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

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 システム情報科学府
819-0395 福岡県西区元岡744番地
sakurai@inf.kyushu-u.ac.jp

あらまし 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、新規領域を秘匿化する検討を行った. 新規領域の付加は、二次元コードの基本単位であるセルを多値化した大容量化により行う. セルの多値化手法には多色方式がある. 上記の新規領域のデータの暗号化の手法として、パターンマスク法を提案する. パターンマスク法は、二次元コードの誤り訂正で用いられているリードソロモン符号に基づくデータコード語及び訂正データコード語を共通鍵パターンによるマスク（排他的論理和）処理によりデータコード語誤りを発生させ、復号を不可能にする. アプリソフトによる暗号化処理等との比較を行う.

Confidentiality of multivalued two-dimensional code of applying a pattern mask to RS code symbols

Nobuyuki Teraura†　　Kouichi Sakurai‡
†Terrara Code Research Institute
53-26 Gochu Kagiya-cho Tokai-city,　477-0032, JAPAN
TerraNob@terrara.jp
‡Information Science and Electrical Engineering, Kyushu University
744 Motooka Nishi-ku Fukuoka,819-0395, JAPAN
sakurai@inf.kyushu-u.ac.jp

Abstract we propose a two-dimensional code having an area of two, the public section which can be read in conventional equipment and private section which reading has been limited. A cell is expressed with multiple color using gray or color. The color used for it is stratified in a white group and a black group on the basis of a lightness. White and black are expressed into an applicable group and a public part is constituted. About each group, a 1 to 3-bit data is coded using 2 to 8 colors.

†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二次元コードにおいて、新規領域を秘匿化するために、パターンマスクを用いる手法を提案し、既存の手法との比較を行なう.

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、すべての人への情報提供を目的とした応用だけでなく、特定の人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ことを検討する.

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] [11] [12]がある.

1．4　課題

互換性を維持するために互換領域を設定し、セルの多値化によって新たに大容量化によって追加した領域を秘匿化することが課題である.

また、セルの多値化に際して、既存の二次元コードとの互換性を維持する既存領域を設け、既存領域のデータを既存機器を使用するユーザーで利用可能とし、既存の二次元コードユーザの利用や本提案の二次元コードを用いる新システムと従来の二次元コードを用いるシステムの併存が可能とする.

2. 多値化

二次元コードの大きさを維持しつつ大容量化を図るためには、基本要素であるセルを多値化する必要がある. 互換性を維持した多値化には、多色化[10]と多領域化[11]がある.

図2に、通常の白黒の二次元コードと多色化及び多領域化二次元コードの例を示す.

白黒既存方式　多色方式　多領域方式

図 1　セルが1値と多値の二次元コード

次に、文献[10] に従って、互換領域を有する多色化による大容量化の概要を述べる.

2.1　多色化によるセルの多値化

現在普及している二次元コードは、セルを白と黒の 2 色で表現するため、セルは 1 ビットの情報を有している. これを k^2 色で表現すれば、k ビットの情報を有することができる. 従って、8 色または 16 色で表現すれば、それぞれ 3 ビット、4 ビットの情報を有することができる.

2.2　互換性

8 色を用いた多色化では、8 色を輝度（反射率の代替え指標）によって 4 色ずつ白グループと黒グループに分別し、既存の二次元コードの白または黒に対応する色グループの色を割り当てる. そして、白グループの最小輝度と黒グループの最大輝度の差を ISO/IEC の規定[13]の大きさに設定する. これにより、既存の二次元コードの読取り装置では、白グループの色は白に、黒グループの色は黒と識別されるので、既存の装置で読取り可能となり、互換領域を実現可能である.

色の選択の事例と選択した各色の RGB の具体

値を表 1 に示す. この場合では、白と黒のグループ間の輝度差は 0.44 に設定されている. ここで、輝度(Y)と RGB 値の変換式は、ITU-R BT.601[14]で規定されている次式を用いた.

$$Y = 0.299R + 0.587G + 0.114B$$

表 1　色コードと色の対応事例

色群	色コード	RGB			輝度	色
		R	G	B		
白グループ	000	255	255	255	1	
	001	255	255	0	0.93	
	010	64	255	255	0.84	
	011	0	255	0	0.72	
黒グループ	100	255	0	255	0.28	
	101	128	0	255	0.18	
	110	159	0	0	0.13	
	111	0	0	0	0	

ただし、実際の適用に当たっては、印刷時の発色、経時劣化、撮像時の変色など設計色と読み取り時の色の差異の検討が必要である.

2.3　色の符号化

選択した 8 色について、000 から 111 までの 3 ビットで表現した色コードを割り当てる. この割当ての例を表 1 に示す.

この色コードで示された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示す符号化テーブルを表 2 に示す. この例では、色コード 000(白)はデータ 00 を保持する. 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.

表 2　多色化の符号化テーブル

	色コード	色	符号化データ
白グループ	000		00
	001		01
	010		10
	011		11
黒グループ	100		00
	101		01
	110		10
	111		11

3.　QR コードの構造とパターンマスク

ここでは、二次元コードの事例として、QR コード[1]を取り上げる. QR コードの構造を図 2 に示し、その概略を説明する.

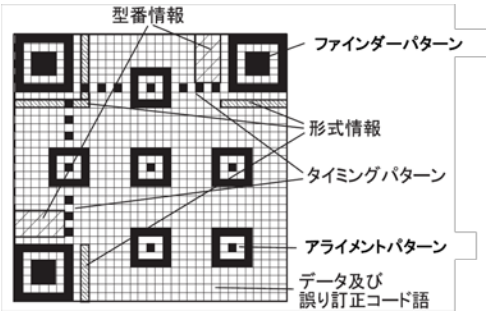


図 2　QR コードの構造

QR コードには、記憶するデータによって変化しない固定部と変化する可変部がある.

3.1　固定部

固定部には、撮影した画像の中から二次元コード部分を識別し、その範囲を確定し、回転角や曲がりの補正を行うためのパターンが埋め込まれている.

ファインダーパターンは、三隅に設定されたパターンであり、二次元コードの存在を識別するためのパターンである. その中心を横切る走査線は、どの方向の走査でも 11311 の長さの白黒パターンとなる. これにより、位置と回転角を判別する. タイミングパターンは白と黒のセルが交互に配置されており、セルの座標を判別する. アライメントパターンは、飲料容器などの曲面上に印刷された場合の画像の歪みを補正するのに用いる.

3.2　可変部

可変部には、データを保持するデータコード語部、誤り訂正を可能とする訂正データコード語部及び管理データ部がある.

管理データ部には、QR コードの大きさ(バージョン)を示す型式情報部と誤り訂正レベルとマスクパターンの情報を示す形式情報部がある.

3.3 パターンマスク処理

二次元コードの読出しを確実にするために、白と黒のセルをバランスよく配置され、また、ファインダーパターンに見られる黒白黒黒黒白黒のセルパターンがなるべく出現しないのが望ましい.

マスク処理は符号化領域(型式情報及び型番情報を除く)で、データパターンとマスクパターンとで順に XOR 演算による白黒変換を行わせる処理である[1].

マスクパターンの条件式を表 3 に、条件式に対応するパターンの例を図 3 に示す. ただし、見やすくするために、機能パターン部を併せて示す.

表 3 パターンマスクの条件式

マスクパターン番号	条件
000	(x+y)mod 2 = 0
001	X mod 2 = 0
010	Y mod 3 = 0
011	(x+y)mod 3 = 0
100	((x div 2)+(y div 3)) mod 2 = 0
101	(xy) mod 2 + (xy) mod 3 = 0
110	((xy) mod 2 + (xy) mod 3) mod 2 = 0
111	((xy) mod 3 + (x+y) mod 2) mod 2 =0

000　　011　　100　　111

図 3 パターンマスクの図示

4. パターンマスクを用いた暗号化

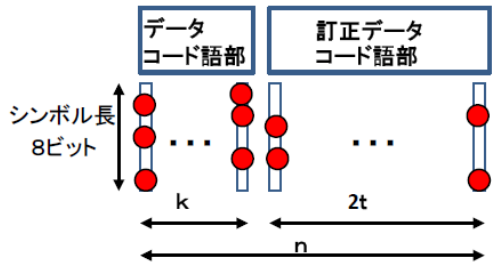
多値化二次元コードの新規領域に記憶するデータを秘匿化する手法として、パターンマスク法、符号化テーブル法、個別アプリケーション(個別アプリ)によるデータの暗号化法がある. ここでは、パターンマスク法について詳しく述べ、その他の手法を簡単に紹介し、これらの手法との比較を行う.

4.1 パターンマスク法

4.1.1 考え方

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処理を、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、訂正できず複合できない. その誤りの発生を 3.3 節で説明した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 4 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. すなわち、乱数を用いて全ての新規領域(データ部と訂正部)のビット反転について、決定する. これらはまた、すべての新規領域について、乱数によって 0 または 1 を決定し、この値と新規領域セルの値の XOR の計算を行うことと等価である. そして、この処理は、3.3 節で述べた既存のパターンマスクの処理と同じである.

4.1.2 訂正可能確率の検討

パターンマスク処理によって、各データコード語に誤りを与えるが、誤りのあるデータコード語が t 個以下である場合には、誤り訂正の能力によって、正しく復号される. そこで、その確率を計算する.

一つの 8 ビットで構成されるデータコード語が誤りを含まない確率 Ps は、

$$Ps = (1/2)^8$$

である. 一方、n 個のデータコード語の中から m 個を選択する組み合わせの数 N は、

$$N = nCm$$

である. そこで、n 個のデータコード語の中から m 個のデータコード語を選択し、それらが誤りを含まない確率 Pm は、

$$Pm = nCm \times Ps^n$$

である. そこで、誤りの無いデータコード語が m 個以下である確率 P は

$$P = \sum_{k=1}^{m} nCk/2^{8n}$$

具体的な二次元コードの各バージョンについて計算した結果を表 4 に示す. 誤り訂正レベルは最大の訂正能力を有する L レベル[1]である.

この結果により、訂正可能確率は無視できる程度であることが判る.

表 4 訂正可能確率

バージョン	データコード語数	訂正データコード語数	訂正可能確率
2	16	28	2.2×10^{-95}
3	26	44	1.9×10^{-151}
4	36	64	3.9×10^{-215}

4.1.3 誤り訂正による脆弱性

正しいパターンマスクデータを適用しなくとも、誤り訂正機能により復号できる場合がある. そこで、攻撃者によるラウンドロビン攻撃において、一つの復号可能なパターンマスク(復号鍵)あたりの場合の数は減少する. すなわち、誤り訂正機能によって脆弱性が発生する.

256 ビットのパターンマスクを用いる場合、その場合の数 Np は

$$Np = 2^{256} \fallingdotseq 1.2X10^{77}$$

である. また、訂正可能なパターンマスクの場合の数 Nc は

$$Nc = \sum_{k=1}^{t} nCk \times 2^{8k}$$

である. バージョン 2 の場合には、

$$n = 44, \quad t = 14$$

であるので、

$$Nc \fallingdotseq 6.0X10^{44}$$

である. そこで、復号可能なパターンマスク当たりの場合の数 Nr は、

$$Nr = Np / Nc \fallingdotseq 1.9X10^{32}$$

となる. 誤り訂正による脆弱性から復号可能なパターンマスクあたりの場合の数は減少するが、それでも十分な計算量的安全性を有していると言える.

4.2 他の暗号化手法

4.2.1 符号化テーブル方式

符号化テーブルは、多色のセルを多層の白黒のセルに読み替えるテーブルであり、このテーブルを符号化と復号で共有しなければ、正しく復号することができない. そこで、符号化テーブル自体を暗号の共通鍵と捕らえることが可能である[8].

表 1 に示す 8 色の場合には、白と黒の各グループで、4!組合せがあるので、全体の組合せ Nt は、

$$Nt = 4! \times 4! = 576$$

である. これをデータコード語を構成する 8 個のセルに異なる符号化テーブルを適用すると、すべての組合せ Na は

$$Na = Nt^8 \fallingdotseq 1.2 \times 10^{22}$$

となる. この場合のは、暗号鍵の長さは、一つの符号化テーブルを 24 ビットで表現できるので、その 8 倍の 192 ビットとなる.

また、偶数番目のデータコード語と奇数番目のデータコード語について、さらに異なる符号化テーブルセットを適用するとすれば、

$$Na = Nt^{16} \fallingdotseq 1.5 \times 10^{44}$$

となり、計算量的安全性を確保可能である.

また、符号化テーブル法は、色の表現に 3 ビットを用いており、暗号化鍵長あたりの場合の数が少なく、暗号化鍵長が同じ場合にはパターンマスク法と比較して、ラウンドロビン攻撃に弱いと言える.

そして、誤り訂正による脆弱性を、パターンマスク法と同様に有する.

4.2.2 個別アプリによる暗号化方式

パターンマスク及び符号化テーブルを用いる二次元コード固有の暗号化の他に、一般的に用いられている共通鍵の暗号化手法を適用することも可能である. すなわち、記憶すべきデータを個別アプリにより共通鍵で暗号化したデータを二次元コードに記憶させ、読取り時に読取ったデータを個別アプリにより共通鍵で復号する手法である.

4.3 他の暗号化手法との比較

パターンマスク法と符号化テーブル法及び個別アプリによる暗号化の比較を行う.

4.3.1 システム構成の煩雑性

パターンマスク法と符号化テーブル法は、多値二次元コードの特性を用いた手法であり、システムの構成は同じであり図 5 となる. すなわち、多値二次元コードの発行システムでは、個別のアプリは暗号化キイを意識することなく多値二次元コードを発行する. そして、読取りシステムでは読取り装置の中に復号キイが記憶され、読取装置によって暗号の復号がなされ、復号されたデータがアプリに引き渡される.

それに対して、個別アプリによる暗号化では、図 6 に示す構成となり、発行システムの個別アプリが暗号化キイを識別し、読取りシステムにおいても個別アプリが読取装置から受取ったデータを復号処理する必要がある. また、個別のシステム毎

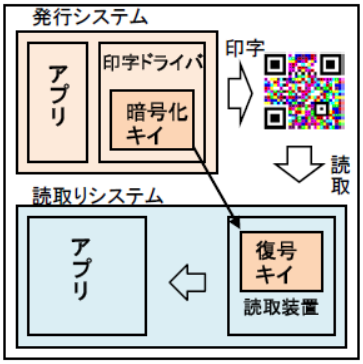


図 5 パターンマスク法及び符号化テーブル法のシステム構成

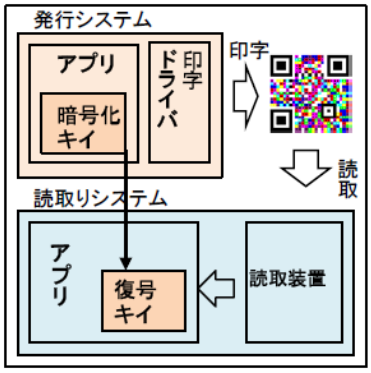


図 6 個別アプリ法のシステム構成

に復号処理を行う個別アプリが必要となり、煩雑である.

従って、煩雑性の観点からは、パターンマスク法や符号化テーブル法が優れていると言える.

4.3.2 ラウンドロビン攻撃への耐性

4.2.1 で述べたように、符号化テーブル方式は、単位暗号化キイ長当たりの場合の数が少なく、また誤り訂正機能による脆弱性を有する. 一方、個別アプリ法では任意の暗号化手法が使用可能であり、計算量的安全性は高いと言える.

4.3.3 演算量

新規領域のパターンマスク処理は不可欠な演算ではないが、既存領域で行われている演算であり、演算量が増加しない。また、符号化テーブル法は多値化(カラー化)を行うための不可欠な処理である。

それに対して、個別アプリによる暗号化は、付加的に行う処理であるので、演算量は増大する。

4.4 併用

これらの三つの手法は、それぞれ独立しており、三つを同時に適用することが可能である.

上記のように、符号化テーブル法は暗号化キイ長あたりの場合の数が少なく、誤り訂正機能による脆弱性がある. そこで、通常の秘匿化ではパターンマスク法単独で用い、特に大きな秘匿性が必要な場合には、パターンマスク法と個別アプリ法の併用による暗号化を行うのが最適と言える.

5. 符号化と復号の処理

前節で述べたパターンマスク方式を用いた暗号化について、その符号化と復号の処理について具体的に説明する.

ここでは、色数が 8 色、暗号化キイ長が 256 ビットの場合について説明する. 8 色を用いてセルの多値化を行うので、一つのセルは 3 ビットを表現する. そこで、既存領域に 1 ビット、新規領域に 2 ビットが割当てられる.

ここで、既存領域に収容するデータ *d0* 及び新規領域に収容するデータ *d1,d2* からなる収容データを D = (*d0,d1,d2*)とする. また、訂正部データを D1c=(*d0c,d1c,d3c*)とする. これらのデータを白と黒に符号した白黒符号部を U = (Ud, Uc)とし、Ud,Uc, はそれぞれデータ部、誤り訂正部の符号部であり、それぞれ下に示すように、三つの白黒符号化データから構成される.

Ud = (*u0, u1, u2*)

Uc = (*u0c, u1c, u2c*)

また、これらの三つの仮想白黒セルをカラー8 色に符号化したカラー符号を S=(Sd, Sc)とし、Sd,Sc はそれぞれデータ部、誤り訂正部の符号部である. これらの個別のデータ配置を表 9 に示す.

表 9　データの配置

項目			データ部	訂正部
全体		データ	*d0,d1,d2*	*d0c,d1c,d2c*
		カラー符号	*Sd*	*Sc*
既存領域 非暗号化データ		データ	*d0*	*d0c*
		白黒符号	*u0*	*u0c*
新規領域	暗号化データ1	データ	*d1*	*d1c*
		白黒符号	*u1*	*u1c*
	暗号化データ2	データ	*d2*	*d2c*
		白黒符号	*u2*	*u2c*

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,d2*)を準備する.

ステップ 2:既存領域の二次元コードの生成

ステップ 2-1:RS符号化

既存領域のデータ *d0* について、8 ビット単位の RS 符号のデータ語とし、訂正部データ語を計算し、訂正データ *d0c* を得る.

ステップ 2-2:パターンマスク処理

データ部と訂正データ部について、予め定められたマスクパターンを順次に選択し、ファインダーパターンと一致するパターンを有しないマスクパターンを選択し、そのマスクパターンを適用した *U0, U0c* を得る. これは通常の二次元コードと同じ処理である.

ステップ 3:新規領域の二次元コードの生成

ステップ 3-1:マスクパターンの生成

マスク処理を行うパターンを生成する. 乱数を用いて、順に 0 と 1 とを選択して 256 ビットを決定し、マスクパターン Pm とする.

ステップ 3-2:RS符号の符号化処理

新規領域データ *d1,d2* についてそれぞれ 8 ビット単位の RS 符号のデータ語とし、訂正部データ語を計算し、訂正部データ *d1c,d2c* を得る.

ステップ 3-3:パターンマスク処理

ステップ 3-1 で生成した二次元コードのマスクパターン Pm を用いてマスク処理を行う. 具体的には、二次元コードのパターン((*d0,d0c*)及び(*d1,d1c*))とマスクパターン Pm の XOR の演算を行う. Pm は繰り返し適用する。

ステップ 4:セル色の決定

既存領域および新規領域の二次元コードパターン U = (*u0,u1,u2*)について、符号化テーブルを用いてセル色を決定し、最終的なカラー二次元コード S=(Sd, Sc)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

二次元コードの可変領域のセルについて、二次

元コード画像から各セルを切り出し、セル色及びユニット色の識別を行い、セルの色コード S=(Sd,Sc)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、指定された符号化テーブルを用いて、セルの色コード S=(Sd,Sc)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 U = (Ud, Uc)を得る.

具体的には、i 番目のセルのカラーセル色 Si を符号化テーブルにより、白黒のセル色に分解する. この復号処理を全てのデータ語を構成するセルについて行い U = (*u0,u1,u2*)を得る.

ステップ 4:既存領域の復号

ステップ 4-1:パターンマスク処理

多値化されていない型式情報部から適用したマスクパターンを識別し、当該マスクパターンを用いて既存領域のデータ部及び訂正データ部のマスクパターン復号処理を行い、D=(*d0, d0c*)を得る.

ステップ 4-2:RS符号の復号処理

既存領域(*u0*)のデータ部及び訂正データ部について RS 符号の誤り訂正処理を行い、*d0* に誤りがあれば訂正する. 以上は、通常の二次元コードの復号処理である.

ステップ 5:新規領域の復号

ステップ 5-1:パターンマスク処理

新規領域(*u1, u2*)のデータについて、予め符号化した者から通知されたマスクパターンを用いて新規領域のデータ部及び訂正データ部のマスクパターン復号処理を行い、D=(*d1, d2)*を得る.

具体的には、新規領域1(*d1*)を例にとると、i 番目のセルと i 番目のパターンマスク値について、XOR の演算を行う.

ステップ 5-2:RS符号の復号処理

ステップ 5-1 で得た新規領域(*d1, d2*)のデータ部及び訂正データ部のデータ語を用いて RS 符号の誤り訂正処理を行い、*d1, d2* に誤りがあれば訂正する.

以上の復号処理で、データ D=(*d0,d1,d2*)が求められる.

6. 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、新規領域を秘匿化する検討を行った. 秘匿化の手法として、マスクパターンを暗号化キイとして用いる手法を提案し、その有効性を示した.

今後、オープンな環境で使用を可能とするため、マスクパターンを公開鍵で暗号化して、二次元コードに組み込む手法を検討していく予定である.

謝辞

第一著者の研究は、財団法人生涯学習開発財団より奨学資金を得て行われた. ここに記して、感謝の意を表します.

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、グレイ及びカラー化による二次元コードの情報ハイディング、コンピュータセキュリティシンポジウム (CSS2012), 309-316, 2012

[11] 寺浦 信之、櫻井 幸一、'セルの微細分割による二次元コードの情報ハイディング'、第 11 回情報科学技術フォーラム (FIT2012), 571-578, 2012

[12] 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

[13] ISO/IEC 15415:2011 Information technology – Automatic identification and data capture techniques – Bar code symbol print quality test specification – Two-dimensional symbols.

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