

## 視覚復号型秘密分散法の QR コードへの応用

日大生産工(学部) ○大川 直也 日大生産工 柄窪 孝也

### 1. まえがき

視覚復号型秘密分散法とは、1979年に Shamir[1]が提案した秘密分散法を画像に応用した手法であり、1994年に Naor と Shamir[2]が提案している。この手法では、秘密にしたい画像を複数枚のシェアと呼ばれる画像に分散処理し、そのシェア画像単体からでは元の秘密の画像はわからないが、あらかじめ定められたしきい値以上のシェア画像を重ね合わせることで、元の秘密の画像を復元することのできる秘密情報の分散管理方式である。一方、QRコード[3]とは、株式会社デンソーウェーブが開発した2次元コードであり、URLなどの埋め込み以外にも、近年では決算方式での利用が増えてきている。

視覚復号型秘密分散法を QR コードに適用した研究としては、2016年に Cao ら[4]が視覚復号型秘密分散法を用いて、2枚のシェア画像を重ねることにより QR コードの秘密画像を復号する手法を提案している。さらに2018年に Jiang ら[5]と Zhang ら[6]は、Ateniese ら[7]が提案した拡張視覚復号型秘密分散法を QR コードに適用した手法を提案している。Jiang らの手法では、XOR 演算を用いた拡張視覚復号型秘密分散法を QR コードに適用している。また、Zhang らは QR コードのデータ部分に着目し、OR 演算を用いた拡張視覚復号型秘密分散法を QR コードのデータ部分にのみ適応している。しかしながら、Jiang らの研究では、XOR を処理するための媒体が必要となってしまう、Zhang らの研究では、同じバージョンの QR コード同士にしか適用できないため汎用性がなくなってしまう。

そこで、本稿では、Cao らの手法を拡張し、視覚復号型秘密分散法ではなく拡張視覚復号型秘密分散法を用いることでそれぞれ別の情報が載った2枚の QR コードのシェア画像から秘密の QR コードを復元できる手法を提案する。従来手法では、シェア画像は白いピクセルと黒いピクセルがランダムに配置された砂嵐のような画像となるが、提案手法では、

シェア自身にも意味のあるデータを組み込むことが可能になる。

### 2. 準備









#### 2.1 秘密分散法

Shamirの提案した $(k, n)$  しきい値法とは、秘密情報を $n$ 個のシェアに分割し、 $n$ 個のうち任意の $k$ 個のシェアを集めることにより秘密情報を復元することができる手法であり、 $k-1$ 個のシェアからは元の秘密情報がまったく得られない。

#### 2.2 視覚復号型秘密分散法

視覚復号型秘密分散法では、画像データに秘密分散法を適用する。一般的な $(2,2)$ しきい値型視覚復号型秘密分散法の場合、秘密画像データの1ピクセルを4分割し、シェア画像を重ねたときにOR演算により、秘密画像データの元ピクセルが黒であったら四つの黒ピクセルになり、白であったら三つの黒ピクセルと一つの白ピクセルになるようにシェア画像を定めて濃淡差を表現している(表1)。 $(2,2)$ しきい値型視覚復号型秘密分散法の例を図1に示す。

表1  $(2,2)$ しきい値型視覚復号型秘密分散法のシェアの組み合わせ例

元の Pixel		
share1 Pixel		
share2 Pixel		
重ねた Pixel		

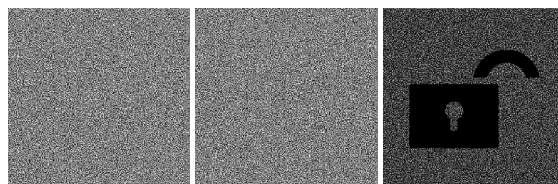


図1  $(2,2)$ しきい値型視覚復号型秘密分散法の例(左:シェア1, 中:シェア2, 右:復元画像)

一方、拡張視覚復号型秘密分散法は、シェア画像を重ねたときにOR演算により、秘密画像データの元ピクセルが黒であったら四つの黒ピクセルになり、白であったら三つの黒ピクセルと一つの白ピクセルになることは視覚復号型秘密分散法と同じであるが、シェア画像において、シェア画像に載せる画像データの元ピクセルが黒であったら三つの黒ピクセルと一つの白ピクセルになり、白であったら二つの黒ピクセルと二つの白ピクセルになるようにシェア画像のピクセルを定めている(表2)。これにより、シェア画像にも中間の濃淡差を用いて、黒ピクセルと白ピクセルを表現することができる。図2に(2,2)しきい値型拡張視覚復号型秘密分散法の例を示す。

表2 (2,2)しきい値型拡張視覚復号型秘密分散法のシェアの組み合わせ例

元のPixel		
share1 Pixel		
share2 Pixel		
重ねたPixel		

元のPixel		
share1 Pixel		
share2 Pixel		
重ねたPixel		



図2 (2,2)しきい値型拡張視覚復号型秘密分散法の例(左:シェア1,中:シェア2,右:復元画像)

### 2.3 QRコード

QRコードには、生成するQRコードを構成している四角い黒白の点であるセル数によって、バージョン1(21セル×21セル)から40(177セル×177セル)まで存在する。バージョンが高くなると縦横それぞれ4セルずつ増えていき、QRコードに埋め込める文字数が多くなる。また、QRコードにはそれぞれのバージョンに四つの誤り訂正能力のレベルがある。誤り訂正能力とは、QRコードの汚れなどによるノイズによって、誤った読み取りを行っても、その誤りを訂正して正しい情報を読み取ることができる能力である。

QRコードの誤り訂正能力は、誤り訂正能力7%のレベルL、誤り訂正能力15%のレベルM、誤り訂正能力25%のレベルQ、誤り訂正能力30%のレベルHの四つである。同じバージョンであったとしても選択する誤り訂正能力のレベルによって、QRコードに埋め込める文字数は変わり、Hが一番少なく、Lが一番多くの文字を埋め込める。本稿では、漢字36文字埋め込み可能なバージョン6でレベルHのQRコードを用いる。

### 3. 拡張視覚復号型秘密分散法のQRコードへの応用

#### 3.1 従来手法

Caoらの(2,2)しきい値型視覚復号型秘密分散法では、秘密画像の1ピクセルを16分割している。この手法では、表3に示すシェアの組み合わせにより、白ピクセルと黒ピクセルを分散している。また、Caoらは、シェア画像の白ピクセルと黒ピクセルの偏りをなくすためにシェアのピクセルパターンを減らし、さらに、復元画像を明るくするためにシェア画像を重ね合わせたときに白ピクセルになる組み合わせを同じピクセルパターンにしている。

表3 従来手法のシェアの組み合わせ

share1					
share2					Secret Pixel
					Secret Pixel

図3は、Caoらの手法を用いて作成したシェア画像である。図4は、図3の二つのシェア画像を重ねたときに復号された秘密画像と元の秘密画像である。

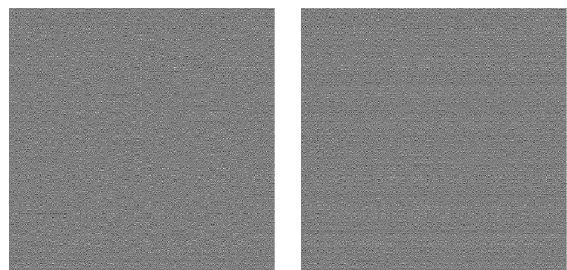


図3 従来手法でのシェア1(左), 2(右)

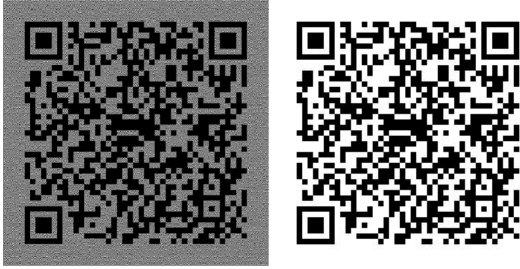


図4 復元画像(左)と元のQRコード画像(右)

### 3.2 提案手法

従来手法のシェアでは、二つのシェア画像から一つのQRコードを復元することができるが、シェア画像は白いピクセルと黒いピクセルがランダムに配置された砂嵐のような画像となり、シェア画像単体では意味のある画像にはなっていない。一方、本稿で提案する手法では、(2,2)しきい値型拡張視覚復号型秘密分散法で秘密画像の1ピクセルを4分割にしたシェアの組み合わせのピクセルパターン(表4)をQRコードに適用することで、シェア自身にも意味のあるデータを組み込むことが可能になる。このため、そのシェア画像が何のシェアであるのか示したり、それぞれのシェア画像に別々のQRコードの情報を載せたりすることで扱えるデータの量が今までよりも格段に多くなる。

提案手法では、二つの黒ピクセルと二つの白ピクセルから構成される白を表すピクセルと三つの黒ピクセルと一つの白ピクセルから構成される黒を表すピクセルを用いることで、シェア画像にも中間の濃淡差を用いることができ、シェア画像と復元画像の両方に黒ピクセルと白ピクセルを表現することができる。また、従来手法が秘密画像データの1ピクセルを16分割にしていたのに対して、提案手法では、1ピクセルを4分割にしている。これにより、ピクセルパターンに白ピクセルと黒ピクセルの偏りが少ないため、シェアのピクセルパターンを減らさずにシェアにランダム性を与えている。なお、復元画像を明るくするために従来手法をそのまま提案手法に適用すると、シェア画像を重ね合わせたときに白ピクセルになる組み合わせは同じピクセルパターンになるため、復号した際にシェア画像に載せている画像が透けて見えてしまうという問題があり、秘密画像のQRコードを読み取る際に透けたシェア画像のQRコードを読み取ってしまう可能性がある。そこで提案手法では、シェア画像を重ね合わせたときに白ピクセルになる組み合わせに同じピクセルパターンを用いない。

表4 拡張視覚復号型秘密分散法のシェアの組み合わせ

share1	share1 Pixel				share1 Pixel				Secret Pixel
	■	■	■	■	■	■	■	■	
share2	■	■	■	■	■	■	■	■	Secret Pixel
	■	■	■	■	■	■	■	■	Secret Pixel
	■	■	■	■	■	■	■	■	Secret Pixel
	■	■	■	■	■	■	■	■	Secret Pixel

### 4. 評価

図5のQRコードに提案手法を適用し、従来手法のQRコードと提案手法で生成したシェア画像と復元した秘密画像を株式会社デンソーウェーブが公式でリリースしているQRコードリーダーで読み込み、提案手法との読み取り精度の比較を行う。図6-8は、表4のシェアの組み合わせを実際に図5のQRコードに適用したシェア画像とその復元画像である。



図5 元のQRコード画像

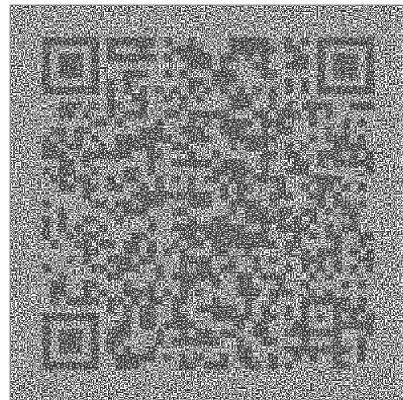


図6 提案手法のシェアのピクセルパターンで作成したシェア1

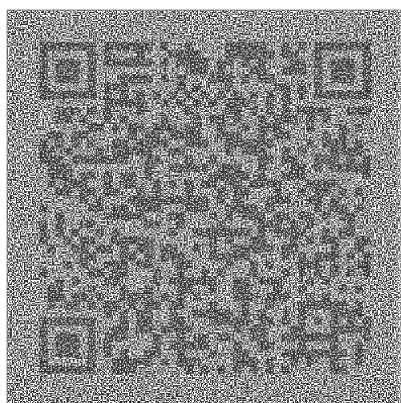


図7 提案手法のシェアのピクセルパターンで作成したシェア2

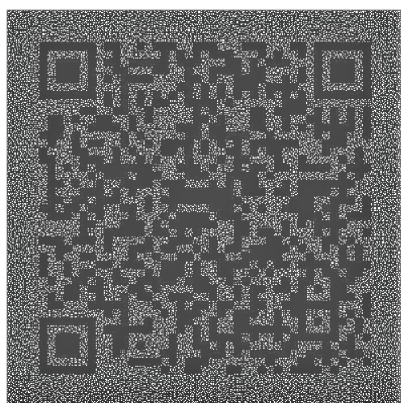


図8 提案手法のシェア1とシェア2を重ねたときの復元画像

提案手法とCaoらの手法のQRコードを実際にQRコードリーダーで読み込んでみた結果、どちらの手法でもQRコードを読み込むことに成功した。しかし、提案手法のシェアのQRコードでは、QRコードの濃さが薄く、認証に少し時間がかかってしまう場合があった。

また、今回用いたQRコードのピクセル数は $196 \times 196$ であったので、従来手法は秘密画像の1ピクセルを16分割しており、シェア画像は $784 \times 784$ ピクセルになるのに比べ、提案手法では1ピクセルを4分割しており、シェア画像は $392 \times 392$ ピクセルになる。そのため、同じ大きさの画像にした際に画像の滑らかさに差が生じ、従来手法に比べ提案手法のシェア画像と復元画像は荒くなってしまい、QRコードの読み取り精度が落ちてしまった。

## 5. まとめ

提案手法をQRコードに適用した場合、シェアの画像のQRコードをQRコードリーダーで読み込むことは可能であった。また、復元画像においてはシェア画像を重ねたときに白ピクセルになる個数によって復元画像の濃淡差が変化するため、その明るさを上げることによ

て読み取り精度が向上する。ただし、シェア画像や復元画像を明るくするために余計に濃淡差の階層を増やしてしまうとQRコードリーダーの読み取り精度が落ちてしまう。また、拡張視覚復号型秘密分散法では、シェアの画像との濃淡差を消すために視覚復号型秘密分散法ほど明るくすることはできない。これは、分割数を増やすことにより、シェアの取り得る組合せ数が増えるので改善される可能性がある。また、シェア画像のピクセル数も増えるため、同じ大きさの画像で比較した場合、分割数が多い方がシェア画像と復元画像は滑らかな画像になる。

今回は株式会社デンソーウェーブが開発したQRコードリーダーを用いて、誤り訂正能力が最大のQRコードを使用した。QRコードの誤り訂正能力を低くした場合の評価やスマートフォンなどに最初から入っているQRコードリーダーの場合でもスムーズにQRコードを読み取れるようにできるかが今後の課題である。

謝辞 本研究はJSPS科研費18K11303の助成を受けたものです。

## 参考文献

- [1] Adi Shamir, "How to share a secret," *Communications of the ACM*, vol.22, no.11, pp.612-613, 1979.
- [2] Moni Naor and Adi Shamir, "Visual Cryptography," *Lecture Notes in Computer Science* vol.950, pp.1-12, 1995.
- [3] JIS X 0510, "二次元コードシンボル—QRコード—基本仕様," 日本規格協会, 2004.
- [4] Xiaohe Cao, Liuping Feng, Peng Cao and Jianhua Hu, "Secure QR Code Scheme Based on Visual Cryptography," *Advances in Intelligent Systems Research*, vol.133, pp.433-436, 2016.
- [5] Yue Jiang, Yuliang Lu, Xuehu Yan, Lintao Liu, "Extended Secret Image Sharing with Lossless Recovery Based on Chinese Remainder Theorem and Quick Response Code," 2018 IEEE 3rd ICIVC, pp.678-683, 2018.
- [6] Xin Zhang, Jia Duan and Jiantao Zhou, "A Robust Secret Sharing QR Code via Texture Pattern Design," 2018 APSIPA ASC, pp.903-907, 2018.
- [7] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Extended capabilities for visual cryptography," *Theor. Comput. Sci.*, Vol.250, pp.143-161, 2001.