ハードウェア向け反応拡散モデルのステガノグラフィ応用とその FPGA 実装

小室勝郎† 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

概要 近年，反応拡散系のステガノグラフィ応用に関する研究が進んでいる．反応拡散系のステガノグラフィ応用のためには，縞状の空間パターンを自己組織化する反応拡散モデルが必須であるが，これまでステガノグラフィに利用されてきた反応拡散モデルは複雑なダイナミクスを有するため，実応用で重要となるハードウェアコストが問題になる．本研究発表では，少ない演算量で縞状の空間パターンを自己組織化する反応拡散モデルを採用し，このハードウェア向け反応拡散モデルがステガノグラフィに応用できることを示す．また，この簡易モデルをデジタル回路化し，FPGA 上に反応拡散ステガノグラフィシステムを実装した．このシステムの評価結果についても併せて報告する．

キーワード: 反応拡散系，ステガノグラフィ，FPGA

1 はじめに

1952年，Alan Turingは空間的パターンの上で拡散が一様な状態から，不一様な安定状態へ移行する現象に対して，拡散不安定性（Turing不安定性）の概念を提唱した．このシステムは，時間変化を反応と拡散の和によって記述する．反応はある点における時間変化での増大の過程を表し，拡散はある点に隣接した点における時間変化での減衰の過程を表している．自己組織化された縞や斑点等のパターンは自然界でも見られる．Turingモデルと呼ばれる反応拡散の自己組織化概念によると，パラメータを制御することにより動物等の体表面に安定した縞や斑点のパターンを生成できることが示されている．現在この反応拡散を利用したステガノグラフィ[1)2)]が研究されており，本研究では，ハードウェア向けの反応拡散モデルを用いてステガノグラフィを実現できることを示す．また，このモデルをFPGA上に実装し，ステガノグラフィに応用できる可能性を示す．

ステガノグラフィとは，データの埋め込みによる最新のデータ隠蔽方法の一つである．メッセージを他のデータの中に埋め込むことにより，送信者と受信者の間でやりとりされる隠されたデータの存在が，第三者に認知されることを防ぐことができる．一方，従来の暗号通信はメッセージを保護するが，通信路で第三者にその存在を認知されてしまう．

ステガノグラフィを用いた通信は，送信者が画像内にメッセージを埋め込んだ後に送信する．通信路上で第三者が傍受した場合，画像自体を認知することはできるが，その中に含まれるメッセージを読み取ることはできず，メッセージの存在さえも認知できない．そして受信者は，秘密鍵を使用して，隠されたメッセージを抽出することができる．

しかし，この従来のステガノグラフィを用いた秘匿通信は，人間の目では隠されたメッセージを検出することが出来ないが，統計分析を用いることで，メッセージが取り出されてしまう危険性を伴う．

このような問題点を解決する為に反応拡散を利用したステガノグラフィが提唱されている[1)2)]．このシステムの概要は以下のようになる．まず送信者と受信者は，ランダムな初期パターンの画像と反応拡散パラメータを秘密鍵として所有する．送信者はランダムなパターン内にメッセージを埋め込んだ後，反応拡散により縞・斑点模様のパターンを生成し，送信する．受信者は秘密鍵である初期パターンと反応拡散パラメータを用いて縞・斑点模様を生成する．そして最後にこれらの差分を取ることで，隠されたメッセージを抽出する．この方法を用いることで，第三者は同じ秘密鍵を入手しない限り，初期パターンから生成した画像内に隠されたメッセージを抽出することができない．

2 反応拡散セルオートマトンモデル

本研究では，簡易なダイナミクスを有する反応拡散モデルとして，反応拡散セルオートマトンモデル[3)]を用いた．このモデルでは，各々のセルの状態は，シグモイド関数と四つの隣接セル間で作用する重み付け加算によって決定される．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，各点(x, y)において，活性因子u，および抑制因子vの二つの状態の差分を取って計算される．uとvによる拡散方程式を，時間δtで積分する．セルの次の状態は，$u-v$のシグモイド関数の値によって決定される．このモデルのダイナミクスは以下のように示される．

1(Diffusion)

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

2(Reaction)

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

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

nは時間のカウント，$\mathbf{r}$は(x, y)座標，cはシグモイド関数のオフセット値，βは関数の勾配の尺度を示して

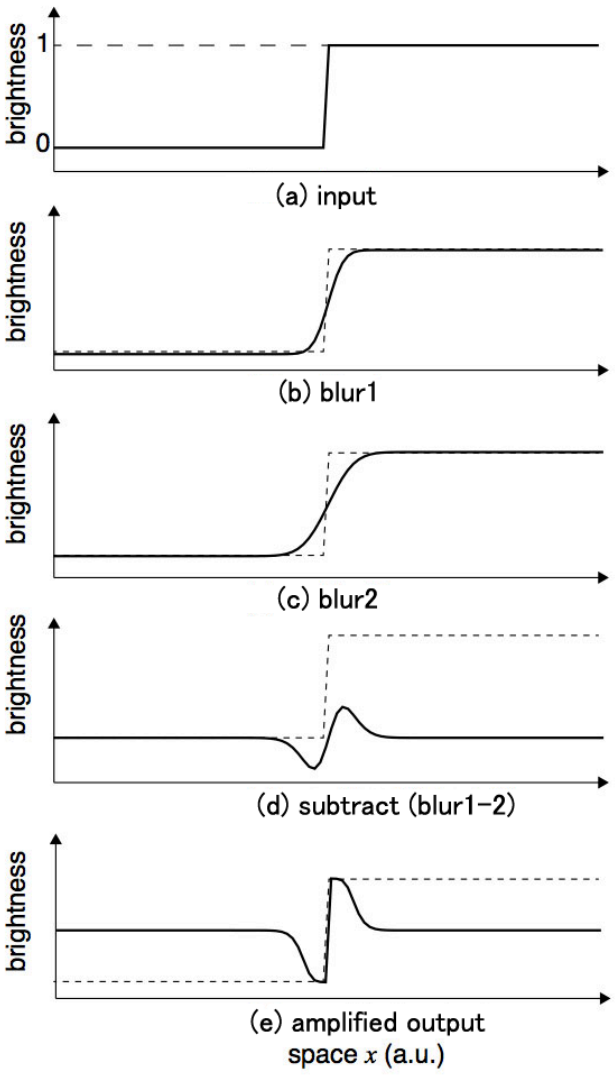

Fig.1: The process of generating stripe patterns in a one-dimensional Reaction Diffusion model: (a) initial conditions (step function), (b) after diffusion for Δt_0, (c) after diffusion for $\Delta t_1 - \Delta t_0$, (d) subtraction of the activator from the inhibitor, and (e) the subtraction in (d) amplified by the sigmoid function.

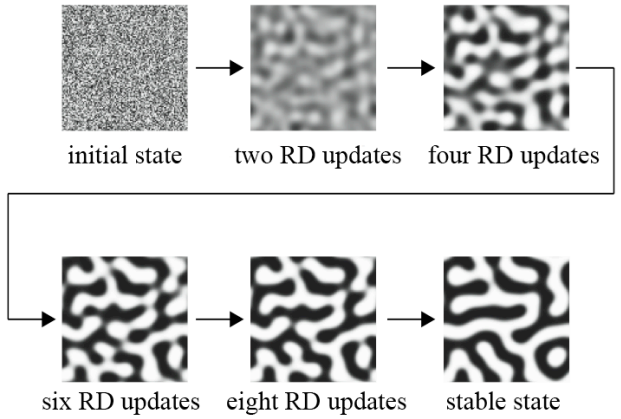

Fig.2: Snapshots of striped patterns for a two-dimensional model with a random initial distribution.

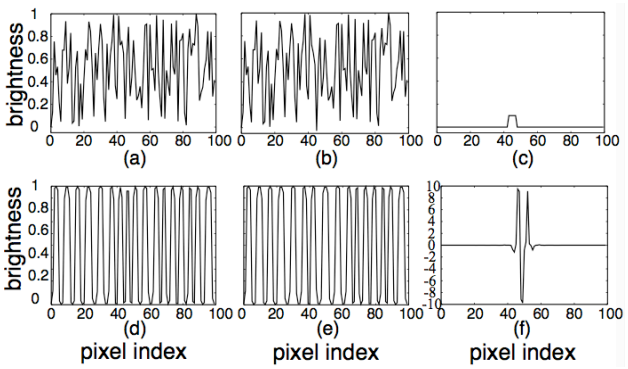

Fig.3: One-dimensional model of Reaction Diffusion steganography. The vertical axis shows the normalized state of the pixels, i.e., prior to starting and after completion of the Reaction Diffusion process. (a) Initial pattern with random initial conditions. (b) Initial pattern that has been perturbed in rows 43 through 47 in an subtractive way. (c) Subtractive perturbation pattern. (d) Final pattern that developed from the random initial conditions. (e) Final pattern that developed from the perturbed initial conditions. (e) Difference of the states in (d) and (e).

いる．Fig.1(a)~(e)は，一次元での反応拡散における波の生成過程を示している．Fig.1(a)はステップ関数を入力した初期状態を示している．Fig.1(b)はステップ関数がδt_0の時点で，パラメータD_vで拡散した後の様子を示している．Fig.1(c)はδt_1-δt_0間で拡散させ，パラメータD_uでステップ関数を変化させたことを示している．Fig.1(d)はFig.1(b)とFig.1(c)の差分であり，これは活性因子と抑制因子の差分に相当することを示している．最後にこの差分がシグモイド関数により増幅される様子をFig.1(e)に示す．ここで，Fig.1(e)に示される生成波形を，再び反応拡散モデル式に代入するプロセスを，入力信号の“更新”と定義する．一次元の縞のパターンは，この更新を繰り返すことによって形成される．同様に，Fig.2では二次元モデルの縞のパターン形成の一例を示している．入力信号を出力信号で更新するプロセスを繰り返すことで、安定した縞のパターンが形成されることがわかる．

3　一次元での反応拡散によるステガノグラフィ

ここでは，反応拡散セルオートマトンモデル（上記の波形処理）をステガノグラフィに適用させた様子を解説する．Fig.3 は，8 ビットの値を持つ，100 個のセルが直列に接続された一次元上で，反応拡散によるステガノグラフィを実行する際の原理を示している．

まず初期条件として，境界条件は一定の空間周波数を持つパターンの生成を可能にするように設定されている．各セルの初期値はガウシアンノイズによりランダムな値に設定する．次に，摂動としてメッセージを組み込む．摂動は反応拡散のパラメータの一つとして利用され，ここでは43～47番目のピクセルの値を，初期値の約10%減算するように作用する．

初期ランダムパターンをFig.3(a)に，初期の波形に摂動としてメッセージを組み込んだ状態をFig.3(b)に示す．波形の中央が摂動によりわずかに減少しているのがわかる．Fig.3(c)は，初期状態とメッセージとして摂

動を組み込んだ状態の差分を示している．そして初期状態と，摂動を組み込んだ後の状態の波形に対し，反応拡散による入力波形の更新プロセスを6回繰り返し，安定させた波形の状態をFig.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見なせる．Fig.3(f)はその二つの波形の差分を取った様子を示している．この波形を観測することで隠されたメッセージを抽出できていることがわかる．これは摂動としてメッセージを埋め込んだ際に生じたわずかな変化が，インパルス応答特有の性質により増幅されて得られる結果である．波形中央の周囲に見られるエッジは，最初に隠したメッセージの境界を検出した結果であり，エッジの外側の領域が平坦な値を示していることから，メッセージ部のみが反応拡散による変化に影響し，その周囲は影響していないことがわかる．

4 二次元での反応拡散によるステガノグラフィ

ここでは，ステガノグラフィシステムを二次元画像の反応拡散ステガノグラフィアプリケーションとして利用できるように拡張した行程を示す．反応拡散が十分に行われた後隠蔽したデータが視覚的に判別できないようにする為，初期のランダムパターンに摂動として文字を隠蔽する．

Fig.4 では，100×100 ピクセルのランダムな初期パターンに，メッセージ“T”のドット状の画像を摂動として埋め込んでいる．この画像の境界条件は固定されており，明るさは 8 ビットに設定されている．Fig.4(a)より，“T”のドットが初期状態の摂動として埋め込まれていることが視認できる．これに対して反応拡散処理を施し，6 回更新を行った後の様子を Fig.4(b)に示す．縞模様を見る限り“T”は視認できない．Fig.4(c)は、摂動を与えていない初期のランダムパターンを示している．Fig.4(d)は，摂動を含まない初期パターンに対して反応拡散処理を施し，縞模様が形成された後の様子を示している．Fig.4(b)と Fig.4(d)で得られた縞模様は，視覚的には同様の画像に見えるが，Fig.4(e)に示すように，Fig.4(b)と Fig.4(d)の画像データの差分を取ることで，最初に隠したメッセージ“T”が観測できる．一方で，“T”に隣接する境界が周辺に拡散してしまっていることもわかる．

Fig.5 では反応拡散によるステガノグラフィ技術を用いて，自然画像を隠蔽できる可能性を示している．自然画像を埋め込んだ際は，文字を埋め込んだ場合と同様に，画像の輪郭部分は検出されるが，それ以外の領域は基本的に完全に復元することができない．この自然画像の反応拡散プロセスには 512×512 ピクセルを使用している．Fig.5(a)は初期ランダムパターンに摂動として自然画像を埋め込んだ様子を示している．Fig.5(b)は Fig.5(a)に対し反応拡散処理を施し 6 回更新した後の様子を示す．摂動によって初期ランダムパターンから縞模様が形成され，元の画像を視認することができなくなることがわかる．Fig.5(c)は、摂動を与えていない初期ランダムパターンの状態を示している．Fig.5(d)は，反応拡散を引き起こさせた後に形成された縞模様を示している．Fig.5(e)は Fig.5(b)と Fig.5(d)で観測されたデータの差分を示している．差分を取ることによって元の画像の輪郭を検出することができる．前述した通り，この方法では画像の輪郭の検出は可能であるが，完全な元画像を復元することはできない．

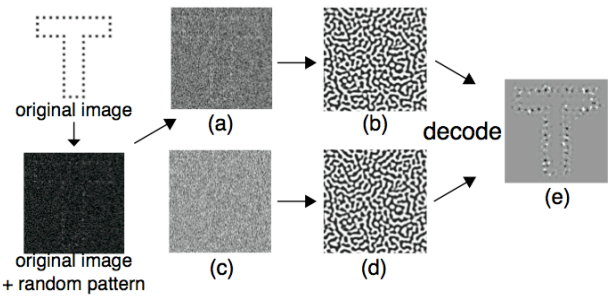

Fig.4: Two-dimensional pattern evolution with striped formation parameters. The shape of a “T” is hidden, which is formed by a solid-block perturbation. (a) Initial perturbed state. (b) Pattern state after six Reaction Diffusion cycles. (c) Initial random image state. (d) Pattern state after sic Reaction Diffusion cycles. (e) Image resulting from the difference of images in (b) and (d).

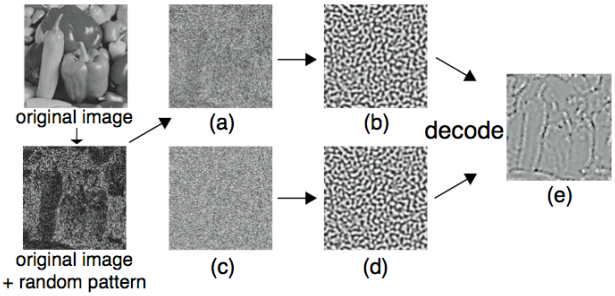

Fig.5: Two-dimensional pattern evolution with striped formation parameters. A natural image (peppers) is hidden, which is formed by a solid-block perturbation. (a) Initial perturbed state. (b) Pattern state after six RD cycles. (c) Initial random image state. (d) Pattern state after six Reaction Diffusion cycles. (e) Image resulting from the difference of images in (b) and (d).

Fig.6 は反応拡散によるステガノグラフィを用いた安全な通信を実現する方法を示している．送信者は，受信者へ秘匿メッセージを画像として送信する．送信者と受信者は、反応拡散を引き起こす為のパラメータと，画像サイズが同一な初期ランダムパターン(Fig.6(a, b))を秘密鍵として所有する．送信者は，初期ランダムパターンに摂動としてメッセージを埋め込み，反応拡散システムを通して画像を変化させる．Fig.6(e)は，送信するメッセージに対して反応拡散処理を行った後の画像である．受信者は送信者が反応拡散処理を施して変化させた画像を受信した後，秘密鍵のひとつである元画像 Fig.6(b)に反応拡散処理を施す(Fig.6(c))．そして二つの画像(Fig.6(c, f))の差分を取り，Fig.6(g)に示される画像を取り出す．この方法では，完全な秘密鍵（初期ランダムパターンと反応拡散パラメータ）を用いない限り，隠蔽されたメッセージを取り出すことはできない．すなわち，縞模様に隠された画像の輪郭を検出することができないということになる．よってメッセージを送信する際，反応拡散パラメータおよび摂動の強度によって秘匿性が向上することがわかる．

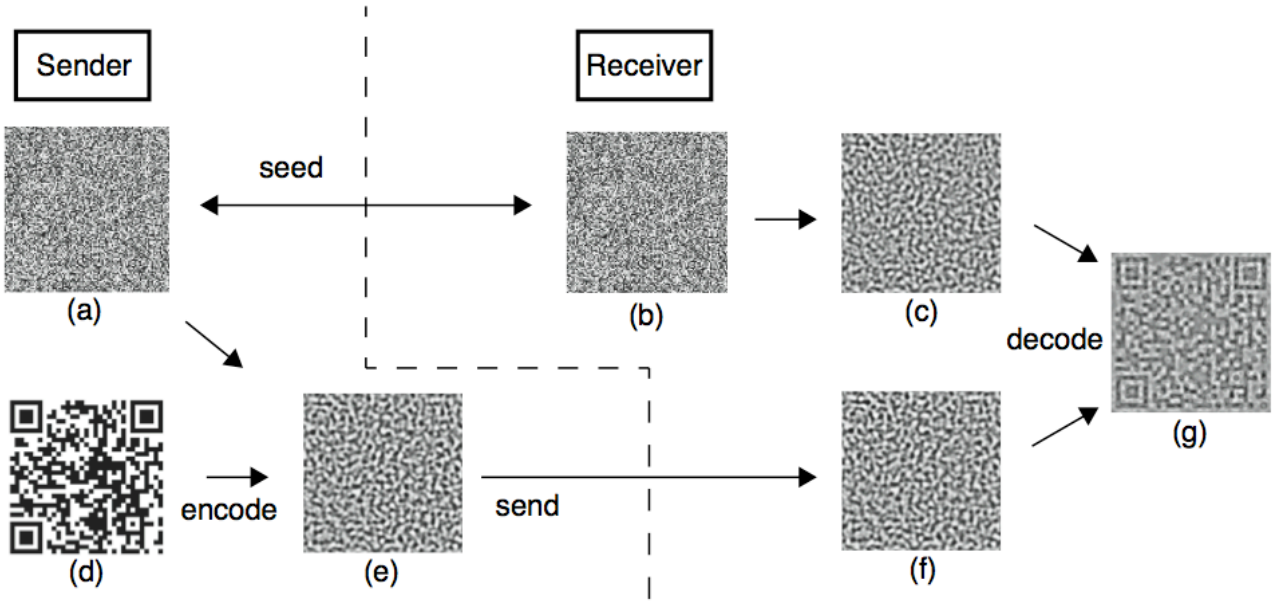

Fig.6: A method for a secure communication using RD-based steganography.

5 簡易モデルを用いた一次元反応拡散プロセッサの実装

前述のシミュレーションにより，反応拡散セルオートマトンモデルをステガノグラフィに応用できることが確認できた．ここではこのシステムをデジタル回路化し，実装するまでの過程を示す．

Fig.7 に反応拡散プロセッサのアーキテクチャを示す．このアーキテクチャは Fig.8 に示す波生成の様子に対応している．ここではステップ関数を入力として用いている．このアーキテクチャのフィルタ部は，ぼかしの強度が異なる二つのフィルタで構成されており，各フィルタが二つの異なる波形を出力した後，差分計算し，増幅を行うことで反応拡散を実現する仕組みになっている．

Fig.9 はそのアーキテクチャのフィルタ部の構成を示している．入力波形は，まず始めにメモリ内部に格納される．その直後初期状態の波形をメモリから取り出し，カーネル 1 とカーネル 2 で構成されたフィルタに通す．これらのカーネルはぼかし強度の異なる二つのフィルタで構成されており，フィルタから排出されたデータの差分を計算することで出力波形が得られる．このユニットの構成は一般的にラプラシアンフィルタと呼ばれ，エッジ検出や先鋭化に用いられるフィルタの一種である．二つのフィルタを通す際，処理するデータ幅が異なることから出力の遅延が発生するため，フィルタを通した後基準となるデータ幅に調整する．その後それら二つのフィルタから出力されたデータの差分を取りアンプで増幅させ，波形を出力する．出力された波形は逐次メモリに更新し，次の入力波形として読み出される．

このアーキテクチャは，前述のシミュレーションで使用した反応拡散方程式を簡略化したラプラシアンフィルタに置き換えることで構成されていることから，ハードウェアに実装する際の大幅なコストダウンを計ることができると予想される．

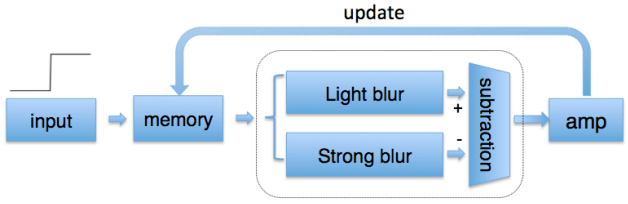

Fig.7: Concept of the digital Reaction Diffusion processor.

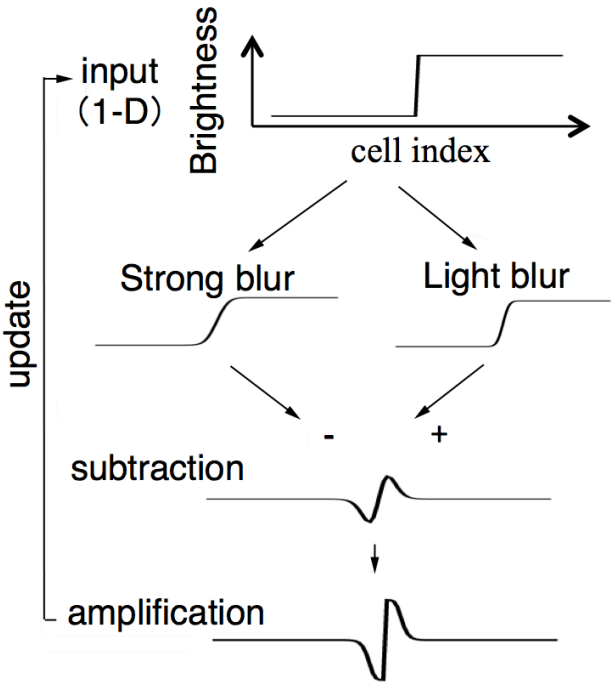

Fig.8: Show input waveform for through the filter in Reaction Diffusion.

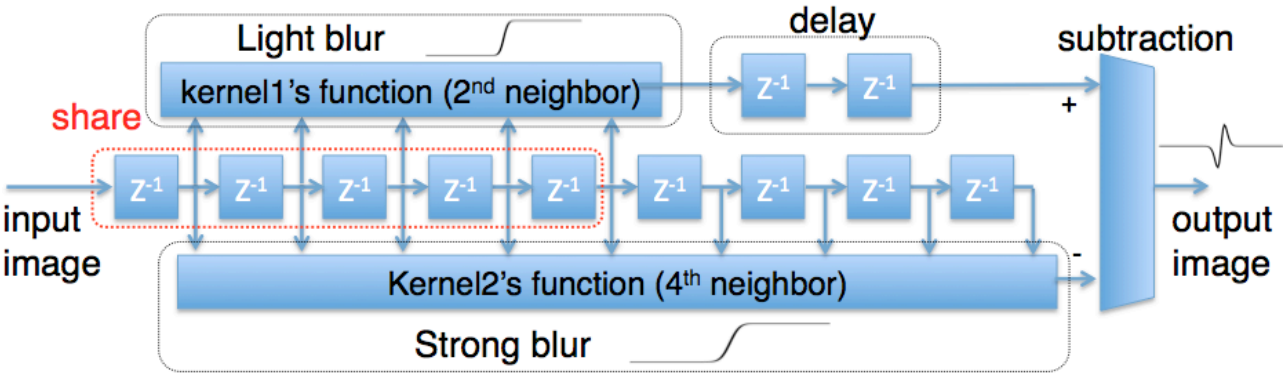

Fig.9: A digital laplacian filter for Reaction Diffusion (1D).

次に、この一次元反応拡散プロセッサを FPGA に実装した結果を示す．Fig.10 は FPGA に反応拡散プロセッサを実装し，ステップ関数を与えて反応拡散を行った結果を示している．横軸は入力波形のセルで，中心の位置を固定して出力データが変わっていく様子を表している．縦軸は更新の回数を表している．FPGA には SRAM が配置されており，この SRAM は最初入力波形の情報を保存し，フィルタを介して差分計算された後の出力される波形によって逐次データを更新する．更新されたデータは，直後に入力波形としてフィルタに通される．反応拡散を繰り返していくことで，始めはステップ関数だった波形から，徐々に波が生成されていく様子が観測できる．

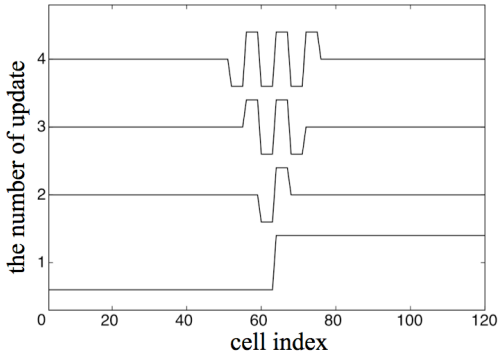

Fig.10 Implementation results for FPGA (1D)

6 簡易モデルを用いた二次元反応拡散プロセッサの実装

ここでは，一次元の反応拡散プロセッサをもとに、二次元の反応拡散プロセッサを実装するまでの過程を示す．Fig.11 は，一次元の反応拡散プロセッサを応用した二次元の反応拡散プロセッサの構成を示している．二次元のアーキテクチャでは，x 軸，y 軸の二方向を処理するが，この演算を短縮するためには処理の並列化が必要になる．一次元で用いたラプラシアンフィルタを二つ用意し，それぞれ x ラプラシアンフィルタ，y ラプラシアンフィルタとし，さらにその二つのフィルタの直後に x メモリと y メモリといった二つのメモリを用意する．また，画像を処理するメモリは，一次元で用いた 1 ポート SRAM とは違い，2 ポート SRAM を使用する．2 ポート SRAM を使用することにより，x 軸，y 軸のフィルタ処理を並列化することができる．そして x 軸，y 軸それぞれの出力を加算器に通し，アンプで極値化し，SRAM に出力を返す．このサイクルを繰り返すことによって，二次元の反応拡散を行う．

二次元反応拡散プロセッサの出力の様子を Fig.12 に示す．画像サイズは，45×45 のものを使用している．まず中心に初期値としてインパルスを与えた画像データを用意する．これを初期状態とし，反応拡散させていく．反応拡散を繰り返すと，波が x 軸，y 軸それぞれの方向に二次元的に広がっていく．この結果から，より簡素なモデル式を用いることで二次元の反応拡散プロセッサを実装できることが示された．

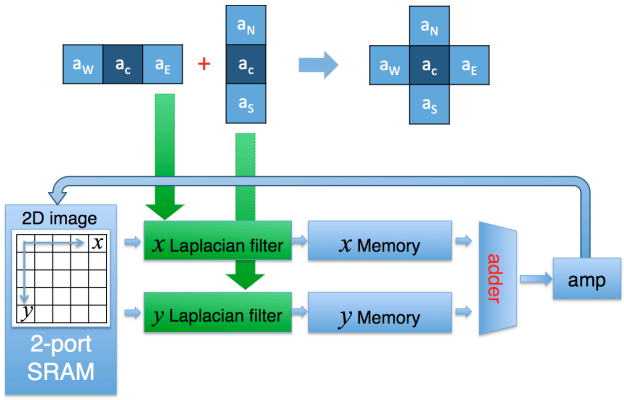

Fig.11: A 2D digital Reaction Diffusion processor

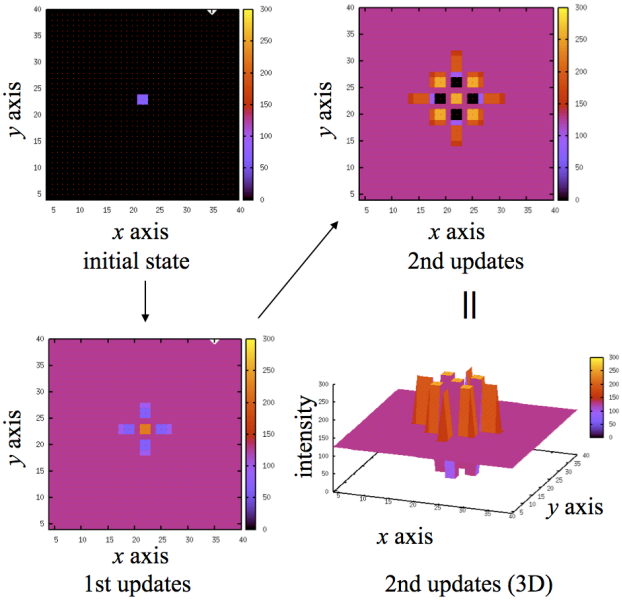

Fig.12: Implementation results for FPGA (2D)

7　まとめ

反応拡散を応用したステガノグラフィ技術はシミュレーション上での動作は可能だが，モデル式が複雑なことから工学的応用が難しかった．そこで，より簡潔で同様の動作が可能な反応拡散システムを応用することで，ハードウェア化できる可能性を示した．まず一次元反応拡散プロセッサを FPGA に実装し，波が伝搬する様子を観測することができた．そして一次元で用いたアーキテクチャを応用することで，二次元反応拡散プロセッサを構成することができた．今後はこの二次元反応拡散プロセッサを利用した秘匿通信を実現できるように適用させていくことが課題となる．

参考文献

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. Tagulskis “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 1si 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.
6) K. Ishimura, A. Schmid, T. Asai M. Motomura “Image Steganography based on Hardware-oriented Reaction-diffusion Models”, NOLTA 2013.