

カオス理論の情報技術への応用

■ 情報工学部 情報システム工学科 教授 山口 明宏

○ 研究分野：応用数理

○ キーワード：カオス、CDMA、暗号、擬似乱数生成、神経回路網

I 研究概要

カオス力学系は、単純なシステムでも非常に複雑な系列を生成することができる。

本研究室では、カオスの複雑さの情報技術への応用として、暗号システムのための擬似乱数系列の生成や、CDMA通信システムのためのスペクトル拡散符号の構成について研究を行っている。

図1は、Arnold's cat mapと呼ばれるカオス写像で、数回の変換によって元の画像の情報は攪拌されて、一見情報を失ったように見えるが、この写像は可逆であり、逆写像を順次適用すると元の情報を完全に復元することができる。暗号化と復号化に対応付けることができる。

図2は、Arnold's cat mapを4つ使用した多次元写像を用いた擬似乱数生成回路のシミュレーション結果である。このようなカオス写像を応用することで、実際の乱数に近い統計的性質を有する擬似乱数系列を生成することができる。

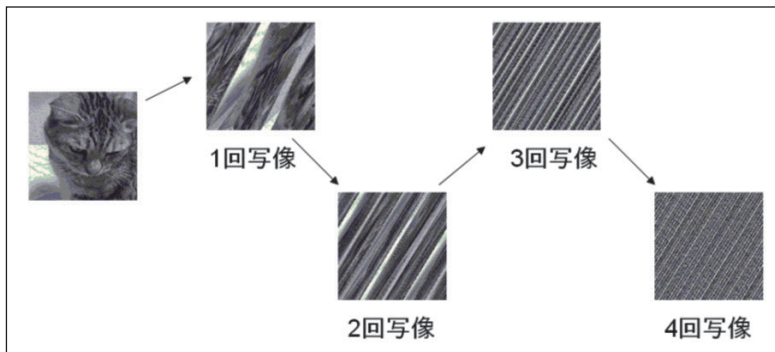


図1：2次元キャットマップを用いた画像の暗号化の例
逆写像を適用すると画像を復元することができる。

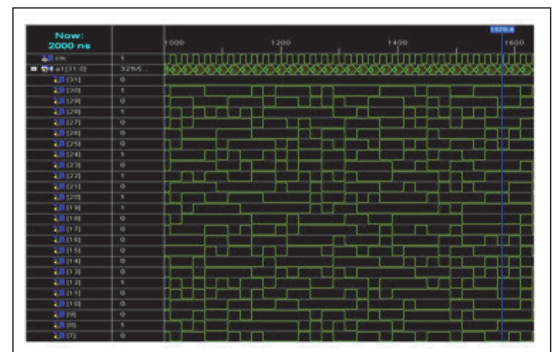


図2：キャットマップを用いた擬似乱数回路の
シミュレーション結果

I 利点特徴

- ・カオス系列の多様性を応用することで、理想的な乱数系列に近い統計的性質を有する擬似乱数系列を生成することができる。
- ・スペクトラム拡散符号の生成においても、単純なカオス力学系を用いて多様な符号集合を構成することができる。

I 応用分野

データの秘匿化のための擬似乱数生成システム及びCDMA通信などの多重化通信システムへの応用

