1E-01

カラー二次元コードを用いた認証のためのシステム構築

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

ブランド品や信頼のあるメーカ品など，偽造や模倣された物品が流通を脅かしている．このような物品がどのような素性であるかなどの情報から，認証を行うことをめざしている．

物品を特定するためには，物品固有の情報を付与し，その情報から関連する素性を取得して認証する．この方法のとき，物品固有の情報が流用されたり，任意の固有情報が物品に付与されたりすると，正規品と誤認識されてしまう．

そこで，複製されにくいコードを生成することとした．暗号化やシャッフル等を用いて生成するコードを物品に付与する．そのコードの存在が容易に認識できないようにするため，ステルスインクによって印字し，存在を知っている者だけがわかるように，カラーコードとする．

このコードを用いて，物品に印字したコードを読み出し，解析して，物品の素性情報を取得して，認証する手順を実装したシステムを構築して検証した．そのシステム及び検証結果および，課題を述べる．

2. カラー二次元コード

GK コードと呼称する，カラー二次元コードを生成する手順を述べる．

(1) AES 暗号化

物品に付与する固有の情報を，AES-128-ECB にて暗号化する．物品に付与する固有の情報 31 バイトから，32 バイトの暗号文を得る．

(2) QR コード生成

32 バイトのデータを格納し，高い誤り訂正を適用するために，4 型，誤り訂正レベル H の QR コードを生成する．暗号化された系列を 34 バイトにするために，AES 暗号された 32 バイトに，埋め草を含めて QR コードのデータとする（図 1(a)）．

(a) QR コード　　(b) シャッフル適用

図 1　QR コードとシャッフル適用

System Developing for Goods Authentication using Color 2-Dimension Code
Yutaka FUJITA†, Shoichi ITO†, Yoshinori FUJISAWA†,
†National Institute of Technology, Nagano College

(3) シャッフル

QR コードにカラーマスクをかけてカラーコードにすると，QR コードの機能パターン部分では，マスクが明らかであることから，脆弱性になる可能性がある[1]．それに対応するために，QR コードのエレメントをシャッフルする(図 1(b))．QR コードの二次元行列を 1 行ごと連結し，その位置番号を離散対数問題によるメッセージ M とする．算出された値 y を移動先番号とする．定数 a と素数 p は互いに素である（式(1)）．

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

(4) マスク生成と適用

白黒からなるコードを，カラー化して，ステルスインクで印字できるようにする．

マスクパターンは，メルセンヌ・ツイスタの乱数を用い，与えるシードにて生成される 0 から 1 未満の倍精度型の値を 8 倍して，整数型にキャストすることで 0 から 7 までの値を取得し，それを 8 色の色に割り当てる（図 2(a)）．

シャッフルした QR コードとマスク画像の排他的論理和にてマスクを適用する（図 2(a)(b)）．

(5) GK コード化

コード読み取り時に，エレメントサイズを推測して，コードの方向を定めるためのパターンとして，緑と黒が交互に続くパターンを上部と右側に付与して，GK コードを生成する．

2.2 複雑度

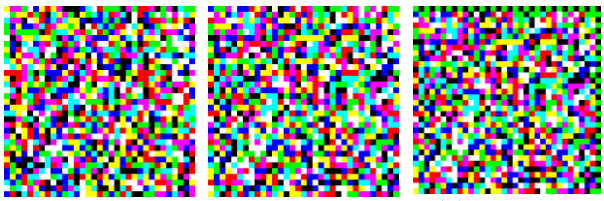
(1) AES 暗号化

AES-128-ECB の暗号化アルゴリズムによる攻撃は困難であるとしたとき，暗号鍵のパターンとして，128 ビットのあらゆるパターンが考えられることから，式(2)となる．

$$2^{128} \cong 2.917 \times 10^{38} \qquad (2)$$

(2) シャッフル

シャッフルのパターンとして，a と p の組み合わせで与えられるため，その組み合わせは無



(a) カラーマスク　(b) マスク適用　(c) GK コード

図 2　カラーコード化

限である．ただし，1-1089 までの有限範囲での入れ替えであることから，1089 個の値の置き換え先が 1 個目で 1089 箇所，2 個目が 1088 箇所，3 個目が 1087 箇所と続くことから，全てを置き換えるパターンは，式(3)となる．

$$1089! \cong 1.969 \times 10^{2836} \quad (3)$$

(3) カラーマスク

カラーマスクは，乱数生成のシードによって決まることから，符号なし整数型のシードとして，32 ビットとして，式(4)となる．

$$2^{32} \cong 4.294 \times 10^{9} \quad (4)$$

3. 認証システム

カメラが搭載されたモバイル端末でカラーコードを読み込んで認証できる形態を想定している．そのため，ウェブアプリで実現することとした．また，サーバに問い合わせる際には，鍵などの情報をクライアントに保存することが無いように，サーバ側で復号するようにした．

3.1 認証サーバ

認証を行うためのウェブサーバは，物品情報を管理するページ，復号情報を管理するページ，コードリーダのページを持つ．

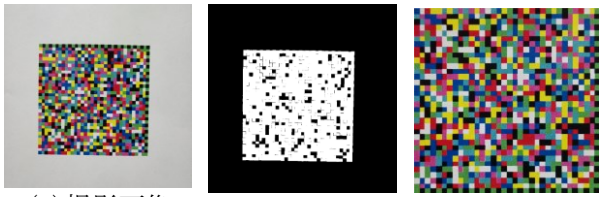
物品固有の情報にひもづいた製造や店舗の情報のデータベースを持つ．また，カラーコード復号のためのマスクパターン，シャッフルパターン，AES 復号の鍵の情報，これらの組み合わせのパターンがあり，それを管理・登録するページを持つ．さらに，物品番号のブラックリストの情報を有している．

3.2 コードリーダ

コードリーダは，撮影した画像から GK コードを認識して，34×34 のエレメントに分割し，デジタル情報として格納する．34×34 からなる GK コードの色情報をサーバに送る．

撮影画像（図 3(a)）から，000,00F...FFF の 8 色の範囲を決めてそれぞれを抽出する．8 色の内，背景色以外の抽出結果の論理和を取る（図 3(b)）．その結果を元に，輪郭を取る．その輪郭で切り取った範囲を正方形に伸縮させて，340×340 の画像とする（図 3(c)）．

その正方形を 10 ピクセル刻みの格子状に捉え，各範囲の色を抽出して，34×34 のコードとする．



(a)撮影画像　(b)色別認識合成　(c)範囲伸縮後

図 3　コード認識手順

下辺または左辺に GK パターンがある場合は，正規の位置まで回転させる．これらの画像の処理は，opencv.js を用いる．

3.3 コード復号

サーバ側では GK コードのデータ部を取り出し，マスクを解除し，シャッフルを解除して，QR コードからデータを取り出し，AES 暗号を解除する．

コード復号のために，マスクパターン，シャッフル，AES 復号のための復号情報をサーバから取得する．取得した全てのパターンで，マスク解除，シャッフル解除，QR コード復号，AES 復号の順に適用していき，最も適切に復号されたパターンと，その復号結果を結果として出す．

3.4 認証

コードから得られた物品固有の情報について，データベースにアクセスして，製造や販売などの情報を得て，検証して判定する．

物品番号に関する素性情報の他，ブラックリスト登録情報の有無，登録された番号が存在しない場合に「危険」，認証アクセス頻度が頻繁である場合に「注意」，それ以外のときに「安全」とする，3 段階で判断し，判定コードを与える．素性情報と判定結果をアクセス元に返す．アクセス元の端末に，その素性情報と判定結果を表示する．

4. 考察

検証のために白紙に印刷したコードを Android や iOS のモバイル端末で読み取ることができ，認証結果が表示されることが確認できた．各段階における，課題について述べる．

4.1 色の調整

ウェブブラウザから立ち上げたカメラで撮影して，そこからコードを認識して GK コードのデジタル情報に変換する部分において，色調によって，本来の色が認識できない場合があった．コントラストや明るさについて，色調を整える必要がある．

4.2 コードの輪郭

コードの輪郭を取って，その範囲を正方形に整形するとき，コード全体を包含する輪郭でない対象が選ばれることがある．認識範囲の制限などによる改善が考えられる．

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，情報処理学会，第 82 回全国大会講演論文集，vol.2021，no.3，pp.383-384，2021-3-19