワードは、データコードワードシーケンス内の任意の適切な場所または複数の場所に挿入されることができる。それぞれのデータストリームを結合することは、それぞれのデータストリームを連結することを含むことができる。

【００１２】

第1の態様の例では、本方法は、割り当て規則に従って、第1のQRコードの符号化領域にわたって分散された複数のデータピクセルに符号化データの一部または全体を分散的に格納することをさらに含むことができ、データピクセルはQRコードにおけるデータ記憶単位として定義される。それによって、第1のQRコードの任意の局所的な損傷は複数のアプリケーションにわたって分散されることができ、これは、アプリケーションごとの損傷がより少なく、アプリケーションごとの完全な訂正の確率がより高いことを保証する。またこれは、QRコードリーダが各アプリケーションのアプリケーションデータのみを読み取ることを可能にし、読取処理を高速化することができる。

【００１３】

第1の態様の例では、本方法は、符号化データの一部を分散的に格納するステップを含む場合、符号化データの別の部分を第1のQRコード以外の第2のQRコードに記憶することをさらに含む。これにより、データ記憶資源を最適化するために、複数のアプリケーションのための符号化データの格納を他のQRコードと共有することができる。

【００１４】

第1の態様の例では、アプリケーションごとに使用される、誤り検出または訂正機構からのそれぞれの誤り検出または訂正データは、アプリケーションごとの各データコンテナに含まれる。これにより、各データコンテナの符号化データ中の誤りを検出または訂正することができる。

【００１５】

第1の態様の例では、符号化データは、他のデータコンテナ内の情報（例えば、コードワード）に基づいてそれぞれのデータコンテナ内に誤りがあるかどうかを検出するために複数のアプリケーションの全てのアプリケーションによって共有される全体的な誤り検出機構とともに使用するために構成されたデータ、および/または、他のデータコンテナ内の情報（例えば、コードワード）に基づいてそれぞれのデータコンテナ内の誤りを訂正するために複数のアプリケーションの全てのアプリケーションによって共有される全体的な誤り訂正機構とともに使用するために構成されたデータを含む。これにより、誤り検出及び誤り訂正能力を高めることができる。

【００１６】
第1の態様の例では、ヘッダは、各アプリケーションのためのそれぞれのアプリケーション長パラメータを含む。それによって、例えば、いくつかのアプリケーションは第1のQRコードの記憶容量の半分より多くを必要とするが、第1のQRコードの記憶容量が複数のアプリケーションの間で等しく分割されると仮定される場合に、データリソースの無駄を回避するか、または少なくとも軽減するために、各アプリケーションのためにビット中のデータが第1のQRコードにどのように格納されるかに関する情報を示すことができる。
【００１７】
第1の態様の例では、入力ビット列は、それぞれのアプリケーションに関連するヘッダの一部を含む。これにより、各アプリケーションに関連するヘッダの情報をアプリケーションデータに含めることができるので、各アプリケーションの誤り訂正能力によって、ヘッダの当該部分を誤りから保護することができる。したがって、それぞれのアプリケーション内のパリティビットまたは誤り訂正ビットは、ヘッダ内の特定のフィールドを保護することができる。
【００１８】
第1の態様の例では、本方法は、第1のQRコード上に物理的に重畳されているグラフィカル表現から画像データを収集することをさらに含み、符号化データのヘッダ内に、グラフィカル表現の存在と、第1のQRコード上のグラフィカル表現によって占有される領域との指標を含み、グラフィカル表現によって占有される領域と一致する第1のQRコード内の領域を占有する第1のQRコードの符号化領域のデータピクセルは符号化データの一部または全体の格納から除外される。これにより、重畳されたグラフィック表現によってもたらされる誤りを訂正するための第1のQRコードの誤り訂正能力を維持することができるので、符号化データに誤りを意図的に導入する方法を使用するよりも大きなグラフィック表現（例えば、文字、図形、画像、ロゴ、アイコン、デザイン、パターン、モデルなど）を第1のQRコードに重畳することができる。
【００１９】
第1の態様の例では、本方法は、複数のアプリケーションの全てのアプリケーションによって共有される単一の誤り訂正機構よりも低い誤り訂正レベルでアプリケーションごとにそれぞれの誤り訂正機構を構成することをさらに含む。この構成情報は、ヘッダまたはデータコンテナに格納されることができる。誤り訂正の既知のレベルL、M、Q、Hのリストから、アプリケーションごとのECMは、例えば、最低の誤り訂正レベルLを有することができ、一方、複数のアプリケーションの全てのアプリケーションによって共有されるECMは、例えば、最高の誤り訂正レベルHを有することができる。第1のQR符号が誤り訂正機構としてリードソロモン誤り制御コードを使用する場合、4つの誤り訂正レベルL、M、Q、Hはそれぞれ約7％、15％、25％、30％の回復能力を提供する。
【００２０】
第1の態様の例では、第1のQRコードが少なくとも公開鍵の情報を記憶するためのデバイスプロビジョニングプロトコル（DPP）またはWi-Fi Easy Connectブートストラッピング情報を含む。それによって、それぞれのWi-Fi接続が複数のコンフィギュレータと第1のQRコードが添付されるエンローリーとの間で確立され得る場合、各コンフィギュレータは、ブートストラップ処理中にエンローリーの第1のQRコードをスキャンし、そのそれぞれの公開鍵、例えば、その公開識別鍵を読み出すことができる。
【００２１】
第2の態様によれば、第1のQRコード内の複数のアプリケーションのうちのそれぞれのアプリケーションの情報を復号することに向けられ、情報は、第1のQRコードにおいて符号化データとして格納され、符号化データは少なくともヘッダとアプリケーションごとのそれぞれのデータコンテナとを含み、当該方法は少なくとも、第1のQRコードのヘッダを読み取るステップであって、このヘッダは少なくとも、複数のアプリケーションの存在を示す単一の識別子と、アプリケーションごとのそれぞれのアプリケーション識別子とを含む、ステップと、ヘッダから、複数のアプリケーションの存在を示す単一の識別子を使

用することによって、第1のQRコードを識別するステップと、ヘッダから、それぞれのアプリケーションを識別するステップと、それぞれのアプリケーションに関連付けられたそれぞれのデータコンテナを識別するステップとを含む。代替として、第1のQRコードは、例えば、ユーザが理解できる印刷パターン（例えば、マスタを指定するための文字MまたはMatterに基づくQRコード）によって視覚的に識別されることができ、その結果、識別は、例えばQRコードリーダ操作する人によって実行されることができる。

【００２２】

第2の態様の例では、本方法は、それぞれのアプリケーションのデータコンテナに関連付けられた全てのピクセルを読み取って、それぞれのアプリケーションに関連付けられた少なくとも1つのデータコードワードと、複数のアプリケーションの全てのパリティまたは誤り検出または誤り訂正ビットとを読み出すステップと、それぞれのアプリケーションの誤りの無いアプリケーションデータを取得するステップとをさらに含む。これにより、例えばQRコードリーダなどの復号装置によって、第1のQRコードの全てのデータピクセルを読み取る必要なく、各アプリケーションのデータピクセルのみを読み取ることで、複数のアプリケーションのうちの各アプリケーションの情報を選択的に取り出すことができ、これにより、読み取りプロセスを高速化することができる。

【００２３】

第2の態様の例では、本方法は、事前構成されたアプリケーションまたはポリシーまたはコンテキストに基づいて複数のアプリケーションの中からアプリケーションを選択するステップと、アプリケーションまたはプロトコルを開始するためにそれぞれのアプリケーションから復号された情報を使用するステップとをさらに含む。例えば、開始されるアプリケーションまたはプロトコルは、ワイヤレス製品のためのコミッショニングアプリケーションであり得る。前記の事前構成を例示すると、QRコードリーダは、例えば、特定のアプリケーション、例えば、MatterなどのSHSのみを使用するように事前構成する製造業者からのものであることができる。しかし、QRコードリーダが、例えば、Wi-Fiを使用する別の製造業者からのものである場合、この別の製造業者は、エンドユーザがWi-Fiネットワークを使用するのかSHSネットワークを使用するのかを知ることができず、その選択はコンテキストに依存する。

【００２４】

第2の態様の例では、本方法は、第1のQRコードから第1のコミッショニングアプリケーションとして複数のアプリケーションのうちからアプリケーションを選択するステップと、選択された第1のコミッショニングアプリケーションに関連するコミッショニングデータを読み出すステップと、第1のコミッショニングアプリケーションを開始するステップと、第1のコミッショニングアプリケーションが成功するかまたは失敗するまで第1のコミッショニングアプリケーションを実行するステップとをさらに含む。第1のコミッショニングアプリケーションが失敗した場合、本方法は、第1のQRコードから第2のコミッショニングアプリケーションとして複数のアプリケーションのうちの別のアプリケーションを選択するステップと、第2のコミッショニングアプリケーションに関連するコミッショニングデータを読み出すステップと、第2のコミッショニングアプリケーションを開始するステップとを含む。これにより、複数のコミッショニングアプリケーションの組み合わせを回避することができる。

【００２５】

通信プロトコルのためのコミッショニング情報を符号化する第2の態様の例では、本方法は、事前構成された値、ポリシー、コンテキストおよび第1のQRコード内のデータの一部のうちの少なくとも1つに基づいて第1のコミッショニングプロトコルを選択するステップをさらに含む。

【００２６】

第2の態様の例では、第1のプロトコルが開始され、第1のプロトコルが終了しない限り第2のプロトコルはトリガされない。

【００２７】

第2の態様の例では、本方法は、第1のQRコードを読み取るステップと、読み取られた第1のQRコードから複数のアプリケーションのうちのサポートされるアプリケーションを決定するステップと、事前構成された選択、ポリシー、コンテキストおよび第1のQRコードに含まれるプレファレンスのうちの少なくとも1つに基づいて、サポートされるアプリケーションの中からアプリケーションを選択するステップと、選択されたアプリケーションを第1の選択されたアプリケーションとして開始するステップとを含む。コミッショニングアプリケーションの場合、コンフィギュレータまたはコミッショナは、第1の選択されたアプリケーションが成功しなかったかまたは失敗した場合に限り、例えば、最小限の回数N（例えば、N = 1、2、・・・）、第1の選択されたアプリケーションに関連するコミッショニングプロセスが成功しなかったかまたは失敗した場合に限り、第2の選択されたアプリケーションを開始してはならない。

【００２８】

第２の態様の例では、 本方法は 第1のQRコードを読み取るステップと、 読み取られた第1のQRコードから複数のサポートされているアプリケーションを決定するステップと、事前設定された選択肢、ポリシー、コンテキストおよび前記第1のQRコードに含まれるプリファレンスのうちの少なくとも1つに基づいて、アプリケーションの実行順序を選択するステップと、 最初のアプリケーションを開始するステップと (コミッショニングアプリケーションの場合、コンフィギュレータまたはコミッショナは、少なくとも、事前に設定されたターゲットステップまで、例えば、第1の選択されたアプリケーションに関連するコミッショニングプロセスが最小回数N（例えば、N＝1、2、...）成功しなかったかまたは失敗した場合に限り、第2の選択されたアプリケーションを開始すべきではない)、第１のアプリケーションの実行が成功した場合（第２のコミッショニングプロトコルが中間段階として第１のコミッショニングプロトコル（DPP）に依存する可能性がある場合、部分的な成功でもよい）、 第２のアプリケーションを開始するステップとを有する。後者の2つのアプリケーションの使用例としては、Wi-Fiネットワークにデバイスを登録するために、第2のアプリケーションを使用する代わりに、第1のアプリケーションの中間ステップとして第1のコミッショニングプロトコル（DPP）を使用し、第2のアプリケーションを使用してデバイスをクラウドサービスやクラウド内のバックエンドなどに接続することが考えられる。これの利点は例えば、第1のアプリケーションが、正しいクラウドサービスへの接続を提供しない一方で、第2のアプリケーションよりもWi-Fiネットワークに接続するためのより安全な方法を提供することである。

【００２９】

第3の態様によれば、第1のQRコードに格納するための複数のアプリケーションの情報を符号化するための装置に関し、当該装置は、第1の態様おいて特許請求される方法および/または第1の態様の例のいずれかの方法を実行するように適合される。

【００３０】

第4の態様によれば、第1のQRコード内の複数のアプリケーションの中のそれぞれのアプリケーションの情報を復号するための装置であって、当該情報は、第1のQRコード内の符号化データとして格納され、符号化データは、少なくともヘッダと、アプリケーションごとのそれぞれのデータコンテナとを含み、当該装置は、第2の態様おいて特許請求される方法および/または第2の態様の例のいずれかの方法を実行するように適応される。

【００３１】

関連するQRコードを有するデバイスを対象とする第5の態様によれば、QRコードは2つの異なるコミッショニングプロトコルのためのコミッショニング情報を含み、当該デバイスは、コミッショナーデバイスから第1のコミッショニングプロトコルの初期コミッショニングメッセージを受信すると、第1のコミッショニングプロトコルが終了するまで、第2のコミッショニングプロトコルの初期コミッショニングメッセージを受け入れない。

【００３２】

システムを対象とする第6の態様によれば、当該システムは、少なくとも、カメラおよび

第1の通信インタフェイスを有する第4の態様に記載の装置と、関連するQRコードおよび第2の通信インタフェイスを有する第1のデバイスと、第3の通信インタフェイスを有する第2のデバイスと、第3のデバイスとを含み、前記装置は、第3のデバイスとインタフェイスし、第1のデバイスとの第1のコミッショニングプロトコルを開始および実行するように適応され、かつ/または、第3のデバイスは、第2のデバイスからの第1のデバイスとの、第1のコミッショニングプロトコルと同一かまたは異なる第2のコミッショニングプロトコルをトリガするように適応される。

【００３３】

コンピューティング装置を対象とする第7の態様によれば、コンピュータプログラムは、当該コンピュータプログラムコンピューティング装置の処理ユニット上で実行されるとき、コンピューティング装置が、第1の態様において特許請求される方法および/または第1の態様の例のいずれかの方法を実行するように構成されるプログラム命令またはコード手段を有する。

【００３４】

コンピューティング装置を対象とする第7の態様によれば、コンピュータプログラムは、当該コンピュータプログラムコンピューティング装置の処理ユニット上で実行されるとき、コンピューティング装置が、第２の態様において特許請求される方法および/または第２の態様の例のいずれかの方法を実行するように構成されるプログラム命令またはコード手段を有する。

【００３５】

上記の装置は、ディスクリートハードウェアコンポーネント、集積チップ、またはチップモジュールの配列を有するディスクリートハードウェア回路に基づいて、またはメモリに記憶された、コンピュータ可読媒体上に書き込まれた、またはインターネットなどのネットワークからダウンロードされたソフトウェアルーチンもしくはプログラムによって制御される信号処理デバイスもしくはチップに基づいて実装され得ることに留意されたい。

【００３６】

本発明の好ましい実施形態は、従属請求項又は上記の実施形態及びそれぞれの独立請求項との任意の組み合わせであることができることを理解されたい。

【００３７】

本発明のこれら及び他の態様は、以下に記載される実施形態から明らかになり、それらを参照して説明される。

【図面の簡単な説明】

【００３８】

本出願をより良く理解するために、ここで、例として添付の図面を参照する。

【図１】従来の実施形態に係るバージョン7のQRコードシンボルの構造を示す図。

【図２】本発明の実施形態による例示的な符号化手順を説明する概略フローチャート。

【図３】本発明の実施形態による2つのアプリケーションのための符号化データへのQRコードのデータピクセルの概略的な割り当てを示す図。

【図４】本発明の実施形態による3つのアプリケーションのための符号化データへのQRコードのデータピクセルの概略的な割り当てを示す図。

【図５】本発明の実施形態によるピクチャの存在下での2つのアプリケーションのための符号化データへのQRコードのデータピクセルの概略的な割り当てを示す図。

【図６】本発明の実施形態による例示的な復号手順を説明する概略フローチャート。

【図７】本発明の実施形態による別の例示的な復号手順を説明する概略フローチャート図。

【図８】本発明の実施形態による別の例示的な復号手順を説明する概略フローチャート。

【図９】本発明の実施形態による複数のアプリケーションの情報を符号化してQRコードを作成することが可能なデバイスの概略ブロック図。

【図１０】本発明の実施形態によるコミッショニングのための概略システムを示す図。

【図１１】従来の実施形態によるコミッショニングプロトコルを示す図。

【図１２】本発明の実施形態によるコミッショニングプロトコルを示す図。
【図１３】本発明の実施形態によるコミッショニングプロトコルを示す図。
【図１４】本発明の実施形態によるQRコードの単一スキャンを用いて読取りおよび処理するためのシステムを示す図。
【発明を実施するための形態】
【００３９】
本発明の実施形態は、QRコード、特に複数のアプリケーションまたは実装を扱うことができるQRコードに基づいて説明される。
【００４０】
国際標準化機構（ISO）は、次のようにQRコードの規格化されたシンボル構造を定義する、"Information technology - Automatic identification and data capture techniques - QR code bar code symbology specification"という名称のQRコードのための規格ISO/IEC18004:2015を確立した。QRコードシンボルは、モジュールと呼ばれる、明るい正方形および暗い正方形の2次元アレイとして構築される。バージョン1 からバージョン40 までの40種類のサイズのQRコードシンボルバージョンがある。各QRコードシンボルバージョンは異なる数のモジュールから構成され、したがって、異なるQRコードバージョンは異なるデータ容量を生じさせる。規格ISO/IEC18004:2015の段落6.3.1の図3から、本出願の図1は、符号化領域1（すなわち、フォーマット情報、バージョン情報、データコードワードおよび誤り訂正コードワード）、および機能パターン2（すなわち、ファインダ、セパレータ、タイミングパターンおよびアライメントパターン）からなるバージョン7のQRコードシンボルの構造を示す。機能パターンはデータを符号化せず、そのシンボルは、4つの辺全てにおいてクワイエットゾーン3として示される空の領域によって囲まれる。
【００４１】
メッセージデータは、コードワードのシーケンスに分割されるビットストリームとして符号化される。全てのコードワードは8ビット長である。コードワードは、QRコードバージョンおよび誤り訂正レベルに基づいて、いくつかの誤り訂正ブロックにグループ化され、適切な数の誤り訂正コードワードが各ブロックのために生成される。誤り訂正メカニズム（ECM）は、シンボルの一部が汚れているかまたは損傷している場合に、メッセージの正しい復号を可能にする。規格ISO/IEC18004:2015のQRコードは、誤り検出及び訂正のためにリードソロモン誤り制御符号を使用する。リードソロモン符号は［n, k, n-k + 1］符号であることが知られており、すなわち、次元kおよび（有限体にわたる）長さnの線形ブロック符号であり、最小ハミング距離がn-k + 1に等しい。（任意のMDS符号などの）リードソロモン符号は、誤り（すなわち、未知の位置における誤ったコードワード）の2倍の数の消失（すなわち、既知の位置における誤ったコードワード）を訂正することができ、誤りおよび消失の任意の組合せは、関係2E + S≦n-kが満たされる限り訂正することができ、ここで、Eはブロック内の誤りの数であり、Sはブロック内の消失の数である。これらのECMのさらなる例は、ハミングコードまたは低密度パリティチェックコードを含むことができる。ユーザが選択することができる4つの誤り訂正レベルL、M、Q、Hがある。各レベルは異なる誤り訂正能力を提供し、Lは7％まで、Mは15％まで、Qは25％まで、Hは30％までである。より高い誤り訂正レベルは回復能力を改善するが、符号化データの量、またはパリティシンボルの量も増加させる。これは、同じメッセージがより高い誤り訂正レベルを使用して符号化される場合、より大きなQRコードバージョンが必要とされることを意味する。データコードワード、誤り訂正ブロック及び誤り訂正コードワードの数は、QRコードバージョン及び誤り訂正レベルに依存する。
【００４２】
本発明の例示的な実施形態では、オブジェクト、製品またはデバイスに添付された第1のQRコードは、複数のアプリケーション（または実装）のための符号化データを格納するために使用される。単一のアプリケーションのための符号化データを格納するQRコードと区別するために、「マスタQRコード」という用語は、第1のQRコード、すなわち、複

数のアプリケーションのための符号化データを格納するQRコードを互換的に表すために、説明において使用され得ることに留意されたい。第1のQRコードは、符号化された形で複数のアプリケーションの情報を含むことができる。「アプリケーションのための」という表現は、本明細書では「アプリケーションと共に使用するように構成された」を意味すると理解される。

【００４３】

それぞれのアプリケーションの情報は、例えば、アプリケーションの名前（例えば、「会社XへのURL」、または「Wi-Fiネットワーク構成」）、それぞれのアプリケーションを一意に識別する識別子、OAのための設定データ、そのQRコードおよびアプリケーションのために使用するアプリまたはプログラムへのURL、およびそれぞれのアプリケーションのためのQRのロケーション（例えば、「緑色の矢印によって示されるQRコード」、または「青色の長方形によって示されるQRコード」、または「オン/オフスイッチの右側のQRコード」）のうちの少なくとも1つを非網羅的に表すことができる任意の文字のセットであることができる。

【００４４】

符号化された情報からの符号化されたデータは、少なくともヘッダと、アプリケーションごとのそれぞれのデータコンテナとを含むことができる。ヘッダは、複数のアプリケーションの存在を示す単一の識別子と、複数のアプリケーションのカウントと、アプリケーションごとのそれぞれのアプリケーション識別子とを含むことができる。単一の識別子は、複数の（特定の）アプリケーション、例えば、Wi-Fi Easy ConnectおよびSHSに関連する2つのアプリケーションの存在を暗黙的に示すことができる。データコンテナは、アプリケーションのアプリケーションデータを含むことができ、アプリケーションデータを格納するために予約された第1のQRコードのデータピクセルを指すことができる。追加の実施形態では、データコンテナは、アプリケーションデータを格納するために使用される第1のQRコード内の物理的位置を指すこともできる。データコンテナは、アプリケーションに関連付けられたデータを含むビット列の一部を指すこともできる。

【００４５】

なお、本発明において、「データピクセル」とは、QRコードにおける格納単位をいう。例えば、「データピクセル」がQRコード内の最小の可能な格納単位である場合、それは、ある量のビット、例えば1ビットを格納することのみが可能である。「データピクセル」がDビットを格納することができるQRコードにおいてbビットを記憶することができるデータ格納単位を指す場合、QRコードは、D/b「データピクセル」を格納することができる。したがって、「データピクセル」という用語は、「画像ピクセル」という用語と混同されるべきではない。例えば、QRコードの画像は、カメラによるキャプチャ時の画像ピクセルからなり、1つまたは複数のピクチャピクセルのグループは、それぞれのデータピクセルを表し得る。

【００４６】

それぞれのECM(例えば、リードソロモン符号、ハミング符号、低密度パリティチェック符号など）は、アプリケーションごとにそれぞれのデータコンテナの符号化データにおける任意の誤りを訂正するために、アプリケーションごとに各データコンテナに含まれることができ、それによって、単一よりも多くのアプリケーションで使用するための符号化データを含む第1のQR符号におけるアプリケーションデータの高速読み取りを可能にする。特に、OAiによって示されるそれぞれのアプリケーションがアプリケーションデータDiを符号化することを必要とする場合、ECMは、Diをコードワードciにマッピングするために使用される。ECMは、ciに何らかの誤りを含む場合であっても、ciからDiを取り出すことができる。まず、アプリケーションデータDiをb個のブロックに分割し、合計b個のコードワードを得ることができる。アプリケーションデータに引き起こされる損傷のリスクを低減するために、これらの異なるコードワードのビットまたはシンボルはインターリーブされ、すなわちミックスされることができ、したがって、（例えば、QRコードの物理的エリアに引き起こされる損傷に起因して）誤りのバーストが発生する場合、誤

りは複数のコードワードにわたって分散される。
【００４７】
オプションの実施形態では、それぞれの誤り検出機構(ＥＤＭ)(例えば、巡回冗長検査（ＣＲＣ）、パリティ検査、チェックサムなど）またはそれぞれの誤り訂正機構（ＥＣＭ）が、アプリケーションごとに各データコンテナの符号化データの誤りを検出または訂正するために、アプリケーションごとに各データコンテナに含まれることができる。
【００４８】
オプションの実施形態では、符号化データは、1つまたは複数の他のデータコンテナ内の情報に基づいてデータコンテナ内の誤りを検出するために、複数のアプリケーションの全てのアプリケーションによって共有される全体的なＥＤＭを含むことができる。
【００４９】
オプションの実施形態では、符号化データは、1つまたは複数の他のデータコンテナ内の情報に基づいてデータコンテナ内の任意の誤りを訂正するために、複数のアプリケーションの全てのアプリケーションによって共有される全体的なＥＣＭを含むことができる。
【００５０】
図2は、本発明の例示的な実施形態による、第1のＱＲコードに格納するための複数のアプリケーションの情報を符号化する例示的な符号化方法を説明する概略フローチャート200を示す。
【００５１】
ステップ210において、複数のアプリケーションの情報が収集される。
【００５２】
ステップ220において、情報は符号化データへと符号化され、符号化データは少なくともヘッダとアプリケーションごとのそれぞれのデータコンテナとを含む。ヘッダは、複数のアプリケーションの存在を示す単一の識別子と、複数のアプリケーションのカウントと、アプリケーションごとのそれぞれのアプリケーション識別子とを含むことができる。
【００５３】
図2の上記の符号化方法を参照する詳細な例では、各アプリケーションがデータコンテナに関連付けられている複数のアプリケーションの情報は、第1のＱＲコードに格納するために、全てのデータコンテナおよびヘッダによって共有されるＥＣＭと、オプションとしてＥＤＭとを使用して、以下の例示的な方法に従って、上記の符号化データへと符号化されることができる。　この例では、単一のＱＲコードが複数のアプリケーションへの情報を含むことができることに留意されたい。
【００５４】
第1のステップでは、第1のＱＲコード（すなわち、マスターＱＲコード）に関連する入力データが収集される。そしてこの入力データは、複数のアプリケーションのカウントと、アプリケーションごとのそれぞれのアプリケーション識別子とを少なくとも含むことができる。ＯＡ1、・・・、ＯＡＮとして参照されるＮ個のアプリケーションの例では、ヘッダデータ（ＨＤ）と呼ばれるこれらの入力データは、Ｎ，ＯＡ1，・・・，ＯＡＮのように構成されることができる。それぞれのアプリケーション識別子は、例えばそれらを登録または標準化することによって、それぞれ一意であることに留意されたい。識別子ＯＡ1およびＯＡ2を有する2つのアプリケーションの例では、ヘッダのコンテンツは、"2，ＯＡ1，ＯＡ2"として明示的に構造化されることができ、あるいは、暗黙的に“２，ＯＡ1,ＯＡ2"を意味する単一の識別子（ＩＤ）がヘッダに含まれることができる。ヘッダはまた、コンテナの使用順序を示すために使用されることができる。
【００５５】
なお、上記の入力データは、アプリケーション毎に何ビットのデータが格納されているかについての情報を与えない。この場合、前述のように、所与の格納容量を有するＱＲコードについて、ＱＲコードリーダは、利用可能なそれぞれのアプリケーションの数の間で格納容量が等しく分割されると仮定する必要があるだろう。これは、例えば、１つのアプリケーションが非常にわずかなデータ格納しか必要とせず、別のアプリケーションがはるか

に多くの、特に所与のQRコードタイプの格納容量の半分をわずかに超えるデータ格納を必要とする場合、リソースの浪費につながる可能性がある。この場合、その長さが含まれない場合、これらの2つのそれぞれのアプリケーションは、より大きいQRコードで符号化される必要がある。この問題を回避するために、オプションの実施形態では、ヘッダデータ（HD）は、各アプリケーションについての長さのパラメータも含み、したがって、N, OA1, ..., OAN, L1,..., LNのように構成されることができる。

【００５６】

第2のステップでは、N個のそれぞれのアプリケーションのそれぞれについて、それぞれのアプリケーションOAiのアプリケーションデータDi(すなわちDi内の文字）が収集される。

【００５７】

第2のステップの第1のサブステップにおいて、Diからのそれぞれのビットストリームデータ（BSD）（すなわち、Diからの入力ビット列BSDi）が計算される。なお、この入力ストリングは、各アプリケーションOAiに関するヘッダデータ（HD）の部分、例えば、各アプリケーションOAiのOAi識別子及びN個のアプリケーションのリストにおける位置、又は各アプリケーションOAiの長さLiを含むことができる。このHD情報を入力ビット列BSDiに含める利点は、それぞれのアプリケーションに関連するECMおよびオプションとしてEDMによって、HD情報を誤りから保護することである。言い換えれば、それぞれのアプリケーションのアプリケーションデータ内のパリティビットは、ヘッダ内の特定のフィールドを保護することができる。さらに、ヘッダの信頼性を高めるために、2つのオプションが、単独でまたは組み合わせて、提案されることができる。第1のオプションでは、ヘッダが入力ビット列BSDiにアクセスする前に任意の誤りが訂正され得るように、ヘッダがそれ自体の誤り訂正能力を含むことができる。第2のオプションでは、ヘッダ情報は、例えば、1つ、2つまたは3つの「眼」または「位置マーカ」または「3つのコーナーにおけるスクエア中のスクエア」に近いピクセルに物理的に格納されることができる。その理由は、これらの位置マーカがQRコードを識別して位置決めするために必要とされるからである。これは、図1に示すフォーマット情報およびバージョン情報と同様である。　したがって、位置マーカが除去されるかまたは損傷を受ける場合、QRコードはいずれにしても読み取ることができない。しかしながら、ヘッダ情報が例えば1つまたは複数の位置マーカに近いいくつかの既知の物理的位置に配置される場合、ヘッダ情報が読み取られる可能性が増大する。

【００５８】

第2のステップの第2のサブステップにおいて、誤り検出ビット列EDi、例えばEDMがCRCベースである場合にはCRCが、入力ビット列BSDiからオプションとして計算される。

【００５９】

第2のステップの第3のサブステップでは、潜在的な誤りを拡散するためにEDiおよびBSDiをインターリーブすることによって、IBSDiによって表されるインターリーブされた入力ビット列BSDiがオプションとして取得される。インターリーブが行われるかどうか、およびどのように行われるかをQRコードリーダが知らなければならないことに留意されたい。これは規格に基づくことができ、または例えば、ヘッダ内に明示的または暗黙的に格納されることができる。これは、本発明の他の実施形態における他のインターリーブステップにも当てはまる。

【００６０】

第2のステップの第4のサブステップにおいて、インターリーブされた入力ビット列BSDiを1つ以上の8ビットデータコードワードのシーケンスに分割し、ECM（例えば、リードソロモン符号）を処理できるようにデータコードワードシーケンスを（QR符号のバージョンおよび誤り訂正レベルL、M、Q、Hに応じて）必要な数のブロックに分割し、各ブロックのために1つ以上の8ビット誤り訂正コードワードを生成し、誤り訂正コードワードをデータコードワードシーケンスの末尾に付加するかまたは誤り訂正コードワードをデータコードワードシーケンスの任意の適当な場所に挿入することによって、１つ以上の8

ビットコードワードCiが計算される。
【００６１】
この第4のサブステップは、OAごとに誤り訂正能力があることを明らかにすることに留意されたい。2つのアプリケーションOA1，OA2のアプリケーションデータを、全てのアプリケーションデータに使用される単一の誤り訂正ビット列とともに格納する場合、トータルの格納要件は、D = D1 + D2 + PBとなり、ここで、D1およびD2はそれぞれOA1およびOA2のアプリケーションデータを指し、PBは2つ全てのアプリケーションOA1およびOA2のパリティビットを指し、誤り訂正のために必要とされる。対照的に、現在の第4のサブステップにおいて、例えば、2つのアプリケーションOA1，OA2のアプリケーションデータを格納しなければならない場合、OA1およびOA2のそれぞれのアプリケーションデータに適用される誤り訂正ビット列が存在する。つまり、トータルの格納要件は、Dではなく、D' = D1 + D2 + PB1 + PB2 になる。ここで、D1 とD2 はそれぞれOA1 とOA2 のアプリケーションデータを指し、PB1 はアプリケーションOA1 のパリティビットを指し、PB2 はアプリケーションOA2 のパリティビットを指す。D'はDより大きいかもしれないが、QRコードリーダはアプリケーションOA1に関心がある場合にはD1 + PB1のみを読み取るだけでよく、アプリケーションOA2に関心がある場合にはD2 + PB2のみを読み取るだけでよいので、この合計D1 + PB1またはD2 + PB2はDより小さくなると予想される。
【００６２】
第2のステップの第5のサブステップでは、1つまたは複数の8ビットコードワードCiは、オプションとして、それぞれのアプリケーションOAiのためのインターリーブされたコードワードICiを得るために、それ自体と、IBSDiと、またはそれらの組み合わせと、インターリーブされる。
【００６３】
上記のサブステップは、異なる順序で実行され得ることに留意されたい。例えば、第4のサブステップは第2のサブステップの次でもよく、第3のサブステップは第4のサブステップの後でもよい。
【００６４】
第3のステップでは、N個のアプリケーションOA1，...,OANのそれぞれに対するそれぞれのインターリーブされたコードワードICi、および、上記入力ストリングがそれぞれのアプリケーションOAiに関連するHDの一部も含む場合にはオプションとしてヘッダデータ（HD）を所与として、IC1,...，ICNの、およびオプションとしてHDの連結TICが得られる。
【００６５】
第3のステップの第1のサブステップでは、オプションとして、第2のEDMを適用してTICの誤りを検出できるようにする誤り検出ビット列ED（例えば、CRC）を計算し、この誤り検出ビット列EDをICに付加することによって、EDTIC= TIC ┆ EDが得られる。
【００６６】
第3のステップの第2のサブステップにおいて、IEDTICは、オプションとして、、任意の潜在的な誤りを拡散するためにEDおよびTICをインターリーブすることによって得られる。一例では、インターリービングは、各IC内のEDの一部および/または各IC内のED全体をインターリーブすることができる。
【００６７】
第3のステップの第3のサブステップにおいて、パリティビット（PB）は、オプションとして、IEDTIC上で、およびオプションとしてHD┆IEDTIC上で、1つまたは複数の8ビットコードワードを計算するために第2のECMを適用することによって取得される。　第2のECMはICi自体を変更してはならないことに留意されたい。例えば、第2のECMは、IEDTICに付加されることができるパリティビット（PB）を計算することからなる。
【００６８】
第3のステップの第4のサブステップでは、第2のECMによって計算されたパリティビッ

ト（PB）は、オプションとして、各アプリケーションOAiのためのそれぞれのインターリーブされたコードワードICiの間で（例えば、インターリーブによって）分散される。例えば、k個のパリティビット（PB）が取得され、2つのアプリケーションOA1およびOA2があると仮定すると、k個のパリティビットは、これらの2つのアプリケーションOA1およびOA2に関連するデータコンテナ中に分
散されることができる（例えば、OA1に関連するデータコンテナに対してk-xビットと、OA2に関連するデータコンテナに対してxビット）。例示的な変形例では、k個のパリティビットが両方のデータコンテナに格納されることができる。アプリケーションごとにデータコンテナに格納されるように選択されたパリティビット（PB）は、それぞれのアプリケーションのICi上で分散される。

【００６９】

例示的な実施形態では、アプリケーションごとのECM（すなわち、データコンテナごとのECM）は、複数のアプリケーションの全てのアプリケーションによって共有される単一のECM（例えば、第2のECM）よりも低い誤り訂正レベルで構成されることができる。例えば、誤り訂正の既知のレベルL、M、Q、Hのリストから、アプリケーションごとのECMは最低の誤り訂正レベルLを有することができ、一方、複数のアプリケーションの全てのアプリケーションによって共有されるECMは最高の誤り訂正レベルHを有することができる。第1のQRコードがリードソロモン誤り制御コード化を使用する場合、4つの誤り訂正レベルL、M、Q、Hはそれぞれ約7％、15％、25％、30％の回復能力を提供する。これは、より少ないアプリケーションデータが関与するので、それぞれのアプリケーションのアプリケーションデータの迅速な読み取りを可能にすることができる。

【００７０】

オプションの実施形態では、符号化データの一部または全体が、割り当て規則に従って、第1のQRコードにわたって、より正確には第1のQRコードの符号化領域にわたって分散された複数のデータピクセルに分散して格納されることができる。

【００７１】

第1のQRコードのデータ格納リソースが制限される例では、符号化データは、符号化データの全体が第1のQRコードに格納される代わりに、符号化データの一部が第1のQRコードに格納され、残りの部分が第2のQRコードに格納されるように、複数の異なるQRコード、例えば、第1のQRコードおよび第2のQRコードに格納され得る。この場合、マスタQRコードとしての第1のQRコードは、マスタQRコードに対する他のQRコード（例えば、第2のQRコード）の位置を示す、ユーザが理解可能な印刷パターンをその内部に含むことができる。一例では、ユーザが理解可能なパターンは、他のQRコードの各々（例えば第2のQRコード）を指す1つまたは複数の（着色された）矢印であるか、またはマスタQRコードおよび全ての他のQRコード（例えば第2のQRコード）を表す（着色または番号付けされた）矩形を有する一種のチェッカーボードであることができる。

【００７２】

第1のQRコードの符号化領域にわたって符号化データを分散的に格納するためのこれらのデータピクセルの決定は、異なる割り当て規則に従って実行され得る。なお、ヘッダデータは、符号化データと同様に分散されることができる。

【００７３】

第1のQRコードがAおよびBによって示される2つのアプリケーションのアプリケーションデータを含み、データ容量がアプリケーションAおよびBのためのそれぞれのデータコンテナの両方の間で均等に共有されると仮定すると、例示的な割り当て規則は、図3に示されるように、第1のQRコード（の符号化領域）内の交互のデータピクセルにおいて、アプリケーションAおよびBのためのそれぞれのデータコンテナの符号化されたデータを格納すること（すなわち、符号化されたアプリケーションデータだけでなく、パリティ（EDMまたはECM）ビットも格納すること）を含むことができる。

【００７４】

第1のQRコードがA、BおよびCで表される3つのアプリケーションのアプリケーションデ

ータを含み、データ容量がアプリケーションA、BおよびCのための3つのそれぞれのデータコンテナの間で均等に共有されると仮定すると、例示的な割り当て規則は、図4に示されるように、第1のQRコード（の符号化領域）のデータピクセルにおいて、アプリケーションA、BおよびCのためのそれぞれのデータコンテナの符号化データを格納すること（すなわち、符号化されたアプリケーションデータだけでなく、パリティ（EDMまたはECM）ビットも格納すること）を含むことができる。

【００７５】

この例示的な割り当て規則は、QRコードの特定の部分における損傷が、それぞれのアプリケーションのための符号化されたデータまたはこれらの符号化されたデータの高い割合を損傷しないことを保証する。

【００７６】

別の例示的な割り当て規則では、アプリケーションごとのそれぞれのデータコンテナの符号化データを格納する第1のQRコード内の特定のデータピクセルは、例えば以下のように計算されることができる:(1)データピクセルがそのデカルト座標（i, j）によって識別される場合、(2)座標系（I, J）内の識別子（i,j）を有するデータピクセルは、アプリケーションごとにそれぞれのデータコンテナの符号化データを格納するために使用される(3)第1のQRコードはMxM個のデータピクセル（または要素）を有し、かつ(4)同じ量のデータピクセル（または要素）が、全てのアプリケーションの符号化データに割り当てられる(5)そして、アプリケーション番号k（0≦k≦N-1）に関連付けられた符号化データは、例えば、以下の関係式（1）を満たすデータピクセルに格納されることができる:(i* M + j) (mod N) = k with (i,j) in (I,J)　　(1)

【００７７】

それぞれのアプリケーションが異なる格納要件を有する場合、データピクセルの割り当ては、これを考慮に入れることができる。特に、N個のアプリケーションが、アプリケーションごとにそれぞれのデータコンテナの符号化データのためにL1, L2, ・・・, LNビットの長さパラメータを必要とする場合、以下の関係式（2）によって与えられるように、それらの全てを最小のもので除算し、その結果をRoundUp（）関数によって上に丸めることによって、長さを正規化することが必要とされる:NL1, NL2, ..., NLN = RoundUp(L1/Lmin), RoundUp(L2/Lmin), ..., RoundUp(LN/Lmin)　　(2)

【００７８】

RoundUp（）関数の使用は、いくつかのまたは全てのそれぞれのアプリケーションにいくつかのダミービットを付加する必要があることを意味することに留意されたい。ダミービットの内容は、例えば、誤り訂正能力が改善されるように、またはクロック再生が改善されるように、選択されることができる。明確にするために、クロック再生は、QRコードの全てのピクセルを取得するために、場合によっては（光学的に）歪み、場合によっては回転されたQRコードを含む画像をどこでサンプリングするかを決定することを意味する。QRコードの両方向にランレングス制限を実施することによって、QRコードのデータピクセル間の境界がどこにあるかの推定を改善することができる。したがって、例えば、ダミービット領域内のQRコードのデータピクセルのチェッカーボードパターンを作成することによって、特定の閾値を上回る両方向の長いランレングスが防止されるかまたはさらに良好であるように、かつ、両方向のランレングスが最小化されるように、ダミービットが選択されるべきである。これは、QRコードが曲面に印刷される場合に特に有用である。

【００７９】

別の例示的な割り当て規則では、第1のQRコードのデータピクセルを使用して、N個の異なるアプリケーション（1からNまでインデックス付けされる）のためのそれぞれのデータコンテナの符号化データを連続ラウンドで格納することができる:

【００８０】

ラウンド1:第1のアプリケーションのための符号化データの最初のNL1ビットが第1のQRコードの最初のNL1ビットに格納され、第2のアプリケーションのための符号化データ

の最初のNL2ビットが第1のQRコードの次のNL2ビットに格納され，...,第Nのアプリケーションのための符号化データの最初のNLNビットが第1のQRコードの次のNLNビットに格納される;

【００８１】

ラウンド2:第1のアプリケーションについての符号化データの次のNL1ビットが第1のQRコードの次のNL1ビットに格納され、第2のアプリケーションについての符号化データの次のNL2ビットが第1のQRコードの次のNL2ビットに格納され，...,第Nのアプリケーションについての符号化データの次のNLNビットが第1のQRコードの次のNLNビットに格納される;

【００８２】

ラウンドi:第1のアプリケーションのための符号化データの次のNL1ビットが第1のQRコードの次のNL1ビットに格納され、第2のアプリケーションのための符号化データの次のNL2ビットが第1のQRコードの次のNL2ビットに格納され，...,第Nのアプリケーションのための符号化データの次のNLNビットが第1のQRコードの次のNLNビットに格納される。

【００８３】

別の例示的な割り当て規則では、アプリケーションごとのそれぞれのデータコンテナの符号化データを格納する第1のQRコード内の特定のデータピクセルは、例えば以下のように計算されることができる:(1)データピクセルがそのデカルト座標（i，j）によって識別される場合、(2)座標系（I，J）内の識別子（i,j）を有するデータピクセルは、アプリケーションごとのそれぞれのデータコンテナの符号化データを格納するために使用される(3)QRコードはMxMピクセル（または要素）を有する(4) SNL_k = NL1 + NL2 + ...+ NLkを定める。ここで、k = 1、2，...,Nであり、NL1，NL2，...,NLNは関係式（2）によって与えられるようにそれぞれのアプリケーションのための符号化データの正規化された長さである(5)そして、SNL_kに基づいて、（I，J）におけるデータピクセル（または要素)(I,j)が、以下の関係式（3）に従ってアプリケーション番号kに関連付けられた符号化データに割り当てられる:SNL_k ≦ (i*M + j) (mod SNL_N) 〈 SNL_{k+1}　　(3)

【００８４】

なお、関係式（2）は、最小の正規化された長さが1になることを意味する。関係式（1）に関連する上記スキームは、1のグループにおいてインターリーブする。ビットはまた、長さk（k＞1）のグループにおいてインターリーブされ得ることに留意されたい。kビットの各々が1つのアプリケーションからのものである。各アプリケーションのビットは、QRコード内の領域、例えば正方形または長方形の領域にわたって分散され得る。例えば、上記の図の正方形は、1つのアプリケーションのデータピクセルを含む個々のデータピクセルまたは矩形領域を示すことができる。上述の式は、単一のデータピクセルのみではなく、s個のデータピクセルを有する矩形i，jを指し得る。領域は、形状が矩形でなくてもよく、むしろ別の形状、例えば三角形またはダイヤモンド形（すなわち、水平方向および垂直方向にその軸を有する4つのコーナーを有する菱形）を有することができることにも留意されたい。1ピクセル(すなわち1*1)より大きい矩形を有することは、両方の次元においてランレングスを制限することも可能にし、したがって、湾曲面またはしわの寄った面上のサンプリングエラーを最小限にすることに留意されたい。

【００８５】

アプリケーションごとのそれぞれのデータコンテナの符号化されたデータのためにL1，…,LNビットの異なる長さパラメータを必要とするアプリケーションを扱う別の方法は、以下の通りであり得ることに留意されたい:gが、L1，…,LNの最大公約数、すなわちL1，L2，…,LNの全てを除算する最大の整数を示すとする。ビットストリームはg個の部分に分割され、各部分は第1のアプリケーションからのL1/gビット、第2のアプリケーションからのL2/gビットなどを含む。各部分において、最初のL1/gビットは第1のアプリケーションに対応し、次のL2/gビットは第2のアプリケーションに対応し、以下同様である。例えば、N=3、L1=20、L2=30およびL3=40である場合、g=10である。10個のグ

ループの各々は、ビットAABBBCCCCを有し、ここで、A、BおよびCは、それぞれの第1、第2および第3のアプリケーションからのビットを示す。変形例は、各部分において、各アプリケーションからの最初の1つのシンボルが配置され、次いで各アプリケーションからの2番目のシンボルが配置され、各部分に2つ以上のシンボルが配置される。この場合、上記のビットシーケンスAABBBCCCの代わりに、ビットシーケンスABCABCBCCが生成される。この他の方法の利点は、それが、上向きの丸めに起因するダミービットを導入しないことである。

【００８６】

例示的な一実施形態では、これらの上記で計算されたデータピクセルに格納されるべきそれぞれのアプリケーションのための符号化データは、以下で定義されるような結合ビット列に対応することができる。第2のステップの第5のサブステップから導出される出力ビット列IC全体は、N個のアプリケーションの全てについて、アプリケーションOAi(i = 1, 2, ...,N）ごとのインターリーブされたコードワードICiの総数に対応する数のICを含むようになっている。第3のステップの第2および第3のサブステップでは、全てのアプリケーションに関連する誤り検出情報（EDI）および誤り訂正情報（ECI）がN個のアプリケーションの全てにわたって分散される。ICが長さLを有し、ECI/EDIが長さHを有する場合、全長は、Z = L + Hである。ECI/EDIのビットは、出力ビット列ICにおいて均等に分散され得る。これは、上述のように、LおよびHをJ = Min(L, H)で除算することによって正規化し、l = RoundUp(L/J)およびh = RoundUp(H/J)を得ることによって行うことができる。そして、ICおよびECI/EDIは、lビットおよびhビットのブロックに分割される。結合ビット列は、ICとECI/EDIのlビットブロックとhビットブロックを交互に連結することによって取得される。上記で計算されたデータピクセルに格納されるべき結合ビット列は、OAのICと、QRコード全体からのECI/EDIとを含むことができる。例えば、破損したQRコードに起因する誤り、またはQRコードの穴に起因する誤りのように、誤りがバーストで発生するという仮定の下では、この誤り訂正能力は、各アプリケーションのほんの一部のみが影響を受けるので、アプリケーションごとの完全訂正の高い可能性が維持されることを可能にすることに留意されたい。

【００８７】

現在のプラクティスは、QRコード上に、グラフィック表現（例えば、文字、図形、画像、ロゴ、アイコン、デザイン、パターン、モデルなど）を重ね合わせることである（例えば、QRコード上の企業ロゴの画像）。これはユーザがQRコードの目的をより容易に識別するのを助け、例えば、ユーザが理解できる印刷パターン、例えば、文字Mを重ね合わせることによってマスタQRコードであるかどうかを識別するのを助ける。QRコードは誤り訂正メカニズムに依存しており、誤り訂正機能は、重ね合わされたグラフィック表現によってもたらされるあらゆる誤りを訂正するために使用されるため、グラフィック表現（例えば、画像）を重ね合わせ、それでも機能するQRコードを得ることは実現可能である。しかしながら、これはある程度は機能するが、いくつかの制限が存在し、例えば、重畳される画像は任意に大きくすることができず、なぜなら、さもなければ、利用可能な最も強い誤り訂正符号が適用されても訂正することができない多すぎる誤りが導入されるからである。この問題に対処する例示的な実施形態は、グラフィック表現が第1のQRコードの所与の物理領域内で第1のQRコードに重畳されるという指標を含む第1のQRコードに関連する。解決策としては、第1のQRコードの符号化領域のデータピクセルのうち、第1のQRコードにおいてグラフィック表現が占める領域と一致する領域を占めるものをデータ格納から除外することが考えられる。一例では、この指標はヘッダ情報に含まれることができ、例えば、第1のQRコードの1つ、2つ、または3つの「目」または「位置マーカ」、あるいは「3つのコーナーにおける正方形中の正方形」に近いデータピクセル、すなわち、グラフィカル表現画像が通常配置される第1のQRコードの中央領域に配置されていないデータピクセルに物理的に格納されることができる。

【００８８】

一例では、この領域は、重畳されたグラフィック表現によって影響を受ける第1のQRコ

ードのデータピクセルを列挙し、領域の中心、領域形状（例えば、円形、正方形、長方形、三角形、菱形など）、および領域形状のサイズまたは半径のうちの少なくとも1つを指定することによって、特定されることができる。

【００８９】

一例では、指標は、グラフィック表現の存在を示すビット（すなわち0または1）で構成されることができ、重ね合わされたグラフィック表現が存在する場合、指標はさらに、グラフィック表現の形状（例えば、円に対して0、正方形に対して1）、および、数ビット、例えば3ビットで符号化されたグラフィック表現の（スケーリングされた）半径rで構成されることができる。半径は、例えば、QRコードバージョンに応じた固定値によってスケーリングされることができ、例えば、半径の値rは、ピクセルにおけるグラフィック表現の実際の半径がr*Fであるように、スケーリング因子Fによって乗算されることができる。この例示的な実施形態は複数の利点を有し、それらのうちの1つは、より大きなグラフィック表現をQRコードに重ね合わせることができることである。

【００９０】

ヘッダがグラフィック表現の存在を示す場合、第1のQRコードの示された物理領域内のデータピクセルは、データを格納しないことに留意されたい。したがって、第1のQRコードはこれらのデータピクセルを使用してデータを格納せず、第1のQRコードがQRコードリーダによってスキャンされるとき、これらのデータピクセルはQRコードリーダによって無視される。したがって、これは第1のQRコードに格納することができる符号化データの量に影響を与えるが、これはまた、QRコードリーダの読取りプロセスを高速化する。図3の例に基づいて、図5は、画像が存在する場合に、データピクセルがアプリケーションAとBのアプリケーションデータに交互に割り当てられる様子を示している。この技法は、単一のアプリケーションを格納するQRコードにも適用可能であることに留意されたい。図5は、第1のQRコードの中央の25個のデータピクセルによって占められる領域と一致する領域を持つ画像の存在を示し、画像の中心は文字「CI」のグループによって示され、画像によって占められる領域の他のデータピクセルは文字「I」によって示される。画像を挟んだ2つの "連続した "データピクセル同じアプリケーションAまたはBのアプリケーションデータに割り当てられる可能性があるとしても、画像の存在は、画像の領域と一致しない領域のデータピクセルの初期の割り当てを変更しないことがわかる。

【００９１】

前述のように、各データコンテナ内でECMおよびオプションとしてEDMを使用する例示的な方法は、第1のQRコード内に格納するための複数のアプリケーションの情報を符号化データ内に符号化するように説明されている。

【００９２】

本発明の例示的な実施形態では、QRコードリーダが第1のQRコード（すなわち、マスタQRコード）に格納されたアプリケーションごとのこれらの符号化データをスキャンし、選択的に読み取ることができる。これは、複数のアプリケーションのうちのそれぞれのアプリケーションの情報を復号する例示的な方法600によって達成することができ、情報は第1のQRコード中に符号化データとして格納され、符号化データは、少なくともヘッダとアプリケーションごとのそれぞれのデータコンテナとを含む。図6に概略的に記載された例示的な方法600は、少なくとも以下のステップを含むことができる：

【００９３】

ステップ602において、第1のQRコードのヘッダを読み取る。ヘッダは、複数のアプリケーションの存在を示す単一の識別子と、複数のアプリケーションのカウントと、アプリケーションごとのそれぞれのアプリケーション識別子とを含む;

【００９４】

ステップ604において、ヘッダから、複数のアプリケーションの存在を示す単一の識別子を使用することによって、第1のQRコードを識別する;

【００９５】

ステップ606において、ヘッダからそれぞれのアプリケーションを識別する。例えば、Q

Rコードリーダは、それぞれのアプリケーション識別子に対応する事前構成されたアプリケーション識別子を格納することができる;

【００９６】

ステップ608において、例えば、それぞれのアプリケーション識別子がQRコードリーダのディスプレイ上に現れる位置に基づいて、それぞれのアプリケーションに関連するそれぞれのデータコンテナを識別する;

【００９７】

ステップ610において、それぞれのアプリケーションのデータコンテナに関連付けられた全てのピクセルを読み出して、それぞれのアプリケーションに関連付けられた少なくとも1つの（例えば8ビット長の）データコードワードと、それぞれのアプリケーションのためのパリティビット（PB）、誤り検出情報（EDM）ビットまたは誤り訂正情報（ECM）ビットとを取り出す。QRコードリーダは、読み取った少なくとも1つの（例えば8ビット長の）データコードワードにリンクされたEDMまたはECMを使用して、任意の誤りを検出または訂正することができる;

【００９８】

ステップ612において、それぞれのアプリケーション（例えば、OAi）の誤りの無いアプリケーションデータD（例えば、Di）を取得する;

【００９９】

ステップ614において、ECM/EDMが全ての誤りが訂正されたかどうかを検出する能力を有する場合、ECM/EDMを使用して、それぞれのアプリケーションの取り出されたアプリケーションデータDに誤りが存在するかどうかを検出する。

【０１００】

これは、DがCRCを含む場合、またはECMがリードソロモン符号のように誤りを検出することができる場合に実行されることができ、ステップ616において、誤りが検出された場合、QRコードリーダによって、全てのデータコンテナのアプリケーションデータ全体を読み取る。そして、QRコードリーダは、残りのアプリケーションのためのパリティビット（PB）、誤り検出情報（EDM）ビットまたは誤り訂正情報（ECM）ビット（すなわち、他のデータコンテナからのパリティビット）を取り出し、これらのビットならびに全てのデータコンテナ内のアプリケーションデータを使用して、対象のそれぞれのアプリケーション内に依然として存在する誤りを訂正しようと試みることができる。

【０１０１】

ヘッダデータ（HD）を読み取るステップの後、QRコードリーダはさらに、ヘッダがそれ自体の誤り検出/訂正能力を有する場合にのみ、ECM/EDMをヘッダに適用することができることに留意されたい。

【０１０２】

なお、QRコードリーダは、各アプリケーションのデータコンテナに関連付けられた全てのピクセルを読み出すステップと、ECM/EDMを用いて、各アプリケーションの読み出されたアプリケーションデータDに誤りが存在するか否かを検出するステップにおいて、誤り検出/訂正能力が各アプリケーションだけでなく、ヘッダとアプリケーションデータとの連結にも適用される場合、ECM/EDMをヘッダに適用することができる。

【０１０３】

なお、ヘッダデータ（HD）を読み出すステップにおいて、ヘッダデータ（HD）が適切に読み出されることを確実にするために、QRコードリーダは、（ヘッダの複数のコピーが第1のQRコードにおいて利用可能である場合）ヘッダの複数のコピーを読み出すことができる。

【０１０４】

本発明の別の例示的な実施形態では、QRコードリーダは、第1のQRコード（すなわちマスタQRコード）に格納されたアプリケーションごとに、これらの符号化データをスキャンし、選択的に読み取ることができる。これは、複数のアプリケーションのうちのそれぞれのアプリケーションの情報を復号する例示的な方法700によって達成することができ

、情報は第1のQRコード中に符号化データとして格納され、符号化データは、少なくともヘッダとアプリケーションごとのそれぞれのデータコンテナとを含む。図7に概略的に説明した例示的な方法700は、少なくとも以下のステップを含むことができる：ステップ702において、（例えば、単一の識別子などの何らかのヘッダデータ情報から）第1のQRコードを、マスタQRコード、すなわち複数のアプリケーション（例えば、Easy ConnectおよびSHSに関連する2つのアプリケーション）を取り扱うQRコードであるとして識別する;ステップ704において、QRコードのシンボルを読み取り、誤り訂正後にQRコードからビット列を抽出し、ビット列は複数のアプリケーションに関連するデータを含む;ステップ706において、抽出されたビット列から、サブビット列とも呼ばれる、第1のアプリケーションに関連するビット列の一部（すなわち、データコンテナ）を特定する。ここで、サブビット文字列（すなわち、データコンテナ）の位置は、ヘッダデータまたは事前に構成されたポリシーまたはコンテキストから決定される（例えば、2つのアプリケーションEasy ConnectとSHSが異なるセマンティクスを使用する場合、ビット列の一部がEasy Connect用であり、残りの一部がSHS用であることに合意しうる）。

【０１０５】

この図7の実装は、QRコードの規格に対してほとんど変更を必要としないという利点がある。

【０１０６】

本発明の別の例示的な実施形態では、QRコードリーダは、第1のQRコード（すなわち、マスタQRコード）に格納されたアプリケーションごとのこれらの符号化データをスキャンし、選択的に読み取ることができる。これは、複数のアプリケーションのうちのそれぞれのアプリケーションの情報を復号する例示的な方法800によって達成することができ、情報は第1のQRコード中の符号化データとして格納され、符号化データは、少なくともヘッダとアプリケーションごとのそれぞれのデータコンテナとを含む。図8に概略的に記載された例示的方法800は、少なくとも以下のステップを含むことができる：ステップ802において、ストリング（例えば、所与の符号化に従う文字のシーケンス）を抽出する;ステップ804において、文字列内のヘッダ（例えば、単一の識別子）、例えば文字列内の最初のN文字を見ることによって、QRコードが複数のアプリケーション（すなわち、2つ以上のアプリケーション）を含むかどうかをチェックする;ステップ806において、ヘッダが一致する場合、それぞれのアプリケーションの情報を含むサブストリングにアクセスする。

【０１０７】

この図8の実装は、QRコードの規格に対して変更を必要としないという利点がある。

【０１０８】

第1のQRコードをマスタQRコード、すなわち複数のアプリケーションを扱うQRコードであると識別するために、一例では、QRコードリーダを扱う人が、例えばマスタQRコードに重ね合わされたユーザが理解可能な印刷パターン（例えば、文字M）によって、マスタQRコードを視覚的に識別することができる。別の例では、QRコードリーダを扱う人が、複数のQRコードのうちのどのQRコードが正しいマスタQRコードであるかを知らず、したがって、同時にキャプチャされるように複数のこれらのQRコードにQRコードリーダを向ける場合、QRコードリーダはこれらのQRコードの全てを識別し、例えば、マスタQRコードであることを示す特有の特徴（例えば、数個のピクセル）をモニタすることによって、または複数のアプリケーションの存在を示す単一の識別子を識別するためにヘッダデータを読み取ることによって、マスタQRコードの存在を決定することができる。

【０１０９】

複数のQRコードが同時に読み取られる実施形態では、それぞれのコンテナのヘッダは、コンテナがどの順序で使用されることが意図されているかを示す指標が含むことができる。

【０１１０】

図9は本発明の一実施形態による、複数のアプリケーションの情報を符号化し、QRコード910を作成することができる装置905の概略ブロック図900を示す。装置905は計算装置、例えば、コンピュータであってもよく、コンピュータは、複数のアプリケーションからの入力として情報を受け取り、次いで、図2を参照して上述の実施形態で説明したように、複数のアプリケーションの情報を符号化して、第1のQRコード910、すなわち複数のアプリケーションを扱うことが可能なQRコードを作成する。

【０１１１】

図10は、本発明の一実施形態によるコミッショニングのための概略システム1000を示す。システム1000は、第1のQRコード1010が関連付けられる少なくとも第1の装置1005と、カメラ1020を備えたQRコードリーダ1015とを含む。第2の装置1025および/または第3の装置1055も存在し得る。QRコード1010は、QRコード1010を第1の装置1005に物理的に取り付けること、および/または、QRコード1010を第1の装置1005上にもしくは第1の装置1005が入ったパッケージング上に印刷することのような任意の様々な態様によって、第1の装置1005に関連付けられることができる。

【０１１２】

第1のQRコード1010が関連付けられた第1の装置1005は、第1の通信インタフェイス1030を備える。QRコードリーダ1015のカメラ1020は、第1のQRコード1010をスキャンして読み取るために使用される。第1のQRコード1010を復号すると、QRコードリーダ1015は、例えば、ローカルポリシーまたはコンテキストに基づいて、第1のQRコード1010から選択されたアプリケーション、および第1の装置1005で実行するコミッショニングプロトコルを決定する。第1の代替形態では、QRコードリーダ1015は、第1のデバイス1005との第1のコミッショニングプロトコル1040を開始および実行するために使用される第2の通信インタフェイス1035を含み、これは、専用通信ネットワーク1045を介して、または通信インタフェイス1035と1060との間で直接、例えばWi-Fiアクセスポイント（AP）もしくはゲートウェイ装置である第3の装置1055、すなわち追加のネットワーキングデバイス1055とインタフェイスすることができる。専用通信ネットワーク1045は、例えば、イーサネット（登録商標）、Wi-Fi、Zigbeeなどのようなローカルエリアネットワーク（LAN）、またはセルラーネットワークもしくはインターネットのような広域ネットワーク（WAN）、またはネットワークの任意の組合せであることができる。第1のプロトコルは、第1のデバイス1005と追加のネットワーキングデバイス1055との間の（セキュアな）通信をセットアップするためのプロトコルであることができる。第2の代替案では、QRコードリーダ1015は、第3の装置1055（すなわち、第3の通信インタフェイス1060を含む追加のネットワーク装置1055）および通信ネットワーク1045を介して、第1の装置1005と第2の装置1025（後者はクラウドサービスのサーバ、すなわち「管理者」装置である場合がある）との間で、第1のコミッショニングプロトコルと同一であるか、または第1のコミッショニングプロトコルとは異なる第2のコミッショニングプロトコル1050をトリガする。

【０１１３】

第3の代替案は、以前の2つの代替案の一種の組合せの一種であることができ、QRコードリーダ1015は、第1のQRコード1010内の情報に基づいて、第1のコミッショニングプロトコルをトリガして、第1のデバイス1005と、例えばWi-Fi APまたはゲートウェイデバイスであることができる第3のデバイス1055との間の（セキュアな）通信を設定し、第1のコミッショニングプロトコルと同一のまたは異なる第2のコミッショニングプロトコルをトリガして、第3のデバイス1055およびネットワーク1045を介して第1のデバイス1005と第2のデバイス1025（後者は例えばクラウドサービスのサーバ、または「管理者」デバイスであることができる）との間の（セキュアな）通信を設定する。

【０１１４】

図11は、第1の通信インタフェイス1120を備える第1の装置1110と第2の通信インタフェイス1140を備える第2の装置1130との間の従来の実施形態によるコミッショニングプロトコル1100を示す。第1の装置1110は、コミッショニングプロトコル1100に

関連するコミッショニングメッセージ1150によって、その存在をアナウンスすることができる。第2の装置1130は、メッセージ1160を返すことによって、コミッショニングプロトコル1100のコミッショニングフローを開始する。

【０１１５】

図12は、第1の通信インタフェイス1220を備える第1の装置1210と第2の通信インタフェイス1240を備える第2の装置1230との間の本発明の実施形態によるコミッショニングプロトコル1200を示す。図11の第1の装置1110とは異なり、 図12の第1の装置1210には、第1のQRコード1250が付加されている。 この第1のQRコード1250は、第1の装置1210の同じ（第1の）通信インタフェイス1220上で動作し得る異なる2つのコミッショニングプロトコルのためのコミッショニング情報を含む。第1の装置1210は、2つのコミッショニングプロトコルのうちのそれぞれのコミッショニングプロトコルに関連するコミッショニングメッセージ1260および1270によって、その存在およびそのコミッショニング能力をアナウンスすることができる。第1の装置1210に付加された第1のQRコード1250を復号した後、第2の装置1230は、メッセージ1280を返すことによって、2つのコミッショニングプロトコルのうちの選択されたコミッショニングプロトコルを開始する。

【０１１６】

Wi-FiまたはIEEE 802.11を使用するネットワークで使用されるデバイスプロビジョニングプロトコル（DPP）のような、デバイス制御される設定方法では、DPPコンフィギュレータとして動作する装置は、例えばWi-Fiアクセスポイント（AP）に接続するためのエンローリーとして動作する任意のWi-Fi対応装置を安全に設定することができる。本発明では、第1のQRコードは、複数のアプリケーションの情報を格納することができるマスタQRコードである。例示的な実施形態では、それぞれのWi-Fi接続が、複数のコンフィギュレータと、エンローリーとして動作し、第1のQRコードが付加されている第1のWi-Fi対応装置との間で確立されることができる。それによって、第1のQRコードは、第1のWi-Fi対応装置のDPPブートストラッピング情報、例えば、符号化された形の公開鍵を含むことができ、各コンフィギュレータは、ブートストラップ処理第1のWi-Fi対応装置の第1のQRコードをスキャンして、それぞれの公開鍵を読み出す。

【０１１７】

DPPでは、プロセスは、2つの装置1210, 1230が接続されていない状態で開始し、装置のうちの1つは問題のWi-Fiネットワークに接続するように設定されていない。1つの装置1230は、無線ネットワークに参加するために、すなわち、ネットワークアクセスポイント（AP）に接続するために、他の装置1210を設定するために使用され、コンフィギュレータ（またはコミッショナ）と呼ばれることができる。第2の装置はエンローリー（またはコミッショニー）と呼ばれることができる。

【０１１８】

第1のフェイズは「ブートストラップ」であり、一方の装置が、他の装置の、その装置を設定するためのブートストラップ公開鍵（BR）を取得する。これは無線通信技術とは別の手段によるものであり、いわゆる「帯域外」通信（OOB）と呼ばれ、ここではユーザが1つの装置に第2の装置上のQRコードを読み取らせる。ブートストラップが成功した場合、装置は「ブートストラップ」され、そうでない場合、装置は「開始」状態に戻る。多くの場合、単純なまたはいわゆるヘッドレス装置（すなわち、ユーザインタフェイスがほとんどまたは全くない装置）は、電源投入後またはリセット後に起動し、設定のためにQRコードに示されるチャネル上で無線をオンにし、認証要求メッセージのリッスンを開始するようにプログラムされる。（例えば、スマートフォンまたはラップトップのような単純ではない装置は、それが設定されることをユーザが望む場合、そのユーザインタフェイスを介してこのモードに設定される）。

【０１１９】

装置は認証手順を実行し、これにより装置は「信頼」を確立する。つまり、ユーザは、装置が自分が信じているものであり、他の未知の（潜在的に悪意のある）装置が問題の装置

のうちの1つまたは他の装置の「ふりをして」いるのではないと確信することができる。認証の開始を要求するメッセージが1つの装置から送信される。このメッセージは、設定を行う装置(コンフィギュレータ) または設定される装置(エンローリ) のいずれかによって送信できる。コンフィギュレータ/コミッショナは、Wi-Fiネットワークに接続されることができるが、これは実施形態が動作するために必ずしも必要ではない。無線通信を開始する装置をイニシエータ、応答する装置をレスポンダと呼ぶ。特に、DPPプロトコルは、コンフィギュレータおよびエンローリー装置の両方がDPPプロトコルのイニシエータとして動作することを可能にし、それによって、他の装置自動的にレスポンダになる。単純な装置またはヘッドレス装置は、通常、レスポンダの役割を担う。

【０１２０】

相手装置がこのメッセージに応答する。認証要求メッセージが正しく復号され、イニシエータがユーザが信じている装置であり、必要な機能を持っていることを示す情報が含まれている場合、応答メッセージは、メッセージが「受け入れられた」ことを示し、イニシエータがレスポンダの資格情報を検証するために必要な情報を含み、必要な機能も持っていることを示す。2つの装
置が他の装置から必要な情報を受信しない場合、プロセスは中断し、装置はブートストラップ状態に戻る。

【０１２１】

DPPプロトコルの場合、最初のメッセージは認証要求メッセージで、応答メッセージはDPP認証応答である。レスポンダは、DPP Authentication Requestメッセージが、レスポンダの公開ブートストラップ鍵の正しく生成された暗号化ハッシュを含むことをチェックし、オプションとして、イニシエータの公開ブートストラップ鍵のコピーを含むかどうかをチェックする。レスポンダは、認証を続行できるかどうかを示すDPP認証応答メッセージを送信する。そうでない場合、例えば、DPP認証要求メッセージ中の暗号化されたナンスの復号化の試行が失敗するため、プロセスは中止される。DPP認証応答は、レスポンダ公開ブートストラップ鍵の暗号化ハッシュを含み、イニシエータ公開ブートストラップ鍵のハッシュを含む場合がある。同様に、イニシエータについては、エンローリーがOOB通信によってこの公開鍵を取得していてもよい。その後、イニシエータの公開ブートストラップ鍵を相互認証に使用できる。イニシエータの公開ブートストラップ鍵がないと、イニシエータのみがエンローリーを認証できるが、その逆はできない。

【０１２２】

認証応答メッセージが、レスポンダが認証要求メッセージを受け入れたことを示し、応答がイニシエータのセットアップによって課された基準を満たす場合、イニシエータは認証確認メッセージを発行する。認証応答および確認メッセージ内の認証値が関連する装置によって正しいことが見出された場合、プロトコルのこの部分、認証部分は成功し、設定が開始することができる。確認メッセージは、エンローリーがイニシエータでもある以前の設定試行の結果の指標を含むこともできる。

【０１２３】

DPPプロトコルの場合、認証確認メッセージはDPP 認証確認(Authentication Confirm)メッセージである。

【０１２４】

そして、エンローリー装置は、エンローリーが望む設定のタイプに関する情報を含む設定要求メッセージを送信する。コンフィギュレータが要求を許可できる場合、ネットワーク鍵など、エンローリーが必要とする情報を含むメッセージを送信する。そして、プロセスは、エンローリーの正常な設定で終了する。

【０１２５】

DPPの場合、要求メッセージはDPP Configuration Requestであり、コンフィギュレータ応答はDPP Configuration Responseメッセージである。DPP設定応答には、エンローリーが接続するネットワークのサービスセット識別子(SSID)が含まれている場合があり、DPPコネクタが含まれている場合がある。DPPコネクタはコンフィギュレータ

によってデジタル署名された証明書と見なされることができ、特にエンローリーの公開ネットワークアクセス鍵を含む。DPPコンフィギュレータ応答メッセージは、コンフィギュレータの公開署名鍵も含む。同じコンフィギュレータによって設定された他の装置は、それによって、他の装置の公開ネットワークアクセス鍵を信頼できるかどうかを確認できる。DPP設定応答メッセージには、ネットワークのWi-Fiパスフレーズまたは事前共有鍵(PSK)が含まれている場合もある。エンローリーは、(DPPのバージョンに応じて)DPP設定結果メッセージをコンフィギュレータに送信して、設定を受け入れるかどうかを知らせる。コンフィギュレータがこのメッセージを受信しないことは、コンフィギュレータとエンローリーとの間にWi-Fiの問題があったことをコンフィギュレータに示すことができる。そして、「設定されていると思われる」エンローリーは、そのコネクタをDPP設定APに送信することができる。コネクタ 署名が正しいことが分かり、APが、一致するConnector、すなわち同じコンフィギュレータによって署名された同じネットワークのためのConnectorがある場合、APは自身のConnectorをエンローリーに送信する。エンローリーとAPは、コネクタ中の互いのネットワークアクセス鍵及び、Diffie/-Hellman方式の自身のプライベートネットワークアクセス鍵に基づいて、対称鍵を計算することができる。

【０１２６】

エンローリーがWi-FiパスワードまたはWi-Fi Pre Shared key(PSK)を受信した場合、エンローリーは、IEEE 802.11 規格で規定されている4 ウェイハンドシェイクを通した通常の方法でAPに関連付けることを試みる。SHSネットワークに参加するための装置を設定またはコミッショニングするためのプロトコルは鍵の交換を含む場合があり、コードがコミッショニング装置に提供される。このコードはパスワードとして機能し、帯域外方法によって提供される。この例では、このパスコードがSHSコミッショニングアプリケーションに関連するエンローリー装置のQRコードの一部に組み込まれることができる。

【０１２７】

本発明の例示的なケースでは、装置、例えば無線装置またはWi-Fi無線装置は、SHSブートストラップロトコルによってDPPまたはSHSネットワークによるWi-Fiネットワークに参加することが可能である。この場合、装置は、DPPおよびSHSブートストラップロトコルに関連する情報を格納することができる、本発明で定義されるような第1のQRコードを有することができる。例示的な実施形態では、コンフィギュレータまたはコミッショナは、（1）QRコードリーダにおける事前設定、（2）QRコードリーダにおいて利用可能なポリシー、および（3）装置が配備されている環境において利用可能なコンテキスト要件のうちの少なくとも1つに基づいて、DPPまたはSHSブートストラップロトコルをトリガする、装置に付属する第1のQRコードを読み取るQRコードリーダを実装（またはQRコードリーダと通信）する。したがって、この例示的な実施形態に必要とされるステップは以下を含む:a)最初のQRコードを読み取るステップ;b)読み取られた第1のQRコードから、サポートされているアプリケーション、特にサポートされているコミッショニングプロトコルを決定するステップ;c)（1）事前設定された選択、（2）ポリシー、（3）コンテキスト、および（4）第1のQRコードに含まれる選好のうちの少なくとも1つに基づいてアプリケーション（例えば、好ましいアプリケーション）を選択するステップ。例えば、QRコードリーダは、DPPベースのコミッショニングのためのQRコードリーダであり、DPPを実行することのみが可能である場合がある。例えば、ポリシーは、利用可能であればアプリケーションの使用を好み、（第1のQRコードによって示されるように）サポートされていればそれを使用することができる。例えば、QRコードリーダは、装置が展開されるべきコンテキストまたは環境（例えば、自宅または病院）が所与のアプリケーションのみをサポートする（例えば、高度にセキュアなDPPベースのWi-Fi設定プロセスのみをサポートする）かどうかを検出することができ、そして、これに基づいてアプリケーションの選択を行うことができる。検出は、例えば、装置によって送信されたビーコンの存在またはコンテンツに基づくことができる。例えば、第1のQRコードは、コ

ンテキストに応じてQRコードリーダに好ましいアプリケーション選択を示すフィールドを含むことができる；ｄ）第1の選択されたアプリケーションとして選択されたアプリケーション（例えば、選択された好ましいアプリケーション）を開始するステップ。コミッショニングアプリケーションの場合、コンフィギュレータまたはコミッショナは、第1の選択されたアプリケーションが成功しなかったか、または失敗した限り、例えば、第1の選択されたアプリケーションに関連するコミッショニングプロセスが、最小回数N（例えば、Ｎ＝１、２、・・・）成功しなかったか、または失敗した限り、第2の選択されたアプリケーションを開始してはならない。

【０１２８】

本発明の例示的な実施形態では、本発明で定義される（製品または装置に取り付けられる可能性がある）第1のQRコードは2つ以上のアプリケーションに関連する情報を含むことができる。それを読み取るQRコードリーダは、事前設定、ポリシーまたはコンテキストに基づいて両方のアプリケーションを実行することができる。両方のアプリケーションの実行は、例えば、ポリシーによって定義される順序で、連続的であり得る。アプリケーションのうちの1つの実行は、部分的であってもよい（例えば、第2のコミッショニングプロトコルが、中間ステップとして第1のコミッショニングプロトコル（DPP）に依存する場合）。アプリケーションまたはアプリケーションのそれぞれの段階が複数回実行されることができる。更なる例として、第1のQRコードが装置、例えば、無線装置またはWi-Fi無線装置に取り付けられる場合、装置は、（1）、基礎をなす無線ネットワーキング技術（例えばWi-Fi）、および（2）SHSのコミッショニングプロトコルに依拠することによって、スマートホームシステム（SHS）に参加することが可能である。この場合、装置は、SHSの無線ネットワーキング技術およびブートストラップロトコルに関連する情報を格納することができる、本発明で定義されるような第1のQRコードを有することができる。例示的な実施形態では、コンフィギュレータまたはコミッショナは、（1）QRコードリーダにおける事前設定、（2）QRコードリーダにおいて利用可能なポリシーおよび（3）装置が配備されている環境において利用可能なコンテkスト要件のうちの少なくとも1つに基づいて、DPPブートストラップロトコルおよびSHSブートストラップロトコルをトリガする装置に取り付けられた第1のQRコードを読み取るQRコードリーダを実装（またはQRコードリーダと通信）する。したがって、この例示的な実施形態に必要とされるステップは以下の通りである:a)第1のQRコードを読み取るステップ;b)読み取られた第1のQRコードから、サポートされているアプリケーション、特にサポートされているコミッショニングプロトコルを決定するステップ;c)（1）事前設定された選択、（2）ポリシー、（3）文脈および（4）第1のQRコードに含まれる選好のうちの少なくとも1つに基づいて、アプリケーション実行順序（例えば、好ましいアプリケーション実行順序）を選択するステップ。例えば、QRコードリーダは、DPPベースのWi-Fiネットワークとの相互運用性が可能なSHS用のQRコードリーダであることができる。例えば、QRコードリーダは、装置が展開されるべきコンテキストまたは環境（例えば、家庭、または病院）が両方のアプリケーション（例えば、セキュアDPPベースのWi-Fi設定プロセスおよびSHS設定プロセス）を必要とするかどうかを検出することができ、そして、これに基づいてアプリケーション選択を行うことができる;d)最初のアプリケーションを開始するステップ。コミッショニングアプリケーションの場合、コンフィギュレータまたはコミッショナは、少なくとも、予め設定された目標ステップまで、第1の選択されたアプリケーションが成功していないかまたは失敗している限り、例えば、第1の選択されたアプリケーションに関連するコミッショニングプロセスが、最小回数N(例えば、Ｎ＝１、２、...)成功していないかまたは失敗している限り、第2の選択されたアプリケーションを開始すべきではない；e）第１のアプリケーションの実行（第２のコミッショニングプロトコルが中間段階として第１のコミッショニングプロトコル（DPP）に依存する可能性がある場合、部分的な実行の可能性もある）が成功すると、第２のアプリケーション、例えばコミッショニングプロトコルの場合、装置をネットワークに接続するための更なる設定をデバイスに提供する第２のコミッショニングプロトコルを開始し； f)オプションとして、

ステップe)および第2のアプリケーションの実行の成功（失敗）に応じて、第1のアプリケーションに戻って終了する。

【０１２９】

この例示的な実施形態は、付加された第1のQRコード1330および第1の通信インタフェイス1340を備える第1の装置1310と、第2の通信インタフェイス1350およびQRコードスキャンのためのカメラ1360を備える第2の装置1320との間のコミッショニングプロトコル1300を示す図13によって説明される。第2の装置1320は、第1のQRコード1330をスキャンし、例えばポリシーに基づいて、通信インタフェイス1350および1340を介して第1の装置1310と、第1のQRコード1330において利用可能な第1および第2のアプリケーションに属するコミッショニングステップ1371, 1372, 1373を実行することを決定する。例示的なシナリオでは、ステップ1371は、第1のコミッショニングプロトコルを参照することができ、ステップ1372は、ステップ1371が特定の段階に達したときに第2のコミッショニングプロトコルを参照することができ、ステップ1373は、ステップ1372の成功した（失敗した）実行に応じて、第1のコミッショニングプロトコルを再び参照することができ、ステップ1371の実行を継続する。

【０１３０】

本発明において、装置、例えばWi-Fi製品が、例えばDPPアプリケーションおよびSHSアプリケーションなどの2つのアプリケーションを含む付加された第1のQRコードを有する場合、コミッショニングデバイスは、Wi-Fiコミッショニングのために Wi-Fi Easy Connectを、そして第1のQRコードが付加された装置をクラウドサービスおよび他の全ての上位レベルサービスに接続するためのSHSプロトコルを使用することを選択することもできる。

【０１３１】

本発明では、装置、例えばWi-Fi製品が、例えばDPPアプリケーションおよびSHSアプリケーションなどの2つのアプリケーションを含む付加された第1のQRコードを有する場合、第1のQRコードが付加された装置は、第1のQRコードを読み取りに応じたコンフィギュレータ（例えば、DPP）またはコミッショナ（例えば、Matter）からの要求に反応する必要があるだろう。装置が第1のQRコードにおいて識別された第1のアプリケーションについての第1の要求を受信すると、装置は、第1のアプリケーションが終了していない限り、第1のQRコードに含まれる第2のアプリケーションについての後続の要求を受け入れるべきではない。

【０１３２】

本発明では、装置が所与のアプリケーションをサポートする場合、装置に付加され、アプリケーションに関する情報を含む第1のQRコードは、その情報が（平文であるか否かを問わず）ブロードキャストされるか否かを示し得る。例えば、いくつかのフィールドは、プライバシーを理由としてブロードキャストされることができないが（代わりに0ビット列がブロードキャストされる）、これは、装置が、例えばソフトアクセスポイント（softAP）になることによって所与の設定状態に入るとき、コミッショナ（第1のQRリーダによってトリガされる）が正しい装置からのコミッショニングメッセージ、例えば、正しい装置のサービスセット識別子（SSID）を含むメッセージを選択することを妨げる可能性がある。あるいは、例えばビーコンに含まれて、または装置のSSIDの一部としてブロードキャストされる前に、、第1のQRコードに含まれるフィールドのいくつかをXOR(暗号化）するために使用されるランダムビットマスク、例えば装置ごとに固有のランダムビットマスクを第1のQRコードが含むことができる。そして、QRコードからこの情報、例えばランダムビットマスクを読み取る装置は、装置から受信された無線ビーコンに含まれる情報をどのように復号するかを知る。

【０１３３】

要約すると、本発明は、第1のQRコードまたはマスタQRコードによって表される、複数のアプリケーションの情報を、それぞれの情報が信頼性があり時間効率的な態様で各アプ

リケーションについて読み出されることができるように格納することが可能な、複数のアプリケーションのQRコードに関する。情報は、少なくともヘッダ（例えば、単一の識別子）と、アプリケーションごとのそれぞれのデータコンテナ（例えば、ビット列の一部または完全なビット列中のサブビット列）とを含む符号化データに符号化される。ヘッダは、複数のアプリケーションの存在を示す少なくとも1つの識別子と、アプリケーションごとのそれぞれのアプリケーション識別子とを含むことができる。それぞれの誤り訂正機構は、アプリケーションごとの各データコンテナに含まれることができる。符号化されたデータは、割り当て規則に従って、第1の/マスタQRコードの符号化領域にわたって分散された複数のデータピクセルに分散して格納される。QRコードリーダは、それぞれの関心アプリケーションに関連するデータピクセルにアクセスして処理することによってのみ、およびこのそれぞれのアプリケーションに特有の誤り訂正を使用することによって、QRコードに格納された情報を読み出すことができる。

【０１３４】

本発明は、図面及び前述の説明において詳しく図示及び説明されてきたが、そのような図示及び説明は、例示的又は説明的であり、限定的ではないと考えられるべきである。さらに、本発明は、ネットワークインタフェイス（例えば、Wi-Fi、Bluetooth Low Energyまたは他のタイプ）またはコミッショニングプロトコル（例えば、Wi-Fi Easy Connect、またはMatterのようなスマートホームシステム）を実装する任意の製品に適用されることができる。QRコードリーダは、製品によって実装される同じネットワークインタフェイスを使用することによって直接通信することができ、または間接的に、例えばアクセスポイント（AP）またはゲートウェイを介して、製品と通信することができる。

【０１３５】

同様に、本発明の一実施形態によるQRコードの単一のスキャンを用いて読み取りおよび処理するためのシステム1400は、単一の人または複数の人に関連する個人データを要求し、格納し、表示するためにユーザによって使用される個人データアプリ（携帯電話上で使用されるものなど）を含むことができる。そのようなデータの例は、ワクチン接種、感染試験、または特定の感染からの回復を示す証明書に関するレポートであり得る。

【０１３６】

図14は、モバイルQRコード読取装置1420（例えば、携帯電話）上で動作する個人データアプリ（1431）によって表示されるQRコード1410によって符号化された少なくとも個人レポートを含むシステム1400を示す。QRコード1410は、カメラ1430を備えたQRコードリーダ1420によってスキャンされることができる。第1の管理エンティティ1440は、何らかの識別資格を与えられた人物の識別/認証時に、個人レポート、例えば疾患に関する人物ステータスに関するレポートを配信することを担当する。この管理エンティティは、個人レポートに署名するために、いくつかの秘密鍵材料、例えば、秘密鍵を管理することもできる。オプションとして、第2の管理エンティティ1450は、例えば、個人レポートのデジタル署名をチェックすることによって、または複数のレポートをポリシーと照合することによって、個人レポートの検証を担当する。 第2の管理エンティティ1450および個人データアプリ1431は、第1の管理エンティティ1440から個人データアプリ1431に個人レポートを配信するためにインタラクトする。個人データアプリ1431は、QRコードリーダ1420内の第2の管理エンティティ1450の一部として実装されることができ、またはQRコードリーダ1420は、検証のために、読み出された個人レポートを管理エンティティ1450に転送することができる。

【０１３７】

単一の人または複数の人に関連付けられた個人データは、複数アプリケーションQRコードによって符号化され、モバイルアプリに記憶されることができる。

【０１３８】

個人データが前述のワクチン接種/回復/試験レポートのような公式な性質のデータに関する場合、管理エンティティは、何らかの識別情報、すなわち、第1の管理エンティティ1440に対応する識別情報を使用した人の識別/認証時に、問題の人の個人データ記録を

作成するタスクを委託され得る。この管理エンティティ1440はまた、個人データレポートに署名するために、いくつかの秘密鍵材料、例えば、秘密鍵を管理することができる。そのような場合、例えば、レポート上のデジタル署名をチェックすることによって、またはポリシーに対して複数のレポートをチェックすることによって、個人データレポートを検証することを担当する第2の管理エンティティ（すなわち、上述の第2の管理エンティティ1450）が存在することができる。

【０１３９】

第2の管理エンティティ1450のために行動する人員は、（例えば、個人データレポート1410を読み取るために使用されるモバイルアプリとして動作し、個人データレポートの読み取りの結果に基づいてポリシーを実施する）QRコードリーダ1420を使用することができる。そのようなポリシーは、アクセスまたは通過に関する制限などの公式ポリシーを含むことができるが、これらに限定されない。

【０１４０】

単一の人に関連付けられた個人データレポートを含むQRコードは、QRコードリーダ（またはQRコードリーダによってQRコードから読み取られたデータを検索し検証する検証エンティティ）が全ての個人データレポートが互いにリンクされていることをチェックすることを可能にする総合シグネチャを含むことができる。

【０１４１】

これを達成するために、各々の個人データレポートは、上述のように異なるデータコンテナに含まれる必要がある。さらに、総合シグネチャは、例えば、最後のデータコンテナに、またはヘッダの一部として含まれる。

【０１４２】

複数の人物に関連付けられた個人データレポートを含むQRコードは、QRコードリーダ（またはQRコードリーダによってQRコードから読み取られたデータを検索し検証する個人データ検証エンティティ）が全ての個人データレポートが互いにリンクされていることをチェックすることを可能にする総合シグネチャを含むことができる。

【０１４３】

これを達成するために、複数のユーザは、例えば彼らの公的資格証明を使用することによって、同じ個人データアプリを通じて、自分自身を識別/認証することができる。ユーザが同じアプリで自身を識別/認証するたびに、その個人データアプリでこれまでに識別/認証された全てのユーザの個人データレポートを含む新しいQRコードが作成される。各々の個人データレポートは、異なるデータコンテナに含まれる。Covid 19（ワクチン接種/回復/試験）レポートを証明する責任を負う認証局によって生成された総合シグネチャは、例えば、最後のデータコンテナ内に付加されて含まれ、例えばQRコード内の全ての個人データレポートが一緒に読み取られ得ること、例えば、一緒に生活する人々のグループに属することを検証することを可能にする。

【０１４４】

QRコードが、国内旅行または国際旅行の個人データレポートを含む場合、QRコードリーダは、コンテキストに基づいて、例えば位置に基づいて、好ましいアプリケーションを自動的に選択することができる。QRコードは、例えばヘッダに自国を含むことができる。そして、QRコードリーダは、QRコードリーダの位置に基づいて、特定のデータコンテナ（すなわち、特定の領域で使用するための個人データレポート）を選択することができる。

【０１４５】

QRコードが定期的なワクチン接種接種にリンクされた複数の個人データレポートを含む場合、QRコードリーダは、それらが新しい（所与の期間内に発行された）ものであり、個人データレポートが第2の管理エンティティによって展開されたポリシーを満たす場合にのみ、個人データレポートを受け入れることができる。そのようなポリシーの例は、例えば、最も多くのワクチン接種が最後のXヶ月（例えば、過去3ヶ月）内に行われたこと、又は（家族）グループの誰も、メンバーのうちの1人が肯定的な回復報告を有していな

い場合、許可されるべきではないことを述べることができる。
【０１４６】
QRコードが複数の人、例えば家族メンバーに関連する個人データレポートを含む場合、それらの家族メンバーは、単一のQRコードを使用してそれらのIDを示すことによって、それらの身元を一緒に立証することが期待される。したがって、複数の人に関連付けられた個人データレポートを含む複数アプリケーションQRコードは、例えば、複雑なポリシーに基づいて、QRコードリーダによってのみ受け入れられることができる:
【０１４７】
そして、複数アプリケーションQRコードは、少なくとも2人の人が有効なIDを伴って存在する場合にのみ、QRコードリーダによって受け入れられることができる。
【０１４８】
グループの個人データをグループ方式で処理することは、顕著な利点を提供する。第1に、第2の管理エンティティの人員が個人データレポートを読み、チェックしている場合には、時間およびトラブルが大幅に節約される。これらの人員は、しばしば、人々を迅速に処
理するようにプレッシャーを受けており、しばしば、空間の物理的な配置が、これを扱いにくくする場合がある。単一の読み出しおよびチェック動作により、グループ全体がチェックされ、進行することを許可される（または許可されない）ことができ、これは各QRコードを個々に処理する必要がある場合よりもはるかに速く、誤りが生じにくい。さらに、この実施形態による処理は、第2レベルの認証、すなわち、個々のコンテナの認証およびQRコード全体の認証が存在する点で、個人データレポートを悪用することをより困難にする。
【０１４９】
開示された実施形態に対する他の変形例は、図面、開示及び添付の請求項の検討から、請求項に記載された発明を実施する際に当業者によって理解され及び実施されることができる。請求項において、単語「有する」は、他の要素又はステップを排除するものではなく、不定冠詞「a」又は「an」は、複数性を排除するものではない。単一のプロセッサまたは他のユニットは、特許請求の範囲に列挙されるいくつかのアイテムの機能を満たすことができる。特定の手段が相互に異なる従属請求項に記載されているという単なる事実は、これらの手段の組み合わせが有利に使用されることができないことを示すものではない。
【０１５０】
前述の説明は、本発明の特定の実施形態を詳述する。しかしながら、上記が本文中でいかに詳細であっても、本発明は多くの態様で実施することができ、したがって、開示された実施形態に限定されないことが理解されよう。本発明の特定の特徴または態様を説明する際の特定の用語の使用は、その用語が関連する本発明の特徴または態様の特定の特徴を含むように限定するように本明細書においてその用語が再定義されることを意味するものではないことに留意すべきである。
【０１５１】
単一のユニット又は装置が、請求項に列挙されるいくつかの項目の機能を満たしてもよい。特定の手段が相互に異なる従属請求項に記載されているという単なる事実は、これらの手段の組み合わせが有利に使用されることができないことを示すものではない。
【０１５２】
説明した動作は、コンピュータプログラムのプログラムコード手段として、および/または専用ハードウェアとして実装されることができる。コンピュータプログラムは、他のハードウェアとともに、または他のハードウェアの一部として供給される光記憶媒体またはソリッドステート媒体などの適切な媒体上で記憶および/または配布され得るが、インターネットまたは他の有線もしくは無線電気通信システムなどの他の形態で配信されることもできる。
【０１５３】
参考資料:[DPP] Device Provisioning Protocol - Technical Specification -

Version 2.0, Wi-Fi Alliance, 2020, (https://www.wi-fi.org/downloads-public/Wi-Fi_Easy_Connect_Specification_v2.0.pdf/35330) [ISO 18004] ISO/IEC 18004:2015: Information technology - Automatic identification and data capture techniques: "QR Code bar code symbology specification"

【図面】

【図１】

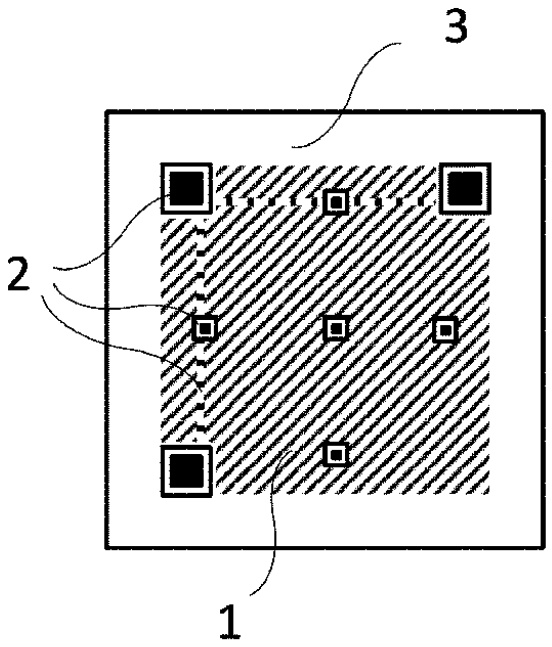

Fig. 1

【図２】

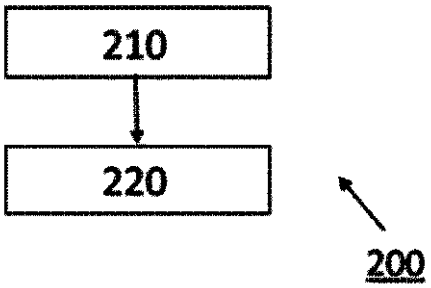

Fig. 2

【図３】

...	...	...	...	...	...	...
...	A	B	A	B	A	...
...	B	A	B	A	B	...
...	A	B	A	B	A	...
...	B	A	B	A	B	...
...	A	B	A	B	A	...
...	...	...	...	...	...	...

Fig. 3

【図４】

...	...	...	...	...	...	...
...	A	B	C	A	B	...
...	B	C	A	B	C	...
...	C	A	B	C	A	...
...	A	B	C	A	B	...
...	B	C	A	B	C	...
...	...	...	...	...	...	...

Fig. 4

【図５】

...	...	...	...	...	...	...	...	...	...	...
...	A	B	A	B	A	B	A	B	A	...
...	B	A	B	A	B	A	B	A	B	...
...	A	B	I	I	I	I	I	B	A	...
...	B	A	I	I	I	I	I	A	B	...
...	A	B	I	I	CI	I	I	B	A	...
...	B	A	I	I	I	I	I	A	B	...
...	A	B	I	I	I	I	I	B	A	...
...	B	A	B	A	B	A	B	A	B	...
...	A	B	A	B	A	B	A	B	A	...
...	...	...	...	...	...	...	...	...	...	...

Fig. 5

【図６】

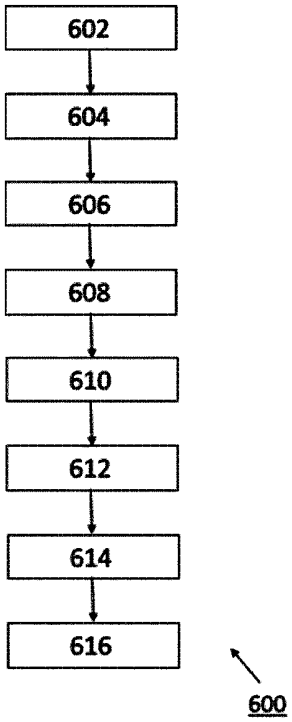

Fig. 6

【図７】

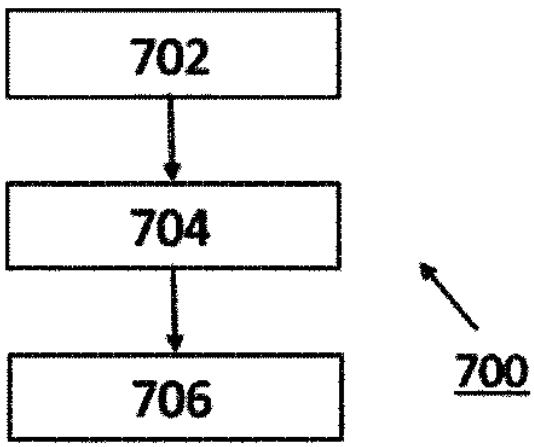

Fig. 7

【図８】

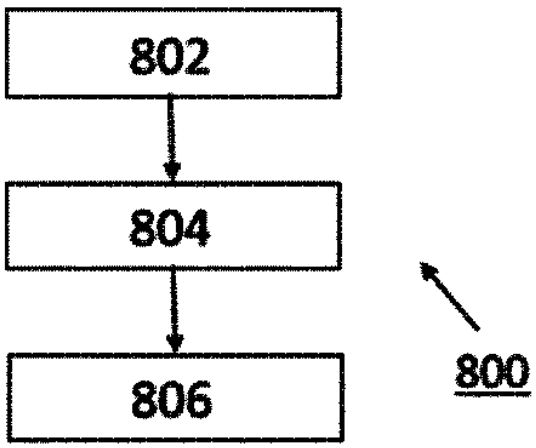

Fig. 8

【図９】

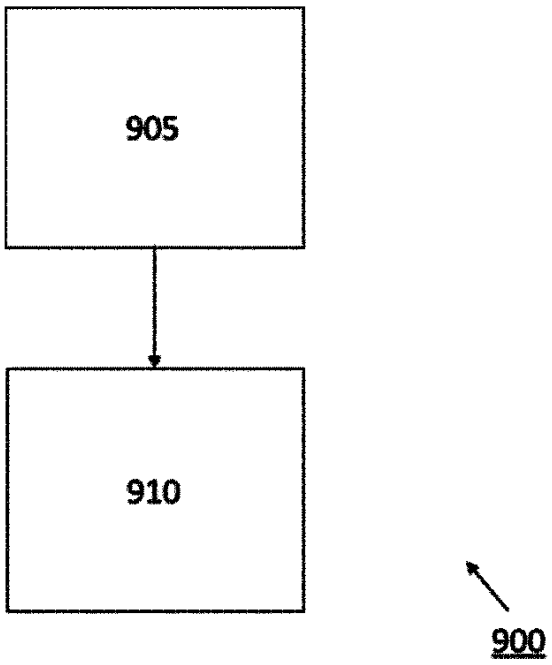

Fig. 9

【図１０】

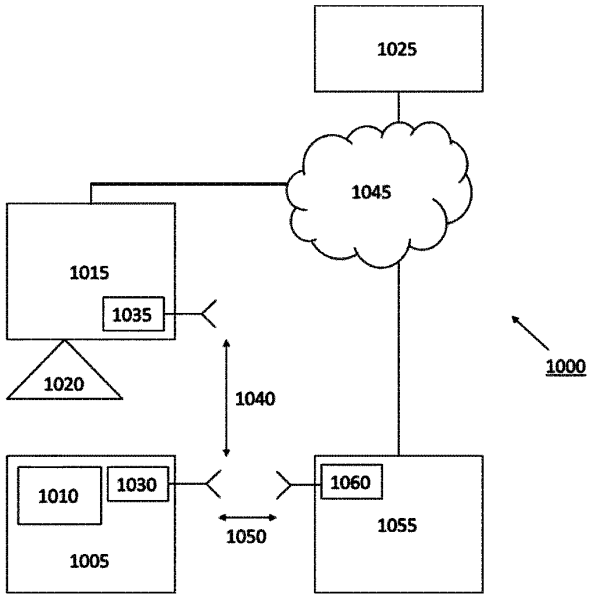

Fig. 10

【図１１】

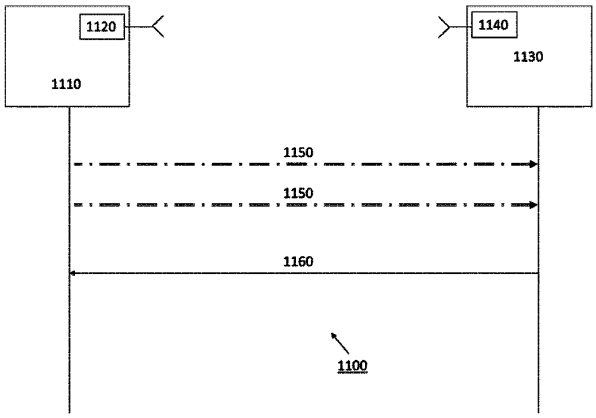

Fig. 11

【図１２】

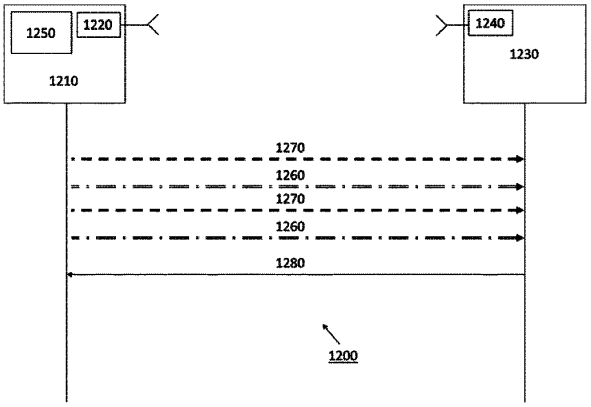

Fig. 12

【図１３】

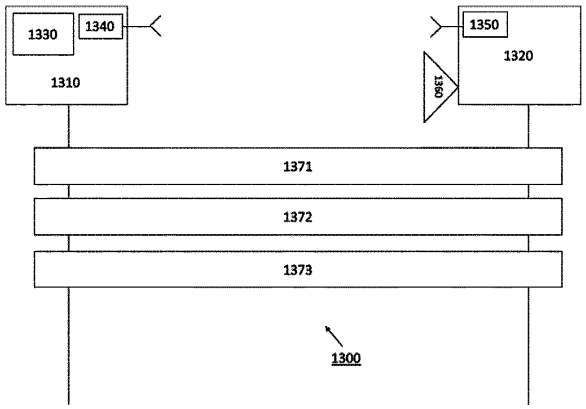

Fig. 13

【図１４】

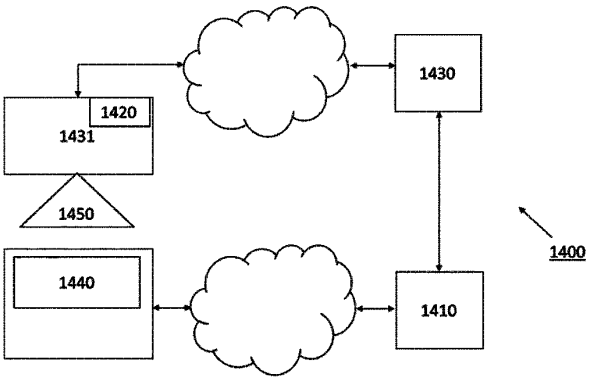

Fig. 14

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2022/087384

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F11/10 G06K7/14 G06K19/06 H03M13/15
ADD.

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 G06K H03M

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 2021/326417 A1 (CABRERA RICARDO [US]) 21 October 2021 (2021-10-21) abstract; figures 1,2 paragraphs [0001], [0008] - [0023], [0027]	1,10 2-9, 11-18
A	US 2019/102588 A1 (LIN PEI-YU [TW]) 4 April 2019 (2019-04-04) abstract; figures 1,2,5 paragraphs [0027] - [0030], [0033] - [0039]	1-18
A	US 2017/193260 A1 (PRUSIK THADDEUS [US] ET AL) 6 July 2017 (2017-07-06) abstract; figures 1-5 paragraphs [0070] - [0074], [0084], [0119] - [0122]	1-18

-/--

[x] Further documents are listed in the continuation of Box C. [x] 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
7 March 2023	17/03/2023

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Weber, Vincent

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2022/087384

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2013/126601 A1 (LEE JAE S [US]) 23 May 2013 (2013-05-23) abstract; figures 4-5 paragraphs [0011], [0014] - [0021], [0025], [0030], [0034], [0038], [0039]	1-18
A	EP 3 065 088 A1 (TOPPAN TDK LABEL CO LTD [JP]) 7 September 2016 (2016-09-07) abstract; figure 3 paragraphs [0116], [0119], [0182]	1-18

2

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2022/087384

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2021326417 A1	21-10-2021	NONE	
US 2019102588 A1	04-04-2019	TW 201915833 A	16-04-2019
		US 2019102588 A1	04-04-2019
US 2017193260 A1	06-07-2017	US 2017193260 A1	06-07-2017
		US 2020234019 A1	23-07-2020
		US 2023037129 A1	02-02-2023
US 2013126601 A1	23-05-2013	US 2013126601 A1	23-05-2013
		WO 2013078427 A1	30-05-2013
EP 3065088 A1	07-09-2016	CN 105706118 A	22-06-2016
		EP 3065088 A1	07-09-2016
		JP 5978315 B2	24-08-2016
		JP 6518625 B2	22-05-2019
		JP 2016189197 A	04-11-2016
		JP WO2015064334 A1	09-03-2017
		US 2016267370 A1	15-09-2016
		WO 2015064334 A1	07-05-2015

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(51)国際特許分類　　ＦＩ
　　Ｇ０６Ｋ　　7/14　　０７３

,MC,ME,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,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,MG,MK,MN,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,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．ＱＲコード
２．ＢＬＵＥＴＯＯＴＨ
３．ＺＩＧＢＥＥ

弁理士　矢ヶ部 喜行
(72)発明者　ベルンセン ヨハネス アルノルドス コルネリス
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ５ フィリップス インターナショナル ベー ヴェ インテレクチュアル プロパティ アンド スタンダーズ
(72)発明者　ガルシア モルション オスカー
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ５ フィリップス インターナショナル ベー ヴェ インテレクチュアル プロパティ アンド スタンダーズ