二重符号化 QR シンボルの分割によるしきい値秘密分散とタイムスロット符号化

寺浦　信之[†1]　越前　功[†2]　岩村　惠市[†3]

概要：二重符号化を用いて QR コードを複数のシンボルに分割して秘密分散する手法を検討した．QR コードでは，符号化の基本単位であるセルを黒セルまたは白セルとすることで符号化している．二重符号化は，さらに特性の異なる手段でセルを符号化するものである．例えば，1 値を符号化する場合には，色の違いを利用して黒セル領域を青と赤で符号化する．この二重符号化した QR シンボルを青と赤のセルグループにして，二つのシンボルに分割し，秘密分散を行う．N ビットを符号化することによって，$(2^N, 2^N+1)$しきい値秘密分散を実現可能である．さらに，二重符号化を時間軸で行うことにより，スマホなどでの画面表示で，安全なデータの伝達を可能する．現状の QR コードの読取りとの互換性があれば，順次導入が可能となる．そこで，タイムスロット符号化した分割シンボルと元の QR コードを連続表示し，元の QR コードの読取り実験を行ない，互換性を確認した．

キーワード：QR シンボル，二重符号化，秘密分散，タイムスロット符号化，連続表示，互換性

Threshold Secret Sharing by Dividing Double-encoded QR symbols and Time Slot Encoding

Nobuyuki Teraura[†1]　Isao Echizen[†2]　Keiichi Iwamura[†3]

Abstract: We examined a method of secret sharing by dividing a QR code into multiple symbols using double coding. In the QR code, a cell that is a basic unit of encoding is a black cell or a white cell for encoding. Double coding is a method of coding cells by means having different characteristics. For example, when encoding one value, the black cell area is encoded in blue and red by utilizing the difference in color. This double-encoded QR symbol is divided into blue and red cell groups and secret sharing is performed. $(2^N, 2^N+1)$ threshold secret sharing can be realized by encoding N-bit multi-valued. Furthermore, by performing double encoding on the time axis, it is possible to transmit data safely on a screen display on a smartphone or the like. If it is compatible with the current QR code reading, it can be introduced sequentially. Therefore, the time-slot-encoded divided symbols and the original QR code were continuously displayed, and the original QR code was read out to verify compatibility.

Keywords: QR symbol,　Double encoding,　Secret share,　Compatibility,　Timing slot encoding

1. はじめに

1.1 秘密分散 QR シンボルの提案

現在，QR コード[1]は，スマートフォン（スマホ）を用いた WEB 参照や産業用のデータキャリア用途など様々な用途で利用されている．しかし，QR コードは誰でもが簡単に作成可能であり，誰でもがスマホを用いて読取ることが可能である．一方，秘密情報の受渡しや偽造防止などセキュリティが必要な用途も存在している．

QR コードを用いた秘密情報の受渡しの手段として，種々の手段が提案されているが，その一つとして秘密分散を用いる提案がなされている．

1.2 既存の研究

QR コードを複数のシンボルに分割して，秘密分散を行う手法として，視覚復号型手法が提案されている．この手法[2]は秘密にしたい画像を複数の画像に分散処理し，1 枚の画像からは元の画像が判らないが，あるしきい値以上の画像を重ね合わせることで画像を復元することができる分散方式である．この手法を QR コードに適用した提案[3][4]がなされている．また，二つの QR コードのデータ収容部の未利用部分に秘密にするデータと分割した他の QR コードのデータ部に収容したデータとを XOR 処理して収容する手法[5][6]が提案されている．そして，QR コードの誤り訂正機能を用いて，単独では訂正できず復号できないが，

†1 テララコード研究所
Terrara Code Research Institute
†2 情報学研究所
National Institute of Informatics
†3 東京理科大学
Tokyo University of Science

© 2020 Information Processing Society of Japan

2 枚の画像を OR 処理すると，誤りが訂正可能になり復号可能とする手法[7][8]が提案されている．

1.3 本論文の提案手法

本論文では，二重符号化手法を用いてシェアシンボル画像を作成する手法を提案する．そして，二重符号化の方法としてタイムスロット法を併せて述べる．

なお，本論文では ISO/IEC で規定する仕様[1]に合致するシンボルを QR コードと呼び, QR コードと互換性があり，二重符号化により機能が付加されたシンボルを QR シンボルと呼ぶ．また，QR シンボルを分割し，QR コードと同じ固定領域を有するシンボルを分割（QR）シンボルと呼ぶ．

2. 二重符号化による QR シンボルの分割

2.1 二重符号化

QR コードの二重符号化とは，黒セル領域または白セル領域について，識別可能な特性の異なる手段でさらに符号化する手法である[9]．例えば，赤外線特性の異なる黒インク（K 黒インクと CMY 黒インク）を用いて符号化する [10].

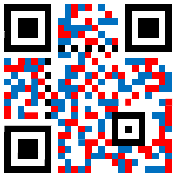
2.2 黒セル領域または白セル領域の 1 値二重符号化

色の違いを利用して，識別可能な 2 色を用いて二重符号化を行うことが可能である．二重符号化の対象とする QR コードを図 1 に示す．最初に，この QR コードの黒セル領域を二重符号化する場合について述べる．二重符号化は，表 1 に示す符号化テーブルに従って行う．二重符号化する値が 1 の場合には当該セルを青とし，0 の場合には赤とする．このようにして，二重符号化を行った黒セル領域の二重符号化 QR シンボルを図 2 の左図に示す. また, 同様に, 図 1 の QR コードの白セル領域を表 1 の符号化テーブルを用いて符号化した白セル領域の二重符号化 QR シンボルを図 2 の右図に示す.

表 1　符号化テーブル（1 値）

色		画像番号	符号化データ
黒	白		
青	桃	1	1
赤	黄	2	0

図 1　二重符号化対象 QR コード



黒セル領域の二重符号化

白セル領域の二重符号化

図 2　1 値二重符号化 QR シンボル

2.3 黒白セル両領域の 1 値二重符号化

前節では，黒セル領域または白セル領域のどちらかを 2 色を用いて二重符号化を行った．一方，黒セル領域と白セル領域の両方を二重符号化することも可能である．図 1 に示す QR コードについて，表 1 の符号化テーブルに従って二重符号化を行った黒白セル両領域の二重符号化 QR シンボルを図 3 に示す.

図 3　黒白セル両領域の 1 値二重符号化 QR シンボル

2.4 二重符号化シンボルのデータ構成

QR コードは，表 2 の左表に示すように，公開データ領域を 1 領域有するシンボルである．それに対して，二重符号化 QR シンボルでは，表 2 の右表に示すように，公開データ領域に加えて，秘匿データ領域とすることが可能な第二のデータ領域を有するシンボルである.

表 2　シンボルのデータ構成

QR コードのデータ構成

領域番号	データ領域
1	公開データ領域
	ー

二重符号化 QR シンボルのデータ構成

領域番号	データ領域
1	公開データ領域
2	秘匿データ領域

次章以降で，秘密分散について述べるが，秘密分散の対象となるデータ領域は，秘密データ領域である．公開データ領域を秘密分散の対象とすることも可能である．それらについては，次章以降で述べる.

3. 二重符号化シンボルの分割

この章では，前章で示した色を用いて二重符号化した QR シンボルを色別に分割することを述べる.

3.1 QR コードのシンボル構成

QR コードのバージョン 2（v2）の場合のシンボル構成を図 4 に示す[1].

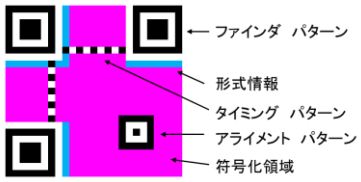


図 4　QR コードのシンボル構成（V2 の場合）

QR コードは，大別して二つの領域に分類することが可能なセル領域から構成されている．第一のセル領域は，収

容するデータに依存せず，常に同じ位置に同じ配色がなされる図 5 に示す固定領域である．固定領域には，シンボルの存在を発見するためのファインダパターン，セルの配置を示すタイミングパターン，シンボルの歪を補正するためのアライメントパターンがある．これらは，バージョン毎に定められた位置に配色されている．

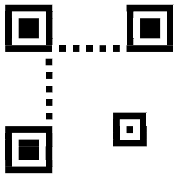


図 5　固定領域

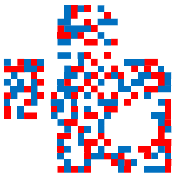


図 6　変動領域（図 2 左図）

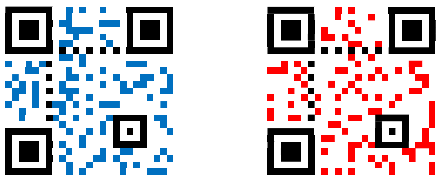
第 2 のセル領域は，データの符号化領域及び形式情報などのシンボル記述領域であり，収容するデータなどに伴って配色パターンが異なる図 6 に示す変動領域である．

3.2　シンボルの分割

シンボルを分割するにあたって，前記の固定領域は分割後のシンボルにも配置する．固定領域の各パターンは，セルの位置を特定するために必要であり，復号時に不可欠である．そして，固定領域に加えて，変動領域の色グループ毎にセルを分割し，配置する．

①黒セル領域の二重符号化シンボルの分割

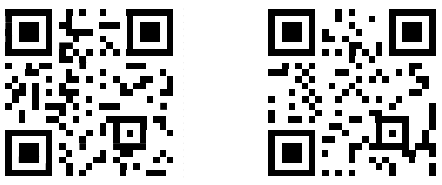
黒セル領域を二重符号化した図 2（左図）に示すシンボルについて，図 5 に示す固定領域と白セル領域及び図 6 に示す変動領域の色グループ毎に 2 分割したセルを合体して生成したシンボルを図 7 に示す．



固定領域と青部　　固定領域と赤部

図 7　色別に分割したシンボル（黒セル領域）

図 7 に示した分割シンボルについて，青セル及び赤セルを黒セル化したシンボルを図 8 に示す．

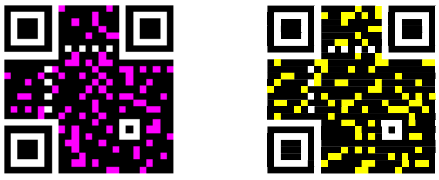


分割シンボル 1　　分割シンボル 2

図 8　黒セル領域の二重符号化による(2, 3)秘密分散シンボル

②白セル領域の二重符号化シンボルの分割

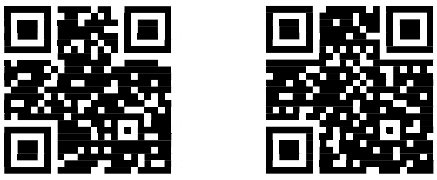
次に，図 1 の QR コードの白セル部を二重符号化した図 2（右図）に示す QR シンボルについて，固定領域と黒セル領域及び図 7 に示す変動領域の色グループ毎に 2 分割したセルを合体して生成したシンボルを図 9 に示す．



固定領域と桃部　　固定領域と黄部

図 9　色別に分割したシンボル（白セル領域）

図 9 に示した分割シンボルについて，桃セル及び黄セルを白セル化したシンボルを図 10 に示す．

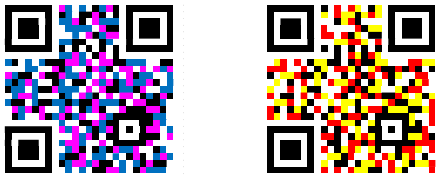


分割シンボル 3　　分割シンボル 4

図 10　白セル領域の二重符号化による(2, 3)秘密分散シンボル

③黒セルと白セルの両領域の二重符号化シンボルの分割

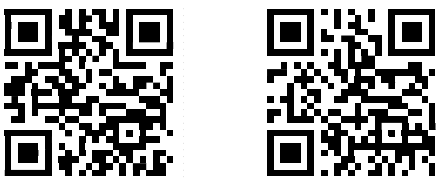
次に，黒セル領域と白セル領域の両方を二重符号化した図 3 に示す QR シンボルについて，固定領域と変動領域の同じ符号化値とする色毎に 2 分割したセルを合体して生成したシンボルを図 11 に示す．



固定領域と青桃部　　固定領域と赤黄部

図 11　色別に分割したシンボル（黒白セル領域）

図 11 について，黒セル領域を符号化した青セルと赤セルを黒セル化し，白セル領域を符号化した桃セルと黄セルを白セル化したシンボルを図 12 に示す．



分割シンボル 5　　分割シンボル 6

図 12　黒白セル領域の二重符号化による(2, 3)秘密分散シンボル

4. 多値二重符号化とシンボルの分割

第 3 章③では，黒セル領域と白セル領域の両領域を 1 ビットの二重符号化する場合を述べた．ここでは，セルを 2 ビット及び N ビット（多ビット）の二重符号化する場合について述べる．

4.1 黒白セル両領域の 2 値二重符号化

セルを 1 ビットで符号化するためには 2 色必要である．また，2 ビットを符号化するためには，4 色が必要である．そして，黒セル領域と白セル領域でそれぞれ異なる色を用いると，総計 8 色が必要である．この 8 色についての符号化テーブルの例を表 3 に示す．

二重符号化は，表 3 に示す符号化テーブルに従って行う．二重符号化処理を行う前に，収容するデータを 2 ビット毎に分割する．分割して二重符号化する値が 11 の場合には黒部の当該セルは青とし，白部では桃とする．00 の場合には，それぞれ赤及び黄とする．

図 1 に示す QR コードについて，表 3 の符号化テーブルに従って二重符号化を行った黒白セル両領域の 2 値二重符号化 QR シンボルを図 13 に示す．

表 3　符号化テーブル（2 値の場合）

色		画像番号	符号化データ
黒	白		
青	桃	1	11
紫	金	2	10
茜	緑	3	01
赤	黄	4	00

図 13　黒白セル両領域の
2 値二重符号化 QR シンボル

図 13 に示す QR シンボルについて，固定領域と変動領域の同じ符号化値とする色毎に 4 分割したセルを合体して生成した 4 個のシンボルを図 14 に示す．

固定領域と青桃部

固定領域と紫金部

固定領域と茜緑部

固定領域と赤黄部

図 14　色別に分割したシンボル（2 値黒白セル領域）

図 14 について，黒セル領域を符号化した青紫茜赤セルを黒セル化し，白セル領域を符号化した桃金緑黄セルを白セル化したシンボルを図 15 に示す．

分割シンボル 7

分割シンボル 8

分割シンボル 9

分割シンボル 10

図 15　2 値二重符号化による(4, 5)秘密分散シンボル

4.2 黒白セル両領域の N 値二重符号化

前節では，セルを 2 ビット符号化する場合について述べた．この節では，セルを N ビット符号化することを検討する．この場合の符号化テーブルを表 4 に示す．

表 4　符号化テーブル（N 値の場合）

色		画像番号	符号化データ
黒	白		
B1	W1	1	111..11
B2	W2	2	111..10
..	..	..	....
$B2^N$-1	$W2^N$-1	2^N-1	000..01
$B2^N$	$W2^N$	2^N	000..00

この場合には，2^N 個の画像に分割される．例えば，N=3 の場合には 8 個のシンボルに，N=4 の場合には 16 個のシンボルに分割される．

5. 秘匿分散

5.1 しきい値秘密分散

分割して生成したシンボルは，単独では復号することができない．分割シンボルを必要数読取ることによってはじめて復号することができるしきい値秘密分散となっている．

黒セル領域のみ，白セル領域のみについての 1 ビット二重符号化では，分割シンボルを 2 個または元の QR コードと分割シンボルのいずれか 1 個から復号可能であるので(2, 3) 秘密分散と言える．また，黒セル領域及び白セル領域の

両領域についての 1 ビット二重符号化では，元の QR コードと分割シンボルのいずれか 1 個から復号可能であるので同じく(2, 3) 秘密分散と言える．同様に，N ビットの二重符号化では，$(2^N, 2^N+1)$ 秘密分散となる．

5.2 復号の可能性検証

次に，(k,n) しきい値秘密分散において，1 個及び(k-1) 個では，復号不可であることを述べる．また，二重符号化を行う基礎となる QR コードを親シンボル，二重符号化して分割したシンボルを子シンボルと呼ぶ．

①1 個の場合

(1)親シンボル

親シンボルは二重符号化される前のシンボルであり，二重符号化に関するデータを保持していない．そこで，親シンボルから二重符号化データを復号することはできない．

(2)子シンボル

N ビットの符号化をした場合には，2^N 個の子シンボルが生成される．1 個の子シンボルの二重符号化データのデータ欠損率 R_N は，

$$R_N = (2^N - 1) / 2^N$$

である．欠損したセルに 0 または 1 を充てた場合，平均的に半数が誤る．そこで，8 ビットのデータコード語では，データコード語当たりの誤りビット数 E_N は

$$E_N = R_N \times 8 / 2$$

となる．E_N を N について計算した結果を表 5 に示す．

最小値となる N=1 の場合でも，E_N は 2 であり，平均的にすべてのデータコード語に誤りが発生し，RS 符号の訂正限界を大きく超えている．そこで，1 個の子シンボルからの復号は不可能である．

② (k-1) 個の場合

(k-1) 個の子シンボルが集まった場合のデータ欠損率 R_N は，子シンボルが 2 個欠損しているので，

$$R_N = 2 / 2^N$$

である．そこで，上記と同様にして，誤りビット数 E_N は

$$E_N = R_N \times 8 / 2$$

となる．E_N を N について計算した結果を表 5 に示す．

QR コードの誤り訂正レベルは 4 種類設定されており，H レベルは最大の訂正率を有し 30%程度であり，L レベルは最低の訂正率であり 5%程度である．さて，表 5 において，N=5 の場合には，平均的に 25%のデータコード語で誤りが発生する．そこで，誤り訂正レベルが H レベルの場合には，多くの場合に復号可能となる．また，N=7 の場合には，平均的に 6.3%のデータコード語に誤りが発生するので，誤り訂正レベルが L レベルの場合でも訂正可能な場合が発生すると考えられる．

そこで，訂正レベルが H レベルの場合には N=4，訂正レベルが L レベルの場合には N=6 まで(k,n)しきい値秘密分散が成立すると言える．

表 5　データコード語中の平均誤りビット数

N	提示シンボル数	
	1個	(2^N-2)個
1	2	-
2	3	2
3	3.5	1
4	3.75	0.5
5	3.88	0.25
6	3.94	0.125
7	3.97	0.063
8	3.98	0.031
N	$(2^N-1)/2^N*4$	$2/2^N*4$

5.3 秘密分散のデータ量

符号化ビット数 N と符号化対象領域に対する分割シンボル数及び収容データ量を表 6 に示す．ここで，秘匿部は二重符号化部であり，その収容データ量は公開データ部の収容データ量を 1 とした場合のおおよその倍数である．二重符号化は黒セル及び白セルを対象に行い，その数は収容する公開データに依存するので，変動する．しかし，黒セル数と白セル数はマスク処理により調整され概ね等しい．

分割シンボル数は符号化ビット数 N について 2^N 個となるが，その収容データ量は N 倍である．これは，図 14 に示すように，分割シンボル 2^N 個の中で 1 個のみがデータを保持し，その他の 2^N-1 個は固定色となり，当該セルではデータを保持しないからである．

表 6　分割シンボル数，秘密分散，収容データ量

二重符号化対象		分割シンボル数	秘密分散	データ量	
符号化ビット数	対象セル領域			公開部	秘匿部
1	黒セル	2	(2,3)	1	0.5
	白セル	2	(2,3)	1	0.5
	黒白セル	2	(2,3)	1	1
2	黒白セル	4	(4,5)	1	2
3	黒白セル	8	(8,9)	1	3
N	黒白セル	2^N	$(2^N, 2^N+1)$	1	N

6. 処理アルゴリズム

6.1 データ構成

秘密分散の基礎となる QR コードとその二重符号化シンボル及びその分散シンボルのデータの構成を表 7 に示す．ここで，d0 は公開データ部に収容する公開データであり，d1 は二重符号化データである．書式化データ fd0, fd1 は公開データ d0 及び二重符号化する秘密データ d1 を定められた書式に従って，データ種別毎にデータ圧縮などをした書式化データである．

u0 は，fd0 を基に RS 符号で作成したデータコード語であり，データ部データコード語 u0,d と訂正部データコード語 u0,e から成る．同様に，u1 は fd1 を基に生成したデータコード語であり，データ部 u1,d，訂正部 u1,e から成る．

pu0 は u0 に対してマスク処理[1]を行った後のデータパターンである．u1.B, u1.W はデータコード語 u1,d , u1,e を黒セル領域及び白セル領域に収容するために分割したデータである．二重符号化処理は u1.B , u1.W に対して行う．pu1,i は i 番目の分割シンボルに分配されたデータパターンである．

表 7　データ構成

	公開データ部		二重符号化部		分散シンボル
	データ部	訂正部	データ部	訂正部	
ユーザデータ	d0		d1		
書式化データ	fd0		fd1		
収容データコード語	u0		u1		
	u0,d	u0,e	u1,d	u1,e	
			u1.B , u1.W		
マスク処理後収容データパターン	pu0				pu1,i
	pu0,0	pu0,1			

6.2 秘密分散処理

ステップ 1　データの準備

公開データ部, 二重符号化部に収容する公開データ d0 及び二重符号化データ d1 を準備する．

ステップ 2　公開データ部の符号化

公開データ部データ d0 を, セルの黒と白で符号化する．

①書式化

d0 についてデータ圧縮などを行い書式化し，書式化データ fd0 を得る．

②RS 符号化

fd0 から公開データ部にセットするデータコード語 u0 を作成する．データ部データコード語 u0,d に対して，RS 符号に基づいて誤り訂正部データコード語 u0,e を作成する．

③マスク処理

予め設定された 8 種類のマスクパターンについて演算を行い, 選択されたマスクパターンによるマスク処理を行い, pu0 を得る．

④公開データ部のシンボル生成

pu0 を収容するシンボルを生成する．このステップ 2 の処理は，QR コードのシンボルの生成処理と同じである．

ステップ 3　二重符号化部への収容データの生成

二重符号化部の符号化では，データ配置の方法は種々の方式が可能である．ここでは，黒セル領域と白セル領域を単一のデータ領域とする．また, データ圧縮等の書式は QR コードと同じとする．

①書式化

ステップ 2 と同様に，d1 から fd1 を作成する．

② RS 符号化

fd1 からデータコード語 u1 を作成する．データ部データコード語 u1.d に対して，RS 符号に基づいて誤り訂正部データコード語 u1.e を作成する．u1 を分割して，u1.B, u1.W を生成する．

ステップ 4　黒セル領域の二重符号化処理

①黒セルの位置検索

ステップ 2 で作成した QR コードにおいて，予め設定した経路でセル色が黒か白かを判定し，黒セルを選定して黒ポインタ B(Xn, Yn)を作成する．このとき，データコード語部のみを検索対象とする．ここで，Xn, Yn は QR コードの左上部を原点とする n 番目のセルの位置を示す．

②仮想色の配置

データコード語を黒セルポインタ B(Xn, Yn)に基づき, 仮想色 B1 から $B2^N$ を対象セルに配置する．

二重符号化データ u1.B を N ビットずつに分割し，当該 N ビットについて表 4 の符号化テーブルに従って対応する仮想色を選択して配置し符号化する．例えば，N ビットのデータが 111..10 の場合には，B2 色を配置する．

ステップ 6　白セル領域の二重符号化処理

黒セル領域の処理と同様に，白セル領域について白セルポインタ W(Xn, Yn)を作成する．u1.W を表 4 の符号化テーブルに従って対応する仮想色を配置し符号化する．

ステップ 5 とステップ 6 の処理によって作成されるシンボルは，N=2 の場合の図 14 に示す QR シンボルである．

ステップ 7　二重符号化シンボルの分割処理

次に，ステップ 5，ステップ 6 で作成した二重符号化シンボルを 2^N 個のシンボルに分割する．

i 番目のシンボル画像では，初めに二重符号化シンボルの固定領域を継承する．次に，表 4 の符号化テーブルの画像番号 i に対応する色 Bi，Wi の色を探索し，当該色であるセルの位置に黒または白を設定する．親シンボルの黒セル領域では，黒に設定する．Bi 色以外のセルでは白とする．また同様に，親シンボルの白セル領域では白セルとし，Bi 色以外のセルでは黒とする．

以上の処理を i=1 から $i=2^N$ まで行い，分割シンボルを 2^N 個得る．これにより，秘密分散を行う分割シンボルの生成処理を完了する．

ステップ 7 の処理で作成されるシンボルは，N=2 の場合の図 15 に示す分割シンボルである．

なお，分割シンボル画像 i の黒セル数は，親シンボルの黒セル領域では，$1/2^N$，白セルは$(1-1/2^N)$ の比率となる．そして，親シンボルの白セル領域では，白セルは $1/2^N$，黒セルは$(1-1/2^N)$ の比率となる．そこで，分割シンボル i の 黒セルと白セルの比率はほぼ 1 対 1 が維持される．

6.3 秘密復号処理

分割して生成された子シンボルは 2^N 個存在する．この中から，親シンボルと子シンボルが(2^N-1) 個提示された場合の秘密復号処理について述べる．

ステップ 1　シンボル画像撮影

親シンボルと子シンボルを(2^N-1) 個を撮像する．得られ

た画像データからファインダパターンを用いてシンボルの存在を検出し，親シンボルと子シンボルの画像を抽出する．

ステップ 2　親シンボルの復号処理

①セル色の判定

抽出した画像を既存の QR コードとして識別し，サンプリングデータ pu0’を得る．そして，マスク解除処理を行い，u0’を得る．

②RS 符号の復号

u0’を基に，RS 符号の誤り訂正処理を行い，fd0 を経て，d0 を得る．このステップ 2 の①②処理は，QR コードの復号処理と同じである．

③セルポインタの作成

RS 符号の誤り訂正処理によって得た正しいデータコード語 u0 を基にシンボルデータ pu0 を得る．

pu0 について，二重符号化処理時と同様に，各セルが黒セルか白セルかを判定し，黒セルポインタ B(Xn, Yn)及び白セルポインタ W(Xn, Yn)を作成する．

ステップ 3　子シンボルの復号

子シンボル i について，親シンボルと同様に，固定領域のパターンを用いて，各セルの位置を特定し，黒セルまたは白セルの判定を行い，pu1,i を作成する．

子シンボル i について，i=1 から i=2^N-1 まで処理を行う．

ステップ 4　復元処理

子シンボルは，2^N-1 個が提示されており，1 個が提示されていない．二重符号化の復号にはすべての子シンボルが必要である．そこで，親シンボルと提示された子シンボル 2^N-1 個から未提示子シンボルを復元する．

①黒セル領域の復元処理

黒セルポインタ B(Xn, Yn)に基づき，当該位置のセルについて，黒セルである子シンボルを pu1,i から探索する．黒セルが存在していれば，未提示子シンボルの当該セルは白セルであり，存在しなければ黒セルと判定する．全ての黒セル領域について上記処理を行い，未提示子シンボルの pu1,i を復元する．

②白セル領域の復元処理

上記の黒セル領域と同様に，白セルポインタ B(Xn, Yn)に基づき，当該位置のセルについて白セルである子シンボルを pu1,i から探索し，未提示子シンボルの pu1,i を復元する．

ステップ 5　黒セル領域の復号処理

親シンボルの黒セルポインタ B(Xn, Yn)に基づき，当該位置での黒セルである子シンボル i を pu1,i から検索し，子シンボル i を特定する．特定した子シンボルの画像番号 i から表 4 の符号化テーブルに従って，対応する符号化値を決定し，N ビットのデータを復号する．この処理を B(Xn, Yn)で示されるすべてのセルに対して実施することにより，u1,B を得る．

ステップ 6　白セル領域の復号処理

ステップ 5 と同様にして，親シンボルの白セルポインタ W(Xn, Yn)を用いて，親シンボルが白セル領域であるセルについて順に復号し，u1,W を得る．

ステップ 7　二重符号化データの復号

親シンボルの黒セル領域と白セル領域にそれぞれ符号化されていたデータ u1,B と u1,W からデータコード語 u1’を再構成する．u1’に対して RS 符号の誤り訂正処理を行い，正しい u1 を得る．u1 から書式化データ fd1 を経て，二重符号化データ d1 を得る．

7.　時分割表示

7.1　タイムスロット符号化

前章までは，セルの二重符号化において，符号化データに対応する『色』を設定し，当該色を媒介にして，セルに同じ値が符号化されているセルを抽出して，分割シンボルを構成していた．

このシンボルを時間的に連続表示する場合を考える．この場合には，図 16 に示すように，表示順に符号化することが可能である．表 8 に示す符号化テーブル（タイムスロット）に従い，表示順に符号化する値を対応させれば，タイムスロット二重符号化した分割シンボルは図 15 に示した分割シンボルと同じシンボルとなる．

表 8　符号化テーブル（タイムスロット）

タイムスロット番号	符号化データ
1	11
2	10
3	01
4	00

図 16　タイムスロット符号化

7.2　互換性の効果と成立理由

現在，QR コードをスマホに表示し，それを読取ることで決済などの処理が行われている．これに電子署名データをタイムスロット二重符号化して連続表示する場合を想定する．表示するシンボルには基礎となる QR コード（親シンボル）が含まれている．既存の読取り装置で親シンボルを読取ることができれば，互換性を実現できる．

既存の読取り装置で連続表示シンボルを読む場合には，電子署名部分を読取れないため，認証は行えないが従前の処理は可能である．一方，連続表示対応の読取りソフトウェアを用いれば，電子署名を用いた認証が可能となる．このような互換性があれば，既存の QR コードの単一表示方式と連続表示方式の共存が可能であり，逐次に連続表示の使用を拡大することが可能となる．

既存の読取り装置が QR コード（親シンボル）を選別し

て読取り可能であるのは，表示される他のシンボル（子シンボル）が単独では復号不可であるからである．読取りソフトウェアは，子シンボルを撮像した場合には復号できないので，再度読取り処理を行う．

7.3 読取り予備試験

互換性の実現可能性を確認するために読取り予備試験を行った．読取り試験は，親シンボル単独表示と 2 値符号化した図 16 に示したシンボルを含む連続表示（2 秒）画像について行った．読取りは，画像の表示を 30FPS の条件下で，1F(フレーム)のみの場合と 2F，3F 連続表示の場合について各 10 回実施した．読取り試験の結果を表 9 に示す．読取りに用いたスマホは，SONY 製エクスペリア(SO-03G)であり，読取りソフトウェアは表中に記載のとおりである．

単一表示では，1F(33ms)表示場合には読取れない場合が全ソフトウェアで発生している．2F(66ms)表示では，2 社のソフトウェアで 100%読取りが可能であった．

連続表示では，1F(33ms)毎の繰り返し表示では 1 社で，2F(66ms)毎の繰り返し表示では 2 社で 100%読取りが可能であった．

表 9　単一表示及び連続表示時の読取り率

表示方法	単一表示			連続表示（2秒間）		
表示フレーム数	1F (33ms)	2F (67ms)	3F (100ms)	1F	2F	3F
デンソー	80%	100%	100%	100%	100%	100%
NTTドコモ	60%	100%	100%	80%	100%	100%
COGNEX	70%	60%	80%	60%	90%	90%

8. 応用システム

8.1 秘匿分散としての応用

基礎となる QR コードと分割シンボル，すなわち親シンボルと 1 個の子シンボルで構成する(2, 3)秘密分散では，親シンボルを共通鍵とし，子シンボルの受け渡しによって，二重符号化データを安全に伝達可能となる．また，親シンボルは，QR コードの公開データ部のデータで決定されるので，公開データ部のデータが共通鍵となり，親シンボルの受け渡しではなく，公開データ部のデータの受け渡しで足りる．

8.2 時分割表示としての応用

スマホに QR コードを表示して，読取り端末で読取り，処理を行わせるシステムが多く出現している．その代表的なシステムがスマホ決済である．この他にも，会員証として会員番号を表示するシステムもある．電子会員証である．

しかし，スマホに表示された QR コードが撮影され，悪用される可能性がある．そこで，タイムスロット符号化による連続表示をすることによって，撮影リスクを低減する．

①電子署名の伝達

上記のように，スマホ決済で，QR コードが用いられている．情報伝達は公開データ部のデータの受け渡しによってなされている．そのデータの信頼性は保証されていない．そこで，公開データ部データに対する電子署名を作成し，同時に伝達すれば，データの改ざんの有無を検査可能となり，また QR シンボルの作成者が特定され，より安全にデータ伝達が可能になる．この方式は，通常の電気通信で行われる PKI の方式と同じ方式である．

②秘密データの伝達

公開データ部には知られても構わないデータを記憶し，二重符号化部には秘匿するデータを記憶する．例えば，氏名を公開部に記憶し，口座番号とパスワードを二重符号化部に記憶して受け渡す．

9. おわりに

本論文では，QR コードを二重符号化手法を用いて符号化したシンボルを複数のシンボルに分割する秘密分散法を提案した．これにより，$(2^N\text{-}1, 2^N)$ しきい値秘密分散が可能であることを示した．また，これらをタイムスロット符号化することにより，スマホなどでより安全にデータを受け渡すことが可能になる．

参考文献

[1] ISO/IEC 18004:2015 Information technology -- Automatic identification and data capture techniques -- QR Code bar code symbology specification.

[2] Naor M., Shamir A. ,Visual cryptography. In: De Santis A. (eds) Advances in Cryptology — EUROCRYPT'94. EUROCRYPT 1994. Lecture Notes in Computer Science, vol 950. 1995.

[3] 大川直也，栃窪孝也，(2,3)しきい値拡張視覚復号秘密分散法の QR コードへの適用，信学技法，ISEC2019-98(2020-03),P.79-86,2020.

[4] Xiaohe Cao, Liuping Feng, Peng Cao, Jianhua Hu, Secure QR Code Scheme Based on Visual Cryptography, AISR, Vol,133, PP.433-436, 2016.

[5] 倉本雅樹，河野和宏，伊藤義道，馬場口昇，秘密分散機能を有する QR コードの生成法，信学技法，EMM2014-92(2015-03),P.91-96,2015.

[6] Bin You, Zhengxin Fu ,Sijia Liu, A Novel Three-Layer QR Code Based on Secret Sharing Scheme and Liner Code. Security and Communication Networks. 1-13. 10.1155/2019/7937816.2019

[7] 本庄俊太郎，古賀弘樹，2 枚の二次元コードを用いた秘密分散法の一実現法，電子情報通信学会論文誌 A,Vol.J98-A No.2,PP.221-231,2015

[8] Chow YW, Susilo W, Yang G, Phillips JG, Pranata I, Barmawi AM, Exploiting the error correction mechanism in qr codes for secret sharing. Lecture Notes in Computer Science, Springer 9722:409–425,2016.

[9] 寺浦 信之，岩村 惠市，越前 功，櫻井 幸一,二重符号化二次元コードのパターンマスク秘匿化への RS 符号を用いた誤り訂正の影響検討，信学技報，117(40), EMM2017－11 (2017－05), p.67-72, 2017.

[10] 寺浦 信之，越前 功,岩村 惠市，菱形サブセルを用いた公開領域と秘匿領域の両方を対象とした電子署名を有する QR シンボルの検討,SCIS2020,PP.1-8, 2020