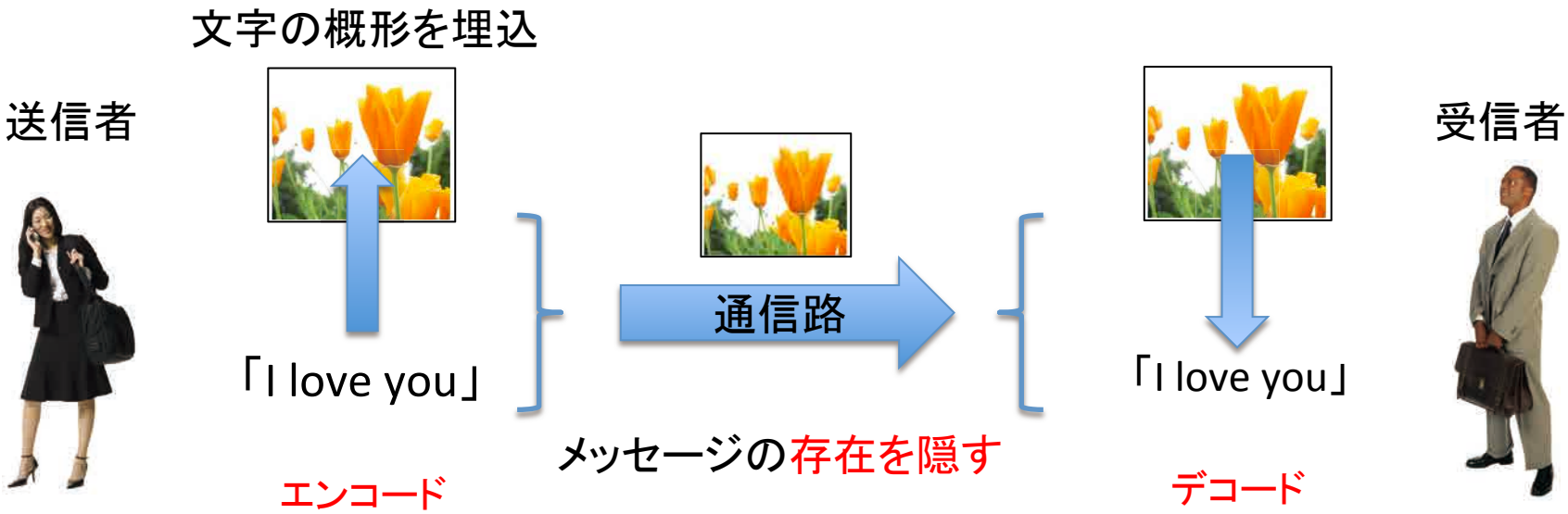
学生27

統計的解析法に耐性のあるステガノグラフィアルゴリズムとそのFPGA実装

石村　憲意[1]　小室　勝郎[1]　Alexandre Schmid[2]
浅井　哲也[1]　本村　真人[1]
[1]北海道大学大学院情報科学研究科
[2]Swiss Federal Institute of Technology (EPFL)

ステガノグラフィとは

ステガノグラフィ：音声や画像などのデータに秘密のメッセージを埋め込む技術

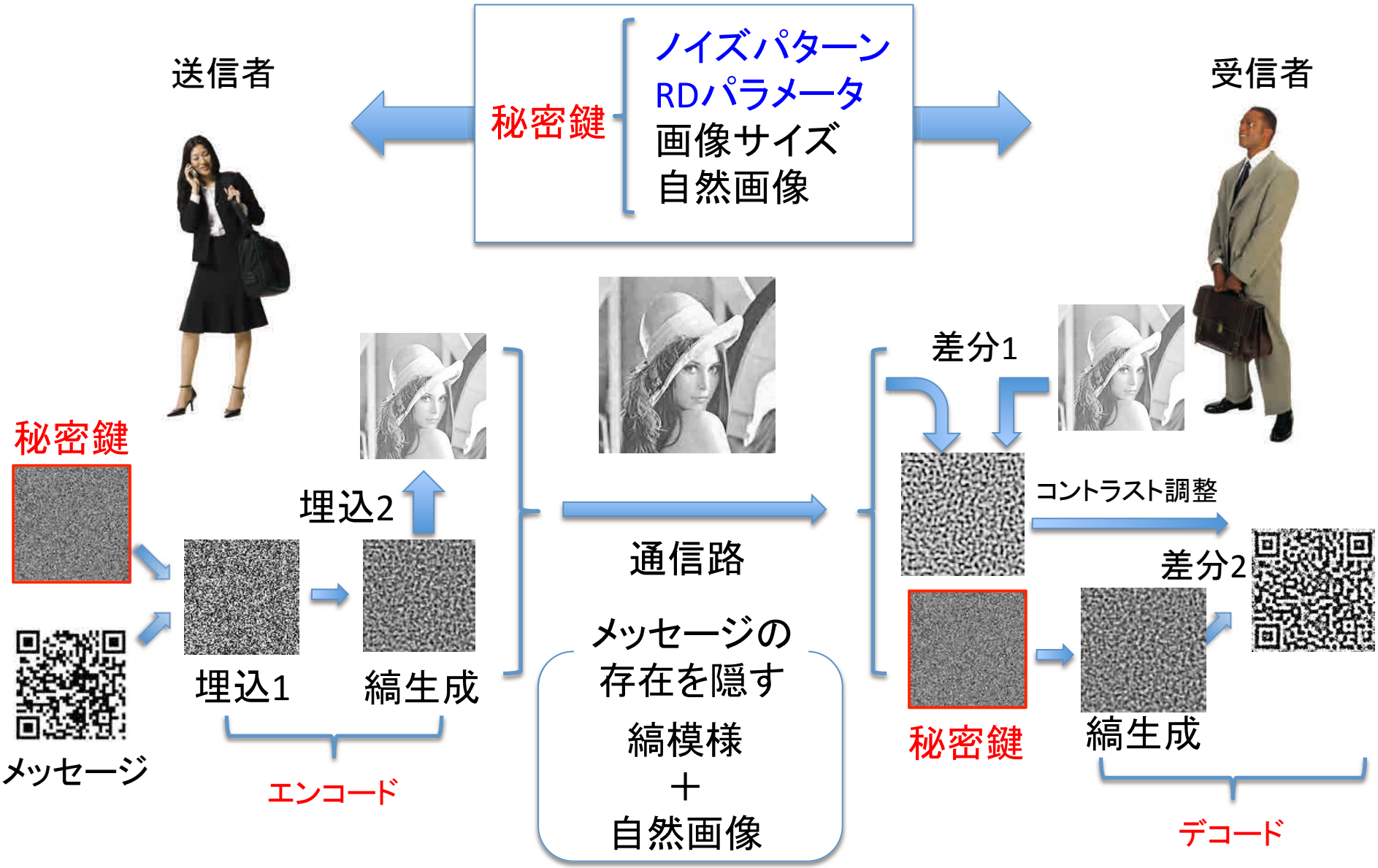


既存技術：冗長性を持った音声・画像データの中に隠したいデータを織り込ませる
（統計的分散から解析できてしまう場合がある）

ステガノグラフィに**反応拡散系**を利用する方法が提案されている[1]

[1] L. Saunoriene and M. Ragulskis" **Secure steganographic communication algorithm based on self-organizing patterns**."
Phys Rev E Stat Nonlin Soft Matter Phys. 2011

反応拡散(RD)ステガノグラフィ



反応拡散(縞模様生成)によるエンコードおよびデコードキー生成

エンコード前とデコード後のメッセージ比較

差分の
絶対値

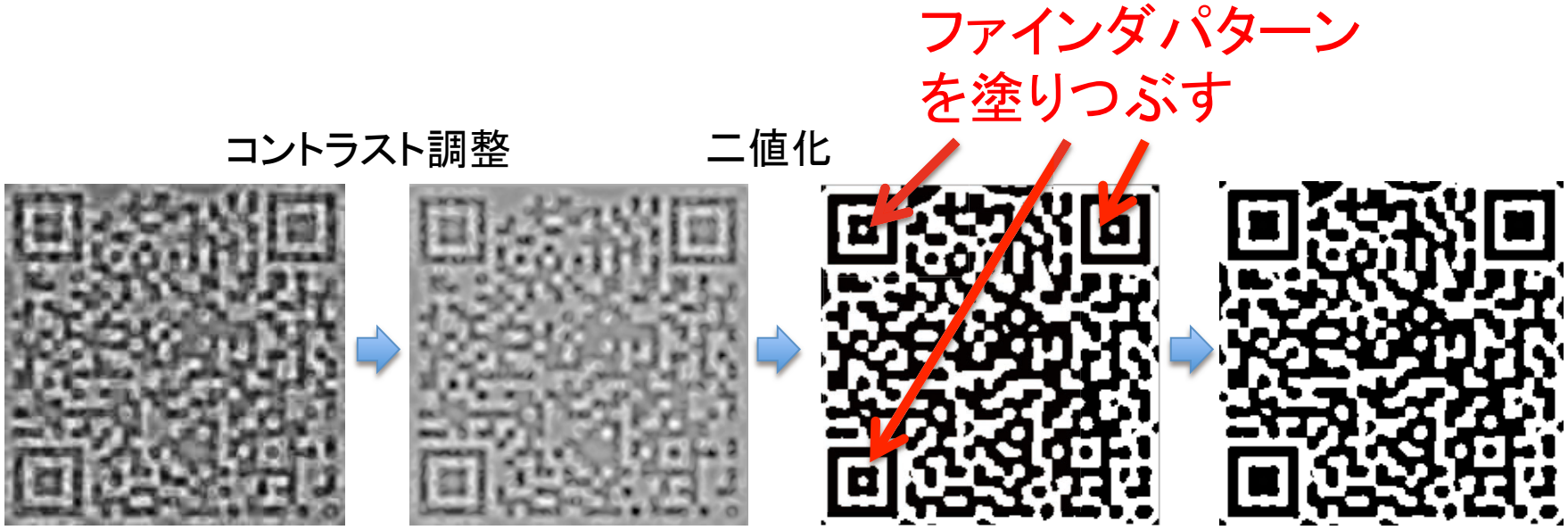
無視出来る
エラー

境界線
パターン内部

修正が必要な
エラー

ファインダパターン
内部のエラー3カ所

RDステガノグラフィのデコードの後処理

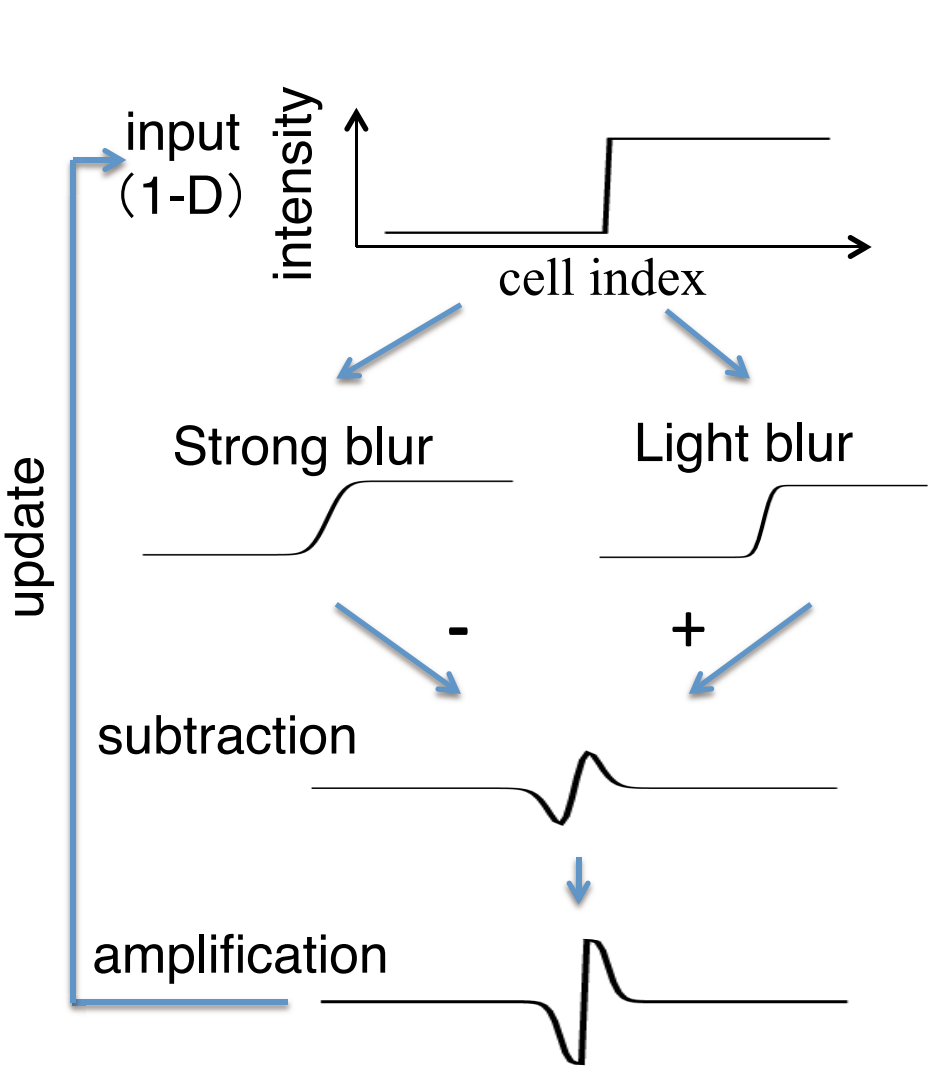


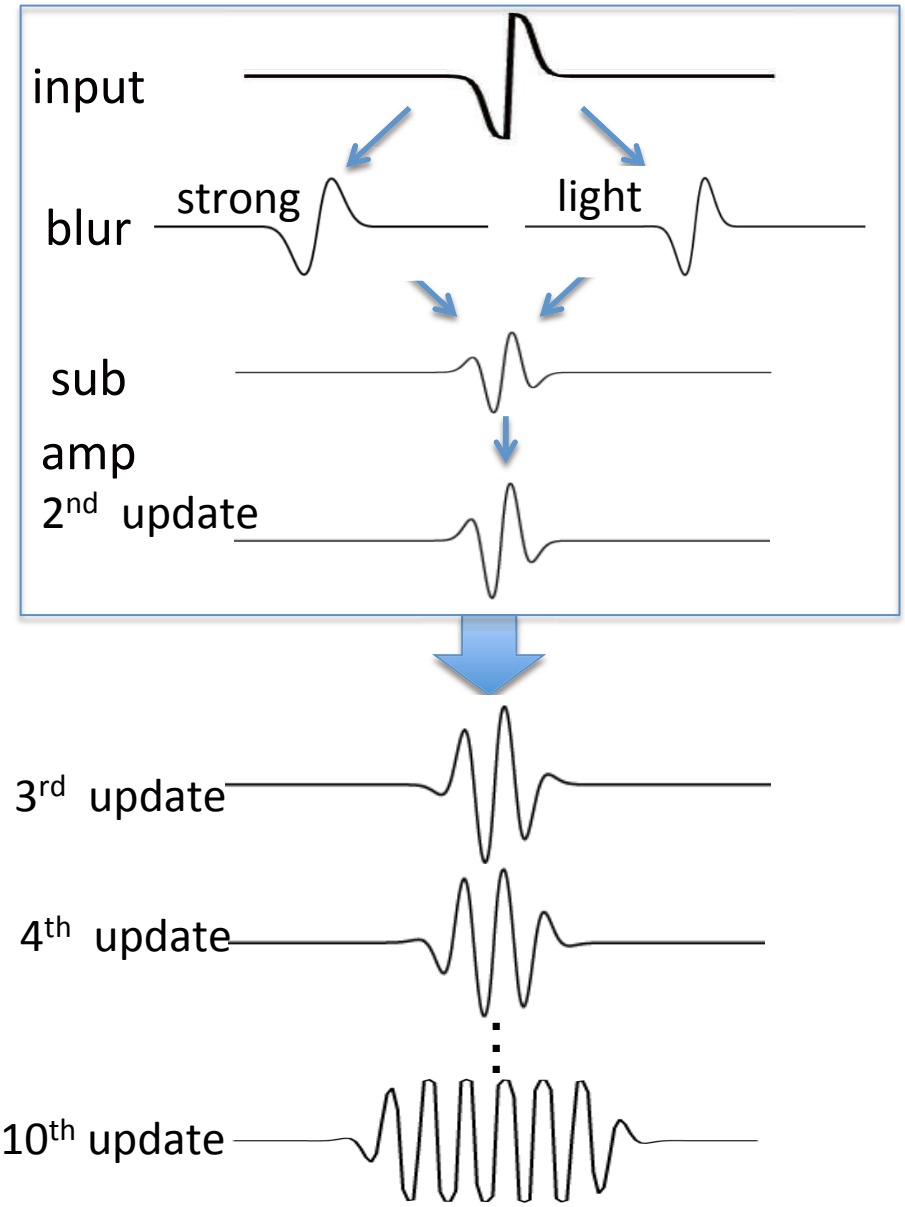
メッセージ埋め込みから読み取りまで
シミュレーションで確認

RDステガノグラフィの
ハードウェア実装へ

ハードウェア化が容易な縞模様生成モデルを利用

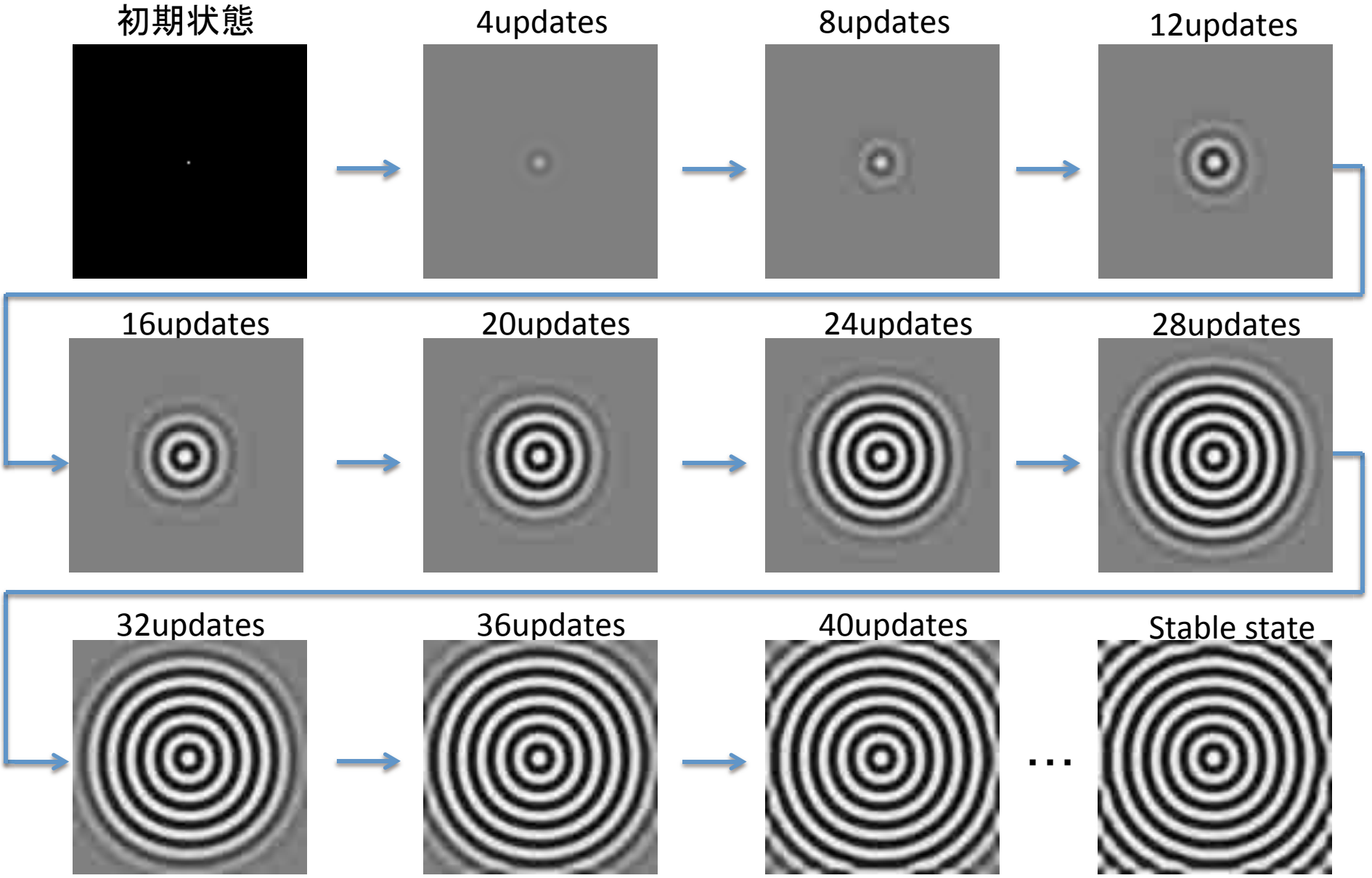
反応拡散セルオートマトン(RDCA)モデル[2]





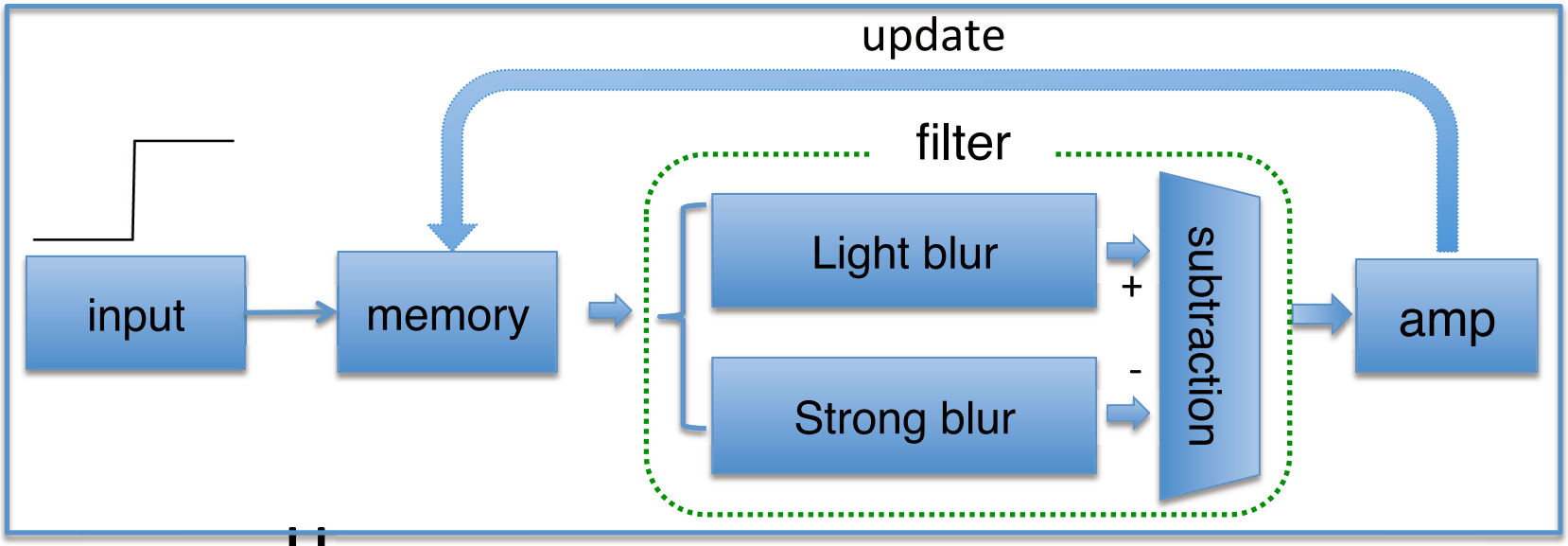
[2] Asai T. and Motoike I.N., "Self-organizing striped and spotted patterns on a discrete reaction-diffusion model," Nonlinear Theory and Its Applications, vol. 2, no. 3, pp. 363-371 (2011).

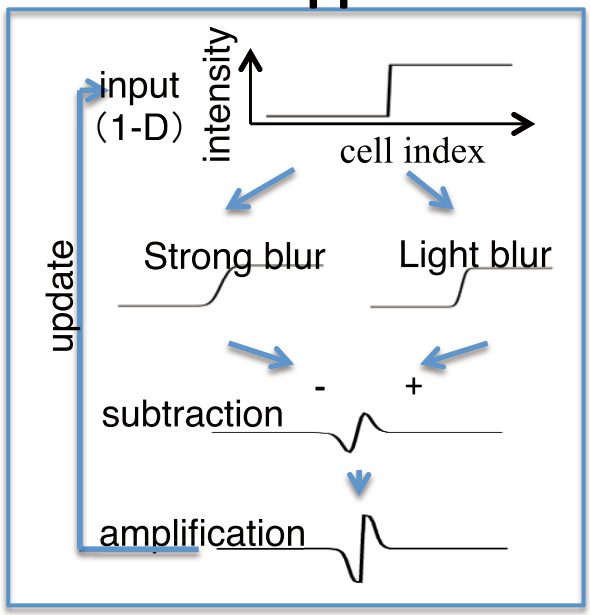
RDCAモデルの二次元シミュレーション(インパルス)



縞模様を生成するRDCAモデルのハードウェア実装へ

一次元ディジタルRDプロセッサのアーキテクチャ





メモリから値を読み出し

↓

強度の異なる二つのぼかしフィルタ処理

↓

差分を取って小さな波を生成

↓

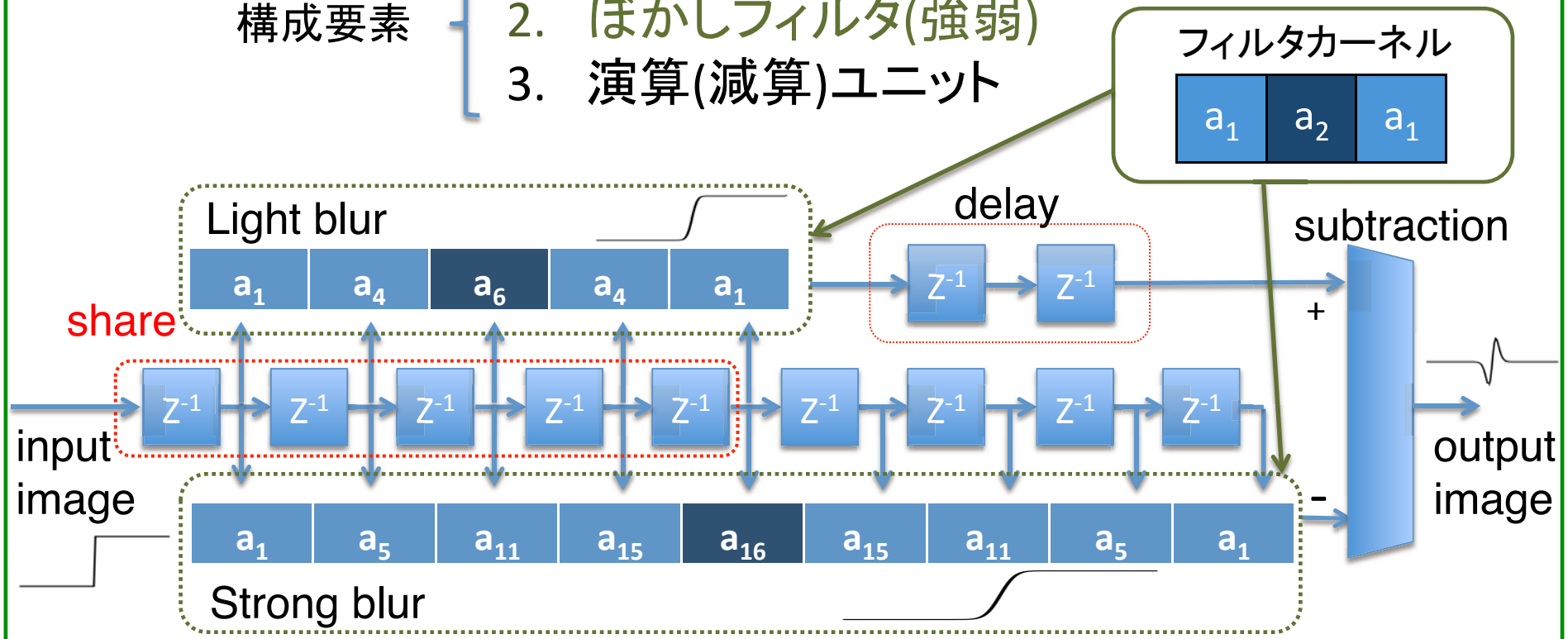
増幅してメモリに書き戻して更新

↓

繰り返すことで一次元方向に波が生成

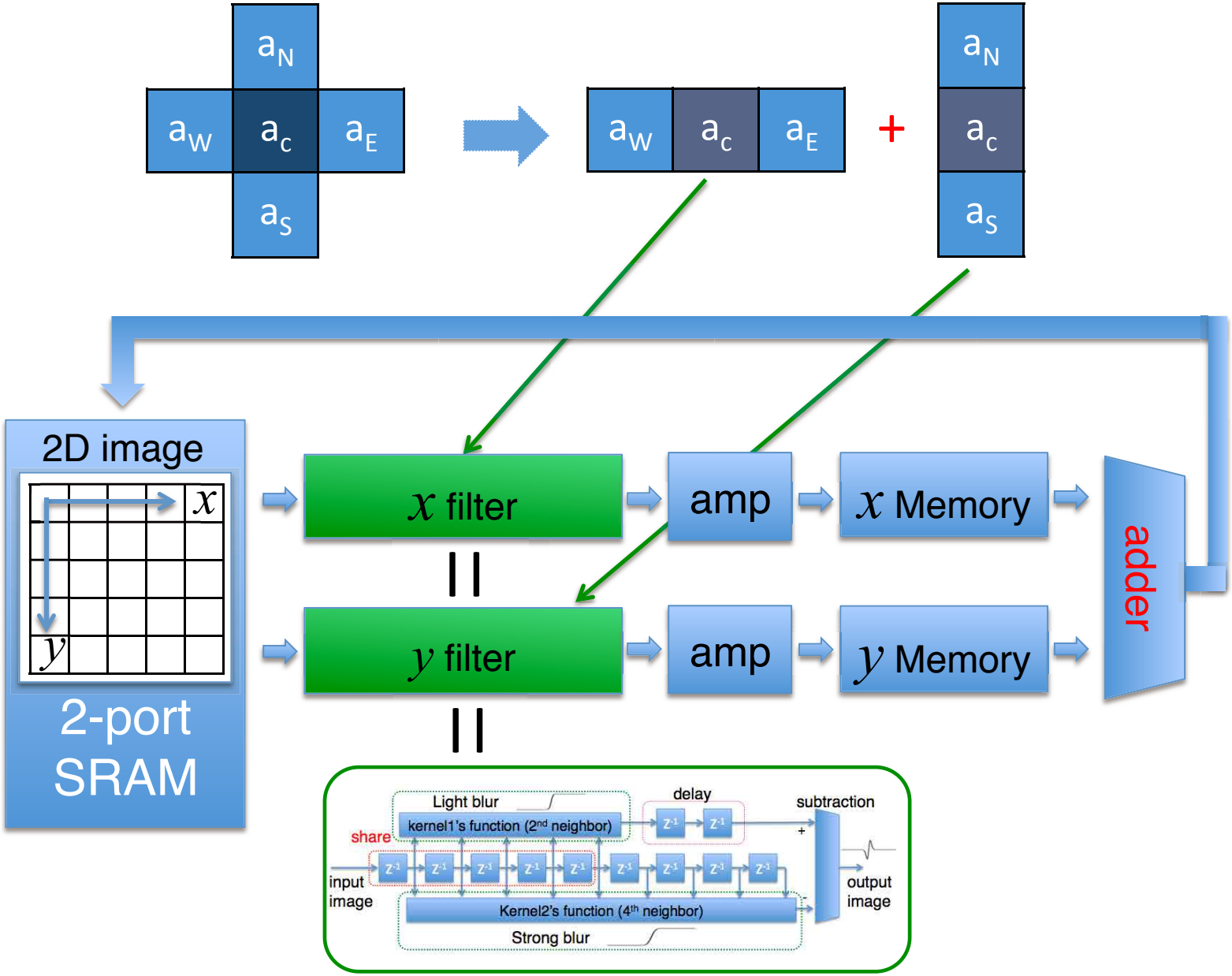
フィルタ設計

構成要素
1. ストリーム処理可能なI/O
2. ぼかしフィルタ(強弱)
3. 演算(減算)ユニット

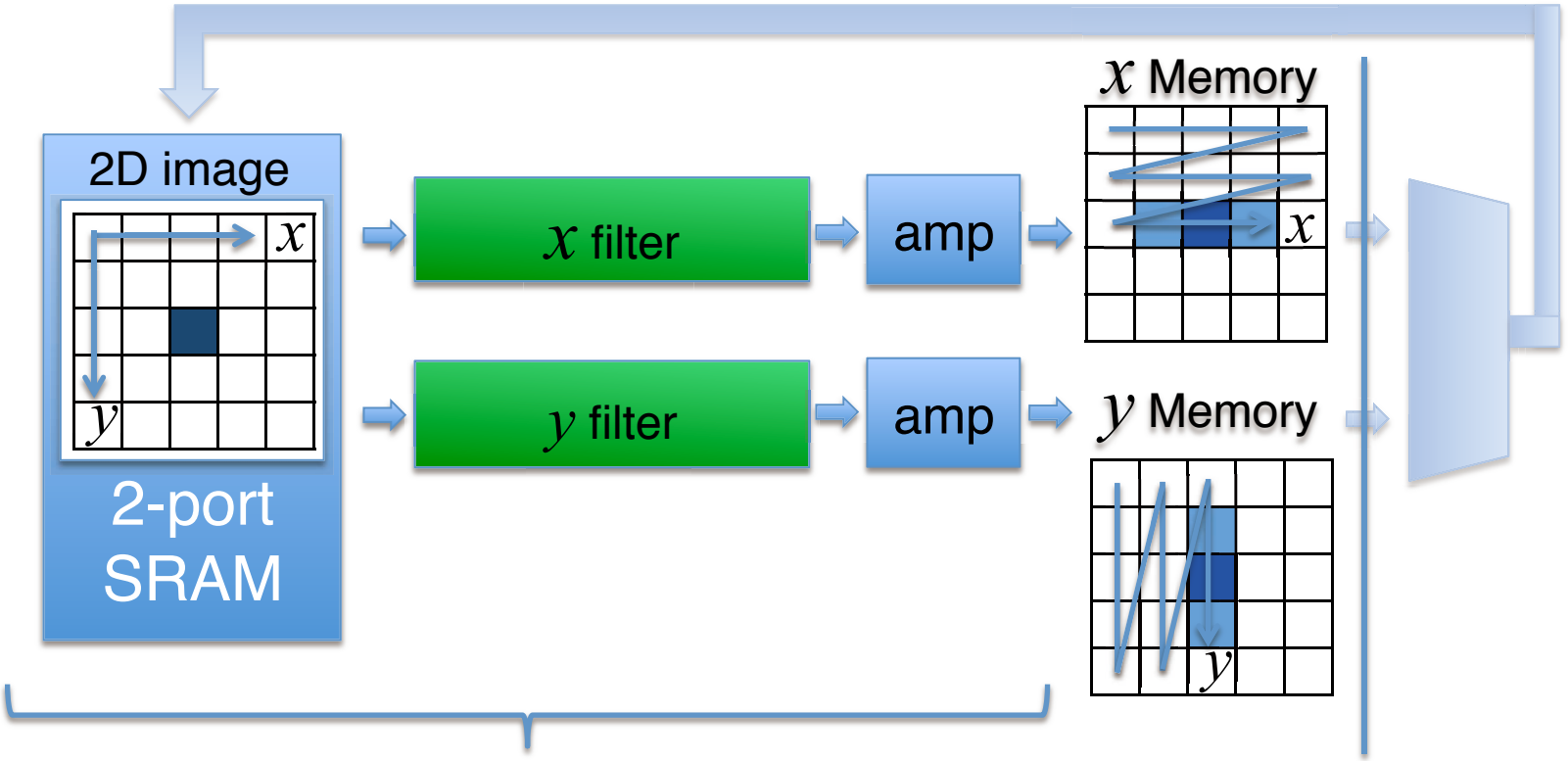


Design note:
1. ぼかしフィルタの一部レジスタの共有
2. Delayレジスタによる減算タイミング調整

ディジタルRDプロセッサアーキテクチャの二次元への拡張



二次元ディジタルRDプロセッサの動作1/2

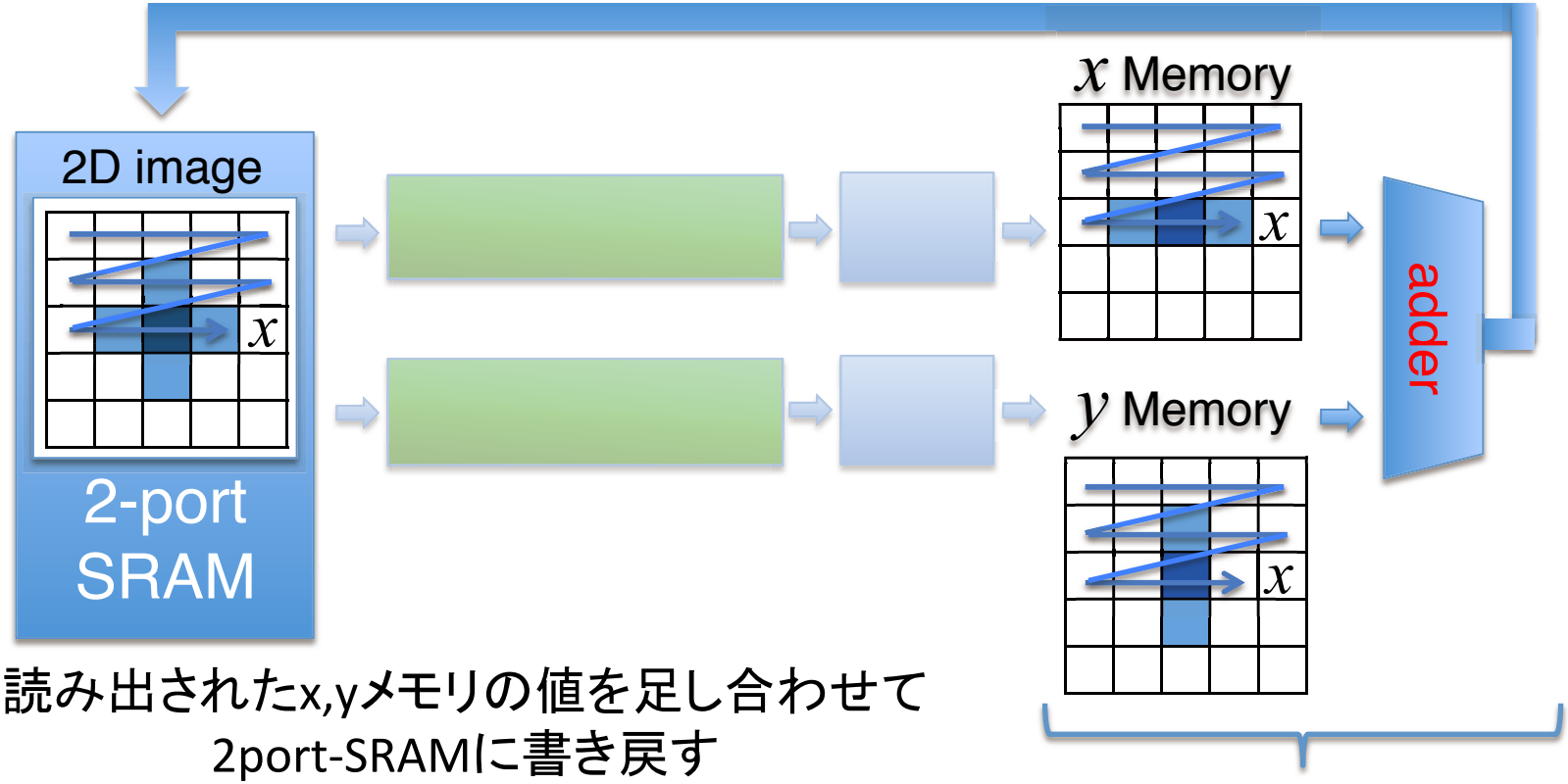


二種類のアドレスカウンタを用いて
x,y軸方向に分解して読み出し

並列ぼかし処理

メモリと同容量のバッファx2を
用いてタイミング調整

二次元ディジタルRDプロセッサの動作2/2



読み出されたx,yメモリの値を足し合わせて
2port-SRAMに書き戻す

二次元に拡散した結果が得られる

二つのメモリから
同方向に読み出し

以上二つの動作フェーズを繰り返す

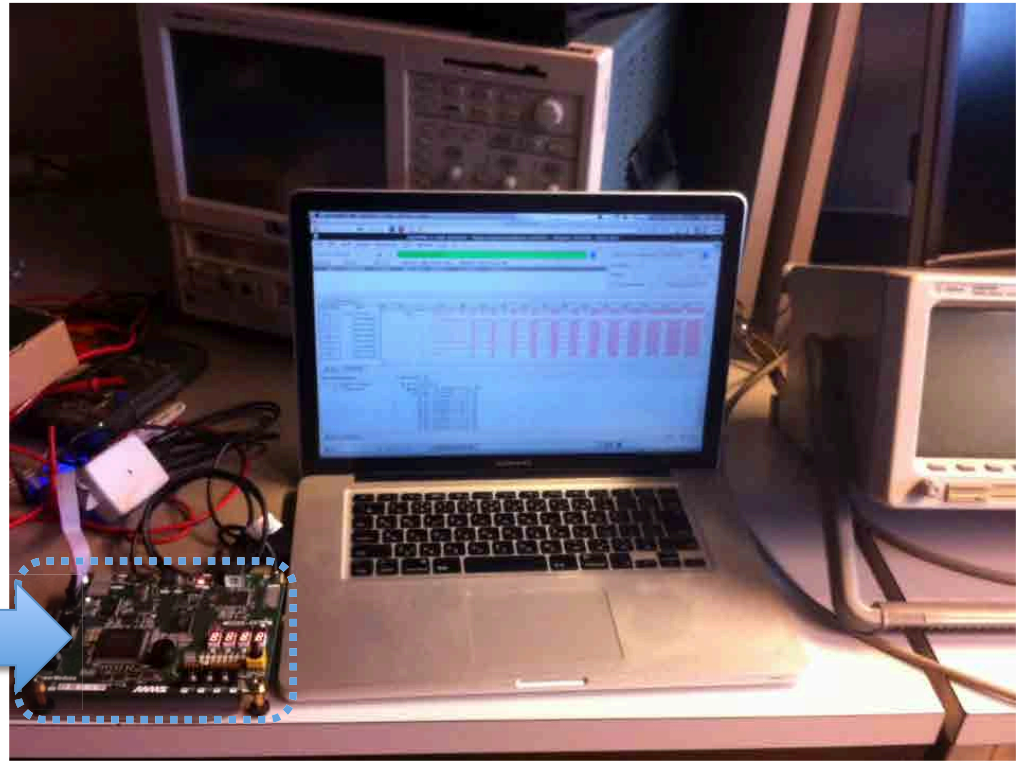
縞模様生成

RDステガノグラフィの FPGA実装環境

MU200-EK specs:

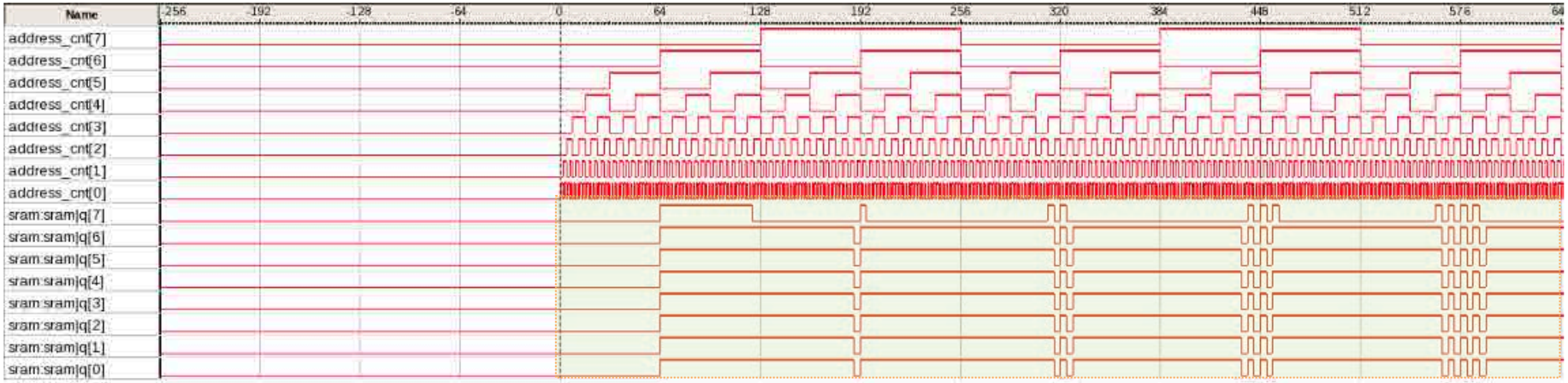
Cyclone II(EP2C5)

Total logic elements: 4,608
Total combinational functions: 4,608
Dedicated logic registers : 4,608
Total registers: 593
Total pins: 142
Total memory bits: 119,808
Embedded Multiplier
9-bit elements: 26
Total PLLs: 2
Total LUT:7000



Verilog HDL on QUARTUS II

一次元ディジタルRDプロセッサの実装結果



Number of cells: 128

Depth: signed 8-bit

Boundary: Neumann

Clock freq: 10MHz

Total logic elements: 1,275 / 4,608 (28 %)

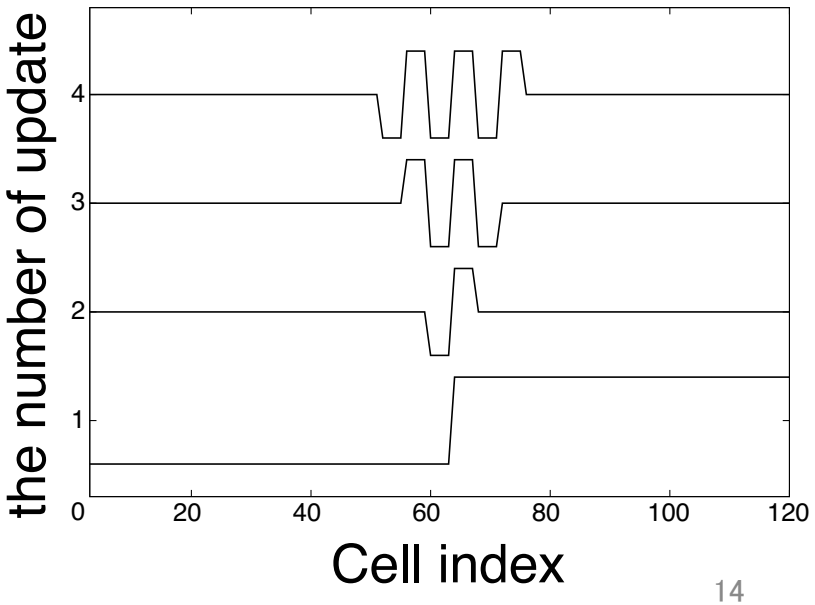
Total combinational functions: 1,044 / 4,608 (23 %)

Dedicated logic registers: 593 / 4,608 (13 %)

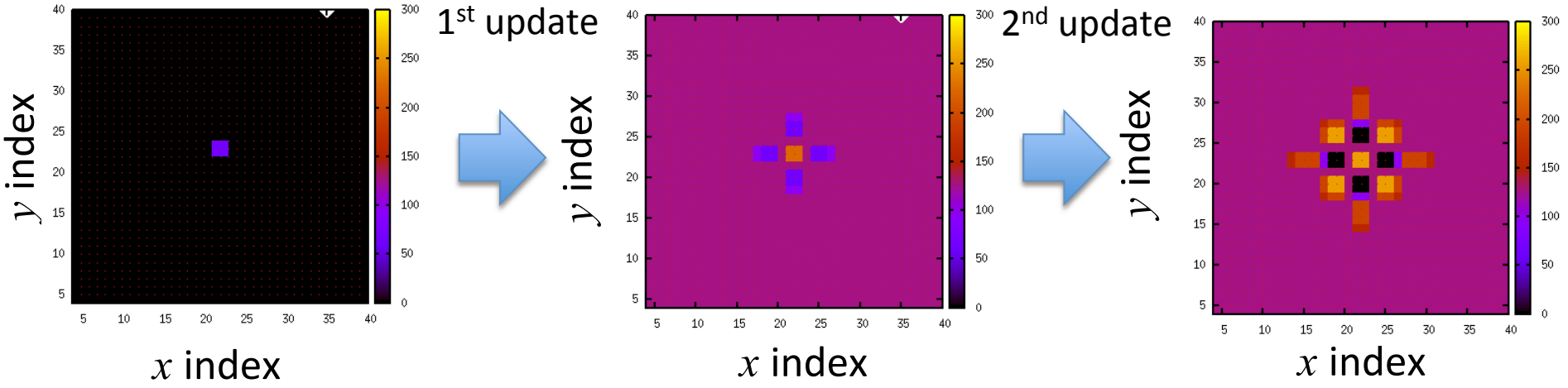
Total registers: 593

Total pins: 6 / 142 (4 %)

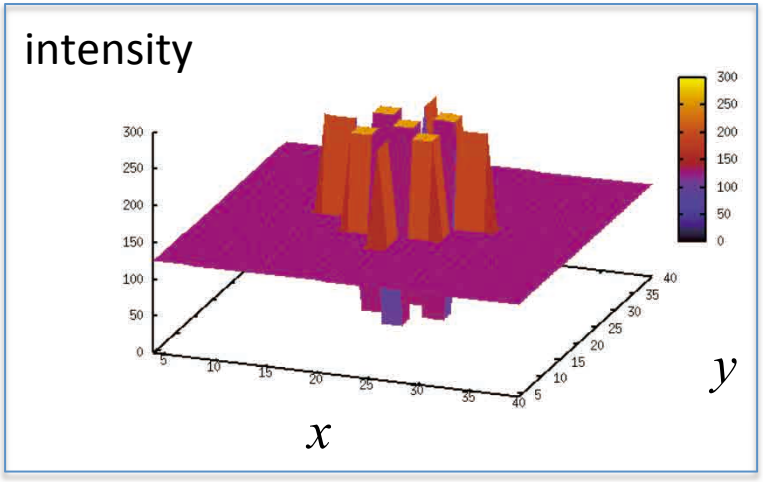
Total memory bits: 55,296 / 119,808 (46 %)



二次元ディジタルRDプロセッサの実装結果



=



Number of cells: 45x45

Depth: signed 8-bit

Boundary: Neumann

Clock freq: 10MHz

Total logic elements 2,520 / 4,608 (55 %)

Total combinational functions 2,282 / 4,608 (50 %)

Dedicated logic registers 849 / 4,608 (18 %)

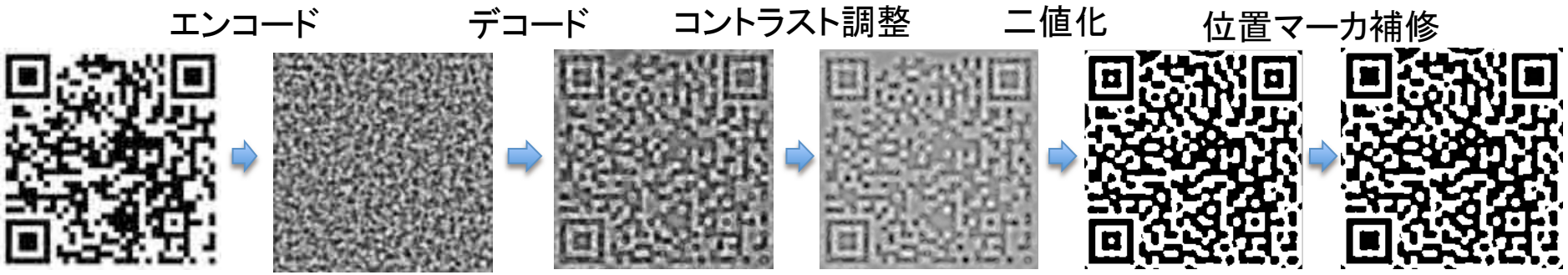
Total registers 849

Total pins6 / 142 (4 %)

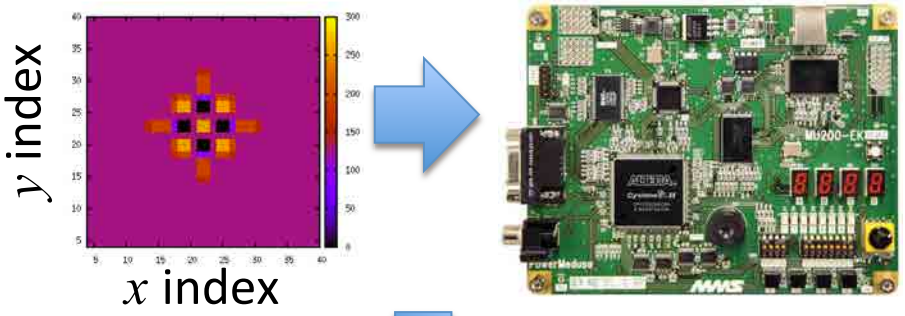
Total memory bits 90,112 / 119,808 (75 %)

まとめ

- RDCAモデルによる反応拡散ステガノグラフィシミュレーション



- 反応拡散ステガノグラフィに必要な縞模様生成をFPGA上で確認



解像度100x100以上の画像処理

低コスト or 高速動作 (800MHz～)	安価なFPGA (cyclon1: 千円/chip)	+	外部メモリチップ (数百円～)	処理時間 (100x100) 約1s 10ms以下
	高クロック周波数&大容量メモリ搭載FPGA (cyclone5 E 数千円/chip)			