K-056

画像合成による拡張視覚復号型暗号
Extended Visual Cryptography Based on Image Blending

生源寺 類 †
Rui Shogenji

1. はじめに

秘密画像を複数のシェア画像に分散し，それらを重ね合わせることで秘密画像が復号される視覚復号型暗号が提案されている [1]．視覚復号型暗号で生成されるシェア画像はランダムなパターンとなるため，単一のシェア画像からは秘密画像の情報は得られない．これまでに，カラー画像を復号する手法 [2] や複数の秘密画像を埋め込む手法 [3]，シェア画像として意味のある画像を生成する手法 [4, 5] など，様々な手法が提案されている．特にシェア画像として自然画像などの意味のある画像を生成する手法は，拡張視覚復号型暗号と呼ばれる．また，生成されるシェア画像を拡張シェア画像と呼ぶ．拡張視覚復号型暗号では，暗号の存在自体を隠すことができるため様々な応用が期待できる．一方，秘密画像を拡張シェア画像へ分散するのと同時に，秘匿用画像（カバー画像）への埋め込みを行うため，通常の視覚復号型暗号と比較して複雑な演算が必要である．

本研究では，視覚復号型暗号法で生成したシェア画像と任意の画像との合成による，拡張シェア画像の簡易生成手法を提案する．提案手法は，単純な処理を逐次的に実行することで拡張シェア画像の生成が可能であり，これまでに提案されてきた視覚復号型暗号法への適用が容易である．

2. 画像合成による拡張視覚復号型暗号

2.1. 拡張シェア画像生成手法

拡張シェア画像生成の流れを図 1 に示す．提案手法による拡張シェア画像は，シェア画像の生成，画像の合成，および合成画像の 2 値化処理により生成される．シェア画像の生成では，従来の視覚復号型暗号法が適用可能である．生成されるシェア画像は 2 値のランダムパターンとなる．

次に，生成されたシェア画像ごとに，カバー画像との合成を行う．この合成処理は，アルファブレンディングなどの単純な手法で実現可能である．本稿では画素値の加減算により行う．カバー画像，シェア画像および合成量を，それぞれ $f(x,y)$，$g(x,y)$，w とすると，合成画像 $h(x,y)$ は次式で表される．

$$h(x,y) = \begin{cases} f(x,y) + w, & \text{if } g(x,y) \text{ is white,} \\ f(x,y) - w, & \text{if } g(x,y) \text{ is black.} \end{cases} \quad (1)$$

すなわち，シェア画像の画素が白であれば，カバー画像の対応する画素に画素値 w を加算し，シェア画像の画素が黒であれば，画素値 w を減算することで合成する．またこのとき，合成量 w を小さくすると，拡張シェア画像へのカバー画像の影響が大きくなるため，秘匿性の高い拡張シェア画像となる．しかしながら復号結果の画質の劣化も大きくなるため，適切な合成量の設定が必要である．

最後に合成画像をハーフトーン処理により 2 値化することで，拡張シェア画像が生成される．ハーフトーン処理として，組織的ディザ，ランダムディザ，誤差拡散法など様々な手法の利用が可能である．本稿では，誤差拡散法によるハーフトーン処理を適用する．

2.2. 拡張シェア画像

提案手法の例として，2 枚のシェア画像のうちの 1 枚をカバー画像と合成し，拡張シェア画像を生成した．また，シェア画像の生成，カバー画像との合成，2 値化処理は，Adobe Photoshop CS3 を使用して行った．秘密画像として 128 × 128 画素の 2 値画像を使用し，2 枚のシェア画像（256 × 256 画素）に分散した．カバー画像との合成により生成した拡張シェア画像を図 2 に示す．このとき合成量は 32 とした．拡張シェア画像から秘密画像の埋め込みを認識することは，困難であることがわかる．拡張シェア画像にシェア画像を重ね合わせて復号した結果を図 3 に示す．カバー画像の情報が残っているため，画質の劣化が見られるが，秘密画像の情報（FIT2011）は確認できる．

3. まとめ

画像合成による拡張シェア画像の簡易生成手法を提案した．提案手法は，単純な処理を逐次的に実行することで拡張シェア画像の生成が可能である．それぞれの処理は独立しているため，カバー画像への埋め込みによる暗号強度の低下は生じない．また，合成量を変化させることで，用途に応じた拡張シェア画像の生成が可能である．さらに，提案手法は市販の画像編集ソフトウェアを用いて実現できるため，セキュリティ応用以外にも，アミューズメントや教育教材などへの利用も期待できる．

参考文献

[1] M. Naor and A. Shamir, in Advances in Cryptography - EUROCRYPT'94, **950** of Lecture Notes in Computer Science, pp. 1–12 (1994).

[2] H. Koga and H. Yamamoto, IEICE Trans. Fundamentals **E81-A**, No. 6, pp. 1262–1269 (1998).

[3] 坂本太志, 古賀弘樹, 信学技報 **107**, No. 143, pp. 1–6 (2007).

[4] G. Ateniese, C. Blundo, A. Santis, and D. R. Stinson, Theoretical Computer Science **250**, pp. 143–161 (2001).

[5] M. Iwamoto and H. Yamamoto, IEICE Trans. Fundamentals **E85-A**, No. 10, pp. 2238–2247 (2002).

†静岡大学工学部, Faculty of Engineering, Shizuoka University

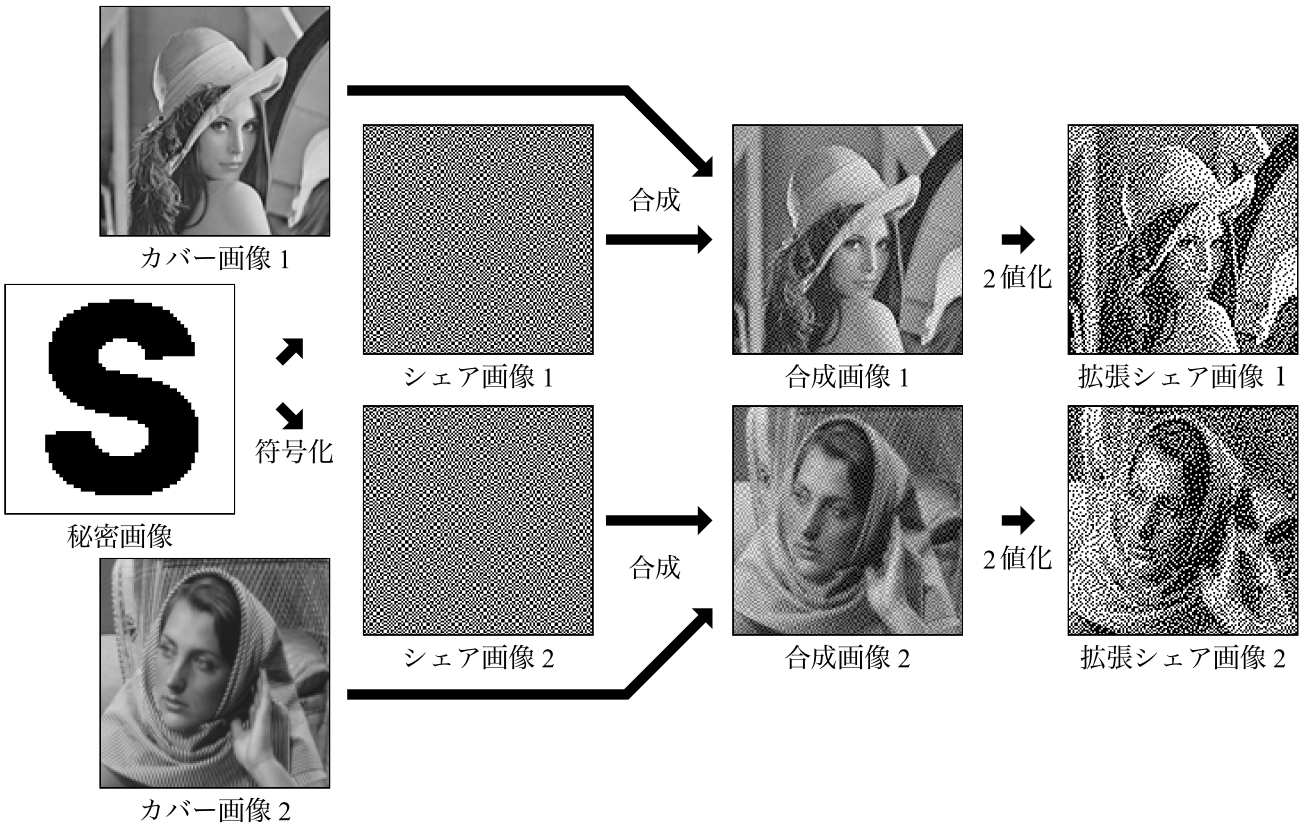

図 1: 拡張シェア画像生成の概略図.

図 2: 拡張シェア画像.

図 3: 復号結果.