情報処理学会論文誌 Vol.62 No.9 1476–1486 (Sep. 2021)

QRコードへ適用可能な拡張視覚復号型秘密分散法

大川 直也[1] 栃窪 孝也[1,a)]

受付日 2020年11月30日, 採録日 2021年6月7日

概要：本論文では，視覚復号型秘密分散法において中間層の濃淡差を用いた拡張視覚復号型秘密分散法をQRコードへ適用する手法を提案する．従来手法には，読みだすことのできる情報量に制限があるものやシェア画像が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画像になってしまうという問題がある．一方，提案の $(2,2)$ しきい値拡張視覚復号型秘密分散法の場合，2枚のシェア画像を重ねることにより，秘密のQRコードを復元することができるとともに，2枚のシェア画像も砂嵐画像ではなく，それぞれ秘密のQRコードとは異なる別のQRコードを埋め込むことができる．さらに，これを拡張して $(2,3)$ しきい値拡張視覚復号型秘密分散法をQRコードに適用する手法も提案する．提案手法は，QRコードの誤り訂正能力を用いないため復元画像で読みだすことのできる情報量に制限がないのが特徴である．

キーワード：QRコード，秘密分散法，視覚復号型秘密分散法，拡張視覚復号型秘密分散法

Extended Visual Secret Sharing Schemes Applicable to QR Code

Naoya Okawa[1] Kouya Tochikubo[1,a)]

Received: November 30, 2020, Accepted: June 7, 2021

Abstract: In 2015, by using the error correction ability of QR codes Honjo and Koga proposed a visual secret sharing scheme for QR code. Their scheme can embed QR codes in both the recovered image and the share images. However, in their scheme the embedded secret information is about 10% of normal QR codes. In 2016, Cao, Feng, Cao and Hu proposed a visual secret sharing scheme for QR code. However, their scheme can only embed the secret QR code in the recovered image. In this paper, we propose extended visual secret sharing schemes for QR code. Our proposed schemes can embed the secret QR codes in the share images as well as the recovered image.

Keywords: QR code, secret sharing scheme, visual secret sharing scheme, extended visual secret sharing scheme

1. はじめに

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分からないが，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により，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．また，NaorとShamirは，シェア画像にも意味のある画像を載せることのできる拡張視覚復号型秘密分散法も同論文内で示唆している．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，2015年に本庄らのQRコードの誤り訂正能力を利用した手法がある [4]．本庄らの手法は，2枚のシェア画像を重ねると秘密のQRコードを復元することができるとともに，2枚のシェア画像も砂嵐画像ではなく，それぞれ秘密のQRコードとは異なる別のQRコードを埋め込むことが

[1] 日本大学
Nihon University, Narashino, Chiba 275–8575, Japan
[a)] tochikubo.kouya@nihon-u.ac.jp

できる．しかしながら，本庄らの手法ではシェア画像の黒いピクセル（セル）は 2 枚のシェア画像を重ねた復元画像においても黒いピクセルになってしまうため復元画像で読みだすことのできる情報は通常の QR コードの 10%程度となってしまう．また，2016 年に Cao ら [5] が提案した視覚復号型秘密分散法は 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元する手法であり，QR コードの誤り訂正能力を用いないため復元画像で読みだすことのできる情報量に制限がないが，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画像となってしまう．なお，本庄らの手法や Cao らの手法がシェア画像を重ねるという OR 演算により秘密画像を復元する視覚復号型秘密分散法であるのに対し，XOR 演算により秘密画像を復元する視覚復号型秘密分散法も提案されている [6], [7]．しかしながら，XOR 演算に基づく手法は，OR 演算に基づく手法とは異なり，シェア画像を重ねるだけでは復元画像を得ることができず，復元には追加の装置や処理が必要となる．したがって，本論文では復元に追加の装置や処理を必要としない OR 演算に基づく手法を対象とする．

本論文では，Cao らの手法を拡張し，視覚復号型秘密分散法ではなく QR コードの 1 ピクセルをさらに分割することで生じる中間層の濃淡差を用いた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．提案手法では，シェア自身にも意味のあるデータを埋め込むことが可能になる．しかし，この手法では，従来手法と同様に，しきい値法の利点の 1 つであるシェアを欠損しても復元可能であるという性質を利用することができない．そこで，本論文では，この手法を発展させ $(2,3)$ しきい値拡張視覚復号型秘密分散法を QR コードに適用する手法も提案する．Cao らの手法と同様に，提案も QR コードの誤り訂正能力を用いないため復元画像で読みだすことのできる情報量に制限がないのが特徴である．

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．

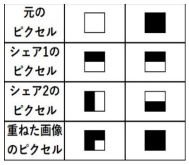
2.2 視覚復号型秘密分散法

Naor と Shamir が提案した視覚復号型秘密分散法では，1 枚の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，シェア画像は 2 個の黒ピクセルと 2 個の白ピクセルから構成されるピクセルパターンになり，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画像となる．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 4 個の黒ピクセルになり，白であったら 3 個の黒ピクセルと 1 個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**）．$(2,2)$ しきい値視覚復号型秘密分散法の例を**図 1**，**図 2**，**図 3** に示す．

一方，Ateniese ら [8] が提案した (k,k) しきい値拡張視覚復号型秘密分散法は，n 枚のシェアに載せる画像と 1 枚の秘密画像をピクセル単位で処理を行う．各ピクセルは，入力された $n+1$ 個のピクセル値から，n 枚の画像に対応する m 個の黒または白のピクセルパターンから構成されるシェア n 個に変換される．この白と黒のピクセルの割合によって，ピクセルの濃淡が実現される．このときのピクセルパターンを構成するピクセルの個数 m をピクセル拡大と呼ぶ．

$n=2$，$m=4$ の場合，シェア画像を重ねたときに OR

表 1 $(2,2)$ しきい値視覚復号型秘密分散法のシェアの組合せ例
Table 1 Example of $(2,2)$-VSSS share combination.



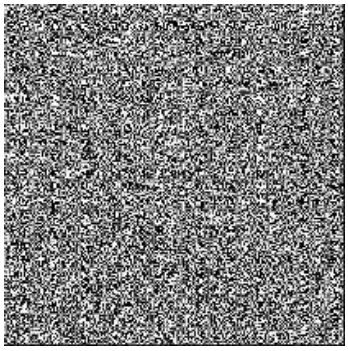


図 1 $(2,2)$ しきい値視覚復号型秘密分散法の例（シェア画像 1）
Fig. 1 Example of $(2,2)$-VSSS (share 1).

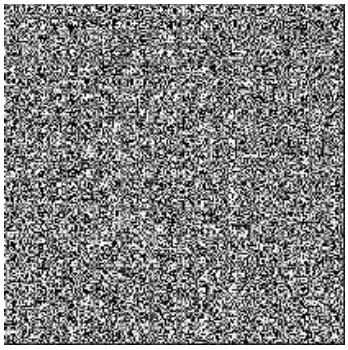


図 2 $(2,2)$ しきい値視覚復号型秘密分散法の例（シェア画像 2）
Fig. 2 Example of $(2,2)$-VSSS (share 2).

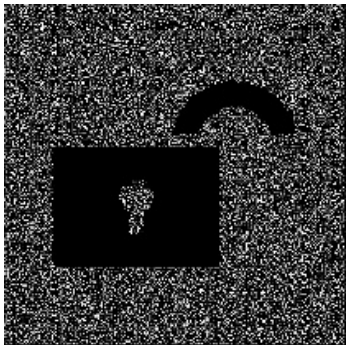


図 3 (2, 2) しきい値視覚復号型秘密分散法の例（シェア画像 1 とシェア画像 2 を重ねた復元画像）
Fig. 3 Example of (2, 2)-VSSS (recovered image).

表 2 (2, 2) しきい値拡張視覚復号型秘密分散法のシェアの組合せ例
Table 2 Example of (2, 2)-EVSSS share combination.

元のピクセル		□	■
シェア1のピクセル	□	▬	▬
シェア2のピクセル	□	◧	▬
重ねた画像のピクセル		◧	■

元のピクセル		□	■
シェア1のピクセル	■	◧	◧
シェア2のピクセル	□	▬	▬
重ねた画像のピクセル		◧	■

元のピクセル		□	■
シェア1のピクセル	■	◧	◧
シェア2のピクセル	□	▬	▬
重ねた画像のピクセル		◧	■

元のピクセル		□	■
シェア1のピクセル	□	▬	▬
シェア2のピクセル	■	◧	◧
重ねた画像のピクセル		◧	■

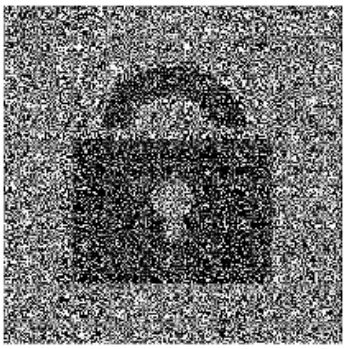


図 4 (2, 2) しきい値拡張視覚復号型秘密分散法の例（シェア画像 1）
Fig. 4 Example of (2, 2)-EVSSS (share 1).

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 4 個の黒ピクセルになり，白であったら 3 個の黒ピクセルと 1 個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 3 個の黒ピクセルと 1 個の白ピクセルになり，白であったら 2 個の黒ピクセルと 2 個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 4**，**図 5**，**図 6** に (2, 2) しきい値拡張視覚復号型秘密分散法の例を示す．

図 5 (2, 2) しきい値拡張視覚復号型秘密分散法の例（シェア画像 2）
Fig. 5 Example of (2, 2)-EVSSS (share 2).

図 6 (2, 2) しきい値拡張視覚復号型秘密分散法の例（シェア画像 1 とシェア画像 2 を重ねた復元画像）
Fig. 6 Example of (2, 2)-EVSSS (recovered image).

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 1 つ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 4 個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読み取りで誤りが生じても，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 4 種である．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 コードに埋め込むことができる文字数は変わり，H が一番少なく，L が一番多くの文字を埋め込むことができる．本論文では，標準として漢字 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．

バージョン 6 の QR コードにおいて共通している構造を**図 7** に示す．切り出しシンボルは，QR コードの 3 個のコーナーに配置することで，シンボルの位置や大きさ，

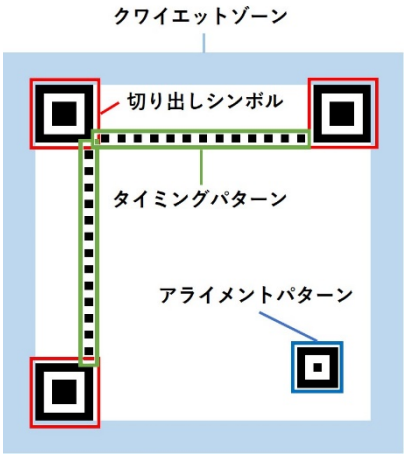


図 7 バージョン 6 の QR コードの共通構造
Fig. 7 QR code Common Structure (Ver. 6).

傾きなどを検出するためのパターンである．タイミングパターンは，白セルと黒セルが交互に配置された，シンボル内のモジュール座標を決定するためのパターンである．アライメントパターンは，歪みによって生じる各セルの位置ずれを補正するためのパターンである．クワイエットゾーンはセルで構成された正方形のコードの周囲の空白部分である．切り出しシンボルを最初に検索することで QR コードの位置を 360° どの方向からでも認識することができ，高速な読み取りを可能にしている．

3. (2, 2) しきい値拡張視覚復号型秘密分散法の QR コードへの適用

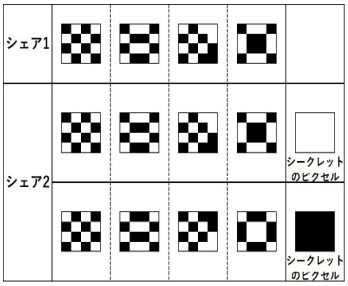
3.1 従来手法

Cao らの (2, 2) しきい値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** に示すシェアの組合せにより，白ピクセルと黒ピクセルを分散させている．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合せを同じピクセルパターンにしている．なお，表 3 のシークレットのピクセルは秘密画像の元々のピクセルが黒であったのか，白であったのかを表すとともに，シェア 1 とシェア 2 のピクセルパターンを重ねたときに白ピクセルか黒ピクセルかのどちらに復元されるのかを示している．

図 8 は，Cao らの手法を用いて作成したシェア画像と元の秘密画像である．**図 9** は，図 8 の 2 個のシェア画像を重ねたときに復元された秘密画像である．Cao らの手法を用いて復元した QR コードの画像は，白を 8 個の白ピクセルと 8 個の黒ピクセル，黒を 16 個の黒ピクセルで表現している．

シェア画像を重ねたときに OR 演算により秘密画像を復元する視覚復号型秘密分散法ではないが，関連研究として

表 3 従来手法のシェアの組合せ
Table 3 Combination of shares of the previous scheme.



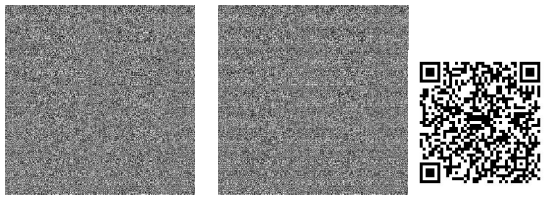


図 8 従来手法のシェア画像 1 (左)，2 (中)，秘密の QR コード (右)
Fig. 8 Share 1 (Left), 2 (Center) of the previous scheme and Original QR code (Right).

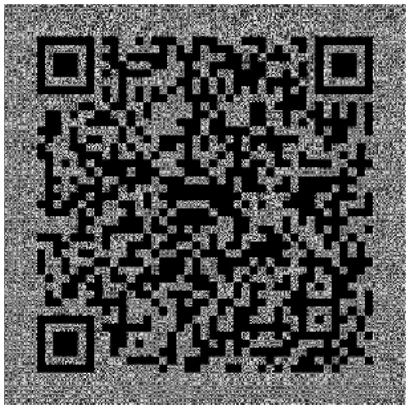


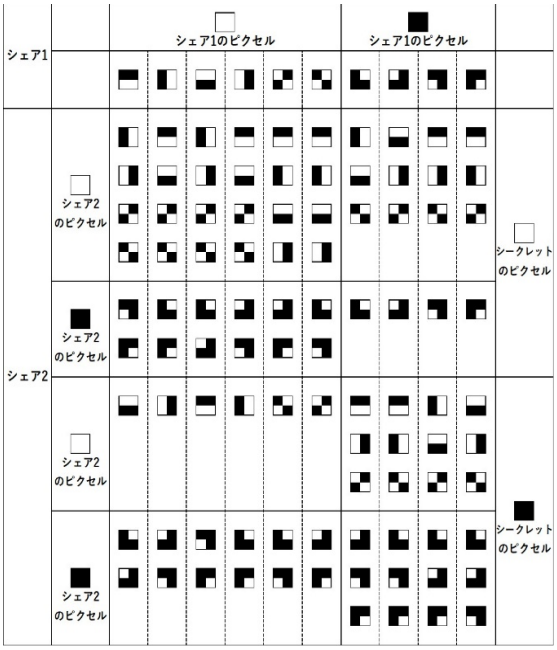
図 9 従来手法のシェアを重ねた復元画像
Fig. 9 Recovered image of the previous scheme.

Jiang らの手法 [6] や Zhang らの手法 [7] がある．Jiang らの手法では，XOR 演算を用いた画像に対する秘密分散法を QR コードに適用している．また，Zhang らは，QR コードのクワイエットゾーン，タイミングパターン，アライメントパターン，左下の切り出しシンボル，右上の切り出しシンボル以外のデータ部分と左上の切り出しシンボルに対して，秘密分散法をピクセル単位ではなく，QR コードのセル単位でパターンの置き換えを用いて適用している．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い，Zhang らの研究では，秘密画像を復元するために 2 枚のシェアのデータから再度パターンを読み込み，さらに，パターンを置き換える処理を行わなければならない．

3.2 提案手法

従来手法のシェア画像では，2 枚のシェア画像から 1 個

表 4 提案手法 1 の拡張視覚復号型秘密分散法のシェアの組合せ
Table 4 Combination of shares of the proposed scheme 1.



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，本論文で提案する手法 1 では，Ateniese らの拡張視覚復号型秘密分散法を QR コードに適用させ，秘密画像の 1 ピクセルを 4 分割にしたシェアの組合せのピクセルパターンを 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（**表 4**）．したがって，提案手法では，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いままでよりも格段に多くなる．なお，表 4 のシェア 1 のピクセル，シェア 2 のピクセルとはシェア画像に載せる画像の元々のピクセルが黒であったか，白であったのかを示している．

提案手法 1 では，秘密画像の 1 ピクセルを 4 分割にしているので，シェア画像と復元画像において濃淡差が小さくなってしまう．そこで，シェア画像と復元画像が明るくなるように改良したものが提案手法 2 である．提案手法 1 では，秘密画像の 1 ピクセルを 4 分割し，2 個の黒ピクセルと 2 個の白ピクセルから構成される白を表すピクセルと 3 個の黒ピクセルと 1 個の白ピクセルから構成される黒を表すピクセルをシェア画像において用いているが，提案手法 2 では，秘密画像 1 ピクセルを 16 分割し，6 個の黒ピクセルと 10 個の白ピクセルから構成される白を表すピクセルと 9 個の黒ピクセルと 7 個の白ピクセルから構成される黒を表すピクセルをシェア画像で用いるように変更している（**表 5**）．また，提案手法 2 では，シェア画像の黒ピクセルを表現するピクセルパターンを重ね合わせたときに復元

表 5 提案手法 2 の拡張視覚復号型秘密分散法のシェアの組合せ
Table 5 Combination of shares of the proposed scheme 2.

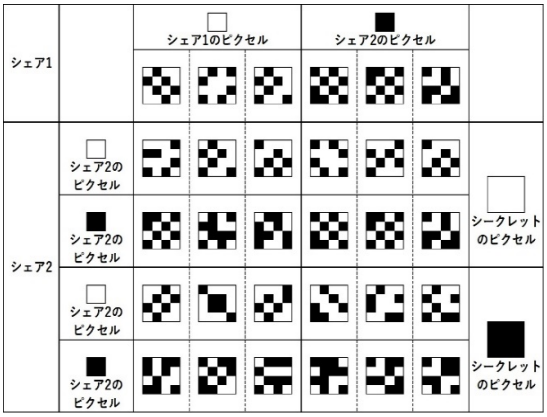


図 10 元の QR コード画像
Fig. 10 Original QR codes.

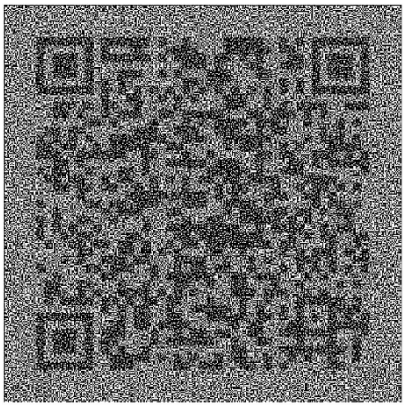


図 11 提案手法 1 のシェア画像 1
Fig. 11 Share 1 of the proposed scheme 1.

画像で白ピクセルになる組合せを共通にすることにより，Cao らの手法が復元画像を明るくするために行っていたように復元画像を明るくすることが可能となる．さらに，復元画像を明るくするために復元画像の黒ピクセルを表現するピクセルパターンを 16 個の黒ピクセルから構成されるピクセルパターンから 4 個の白ピクセルと 12 個の黒ピクセルから構成されるピクセルパターンにし，復元画像も中間の濃淡差を用いて表現している．

図 10 の QR コードは，すべて同じバージョン 6 の QR コードである．**図 11**，**図 12** は，図 10 の QR コードを提案手法 1 に適用した場合のシェア画像と復元画像である．また，**図 13**，**図 14** は，図 10 の QR コードを提案手法 2 に適用した場合のシェア画像と復元画像である．

さらに，Zhang らの手法のように QR コードのセルで共

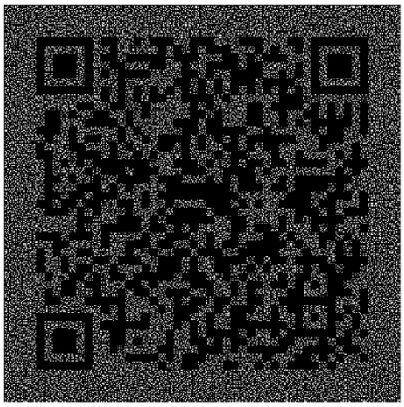


図 12 提案手法 1 のシェア画像 1 とシェア画像 2 を重ねたときの復元画像
Fig. 12 Recovered image of the proposed scheme 1.

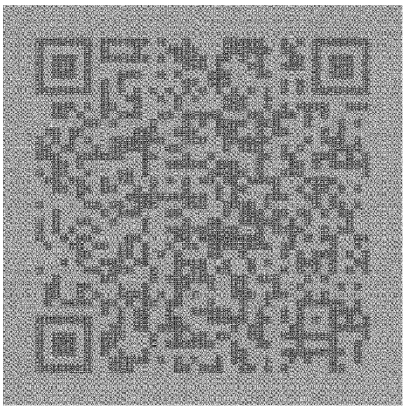


図 13 提案手法 2 のシェア画像 1
Fig. 13 Share 1 of the proposed scheme 2.

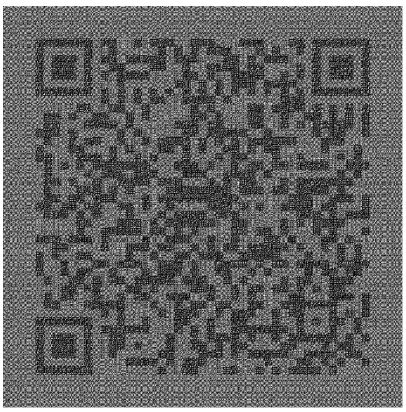


図 14 提案手法 2 のシェア画像 1 とシェア画像 2 を重ねたときの復元画像
Fig. 14 Recovered image of the proposed scheme 2.

通になっている切り出しシンボル，アライメントパターン，タイミングパターン，クワイエットゾーンはそのままにし，それ以外のデータ部分に提案手法 2 を適用したものを提案手法 3 とする．**図 15**，**図 16** は，図 10 の QR コードを提案手法 3 に適用した場合のシェア画像と復元画像である．

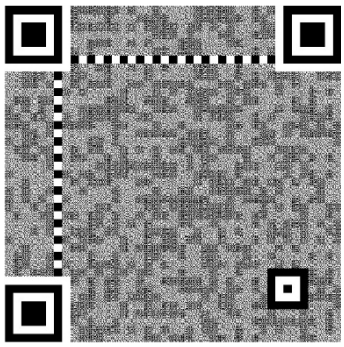


図 15 提案手法 3 のシェア画像 1
Fig. 15 Share 1 of the proposed scheme 3.

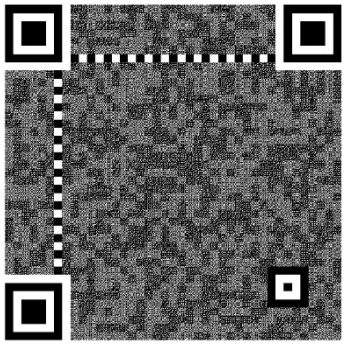


図 16 提案手法 3 のシェア画像 1 とシェア画像 2 を重ねたときの復元画像
Fig. 16 Recovered image of the proposed scheme 3.

3.3 評価方法

iPhone 8 を用いて 5 種の QR コードリーダで紙に印刷した 53 mm × 53 mm の QR コードを読み取る．復元画像は，OHP シートに印刷したシェア画像を重ねたものではなく，PC 上でシェア画像を重ねて復元したものを復元画像とした．生成したシェア画像と復元した秘密画像の QR コードを読み取るために使用する 5 種の QR コードリーダは，株式会社デンソーウェーブが公式でリリースしているアプリケーションクルクル [9]，LINE 株式会社がリリースしているアプリケーション LINE [10]，Twitter 株式会社がリリースしているアプリケーション Twitter [11]，Apple 製品に標準でインストールされているアプリケーションカメラ [12]，Google LLC がリリースしているアプリケーション Chrome [13] である．

5 つの QR コードリーダを用いてそれぞれの手法のシェア画像および復元画像の QR コードの読み取りを黒い机の上で 10 回ずつ行い，何回読み取ることに成功したのかで評価した．1 回の読み取り時間は 30 秒未満とし，30 秒以上かかった場合は失敗とする．

3.4 読み取り精度評価

Cao らの手法と提案手法 1–3 の復元した秘密画像の QR コードや提案手法 1–3 のシェア画像上に載せられた QR コードの読み取り精度にどの程度の差が生じるのかの比較

表 6 提案の (2,2) しきい値拡張視覚復号型秘密分散法の読み取り精度の比較

Table 6 Comparison of read errors for the proposed (2,2)-EVSSS's.

画像	クルクル	LINE	Twitter	Apple	Chrome
Cao らの手法の復元	100%	100%	100%	100%	100%
提案手法 1 シェア 1	100%	90%	100%	90%	80%
提案手法 1 シェア 2	100%	80%	90%	80%	100%
提案手法 1 復元	100%	70%	80%	80%	80%
提案手法 2 シェア 1	100%	100%	100%	100%	100%
提案手法 2 シェア 2	100%	100%	100%	100%	100%
提案手法 2 復元	100%	100%	100%	100%	100%
提案手法 3 シェア 1	70%	70%	70%	40%	80%
提案手法 3 シェア 2	80%	70%	90%	50%	70%
提案手法 3 復元	80%	50%	70%	50%	80%

を行うため，Cao らの手法で生成したシェア画像を復元した秘密画像の QR コード，提案手法 1–3 を QR コードに適用して生成したシェア画像と復元した秘密画像の QR コードを用いて読み取り精度の評価を行った．**表 6** に 3.3 節の評価方法を用いて QR コードの読み取りを行った結果を示す．

Cao らの手法，提案手法 1，提案手法 2 のシェア画像，および復元画像の QR コードを実際に QR コードリーダで読み込んでみた結果，クルクル，LINE，Chrome，Twitter，Apple 標準の 5 種すべての QR コードリーダで，どの手法でも QR コードを読み取ることに成功した．しかし，LINE，Chrome，Twitter，Apple 標準の 4 種の QR コードリーダでは，提案手法 1 は少し読み取ることができなかった．また，QR コードを読み取る際に QR コードが置かれている場所の色が黒色である方がシェア画像と復元画像の QR コードの濃淡差の認識しやすいことが分かった．

提案手法 1 と Cao らの手法を比べてみると，クルクルでは同じ精度で読み取ることができたが，シェア画像と復元画像が暗いため，他の QR コードリーダでは少し低い読み取り精度になってしまった．

提案手法 2 と Cao らの手法を比べてみると，クルクル，LINE，Chrome，Twitter，Apple 標準の 5 種すべての QR コードリーダで，Cao らの手法と同じ読み取り精度であった．提案手法 2 のシェアの QR コードでは，QR コードの濃淡差が薄く，読み取りに少し時間がかかってしまう場合があった．

提案手法 1 と提案手法 2 を比べてみると，LINE, Chrome, Twitter，Apple 標準の 4 種の QR コードリーダで，提案手法 2 で作成したシェア画像と復元画像の QR コードの読み取り精度が向上した．これは，提案手法 1 に比べて提案手法 2 のシェア画像と復元画像が明るくなったことと，1 ピクセルを 4 分割していたものから 16 分割にしたことにより画像の滑らかさが向上し，黒セルと白セルの識別がしやすくなったことが主因だと考えられる．また，提案手法 1 と提案手法 2 のシェア画像，および復元画像での読み取り精度はそこまで差はないが，QR コードの読み取りに時間においては，提案手法 1 よりも提案手法 2 の方が素早く読み取ることが可能であった．

提案手法 3 と QR コード全体に適用した他の提案手法と比べ，シェア画像と復元画像が QR コードであると認識する認識精度は向上したが，読み取り精度自体は落ちてしまった．特に，LINE，Apple 標準の 2 種では，シェア画像と復元画像の読み取り精度が顕著に落ちてしまった．これは，画像内に純粋な黒と白が存在するためシェア画像と復元画像の濃淡差よりもその黒と白の濃淡差を読み取ってしまい QR コードであることは認識してもそれ以外のデータ部分において，黒セルと白セルをうまく認識することができなくなってしまったことが主因であると考えられる．

4. (2,3) しきい値拡張視覚復号型秘密分散法の QR コードへの適用

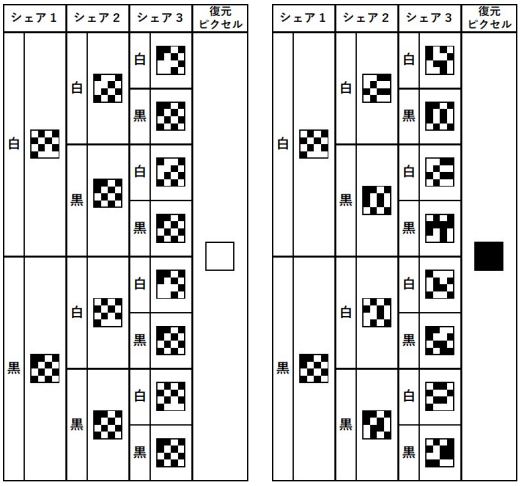
4.1 提案手法

(2,2) しきい値法の提案手法 2 では，シェア画像の白を黒 6 白 10，黒を黒 9 白 7 で表現し，復元画像の白を黒 9 白 7，黒を黒 12 白 4 で表現しており，白と黒の濃淡差がどちらも 3 になっている．しかし，このように秘密画像の 1 ピクセルを 16 分割にし，シェア画像と復元画像を中間の濃淡差を用いて (2,3) しきい値拡張視覚復号型秘密分散法を実現した場合，最大にとれる白と黒の濃淡差は，シェア画像 2・復元画像 3 か，シェア画像 3・復元画像 2 である．そして，この 2 つの濃淡差の場合をそれぞれ提案手法として実現した．

提案手法 4 では，濃淡差をシェア画像 2・復元画像 3 とし，シェア画像では 7 個の黒ピクセルと 9 個の白ピクセルから構成される白を表現するピクセルパターンと 9 個の黒ピクセルと 7 個の白ピクセルから構成される黒を表現する

表 7 復元されるシェアの組合せ（提案手法 4）（左：白復元，右：黒復元）

Table 7 Combination of shares of the proposed scheme 4 (Left: White pixel, Right: Black pixel).



ピクセルパターンを用い，復元画像では 9 個の黒ピクセルと 7 個の白ピクセルから構成される白を表現するピクセルパターンと 12 個の黒ピクセルと 4 個の白ピクセルから構成される黒を表現するピクセルパターンを用いる．

表 7 に提案手法 4 の白と黒に復元されるシェアの組合せの 1 つの例を示す．

提案手法 5 では，濃淡差をシェア画像 3・復元画像 2 とし，シェア画像では 7 個の黒ピクセルと 9 個の白ピクセルから構成される白を表現するピクセルパターンと 10 個の黒ピクセルと 6 個の白ピクセルから構成される黒を表現するピクセルパターンを用い，復元画像では 10 個の黒ピクセルと 6 個の白ピクセルから構成される白を表現するピクセルパターンと 12 個の黒ピクセルと 4 個の白ピクセルから構成される黒を表現するピクセルパターンを用いる．

表 8 に提案手法 5 の白と黒に復元されるシェアの組合せの 1 つの例を示す．

4.2 読み取り精度評価

提案手法 4 と提案手法 5 のシェア画像，および復元画像の QR コードが読み取り可能であるのか，濃淡差の違いによる読み取り精度の変化があるのかについての評価を 3.3 節の評価方法を用いて行った．

図 17 は使用する QR コード，**図 18**，**図 19**，**図 20**，**図 21**，**図 22**，**図 23** は提案手法 4 を適用したシェア画像と復元画像，**図 24**，**図 25**，**図 26**，**図 27**，**図 28**，**図 29** は提案手法 5 を適用したシェア画像と復元画像を示している．

表 9 に QR コードリーダで読み取った読み取り精度の結果を示す．

表 9 の結果から，提案手法 4 ならびに提案手法 5 のシェア画像と復元画像の QR コードを 5 つの QR コードリーダを用いて読み取ることは可能であった．

表 8 復元されるシェアの組合せ（提案手法 5）（左：白復元，右：黒復元）

Table 8 Combination of shares of the proposed scheme 5 (Left: White pixel, Right: Black pixel).

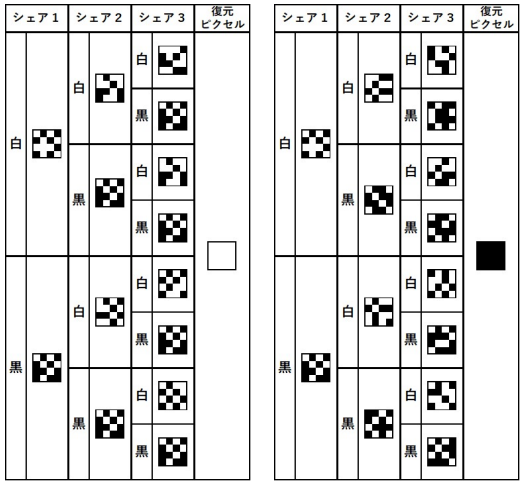


図 17 使用する QR コード

Fig. 17 Embedded QR codes

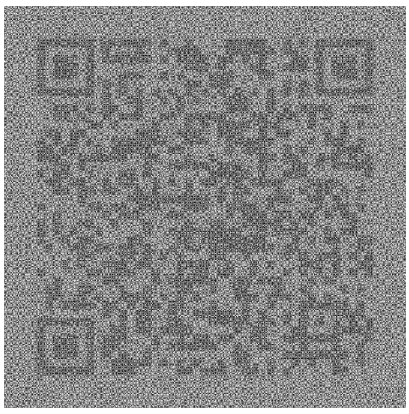


図 18 シェア画像 1（提案手法 4）

Fig. 18 Share 1 of the proposed scheme 4.

シェア画像を比べた場合，シェア画像の濃淡差は提案手法 4 では 2 であり，提案手法 5 では 3 であったので，提案

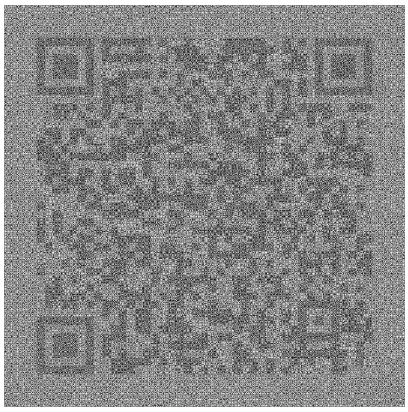


図 19 シェア画像 2（提案手法 4）
Fig. 19 Share 2 of the proposed scheme 4.

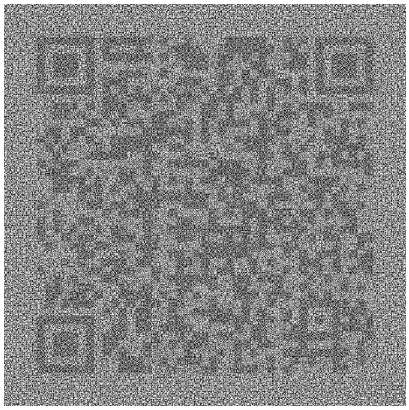


図 20 シェア画像 3（提案手法 4）
Fig. 20 Share 3 of the proposed scheme 4.

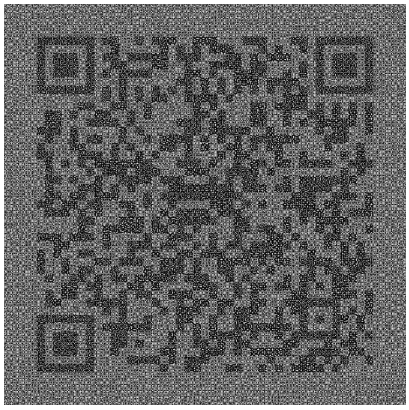


図 21 復元画像 1+2（提案手法 4）
Fig. 21 Recovered image of the proposed scheme 4 (share 1+2).

手法 4 のシェア画像はクルクル以外の QR コードリーダではシェア画像 2 を除いてほとんど読み取ることができず，提案手法 5 のシェア画像はほぼ完全に QR コードを読み取ることに成功した．しかし，提案手法 4 のシェア画像 2 では LINE，Twitter，Chrome で 80%読み取れているので，使用するピクセルパターンの組合せによっては，他のシェア画像でも読み取り精度が向上する可能性がある．

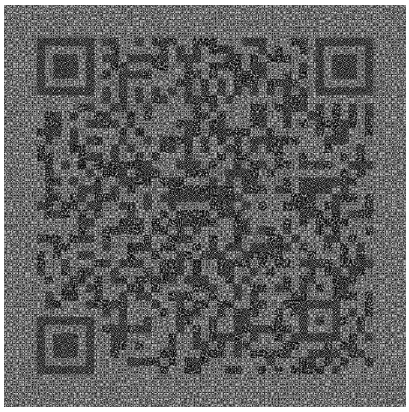


図 22 復元画像 1+3（提案手法 4）
Fig. 22 Recovered image of the proposed scheme 4 (share 1+3).

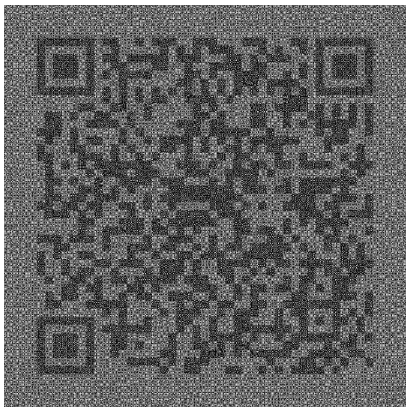


図 23 復元画像 2+3（提案手法 4）
Fig. 23 Recovered image of the proposed scheme 4 (share 2+3).

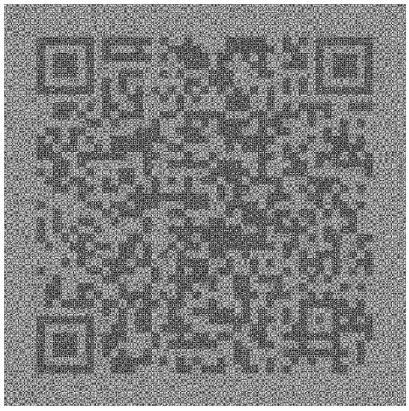


図 24 シェア画像 1（提案手法 5）
Fig. 24 Share 1 of the proposed scheme 5.

復元画像を比べた場合，復元画像の濃淡差は提案手法 4 では 3 であり，提案手法 5 では 2 であったので，提案手法 4 の方が読み取り精度が上ではあったが，提案手法 5 でもシェア 1 とシェア 3 を重ねた復元画像（以降，復元画像 1+3）以外はほぼ完全に読み取れており，復元画像ではシェア画像ほどの読み取り精度の差がでなかった．生成し

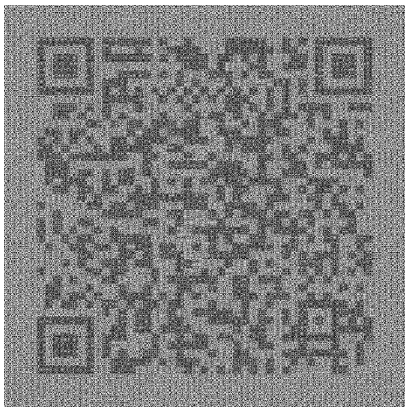


図 25 シェア画像 2（提案手法 5）
Fig. 25 Share 2 of the proposed scheme 5.

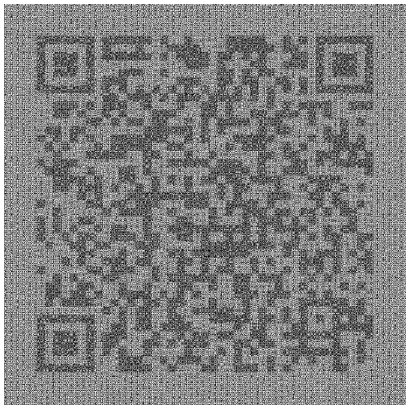


図 26 シェア画像 3（提案手法 5）
Fig. 26 Share 3 of the proposed scheme 5.

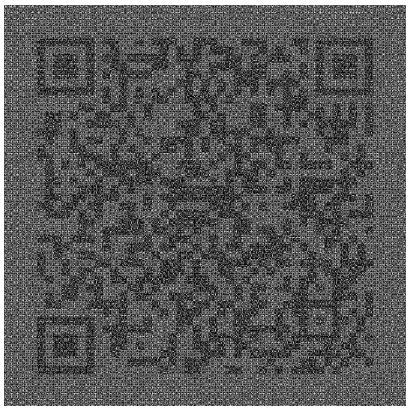


図 27 復元画像 1+2（提案手法 5）
Fig. 27 Recovered image of the proposed scheme 5 (share 1+2).

た 10 枚の復元画像 1+3 とほかの復元画像の画像を見比べてみると，復元画像 1+3 の黒を表現するピクセルパターンのランダム性が低く黒が連続してしまっており，それにより濃淡差を最大限使用することができていなかったため読み取り精度が落ちてしまったと考えられる．

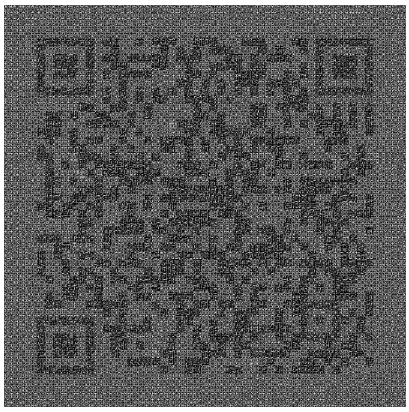


図 28 復元画像 1+3（提案手法 5）
Fig. 28 Recovered image of the proposed scheme 5 (share 1+3).

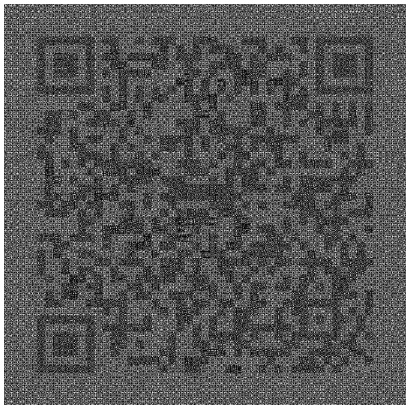


図 29 復元画像 2+3（提案手法 5）
Fig. 29 Recovered image of the proposed scheme 5 (share 2+3).

5. まとめ

本論文では，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ならびに，(2, 3) しきい値拡張視覚復号型秘密分散法を QR コードに適用する手法を提案した．従来手法を QR コードに適用した場合，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画像になってしまう．一方，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．

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 コードリーダで読み取る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って読み取り精度が向上することを明らかにした．

表 9 提案の (2,3) しきい値拡張視覚復号型秘密分散法の読み取り精度の比較

Table 9 Comparison of read errors for the proposed (2,3)-EVSSS's.

画像	クルクル	LINE	Twitter	Apple	Chrome
提案手法 4 シェア 1	100%	20%	40%	20%	10%
提案手法 4 シェア 2	100%	80%	80%	40%	80%
提案手法 4 シェア 3	100%	20%	30%	30%	10%
提案手法 4 復元 1+2	100%	100%	100%	100%	100%
提案手法 4 復元 1+3	100%	100%	100%	100%	100%
提案手法 4 復元 2+3	100%	100%	100%	100%	100%
提案手法 5 シェア 1	100%	100%	100%	100%	100%
提案手法 5 シェア 2	100%	100%	100%	100%	100%
提案手法 5 シェア 3	100%	100%	100%	90%	100%
提案手法 5 復元 1+2	100%	100%	100%	70%	100%
提案手法 5 復元 1+3	100%	40%	50%	40%	60%
提案手法 5 復元 2+3	100%	100%	100%	80%	100%

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] Shamir, A.: How to share a secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).
[2] Naor, M. and Shamir, A.: Visual cryptography, LNCS, 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] 本庄俊太郎, 古賀 弘：2 枚の二次元コードを用いた秘密分散法の一実現法, 電子情報通信学会論文誌 A, Vol.J98-A, No.2, pp.221–231 (2015).
[5] Cao, X., Feng, L., Cao, P. and Hu, J.: Secure QR code scheme based on visual cryptography, *AISR*, Vol.133, pp.433–436 (2016).
[6] Yue Jiang, Y., Lu, Y., Yan, X. and Liu, L.: Extended secret image sharing with lossless recovery based on chinese remainder theorem and quick response code, *2018 IEEE 3rd ICIVC*, pp.678–683 (2018).
[7] Zhang, X., Duan, J. and Zhou, J.: A robust secret sharing QR code via texture pattern design, *2018 APSIPA ASC*, pp.903–907 (2018).
[8] Ateniese, G., Blundo, C., Santis, A. and Stinson, D.: Extended capabilities for visual cryptography, *Theor. Comput. Sci.*, Vol.250, pp.143–161 (2001).
[9] クルクル-QR コードリーダ, 入手先 ⟨https://apps.apple.com/jp/app/qrkodorida-q-wu-liaode-shieru/id911719423⟩ (参照 2020-11-25).
[10] LINE, available from ⟨https://apps.apple.com/jp/app/line/id443904275⟩ (accessed 2020-11-25).
[11] Twitter, available from ⟨https://apps.apple.com/jp/app/twitter/id333903271⟩ (accessed 2020-11-25).
[12] Apple 標準アプリケーションカメラ, 入手先 ⟨https://support.apple.com/ja-jp/HT208843⟩ (参照 2020-11-25).
[13] Chrome – Google のウェブブラウザ, 入手先 ⟨https://apps.apple.com/jp/app/google-chrome-ウェブブラウザ/id535886823⟩ (参照 2020-11-25).

大川 直也

2020 年日本大学生産工学部数理情報工学科卒業. 現在, 情報セキュリティの研究に従事.

栃窪 孝也 (正会員)

1996 年東京理科大学理学部応用数学科卒業. 1998 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了. 2004 年東京工業大学大学院理工学研究科集積システム専攻博士後期課程修了. 1998 年東芝入社. 2006 年日本大学生産工学部数理情報工学科専任講師. 2012 年 Waterloo 大学客員教授. 現在, 日本大学生産工学部数理情報工学科教授. 情報理論・情報セキュリティの研究に従事. 2005 電子情報通信学会論文賞受賞.