QRコードと互換性を持つ二次元コードの大容量化と秘匿化に関する研究

寺浦, 信之

https://doi.org/10.15017/1866317

出版情報：九州大学, 2017, 博士（工学）, 課程博士
バージョン：
権利関係：

（別紙様式 2）

氏　　名　：寺浦　信之

論 文 名　：QR コードと互換性を持つ二次元コードの大容量化と秘匿化に関する研究

区　　分　：甲

論　文　内　容　の　要　旨

従前のバーコードを拡張した二次元コードは，1980 年代後半から 90 年代前半に開発され，今日ではさまざまな用途で使用されている．開発された二次元コードの中で，複数の二次元コードが国際標準となっている．その中で，代表的な二次元コードは QR コードである．QR コードは，従来産業用途に限定して使用されていたが，現在では，スマートフォンで読み取り，WEB 参照を行う主要な手段となっている．そして，情報システムの多様化や通信ネットワークの高速化による IoT 用途に向けて，大容量化と秘匿化の要求がある．大容量化では，文字情報だけでなく，音声や画像情報の収容がある．秘匿化では，特別なユーザにのみデータの読み取りを許し，他者にはデータを秘匿する情報提供の用途も存在する．例えば，産業用途ではコストや品質情報，医療用途での個人情報などである．

大容量化の手法として，二次元コードを構成する基本単位であるセルについて，従来の二次元コードにおける白黒の 2 色による 1 セル 1 ビットに対して，セルの多色化（いわゆるカラー二次元コード）による多ビット化が提案されている．多色化は，複数の色を用いてセルを符号化する手法である．2^n 色を用いる場合には，1 セル当たり n ビットを表現することが可能となり，多くの研究事例がある．これらの研究はセルに用いる色数を増大させ，主に多くの色を識別する手法の検討となっていた．しかし，多色化によって，白黒の既存の二次元コードとして識別した場合には，正しい白黒の二次元コードにはならず，互換性は失われる結果となっていた．

秘匿化の手法として，既存の二次元コードの記憶領域を 2 分割し，通常の領域の終端の背後に秘匿する暗号化データを配置する提案がある．この提案では，通常の領域を読み取る互換性があるが，二次元コードの領域を分割するため，通常の領域が減少する．そして，秘匿領域が単一であるため一人しかアクセスできず、複数領域への分割の実現が課題であった．

本論文の第 1 の課題は，既存の二次元コードと互換性を維持しながら，セルを多値化し，記憶するデータの大容量化を行うことである．セルの多値化の手法として，多色化と多領域化を採用した．多領域化は，セルを複数の領域に分割し，分割された領域を独立して符号化する手法である．第 2 の課題は，増加した記憶領域のデータを秘匿することである．第 3 の課題は，複数のユーザが複数の領域の二次元コードを読み取るに際して，アクセス制御を行い，特定のユーザにのみ情報提供を

可能にすることである．

本論文は，二次元コードを構成する基本単位であるセルを，既存の二次元コードと互換性を維持しながら多色化と多領域化の手法を用いて多値化し，大容量化を図り，既存の二次元コードから増加した記憶領域をランダムマスク法によって秘匿する手法を提案し，さらに記憶領域を複数の領域に分割し複数のユーザのアクセス制御をする手法について検討を行ったものであり，6 章から構成される．

第 1 章は序論であり，本論文の背景と主要な研究課題について述べる．

第 2 章では，既存の二次元コードについて，その種類や識別手法について述べた．本論文で提案する手法は，マトリックス型の二次元コードすべてに適用可能であるが，QR コードを互換性維持の対象としたことを述べる．

第 3 章では，QR コードと互換性を維持しながら，多色化と多領域化の手法を併用し，大容量化を実現するセル構造を提案する．セルを 9 個の正方形のサブセルに分割し，互換性を維持する為に，中央のサブセルを白黒で符号化する．さらに，大容量化の為に，周辺部のサブセルをカラー8 色により符号化する．本論文で提案する二次元コードについて互換性確認試験及び識別性確認試験をした結果について述べる．

第 4 章では，QR コードと互換性を維持する領域は公開領域とし，増加した領域のみを秘匿領域とする手法について述べる．本論文で提案する大容量化方式では，仮想の白黒の二次元コードを重層していると見なすことができる．QR コードは誤り訂正を目的として，リードソロモン符号を用いている．リードソロモン符号では，誤り訂正能力を超えた誤りがある場合には復号できない特性を用いて秘匿化を行う．この仮想の QR コード（秘匿領域）の各セルに対して，乱数（秘密鍵）を XOR 演算することにより，リードソロモン符号の全データコード語に誤りを与え，正しいデータコード語への復号や推定を不可能とする秘匿化を行うことを述べる．

第 5 章では，二次元コードの記憶領域を多領域に分割し，複数のユーザのアクセス制御を行う提案手法を述べる.二次元コードを複数の領域に分割し,分割した領域を秘密鍵による秘匿化を行う．また，複数のユーザにそれらの領域のアクセス権を付与する．付与された領域の秘密鍵をユーザ毎に設定されるパスワードによってさらに秘匿化する．ユーザは自らのパスワードによってアクセスの許された領域の秘密鍵を入手し，領域にアクセスする．これらの手法により，複数ユーザのアクセス制御の課題を解決できたことを述べる．

第 6 章では，本論文の結論を述べ，今後の研究課題を示す．