161B15
2016/3/2

カメラ付き携帯情報端末を用いた復号を目的とした自己復号型ランダムグリッド

二上 尚文[1]　生源寺 類[1,a)]

概要：我々は単一のランダムグリッドから秘密画像の復号が可能な，自己復号型ランダムグリッドを提案している．自己復号型ランダムグリッドは，従来のランダムグリッドと同様に物理的な復号が可能である．例えば，透明フィルムなどに複製した自己復号型ランダムグリッドを，位置をずらして重ね合わせることで秘密画像を復号することができる．本稿では，スマートフォンなどのカメラ付き携帯情報端末を用いた復号について報告する．カメラ付き携帯情報端末を用いることで，物理的な復号におけるアナログ感を残した自由度の高いインタラクティブな復号が可能になる．

Self-Decodable Random Grid for Decoding with a Smart Phone

Naofumi Futagami[1]　Rui Shogenji[1,a)]

Abstract: We propose a self-decodable random grid which can be decrypted from a single random grid. The self-decodable random grids can decrypt physically. The secret image is decoded by superimposing copies of the self-decodable random grid at the certain position. In this paper, decoding self-decodable random grids using a smart phone with camera is demonstrated. The experimental results show validity of our proposed method.

1. はじめに

ランダムパターンに復号用のランダムパターンを重ね合わせることで，秘密画像が復号される視覚暗号技術としてランダムグリッド（Random grids）[1] が提案されている．復号用のランダムパターンを透明フィルムなどに印刷することで，ソフトウェアによる復号演算を行うことなく物理的に秘密画像の復号が可能である．一方，復号時にランダムパターンを重ね合わせる位置が 1 画素でもずれると秘密画像は復号されない．これは暗号として非常にセキュアであると言える反面，物理的な復号を行う上では精細な位置合わせが要求され復号の簡便性は低くなる．

ランダムグリッドと同様に物理的な復号が可能な潜像技術として，周期的なパターンが印刷された透明フィルムを重ね合わせることで秘密画像が浮かび上がるキャリアスクリーン画像（Carrier-screen images）がある [2]．復号に用いる周期的なパターンはキャリアスクリーンと呼ばれ，多数の平行線で構成される万線や周期的な点で構成される網点などがよく用いられる．このキャリアスクリーンの一部の周期や角度などを変調することで秘密画像が符号化される．キャリアスクリーン画像は，キャリアスクリーンの重ね合わせの他に，サンプリング処理による復号も可能である．そのため，有価証券等に印刷される複写牽制パターンとして利用されている．さらに偽造防止技術以外の用途として，その視覚的な復号から絵本 [3], [4] などのエンタテインメント分野でも利用されている．

我々はキャリアスクリーンとしてチェッカパターンを用いた，チェッカパターンキャリアスクリーン画像 [5] を提案している．チェッカパターンをキャリアスクリーンとして用いることで，生成されるキャリアスクリーン画像は正方画素構造となるため，従来の画像処理手法との整合性が良く，これまでに解像度多重化 [6] や角度多重化 [7]，自然画像への埋め込み手法 [8]，パターン投影による撮影防止

[1] 静岡大学 大学院工学研究科
Shizuoka University, Hamamatsu, Shizuoka 432–8561, Japan
[a)] shogenji.rui@shizuoka.ac.jp

手法 [9] を提案している．また，サンプリング処理による復号の一例として，市販のコンパクトデジタルカメラを用いた復号手法を提案している．デジタルカメラを用いた復号手法では，デジタルカメラの液晶モニタへの表示処理におけるサンプリング処理を復号に利用している．すなわちデジタルカメラをキャリアスクリーン画像に向け，撮影距離，カメラの角度を調節することで，デジタルカメラの液晶モニタ上に復号された秘密画像が浮かび上がる．一方，デジタルカメラを用いた復号において，よりコントラストの高い復号結果を得るためには，できるだけ鮮明にキャリアスクリーン画像をイメージセンサ上に結像させる必要がある．そのため従来のキャリアスクリーン画像と比較して，低解像度でキャリアスクリーン画像を出力することが望ましい．しかしながら，低解像度でキャリアスクリーン画像を出力した場合，秘密画像の露見が問題となり潜在化処理が必須である．これまでに誤差拡散法による潜在化手法を提案 [10], [11] している．誤差拡散法による潜在化は，階調の調整およびハーフトーン処理による単純な処理ではあるが，良好な潜在化効果が得られている．しかしながら秘密画像のエッジ部分において白画素と黒画素との密度に差が生じるため，完全な秘匿は困難である．また，復号をコンパクトデジタルカメラの液晶モニタへの表示処理を利用して行なっているため，機種依存を回避することは難しく一部の機種では秘密画像を復号することができない．

本研究では，カメラ付き携帯情報端末を用いた復号が可能な潜像技術として，ランダムグリッドの秘匿性とキャリアスクリーン画像の簡便な復号とを合わせ持つ自己復号型ランダムグリッドを提案する．特に近年，コンパクトデジタルカメラに変わり，スマートフォンなどのカメラ付き携帯情報端末が急速に普及している．カメラ付き携帯情報端末を用いることで，復号用のアプリケーションの開発が可能であり，デジタルカメラの機種依存性の問題を解決することができる．本報告では，スマートフォン用の復号アプリケーションを作成し，復号実験を行い提案手法の有用性を示す．

2. 自己復号型ランダムグリッド

2.1 生成手法

自己復号型ランダムグリッドでは，自己復号型ランダムグリッドを複製し，位置をずらして重ね合わせることで秘密画像が復号される．複製する枚数や重ね合わせ位置（復号移動量）が暗号鍵となる．すなわち，自己復号型ランダムグリッドは，その一部を復号するための暗号鍵を，自身の別の位置に有するランダムグリッドである．また，スマートフォンなどのアプリケーションを用いた復号を想定しているため，重ね合わせにおける演算にも任意の演算を選択できる．

ここでは自己復号型ランダムグリッドを 2 枚複製し，これら 3 枚の画像を位置をずらして重ね合わせ演算することで秘密画像の復号が可能な，自己復号型ランダムグリッドの生成手法について説明する．秘密画像 $f(x,y)$ として幅 w，高さ h の 2 値画像を用いる．暗号鍵である復号時に重ね合わせる 2 枚の複製画像の移動量は，それぞれ水平方向に h_1 画素，垂直方向に v_1 画素，および水平方向に h_2 画素，垂直方向に v_2 画素とする．複製したランダムグリッドがすべて重なり合う位置において秘密画像が復号される．言い換えれば，自己復号型ランダムグリッドでは復号されない領域が存在する．本稿では，この領域を拡張領域と呼ぶ．**図 1** に復号移動量と拡張領域との関係を示す．実線の領域は自己復号型ランダムグリッド，破線および一点鎖線の領域は複製した自己復号型ランダムグリッドを示す．また灰色に塗りつぶした領域が拡張領域である．拡張領域の大きさは復号移動量により決定され，拡張領域の拡張幅 e_w および高さ e_h は次式で表される．

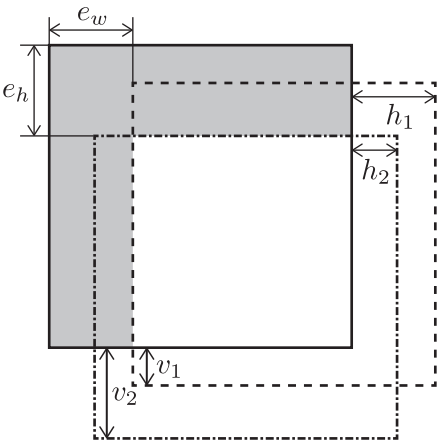

図 1 復号移動量と拡張領域

Fig. 1 Value of decoding shift and extended area for encryption.

$$e_w = \max\{h_i, i = 1,2\} \tag{1}$$

$$e_h = \max\{v_i, i = 1,2\} \tag{2}$$

自己復号型ランダムグリッドの生成は，生成済みのランダムグリッドと秘密画像との情報を用いて未生成の領域に暗号化されたパターンを順次配置することで行われる．まず，拡張領域の各画素に白または黒画素をランダムに配置する．この拡張領域に配置されたランダムパターンを生成済みのランダムグリッドとすると，未生成の領域に配置される画素情報は次式で表される．

$$\begin{aligned} g(x+e_h, y+e_v) = f(x,y) &\oplus g(x+h_1, y+v_1) \\ &\oplus g(x+h_2, y+v_2) \end{aligned} \tag{3}$$

ここで，$\oplus$ は画素ごとの排他的論理和演算を表す．また，秘密画像の大きさから $0 \le x < w$，$0 \le y < h$ とする．生成済みの情報を用いて画素情報を決定するため，生成処理は $g(0+e_h, 0+e_v)$ からラスタスキャン順に行われる．

図 2 秘密画像
Fig. 2 Secret image.

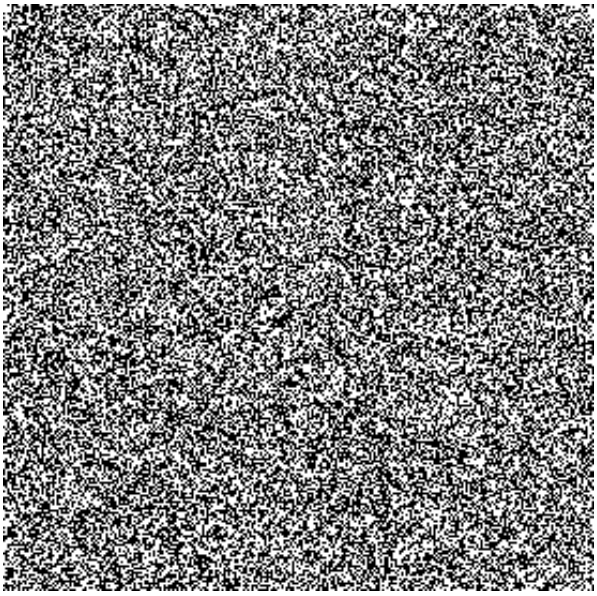

図 3 自己復号型ランダムグリッド
Fig. 3 Self-decodable random grid.

2.2 生成例および復号結果

図 2 に示す 256×256 画素の 2 値画像を秘密画像として使用した．復号移動量は $h_1 = 20$, $v_1 = 15$ および $h_2 = 12$, $v_2 = 18$ とした．このとき，拡張幅および高さはそれぞれ $e_w = 20$，$e_h = 18$ となる．図 2 に示す秘密画像を暗号化した自己復号型ランダムグリッドを**図 3** に示す．生成された自己復号型ランダムグリッドは，276×274 画素となる．生成された自己復号型ランダムグリッドはランダムなパターンであるため，肉眼では秘密画像の情報は一切わからない．

複製した 2 枚のランダムグリッドを，復号移動量に基づいてずらして重ね合わせた復号結果を**図 4** に示す．ここでは，論理積による復号を行った．これは透明フィルムなどに複製して重ね合わせて復号するのと等価である．白画素と黒画素の密度差により秘密画像の情報が表現されている．秘密画像の白画素の部分が完全には復号されていないため細部の情報を正確に得ることはできないが，秘密画像の解像度を適切な値にすることで秘密画像の情報を十分認識できるといえる．

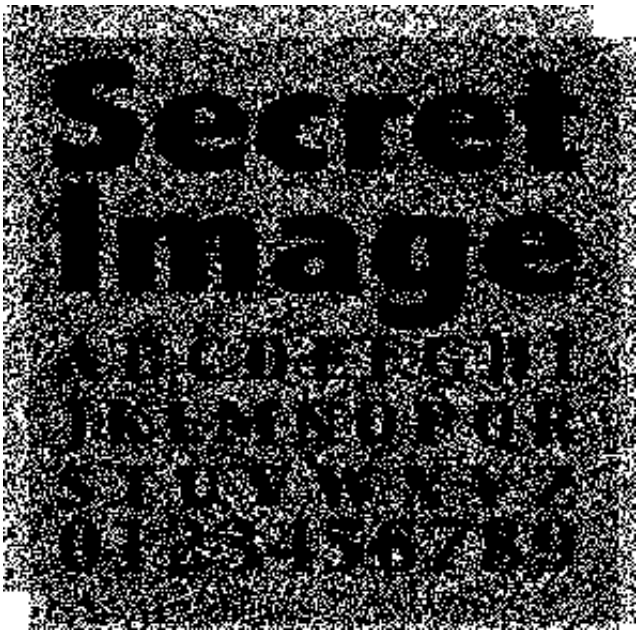

図 4 復号結果（論理積）
Fig. 4 Decrypted result with AND operation.

図 5 復号結果（排他的論理和）
Fig. 5 Decrypted result with XOR operation.

次に，排他的論理和による復号を行った結果を**図 5** に示す．排他的論理和演算では，すべてのランダムグリッドが重なり合った領域において完全に秘密画像が復号されていることがわかる．このようにカメラ付き携帯情報端末を用

いた復号のように，ソフトウェアによる演算が可能な状況においては，排他的論理和による復号は特に有効である．

図 5 の秘密画像が復号された状態から，2 枚目の複製画像の水平方向の移動量（h_2 に対応）を 1 画素ずらして排他的論理和による重ね合わせ演算を行った結果を**図 6** に示す．重ね合わせる位置が 1 画素でもずれると，秘密画像が全く復号されないことが確認できる．

さらに自己復号型ランダムグリッド(図 3)の中央 200×200 画素を切り出した画像を**図 7** に示す．切り出したランダムグリッドを複製し，排他的論理和による復号を行った結果を**図 8** に示す．一部を切り出したランダムグリッドにおいても，すべてのランダムグリッドが重なり合った領域において秘密画像が復号されている．このように部分的な自己復号型ランダムグリッドから秘密画像の情報の一部を取得することが可能である．

3. カメラ付き携帯端末を用いた復号

前述のように自己復号型ランダムグリッドでは，従来のランダムグリッドと同様に物理的な復号も可能である．すなわち，自己復号型ランダムグリッドを透明フィルムなどに複製し，適切な位置で重ね合わせることで復号結果を観察することができる．一方で従来のランダムグリッドとは異なり，復号用のランダムパターンを準備する必要はなく，単一のランダムグリッドからの秘密画像の復号が可能である．そのためカメラ付き携帯情報端末を復号に利用することで，自己復号型ランダムグリッドを撮影したその場で画像処理により復号することが可能である．

自己復号型ランダムグリッドを復号するためのスマートフォン用アプリケーションを作成した．復号用アプリケーションではカメラで取得した画像を複製し，2 値化後，位置をずらして排他的論理和演算による重ね合わせを行うことで復号する．復号結果はリアルタイムにスマートフォンのモニタに表示される．このときカメラで取得した画像中のランダムグリッドを構成する画素のサイズは，自己復号型ランダムグリッドの出力解像度や撮影距離によって変化する．そのためカメラで撮影されたランダムグリッドを構成する画素のサイズを 2 画素と仮定し，生成時設定した復号移動量との積を求めることで重ね合わせ位置を決定した．また，復号移動量はあらかじめアプリケーション内で $h_1 = 20$，$v_1 = 15$ および $h_2 = 12$，$v_2 = 18$ に設定した．

図 3 に示す自己復号型ランダムグリッドを 36 dpi で印刷したものを復号用アプリケーションで復号した．スマートフォンの傾きを調整し，自己復号型ランダムグリッドとの距離を約 200 mm としたとき，良好な復号結果が得られた．このときのスクリーンショットを**図 9** に示す．ランダムグリッドを印刷した紙の歪みや撮影距離のずれ，レンズの収差の影響などにより復号結果にムラが生じているが，秘密画像の情報を認識することが可能である．また，秘密

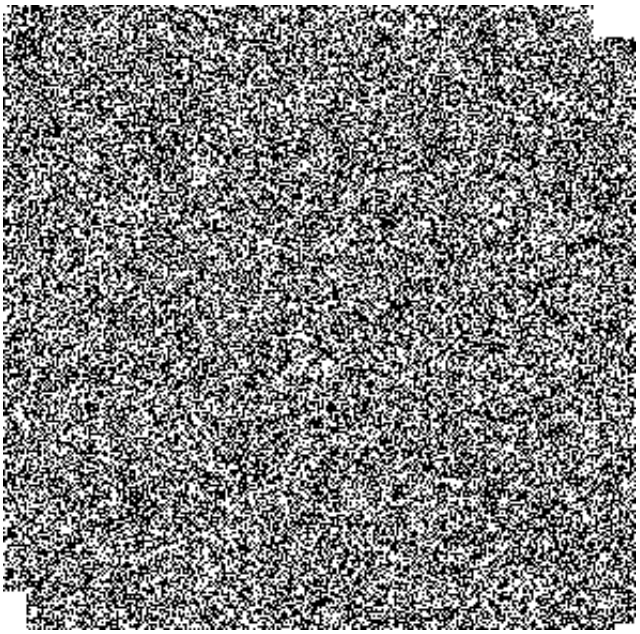

図 6 誤ったパラメータによる復号結果（排他的論理和）
Fig. 6 Decrypted result with wrong parameter.

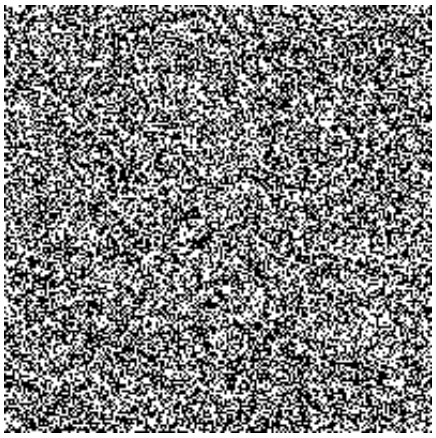

図 7 中央 200 × 200 画素を切り出した自己復号型ランダムグリッド
Fig. 7 Cropped self-decodable random grid to 200 × 200 pixels.

図 8 部分的な自己復号型ランダムグリッドからの復号結果
Fig. 8 Decrypted result of cropped self-decodable random grid.

画像全体は復号されていないが，スマートフォンを走査することで，全体の情報を取得することが可能である．

4. まとめ

本研究では，カメラ付き携帯情報端末を用いた復号が可能な潜像技術として，キャリアスクリーン画像の簡便な復号と，ランダムグリッドの秘匿性を合わせ持つ自己復号型ランダムグリッドを提案した．視覚的な秘匿性はランダムグリッドと同等であり，暗号鍵である復号移動量が 1 画素でもずれると秘密画像を復号することができないことを示した．また，暗号化および復号に排他的論理和演算を用いることで，カメラ付き携帯情報端末による復号においてより良好な復号結果が得られることを示した．さらに，カメラ付き携帯情報端末による復号として，スマートフォン用の復号アプリケーションを作成し，実機での復号実験を行い提案手法の妥当性を示した．暗号鍵を内包することで部分的な復号が可能になり，スマートフォンを用いた復号においてもスマートフォンを走査して復号することで全体の情報を取得することが可能である．

自己復号型ランダムグリッドでは暗号鍵を内包しているため，その暗号強度は複製枚数や復号移動量に依存し，従来のランダムグリッドと比較すると非常に弱い．しかしながら，スマートフォンを用いて復号する場合，撮影距離やカメラの傾き等を調整する必要があるため，復号移動量等のパラメータが既知でない場合，手動での復号はほぼ不可能であると考えられる．また，我々は暗号化手法というよりはむしろ情報提示手法としての利用を考えており，情報を秘匿することで，その情報の価値を高めることが可能であると考えている．さらに提案手法は言わば面倒臭い二次元バーコードであり，情報を入手するためには手動による復号操作を必要とする．人が操作することで秘密の情報が可視化される，このようなインタラクションを通じて，入手した情報への主観的な価値の向上が期待できる．

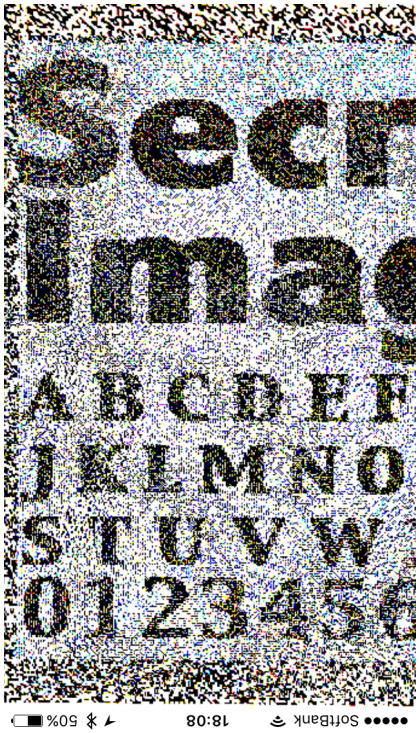

図 9 スマートフォンを用いた自己復号型ランダムグリッドの復号結果

Fig. 9 Decrypted result using a smart phone.

参考文献

[1] O. Kafri and E. Keren: “Encryption of pictures and shapes by random grids,” *Optics Letters*, **12**, 6, pp. 377–379, (1987).
[2] R. L. van Renesse: Optical Document Security, 3rd ed., Artech House, Norwood, MA, (2005).
[3] 香川元太郎：かずの冒険 ⟨ 野山編 ⟩, 小学館 (2009).
[4] ポケットモンスター XY マジックルーペで さがそう！, 小学館 (2012).
[5] R. Shogenji and J. Ohtsubo: “Hiding Information Using a Checkered Pattern,” *Optical Review*, **16**, 5, pp. 517–520, (2009).
[6] R. Shogenji and J. Ohtsubo: “Resolution multiplexing method for checkered-pattern carrier-screen images,” *in Proceedings of DHIP2012*, I021 (2012).
[7] 生源寺類, 大坪順次: “チェッカパターン視覚復号型暗号における秘密画像の角度多重埋め込み”, 第 71 回応用物理学会学術講演会 講演予稿集, p. 03-093 (2010).
[8] R. Shogenji and J. Ohtsubo: “Hiding a Checkered-Pattern Carrier-Screen Image in a Camouflaged Halftone Image,” *Optical Review*, **21**, 3, pp. 237–242, (2014).
[9] R. Shogenji: “Information embedding to a real object by projecting a checkered-pattern carrier-screen image”, *in Proceedings of SPIE 9217*, 92171T (2014).
[10] 生源寺類: “デジタルカメラによる復号が可能な潜像技術: 一様な画像への誤差拡散法による埋め込み”, 情報処理学会 インタラクション 2014, pp. 216–220 (2014).
[11] 生源寺類: “チェッカパターンキャリアスクリーン画像における誤差拡散法による部分的潜在化”, 情報処理学会 インタラクション 2015, pp. 753–758 (2015).