2017 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2017, Cancun, Mexico, December 4-7, 2017

Authentication Scheme Using Pattern Dynamics Based on Coupled Chaotic Maps

Masahiro Wada

Faculty of Intelligence and Infomatics, Konan University
8–9–1 Okamoto, Higashinada-ku, Kobe 658-8501, Japan
Email: wada-m@konan-u.ac.jp

Abstract—
Pattern dynamics on coupled nonlinear systems and generated phase patterns are very interesting for the meanings of the natural phenomena. There are several authentication systems using these nonlinear dynamics. In this study, we propose a design of an authentication system using pattern dynamics based on coupled chaotic maps. There is a feature of uniqueness which the same pattern is generated when the parameters and the initial conditions are all the same. We show a framework of design for the authentication process using these features. Then, we make an application as a software realized on a computer environment. Furthermore, we also carried out statistical analysis for our proposed system and showed validity of the system.

1. Introduction

Pattern dynamics and mechanism of organization in several complex systems and natural fields attract many researchers' attention as a good model which can realize the complicated phenomena in the real world. It is important to investigate that biological patterns in the natural life such animals and plants are individual and unique to distinguish for several characteristics. Several patterns on the biological systems is also attracted for several scientists in the meanings of the natural pattern dynamics and generation mechanism using Turing model[1]. On the other hand, coupled chaotic systems and its dynamics can yield a wide variety of complex and strange phenomena. The coupled oscillatory systems existing in nature exhibit great variety of phenomena. These phenomena can be found in a metabolic network, a human society, the process of a life, self-organization of neuron, a biological system, an ecological system and so many nonlinear systems. As one of features for the chaos, it is difficult to forecast values in the future because of sensitivity of their initial conditions and complexity. Namely, there is a feature of uniqueness that the same phase pattern is only generated when the parameters and the initial conditions are all the same. The studies of coupled map lattice (CML), globally coupled maps (GCM) and so many studies related with such complex systems provided us tremendous interesting phenomena. Especially, we had reported the research on spatio-temporal phase patterns on coupled chaotic maps using several nonlinear functions[2]-[3]. As you know, there are many authentication algorithms of real usage in our computer environment to save several data with security. The previous study, we also reported a framework of an authentication system and a novel algorithm using the uniqueness of chaotic pattern dynamics[4][5]. We focused on the uniqueness of the generation pattern using this dynamics based on the coupled chaotic maps.

In this study, we propose a design of an authentication system using pattern dynamics on a network of the coupled chaotic maps. Dynamics of pattern generation for the coupled chaotic systems and its analysis are very important for the meanings of the natural phenomena. We show a framework and an authentication scheme using the pattern dynamics. Then, we design and make an application as a software realized on the computer environment. Furthermore, we also carried out statistical analysis for our proposed system and showed validity of the system.

2. Pattern Dynamics of the Coupled Chaotic Maps

There are many nonlinear chaotic maps of both continuous and discrete functions which can yield several chaotic behavior. Chaotic maps are generally used for several approaches to investigate complex dynamics and several phenomena on coupled network systems.

In this study, hereafter we use a fifth-power polynomial function with respect to the origin using only odd numbered variables written as follows.

$$f(x) = ax^5 - bx^3 + cx \tag{1}$$

where a, b and c are parameters and positive values which can determine for their chaotic feature. We can easily confirm that it generates chaos in this function when we choose appropriate parameters and condition. We use this nonlinear function as a chaotic cell in the coupled network.

An example of drawing for (1) is shown in Fig. 1 with chaotic trajectories.

Figure 2 shows a two-dimensional CML network system with one coupling strength ε. The chaotic map is regarded as a cell of one of the network component, then let us consider a network structure connected to four neighbors as shown in Fig. 2. We can obtain several phase patterns on the coupled chaotic maps in the computer simulation.

The equation of the network can be described for the two-dimensional network system as follows.

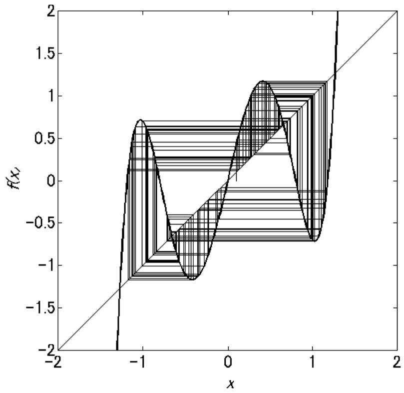

Figure 1: Chaotic map and its trajectories obtained by a = 4.9, b = 10.0, c = 4.4

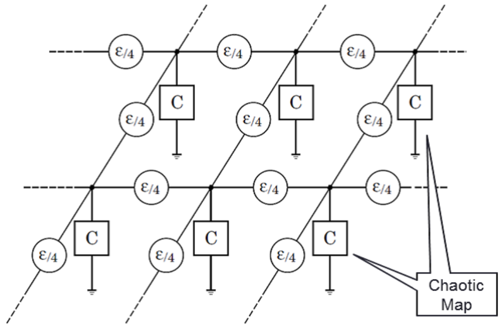

Figure 2: 2-dimensional CML network model which each chaotic cell are coupled to neighbors by coupling strength $\varepsilon/4$

$$x_{ij}(t+1) = (1-\varepsilon) f\big(x_{ij}(t)\big) + \frac{\varepsilon}{4} \sum_{kl \in \Xi} f\big(x_{kl}(t)\big) \qquad (2)$$

where t means a time, i and j are index numbers of the cells, and Ξ means four neighbor cells. The index number obeys the cyclic rule in the coupling structure. Namely, the cells of the edge and corners are attached by a cyclic rule that is connected to the opposite side of the cell elements by circulation.

Figure 3 shows several phase patterns for several parameters and network sizes. The initial value of all the cells are put by random between -1.0 and 1.0. This figure indicates a grade of synchronous state for phase difference with an average of four neighbors, which is illustrated with gray scale monotone colors between white □ and black ■ correspond to synchronous and asynchronous state, respectively. Synchronous or asynchronous state is expressed as a monochrome 256 gradations of gray-scale image by taking from the target cell, when absolute value by the difference between the target and the the average value of the four neighbor cells is calculated. A unique pattern is only obtained for the same parameters, iterations and their initial conditions. It is one of the very important features that the phase pattern generated by the condition and parameters is

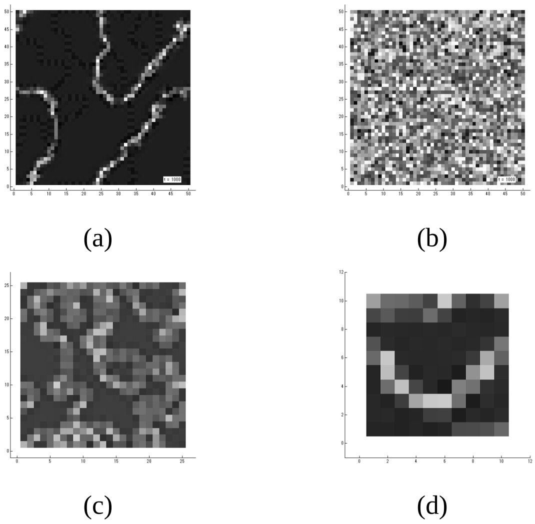

Figure 3: Phase patterns at time t = 1000 for several parameters and network sizes. (a) 50×50, a = 4.87, b = 10.0, c = 3.90, (b) 50×50, a = 6.94, b = 10.0, c = 3.55, (c) 25×25, a = 4.44, b = 10.0, c = 3.33, (d) 10×10, a = 4.90, b = 10.0, c = 3.60

uniqueness. Namely, when the initial conditions, parameters and iterations are all the same, the phase pattern and its dynamics are all the same and shown its uniqueness. This feature is a main concept and is used for an authentication algorithm in this study.

We show some computer simulation results using the proposed system [1]. Figure 4 shows the obtained cipher patterns generated for two different parameters a. These pigment patterns are as cipher images for the authentication process. We easily confirmed that different phase patterns are obtained when the parameters are slightly changed. The image of left hand side means the initial phase pattern, namely the initial phase pattern. The image of right hand side means the generated phase pattern with given parameters after 100 iterations. We calculated the phase patterns when the initial values at any points are changed for the initial conditions. It was changed plus or minus sign of the value for the original one. Figure 5 shows some examples obtained by computer simulation when some initial conditions are changed. Although it is difficult to evaluate from the images, the obtained images are completely different form the original one.

3. Design of the Authentication System using the Pattern Dynamics

We propose a design of an authentication system using these properties of pattern dynamics. Figure 6 shows a framework of the design and the authentication process. At first, we select and decide the parameters of the chaotic

[1] All simulation results were obtained by MATLAB 2012b (32bit) on Windows 7 (64bit), Intel Core i7-820QM(1.73GHz), 4GB memory.

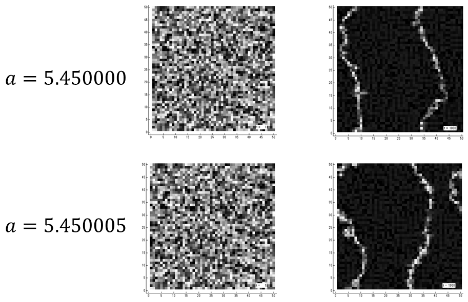

Figure 4: Generated pattern at t=100 for changing slightly the parameter a when the parameters b and c are 10.0 and 4.10

map and the coupling strength ε. We keep and store the generated phase pattern with these parameters after specific iterations as a cipher code. The cipher and authentication keys are these parameters of the chaotic map, iterations and coupling strength in this proposed system. In order to discuss simply, let the initial condition be the same matrix for computer simulation. We can change the values at any position of the initial condition matrix. The authentication process is carried out by comparing the obtained pigment image pattern with the original stored image as a cipher code mentioned before by gray-scale image or the real value of each cell. The flowchart of the process is roughly shown in Fig. 7.

In the authentication process, we can obtain phase patterns with any parameters and iterations. If the same pattern could be obtained, the authentication is success and passed. Therefore, the authentication process is done successfully when the all authentication keys are agreed with the original one. On the other hand, when the parameters and the initial conditions are slightly changed or not same, we cannot never obtain the same phase patterns, that means the authentication is failure and rejected. Therefore, even if the authentication keys are slightly different, the generated pattern is never reproduced to the original pattern. Please note that the initial conditions are the same in whole computer simulation.

If we choose a large scale of the number of the coupled systems, the difficulty of decipher may be expanded to the infinity. However, computer calculation time and costs are increasing simultaneously. Thus, we can easily construct a new scheme of the authentication system using pattern dynamics on the coupled chaotic maps.

Table 1 shows simulation results in several network sizes when the one initial condition is only changed for all cells. It can be seen that the original pattern were never reproduced in the proposed scheme using computer calculation process . Therefore, we consider that the proposed system is valid as one of applications for the authentication algorithms. As one of results in this proposed system, we consider that security is very high, however calculation speed

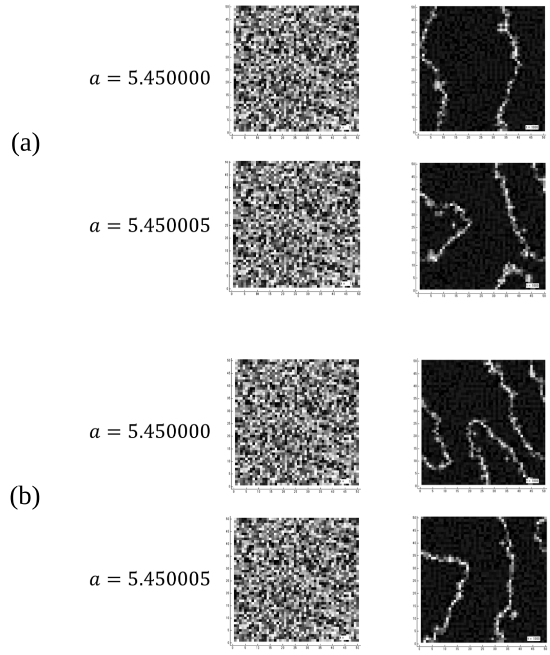

Figure 5: Obtained pattern for changing the initial condition of plus or minus sign at some points. (a) one value at (1, 1) is changed, (b) three values at (1, 1), (1, 6) and (7, 1) are changed

Table 1: Statistic simulation results of pass through the authentication by different initial conditions with changing only one value to the original

Network size	Number of trial	Pass	Cost [sec]
50×50	2500	0	5.697
25×25	625	0	4.189
10×10	100	0	1.359

is very slow as increasing the network size.

We show a software application constructed on the MATLAB environment in order to evaluate the proposed scheme. Figure 8 shows a screen shot of the design of the authentication system as an application realized on the MATLAB environment. In the authentication process, it is assumed that an encrypted image necessary for authentication is stored in advance. To generate a pattern at the time of authentication process, we first enter necessary parameters, the number of calculations, the network size and so on, then we push the button to execute the authentication procedure. After the authentication process, the calculated and obtained image is compared with the stored original image. As a result, if the image is the same, the authentication process is passed successfully. However if it is not the same, the authentication process is failed. Thus, we could show some degree of validity for the proposed sys-

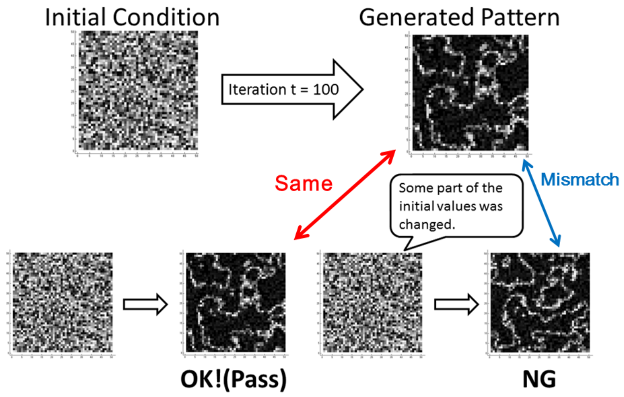

Figure 6: Framework of the authentication system and its process

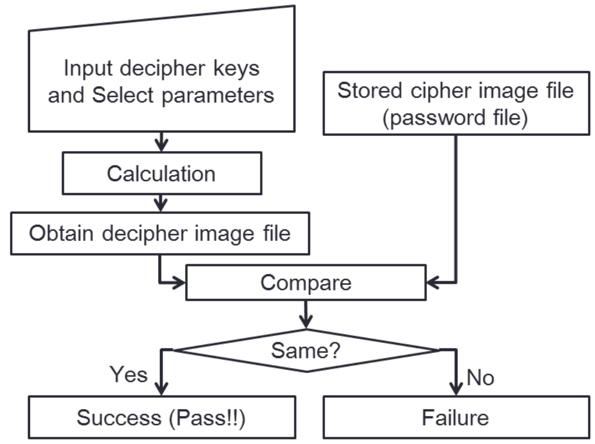

Figure 7: Authentication procedure of the proposed system

tem. At this moment, calculation costs are very high for a large scale network in our proposed system. However, we consider that validity and possibility of the proposed system using chaotic dynamics could be shown. We are now making applications on the other environments to evaluate of effectiveness for this scheme, and will show some examples in the near future.

4. Conclusions

In this study, we had proposed a new scheme of the authentication system using pattern dynamics based on coupled chaos map and showed the effectiveness of our proposed system. As an important property, when the parameters, number of calculations and initial values are all the same, there is uniqueness of the generated phase pattern in the coupled chaotic systems. Therefore, we found that it is not possible to generate the same pattern if the conditions were slightly different. Furthermore, we had evaluated these properties and proposed the authentication system using the pattern dynamics on the coupled chaotic maps. Although there are still problems in actual operation such as computation time, we are planning to solve these problems in the future work.

Acknowledgments

This work was supported in part by MEXT, Japan. I would like to thank Mr. Shintaro Tanaka for supporting several applications coded on MATLAB environment.

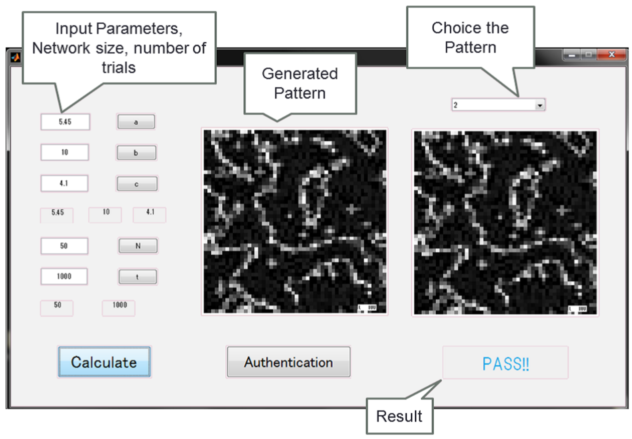

Figure 8: Construction of software implementation on MATLAB environment

References

[1] A. Nakamasu, G. Takahashi, A. Kanbe and S. Kondo, “Interactions Between Zebrafish Pigment Cells Responsible or the Generation of Turing Patterns,” Proc. of the National Academy of Sciences, vol. 106, no. 21, pp. 8429–8434, 2009.

[2] K. Kitatsuji and M. Wada, “Spatio-temporal Chaos and Several Phase Patterns in Coupled Chaotic Maps using Fifth-Power Function,” Proc. of International Workshop on Nonlinear Circuits, Communications and Signal Processing, pp. 113–116, 2005.

[3] M. Wada and T. Fukuda, “Analysis of Several Spatio-Temporal Phase Patterns in Coupled Chaotic Maps by Varying Coupling Strength,” Proc. of International Symposium on Nonlinear Theory and its Applications, pp. 500–503, 2010.

[4] S. Tanaka and M. Wada, “Authentication System using Pattern Dynamics of Coupled Chaotic Maps,” Proc. of 2016 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing, pp. 29–32, 2016.

[5] S. Tanaka and M. Wada, “Design of an Authentication Process and its Application Using Pattern Dynamics of Coupled Chaotic Maps,” Proc. of 2017 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing, pp. 237–240, 2017.