IEICE Technical Committee on
Complex Communication Sciences,
CCS-2013-018

ハードウェア実装にむけた反応拡散ステガノグラフィモデル

石村 憲意† Alexandre Schmid‡ 浅井 哲也† 本村 真人†

†北海道大学大学院情報科学研究科 〒060-0814 北海道札幌市北区北 14 条西 9 丁目
‡ Microelectronic Systems Laboratory, Swiss Federal Institute of Technology (EPFL) Lausanne, CH-1015 Switzerland
E-mail: ishimura@lalsie.ist.hokudai.ac.jp

あらまし 本研究では反応拡散セルオートマトン(RD CA)モデルにおけるステガノグラフィへの応用を示す．
ステガノグラフィ（電子透かし）技術は画像のようなデータに対し，他のデータ（メッセージ等）を埋め込む情報隠匿技術の一つである．近年，prey-predator RD モデルにより生成される自己組織化パターンによる秘匿通信アルゴリズムが提案されている[1, 2]．我々は自己組織化パターンのステガノグラフィへの応用に，より単純な CA モデル[3]を利用した．このモデルはチューリングパターン（人の指紋や動物の体表に表れる模様のような縞や斑点模様）のような模様を生成する．このモデルは単純なダイナミクスを持ち，少ない模様生成サイクル内に縞や斑点模様の平衡状態に収束する．そのため，ステガノグラフィ応用のハードウェア実装に適している．数値シミュレーション上で，RD CA モデルを利用したステガノグラフィによる，メッセージの暗号化と復号化を行った．

キーワード 反応拡散セルオートマトンモデル，ステガノグラフィ，秘匿通信

Image Reaction-diffusion Steganography on Hardware Implementation

Kazuyoshi Ishimura†, Alexandre schmid‡, Tetsuya Asai†, and Masato Motomura†

† Graduate School of Information Science and Technology, Hokkaido University
Kita 14, Nishi 9, Kita-ku, Sapporo 060-0814, Japan
‡ Microelectronic Systems Laboratory, Swiss Federal Institute of Technology (EPFL) Lausanne, CH-1015 Switzerland
E-mail: ishimura@lalsie.ist.hokudai.ac.jp

Abstract We demonstrate a possible application of “steganography” in a reaction-diffusion (RD) cellular automata (CA) model. Steganography is one of the latest techniques that conceal some data (messages) in other data-like images. Recently, a secure communication algorithm based on self-organizing patterns generated by a prey-predator RD model was proposed [1, 2]. In contrast, we employ a simple CA model [3] for steganography applications instead of using the prey-predator RD model. The model generates Turing-like patterns, e.g., stripe and spot patterns observed in human fingerprints, marking patterns on animal skins, etc. This model has simple dynamics and generates stripe or spot patterns at its equilibrium within a few cycles, which implies that the model is suitable for hardware implementation for a steganography application. Through extensive numerical simulations, we demonstrate steganography using the RD CA model in which messages can be encoded and decoded while concealing the messages in communication channels.

Keyword Reaction-diffusion Cellular Automata Model, Steganography, Secure Communication

1. 背景

アラン・チューリングは，拡散が一様状態から安定な空間非一様状態へ移行する“拡散不安定性”の概念を提唱した．系の時間発展は反応項と拡散項の和として記述される[4, 5]．反応項はある範囲内の状態の生成もしくは消滅を表し，拡散項は近傍領域の非一様性を不活性化させるプロセスの拡散を表している．このようにして生成される自己組織化模様は動物の体表など自然界において広く観測される．特に，チューリングモデルはパラメータセットを制御することにより，安定した縞もしくは斑点模様を生成することができる．

本研究では，このような反応拡散(RD)系のステガノグラフィ技術への応用の可能性を示す．ステガノグラフィは新しいデータ秘匿技術の一つである．“クリプトグラフィ (データ秘匿技術)”はデータ通信や保存の際に，データを暗号化する為に使われる方法である．これは第三者からデータを保護する為に使われる．一方で，ステガノグラフィは他のデータの中にメッセージ等のデータを隠す技術であり，送受信者のみが隠蔽されたデータの存在を把握している．このように，ステガノグラフィはデータの存在そのものを隠す技術である．これは，メッセージを保護するという点において，ステガノグラフィがクリプトグラフィに対して優位な

点である．ステガノグラフィ通信において，送信者は画像の中にメッセージを秘匿し，その画像データを送信する．この際に，第三者が通信中のこの画像を傍受したとすると，画像を閲覧することは可能であるが，そこに隠された文字を読むことができないばかりではなく，その存在自体に気づく事がない．そして，受信者のみが鍵を用いてメッセージを復号し，取り出すことができる．しかし，この人の目には読み出せない画像は，統計分析を使う事で，秘匿メッセージを取り出す事が出来る場合もある．反応拡散系をステガノグラフィに適用する際に，ランダムな初期パターンと反応拡散パラメータセットを復号する鍵として利用する[1, 2]．送信者はガウシアンノイズから生成するランダムパターンにメッセージを隠し，反応拡散により縞パターンを生成する．受信者は隠されたメッセージを，初期パターンから生成した縞パターンと，メッセージが隠されている縞パターンとの差分を取る事で復号できる．もし，第三者がこの画像を傍受したとしても，復号する鍵となる縞パターンを初期ランダム状態から作ることが出来ない限り，隠された文字を引き出すことができない．

2. 反応拡散セルオートマトンモデル

本研究では，前述の RDCA モデル[3]を利用する．このモデルでは，各セルの状態がシグモイド関数と四近傍セル間で作用する重み付け加算により決定される．重み付け加算は，それぞれ個別の拡散場における活性因子と抑制因子を表しており，それらは各セルにおいて畳み込まれる．セルの状態はセル(x, y)の各点における，活性因子 u と抑制因子 v の差分として計算される．u と v の拡散方程式は時 Δt で積分する．そして，セルの次の状態は u-v をシグモイド関数にかける．

このモデルのダイナミクスは，

拡散方程式

$$\frac{\partial u(\mathbf{r},t)}{\partial t} = D_u \nabla^2 u(\mathbf{r},t)$$

$$\frac{\partial v(\mathbf{r},t)}{\partial t} = D_v \nabla^2 v(\mathbf{r},t)$$

反応方程式

$$u(\mathbf{r},\delta t(n+1)) = v(\mathbf{r},\delta t(n+1))$$
$$= f(u(\mathbf{r},\delta t(n+1)) - v(\mathbf{r},\delta t(n+1)) - c)$$

$$f(x) = \frac{1}{1+\exp(-\beta x)}$$

として表され，n は時間ステップを，$\mathbf{r}$ は(x,y)を，c はシグモイド関数のオフセット値を，β は関数の傾斜を表している．このダイナミクスから波のパターンが生成される一連の動作を“1 RD サイクル”と定義する．

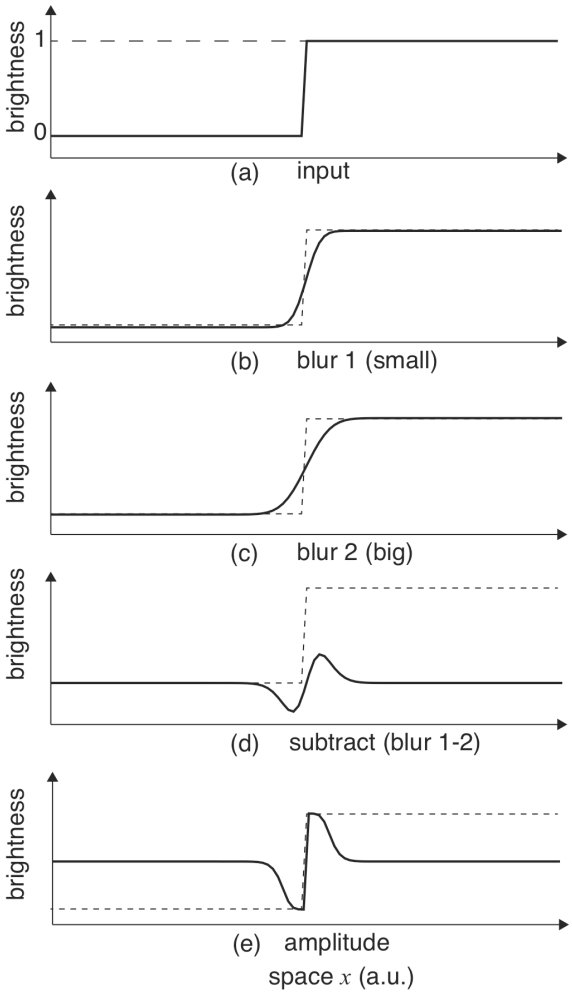

図 1．一次元 RD モデルにおける波生成プロセス: (a) 初期状態(ステップ関数), (b) Δt_0 拡散後の状態, (c) Δt_1-Δt_0 拡散後の状態, (d) 抑制因子(c)から活性因子(v)を減算した状態，(e) 差分結果(d)をシグモイド関数で増幅した状態．

このダイナミクスでは拡散場が二つ必要であり，回路実装では面積が大きくなってしまう．そこで，上記のダイナミクスと等価でありながら，1 つの拡散場から同様な波生成を行なう方法について図 1 に示す．図 1 (a)はステップ関数を入力した初期状態を示している．Δt_0 の拡散後，ステップ関数はパラメータ D_v で Δt_0 の間拡散させたのと同様の傾きを持つ(図 1 (b))．Δt_1-Δt_0 の間拡散した後に ステップ関数はパラメータ D_u で Δt_0 の間の拡散させたのと同様の傾きを持つ(図 1 (c))．図 1(d)に示すようにこれらの差分は活性因子と抑制因子の差分に対応する．最後にこの差分をシグモイド関数により増幅する(図 1(e))．このようにして波模様が生成される．これを二次元に拡張したのが図 2 である．セル同士は上下左右の 4 セルと隣接しており，約 8RD サイクル後に安定な縞パターンが生成される．パラメータは $D_v/D_u \equiv \Delta t_0/\Delta t_1$ で Δt_0=20, Δt_1=70, β =20, c=0 に設定する．

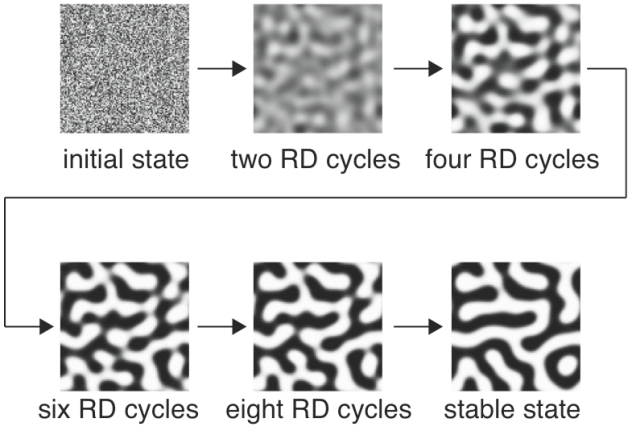

図２．二次元平面上で初期ランダムパターンから RDCA モデルを用いた縞生成の過程．

3. RDCA モデルによるステガノグラフィ

RDCA モデル(図１)を用いて RD ステガノグラフィの原理を，8 ビットの値を持つ 100 個のセルが直列に連なる一次元の場合で説明する(図 3)．最初に，安定した空間周波数パターンの生成が可能になるように，左端と右端の境界を繋いで環状にする．その後に，各セルの初期値をガウシアンノイズによりランダムな値に設定する．次に，メッセージを摂動として，ランダムパターンのセルの値を減算することで，埋め込みを行なう．図 3 では，横軸の 43~47 番目のセルの値を初期値の 10%減算することで埋め込みを行なっている．図 3 (a)は初期ランダムパターン，図 3 (b)は初期状態にメッセージの埋め込みを行なった様子を示している．図 3(c)は初期状態(a)と埋め込んだ直後の状態(b)の差分画像を表している．6RD サイクル繰り返した後，波パターンが安定化した様子を図 3 (d)，(e)に示す．これらの図は見かけ上の区別が難しく，メッセージが反応拡散の波生成により隠されたと考えられる．反応拡散後のランダムパターンの波(d)とメッセージを埋め込んだパターンの波(e)の差分をとることで，隠されたメッセージを抽出することができる(図 3 (f))．この波形は与えた摂動の特性に関連するインパルス応答を表すガウシアンの差分から得られる．中心部のピーク付近の最初にゼロを通過する部分は最初にパターンを隠したエッジ部分に対応する．

4. 二次元 RD ステガノグラフィ

4.1. 文字の埋め込み

この節では，二次元反応拡散ステガノグラフィ応用に拡張する．ここでは，文字や画像を摂動として，初期ランダムパターンの中へ埋め込み，十分な RD サイクル数の後に視覚的に解読できないようにする．図 4 では，100X100 ピクセルの画像の中に，文字“T”を埋め込む．その輪郭を 4X4 ピクセルのブロックの点を 8 ピクセル間隔で配置し，構成する．パラメータは 1

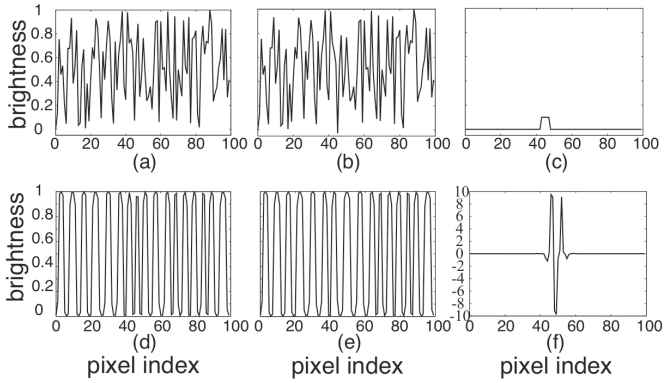

図３．RD ステガノグラフィによる一次元モデル(縦軸は正規化したセルが持つ状態値)．(a)初期ランダムパターン．(b) 43 番目から 47 番目のセルの値を初期値の 10%に減算した(メッセージ埋め込み)状態．(c) (a)と(b)を減算したパターン．(d) 初期ランダムパターンから波生成プロセスを経た安定状態．(e)メッセージを埋め込んだパターンの縞パターン生成後の安定状態．(e) 二つの平衡状態(d)と(e)の差分(メッセージ抽出)．

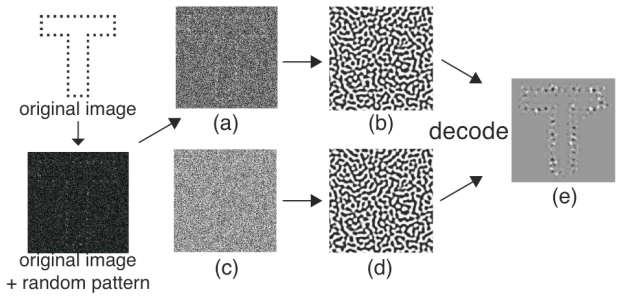

図４．文字“T”(ドットパターン)の埋め込み．(a) 初期埋め込み画像．(b) 6RD サイクル後のパターン．(c) 初期ランダムパターン(d) 6RD サイクル後の初期パターン．(e) 画像抽出((b)と(d)の差分)．

次元の時と同様の値を用いる．図 4 (a)は文字を埋め込んだ直後の状態であり，まだ目視可能である．6RD サイクル後に，文字を埋め込んだパターンから縞模様を生成した様子を示しており，目視出来ない状態である．図 4(c)は文字を埋め込んでいないランダムパターンであり，6RD サイクル後は図 4 (d)に示すような縞模様が生成される．図 4 (b)，(d)に示す縞模様は類似しているが，厳密には異なっている．この部分的な相違が，RD ステガノグラフィの静止画の中に隠されたメッセージの抽出を可能にする．図 4 (b)，(d)における差が図 4(e)として表される．ドット状の“T”は初期ランダムパターンの摂動として埋め込まれるが，周辺の領域に拡散していく．さらに，二次元のガウシアンの差は一次元の時と同様に観測される．このように，RD ステガノグラフィによるメッセージの暗号化と復号化を実際に示した．

4.2. 画像の埋め込み

次に RD ステガノグラフィによる画像埋め込みについてシミュレーションを行なった(図 5). 隠されたパターンの特性はまた，RD ステガノグラフィの埋め込み-抽出プロセスの結果に影響する．画像を埋め込む際に，各ピクセルの初期ランダムパターンの値から，埋め込む画像の値の 20%を減算することで摂動を与える. RD システムの性質から埋め込み画像を完全に再現する事ができないが，その特性としてエッジ検出が可能である．RD プロセスのパラメータセットは上述と同様であり，図 5 の画像サイズは 512X512 ピクセルである，図 5(a)に示すように初期ランダムパターンに画像を摂動として埋め込んでいる．6RD サイクル後に，画像を埋め込んだパターンから縞模様が生成される(図 5(b)). 図 5(c)は摂動が与えられていない初期ランダムパターンであり，6RD サイクル後に縞模様が生成される(図 5(d)). 図 5(b)と(d)の値の差を取った画像を図 5(e)に示す(図 4 と同様). 図 5(e)は(b)と(d)の減算によりから得られる図で，元画像からエッジを抽出している．この方法により，画像のエッジ抽出が可能になるが，画像の完全な再構成はできない.

4.3. RD ステガノグラフィによる通信

図 6 は，どのようにして RD ステガノグラフィを用いた通信を実現するかを，図 4 の文字を埋め込むパターンを元に示している．送信者は画像の中にメッセージを隠して送信する．送受信者は共通鍵として，初期ランダムパターン(図 6(a), (b))，RD パラメータ，画像サイズ，β，C, D_u, D_vを持つ．送信者は初期ランダムパターンにメッセージを摂動として埋め込む事で暗号化し，RD システムで反応拡散処理を行う．図 6 (e)は暗号化後の画像である．この後に送信する．メッセージ受信後，受信者は鍵の一部である初期ランダムパターンから RD プロセスを通して図 6(c)に示す縞模様を生成する．最後に，受信した縞模様と生成した縞模様の差分を取り，隠されたメッセージを抽出する事ができる(図 6 (f)). 送信中のメッセージ(図 6(e))が第三者に傍受されたとしても，鍵のセットが無い状態では抽出できない.

5. まとめ

本研究では，RDCA モデルが RD ステガノグラフィに適している事をシミュレーション上で示した．このモデルを使う事で, メッセージの暗号化(初期ランダムパターンに摂動として文字や画像を埋め込む)と復号化(初期ランダムパターンとメッセージが埋め込まれたパターンをそれぞれ RD プロセスで縞模様にした後に差分を取る)が可能になる．この RD モデルは単純なダイナミクスを持ち，早い RD サイクル数で安定な縞模様を生成するため，計算コストが低い．そのため，

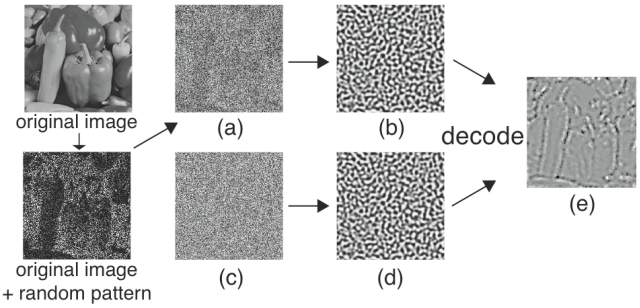

図 5．縞模様生成パラメータによる自然画像を埋め込む二次元パターン生成. (a) 初期埋め込み画像. (b) 6RD サイクル後のパターン．(c) 初期ランダムパターン(d) 6RD サイクル後の初期パターン. (e) 画像抽出((b)と(d)の画像からの差分).

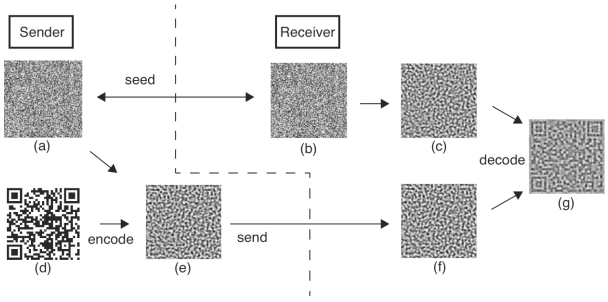

図 6．RD ステガノグラフィによる通信方法.

このモデルを用いて RD ステガノグラフィのハードウェア実装を行なっている．専用ハードウェア化することにより，さらに早い暗号化および復号化を実現できると期待される．その上，より大きいサイズの画像を取り扱うことができるようになると考える.

文　献

[1] L.Saunoriene, and M.Ragulskis “A secure steganographic communication algorithm based on self-organizing patterns,” Phys. Rev. E, vol.84, issue 5, article no. 056213, 2011.

[2] P.Palevicius, L.Saunoriene, and M.Ragulskis “A secure communication system based on self-organizing patterns,” in Proc. of the 2012 Int. Conf. on Security and Management (SAM'12)}, p.421, 2012.

[3] Y.Suzuki, T.Takayama, I.Motoike, and T.Asai “Striped and spotted pattern generation on reaction-diffusion cellular automata: Theory and lsi implementation,” Int. J. Unconv. Comput., vol. 3, pp.1-13, 2007.

[4] A.M.Turing “The chemical basis of morphogenesis,” Phil. Trans. R. Soc. Lond B., vol. 237, pp.37-72, 1952.

[5] D.A.Young “A local activator-inhibitor model of vertebrate skin patterns,” Math. Biosci., vol. 72, pp.51-58, 1984.