IEICE Proceeding Series

Image Steganography based on Hardware-oriented Reaction-diffusion Models

Kazuyoshi Ishimura, Alexandre Schmid, Tetsuya Asai, Masato Motomura

Vol. 2 pp. 138-141
Publication Date: 2014/03/18
Online ISSN: 2188-5079

2013 International Symposium on Nonlinear Theory and its Applications
NOLTA2013, Santa Fe, USA, September 8-11, 2013

Image Steganography based on Hardware-oriented Reaction-diffusion Models

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, Hokkaido, Japan
‡Microelectronic Systems Laboratory, Swiss Federal Institute of Technology (EPFL)
Lausanne, CH-1015 Switzerland
Email: 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.

1. Introduction

Alan Turing proposed the concept of "diffusion-driven instability" for phenomena in systems where diffusion enhances the transition from a homogeneous state to a spatially inhomogeneous stable state. Time development in systems is described by the sum of reaction and diffusion in these systems [4, 5]. Reaction represents the local production or execution of the state, and diffusion represents a transport process that tends to dampen any inhomogeneity in the neighboring region. Self-organized stripe or spot patterns are observed in nature, e.g., the surfaces of animals, fish, etc. In particular, the Turing model can generate stable stripe or spot patterns by controlling the parameter set. In this study, we exhibit a possible application of such RD systems to steganography.

Steganography is one of the latest data-hiding methods. Cryptography (or alternate data-hiding technique) is a method that is used to cipher data for data communication or storage. The cryptographic algorithm is designed to protect data from malicious users. On the other hand, steganography hides data within other data, such that only the sender and receiver know the existence of the hidden data. Hence, steganography conceals hidden data as well as the sender and receiver. This is an advantage of steganography in comparison to cryptography, which only protects messages. In steganographic communication, the sender conceals a message within an image and sends the ciphered message to the receiver. During that time, an intruder who has picked up the image can view the image but not read the message and is not even aware of the existence of the message. Only the receiver can extract the hidden message using a key. It is possible that a computational analysis using a statistical distribution can extract the hidden message, but human eyes cannot detect the hidden message.

When we apply the RD system to steganography, a random initial pattern image and a RD parameter set are used as keys [1, 2]. The sender hides a message within the random pattern and generates a stripe pattern with RD. The receiver extracts the hidden message from the difference in the stripe patterns obtained from an initial pattern (key) and the received image that includes the message. Though some malicious users can sniff the hidden message, they cannot create a key stripe pattern from a random initial state and cannot extract the hidden message.

2. Reaction-diffusion Cellular Automata Model

In this study, we used a RD CA model presented in [3]. In this model, each state of a cell is determined by the sigmoid function and the weighted-sum computation that interacts with four adjacent cells. The weighted-sum computation means that activators and inhibitors diffuse in individual diffusion fields, and they are convoluted in each of the cells. Each state in the cells is computed as the difference between the states of activators, u, and inhibitors, v, at each point of the cells, (x, y). The diffusion equations for u and v are integrated for a time δt. Then, a cell's subsequent state is determined by the value of the sigmoid function for $u - v$. The dynamics are described as

$$
\begin{aligned}
&1(\text{Diffusion}) \\
&\partial u(\mathbf{r}, t)/\partial t &&= D_u \nabla^2 u(\mathbf{r}, t), \\
&\partial v(\mathbf{r}, t)/\partial t &&= D_v \nabla^2 v(\mathbf{r}, t), \\
&2(\text{Reaction}) \\
&u(\mathbf{r}, \delta t(n+1)) &&= v(\mathbf{r}, \delta t(n+1)) \\
& &&= f(u(\mathbf{r}, \delta t \cdot n) - v(\mathbf{r}, \delta t \cdot n) - c),
\end{aligned}
$$

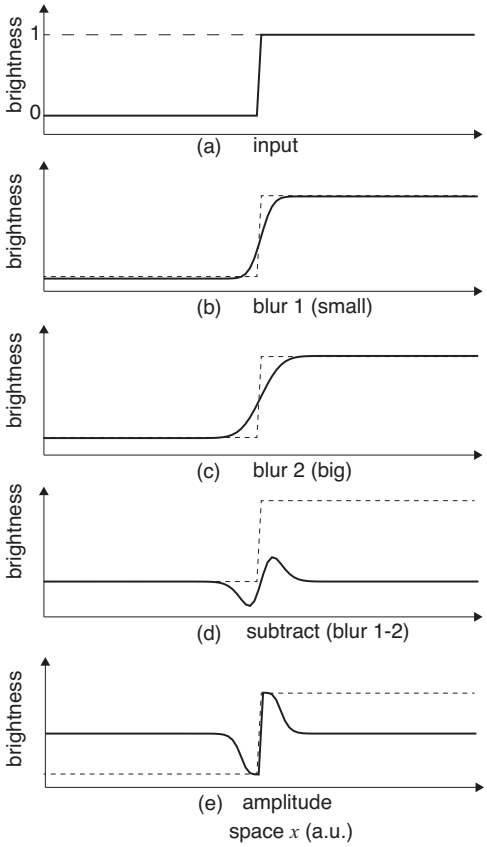

Figure 1: The process of generating stripe patterns in a one-dimensional RD model: (a) initial conditions (step function), (b) after diffusion for Δt_0, (c) after diffusion for Δt_1 - Δt_0, (d) subtraction of the activator from the inhibitor, and (e) the subtraction in (d) amplified by the sigmoid function.

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

where n represents the time step, $\mathbf{r}$ represents (x, y), c is the offset value of the sigmoid function, and β is the measure of steepness of the function. This sequential operation is defined as "one cycle". Figure 1 shows the process of forming a spatiotemporal stripe in one-dimensional RD. This process requires a diffusion field and is equivalent to the abovementioned dynamics. Figure 1 (a) shows an initial condition with a step function. After diffusion for Δt_0, the step function has a slope that corresponds to the diffusion using a factor D_v for Δt_0 in Fig.1 (b). After diffusion for Δt_1 - Δt_0, the step function has a slope that corresponds to the diffusion with D_u for Δt_0 in Fig.1 (c). Figure 1 (d) shows the difference of Figs.1 (b) and (c), that corresponds to the difference of activators and inhibitors. Finally, this difference is amplified by a sigmoid function in (Fig.1 (e)). A wave pattern is formed by repeating this process. In the same manner, Fig.2 shows an example of stripe pattern formation for a two-dimensional model. After approximately eight cycles, a stable stripe pattern is formed.

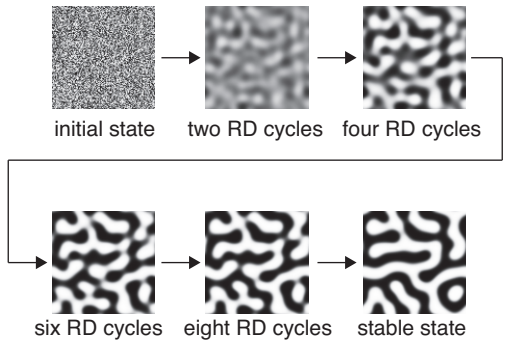

Figure 2: Snapshots of striped patterns for a two-dimensional model with a random initial distribution.

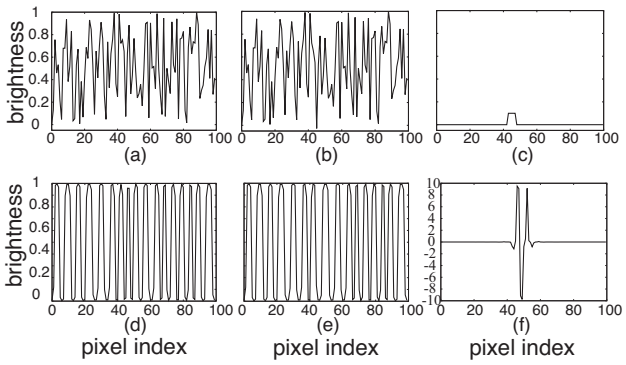

Figure 3: One-dimensional model of RD steganography. The vertical axis shows the normalized state of the pixels, i.e., prior to starting and after completion of the RD process. (a) Initial pattern with random initial conditions. (b) Initial pattern that has been perturbed in rows 43 through 47 in an 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).

3. One-dimensional RD Steganography

In this section, we apply RD (the abovementioned waveform process) to steganography and show the principle of RD-steganography for a one-dimensional case consisting in an array of 100 pixels with 8-bit values in Fig.3. First, the cyclic boundary conditions are set that enable the generation of a pattern with constant spatial frequency. Then, the initial pixel values are defined from a white noise number generator. Next, we include a subtractive perturbation as a steganographic hidden message to the initial random value. The perturbation causes the pixels in rows 43 through 47 to decrease by approximately 10% of their initial intensity value. The initial condition is presented in Fig.3 (a), and the perturbed initial condition is presented in Fig.3 (b). Figure 3 (c) shows the difference between the initial and

perturbed condition as the hidden message. After repeating six RD cycles, the stable wave states presented in Figs.3 (d) and (e) look similar. Therefore, the message is hidden in a wave pattern using RD. When the pixel values of the unperturbed state are subtracted from the perturbed state, we can extract the hidden message shown in Fig.3 (f). Its general shape results from the difference of Gaussians that represent the impulse response related to the step-like nature of the applied perturbation. The first zero-crossing around the central peak corresponds to the edges of the initial hidden pattern.

4. Two-dimensional RD Steganography

In this section, we extend RD-based steganography to two-dimensional images for steganography applications. Here, we conceal a character and an image as a perturbation into an initial random pattern that become indistinguishable using visual or analytical methods after a sufficient number of RD cycles.

In Fig.4, the basic shape representing a "T" is encrypted as a perturbation of the random initial state consisting of groups of 4×4 pixels that indicate the contour of the "T" under a solid block. Square dots are used to define the perturbation areas in a 100×100 pixel image, indicating the contours of the "T". The size and perturbation parameters are the same as defined earlier. The dot pitch is equal to 8 pixels, and no boundary conditions are set. Figure 4 (a) shows the visible dotted "T" perturbing the initial state. After six RD cycles, Fig.4 (b) shows the striped pattern with the perturbation, in which we cannot find the hidden character "T". Figure 4 (c) shows the initial random pattern without perturbation. After six RD cycles, a striped pattern is formed, as seen in Fig.4 (d). The striped patterns obtained in Figs.4 (b) and (d) are visually very similar, while not strictly identical striped patterns. Existing discrepancies enable extracting the hidden message in RD-based steganography for still images. The difference of the intensity values observed between Figs.4 (b) and (d) is shown in Fig.4 (e). The dotted "T" that was initially hidden as a perturbation of an initial random pattern is clearly observed; however, the boundaries have diffused into the surrounding regions. Further, the two-dimensional difference of Gaussians is also observed, similar to the one-dimensional case. Thus, we have demonstrated the encoding and decoding of a message using RD-based steganography.

The possibility of hiding natural images using RD-based steganography is demonstrated in Fig.5. The nature of the hidden pattern also influences the visual results of the RD-based steganographic ciphering-deciphering process. The initial random pattern intensity value of each pixel is perturbed by decreasing its value by approximately 20% of the corresponding full-range intensity of a pixel in the natural image. The fundamentals of RD systems dictate that recovering the natural image in its full dynamic range is not possible. Edges are detectable as the unique remaining feature.

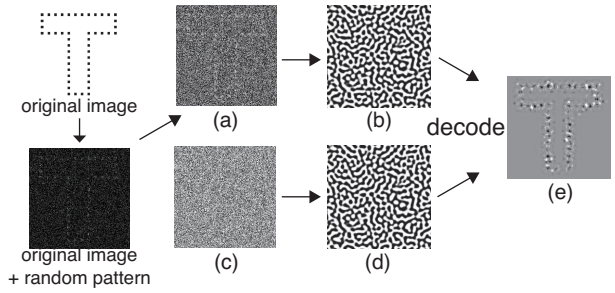

Figure 4: Two-dimensional pattern evolution with striped formation parameters. The shape of a "T" is hidden, which is formed by a solid-block perturbation. (a) Initial perturbed state. (b) Pattern state after six RD cycles. (c) Initial random image state. (d) Pattern state after six RD cycles. (e) Image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

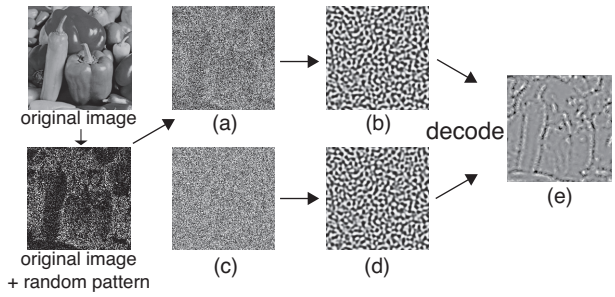

Figure 5: Two-dimensional pattern evolution with striped formation parameters. A natural image (peppers) is hidden, which is formed by a solid-block perturbation. (a) Initial perturbed state. (b) Pattern state after six RD cycles. (c) Initial random image state. (d) Pattern state after six RD cycles.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

The parameter set for the RD process is identical to the parameter set used earlier with $C = 0$, while image sizes of 512×512 pixels are used. The visible natural image perturbing the initial random state is shown in Fig.5 (a). After six RD cycles, a striped pattern is formed from the perturbed initial random image, and the original image cannot be seen, as in Fig.5 (b). Figure 5 (c) shows the initial random state without perturbation. After six RD cycles, a striped pattern has formed in Fig.5 (d). The difference of the intensity values observed in Figs.5 (b) and (d) is shown in Fig.5 (e), as in the case where a character was hidden. Figure 5 (e) shows the natural image reconstruction enabling the detection and visualization of the edges from the original image by subtraction. In this method, the detection of edges in an image is possible, but recovering an image in its full dynamic range is not possible.

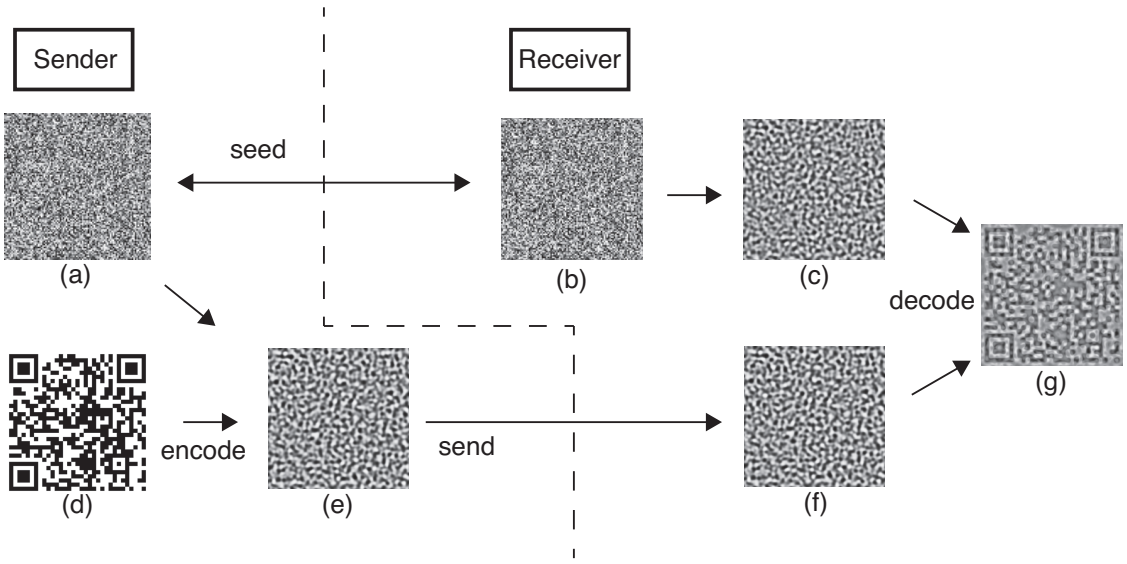

Figure 6: A method for a secure communication using RD-based steganography.

In Fig.6, we demonstrate how to realize secure communication using RD-based steganography. A sender attempts to send a secret message in the form of an image to a receiver. The sender and receiver possess an identical key that consists of the initial random image in Figs.6 (a) and (b), as well as the RD parameters, image size, β, C, D_u, and D_v in RD cycles. The sender encodes the message as a perturbation applied to the initial random pattern and allows the image to evolve through the RD system. Figure 6 (e) is a result of the cryptographic process, which is the message that is sent through the communication link. Upon receiving the message, the receiver applies the RD process to the image part of the key, obtaining Fig.6 (c). The final step consists of subtracting the message from the RD-evolved image part of the key to extract the encoded message in Fig.6 (g). Intercepting the transmitted message in Fig.6 (e) is of no use without the full key (the initial random image state and the RD parameters) under the condition that the image remains visually hidden, i.e., the striped pattern is not prominently interrupted by channels of homogeneous intensity value that follow the contours of the hidden image. This latter condition is visually verified prior to sending the message, and the RD parameters and the intensity of the perturbation are adapted to fulfill the secrecy criterion.

5. Conclusion

We demonstrated that the RD CA model is an effective model for RD-based steganography. Using this model, we hid and extracted messages (a character and an image for perturbating the initial state) by finding the difference between the initial random image state including messages and the RD-evolved image part of the key. This RD-model has simple dynamics and reaches an equilibrium stripe state quickly; thus, the computational costs are low. Therefore, we exhibited that the model is suitable for hardware application and are working on a hardware implementation of RD-based steganography using this model. We expect the realization of fast encoding and decoding of messages using RD-based steganography. Furthermore, we will be able to treat larger-sized images using the application hardware.

References

[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.