NOLTA, IEICE

Paper

Image steganography based on reaction diffusion models toward hardware implementation

Kazuyoshi Ishimura [1 a)], *Katsuro Komuro* [1], *Alexandre Schmid* [2], *Tetsuya Asai* [1], *and Masato Motomura* [1]

[1] *Graduate School of Information Science and Technology, Hokkaido University, Kita 14, Nishi 9, Kita-ku, Sapporo, Hokkaido, Japan*

[2] *Microelectronic Systems Laboratory, École Polytechnique Fédérale de Lausanne CH-1015, Lausanne, Switzerland*

[a)] *ishimura@lalsie.ist.hokudai.ac.jp*

Received January 24, 2014; Revised May 20, 2014; Published October 1, 2014

Abstract: We demonstrate a possible application of "steganography" in a reaction-diffusion (RD) cellular automata (CA) model toward digital hardware (HW) implementation. Steganography is one of data-hiding techniques which conceal hidden data transmitted between the sender and receiver. Recently, a new steganography algorithm based on self-organizing patterns which are generated by a prey-predator model was proposed. However, this model has rich nonlinearity which complicates the HW implementation. Therefore, in this paper, we demonstrate numerical simulations of the RD steganography using the RD CA model which has simple dynamics and generates striped or spotted patterns. Obtained results indicate that the RD CA model is suitable for HW implementation of RD steganography.

Key Words: steganography, reaction-diffusion, digital signal processing, Turing pattern

1. Introduction

Alan Turing proposed the concept of "diffusion-driven instability" for phenomena in systems where diffusion develops a transition from a homogeneous state to a spatially inhomogeneous stable state [1]. The time development of the system state is described by the sum of reaction and diffusion. 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. RD forms Self-organized striped or spotted patterns which are observed in nature, e.g., the skin of animals, fish, etc [2–7]. In particular, the Turing model exhibits striped or spotted patterns at the equilibrium state by controlling the parameter set [8–13].

Recently, a steganography algorithm based on self-organizing patterns which are generated by a prey-predator (PP) model was proposed [14]. In steganography, which is one data-hiding techniques, a sender hides a plain text within an image and, subsequently sends it to a receiver [15–18], who in turn,

Nonlinear Theory and Its Applications, IEICE, vol. 5, no. 4, pp. 456–465 DOI: 10.1588/nolta.5.456

extracts the hidden message from the image. During the transmission process, a malicious user who has picked up the image embedded into the secret message is not aware of the existence of the message. Steganography is one of data-hiding techniques which conceal hidden data transmitted between the sender and receiver. This property differentiates steganography from typical cryptography which only protects messages i.e., without masking its existence.

In RD steganography, a random initial image pattern and a RD parameter set are used as private keys. A sender hides a message within the random pattern. Subsequently, the pattern is transformed into a stable striped or spotted pattern by RD. Embedding a secret message into an image by RD is different from classical steganography. The receiver extracts the hidden message by subtracting the received image from the striped pattern obtained from the initial pattern by RD using on identical parameter set as used in the encoding process. Though some malicious users can analyze the image, they cannot reconstruct a key striped or spotted pattern from a random initial state and cannot extract the hidden message.

Typical steganography which embeds some data into LSB of a cover data is implemented in FPGA HW [19, 20]. Although these dedicated HW for steganography improves processing speed as compared to software, this typical steganography has low tolerability to statistical analysis.

Our purpose is to suggest a model which is suitable for implementation of RD steganography hardware to protect messages from statistical analysis. The RD CA model has been implemented in analog CMOS circuits to repair finger prints [21]. Therefore, to simulate RD steganography, we employed the RD CA model. From these results, we consider the possibility of implementation of RD steganography HW.

This paper is organized as follows. Section 2 describes a RD CA model. Section 3 explains RD steganography based on the proposed model simulated from C implementation. An example of 2-D RD steganography communication is presented in Sect. 4. Section 5 is devoted to discussion related to security of the RD steganography.

2. A reaction-diffusion cellular automata model

The PP model which has rich nonlinearity is described using partial differential equations. Computational costs on the PP model become high by continuous values. Therefore, HW implementation of the PP model is difficult. On the other hand, the RD CA model is described as the weighted summation of adjacent cells. Therefore, computational cost is lower than the PP model. From these points, we can consider that the RD CA model has advantage over the PP model to implement of HW. 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, for each cell (x, y) in the field. The diffusion dynamics is described as

$$\frac{\partial u(x,y,t)}{\partial t} = D_u \nabla^2 u(x,y,t), \tag{1}$$

$$\frac{\partial v(x,y,t)}{\partial t} = D_v \nabla^2 v(x,y,t), \tag{2}$$

where D_u represents the diffusion coefficient of the activators and D_v represents the diffusion coefficient of the inhibitors. D_v and D_u are selected to satisfy that D_v is larger than D_u. The diffusion equations for u and v are integrated for a time δt. Subsequently, they are subtracted from each other. Finally, the subtracted waveform is amplified by the sigmoid function, which is defined as an "update". The update process is described as

$$\begin{aligned} u(x,y,\delta t(n+1)) &= v(x,y,\delta t(n+1)) \\ &= f(u(x,y,\delta t \cdot n) - v(x,y,\delta t \cdot n) - c), \end{aligned} \tag{3}$$

$$f(w) = \frac{1}{1+e^{-\beta w}}, \tag{4}$$

where n represents the time step, β represents the measure of steepness of the function, and c represents an offset value.

Figure 1 shows the process of forming a spatiotemporal stripe in one-dimensional RD, in a diffusion field using $D_v/D_u = 3.0$, $\beta = 20$ and $c = 0$. Figure 1(a) shows an initial condition as an impulse. Subsequently, the initial impulse is blurred for δt with different diffusion coefficients D_v and D_u in individual diffusion fields in Figs. 1(b) and (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 the sigmoid function in Fig. 1(e). In the same manner, Fig. 2(a) shows an example of striped pattern formation for a two-dimensional model ($D_v/D_u = 3.0$, $\beta = 20$ and $c = 0$). A stable striped pattern is formed after approximately eight updates. Figure 2(b) shows an example of spotted pattern

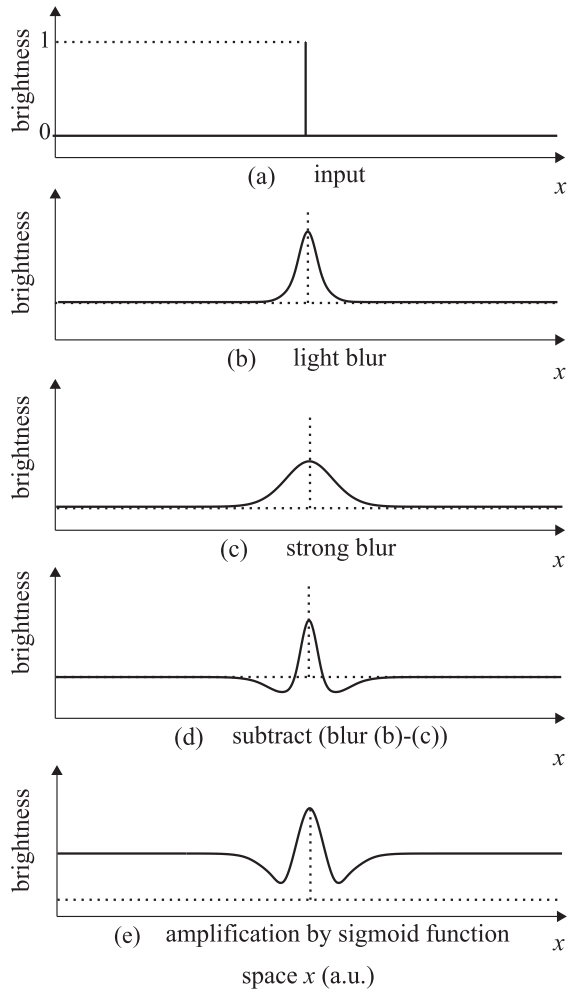

Fig. 1. The process of generating a wave in a one-dimensional RD model: (a) initial conditions (impulse), (b) after diffusion with D_u, (c) after diffusion with D_v, (d) subtraction of the activator from the inhibitor, and (e) the subtraction in (d) amplified by the sigmoid function.

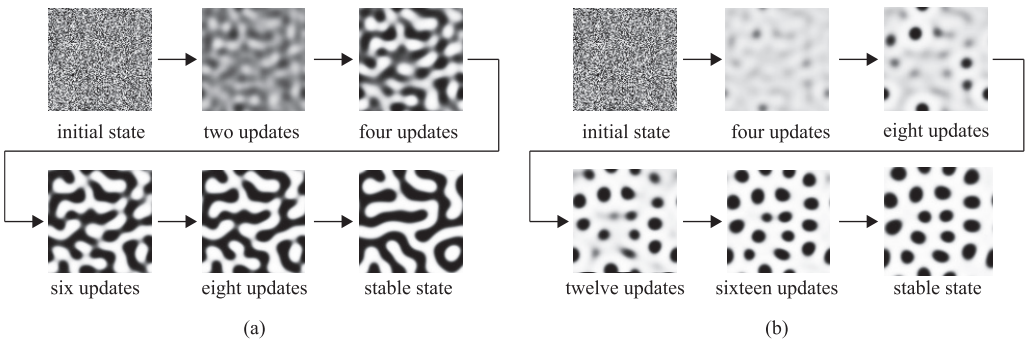

Fig. 2. Snapshots for a two-dimensional RD model with a random initial distribution (a) striped patterns (b) spotted patterns.

formation for a two-dimensional model ($D_v/D_u = 3.0$, $\beta = 20$ and $c = -0.08$). A spotted pattern is formed from an initial random pattern when the offset value is changed from $c = 0$ into $c = -0.08$.

3. RD Steganography based on a RD CA model

3.1 One-dimensional RD steganography

In this section, we apply the RD CA model to steganography and demonstrate RD-steganography for a one-dimensional case consisting in an array of 100 pixels with 8-bit values using the same parameter set ($D_v/D_u = 3.0$, $\beta = 20$ and $c = 0$) as presented in Fig. 3.

First, cyclic boundary conditions are set that enable the generation of patterns with constant spatial frequency. Second, the initial pixel values are defined using a white noise number generator shown in Fig. 3(a). Then, as a hidden message, the pixel values in rows 43 through 47 are set to 10% of 8-bit values as shown in Fig. 3(c). Figure 3(b) shows the secret message embedded into the initial condition as perturbations by subtracting Fig. 3(c) from Fig. 3(a).

After six updates from the initial unperturbed and the perturbed states, the stable wave states presented in Figs. 3(d) and (e) look similar. Hence, the message is hidden in a wave pattern using RD. The hidden message shown in Fig. 3(f) is extracted by subtracting the final pixels values of the perturbed and unperturbed states Figs. 3(d) - (e). 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 located close to the central peak corresponds to the edges of the initial hidden pattern.

3.2 Two-dimensional RD steganography

In this section, RD-based steganography is extended to support to two-dimensional images for steganography applications. A character and an image are concealed as perturbations into an initial random pattern that become visually indistinguishable after a sufficient number of updates.

In Fig. 4, the basic shape representing a character "T" is embedded as perturbations of the random initial state representing a decrease of 10% of the initial pixel intensity values. The dotted "T" which consists of groups of 4×4 pixels repeated with a pitch of 8 pixels is used to define perturbation areas in a 100×100 pixel image. Figure 4(a) indicates the visible dotted "T" perturbing the initial state followed RD parameter set: $D_v/D_u = 3.0$, $\beta = 20$ and $c = 0$. After six updates, Fig. 4(b) shows the striped pattern with the perturbations, in which the hidden character "T" is invisible. Figure 4(c) shows the initial random pattern without perturbations. After six updates, a striped pattern is formed, as seen in Fig. 4(d). The striped patterns obtained in Figs. 4(b) and (d) are visually very

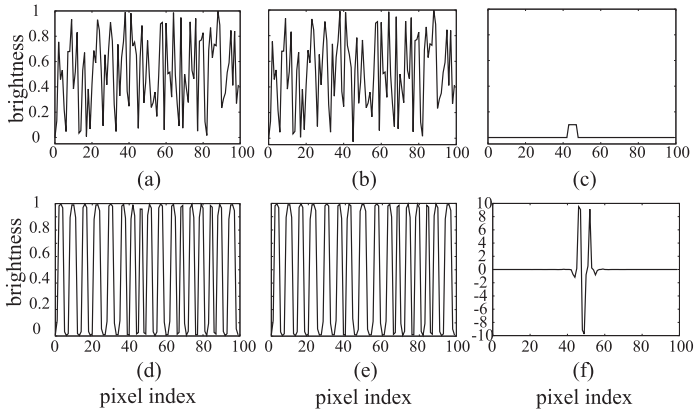

Fig. 3. One-dimensional model of RD steganography. The vertical axis shows the normalized state of the intensity values, i.e., prior to starting and after completion of the RD process. (a) Initial pattern with random initial conditions. (b) Initial pattern that has been perturbed in rows 43 through 47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

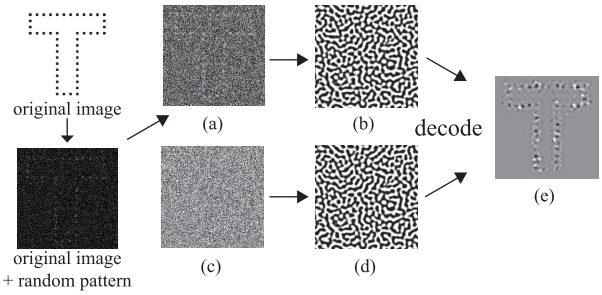

Fig. 4. Two-dimensional pattern evolution with striped formation parameters. The shape of a "T" is hidden, which is formed by a solid-block perturbation. (a) Initial perturbed state. (b) Pattern state after six updates. (c) Initial random image state. (d) Pattern state after six updates. (e) Image resulting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

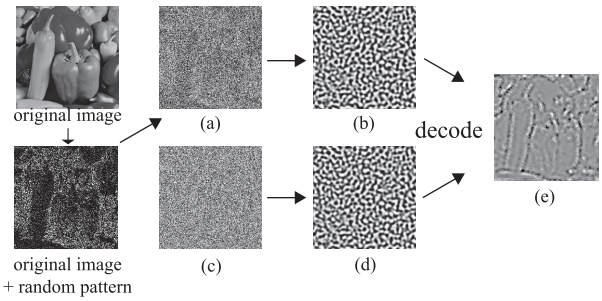

Fig. 5. Two-dimensional pattern evolution with striped formation parameters. A natural image (peppers) is hidden, which is formed by a solid-block perturbation. (a) Initial perturbed state. (b) Pattern state after six updates. (c) Initial random image state. (d) Pattern state after six updates. (e) Image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

similar, but not strictly identical striped patterns. The existence of a difference enable extracting the hidden message. The difference of the intensity value observed between Figs. 4(b) and (d) is shown in Fig. 4(e). The dotted "T" that was initially hidden as perturbations in the initial random pattern is clearly observed; however, the boundaries have diffused into the surrounding regions. Thus, the possibility to apply RD-based steganography for still images is shown to be successful in the encoding and decoding of a text message.

The possibility of hiding natural images using RD-based steganography for $D_v/D_u = 3.0$, $\beta = 20$ and $c = 0$ is demonstrated in Fig. 5. The method of hiding patterns 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 20% of the corresponding full-range intensity of a pixel in the natural image.

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 updates, a striped pattern is formed from the perturbed initial random image, and the original image is no longer visible, as shown in Fig. 5(b). Figure 5(c) shows the initial random state without perturbations. After six RD updates, 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). Figure 5(e) shows the natural image reconstruction enabling the detection and visualization of the edges from the original image by subtraction. Though, in this method, the detection of edges in an image is possible, recovering an image in its full dynamic range is not possible.

In Fig. 7, we demonstrate how to realize a secure communication using the RD-based steganography principles that have been previously demonstrated. A sender and receiver possess an identical key that consists of the initial random image in Figs. 7(a) and (b), as well as the RD parameters ($D_v/D_u = 3.0$, $\beta = 20$ and $c = 0$), the image size in number of RD updates. The sender encodes the message as perturbations applied to the initial random pattern and allows the image to form striped patterns using

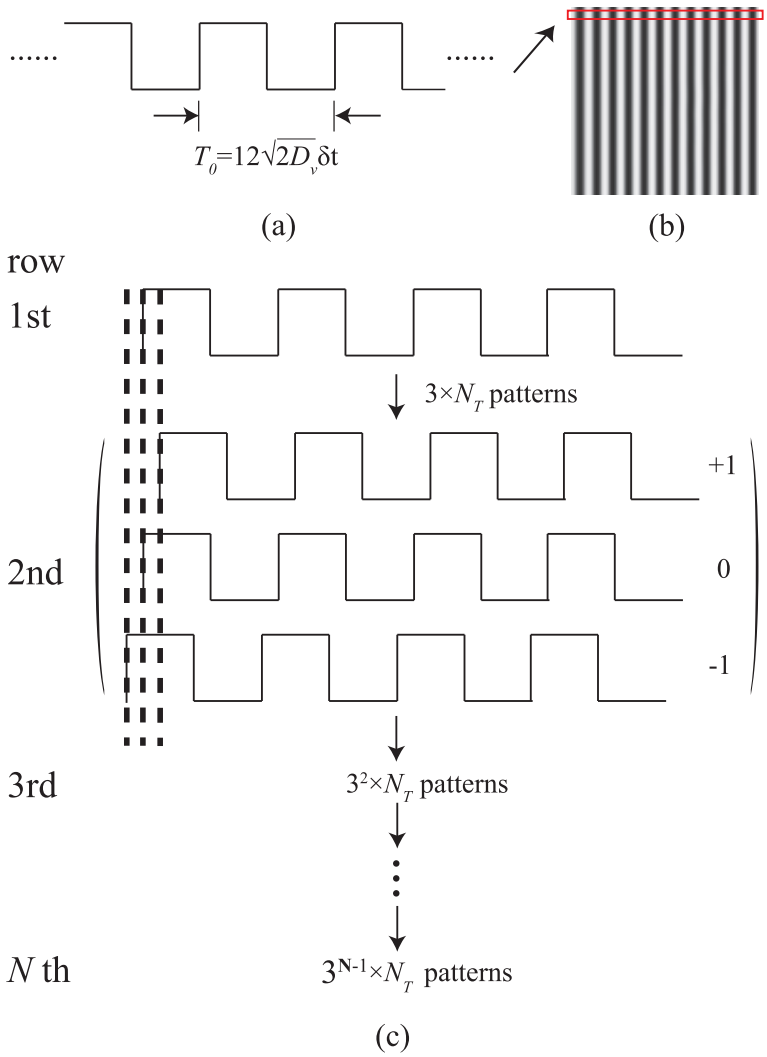

Fig. 6. Calculation of The number of striped patterns with constraint conditions.

the RD system. Figure 7(e) is the result of the RD process, 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. 7(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. 7(g).

We showed processes of RD steganography. Here, we explain a method of counting striped patterns. At first, we analyze wave patterns, which are the number of diverse stable patterns, in 1D space. To find wave length permits calculating the number of wave patterns in 1D space as shown in Fig. 6(a). In that time, we assume that cyclic boundary conditions are set. Then, spatiotemporal period (T_0) is described as

$$T_0 \quad = \quad 12\sqrt{2D_v\delta t} \tag{5}$$

(Eq. (14) in [21]). When we assume that the 1D space consists of array of N pixels, the number of wave patterns (N_T) , which are generated by sliding some pixels within one cycle, can be approximated as $N_T \equiv N \times T_0$ patterns. Then, we expand the calculation method to 2D wave patterns as shown in Fig. 6(b). We assume that cyclic boundary conditions are set in rows, but the top and bottom of rows are disconnected. As noted previously, the top of rows of the striped patterns are $N \times T_0$. And then, we assume that a wave in a row can slide one pixel to the right or to the left, or zero pixel from a wave in an above row. Figure 6(b) shows any rows does not slide. In this assumption, uninterrupted wave patterns are generated. As shown in Fig. 6(c) a wave pattern in the second row is formed in one of three patterns which slide by +1, 0, or -1 pixel from the wave pattern in the first row. In that time,

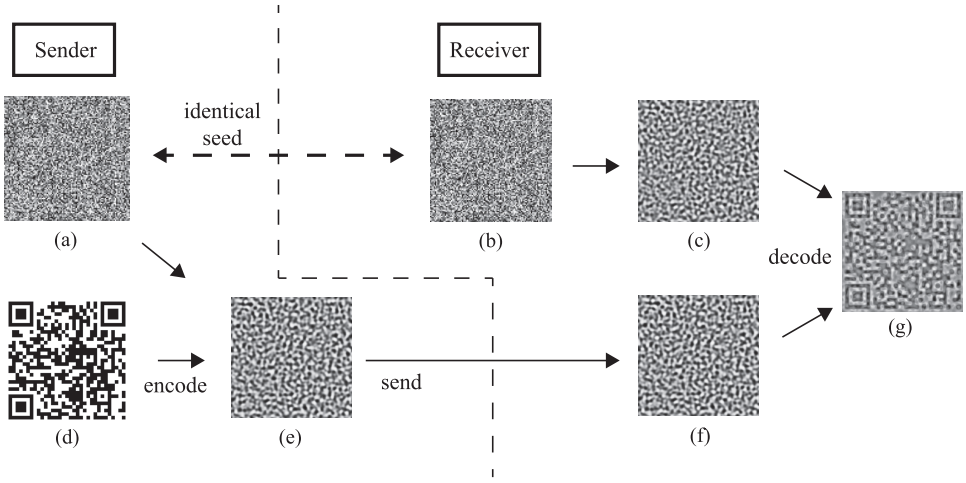

Fig. 7. The concept of the RD steganography technique.

the total wave patterns in the two rows are $3 \times N_T$. A wave pattern in the third row is formed one of three wave patterns which are generated from each of the three wave patterns in the second row. At this point, the total wave patterns in the three rows are $3^2 \times N_T$ patterns. Finally, by repeating this method, $3^{n-1} \times N_T$ wave patterns are generated. Moreover, when we change RD parameters or image size, and clear constraints, the number of generated patterns induces combinatorial explosion. These results indicate that the RD CA model can generate a significant number of striped patterns which can be used as private keys.

RD steganography protects messages doubly for secure communication. First, RD steganography embeds messages into a random dot pattern as classical steganography. Second, nonlinearity which has sensitivity and diversity of behavior protect messages from statistical analysis. In the RD CA model, D_v/D_u can be predicted by formed striped patterns, δt changes striped patterns slightly, and c changes forming patterns when the value is major changed (Fig. 5 in [21]). However, these RD parameters changes striped patterns slightly with similar plural conditions, β which is a parameter in a nonlinear term, changes spatiotemporal frequency. In 1D space, the half of stable wave length is described as

$$x_0 \quad = \quad p_v \sqrt{\frac{F(2/k^2)}{2}} - a, \tag{6}$$

where x_0 represents the half of stable wave length, p_v represents square root of D_v, and $F(\cdot)$ represents the inverse of Lambert's W function where $k \equiv 4\sqrt{\pi}/\beta$ (Eq. (14) in [21]) Therefore, changing parameter β which forms a wide variety of patterns provides safety private keys for RD steganography from similar plural conditions.

From these results, intercepting the transmitted message in Fig. 7(e) is of no use without the full key 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 perturbations are adapted to fulfill the secrecy criterion.

3.3 An example of communication using RD steganography

We demonstrated the principle of RD steganography based on the RD CA model. It was found that edges of an embedded figure are preserved. Furthermore, it was shown that an embedded secret message should optimally cover the entire image area, i.e., should preferably not be localized inside a limited area of the image.

From this latter point, QR codes appear to fulfill the criterion, which have distributed white and black areas. Additionally, a QR code can carry a significant amount of information and has the ability to sustain 10–30% of QR code errors. Nonetheless, striped RD images are suspicious in communications when the images are transmitted on communication channels. Therefore, a method

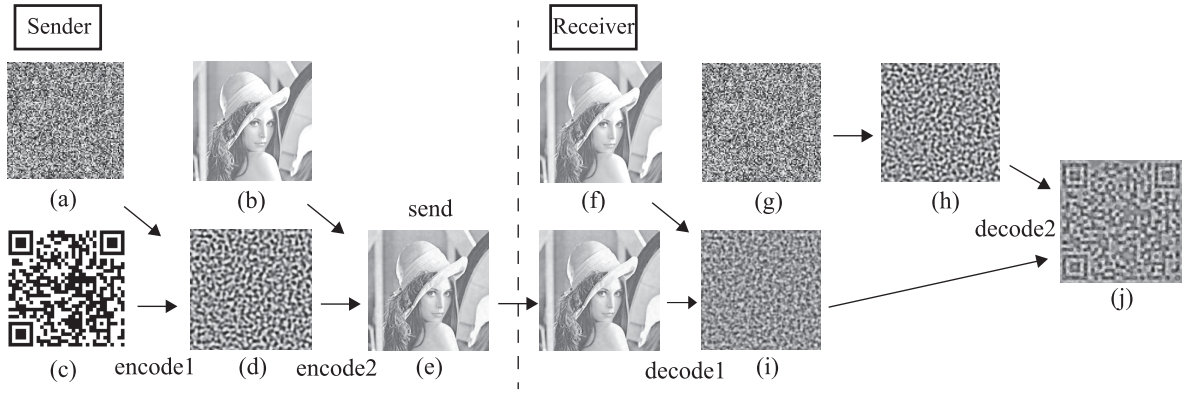

Fig. 8. Method for a secure communication using RD-based steganography.

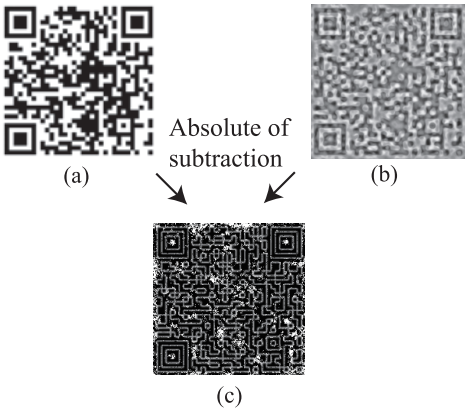

Fig. 9. Comparison of the original QR code and the extracted one by absolute of subtraction.

of RD steganography communication supporting QR codes has been developed as shown in Fig. 8. A sender and receiver share an initial random pattern shown in Figs. 8(a) and (g), a cover image in Figs. 8(b) and (f), and RD parameters ($D_v/D_u = 3.0$, $\beta = 20$ and $c = 0$) as secret keys. At first, the sender embeds a QR code in Fig. 8(c) into the initial random pattern by subtracting 10% of their pixel's intensity value. After transforming the random pattern with the QR code using the RD process shown in Fig. 8(d), the sender embeds it into a natural image in the same way as the QR code is embedded, as shown in Fig. 8(e). This latter data is sent over the communication channel. A malicious user may intercept the data and observe the image, but he can not be aware of the presence of the QR code. To decode the secret message, the receiver extracts the striped pattern as shown in Fig. 8(i) by subtracting the received image from the cover image in Fig. 8(f). Then, the QR code as shown in Fig. 8(j) is decoded by subtracting the extracted striped pattern in Fig. 8(i) from the key striped pattern in Fig. 8(h).

The decoded QR code in Fig. 8(j) needs post-processing to guarantee its machine readability. Differences between the original QR code in Fig. 9(a) and the extracted one in Fig. 9(b) are shown in Fig. 9(c). White lines indicate boundary errors which are negligible. However, three white areas which are located inside position markers require repairs. We therefore show post-processing steps to read the extracted QR code as shown in Fig. 10. Figure 10(a) shows the QR code extracted in Fig. 8(j). First, the image contrast is adjusted (Fig. 10(a)) as shown in Fig. 10(b). Then, Fig. 10(c) is obtained by binarizing Fig. 10(b). Filling in the inside of position markers which have incorrect white areas enable automated machine detection of the extracted QR code as shown in Fig. 10(d). In this case, the latter process has been carried out manually, though it can be automatized from pattern detection methods.

Furthermore, we automated all RD steganography processes: generating QR codes, encoding and decoding QR codes on RD steganography, post-processing for decoded QR codes, and reading adjusted QR codes. Then, we repeated 10,000 times for these processes. From the results, 99 % of readable QR

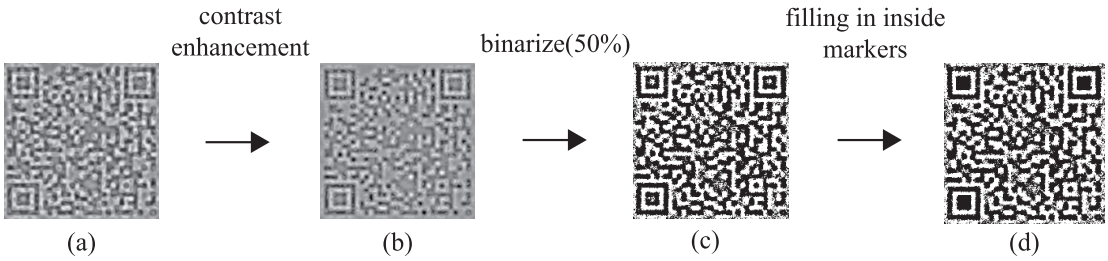

Fig. 10. Post-processing method to read the extracted QR code.

codes can be extracted. Therefore, the proposed model has robustness utilizing RD steganography.

4. Summary and discussion

This paper shows a novel data-masking technology using RD steganography which is based on the RD CA model that is selected on its propensity to HW implementation. The demonstration has been made consisting of merging a message into a two-dimensional random pattern, evolving the obtained image into a striped pattern using RD and subsequently hiding the result by merging it into a natural image for data transmission over an expectedly insecure transmission channel. At the receiver, the secret message is extracted out of the transmitted image by subtraction of a striped pattern obtained from a private key.

A general discussion pertaining to the security of RD steganography can be consulted in [22]. Following the success of steganography, spacial-domain statistical methods have been developed to enable automated machine detection of hidden messages. When RD steganography becomes a common method, many striped pattern will pass over communication channels. Malicious users may become aware of existence of a hidden message inside striped patterns. However, they can not extract the message without the key, since RD is not reversible as a non-linear process that transforms the secret message as well as the initial random pattern. Nevertheless, and akin to all data-hiding techniques, RD steganography may be subjected to brute-force attacks which may uncover the key, from the knowledge of the method and a succession of images hiding data. This time-domain statistical attack may be counterfeited by random insertion of fake images, e.g., without data or including data hidden using alternate keys. From the aspect of security, RD steganography finds applications in fields that require a low-level of security, e.g., a time-limited URL or low-level confidential data. For example, a target group of people who have the key may access a URL coded as a QR code that is hidden into an image which is openly displayed in a public location. Applying RD steganography to QR codes has been demonstrated successful, and has the potentially of hiding relevant amounts of information, which can further be increased by applying the presented technology to video streams. The real-time usage of such technology requires dedicated processor architectures, and its effectiveness in terms of quantifiable security level must be analyzed prior to integration.

Acknowledgments

This study was supported by a Grant-in-Aid for Scientific Research on Innovative Areas [2511001503] from the Ministry of Education, Culture, Sports, Science and Technology (MEXT) of Japan.

References

[1] A.M. Turing, "The chemical basis of morphogenesis," *Phil. Trans. R. Soc. Lond B.*, vol. 237, pp. 37–72, 1952.

[2] G. Nicolis and I. Prigogine, *Self-organization in Nonequilibrium Systems — From Dissipative Structures to Order through Fluctuations,* John Wiley & Sons, Inc., New York, NY, 1977.

[3] Y. Oono and S. Puri, "Study of phase-separation dynamics by use of cell dynamical systems. I. Modeling," *Phys. Rev. A*, vol. 38, no. 1, pp. 434–453, 1988.

[4] I. Epstein and J. Pojman, *An introduction to nonlinear chemical dynamics,* Oxford University press, Oxford, 1998.

[5] A. De Wit, *Spatial patterns and spatiotemporal dynamics in chemical systems, Adv. Chem. Phys.*, vol. 109, pp. 435–513, 1999.
[6] P. Ball, *The Self-Made Tapestry: Pattern Formation in Nature,* Oxford University press, Oxford, 2001.
[7] J.D. Murray, *Mathematical Biology II (3rd Ed.),* Chap. 2, p. 75, Springer, New York, 2002.
[8] D.A. Young, "A local activator-inhibitor model of vertebrate skin patterns," *Math. Biosci.*, vol. 72, pp. 51–58, 1984.
[9] M. Markus and B. Hess, "Isotropic cellular automaton for modeling excitable media," *Nature.*, vol. 347, no. 6288, pp. 56–58, 1984.
[10] M. Gehardt and H. Schuster, "A cellular automaton describing the formation of spatially ordered structures in chemical systems," *Physica D.*, vol. 36, pp. 209–221, 1989.
[11] H. Schepers and M. Markus, "Two types of performance of anisotropic cellular automaton: stationary (Turing) patterns and spiral waves," *Physica A.*, vol. 188, pp. 337–343, 1992.
[12] J.R. Weimar, J.J. Tyson, and L.T. Watson, "Diffusion and wave propagation in cellular automata models for excitable media," *Physica D.*, vol. 55, pp. 309–327, 1992.
[13] Y.-N. Wu, P.-J. Wang, C.-J. Hou, C.-S. Liu, and Z.-G. Zhu, "Turing patterns in a reaction-diffusion system," *Commun. Theor. Phys.*, vol. 45, no. 4, pp. 761–764, 2006.
[14] L. Saunoriene and M. Ragulskis, "A secure steganographic communication algorithm based on self-organizing patterns," *Phys. Rev. E*, vol. 84, no. 5, article no. 056213, 2011.
[15] N.F. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," *IEEE computer*, vol. 31, no. 2, pp. 26–34, 1998.
[16] R.J. Anderson and F.A.P. Petitcolas, "On the limits of steganography," *Selected Areas in Communications IEEE Journal on*, vol. 16, no. 4, pp. 474–481, 1998.
[17] J. Fridrich and R. Du, "Secure steganographic methods for palette images," *Information Hiding*, Springer Berlin Heidelberg, 2000.
[18] C.-K. Chan and L.M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognit.*, vol. 37, no. 3, pp. 469–474. 2004.
[19] S. Mahmoudpour and S. Mirzakuchaki, "Hardware architecture for a message hiding algorithm with novel randomizers," *International Journal of Computer Applications.,* vol.37, no. 8, pp. 46–53, 2012.
[20] G.J. Kumar and U.N.S. Devi, "FPGA hardware LSB steganography technique based on the lifting scheme," *International Journal of Engineering.*, vol. 2, no. 8, 2013.
[21] 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.
[22] "Focus: Hiding Secrets in Spontaneous Patterns," http://physics.aps.org/articles/v4/96.