4D-01

真贋判定のためのカラー二次元コードにおける脆弱性に対するシャッフル方法の改良

藤田　悠†　　伊藤　祥一†　　藤澤　義範†
長野工業高等専門学校†

1. はじめに

模倣品や海賊版の流通が世界的に問題になっている．模倣品の製造技術が向上しており，模倣品を判定することは難しい．そこで，真贋を判断するための手法が必要である．

その手法として，品物そのものを見て判断する方法と，マーカを用いた方法がある．前者については，素材や製造過程の特徴などから判断するため，真贋を直接判断可能ではあるが，目利きが必要である．後者については，ID が含まれたマーカなどを品物に付与し，そのマーカから判別する．マーカを含めて複製された場合でも，重複するマーカが存在する異常状態を検出することで，疑いを検出できる．

我々は，目利きが不要な，マーカを用いる方法を取ることとした．しかし，そのマーカが印字されていることをわかりにくくするために，カラーステルスインクを用いる．そのためのカラー二次元コードを検討した[1]．

そのコードは QR コードをカラーマスクパターンでカラー化して生成するので，QR コードの機能パターンが脆弱性になりうる．その機能パターンを隠ぺいするために，QR コードの行や列を交換する方法でシャッフルした[2]．

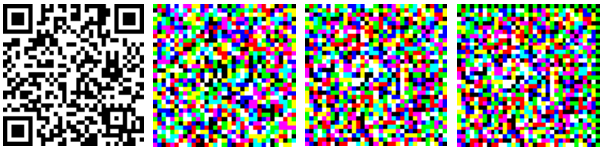
本稿では，従来提案したシャッフル方法では推測が容易である可能性について，改良した手法を提案する．

2. カラー二次元コード

我々は，真贋を判定するためのマーカが記載されていることをわかりにくくするために，ステルスカラーインクでプリントすることを想定した，GK コードを考案した．

2.1 GK コードの生成

図1にコードの生成段階を示す．GK コードは，ID などの情報を AES にて暗号化したデータで生成した QR コードを作成する（**図1**(1)）．その QR コードと，QR コードのセル数に対応するカラーマスクパターン（**図 1**(2)）と排他的論理和をとることで，カラー二次元パターンになる（**図 1**(3)）．このカラー二次元パターンの上側と右側に黒色と緑色からなるタイミングパターンを配置する（**図 1**(4)）．このカラー二次元コードを，特徴的な緑（Green）と黒(Black)のタイミングパターンから，GK コードと呼んでいる．GK コードから，格納した情報を復元することの困難さは，埋め込んだ情報を暗号化する AES の鍵と，QR コードをカラー化するときに用いるマスクパターンに依るものとなる．



(1)　(2)　(3)　(4)

図 1　カラー二次元コードの生成

2.2 GK コードの脆弱性

不正な復号の困難さのうち，カラーコード化する段階を考える．QR コードは，読み取るときの目印となる部分や，タイミングを取るために設けられている部分からなる機能パターンを持つ．したがって，QR コードとカラーマスクパターンで排他的論理和にて変換していることから，機能パターンの部分に相当するマスクパターンの一部分は明らかである．

マスクパターンの一部から，全体を即時に推測できるものではないが，この明らかな部分を元に，全体のマスクパターンを推測することが容易になる脆弱性がある可能性が考えられた．

2.3 従来の脆弱性対応

QR コードをシャッフルしてからカラー化することで，GK コードからマスクパターンを推測することが難しくなると考えた．

従来の提案では，任意の行と行，列と列の入れ替えを繰り返すシャッフル方法を提案した．入れ替えた行番号対応と列番号対応およびその順番が新たな，不正な復号の困難さとなる．

しかし，単純に入れ替える方法では，その入れ替え内容が容易に推測できる可能性があると考えられた．そこで，剰余類による写像を代替のシャッフル方法として適用する．

Improvement to Shuffle Method of Vulnerability to Two-dimensional Color Barcode for Imitation Detection
Yutaka FUJITA†, Shoichi ITO†, Yoshinori FUJISAWA†,
†National Institute of Technology, Nagano College

3. 脆弱性対策のシャッフルの再検討

離散対数問題による剰余類にて白・黒の位置を変換するシャッフル方法を適用する．

3.1 シャッフルアルゴリズム

離散対数問題で変換するには，任意の原始根を用いる必要がある．

素数 p と定数 a が与えられたとき，a^M を素数で割ったときの剰余を y とする（式(1)）．素数 p と定数 a が既知である状態で，与えられた y に対応する M を計算で導出することは難しい．

$$y = a^M \bmod p \qquad (1)$$

定数 a が素数 p を法とする原始根のとき，任意の M に対する y は重複しない．すなわち，p 未満の任意の整数の集合である M と y は式(1)の写像において全単射である．

この性質を用いて，M に変換元の位置番号を入力し，導出された値 y を変換後の位置番号とする．変換後の値から，変換前の値を推測することが難しいことから，不正な方法でシャッフル前に戻すことが困難になる．

3.2 コードへのシャッフル適用

QR コードは，行と列で決まる位置に白と黒を取る二次元の構造を取っている．これを一次元の写像で対応づけるために，二次元の構造を一次元に変換して，シャッフルして二次元に戻す．

セル数 33×33 バージョン 4 の QR コードに含まれる行列から，各行を連結して，1〜1089 の系列と捉える（図 3）．連結した位置から，変換後の位置に置く．定数 a を 2 としたときの変換は図 4 のようになる．それを 33 セルごとに 33×33 に戻す（図 5）．これによりシャッフルが完了する．復号時は，図 3，図 4，図 5 の手順を逆に進めることで，シャッフルした状態から元の QR コードに戻すことができる．

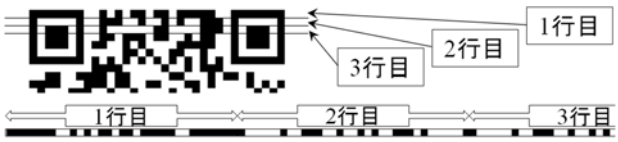


図 3　二次元から一次元への変換

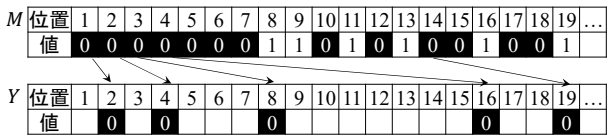


図 4　剰余類の写像による変換

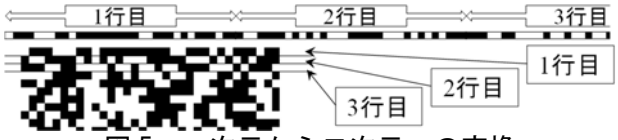


図 5　一次元から二次元への変換

(1)シャッフル前　(2)定数 a を 2　(3)定数 a を 6

図 2　QR コードのシャッフル結果

4. 結果

QR コードを提案法にてシャッフルした結果を示し，実際に運用する際の課題を述べる．

4.1 シャッフル結果

素数 p を 1091 とし，定数 a を変えてシャッフルした結果を図 2 に示す．ただし，1090 の場所については，移動先が 1090 である場所と交換することで，1〜1089 の範囲内で移動できる．

4.2 活用のための検討

定数 a が小さい値であると，小さい M に対する y の値も小さい値になることから，はじめの範囲の変化量が小さい．このことから，定数 a はより大きい値が好ましいと考えられる．

例では，QR コードのエレメント数が 1089 であることから，素数 p をそれに近い 1091 とした．これを固定すると，原始根となる定数 a の個数に限りがあることから推測されやすい．そこで，p を 1090 以上の素数に広げると，1〜1089 までの数値の範囲に収める工夫が必要である．工夫の上で，素数 p と定数 a の選択範囲を広げることで，推測を難しくさせることができる．

5. むすび

真贋判定するための GK コードにおいて，QR コードにカラーマスクパターンをかける段階で，QR コードの機能パターン部分から推測される可能性がある脆弱性があった．

その対策として，行と列の入れ替えによるシャッフルでなく，離散対数問題における剰余類を用いるシャッフル方法を検討し，適用した．これを用いることで，カラーマスクパターンの推測による攻撃に対応できると考えられる．

参考文献

[1] 藤田　悠，伊藤祥一，藤澤義範，真贋判定のためのカラー2 次元コードおよび判定システムの開発，電子情報通信学会，2019 年電子情報通信学会総合大会，D-19-1，pp. 115，2019-03-19

[2] 藤田　悠，伊藤祥一，藤澤義範，真贋判定のためのカラー２次元コードにおける脆弱性とその改善，情報処理学会，第 82 回全国大会講演論文集，vol. 2020，no. 3，pp. 385-386，2020-2-20