

多値セル型二次元コードでの 多分割領域への複数ユーザのアクセス制御

寺浦 信之^{1,2,a)} 櫻井 幸一³

受付日 2015年12月3日, 採録日 2016年6月2日

概要: 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二次元コードのニーズも存在する. 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み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, 複数の読み取り者ごとに読み取り範囲が異なる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広げることができる. そこで, この場合に対応可能なシステムを検討する.

キーワード: 二次元コード, 多値型セル, データ領域分割, アクセス制御

Multi-user Access Control to the Divided Area on Multi-value Cell Two-dimensional Code

NOBUYUKI TERAURA^{1,2,a)} KOUICHI SAKURAI³

Received: December 3, 2015, Accepted: June 2, 2016

Abstract: The need of providing only a specific target with the information, 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.

Keywords: two-dimensional code, multi-value cell, Data area division, access control

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み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, 誰でもが読み取り装置を用いて読み取ることが可能である. 携帯電話に読み取り機能が具備されて以来, 誰でもが容易に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

¹ 株式会社テララコード研究所
Terrara Code Research Institute, Tokai, Aichi 477-0032, Japan

² 九州大学社会人博士課程
Kyushu University, External PhD-course, Fukuoka 819-0395, Japan

³ 九州大学
Kyushu University, Fukuoka 819-0395, Japan

^{a)} nobu@tcodes.jp

*1 本論文は, CSS2015 で発表した論文 [21] の加筆修正版である.

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、セルを多値化するため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], [4], [5], [6], [7], [8] がなされている。そして、セルを微細に分割して大容量化を図る研究がある [9]。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 [10], [11], [12], [13] 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 [14] 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 [15], [16], [17] 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み取り可能とする方式が提案されている [14]。この方式は、図 1 のように、データ領域と読み取り者が 1 対 1 の関係では有効である。

1.4 課題

一方、二次元コードのデータが複数の領域に区分されており、複数の読み取り者ごとに読み取り範囲が異なる図 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広げることができる。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み取るために、複数の復号キイを用いることなく、1つのパスワードで許されたアクセス領域を読み取り可能とする。

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は、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。

この構造はセルを 9 個の正方形の領域（サブセル）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）に割り当てる。互換部は、既存の読み取り装置で読み取り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 1 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、高密度コードを用いた場合の検証を行う。

2.1 互換性の実現

既存のスマートフォンの二次元コードの読み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が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 [15]。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

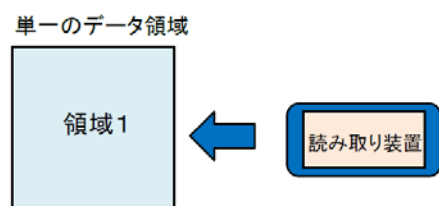


図 1 データ領域と読み取り者が 1 対 1 の場合
Fig. 1 A data area and a reader is 1 to 1.

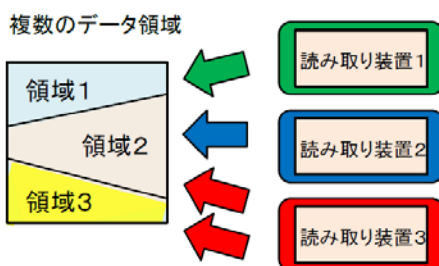


図 2 データ領域と読み取り者が N 対 M の場合
Fig. 2 A data area and a reader is N to M.

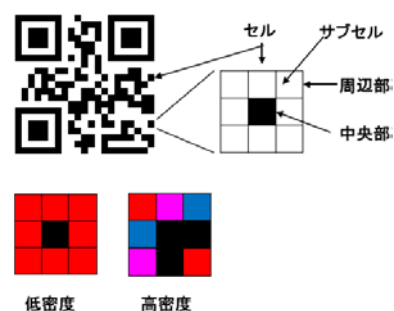


図 3 QRコードとセルの分割
Fig. 3 QR code and cell segmentation.

表 1 カラー 8 色の選択と符号化データ

Table 1 Selecting and encoding eight colors.

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

大きくなる。これは、手振れやピントボケ、解像度不足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とど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させるための補助的な手法といえる。

2.2 多色化

ここでは、8色を用いた場合について、色を選択する基準について述べる。

距離尺度として RGB 空間での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 [18] で規定されている次式を用いた。

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

輝度の値を基に、各色を白または黒グループに分類した。

2.3 色符号化

高密度構成におけるサブセルは、セル色によって、白グループまたは黒グループの 4 色によって符号化される。

4 色による符号化では 2 ビットを表現できる。図 4 に示すように、2 つの同一サイズの白黒の二次元コードの同一位置のサブセルの値を表 1 の符号化データに基づき色を選択することにより符号化する。たとえば、互換部が黒であるセルにおいて、サブセルが両方ともに白 (0) の場合には 00 の 2 ビットを表現し、紫色に符号化される。



図 4 二次元コードの色符号化

Fig. 4 Configuration of color encoding of 2D code.

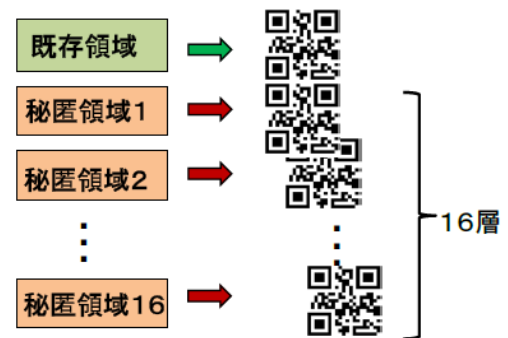


図 5 仮想的な積層構造

Fig. 5 Virtual stacked-layer structure.

2.4 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、1 つのセルが 17 ビットを表現しているので、図 5 に示すように、白黒の既存の二次元コードが 17 層重なっているのと同様である。

以下では個々の仮想的な白黒の二次元コードを層と呼ぶ。

3. 色識別手法

3.1 比較法

色を識別する手法としては、判別法と比較法がある。判別法は入力された画素の RGB 値に基づきあらかじめ定められた色集合から特定の色を判別する手法である。それに対して、比較法は、あらかじめ定められた色集合の色すべてを二次元コードの中の定められた領域に設定しておき、それらの色集合と識別すべき画素色と比較することにより、一番近い色を選択する手法である。

カラー色を用いた二次元コードを紙に印刷する場合には、印刷に用いるインクやトナーによって、元の RGB 値から離れた値になり、それらをスマートフォンで読み取る場合には、用いられる撮像素子の特性によって、入力される RGB 値がさらに変化することが知られている [6]。さら



図 6 パレット色の設定

Fig. 6 Configuration of palette color.

に、印刷された色が経時劣化によって、変化することが想定できる。

そこで、本提案では、これらの影響を回避できる比較法を採用する。比較法（パレット方式）は上記のインクによる発色の差異や経時劣化について、比較対象色（パレット色と呼ぶ）とセル色が同様に差異が発生し、経時劣化などするので、それらの影響を回避可能である。

パレット色を二次元コードの定められた位置に収容する。図 6 に示すように、白および黒グループのパレット色は、それぞれファインダパターンの白部または黒部に配置する。QR コードでは、定められた位置にファインダパターンを有しているので、そこへパレットを配置する。また、これらのパレット色が汚れなどによって正しい色を表現できなくなる可能性があるがあるので、3 つあるファインダパターンのすべてにパレットを設定する。

3.2 識別処理

識別処理は、パレット色 12 色とサブセル色の各 RGB 値を比較する。パレット色の RGB データ C_p を、

$$C_p = (R_i, G_i, B_i) \quad (2)$$

と表現する。

ここで、 i は選択候補であるパレット色 12 色の指標である。 R_i, G_i, B_i は各パレット色の RGB 値であり、0 から 255 の間の値をとる。

同様に、サブセル色の RGB データ C_c は、

$$C_c = (R_c, G_c, B_c) \quad (3)$$

で表現する。 i 番目のパレット色とサブセル色の RGB 値のユークリッド距離 D_i は

$$D_i = \sqrt{(R_c - R_i)^2 + (G_c - G_i)^2 + (B_c - B_i)^2} \quad (4)$$

となる。

D_i が最小値となるパレット色をサブセル色と判定する。

4. 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 [16] を用いる。

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

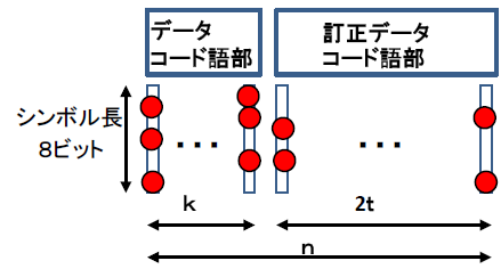


図 7 パターンマスクによる誤り発生

Fig. 7 Error generating by a pattern mask.

n : データコード語総数

k : 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

ある。RS 符号は、ブロック型の誤り訂正符号であり、あらかじ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。したがって、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とらえることができる。

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 [1] を用いて行うことが可能である。

ここでは、確実に復号を不可能とするために、図 7 に示すように、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仮想的二次元コードのセルの値との XOR 演算を行う。

パターンマスクの本来の目的は、データ部のセルの白黒の配置がファインダパターンと同じ 1:1:3:1:1 とならないようにするなど二次元コードの存在と位置を確実に識別する白黒配置を作成することである。これらの目的はセルレベルの処理によって達成されるので、互換部であるセルの中央部のサブセルで構成する仮想的な二次元コードに規定のパターンマスクを適用することにより目的を達成できる。セルの周辺部を構成する 16 個の仮想的な二次元コードはどのような白黒のパターンを有していても、カラーに符号化されるときには中央部のサブセルに従って白グループまたは黒グループの色となり、パターンマスクの目的は達成される。したがって、新規領域の 16 個の仮想的な二次元コードについて、任意のパターンマスクを選択するこ

とができる。

5. 領域分割とその暗号化

5.1 領域分割

2.4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。

秘匿領域は、管理領域とデータ領域に分割される。管理領域はユーザごと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ごと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ごとに 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。

5.2 複数ユーザへのアクセス権割当て

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当ての例を表3に示す。

この例では、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、表3の割

表2 秘匿領域のデータ構成

Table 2 The data structure of a secrecy area.

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
(暗号化領域) データ領域	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	

表3 各ユーザへのアクセス権の割当て

Table 3 An assignment of an access right to each user.

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			○

当て層に示された層が、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 P_n 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 P_1, P_2, P_3, P_4 が生成され、暗号化に用いられる。

一般的に、データ領域数 n 、ユーザ数 m の場合のアクセス権の割当て表は、表4のようにになる。

5.3 ユーザごとのパスワード設定

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 P_1, P_2, P_3 を知る必要がある。しかし、1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、1個のユーザが多値セル型二次元コードを1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1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ためには、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、すべての者が読み取り可能であり、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。

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PW_aを付与され、パターンマスク値(P_1, P_2, P_3)をパスワードPW_aによって暗号化し、暗号化パターンマスクEP_a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EP_a, EP_b, EP_c

表4 一般的なアクセス権の割当て

Table 4 An assignment of a general access right.

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				

表5 パスワードと暗号化パターンマスク

Table 5 A password and the encrypted pattern mask.

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	PW _a	P_1, P_2, P_3	EP _a
ユーザB	PW _b	P_2, P_3	EP _b
ユーザC	PW _c	P_3, P_4	EP _c

を収容する。管理領域に割り当てる層の数は EP_m を収容するに足る層数が割り当てられる。

5.4 安全性の検討

各領域のデータは、複数の仮想的二次元コードに分割されて収容されている。データを収容する仮想的二次元コードは、乱数によるパターンマスクで暗号化されている。乱数によって発生させたパターンマスクは、パスワードによって暗号化されて記録されている。したがって、パスワードを知らなければ、それぞれの領域でパターンマスクを総当たり方式で復号を試みる必要がある。そこで、パターンマスクは必要な安全性によって任意の長さを選択できるので、計算量的安全性を有する。

6. 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 d_0 および秘匿データ領域に収容するデータ $d_1, \dots, d_n$ からなる収容データを $D = (d_0, d_1, \dots, d_n)$ とする。これらのデータを各層に配置したデータ $ld_1, \dots, ld_{16}$ からなる収容データを $LD = (ld_1, \dots, ld_{16})$ 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 $ud_0, ud_1, \dots, ud_{16}$ からなるデータを $UD = (ud_0, ud_1, \dots, ud_{16})$ とする。そして、この白黒符号をカラー化したデータ $cd_1, \dots, cd_8$ からなるデータを $CD = (cd_1, \dots, cd_8)$ とする。

これらの個別のデータ配置を表 6 に示す。

6.1 符号化処理

ステップ 1：データの準備および圧縮

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）ごとに圧縮を行い、データ $D = (d_0, d_1, \dots, d_n)$ 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 d_0 について、通常の白黒二次元コードの生成処理を行い ld_0 および ud_0 を得る。

表 6 データの配置

Table 6 Configuration of a data.

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	d_0	ld_0	
新規領域 (秘匿化領域)	管理領域 (非暗号化領域)	$ld_1, \dots, ld_j$	$cd_1, \dots, cd_8$
(暗号化領域)	データ領域1	d_1	
	データ領域2	d_2	
	$\vdots$	$d_3, \dots, d_{n-1}$	
	データ領域n	d_n	
		$ld_{j+1}, \dots, ld_{16}$	

ステップ 3：管理領域の割り当て

ユーザごとの暗号化パターンマスクおよび層の割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 4：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 層のうち、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 5：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 $P_1, \dots, P_n$ 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 PW_n を用いて暗号化し $EP_a, \dots, EP_m$ を得て、管理領域データにセットする。

ステップ 6：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、 $LD = (ld_1, \dots, ld_{16})$ を得る。その後各層にパターンマスク $P_1, \dots, P_n$ を用いてパターンマスク処理を行い、 $UD = (ud_1, \dots, ud_{16})$ を得る。

ステップ 7：サブセル色の決定

$UD = (ud_1, \dots, ud_{16})$ について、表 1 の符号化テーブルを用いてサブセル色を決定し、最終的な多値セル型二次元コードの各サブセル色 $CD = (cd_1, \dots, cd_8)$ を得る。

6.2 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、セルの中央部およ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 $CD = (cd_1, \dots, cd_8)$ を得る。

ステップ 3：白黒二次元コードに復号

表 1 の符号化テーブルを用いて、サブセルの色コード $CD = (cd_1, \dots, cd_8)$ 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 $UD = (ud_1, \dots, ud_{16})$ を得る。

ステップ 4：既存領域の復号

既存領域の白黒符号 ld_0 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 d_0 を得る。

ステップ 5：新規領域の復号

ステップ 5-1：管理領域の読み取り

新規領域のうち、パターンマスク暗号処理がされていない管理領域から、ユーザ m の暗号化パターンマスク EP_m を読み取り、データ領域の構成を得る。

ステップ 5-2：パターンマスクとデータの復号

ステップ 5-1 で得た暗号化パターンマスク EP_m を、入力されたパスワード PW_m を用いて復号し、割り当てられた層のパターンマスク $P_i, \dots, P_j$ を得る。ここで、

$i, \dots, j$ はユーザ m がアクセスを許可された領域番号である． $P_i, \dots, P_j$ を用いて白黒符号 $UD = (udk, \dots, udl)$ の復号処理を行い $LD = (ldk, \dots, ldl)$ を得る．ここで， $k, \dots, l$ はユーザ m がアクセスを許可された層番号である． $LD = (ldk, \dots, ldl)$ からアクセスが許された収容データ $di, \dots, dj$ を得る．

7. 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．

7.1 商品情報

想定用途の第1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，データ例およびそのアクセス権の付与例を表7に示す．

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．

7.2 偽物検出

想定用途の第2は，偽物検出である．この事例のユーザ例，データ例およびアクセス権の付与例を表8に示す．

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という特性を用いている．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では正規品であることを示すデータを読み取ることができないので，偽物であることが知れる．

表7 商品情報提供の場合のアクセス権割当ての例

Table 7 The example of the access-right assignment in merchandise information offer.

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	○	○	○	

表8 偽物検出の場合のアクセス権割当ての例

Table 8 The example of the access-right assignment in an imitation detection.

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	○	○		

また，ブランド名などの暗号化されたデータは，乱数によるパターンマスクで暗号化されて仮想二次元コードに収容され，符号化テーブルによって色符号化されてカラー二次元コードのサブセルとして印刷されている．上記の乱数によって発生したパターンマスクもパスワードで暗号化されて仮想二次元コードに収容され，同様にカラー二次元コードのサブセルとして印刷されている．これらを規定された方法以外で作成または改変すると，それらはすべて偽造品と判定されるので，偽物検出を無効にすることはできない．

8. 実験結果

5章で説明した符号化処理をパソコン上に，復号処理をスマートフォン上に実装し，多値セル型二次元コードの作成および読み取りの実験を表9に示す条件で行った．作成した多値セル型二次元コードの例を図8に示す．

読み取り実験の結果，データ量が少なく多値セル型二次元コードに収容でき，窓際など明るく，二次元コードの明度分布が一般的な読み取り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み取ることができた．しかし，次の2つの問題点が明らかになった．

(1) データ配置の非効率

データ量が多い場合に，データ量が収容能力以下であるにもかかわらず，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

表9 試験条件

Table 9 Test condition.

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 (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



図8 多値セル型二次元コードの例

Fig. 8 The example of a multiple-value cell two dimensional code.

表 10 読み取り試験結果
Table 10 The result of read test.

二次元コード サイズ(mm)		読み取り率(%)		
コード サイズ	セル サイズ	室内窓際 (明度分布 無し)	室内中央 (明度分布有り)	
			点灯無し	点灯有り
40	1.4	100	5	10
30	1.0	95	10	15

単位で配置する必要がある。

(2) 読み取り性能の不足

多値セル型二次元コードの読み取りを、文献 [17] 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 7 つのサイズについて、その読み取り結果を示した。この読み取り試験結果は、照明があり、かつ二次元コードのセルサイズが比較的大きい場合には、安定して読み取り可能であることを示している。

今回は、照明のない実使用環境で実施した。領域数、データ内容の異なる 2 つの二次元コードを作成し、それぞれ 1 辺を 40 mm と 30 mm とした場合について、3 つの読み取り環境で各 10 回の読み取り試行を行った結果を表 10 に示す。

この結果、スマートフォンの影など二次元コード内に明度分布が発生しない場合には、前記の実験結果とほぼ同じ結果が得られた。一方、天井照明とスマートフォンおよび読み取り対象の二次元コードの位置関係で、スマートフォンの影により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み取り率が低下した。また、スマートフォンの照明を点灯した場合にも、照明が不均一となり、明度分布が発生した。この場合に対応するためには、読み取り時に明度補正機能が必要である。

9. 今後の課題

9.1 ネットワーク管理

本論文での二次元コードへのアクセス制御は、二次元コード内部に記憶させたアクセス制御データ（表 2 の管理領域）に基づき行った。このアクセス制御データを図 9 のように、ネットワークに接続されたサーバに記憶させることで、アクセス制御をダイナミックに行える可能性がある [19]。たとえば、新規のユーザが出現した場合のユーザ追加や既存のユーザのアクセス領域の変更などである。

また、データ領域のデータについても、二次元コードに収容するのは、実際のデータではなく暗号化されたコンテンツ ID とし、実際のデータはコンテンツ ID と対応させてサーバに記憶させれば収容データサイズの限界をなくすことも可能である。

アクセス制御データやコンテンツの変更の鍵の管理などネットワーク化することの諸課題について、今後の検討課題としたい。

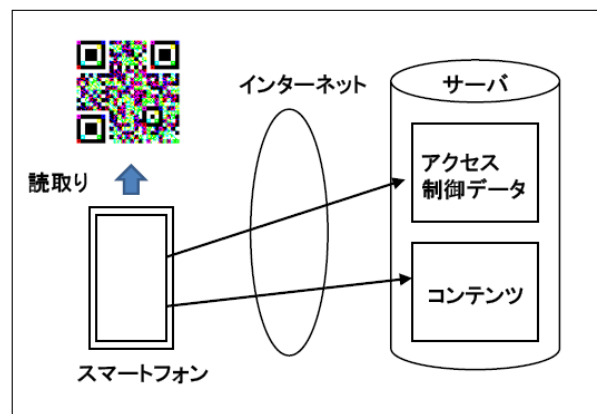


図 9 ネットワーク二次元コード管理システム

Fig. 9 Network two-dimensional code management system.

9.2 誤り訂正

著者らは白色蛍光灯による照明下の実験データ [17] を用いて、誤り訂正の効果を検討した [20]。この場合、二次元コードの照明は均一であり、誤りの主たる原因はサブセルが小さくなると、OS による画像の平均化処理によって、周囲の色がサブセル中心部の画素を混濁させることにあった。このため誤りはほぼ均一に分布していた。この場合、サブセルのサイズがある値以下になると、いっせいに誤りを生じ、多くのデータコード語に誤りが発生し、RS 符号を用いた誤り訂正を無力化していた。そこで、既存の RS 符号を用いた誤り訂正に加えて、拡張グレイ符号などを用いた誤り訂正システムを導入し、実データを用いて効果をシミュレーションした。その結果、RS 符号の誤り訂正レベルが低い場合には、効果が見られた。しかし、拡張グレイ符号ではデータと誤り訂正データはともに 12 ビットずつであり、実効データ密度は 50% となるが、これを超える誤り訂正の効果は見られなかった。

一方、今回の多くの誤りは、照明の不均一に起因しており、誤りは均一に分布していない。そこで、適切な誤り訂正を導入すれば、読み取り率の向上を実現できる可能性がある。照明の不均一に対応する誤り訂正システムの検討も、明度補正とあわせて今後の課題としたい。

10. おわりに

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み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。

読み取り試験によって、その手法が有効であることを確認した。一方、二次元コードの読み取り性能に課題が残る、読み取り性能向上のために、明度補正などの手法の検討が必要であることを示した。

謝辞 誤り訂正についてご指導いただいた広島修道大学の井上徹教授と貴重な示唆をいただいた査読者に感謝いたします。

参考文献

- [1] ISO/IEC 18004:2006: Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification (2006).
- [2] ISO/IEC 16022:2006: Information technology – Automatic identification and data capture techniques – Data Matrix bar code symbology specification (2006).
- [3] Kato, H. et al.: Development of A Novel Finder Pattern for Effective Color 2D Barcode Detection, *Proc. IEEE International Symposium on Parallel and Distributed Processing with Applications, ISPA '08*, Sydney Australia, IEEE Computer Society, pp.1006–1013 (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), pp.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).
- [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 (2012).
- [7] Querini, M.G. and Italiano, F.: Color Classifiers for 2D Color Barcodes, *Proc. 2013 Federated Conference on Computer Science and Information Systems*, pp.611–618 (2013).
- [8] Shimizu, T. et al.: Color Recognition by Extended Color Space Method for 64-color 2-D Barcode, *MVA2011 IAPR Conference on Machine Vision Applications*, pp.259–262 (2011).
- [9] Adams, G. et al.: 2D code sub-coding density limits, *27th International Conference on Digital Printing Technologies and Digital Fabrication*, October 2-6, Minneapolis, Minnesota, USA, pp.696–699 (2011).
- [10] 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, Vol.J94-D, No.12, pp.1971–1974 (2011).
- [11] 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 (2009).
- [12] Vongpradhip, S. and Rungrasungsilp, S.: QR Code Using Invisible Watermarking in Frequency Domain, *9th International Conference on ICT and Knowledge Engineering*, pp.47–52 (2012).
- [13] Hsu, F. et al.: Dual-watermarking by QR-code applications in image processing, *UIC-ATC '12, Proc. 2012 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing*, pp.638–643 (2012).
- [14] 原 昌弘: 二次元コードの生成方法およびその読取装置, 特開 2008-299422.
- [15] 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), 2C3-2 (2013).
- [16] 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), pp.809–816 (2013).
- [17] Teraura, N. and Sakurai, K.: Proposal of Multi-value Cell structure High Density Two-dimensional codes and Evaluation of Readability using Smartphones, *7th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pid1162546-D (2015).
- [18] available from <<https://www.itu.int/rec/R-REC-BT.601/en>>.
- [19] CSS2015 発表時の越前功座長のコメント.
- [20] 寺浦信之, 井上 徹, 櫻井幸一: 高密度二次元コードのブロック誤りとランダム誤りに対応する二重誤り訂正システムの検討, 第 14 回情報科学技術フォーラム (FIT2015), K-045 (2015).
- [21] 寺浦信之, 櫻井幸一: 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, コンピュータセキュリティシンポジウム 2015 (CSS2015), 3C1-1 (2015).



寺浦 信之 (正会員)

1976 年名古屋大学工学部原子核工学科卒業。1979 年同大学大学院工学研究科修士課程修了。同年日本電装(株)入社。2000 年～2009 年まで日本自動認識システム協会(JAISA)RFID 部会部会長。2006 年～2013 年まで日中韓 RFID ラウンドテーブル日本代表。2008 年電子取引推進センター(ECOM)RF タグ技術課題検討委員会委員長。2009 年(株)テララコード研究所設立。2013 年九州大学システム情報科学府社会人博士課程入学。現在,(株)テララコード研究所にてカラー二次元コードおよび耐放射線 RF タグの研究に従事。電子情報通信学会会員。



櫻井 幸一 (正会員)

1988 年九州大学大学院工学研究科応用物理学専攻修士課程修了。同年三菱電機(株)入社。現在,九州大学大学院システム情報科学研究院情報学部門教授。2004 年より九州システム情報技術研究所・第 2 研究室(現,九州先端科学技術研究所・情報セキュリティ研究室)室長兼任。博士(工学)。2000 年情報処理学会坂井特別記念賞,2000 年・2004 年情報処理学会論文賞,2005 年第 1 回 IPA 賞受賞。2012 年第 26 回独創性を拓く先端技術大賞経済産業大臣賞(企業・産・学部門最優秀賞)受賞。日本数学会,応用数理学会,電子情報通信学会,ACM,IEEE,IACR 各会員。