光フラクタル合成器を用いたランダムパターン発生のストリーム暗号への応用

佐々木　亨・東郷　寛之・谷田　純

近年，大規模な通信ネットワークが整備され，金銭やプライバシーに関わる重要な情報が扱われている．その中で，通信内容の漏洩を防ぐための暗号化手法が研究されているが，データ量の増加に伴う暗号・復号処理時間の増加が問題となっている．この問題を解決する手段として，光学的並列処理を用いた手法が注目されている[1,2]．

われわれは，2次元アフィン変換を用いてランダムな輝度分布をもつパターン（以下，ランダムパターン）を発生する手法を考案し，ランダムパターンを用いた暗号手法であるストリーム暗号への応用を検討した[3]．提案手法は，単純な光フィードバック系により並列処理されるため，計算効率のよい乱数発生手法として期待される．本稿では，提案手法の原理，安全性についての検討結果について紹介する．

1.　ストリーム暗号

図1に画像に対するストリーム暗号の手順を示す．暗号化処理では，送信する画像と，乱数発生器により生成したランダムパターンの和をとり，法を n とした剰余演算を行う．受信者側では，送信者が用いた乱数発生器のパラメーターは既知であり，同一の乱数系列を生成可能である．復号処理では，暗号データとランダムパターンの差に対し，剰余演算を行う．これらの処理は，光学系により，対象画像の各画素に対して並列に実行される．このとき，画像の更新と同期して，ランダムパターンを生成できる乱数発生器が必要となる．

2.　2次元アフィン変換を用いたランダムパターン発生法

2次元アフィン変換を用いたランダムパターン発生法の手順を図2に示す．この手法では，初期入力として与えた像を複製し，おのおのに対して異なった2次元アフィン変換を施す．2次元アフィン変換は，式(1)により表される．

$$\boldsymbol{x}' = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{a} \qquad (1)$$

ここで，$\boldsymbol{x}$，$\boldsymbol{x}'$ はおのおの変換前，変換後の画像中の画素座標，$\boldsymbol{A}$ は画像の回転・拡大縮小を表す2次元正方行列，$\boldsymbol{a}$ は画像の平行移動を表す2次元ベクトルである．異なったアフィン変換後のすべての画像を加算し，輝度に対して法を n とした剰余演算を行う．以上の処理を反復することによりパターンの更新を行う．更新回数が少数であるときには，パターンの輝度分布に偏りが生じるが，十分な回数の更新後に，偏りのない輝度分布をもつパターンが生成される．

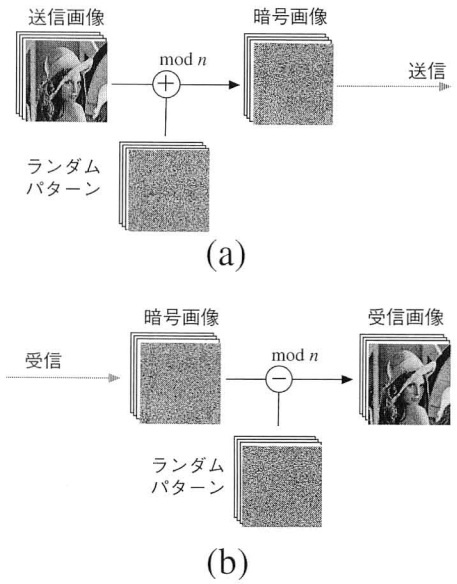

図1　ストリーム暗号．(a) 暗号化処理，(b) 復号処理．

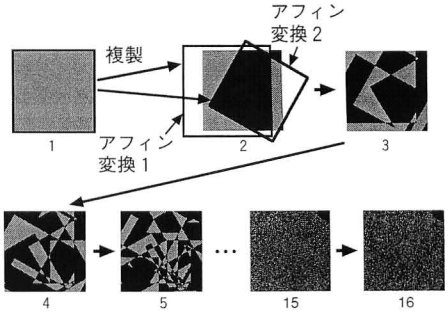

図2　2次元アフィン変換を用いたランダムパターン発生法．

大阪大学大学院工学研究科物質・生命工学専攻（〒565-0871 吹田市山田丘 2-1）
E-mail: sasaki@mls.eng.osaka-u.ac.jp

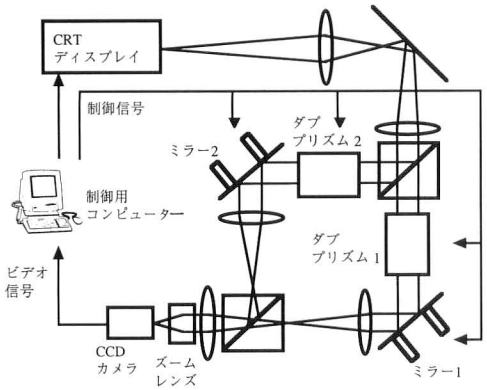

図3　光フラクタル合成器.

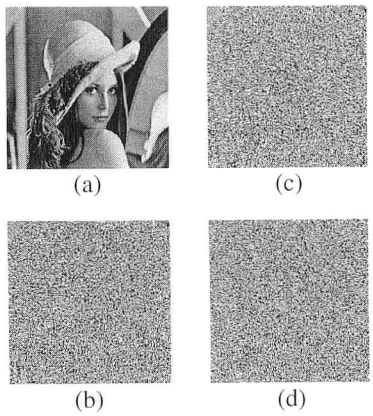

図4　安全性の確認実験.（a）暗号化対象画像,（b)～(d）復号画像.

提案手法は，図3に示す光フラクタル合成器[3]により効率的に実行される．このシステムでは，CRTディスプレイに表示したパターンに対して，ダブプリズムにより回転，ズームレンズにより拡大・縮小変換，ミラーにより平行移動を行う．光学系を用いることにより，変換はパターン中の全画素に対して並列に実行される．

3.　安全性の検証

提案手法の安全性を確認するために，検証実験を行った．まず，提案手法を用いてランダムパターンを生成し，対象画像を暗号化する．次に，暗号化鍵（各アフィン変換における回転，拡大縮小，平行移動量と更新回数）に微小変化を加えて復号鍵を作成し，暗号画像を復号する．このとき，暗号化鍵と復号鍵が異なるため，対象画像が部分的にも再現されないことが期待される．

図4に対象画像および復号画像を示す．表1に暗号化鍵を示す．表1における変換1に変化を与えることで復号鍵を生成した．図4（b)～(d）は，おのおの回転角0.01度，縮小率0.001，反復回数1の変化を与えた復号鍵による復号画像である．いずれの微小変化に対しても，対象画像は復号されていない．この結果より，暗号化鍵と類似した復号鍵による復号は，非常に困難であると考えられる．

暗号の安全性を決める乱数列の周期を評価するため，二値のパターン列を生成し，各画素変化の線形複雑度[4]を計算した．提案手法では，回転・スケール変換時に，画素が対応する格子点の濃度補間を必要とする．濃度補間法として最近傍法[5]を用いることで，非線形変換を除去し，計算と評価の簡単化を図った．また，画像サイズを前の評価に用いた256×256画素から32×32画素に変更した．生成パラメーターとして表1を用いた．線形複雑度の平均値は，全画素数1024に対して827であった．大部分の画素を効率的に利用した長周期乱数列生成が確認された．高次の濃度補間法を用いることで，非線形効果による乱数列の長周期化も期待できる．

表1　ランダムパターン生成パラメーター.

変換	縮小率	回転角（degree）	平行移動（pixel）
1	0.8	60	(50, −10)
2	0.7	200	(−40, −50)
3	1.1	90	(0, 5)

光学系による原理確認実験も行った．しかしながら，現在の光フラクタル合成器実験光学系では，光学系の収差，光源のゆらぎなどの影響により，パターンが正確に再現されないことが確認された．正確に再現するためには，輝度および輝度分布を量子化し，おのおのにおける誤差が伝搬しない系を作る必要があると考えられる．

文　　献

1) P. Refregier and B. Javidi: “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett., **20** (1995) 767-769.
2) M. Madjarova, M. Kakuta, M. Yamaguchi and N. Ohyama: “Optical implementation of the stream cipher based on the irreversible cellular automata algorithm,” Opt. Lett., **22** (1997) 1624-1626.
3) T. Sasaki, H. Togo, J. Tanida and Y. Ichioka: “Stream cipher based on pseudorandom number generation with optical affine transformation,” Appl. Opt. **39** (2000) 2340-2346.
4) 岡本龍明，山本博資：現代暗号（産業図書，東京，1998）pp. 45-54.
5) 尾上守夫：画像処理ハンドブック（昭晃堂，東京，1987）pp. 263-276.

（2000年2月10日受理）