Computer Security Symposium 2018
22 - 25 October 2018

SeQR: ショルダーハック耐性を持つQRコード生成方法

笹崎　寿貴[1]　シュウ　インゴウ[1]　丸山　誠太[1]　森　達哉[1]

概要：QR コードはその利便性から情報の共有手段として広く用いられる一方，安全性についてはセキュリティ上の問題が存在することが知られている．中でも，QR コードは第三者が撮影してもデータを読み取れてしまう性質上，決済などの利用シーンにおいて重要なデータが含まれていてもその内容は保護されないという問題がある．本論文では，特定の距離からのみ読み取ることが可能な QR コード “SeQR” の生成手法を提案し，本手法がこのようなショルダーハッキングによるデータ盗難への対策として有効であることを示す．具体的な生成手法は，QR コードの誤り訂正能力を超えないようデータのランダム化を行う．更に，QR コードのあるモジュールに対し偽色を誘発するパターンを配置する．特定の距離から撮影した場合偽色が発生し，QR コードリーダによりモジュールが解釈されるビットが反転する．偽色は特定の距離でのみ発生するため，背後から撮影した場合にはビット反転が生じず，QR コードを読み取ることが不可能となる．本研究では，SeQR に対して撮影距離による読み取りの成功率を測定し，ショルダーハッキング対策としての有効性を評価する．また，偽色誘発パターンと通常のモジュールを識別されることにより QR コードを復元される可能性があるという脅威モデルについて評価を行う．

キーワード：QR コード，ショルダーハッキング，偽色，モアレ

1. はじめに

QR コードは誤り訂正能力を有しており，様々な角度から素早く読み込みができるといった利便性から情報の共有手段として広く用いられている．例えば，Web サイトの URL の共有であったり，SNS におけるアカウント情報の交換であったり，チケットの識別であったりと利用用途は多岐に渡る．近年では QR コードを決済に用いる動向も活発化しており，中国ではアリペイ [1] やウィーチャットペイ [2] などにより広く普及している．また，本国では携帯電話キャリアの主要三社である NTT ドコモ [3]，ソフトバンク [4]，KDDI [5] が QR コード決済の開始を発表したり，QR コード決済の普及に向け仕様の統一化が進められたり [6] するなど，ますます普及の一途をたどっている．

このように普及が進む一方で，QR コードの安全性についてはセキュリティ上の問題が存在することが知られている．中でも，QR コードに対する攻撃についての研究は多く存在し，Kieseberg ら [7] は効率的に QR コードの白モジュールを黒モジュールに塗り替えることでフィッシングが可能となる QR コードの構成方法を示している．近年では，大熊ら [8] の研究において曖昧な QR コードを作成することにより，読み取った人間を正規のサイトと悪性のサイトに一定の確率で誘導することが可能であることを示した．このように，QR コードをすり替える，または加工することで安全性が脅かされるということはしばしば問題として指摘されており，安全性を確保する必要性が一層高まっている．

ここで，QR コードは含まれているデータを暗号化するものではないという性質に着目すると，QR コードに機密情報や個人に関わる情報が含まれていた場合，QR コードを自分以外の第三者に読み取られてしまうと安全性が損われてしまうという問題がある．

そこで，特定の距離からのみ読み取り可能な QR コードを構成することにより，背後に存在する第三者から QR コードを読み取られるれることを防止することが可能となる．

本研究では，偽色という現象を利用することで特定の距離からのみ読み取り可能な QR コード **SeQR** の生成方法を示すとともに，それを用いることで第三者からのショルダーハッキング対策としての有効性を評価する．

また，SeQR に内在する脅威モデルについて評価を行い，SeQR の安全性について議論を行う．

本研究の貢献は以下の通りである．

- 偽色を応用し，特定の距離からのみ読み取り可能な

[1] 早稲田大学 基幹理工学研究科
Fundamental Science and Engineering, Waseda University

QR コードの生成方法を示した

- 本手法により生成された QR コードが実際に読み取り可能な距離を測定し，計算により得られた距離から撮影した場合に読み取りの精度が高まることを示した
- 本手法により生成された QR コードを遠隔から読み取ることを試みた場合，撮影者と同程度の能力を有するカメラでは 2 m 以上の距離から偽色誘発パターンを識別しづらいことが分かった
- 本手法により生成された QR コードを遠隔から読み取ることを試みた場合，一般的な望遠レンズを備えたカメラでは 12 m 以上の距離から偽色誘発パターンを識別しづらいことが分かった

第 2 章では本研究の理解に必要な背景知識について，第 3 章では本論文における提案手法について，第 4 章では提案手法を元に実施した実験とその結果について，第 5 章では提案手法における制約や課題について，第 6 章では本研究の関連研究について報告する．

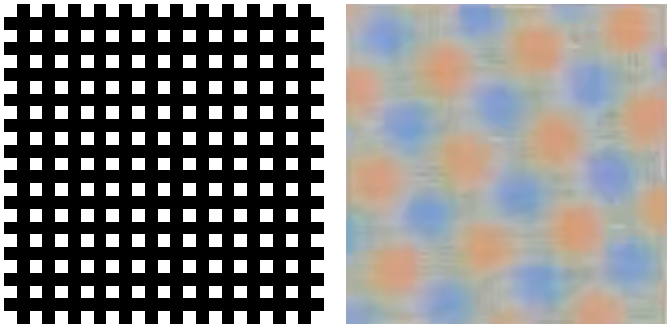
2. 背景

本章では，本研究の理解に必要な背景知識について述べる．

2.1 偽色

偽色とは，カラーフィルタを有するデジタルカメラで周期的なパターンを有する画像を撮影したときに発生する本来存在しない色のことである．近年のデジタルカメラに内蔵されている CMOS イメージセンサにはカラーフィルタと呼ばれるフィルタが搭載されている．このカラーフィルタは，デジタルカメラの受光素子が画素ごとにサンプリングする色を決めるのに用いられ，光の三原色である RGB のうち決められた色をサンプリングしている．画像が仮に周期的なパターンを有していた場合，このパターンの空間周波数とカラーフィルタの空間周波数が干渉することで干渉網が発生する．この干渉網をモアレといい，そのときに発生する本来存在しない色が偽色である．本論文では，偽色を誘発するような周期的な模様を偽色誘発パターンと呼ぶこととし，偽色誘発パターンの例を図 1a に示す．この偽色誘発パターンを液晶ディスプレイに投影し，カラーフィルタを有するスマートフォン (Apple iPhone 8) で撮影した結果が図 1b であり，確かに偽色が発生していることが確認できる．本研究では，この偽色を QR コードに認識される真偽値を反転させる目的で用いる．

また，本研究で用いる偽色誘発パターンは例として示した図 1a と同じものを用いている．これは，パターン中に占める黒の割合が多いため QR コード全体を黒に近づけることが可能となる，繰り返しの周期が最小であるためディスプレイの解像度を最大限に利用することができる，などのためであり，必ずしもこの模様を選択する必要がないことに注意されたい．



(a) 偽色誘発パターン　(b) 撮影された偽色

図 1: 偽色の例

図 1 のように撮影された偽色が QR コードリーダにより真偽値として認識されるとき，真偽どちらに認識されるかは QR コードリーダの実装に依存し，QR コードリーダの実装の多くはブラックボックスであるため明らかではない．本研究では実測に基づき，偽色が特定の距離で真となり，それ以外の距離では偽と認識されるものとしていることに注意されたい．一方で，OSS として公開されている QR コードリーダライブラリも存在しており，このことについては 5 章で議論を行う．

このように，二つの空間周波数の差が極めて小さいときに偽色は発生する．偽色の発生が最大となるのはこれら空間周波数が等しい，つまり差が 0 となるときである．それぞれの空間周波数は次のように表すことができる．ここで，空間周波数とは 1 m あたりの周期数とする．

まず，液晶ディスプレイの解像度に沿って投影された画像の空間周波数は次のように求めることができる．ディスプレイの画素密度を P_d dpi とすると，1 m あたりの画素数は $39.4P_d$ である．投影される画像は 2 画素の繰り返しであるから，1 m あたりの周期数，つまり空間周波数 ν_d は $19.7P_d$ である．

一方，イメージセンサの空間周波数はイメージセンサの大きさ，解像度，焦点距離，撮影距離によって変わる．

焦点距離を f mm，イメージセンサの対角の長さを l mm とし，撮影距離を d m，イメージセンサの像の対角の長さを L m とすると図 2 のような関係になることが知られている．

図 2 から，イメージセンサの像の対角の長さ L は

$$L = \frac{ld}{f} \tag{1}$$

したがって，イメージセンサの解像度を横 x px，縦 y px とすると，空間周波数 ν_i は，

$$\nu_i = \frac{\sqrt{x^2 + y^2}}{2L} \tag{2}$$

例として，$\nu_d = \nu_i$ となるときを考え，機器として本研究でも使用する次のカメラ，ディスプレイを考える．

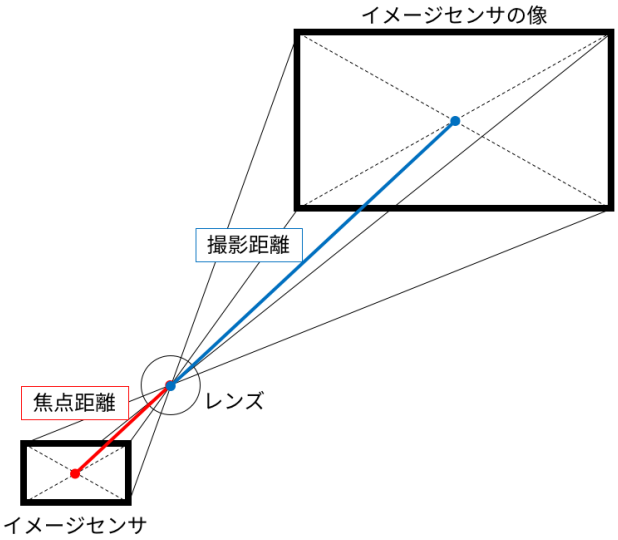


図 2: 撮影距離と発生距離の関係

- カメラ (イメージセンサ) : 対角の長さ 6.02 mm，焦点距離 3.99 mm，解像度 4032 × 3024
- ディスプレイ : 対角の長さ 31.5 in，解像度 3280×2160，画素ピッチ 0.181 mm [9]

上記から，二つの空間周波数が一致する撮影距離は 0.605 m と算出される．

2.2 QR コード

QR コードとは，2 次元コードの一種である．内部にリードソロモン誤り訂正符号を備えているため，汚れや破損によるシンボル誤りを一定の割合修復することが可能となっているのが特徴である [10]．本研究ではこの誤り訂正機能に着目し，特定の距離から撮影した場合に限って誤り訂正が為されるよう QR コードを構築することで，SeQR の生成を可能とする．

QR コードの誤り訂正機能であるが，QR コードに設定する誤り訂正レベルによって訂正可能なコード語数が異なる．誤り訂正レベルには四段階あり，訂正能力が低い順に L，M，Q，H である．訂正レベルが最も高い H は約 30%のコード語の誤りを訂正可能である．詳細には，誤り訂正コード語の数を n としたとき，訂正可能なコード語数は $\lfloor n/2 \rfloor$ である．例として，2 型で誤り訂正レベル H の QR コードは全コード語数が 44，データコード語数が 16，誤り訂正コード語数は 28 である．したがって，訂正可能なコード語数は 14 であり，訂正可能な割合は 約 32%である．この例では 14 コード語までの誤りを訂正可能であるので，15 コード語が誤っていた場合訂正が不可能となる．以降，本研究では上記で述べた 2 型誤り訂正レベル H の QR コードを用いる．

図 3: “secret” が格納された QR コード

3. 手法

3.1 SeQR の生成手法

特定の距離からのみ読み取り可能な QR コード「SeQR」の構成手法について説明する．

QR コードはリード・ソロモン符号を用いた誤り訂正能力を有している [11]．これにより，QR コードの訂正レベルに応じた語数の符号語を訂正することが可能となる．訂正可能な範囲を超えた誤りを有している QR コードに関しては，訂正することが不可能となる．

また，偽色はカラーフィルタを有するデジタルカメラによって撮影されたときに発生する本来存在しない色のことであり，言い換えると色を変動させることができるものである．したがって，QR コードのモジュールに偽色を誘発するようなパターンを用いることでモジュールの真偽値を誤認識させることが可能である．

偽色は特定の距離から撮影したときに発生するため，特定の距離に限り誤認識が発生する．誤認識が発生したときに誤り訂正が可能な範囲に収まっていれば，QR コードは正しく読み取ることが可能となり，そうでなければ読み取りが不可能となる．

以上を踏まえると，以下の手順で構成できる．

(1) 任意の文字列から QR コードを生成する
(2) QR コードの誤り訂正コード語数が n であったとき，データコード語の中から $\lfloor n/2 \rfloor$ 語を異なるコード語に置換する
(3) 置換されなかった任意の 1 コード語における，白のモジュール 1 つを偽色誘発パターンで置換する

以下に本手法により生成された QR コードの例を示す．

図 3 の QR コードは “secret” という文字列が格納された QR コードである．この文字列から誤り訂正レベル H にて符号語を生成すると，

“0x40, 0x67, 0x36, 0x56, 0x37, 0x26, 0x57, 0x40, 0xec, 0x11, 0xec, 0x11, 0xec, 0x11, 0xec,

図 4: データコード語がランダム化された QR コード

図 5: 偽色誘発パターンが挿入された QR コード

0x11, 0xc4, 0x81, 0xc6, 0x1d, 0x0a, 0xd8, 0x67,
0x0f, 0x11, 0x56, 0x5b, 0xda, 0xab, 0x2e, 0x90,
0x57, 0x58, 0x20, 0xe3, 0x92, 0x28, 0xcb, 0x72,
0x45, 0x12, 0xbf, 0x3c, 0xad”

となる．このうち，前半 16 シンボルはデータコード語，後半 28 シンボルは誤り訂正コード語である．したがって，訂正可能なコード語数は 14 語であるから，前述の手法に則り，データコード語 14 語をランダムな語に置換する．置換後のコード語は

“0x9f, 0xba, 0x2a, 0x33, 0xc2, 0x1c, 0x16,
0x8e, 0xa8, 0x6c, 0x7b, 0xe0, 0x34, 0x2c, 0xec,
0x11, 0xc4, 0x81, 0xc6, 0x1d, 0x0a,0xd8, 0x67,
0x0f, 0x11, 0x56, 0x5b, 0xda, 0xab, 0x2e, 0x90,
0x57, 0x58, 0x20, 0xe3, 0x92, 0x28, 0xcb, 0x72,
0x45, 0x12, 0xbf, 0x3c, 0xad”

であり，この符号語による QR コードは図 4 のようになる．この状態では誤り訂正が可能となっているため，ここから白モジュールに対して偽色誘発パターンを挿入することで誤り訂正が不可能な状態にする．挿入を行うのはランダム化を行なっていないシンボル内のモジュールであり，なおかつモジュールが白である箇所である．挿入後の誤り

図 6: 実験セットアップ

は 15 シンボルとなるため，誤り訂正が不可能である．したがって，格納されたデータを復元することはできない．挿入後の QR コードは図 5 に示す通りである．また，図 5 における通常のモジュールの色は偽色誘発パターンを遠隔から認識したときと同色となるような色に設定してある．

4. 実験

4.1 撮影距離による読み取りの成功確率

3 章で示した手法に基づき QR コードを生成し，評価実験を行う．具体的には，図 6 のように液晶ディスプレイからカメラまでの撮影距離を変化させ QR コードの読み取り確率を測定する．撮影距離は 0.15 m から 1.0 m まで 0.05 m 刻みで変化させ，読み取り時の手ぶれを模すため，その距離から 0.01 m 前後させ読み取りが可能か測定する．この測定を各距離に対し 10 回試行し，その内成功した回数が n 回であったときに成功確率を $n/10$ とする．QR コードを表示する機器として液晶ディスプレイ (LG 32UD59-B) を用い，QR コードリーダーとして一般的なスマートフォン (Apple iPhone 8) の標準カメラ機能を用いた．

ここで，表示する QR コードは図 5 と同様のものを用いるが，液晶ディスプレイに表示した場合，偽色誘発パターンと通常のモジュールの色が異なって表示されてしまう．したがって，同じ色に識別されるよう通常のモジュールの色を調整した図 7 の QR コードを本実験では用いた．

また，本実験環境は壁面が白く光源は蛍光灯であるような一般的なオフィス環境である．図 8 に，撮影距離とそれに対応する QR コードの読み取り確率を示す．

図 8 から，読み取り距離が 0.55 m 付近で最も成功確率が高いことが分かる．これは偽色の最大発生距離が 0.605 m であることに起因している．一方で，0.75 m や 0.90 m といった撮影距離でも稀に読み取りに成功していることが分かる．これは，上記の距離であっても空間周波数の差が極めて小さいため，偽色が発生し，そのために誤認識が発生していると考えられる．

また，同様に図 8 から 1.0 m 以上の距離では読み取りに

図 7: 実験に用いた偽色誘発パターン挿入済み QR コード

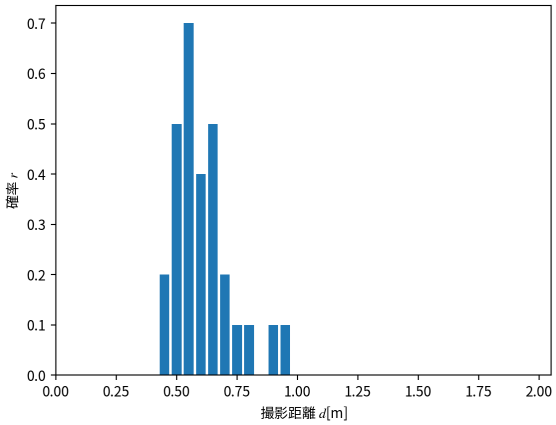


図 8: 撮影距離に対する読み取り成功確率

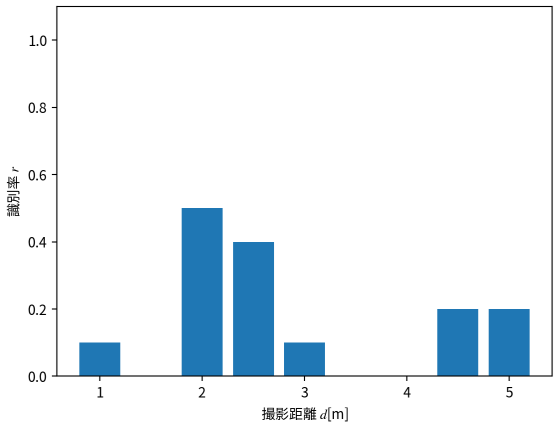


図 9: C_1 による撮影画像における識別率

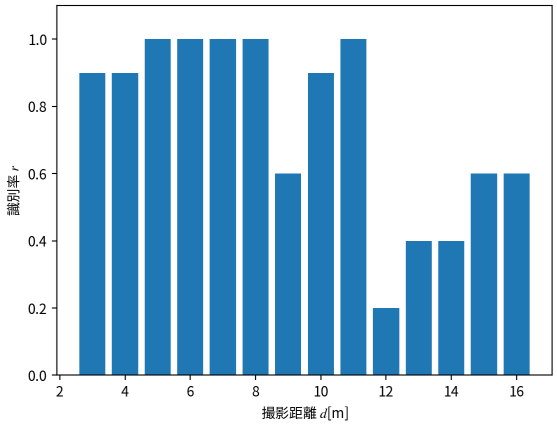


図 10: C_2 による撮影画像における識別率

成功していないことがわかる．これは，撮影者と同じ能力を持つカメラであれば，1.0 m 以上の距離からデータの読み取りを阻止できることを示している．

4.2 脅威モデルの検証

本研究における SeQR は，特定の距離からのみ読み取りが可能な QR コードを生成することで背後から第三者に読み取られることを防ぐというものであった．しかしながら，通常のモジュールと挿入された偽色誘発パターンは異なる模様をしているため，これらが識別可能であった場合偽色誘発パターンを取り除くことで正しく読み取り可能な QR コードが復元できてしまう．

4.1 節では，SeQR は偽色が発生する距離においては読み取りが可能であったが，図 8 から 1.0 m 以上の距離では読み取りができないことが分かった．しかし，これは QR コードリーダが読み取りをできなかったということであり，二つのモジュールの識別が不可能であったということではない．

したがって，本節では撮影能力の異なる二つのカメラを用意し，それぞれにおいて通常のモジュールと偽色誘発パターンの識別が可能であるのか不可能であるのか検証を行う．

この検証では，遠隔からの撮影によって二種類のモジュールを識別可能か定量的に評価するため，次の実験を行う．撮影機材として，SeQR の読み取りに用いたカメラと同じカメラ C_1(Apple iPhone 8) と，望遠レンズを備えたカメラ C_2(Nikon D5600) の 2 つを用いる．また，用いた望遠レンズは “AF-P DX NIKKOR 70-300mm f/4.5-6.3G ED VR” である．それぞれのカメラにより SeQR を撮影し，撮影された QR コードの一部 (6×6 セル) を被験者に提示する．画像を確認した被験者は，挿入された偽色誘発パターンがどれかを指し示し，その結果が正しければ識別可能，そうでなければ識別不可能とする．以上により，通常のモジュールと偽色誘発モジュールの区別が可能であるか検証を行う．

被験者は 20 代から 40 代の男女 10 名であり，裸眼または矯正後の視力に問題ないことを確認した上で実施した．

C_1，C_2 による撮影画像で実験を行った結果としてそれぞれ図 9，図 10 が得られた．

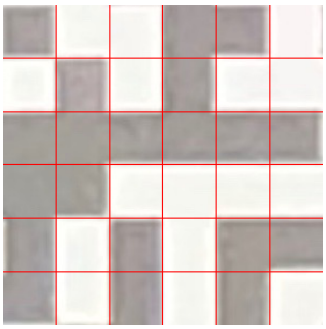


図 11: 実験に用いた画像

アプリケーション	成否
標準カメラ	✓
Google Chrome	✗
Firefox	✓
LINE	✓
Twitter	✗
QR Code (arara inc.)	✓
QR コードリーダー PRO [12]	✓
QR コードリーダー for iPhone [13]	✗
ICONIT	✗

表 1: アプリケーションごとの読み取り可否

図 9 より，通常の読み取り者と同様の撮影能力を持つカメラで撮影された場合は，近距離からの撮影画像であっても識別率が低いことが分かる．撮影距離が 2 m や 2.5 m の場合において，識別率が高まっていることに関しては 5 章で考察するが，同様の能力を持つカメラからは識別が困難であると言える．

一方で，図 10 から能力を大きく超えるカメラにより撮影された場合は，遠距離からの撮影画像であっても識別率が高いことが分かる．したがって，能力を大きく超えるカメラに対しては SeQR は保護されない可能性があることに注意されたい．

5. 議論

本章では，本研究における制約および今後の課題について述べる．

5.1 本手法における制約

3 章で説明した手法は，QR コードリーダに特段手を加えることなく QR コードの生成側で完結するという利点があった．しかしながら，本手法では読み取りに 1 秒以上要することも少なくなく，“Quick Response” である QR コードの性質を損なってため，読み取り時間および読み取り精度の向上は今後の課題である．

5.2 実験における識別率

図 9 で距離 2 m における偽色誘発パターンの識別率は 0.5 と非常に高い数値であった．このように識別率が高くなってしまったのは，実験に用いた画像において色による識別が可能であったためであると考える．

例として，実験に用いた画像を図 11 に示す．この画像において，偽色誘発パターンは左上を基準に座標 (2,2) のところに存在する．偽色誘発パターンを遠隔から撮影したときの色と通常のモジュールの色に僅かながら差異が存在しているため，偽色誘発パターン特有の周期的模様が観測されなくとも判別が可能となってしまっている．

偽色誘発パターンは黒と白の画素を周期的に並べたものであるから，遠隔から見たときの色は並置加法混色より輝度の平均値を算出すれば良いように思える．しかし，偽色誘発パターンは投影する液晶ディスプレイの画素に沿って配置されているため，ディスプレイによっては異なった色に知覚され，本研究においては手作業での色の調整が必要となった．ディスプレイに因らない偽色誘発パターンの設計は今後の課題である．

5.3 総当たりによる解読に対する安全性

本研究において，偽色誘発パターンの挿入数は 1 モジュールとした．攻撃者がこの事実を知っていた場合，モジュール数分白に塗り替える攻撃を試行することで，読み取り可能な QR コードが復元できてしまう．このときの計算量は $O(n)$ であり，容易に攻撃が成立してしまう．

偽色誘発パターンを k モジュール挿入した場合の計算量は $O(n^k)$ である．k を増加させると計算量は指数的に増加し，結果として上記の総当たりによる攻撃耐性が高まる．

しかしながら，偽色誘発パターンを増やすことで秘匿が可能なデータ数が減少してしまうという問題が生じる．

そこで，データ部の末尾に挿入される埋め草コード語に着目する．これは，データ語が既定の語数に満たない場合，残りを埋め草符号と呼ばれる意味を持たない符号後の繰り返しでパディングするというものである．

本研究では偽色誘発パターンの挿入数は 1 モジュールとして実験を行ったが，挿入数を増やしての実験と攻撃耐性の評価は今後の課題である．

5.4 読み取り機器による差異

本研究で読み取りに用いた機器は Apple 社のスマートフォン iPhone 8 であり，アプリケーションは標準カメラの QR コード読み取り機能であった．同一の OS であっても，アプリケーションごとに QR コード読み取り機能の実装は異なっている可能性があり，機器で実験を行うことが望まれる．

本研究では更に複数のアプリケーションを用いて，SeQR の読み取りが可能か検証を行なった．その結果が表 1 であり，これを参照するとアプリケーションにより成否が異なっていることが分かる．

また，スマートフォンだけではなく，店頭で用いられるような読み取り端末でも読み取りが可能か試行したが，読み取ることはできなかった．これは，読み取り端末のイメージセンサがスマートフォンと同じ Bayer Filter でないことで大きく偽色が発生していないことや，スマートフォンと同じ読み取り方式を採用していない可能性が考えられる．

5.5 QR コードリーダの実装

本研究では QR コードリーダの実装はブラックボックスであることを前提に進めた．一方で，OSS である QR コードリーダライブラリも存在し，例えば **ZXing** [14] が存在する．この実装を参照すると，QR コードのモジュールを認識する段階において，グレースケール化，適応的閾値による二値化を行なっていることが分かる．具体的には，RGB の輝度を 1 : 2 : 1 の比重で加重平均をとることでグレースケール画像に変換し，周囲 5×5 モジュールの輝度の平均値を閾値として二値化を行う適応的閾値を適用している．このような例では，周囲のモジュールの色で二値化に用いる閾値が決定されるため，偽色を挿入する位置を周囲に黒モジュールが多い白モジュールにすることで，更に認識率が高まることが考えられる．

5.6 攻撃への応用

偽色誘発パターンを用いることにより，特定の距離から撮影した場合に限り別の Web サイトへ誘導する QR コードを生成することができる．本手法は，大熊ら [8] の研究を元にしたものである．当研究は以下の手順で QR コードの生成が行われる．

(1) URL U_0 から QR コード Q_0 を生成する
(2) U_0 のコード語と距離が最小距離となるような URL U_1 を決定し，QR コード Q_1 を生成する
(3) 異なっているコード語数を d としたとき，Q_1 から $\lfloor d/2 \rfloor$ 語を異なっているコード語から選択し，Q_1 を置換する
(4) 置換されていないコード語の内，両者の間で 1 bit のみ異なっているコード語を選択する
(5) その 1 bit に該当するモジュールの位置に白と黒の中間色のモジュールを挿入する

我々の生成方法では，挿入するモジュールを偽色誘発モジュールとすることで，通常は U_0 が読み込まれるが特定の距離から撮影したときのみ U_1 が読み込まれる QR コードが生成できる．

図 12 に示す QR コードは，特定の距離から読み取ったときのみ “`fsl.cs.waseda.jp`” へ遷移し，それ以外は正規の “`nsl.cs.waseda.ac.jp`” へ遷移するという QR コードである．実際にこの QR コードに対し読み取りを試みたところ，偽色の発生距離から撮影しているときに限り “`fsl.cs.waseda.ac.jp`” と読み込まれることがあることを確認した．ただし，この距離であっても正規 “`nsl.cs.waseda.ac.jp`” が読み込まれることがあるため，誤認識の確率は低いことに注意されたい．

図 12: 偽色を用いた悪性サイトに誘導する QR コード

6. 関連研究

本章では QR コードにおける関連研究について述べる．冒頭でも述べたように，QR コードに対する攻撃として，Kieseberg ら [7] の研究がある．これは，効率的に QR コードの白モジュールを黒モジュールに塗り替えることでフィッシングが可能となる QR コードの構成方法を示している．また，大熊ら [8] の研究では，曖昧な QR コードを作成することにより，読み取った人間を正規のサイトと悪性のサイトに一定の確率で誘導することが可能であることを示した．

また，QR コードを収集，解析を行なった研究として，Kharraz ら [15] の研究が存在する．これは，APK や EXE をダウンロードさせる URL や，フィッシングを行うような URL が含まれているような悪意のある QR コードを収集し，解析を行なったものであり，QR コードを読み込むようなモバイルデバイスでは URL にアクセスする前にサイトの安全性を確認するなどの対策が必要であると結論づけている．

また，QR コードのデータを保護する研究として，Conde-Lagoa ら [16] の研究が存在する．これは，従来の電子チケットとは異なり，含まれているデータをブロック暗号により暗号化することで保護するという新しい電子チケットのモデルを提案するものである．ユーザは QR コードの読み取り後に設定したパスワードを入力することで認証されるが，QR コードリーダの実装に変更を加える必要がある．

一方で本研究では既存の QR コードリーダに変更を加えることなく，QR コードの生成側で QR コードのデータ保護が行えるという利点がある．

7. 結論

QR コードの誤り訂正能力と CMOS イメージセンサに備わるカラーフィルタにより生じる偽色を用いることで，特定の距離からのみ読み取ることが可能な QR コード **SeQR** の生成方法を示した．

この手法により生成した QR コードについて，撮影距離ごとに読み取りの成功確率を測定したところ，ディスプレイから 0.6 m の撮影距離で最も成功確率が高く，その確率は 0.7 であった．また，　撮影距離が 1.0 m 以上の場合は読み取りに成功することはなかった．したがって，背後から QR コードによる読み取りに関しては防ぐことが可能であるといえる．

この手法により生成した QR コードについて，読み取り者と同程度の能力のカメラと望遠レンズを備えたカメラにより QR コードを撮影し，偽色誘発パターンと通常のモジュールを識別可能か実験を行ったところ，同程度の能力のカメラでは 1.0 m 以上では識別が困難となり，望遠レンズを備えたカメラでは 12 m 以上で識別が困難となった．

これは，同程度のカメラはショルダーハッキングによるデータ盗難への対策として有効であるが，それ以上の能力を有したカメラに対しては保護が可能な距離が異なってくることを表している．

本手法を用いるメリットは，QR コードリーダに特別手を加えることなく，背後からの読み取りを防ぐことができるという点にある．したがって，QR コードに含まれるデータをより安全に保護するといった場合は，この手法はもちろん，データをアプリケーション側で暗号化してやりとりするなどの対策が必要であると考える．

artifact 本研究で作成した SeQR のデモンストレーションを `https://youtu.be/4Ft2xX5-vP0` に上げてある．また，`https://github.com/toshs/SeQR` に SeQR の生成に用いたスクリプトや生成された画像等を上げてあるので参照されたい．

参考文献

[1] Alipay: alipay QR コード発行&支払い手順，`https://qr.alipay.com/paipai/open.htm`.

[2] WeChat: wechat pay QR コード発行&支払い手順　，`https://pay.weixin.qq.com/guide/qrcode_payment.shtml`.

[3] NTT ドコモ：報道発表資料：新たなスマホ決済サービス「d 払い」を提供開始，`https://www.nttdocomo.co.jp/info/news_release/2018/01/17_00.html`.

[4] ソフトバンク株式会社：ソフトバンクとヤフーの合弁会社が、インドの Paytm と連携し、バーコードを使った新たなスマホ決済サービス「PayPay」を今秋提供開始，`https://www.softbank.jp/corp/group/sbm/news/press/2018/20180727_01/`.

[5] SankeiBiz: ＫＤＤＩ、ＱＲ決済を年度内に導入　加盟店開拓へ他社と連携を検討，`https://www.sankeibiz.jp/business/news/180406/bsj1804060500001-n1.htm`.

[6] 日本経済新聞：9 日に協議会初会合、ＱＲ決済の規格統一へ議論，`https://www.nikkei.com/article/DGXMZO33908670070820 18EE8000/`.

[7] Kieseberg, P., Schrittwieser, S., Leithner, M., Mulazzani, M., Weippl, E., Munroe, L. and Sinha, M.: *Malicious Pixels Using QR Codes as Attack Vector*, pp. 21–38, Atlantis Press (2012).

[8] 大熊浩也，　瀧田愼，森井昌克：悪性サイトに誘導する QR コードの存在とそれを利用した偽造攻撃，信学技報，ICSS2018-6, Vol. 118, No. 109, pp. 33–38 (2018).

[9] LG エレクトロニクス・ジャパン：32UD59-B, `https://www.lg.com/jp/monitor/lg-32UD59-B`.

[10] 株式会社デンソーウェーブ：誤り訂正機能について，`http://www.qrcode.com/about/error_correction.html`.

[11] 一般財団法人　日本規格協会 一般社団法人　電子情報技術産業協会：JIS X 0510:2018 情報技術―自動認識及びデータ取得技術―ＱＲコード　バーコードシンボル体系仕様 (2018).

[12] KIKAKU, D.: QR コードリーダー PRO, `https://itunes.apple.com/jp/app/qr%E3%82%B3%E3%83%BC%E3%83%89%E3%83%AA%E3%83%BC%E3%83%80%E3%83%BC-pro/id1180529697?mt=8`.

[13] Wada, T.: QR コードリーダー for iPhone, `https://itunes.apple.com/jp/app/qr%E3%82%B3%E3%83%BC%E3%83%89%E3%83%AA%E3%83%BC%E3%83%80%E3%83%BC-for-iphone/id585561686?mt=8`.

[14] ZXing-Project: zxing/zxing: ZXing ("Zebra Crossing") barcode scanning library for Java, Android, `https://github.com/zxing/zxing`.

[15] Kharraz, A., Kirda, E., Robertson, W., Balzarotti, D. and Francillon, A.: Optical Delusions: A Study of Malicious QR Codes in the Wild, *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pp. 192–203 (online), DOI: 10.1109/DSN.2014.103 (2014).

[16] Conde-Lagoa, D., Costa-Montenegro, E., Gonzlez-Castao, F. J. and Gil-Castieira, F.: Secure eTickets based on QR-Codes with user-encrypted content, *2010 Digest of Technical Papers International Conference on Consumer Electronics (ICCE)*, pp. 257–258 (online), DOI: 10.1109/ICCE.2010.5418880 (2010).