多値セル型二次元コードのデータ領域分割と分割領域への複数ユーザのアクセス制御

寺浦 信之† 櫻井 幸一‡
†テララコード研究所
477-0032 愛知県東海市加木屋町郷中53－25
TerraNob@terrara.jp
‡九州大学 システム情報科学研究院
819-0395 福岡県西区元岡744番地
sakurai@inf.kyushu-u.ac.jp

あらまし すべての人への情報提供を目的とした応用だけでなく，特定の対象にだけ情報を提供するニーズも存在する．そこで，二次元コードの基本要素であるセルを多値化して二次元コードを大容量化し，新たに作り出した領域を秘匿化する．単に二次元コードに暗号化領域を設定し，その復号キイを有する端末のみが読取り可能とする方式が提案されている．しかし，二次元コードのデータが複数の領域に区分されており，複数の読取り者毎に読取範囲が異なる場合の対応は想定されていない．二次元コードの活用分野を拡げるために、この場合に対応可能なデータ構造、暗号化手法を検討する．

Data area division of the multi-value cell two-dimensional code and multi-user access control to the divided area

Nobuyuki Teraura† Kouichi Sakurai‡
†Terrara Code Research Institute
53-26 Gochu Kagiya-cho Tokai-city, 477-0032, JAPAN
‡Information Science and Electrical Engineering, Kyushu University
744 Motooka Nishi-ku Fukuoka,819-0395, JAPAN

Abstract The need of providing only a specific target with the informations, including the personal information etc. which were memorized by the 2D code, which should be kept secret is exist. Then, the cell which is a primitive of a 2D code is made into a multiple-valued, and the area which became large capacity and newly made the 2D code is kept secret. The method which sets an encryption area as the storage area of a 2D code, and makes possible reading only of the terminal which has the decoding Key is proposed. However, it is not assumed, when the data on a 2D code is classified into two or more areas and read ranges differ for two or more read persons of each. When this function is realizable, the activity field of a 2D code can be extended. Then, the system which can respond in this case is examined.

†寺浦 信之:九州大学システム情報科学府 社会人博士後期課程

1　はじめに

既存の二次元コードとの互換性を維持する既存領域と，追加のデータ領域である新規領域を有する多値セル型二次元コードにおいて，新規領域を複数のデータ領域に分割し，複数のユーザがアクセス権を付与されたデータ領域のみを読取ることができるアクセス方式の検討を行う.

1.1　背景

現在用いられている二次元コード[1][2]は，誰でもが読取装置を用いて読取ることが可能である. 携帯電話に読取機能が具備されて以来，読取り装置も普及し，文字通り誰でもが二次元コードの内容を知ることが可能となった.

1.2　動機

WEB誘導の事例のように，すべての対象への情報提供を目的とした応用だけでなく，特定の対象にだけ情報を提供するニーズも存在する. そこで，秘匿性のある二次元コードを開発する.

1.3　既存の研究

収容データの大容量化を目的とし，セルを多値化する為の手段として多色化があり，多くの色の識別を目指す研究[3]-[6]がなされている. また，カラー化や電子透かしによってセキュリティ性の向上を目指す研究[7] [8]もなされている. 白黒の二次元コードでは，秘匿性と互換性を考慮した事例[9]が見られる. 一方，現在の白黒の二次元コードとの互換性を考慮した著者らのカラー二次元コードの研究[10] -[12]がある.

単に二次元コードに暗号化領域を設定し，その復号キイを有する端末のみが読取り可能とする方式が提案されている[9]. この方式は，図1のように，データ領域と読取者が1対1の関係では有効である.

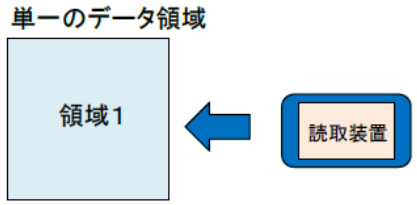


図1　データ領域と読取者が1対1の場合

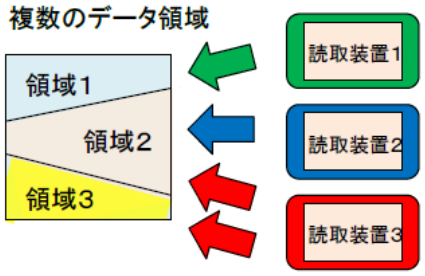


図2　データ領域と読取者がN対Mの場合

1.4　課題

しかし，二次元コードのデータが複数の領域に区分されており，複数の読取り者毎に読取範囲が異なる図2に示す場合の対応は想定されていない. この機能が実現できれば二次元コードの活用分野を拡げることができる. そこで，この場合に対応可能なシステムを検討する.

1.5　提案手法

秘匿性のある二次元コードを開発するために，二次元コードの基本要素であるセルを多値化して二次元コードを大容量化し，新たに作り出した領域を秘匿化する. 複数のユーザに対して，二次元コードに収容されている複数の区分されたデータ領域へのアクセス制御を行う. ユーザが複数の異なる区分された領域を読取るために，複数の復号キイを用いることなく，一つのパスワードで許されたアクセス領域を読取り可能とする.

2　多値化

既存の二次元コードとの互換性を維持しつつ，秘匿領域を追加するために，二次元コードの基本単位であるセルの多値化を行う必要がある．多値化の手法として，多色化と多領域化が知られている．多領域化は，セルを複数の領域に分割し，それぞれに独立した情報を与える方式である．ここでは，互換性と秘匿化のための大容量化のために，多色化と多領域化を併用する．そして，二次元コードとして，QR コード[1]を対象とする．この事例を図 3 左側に示す．QR コードのセルが白または黒の1ビットを表現しているが，それを多値化するために，図 3 右側に示すセルの構造を採用する．

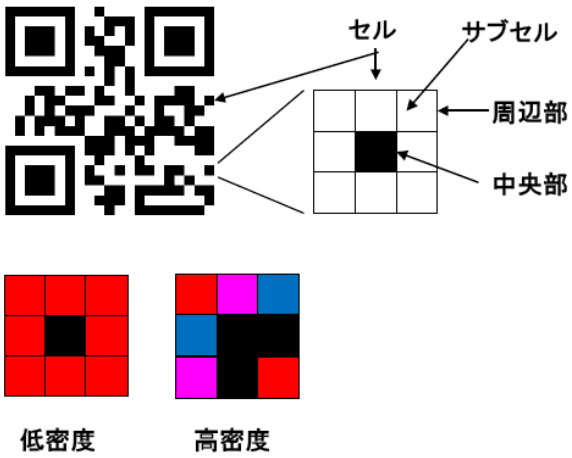


図 3　QR コードとセルの分割

この構造は，セルを 9 個の正方形の領域に分割する．そして，中央部を互換部に，周辺部を新規の追加領域（秘匿部）に割当てる．互換部は，既存の読取装置で読取が容易になるように白色または黒色とする．周辺部は，大容量化のためにカラー色とする．また，周辺部全体を，すなわち 8 個のサブセルを一つの符号化単位とするものを低密度コード，個々のサブセルを符号化単位とするものを高密度コードと呼ぶ．ここでは，高密度コードの利用を前提としている．

2.1　互換性の実現

2.1.1　センター色方式

既存のスマートフォンの二次元コードの読取りソフトウェアは，セルの切り出し後，各セルの中央部の画素の色，すなわち白色または黒色かを判別している．そこで，互換部のデータの識別には，周辺部の寄与は小さい．

しかし，周辺部の色が，互換部と反対の色である場合には，誤って識別される可能性が高くなる．すなわち，互換部が白の場合において，周辺部が黒の場合には，影響が大きくなる．これは，手振れやピントボケ，OSの処理が原因として考えられる．そこで，周辺部の色を白グループ色と黒グループ色に分類し，互換部が白色の場合には，周辺部を白グループ色を割り当て，黒色の場合には黒グループ色を割り当てる．ただし，これらのカラー色は，印刷される場合には，印刷時のインクの発色や経時劣化による変色で，白または黒グループの範囲に止まらない可能性がある．そこで，白または黒グループ色の周辺部への割り当ては，互換部の識別において，中央部の識別に与える影響を低減するための補助的な手法と言える．

2.2　多色化

ここでは，8 色を用いた場合について述べる．

2.2.1　色の選択

距離尺度としてユークリッド距離を用いる．この距離尺度では，RGB の三次元空間で相互に最も離れた色セットが識別が最も容易となる．そこで，相互に最も離れた位置は RGB 空間の立方体の端部であり，当該位置にある色を選択する．

選択した各色の RGB の具体値を表 1 に示す．表 1 に，各色の輝度を示したが，輝度(Y)と RGB 値の変換式は，ITU-R BT.601[13]で規定されている次式を用いた．

$$Y = 0.299R + 0.587G + 0.114B \qquad (1)$$

輝度の値を基に，各色を白または黒グループに分類した．

表1　カラー8色の選択と符号化データ

色群	色コード	RGB			輝度	色	符号化データ
		R	G	B			
白グループ	000	255	255	255	1		00
	001	255	255	0	0.89		01
	010	0	255	255	0.70		10
	011	0	255	0	0.59		11
黒グループ	100	255	0	255	0.41		00
	101	255	0	0	0.30		01
	110	0	0	255	0.11		10
	111	0	0	0	0		11

2.3　仮想的な積層構造

選択した8色について，白グループと黒グループの色はそれぞれ4色であるので，新たに2ビットを表現できる．この色コードと保持するデータの対応を表 1 の符号化テーブルの最右列に示す．この例では，色コード 000(白)はデータ 00 を保持する．周辺部の 8 色の多色化によって，従来と同容量の既存領域と従来の 2 倍の容量の新規領域からなる二次元コードを表現する．

この構成は，一つのセルが 17 ビットを表現しているので，図 4 に示すように，白黒の既存の2次元コードが 17 層重なっているのと同等である．

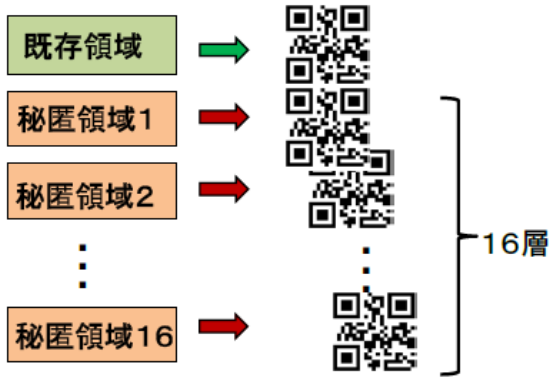


図 4　仮想的な積層構造

以下では，個々の仮想的な白黒の二次元コードを層と称する．

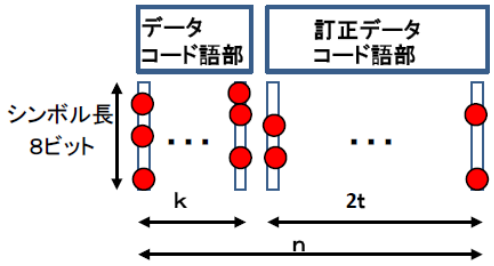
3　層レベルの暗号化

多値セル型二次元コードの新規領域に記憶するデータを秘匿化する手法として，パターンマスク法[11]を用いる．ここでは，パターンマスク法について簡単に紹介する．

3.1　パターンマスク法

パターンマスクによる暗号化は，QRコードの誤り訂正に用いるリードソロモン符号(RS 符号)を用いた暗号化である．RS 符号は，ブロック型の誤り訂正符号であり，予め定義された誤り訂正能力の範囲内の誤りについては，その誤りを訂正することが可能である．しかし，その能力を超えた誤りについては，誤りを訂正することができない．従って，各データコード語に誤りを発生させる行為を，誤りデータビットの位置を共通鍵とする暗号化として捉えることができる．

RS 符号において，t 個のデータコード語の誤りまで訂正可能とすると，t個を超えるデータコード語に誤りを発生させれば，訂正できず復号できない．その誤りの発生をパターンマスクを用いて行うことが可能である．



n: データコード語総数
k: データデータコード語数
t: 訂正可能データコード語数
●: 誤りビット

図 5　パターンマスクによる誤り発生

ここでは，確実に復号を不可能とする為に，全データコード語に誤りを発生させる．また，データコード語を構成するビットについて，平均的に半数

のビットを反転させる. 攻撃者からの推定を避けるために, 乱数を用いて反転ビットを決定する. そして, すべての新規領域について, 乱数によって発生させた値と新規領域セルの値の XOR の計算を行う.

4 領域分割とその暗号化

4.1 領域分割

2.3 節で述べたように, 多値セル型二次元コードは17個(層)の仮想的な白黒の二次元コードから構成される. ここで, 互換領域(層)を除く16層を用いて秘匿領域を構成する. この構成を表2に示す.

表 2 秘匿領域のデータ構成

領域名		収容データ
管理領域(非暗号化領域)		ユーザの暗号化された復号キイ、層の割り当て
データ領域(暗号化領域)	データ領域1	アクセス制御の区分毎の収容データ
	データ領域2	
	⋮	
	データ領域n	

秘匿領域は, 管理領域とデータ領域に分割される. 管理領域はユーザ毎のパスワードに対応するパターンマスク値やデータ領域に対する層割り当てデータを収容する領域であり, 層単位で構成されパターンマスク暗号がかけられない領域である. データ領域はアクセス制御の区分毎に設定されたデータを収容する領域であり, 層単位で構成され, パターンマスク暗号がかけられている領域である.

データ領域は, アクセス制御の区分毎にn個に分割され, 各データ領域を構成する層は, 同一のパターンマスク暗号がかけられる. 各データ領域に割り当てられる層は, 当該データ領域に収容するデータ量によって自動的に割り当てられ, 管理層に記憶される. また, 各データ領域の暗号化に用いるパターンマスク値は乱数によって生成する.

4.2 複数ユーザへのアクセス権割り当て

m 個のユーザに対して, n 個のデータ領域に対するアクセス権の割り当てを行う. ここでは, 一般的な記述の前に, ユーザ数3, データ領域数4の場合のアクセス権の割り当ての例を表 3 に示す.

表 3 各ユーザへのアクセス権の割り当て

データ領域名	割当層	ユーザA	ユーザB	ユーザC
データ領域1	1～4	○		
データ領域2	5～8	○	○	
データ領域3	9～10	○	○	○
データ領域4	11～15			○

この例は, ユーザAはデータ領域 1,2,3 に, ユーザBがデータ領域 2,3 に, ユーザCはデータ領域 3,4 に, それぞれアクセス権が付与されている. そして, 例えば表に示された層が, それぞれのデータ領域に割り当てられる. これらの同一のデータ領域に割り当てられた層は同一のパターンマスクによって暗号化される.

データ領域 n のパターンマスク値を Pn とすると, この例では, 4つの乱数によって生成されたパターンマスク値 P1, P2, P3, P4 が生成され, 暗号化に用いられる.

一般的に, データ領域 n, ユーザ数 m の場合のアクセス権の割り当て表は, 表 4 のようになる.

表 4 一般的なアクセス権の割り当て

データ領域名	割当層	ユーザ1	・・・	ユーザM
データ領域1	各データ領域のデータ量によって割り当て			
データ領域2				
⋮				
データ領域N				

4.3 ユーザ毎のパスワード設定

表 3 の例の場合, ユーザAは3つのデータ領域にアクセス権が付与されており, それらのデータ領域の3つのパターンマスク値 P1, P2, P3 を知る必要がある. しかし, 一つの多値セル型二次元コードについて, 複数の復号キイ(パターンマスク値)を

管理するのは煩雑である．そこで，一つのユーザが一つに多値セル型二次元コードの復号キイを一つのパスワードでアクセスする方法を検討する．

ユーザが一つのパスワードで複数のパターンマスク値を知得していると同様な処理を可能とする為には，多値セル型二次元コードの中にユーザに付与されたデータ領域のパターンマスク値を記憶している必要がある．また，それらを記憶する層はパターンマスクによって暗号化されていない必要がある．そして，記憶されるパターンマスク値はそのままの値を記憶している場合，全ての者が読取り可能であり，暗号化への復号キイの役割を果たすことができない．そこで，共通鍵であるパスワードで暗号化されたパターンマスク値を記憶する．

表 5　パスワードと暗号化パターンマスク

ユーザ名	パスワード	収容パターンマスク値	暗号化パターンマスクセット
ユーザA	PWa	P1, P2, P3	EPa
ユーザB	PWb	P2, P3	Epb
ユーザC	PWc	P3, P4	Epc

これらを整理すると，表 5 のように，ユーザAはパスワード PWa を付与され，パターンマスク値(P1,P2,P3)をパスワード PWa によって暗号化し，暗号化パターンマスク EPa を得て，表 2 の管理領域に格納する．管理領域は全ユーザの暗号化パターンマスク値 EPa,EPb,EPc を収容する．管理領域に割り当てる層の数は EPm を収容するに足る層数が割り当てられる．

5　符号化と復号の処理

符号化と復号の処理について具体的に説明する．暗号化に無関係の誤り訂正処理については省略する．

ここで，既存領域に収容するデータ *d0* 及び秘匿データ領域に収容するデータ *d1,.,dn* からなる収容データを D = (*d0, d1,.,dn*)とする．これらのデータを各層に配置したデータ *ld1..ld16* からなる収容データを LD=(*ld1..ld16*)とする．また，この各層の収容データを白黒符号としたデータ ud0,ud1..ud16 からなるデータを UD=(ud0,ud1..ud16)とする．そして，この白黒符号をカラー化したデータ cd1,.,cd8 からなるデータを CD=(cd1,.,cd8)とする．

これらの個別のデータ配置を表 6 に示す．

表 6　データの配置

項目			収容データ	層(白黒)レベルデータ	カラーレベルデータ
既存領域			d0	ld0	
新規領域（秘匿化領域）	管理領域（非暗号化領域）			ld1..ldj	cd1..cd8
	データ領域（暗号化領域）	データ領域1	d1	ldj+1..ld16	
		データ領域2	d2		
			d3..dn-1		
		データ領域n	dn		

5.1　符号化処理

ステップ 1:データの準備及び圧縮

二次元コードに収容するデータの種別(英数字，漢字，バイナリー)毎に圧縮を行い，データ D = (*d0, d1,.,dn*)を準備する．

ステップ 2:既存領域の二次元コードの生成

既存領域のデータ d0 について，通常の白黒二次元コードの生成処理を行い ld0 及び ud0 を得る．

ステップ 3:管理領域の割り当て

ユーザ毎の暗号化パターンマスク及び層の割り当てデータを記憶する管理領域のデータ量を計算し，新規領域へ必要な層数を割り当てる．

ステップ 3:データの領域分割

n 個のデータ領域について，それらを新規領域の 16 層の内，管理領域に割り当てた層以外の層に割り当てる．

ステップ 4:パターンマスクの生成と暗号化

n 個のデータ領域に適用するパターンマスク P1..Pn を乱数を用いて生成する．それらを各ユーザのパスワード PWn を用いて暗号化し EPa..EPn を得て，管理領域データにセットする．

ステップ 5:新規領域の二次元コードの生成

ステップ 3 で，各データ領域に割り当てた層に．当該データ領域のデータを設定し，

LD=(ld1..ld16)を得る．その後各層にパターンマスク P1...Pn を用いてパターンマスク処理を行い，UD=(ud1..ud16)を得る．

ステップ 6:セル色の決定

UD=(ud1..ud16)について，表1の符号化テーブルを用いてセル色を決定し，最終的な多値セル型二次元コードの各サブセル色 CD = (cd1,..,cd8)を得る．

5.2 復号処理

ステップ 1:画像入力，画像抽出

撮像装置によって，二次元コードを含む画像を撮像し，二次元コードに含まれるファインダーパターンを基に二次元コードを検出し，二次元コードの画像を抽出する．

ステップ 2:セル色の識別

二次元コード画像から各セルを切り出し，セルの中央部及び周辺部のサブセル色の識別を行い，多値セル型二次元コードの各サブセル色 CD = (cd1,..,cd8)を得る．

ステップ 3:白黒二次元コードに復号

各セルについて，表 1 の符号化テーブルを用いて，セルの色コード CD = (cd1,..,cd8)から各層の各セルの白または黒の色を復号し，二次元コードの白黒符号 UD=(ud1..ud16)を得る．

ステップ 4:既存領域の復号

既存領域の白黒符号 ld0 から通常の白黒の二次元コードの復号処理を行い，収容データ d0 を得る．

ステップ 5:新規領域の復号

ステップ 5-1:管理領域の読取

秘匿領域の内，パターンマスク暗号処理がされていない管理領域を読取り，各ユーザの暗号化パターンマスクを読取り，秘匿領域のデータ構成を得る．

ステップ 5-2:パターンマスクの復号

ステップ 5-1 で復号できた暗号化パターンマスクを用いて，割り当てられた層のパターンマスク復号処理を行い LD=(ld1..ld16)を得る．LD=(ld1..ld16)からアクセスが許された収容データ d1,..,dn を得る．

6 用途

本論文で提案する多値セル型二次元コードの複数ユーザへのアクセス制御の想定用途について述べる．

6.1 商品情報

想定用途の第一は，商品情報のユーザを限定した提供である．この事例のユーザ例，データ例及びそのアクセス権の付与例を表 7 に示す．

表 7 商品情報提供の場合のアクセス権割当の例

データ領域名	製造者	物流	販売店	消費者
商品名、商品番号	○	○	○	○
製造年月日 製造ロット番号	○		○	
検査結果	○			
販売期限	○		○	
消費期限	○	○	○	○
連絡先	○	○	○	

この例で示すように，販売店や消費者に知られたくない情報を知らせる必要のあるユーザにのみ的確に提供することが可能になる．

6.2 偽物検出

想定用途の第二は，偽物検出である．この事例のユーザ例，データ例及びアクセス権の付与例を表 8 に示す．

表 8 偽物検出の場合のアクセス権割当の例

データ領域名	製造者	販売店	消費者	偽造者
商品名、商品番号	○	○	○	○
ブランド名	○	○		
シリアル番号	○	○		

この例では，多値セル型二次元コードの作成時に，偽造者が販売店に付与された復号キイを知らないので，当該販売店向けの多値セル型二次元コードを作成できない特性を用いている．誤った暗号化キイを用いて作成した多値セル

型二次元コードの正規品であることを示すデータを読取ることができないので，偽物であることが知れる．

7　実験結果

5 章で説明した符号化処理をPC上に，復号処理をスマートホン上に実装し，多値セル型二次元コードの作成及び読取の実験を表 9 に示す条件で行った．

表 9　試験条件

項目	条件
バージョン	バージョン4（29x29セル）
コードサイズ	40x40,30x30,20x20 mm
誤り訂正	レベルH
印刷紙	マット紙（コクヨ）
スマートフォン	GALAXY Note 2　(SAMSUNG製)
照明	室内の天井照明
焦点合わせ	スマートフォンによる自動焦点

その結果，データ量が少なく多値セル型二次元コードに収容でき，読取条件が良い場合には，予定したとおり，複数のデータ領域の中から複数のユーザがアクセスが許されたデータ領域を読取ることができた．しかし，次の二つの課題が明らかになった．

①データ配置の非効率

データ量が多い場合，データ量が収容可能量以下であるにも関わらず，収容できない場合が発生した．これは，データ領域を層単位で配置したからである．特定の層にはデータ領域が不足する一方，他の層では未使用のデータ領域が存在する場合が発生した．データ配置の効率を向上させるためには，データ領域の配置を層単位ではなく，別の単位で配置する必要がある．

②読取性能の不足

多値セル型二次元コードの読取りを，[12]では白色蛍光灯による照明を用いて実験を行い，二次元コードのサイズについて，その読取り限界を示した．今回は，照明のない実使用環境で実施した．その結果，スマートホンの影など二次元コード内に明度分布が発生する場合には，大きなサイズの二次元コードで読取率が低下した．この場合に対応するためには，読取時に明度補正機能が必要である．

8　終りに

本論文では，既存の二次元コードとの互換性を維持する既存領域と，追加のデータ領域である新規領域を有する二次元コードにおいて，新規領域を複数のデータ領域に分割し，複数のユーザがアクセス権を付与されたデータ領域のみを読取ることができるアクセス方式を提案した．

そして，提案したアクセス制御方式の応用について述べた．

参考文献

[1] ISO/IEC 18004:2006 Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification.

[2] ISO/IEC 16022:2006 Information technology – Automatic identification and data capture techniques – Data Matrix bar code symbology specification.

[3] H. Kato, K. Tan, D. Chai, Development Of A Novel Finder Pattern For Effective Color 2D Barcode Detection, Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications. ISPA '08. (pp. 1006-1013). Sydney, Australia. IEEE Computer Society,2008

[4] 助川 修司, QR コードの多色化による 2 次元コードの大容量化について, 情報処理学会全国大会講演論文集 第 70 回平成 20 年(4), 845-846, 2008

[5] 寺田 遼平, 藤本 敬介, 中山 泰一, カラー二次元コードを高解像化するための認識アルゴリズムの実現と評価, 信学技報, SS2008-57,2009-3

[6] 遠藤祐介,廣友雅徳, 佐治勇樹, 渡辺優平, 森井昌克, 多値二次元コードにおける高階調度認識アルゴリズムの提案, 電子情報通信学会論文誌 D Vol.J95-D No.11 PP.1935-1943

[7] 小野 智司, 電子透かしを用いたカラー二次元コードの複製検知, 電子情報通信学会論文誌. D, 情報・システム J94-D(12), 1971-1974, 2011

[8] 新見道治, 反復型可逆的情報ハイディングを利用した大容量二次元コード, 2009 年電子情報通信学会総合大会, S21-S22

[9] 原 昌弘,‘二次元コードの生成方法およびその読取り装置, 特開 2008-299422

[10] 寺浦 信之, 櫻井 幸一, 互換領域を有する暗号付二次元コードへのセルレベルの誤り訂正の導入, 2013 年暗号と情報セキュリティシンポジウム(SCIS2013),2013

[11] 寺浦 信之, 櫻井 幸一, RS符号データコード語にパターンマスクを適用した多値化二次元コードの秘匿化, コンピュータセキュリティシンポジウム(CSS2013), 809-816, 2013

[12] 寺浦 信之, 櫻井 幸一, 秘匿領域を有する高密度二次元コードの互換性と識別性に関するスマートフォン実装による評価, 2015 年暗号と情報セキュリティシンポジウム(SCIS2015), 1B2-2, 2015

[13] http://www.itu.int/rec/R-REC-BT.601/e.