1F-02

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

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

ブランド品を中心に，模倣品・海賊版の流通が問題になっている．模倣品の精度が向上しており，品物を見て真贋を判定することは難しい．真贋を判定する方法として，AI などを用いてその特徴や傾向から見つけ出す方法や，真贋を判定するための目印を用いて判定する方法などが提案されている．

我々はこれまでの取り組みで，真贋を判定するための情報を暗号化して埋め込んで，商品に直接印字するカラーコードを提案した．カラーコードに含まれる情報をもとに，データベースにアクセスすることで，その商品につけられたID から唯一性が高いかどうか判定するシステムを提案した[1]．

しかし，提案したコードは，誤り訂正のために QR コードをベースに用いていることから，QR コードの機能パターンの特徴からある程度の情報を推測できる脆弱性が存在する．その脆弱性から，コードに埋め込まれた情報を直接推定できることはないが，ブルートフォース攻撃などでは，攻撃パターンを絞り込むことができる．

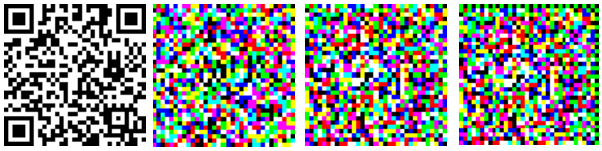
本稿では，脆弱性を回避するために施した工夫を検討し，その工夫による改善を評価する．

2. GK コード

2.1 仕様

我々が提案している 2 次元カラーコードは，黒と緑のタイミングパターンを含むことから，Black と Green から GK コードと呼称している．その作成工程の画像を図 1 に示す．

はじめに，(1)QR コードを生成する．埋め込みたい情報を AES 暗号化して，暗号化した文字列を QR コードに埋め込む．(2)QR コードをカラー画像化するためのマスクパターンを作成する．シードとなる数値をもとに，乱数を生成し，乱数から 7 色のパターンに落とし込む．そのパターンを QR コードのピクセルサイズに合わせて整形して，マスクパターンとする．(3)QR コードとマスクパターンを XOR 演算することで，QR コードをカラーパターンに変換する．(4)コード認識のために黒と緑からなるパターンを上と右に配置する．



(1)　(2)　(3)　(4)

図 1　GK コード生成のための各段階の生成物

GK コードの強靭性は，QR コードに埋め込む情報を AES 暗号化と，QR コードと XOR 演算するマスク画像，からなっている．

AES 暗号化については，その暗号化手法そのものに依存する．一方，マスク画像については，与えられたシードを用いて，生成アルゴリズムから生成された系列をカラーパターンで表している．そのため，シードやマスク画像そのものが漏洩することは，脆弱性となる．アルゴリズムを公開したときは，シードかマスク画像が鍵の役割を果たす．そこで，このマスク画像の脆弱性を検討する．

2.2 脆弱性

作成工程から分かるように，暗号化した QR コードをもとにしていることから，QR コードの機能パターン部分については，マスク画像を確定することができる．確定したマスク画像の 23%からマスク画像全体を導出することは，現状では困難であると考えている．しかし，ブルートフォースアタックの範囲が限定されることから，脆弱性になりうる可能性が高いと考えた．そこで，この脆弱性への対策を検討した．

3. 対策

QR コードの機能パターン部分に対応するマスク画像が推定できることについて，検討した対策を示し，その対策の効果を評価する．

3.1 対策方法

QR コードの機能パターンが原因であることから，機能パターンが明らかにならないように，図 2 のように，QR コードの行と列を交換によってシャッフルして，機能パターンを拡散させる．

復号時にはシャッフルされたものを逆順にリ

Vulnerability and Improvement about Color 2-dimensional Code for Imitation Detection

Yutaka FUJITA†, Shoichi ITO†, Yoshinori FUJISAWA†, †National Institute of Technology, Nagano College

図 2　QR コードのシャッフル

シャッフルする必要があるので，シャッフルする規則を記録しておく必要がある．シャッフルの規則を次のように定める．

交換対象を行または列から選択する項目をsとし，0 を行，1 を列とする．左上のモジュールを 0 行，0 列要素とし，交換する行または列の番号をm,nとする．これらをカンマで区切り，式(1)のように表示する 1 行が 1 回の交換の定義である．

$$(s,m,n) \qquad (1)$$

例えば，(1,2,3)は，「列について，2列目と3列目を交換する」という定義になる．このような定義を 1 行に 1 件記述し，交換回数分の定義を記したファイルをシャッフル定義ファイルとする．

3.2 対策の結果

20 回交換するシャッフルパターンの例を表 1 に示す．破線より左を行番号とし，その右を交換の定義とする．シャッフルする前の画像を図 3(1)の原画像としたとき，このパターンでシャッフルした結果を図 3(2)の原画像に示す．一見，QR コードの機能パターンが拡散しているようにみえる．

4. 評価

シャッフルした結果が，QR コードの特徴となる機能パターンを拡散できているかについて，確認する．確認する方法として，QR コードの機能パターンとして，マーカの部分が分散されていることを確認するために，2 次元スペクトルにて評価する．

シャッフル前の原画像とスペクトルを図 3(1)，シャッフル後の原画像とスペクトルを図 3(2)に，QR コードの機能パターン以外を黒で塗りつぶし

表 1 シャッフル定義ファイルの例

行	パターン	行	パターン	行	パターン	行	パターン
1	0,0,1	6	1,27,20	11	0,0,5	16	1,7,10
2	1,31,32	7	0,13,29	12	1,24,30	17	0,27,23
3	0,12,3	8	1,8,22	13	0,32,5	18	1,27,2
4	1,11,30	9	0,32,34	14	1,26,13	19	0,31,6
5	0,2,5	10	1,3,8	15	0,6,15	20	1,0,26

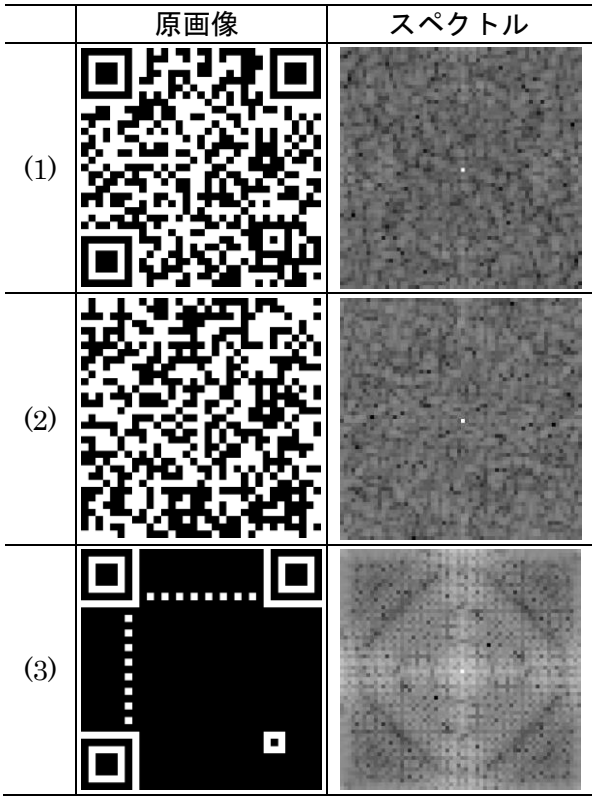


図 3　原画像とスペクトル

た原画像とスペクトルを図 3(3)に示す．これらを比較すると，図 3(3)に示したスペクトルの特徴である，画像中央からダイヤ形状に分布するスペクトルの特徴が，シャッフル前の画像ではうっすらと現れているのに対して，シャッフル後の画像では，そのような特徴あるパターンは見られない．したがって，機能パターンを拡散する方法が有効に作用しているといえる．

5. むすび

真贋判定のための 2 次元コードの元になる QR コードの機能パターンを要因とする脆弱性について，行と列のシャッフルにて対策する方法を提案した．提案方法によって，脆弱性の要因である機能パターンが拡散されていることが，スペクトルにて確認できた．

今後は，シャッフルによる方法を含む符号化及び復号過程における，シャッフルパターンの位置づけを，システムの運用に沿って検討する．

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，pp115，2019-03-19