

大久保伊織*, 李旻哲**

(*九州工業大学大学院情報創成工学専攻, **九州工業大学大学院情報工学研究院)

1. はじめに

近年, 光学的暗号は個人情報を守るために多くの産業で重要視されている. 光学的暗号の代表的な手法として, 二重ランダム位相暗号化(DRPE)が挙げられる. DRPEには, 暗号化結果が複素数となるため, 実部と虚部の2つのデータを送信しなければならず, データ効率が悪いという欠点がある. 3次元情報を取得する画像処理では, 膨大な量のデータを扱う必要があるため, データ効率の改善が求められる. 本研究では, DRPEを改良し, 同時に暗号化可能な枚数を増やすことで, データ効率を向上させることを目的とする.

2. 二重ランダム位相暗号化(DRPE)

DRPEは, 2枚のランダム位相マスクを用いて処理を行う手法である. 暗号化処理では, 実空間に配置した1枚目のランダム位相マスクを用いて元画像に位相情報を付与する. 次にフーリエ変換を行い, 2枚目のランダム位相マスクを掛けた後, 逆フーリエ変換を行うことで暗号化が完了する. 復号処理では, 暗号化画像をフーリエ変換し, 復号鍵である2枚目のランダム位相マスクの複素共役を掛けた後, 逆フーリエ変換を行う. その後, 絶対値を求めることで1枚目のランダム位相マスクで付与した位相情報を取り除き, 復号を完了する.

3. 従来手法

従来手法として, DRPEを改良し, 2枚の画像を同時に暗号化する手法が存在する. この手法では, DRPEの暗号化処理において実空間に配置する1枚目のランダム位相マスクを, 画像から生成した位相マスクに変更することで, 2枚の画像を同時に暗号化する. 復号処理では, 暗号化画像をフーリエ変換し, 復号鍵である2枚目のランダム位相マスクの複素共役を掛けた後, 逆フーリエ変換を行うことで復号データを取得する. 復号データの振幅には画像1, 位相には画像2の情報が含まれているため, 絶対値と位相角を求めることで各画像を復号可能である.

4. 提案手法

提案手法では, 従来手法を改良し, フーリエ空間に配置する2枚目のランダム位相マスクを, 3枚目の画像とシード値を指定した乱数の積から生成したマスクデータに変更することで3枚の画像を同時に暗号化する. シード値を指定することで送信側と受信側で同様の乱数を生成することができ, マスクデータにその乱数から生成した位相マスクの複素共役を掛けることで, 3枚目の画像を復号することができる. この手法では, 指定したシード値が3枚目の画像を復号するための復号鍵となるため, 送信時にRSA暗号を用いて暗号化を行う. 提案手法による暗号化処理の概要を図1に示す.

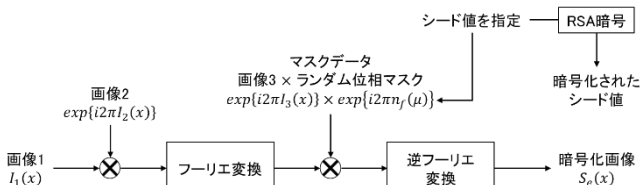


図1 提案手法による暗号化処理の概要

5. 実験環境及び実験結果

本研究では, 256px×256pxのカラー画像3枚に対して暗号化及び復号の処理を行った. 数値的な評価指標としてSSIMとPSNRを用いて, 復号画像の劣化具合を確認した. また, 従来手法と比較する指標として1000px×1000pxのカラー画像36枚を6組送信する場合のデータ効率を計算した. 実験に用いた3枚の画像, 提案手法による暗号化画像と復号鍵であるマスクデータの複素共役, 復号画像をまとめたものを図2に示す.

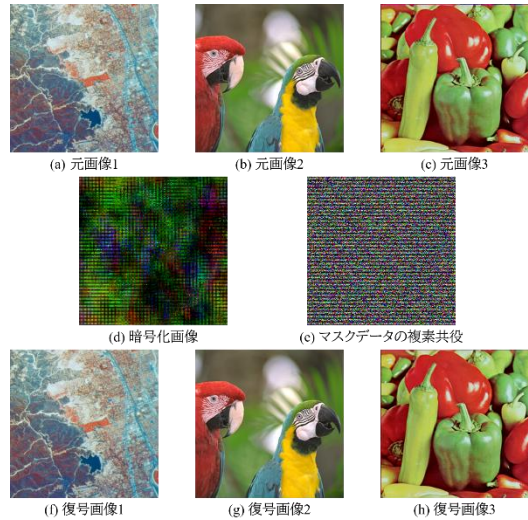


図2 各画像と提案手法による暗号化及び復号画像
SSIM, PSNRを用いて復号画像と元画像を比較した結果を表1に示す.

表1 各指標による評価結果

各画像	SSIM	PSNR[dB]
画像1	1	311.883
画像2	1	316.115
画像3	1	325.505

SSIMの値は0.98以上, PSNRの値は40[dB]以上で元画像と区別がつかないとされている. 表1の結果から, 提案手法は元画像の画質を劣化させることなく, 暗号化及び復号が可能であることが確認できる. 次に基本的なDRPE, 従来手法, 提案手法のデータ効率を比較する. 1000px×1000pxのカラー画像36枚を6組送信する場合, DRPEのデータ効率は次の式で表現される. $1000(H) \times 1000(V) \times 3(\text{RGB}) \times 2(\text{実数値, 虚数値}) \times 36(\text{画像枚数}) \times 6(\text{データの組数}) = 1.296[\text{GB}]$. 従来手法のデータ効率は $1000 \times 1000 \times 3 \times 2 \times 36 \times 3 = 648[\text{MB}]$, 提案手法のデータ効率は $1000 \times 1000 \times 3 \times 2 \times 36 \times 2 = 432[\text{MB}]$ となる. この結果から提案手法は従来手法と比較して約33%データ効率が向上していることがわかる.

6. まとめ

本研究では, 画質を維持したまま3枚の画像を同時に暗号化するDRPEを提案した. 従来手法と比較して, 約33%データ効率を向上させることができた. 今後の展望としては, 同時に暗号化可能な枚数を増加させる手法の提案を行う.