Vol.2020-MPS-130 No.5
2020/9/29

分布系のカオス同期化と深層学習を用いたカラー画像の秘匿通信

陳 鈺涵[1]　佐野 英樹[1]　若生 将史[1]　谷口 隆晴[1]

概要：本研究では, 分布系のカオス同期化と深層学習を用いたカラー画像の秘匿通信手法を提案する．先行研究では，カオス的な挙動をする偏微分方程式を利用した画像の秘匿通信技術が提案されていたが，系を表すパラメータの数はそれほど多くなく，情報の漏洩の可能性があった．本研究では，カラー画像の通信を考慮した上で設計したニューラルネットを用いて系の挙動を学習し，ブラックボックス化することで，情報の漏洩が起こりにくいように改良する．

キーワード：カオス振動，同期化，深層学習，秘匿通信システム

Secret Communication System for Color Images Using Deep Learning and Chaotic Synchronization of Distributed Parameter Systems

Abstract: In this study, we propose a secret communication system for color images using chaotic synchronization of the distributed parameter system and deep learning. Earlier research proposed a technique for secret communication of images using partial differential equations with chaotic behavior, but the number of parameters representing the system was not so large, which could lead to information leakage. In this study, the behavior of the system is learned using a neural network designed to take into account the communication of color images, and the system is black-boxed so that information leakage is less likely to occur.

Keywords: Chaotic vibration, synchronization, deep learning, secret communication system

1. はじめに

本研究では，分布系のカオス同期化とニューラルネットワークを利用してカラー画像を通信するための秘匿通信システムを提案する．

カオス同期化を用いた秘匿通信システムでは，一般に，カオス的に振る舞う信号に通信情報を埋め込んで送信し，受信側ではカオス同期化を利用して情報を取り出す [1][4][5][6]．先行研究 [2] では，非線形性な境界条件により引き起こされるカオス的振動現象を伴う波動方程式を用いた秘匿通信システムが考察されていた．この研究では，カオス的な分布系を秘匿通信システムに応用することで，送信信号をスカラー値からベクトル値に拡張しており，画像信号の暗号化および復号化に適用しやすいシステムとなった．しかし，この非線形な境界条件を表す数式は，比較的，簡単なものであり，境界条件に関する情報が盗難された場合に，情報が漏洩する可能性がある．そこで，本研究では，ニューラルネットワークを用いて境界条件を近似することで，システムをブラックボックス化し，情報が漏洩しにくい手法に改良する．

2. カオス的な分布系と同期システム

本研究では，先行研究 [2] で用いられている，カオス的な分布系とその同期システムを利用する．本節では，まず，これらについて説明する．先行研究 [2] では，領域 $(0, 1)$ 上で定義され，$x = 1$ においてファン・デル・ポール境界条件を与えた波動方程式 [3]

[1] 神戸大学
Kobe University, Kobe, Hyogo 657–8501, Japan

$$\begin{cases} y_{tt}(t,x) = y_{xx}(t,x), \quad t>0,\ x\in(0,1) \\ y_x(t,1) = \alpha y_t(t,1) - \beta y_t^3(t,1), \quad t>0 \\ y_t(t,0) = -\eta y_x(t,0), \quad t>0 \\ y(0,x) = y_0(x),\ y_t(0,x) = y_1(x),\ x\in[0,1] \end{cases} \tag{1}$$

とその同期システムを用いた秘匿通信システムを考えた．ただし，α,β,η はパラメータであり，$\alpha,\beta,\eta>0, \eta\neq 1$ とする．

u，v を

$$\begin{cases} u(t,x) := \frac{1}{2}\{y_x(t,x) + y_t(t,x)\} \\ v(t,x) := \frac{1}{2}\{y_x(t,x) - y_t(t,x)\} \end{cases} \tag{2}$$

で定義すると，これらは (1) のリーマン不変量であり，次の 1 階双曲型方程式を満たす：

$$\Sigma_0 : \begin{cases} u_t(t,x) = u_x(t,x), \quad t>0, x\in(0,1) \\ v_t(t,x) = -v_x(t,x), \quad t>0, x\in(0,1) \\ u(t,1) = F_{\alpha,\beta}(v(t,1)), \quad t>0 \\ v(t,0) = qu(t,0), \quad t>0 \\ u(0,x) = \frac{1}{2}\{y_0'(x) + y_1(x)\} \\ \qquad =: u_0(x), \quad x\in[0,1] \\ v(0,x) = \frac{1}{2}\{y_0'(x) - y_1(x)\} \\ \qquad =: v_0(x), \quad x\in[0,1]. \end{cases} \tag{3}$$

ただし，$q := \frac{1+\eta}{1-\eta}$ であり，関数 $u = F_{\alpha,\beta}(v)$ は

$$\beta(u-v)^3 + (1-\alpha)(u-v) + 2v = 0 \tag{4}$$

の解として定義される．パラメータについては，例えば，$\alpha = 0.5, \beta = 1, \eta = 0.625$ とするが，特に η の設定には注意が必要であり，これを適切な値に選ぶと系の全変動が指数的に増大することが理論的に示されている．全変動は，関数の変化の激しさを表す指標の一つであるため，これが増大することは，系がカオス的な挙動をすることを意味する．実際，上記のように，リーマン不変量を用いて方程式を書き換えると，波は左右の境界で境界条件として与えられている $F_{\alpha,\beta}$ と q 倍するという関数によって繰り返し写像されることが分かる．η が，ある範囲に存在するときに，これらを合成した $qF_{\alpha,\beta}$ という写像はカオス的になり，これが解の全変動を増大させる要因となる．

先行研究 [2] では，このカオス的な挙動を情報の隠蔽に利用するとともに，受信側で正しく情報が取り出せるように，この系に同期するような別のシステムを利用する．具体的には，システム (3) に対して，図 1 のように，二つの信号 $u(t,0)$ と $v(t,1)$ を入力とする以下のシステムを考える：

$$\Sigma_1 : \begin{cases} \hat{u}_t(t,x) = \hat{u}_x(t,x), \quad t>0, x\in(0,1) \\ \hat{v}_t(t,x) = -\hat{v}_x(t,x), \quad t>0, x\in(0,1) \\ \hat{u}(t,1) = F_{\alpha,\beta}(v(t,1)), \\ \qquad \hat{v}(t,0) = qu(t,0), \quad t>0 \\ \hat{u}(0,x) = \hat{u}_0(x), \\ \qquad \hat{v}(0,x) = \hat{v}_0(x), \quad x\in[0,1]. \end{cases} \tag{5}$$

ここで，二つのシステムの状態の差を表す変数 $\tilde{u} := u - \hat{u}$, $\tilde{v} := v - \hat{v}$ を導入すると

$$\begin{cases} \tilde{u}_t(t,x) = \tilde{u}_x(t,x), \quad t>0,\ x\in(0,1) \\ \tilde{v}_t(t,x) = -\tilde{v}_x(t,x), \quad t>0,\ x\in(0,1) \\ \tilde{u}(t,1) = 0,\ \tilde{v}(t,0) = 0, \quad t>0 \\ \tilde{u}(0,x) = \tilde{u}_0(x),\ \tilde{v}(0,x) = \tilde{v}_0(x), \quad x\in[0,1] \end{cases} \tag{6}$$

を得るが，特性曲線法により，(6) の解 $\tilde{u}(t,\cdot)$，$\tilde{v}(t,\cdot)$ は任意の初期値 $\tilde{u}_0, \tilde{v}_0$ に対し，時刻 $t=1$ で完全にゼロになることがわかる．すなわち，システム (5) はシステム (3) に対して，時刻 $t=1$ で同期する．

先行研究 [2] では，(5) を定めるために必要な系のパラメータや境界条件に関する情報などをあらかじめ共有すると仮定されている．その上で，送信側は，秘匿通信のために，カオス的な系の状態を利用して変調した情報を送信するが，同時に受信側は，送信側での同期に必要な境界での値 $u(t,0)$，$v(t,1)$ を同期システムに送信して発展させ，変調の際に利用された系の状態を復元し，それを用いて復調する．

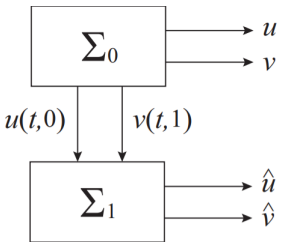


図 1 同期システム Σ_1.

より具体的には，隠蔽通信のための変調部を

$$\begin{aligned} &w(k+1) = \\ &C(w(k))\{0.03m|\hat{u}(k)|_V + 0.03m|\hat{v}(k)|_V\} \\ &+ \{0.5C(w(k)) + 0.1I\} \\ &\times \{0.08m|\hat{u}(k)|_V + 0.08m|\hat{v}(k)|_V + s_1(k+1)\}, \\ &c_{12}(k) = w(k) \end{aligned} \tag{7}$$

のように，復調部を

$$
\begin{aligned}
&t_2(k+1)\\
&=\frac{1}{m}[\{0.5C(c_{12}(k-1))+0.1I\}^{-1}\\
&\times[c_{12}(k)-C(c_{12}(k-1))\\
&\times\{0.03m|u(k-1)|_V+0.03m|v(k-1)|_V\}]\\
&-0.08m|u(k-1)|_V-0.08m|v(k-1)|_V] \qquad (8)
\end{aligned}
$$

のように設定する．ここで，$w(k)\in\mathbb{R}^{L+1}$，$s_1(k)\in\mathbb{R}^{L+1}$ であり，I は $(L+1)$ 次の単位行列，$m\in\mathbb{R}$ はパラメータである．また，ベクトル $f=[f_0,f_1,...,f_L]^T$ に対して，$C(f):=\mathrm{diag}(|f_0(1-f_0)|,...,|f_L(1-f_L)|)$，および $|f|_V:=[|f_0|,|f_1|,...,|f_L|]^T$ とする．s_1 は送信したい情報を表しており，$c_{12}=w$ は通信時にシステム間で送受信する情報である．t_2 は復調によって取り出した情報であり，２つの系が同期している場合には s_1 に一致する．

3. 提案手法

本研究では，ニューラルネットワークを用いて境界条件をブラックボックス化することで手法の安全性を向上させる．

まず，カラー画像を扱えるように，Σ_0 及び Σ_1 を RGB のそれぞれの色に対応するよう，従属変数 u,v を３次元に拡張する．次に，それを風上差分で近似する．N を空間の分割数として，空間・時間方向の刻み幅を $\Delta x=1/N$，Δt とする．$u_i(k)\in\mathbb{R}^3$ を $u(k\Delta t,i\Delta x)\in\mathbb{R}^3$ の近似値とすると，離散化後の系は

$$
\Sigma_{0,\mathrm{d}}:\begin{cases}
\frac{u_i(k+1)-u_i(k)}{\Delta t}=\frac{u_{i+1}(k)-u_i(k)}{\Delta x},\\
\quad k>0, i\in[1,N-1],\\
\frac{v_i(k+1)-v_i(k)}{\Delta t}=-\frac{v_i(k)-v_{i-1}(k)}{\Delta x},\\
\quad k>0, i\in[1,N-1],\\
u_N(k)=F_{\alpha,\beta}(v_N(k)),\quad k>0,\\
v_0(k)=qu_0(k),\quad k>0
\end{cases} \qquad (9)
$$

となる．ここで，空間･時間の刻み幅として $\Delta t=\Delta x=1/N$ と設定すると

$$
\begin{aligned}
u_i(k+1)&=u_{i+1}(k),\quad k>0, i\in[1,N-1],\\
v_i(k+1)&=v_{i-1}(k),\quad k>0, i\in[1,N-1]
\end{aligned}
$$

となり，結果として，$u_i(k)$ を $u_{i-1}(k+1)$ へ，$v_{i-1}(k)$ を $v_i(k+1)$ へ推移させるというアルゴリズムを得る．Σ_1 についても，同様に離散化する．

先行研究 [2] では，同期化のための信号として境界上の値を送り，それに境界条件を適用することで時間を発展させていた．本研究では，この境界条件部分をニューラルネットワークに置き換える．ニューラルネットは，バッチ正規化層をもつ７層の多層パーセプトロンとして構成し，$qF_{\alpha,\beta}$ を近似するように学習する．ただし，第４層は３つのセルからなるように設計しておき，第１層から第４層，第５層から第７層が定める関数を F_0，F_1 とすることで，全体を２つの部分に分割する．学習したニューラルネットワークを利用して，左端の値 v_0 に関する境界条件を，$v_0(k+1)=qu_0(k)$ からニューラルネットワークの前半分 F_0 に変換し，右端の値 u_L については $u_L(k+1)=F_{\alpha,\beta}(v_L(k))$ からニューラルネットワークの後半分 F_1 に変換する．これによって，システムの境界条件をブラックボックス化し，情報が漏洩しにくくなるようにする（図２参照.）

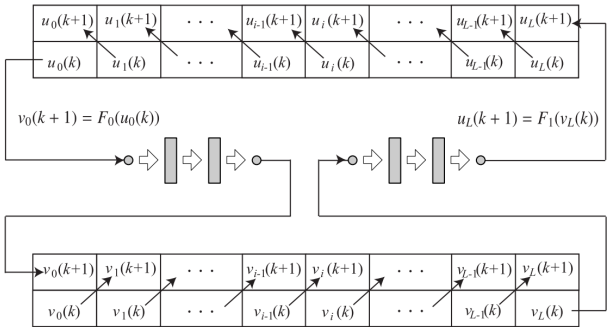


図 2 離散化したニューラルネットを用いたシステムにおける $u(k)$ と $v(k)$ の時間発展.

4. 数値実験

提案手法の評価のために，以下のような構造のニューラルネットワーク，学習データ，パラメータを用いて数値実験を行った．

実験における学習データとして，$\alpha=0.5,\beta=1,\eta=0.625$ とおいて，区間 $(-2,2)$ から等間隔に入力 x を選び，方程式 (4) を，ニュートン法を用いて解いた解をニューラルネットワークのターゲット y とした．データ数 N_d は 30000 とした．なお，学習に用いる入力データ x の偏りを減らすために，訓練データ，および，テストデータの選択に scikit-learn の train_test_split 関数用いて，ランダムにデータセットを分割した．ニューラルネットワークの実装には PyTorch を用い，実行は Google Colaboratory の Tesla K80 で行った．

まず，用いたニューラルネットワークの構造について説明する．本研究で用いたニューラルネットワークは，バッチ正規化層をもつ７層のパーセプトロンである．各層は，重み W とバイアス b をもち，以下のような非線形計算を行う:

$$\hat{y}=g(Wx+b).$$

ここで $g(\cdot)$ は活性化関数である．第１層，および，第４層は，カラー画像を扱うために，3 つのノードをもつ層として定義する．これらの層では，入力値を -1.0 から 1.0 の範囲の数値に変換して出力するように双曲線関数（tanh）

$$g(r) = \tanh(r) = \frac{\mathrm{e}^{r} - \mathrm{e}^{-r}}{\mathrm{e}^{r} + \mathrm{e}^{-r}}$$

を活性化関数とする．第 2 層，第 3 層，および，第 5 層では 50 個のノードを設定し，正規化線形関数 (ReLU)

$$g(r) = \begin{cases} 0, & \text{for} \quad r < 0 \\ r, & \text{for} \quad r \geq 0 \end{cases}$$

を用いて計算した．学習精度を示す訓練誤差，および，汎化性能を判断するテスト誤差については，平均二乗誤差 (MSE)

$$J = \frac{1}{N_{\mathrm{d}}} \sum_{i=1}^{N_{\mathrm{d}}} (y_i - \hat{y}_i)^2$$

を用いて評価した．ここで，$\hat{y}_i$ は出力値，y_i はターゲット値である．学習におけるパラメータ更新の際の最適化アルゴリズムには Adam を利用した．学習率は 0.001 に設定し，学習のエポック数は 1000 回とした．その際の訓練誤差とテスト誤差は，例えば，図 3 のようになった．学習結果はパラメータの初期化などに用いられる乱数に依存するため，乱数のシードを変えながら学習を 10 回実行し，実行結果の平均値と標準偏差を用いてニューラルネットワークの性能を評価した．

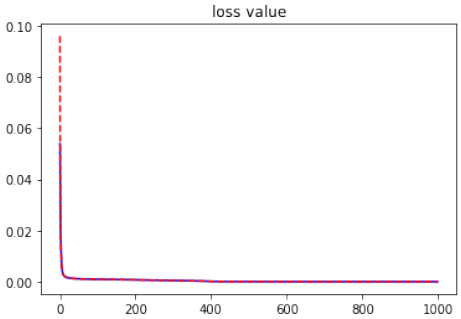


図 3 学習過程においてニューラルネットワークの訓練誤差（青い線）およびテスト誤差（赤い線）．

図 3 より，訓練，および，テストが進むごとに誤差が下降し，早い段階で収束することが確認できる．訓練誤差およびテスト誤差の評価数値は，表 1 のように，それぞれ 0.000694 ± 0.000035，0.000919 ± 0.000033 であった．

表 1 10 回で実行した結果の平均値±標準偏差．

エポック数	データセット	平均値 ± 標準偏差
1000 回	train	0.000694 ± 0.000035
	test	0.000919 ± 0.000033

学習したニューラルネットワークによって境界条件を設定したシステムを用いて，変調部，および，復調部におけるパラメータ m を $m = 7.5$ とおき，図 4 のようなカラー画像を用いた時の数値実験結果を図 5 に示す．図 4 に示されている画像の大きさは 512 x 512 ピクセルである．図 5(a) のように，暗号化された画像からは元の画像はほとんど確認できない．図 5(b) には，復調部を経て復元された画像を示す．送信画像と復元画像の区別はほとんど見られない．

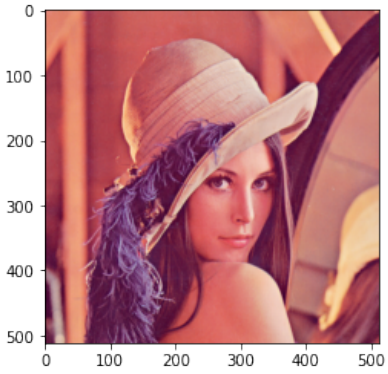
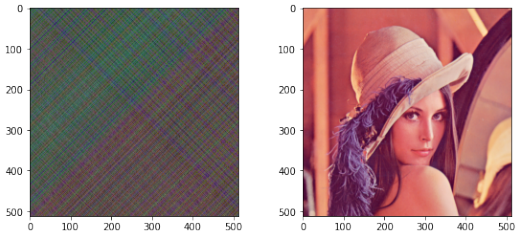


図 4 元カラー画像．



(a) 暗号化されたカラー画像．　(b) 復元画像．

図 5 本研究の提案手法における暗号化されたカラー画像と復元画像．

謝辞 本研究は JST CREST (JPMJCR1914) の助成を受けている．

参考文献

[1] L. Kocarev and U. Parlitz: General approach for chaotic synchronization with applications to communication, Physical Review Letters, Vol. 74, (1995).
[2] 佐野英樹，若生将史，谷口隆晴：分布系のカオス同期化を用いた秘匿通信システム，投稿中．
[3] G. Chen, S.B. Hsu and J. Zhou: Chaotic Vibration of the Wave Equation with Nonlinear Feedback Boundary Control: Progress and Open Questions, in: Chaos Control – Theory and Applications, G.R. Chen and X. Yu (Eds.), LNCIS 292, Springer-Verlag, Berlin(2003).
[4] K.M. Cuomo and A.V. Oppenheim: Circuit implementation of synchronized chaos with applications to communications, Physical Review Letters, Vol. 71(1993).
[5] 潮 俊光:カオス同期化制御とその秘匿通信への応用, 情報処理学会論文誌, Vol.36(1995).
[6] K. Yoshimura: Multichannel digital communications by the synchronization of globally coupled chaotic systems, Physical Review E, Vol.60(1999).