The composition of the improved logistic map and the MS map in generating a new chaotic function

Yudi Satria, Suryadi MT, Ita M Solihat, Luqman N Prawadika, Venny Melvina
Department of Mathematics, Universitas Indonesia, Depok, 16424, Indonesia
E-mail: ysatria@sci.ui.ac.id, yadi.mt@sci.ui.ac.id, summerbreeze91.im@gmail.com, nuradip.luqman@yahoo.com, venny.melvina@sci.ui.ac.id

Abstract. A new chaotic map is proposed from the composition of the improved logistic map and the MS map. The composition is done by mapping the MS map first, where the result is then mapped by the improved logistic map. The new map as the result of the composition is chaotic. This is shown by the Lyapunov Exponent analysis, bifurcation diagrams, and the NIST randomness test. The Lyapunov Exponent results with $x_0 = 0.1$ are non-negative for $r \in [1, 4]$. Its bifurcation diagrams with $p \in (0, 4)$ has a better density at $r = 2.5$. The new chaotic function also passes 10 out of 16 NIST test, with initial value and parameter values $x_0 = 0.1$, $r = 2.5$, and $p = 2.5$.

1. Introduction
Many attempts have been done in order to secure digital data by encryption, such as the chaos function usage. Chaotic systems are used to generate a keystream for data encryption [1]. Currently, many chaotic maps have been produced from researches applied in digital data encryption process [2-18]. Generating a new chaotic function by modification or combination of two or more chaotic functions is an effort to improve chaos based on cryptography encryption algorithm resistance [19-25].

Referring to previous researches, specifically those that utilizes the improved logistic map [26] and the MS Map [24, 25], in this paper, a new chaotic map will be developed from both maps by composition. The resulting function is also chaotic. Therefore, this new map is suitable as a new alternative for a random number generator, which later is applied in digital data encryption.

2. Research Method
The two functions used here are the modified versions of the Logistic Map. The Improved Logistic Map, introduced by Chanil et al. [26], is defined as:

$$x_{n+1} = F(u, x_n, k) = \mod\left(F_{\text{chaos}}(u, x_n) - F'_{\text{chaos}}(u, x_n)\right) \times G(k), 1 \right)$$  \hspace{1cm} (1)

where

$$G(k) = 2^k, 9 \leq k \leq 16$$
$$F_{\text{chaos}}(u, x_n) = 1D \text{ ordinary chaotic map}$$
$$F'_{\text{chaos}}(u, x_n) = \text{a function where } u \text{ in } F_{\text{chaos}}(u, x_n) \text{ is replaced by } (4-u)$$
$$\text{u = control parameter with range } [0, 2) \cup (2, 4]$$

Equation (2) shows the improved Logistic Map with $k = 12$ [26]:
\[ x_{n+1} = \text{mod} \left( (u \times x_n \times (1 - x_n) - (4 - u) \times x_n \times (1 - x_n)) \times 2^{12}, 1 \right) \]  

As for below is its Lyapunov Exponent and bifurcation diagram, shown in Figure 1 and Figure 2.

**Figure 1.** Lyapunov Exponent diagram of the improved Logistic Map [26]

**Figure 2.** Bifurcation Diagram of the Improved Logistic Map [26]

Meanwhile, the MS Map is defined as [24, 25]

\[ f(x) = \frac{r p x}{1 + p (1 - x)^2} \text{ (mod 1)} \]  

with \( x \text{ mod 1} \) is defined as

\[ x \text{ mod 1} = x - \lfloor x \rfloor \]  

Equation (1) and (3) can be rewritten in a recursion as

\[ x_{n+1} = \frac{r p x_n}{1 + p (1 - x_n)^2} \text{ (mod 1)} \]  

\[ x_{n+1} = \text{mod} \left( \frac{r p x_n}{1 + p (1 - x_n)^2}, 1 \right) \]  

with \( n = 0, 1, 2, 3, ..., \) initial value \( x_0 \in (0, 1) \), and parameter values \( r \in (0, 4) \) and \( p \in (0, 4) \).
Below is the formation of the new chaotic map through composition. Let \( f(x) \) be the improved Logistic Map and \( g(x) \) be the MS Map. The composition \( f \circ g \) is equal to

\[
(f \circ g)(x) = \text{mod}\left(\frac{(2r-4)(rpx_0)(p(1-x)^2)}{(1+p(1-x)^2)^2} \times 2^{12}, 1\right) 
\]

This new function as in equation (7) with little bit modification is then declared as the SIYu Map, whose recursive form is

\[
x_{n+1} = \text{mod}\left(\frac{(2r-4)(rpx_0)(p(1-x_0)^2)}{(1+p(1-x_0)^2)^2} \times 2^{14}, 1\right) 
\]

with \( n = 0,1,2,3,... \), initial value \( x_0 \in (0,1) \), and parameter values \( r \in (0,4) \) and \( p \in (0,4) \).

3. Result and Analysis

The SIYu Map as in equation (8) is chaotic. This is shown by the Lyapunov Exponent and the bifurcation diagram analysis [1,23,24,25]. Furthermore, the number sequence generated by the SIYu map is random. This is checked using the NIST randomness test [28].

3.1 Lyapunov Exponent

The Lyapunov Exponent of a dynamical system is the rate of separation of any two infinitesimally close trajectories.

Definition 1. [27]:

Suppose \( X \) is a set. The map \( f : X \to X \) is chaotic in \( X \) if \( f \) is sensitive to initial conditions, topologically transitive, and its periodical points are dense in \( X \).

A map \( f \) is chaotic if its Lyapunov Exponent is positive. Its equation is defined as [27]:

\[
h(x_i) = \lim_{n \to \infty} \frac{1}{n}\sum_{j=1}^{n} \ln|f'(x_j)| 
\]

For the SIYu map, the form of \( f'(x_j) \) based on equation (8) and (9) is

\[
(f \circ g)'(x) = \left(\frac{(2r-4)(rpx_0)(p(1-x)^2)}{(1+p(1-x)^2)^2} - (2p(px-p-1))(2r-4)(rpx)(p(1-x)^2))\right) \times 2^{14} 
\]

Figure 1 shows the Lyapunov Exponent graphic of the SIYu Map with \( x_0 = 0.1 \) and \( p = 2.5 \), obtained based on the following algorithm.

Algorithm 1. Lyapunov Exponent Diagram:

Input : \( x_0, p \), and \( r \)

Output : \( h(x) \) plot

1. Read initial value, parameters, number of iterations (\( n \))
2. For \( j = 1 \) to \( n \)
3. Calculate \( h(x_j) \) based on equation (9)
4. Plot \( h(x) \)
5. Next \( j \)
6. Stop
Figure 3 shows that for \( r \in [1,4] \), the map has positive Lyapunov Exponents. This means the new function is chaotic.

3.2 Bifurcation Diagram
The bifurcation diagram of a dynamical system is a diagram that shows asymptotically visited values of the system as a function of its parameters. The chaotic behaviour of a system can be observed based on the density of its bifurcation diagram [1,25].

**Algorithm 2. Bifurcation Diagram:**
- **Input**: \( x_0, p \) and \( r \)
- **Output**: plot \( x_n \)
  1. Read \( x_0 \), parameter value, number of iterations (k)
  2. For \( n = 1 \) to \( k \)
  3. Calculate \( x_n \) from equation (8)
  4. Plot \( x_n \)
  5. Next \( n \)
  6. Stop

As seen in Figure 4, the map's bifurcation diagram is dense for \( p \in (0, 4) \), meaning that the SIYu Map is chaotic for the initial value \( x_0 = 0.1 \) and parameter values of \( r = 2.5 \) and \( p \in [0, 4] \).
3.3. **NIST Randomness Test**

To check the randomness level of the number sequence generated by the SIYu Map, the NIST randomness test is conducted. This test suite is a statistical package that contains 16 test developed in binary form [28]. The result is shown on Table 1.

| Type of Test                                      | P-Value               | Conclusion    |
|--------------------------------------------------|-----------------------|---------------|
| 01. Frequency Test (Monobit)                      | 8.76466 × 10^{-29}    | Non-Random    |
| 02. Frequency Test within a Block                 | 0.88184               | Random        |
| 03. Run Test                                      | 0.0                   | Non-Random    |
| 04. Longest Run of Ones in a Block                | 0.24293               | Random        |
| 05. Binary Matrix Rank Test                       | 0.17896               | Random        |
| 06. Discrete Fourier Transform (Spectral) Test    | 0.89778               | Random        |
| 07. Non-Overlapping Template Matching Test        | 0.24092               | Random        |
| 08. Overlapping Template Matching Test            | 4.17413 × 10^{-5}     | Non-Random    |
| 09. Maurer's Universal Statistical test           | 0.55838               | Random        |
| 10. Linear Complexity Test                        | 0.71338               | Random        |
| 11. Serial test:                                  | 0.84669               | Random        |
| 12. Approximate Entropy Test                      | 0.08883               | Non-Random    |
| 13. Cumulative Sums (Forward) Test                | 4.00597 × 10^{-29}    | Non-Random    |
| 14. Cumulative Sums (Reverse) Test                | 1.51964 × 10^{-29}    | Non-Random    |
| 15. Random Excursions Test                        | 0.48352 *             | Random        |
| 16. Random Excursions Variant Test                | 0.56990 *             | Random        |

* average test value

Table 1 shows that the SIYu Map passes 10 out of 16 NIST test. Therefore, this function is a high quality random number generator with randomness rate of 62.5%.

4. **Conclusion**

The composition of the improved Logistic Map and MS Map generated the new chaotic SIYu Map. Its chaotic behavior is seen from its nonnegative Lyapunov Exponents and its dense bifurcation diagram for $x_0 = 0.1$, $r = 2.5$, and $p = 2.5$. The NIST randomness test shows that the chaotic SIYu map has a randomness level of 62.5%.

**Acknowledgments**

This research is funded by Direktorat Riset dan Pengabdian Masyarakat Universitas Indonesia in the scheme of Hibah PITTA B based on the contract No. NKB-0672/UN2.R3.1/HKP.05.00/2019.

**References**

[1] Kocarev L and Lian S. 2011 Chaos-Based Cryptography: Theory, Algorithm and Applications, (Berlin: Springer-Verlag)

[2] Laptyeva TV, Flach S and Kladko K. 2011 The weak password problem: Chaos, criticality, and encrypted p-CAPTCHAs *EPL* **95** 981-981

[3] Qinan L. 2011 Color image encryption algorithm and its decryption method protecting from shearing attack *Computer engineering and design* **32** 509-512

[4] Liu L, Zhang Q and Wei X. 2012 A RGB image encryption algorithm based on DNA encoding and Chaos Map *Computers and Electrical Engineering design* **38** 1240-1248

[5] Ahmad J and Ahmed F. 2012 Efficiency Analysis and Security Evaluation of Image Encryption Schemes *International Journal of Video & Image Processing and Network Security* **12** 18-31

[6] Eva N and Suryadi MT, 2013 Chaos-Based Encryption Algorithm for Digital Image *Proceedings IICMA* **169** 176-177

[7] Abu Zaid, Osama M., El-Fishawy, Nawal A., Nigm, E.M. 2013 Cryptosystem Algorithm Based on Chaotic System for Encrypting Colored Image, *International Journal of Computer Science Issues*, **10**, Issue 4, No 2, 215-224.

[8] Suryadi MT, Eva Nurpeti, and Dhian Widya 2014, Performance of Chaos-Based Encryption
Algorithm for Digital Image, Journal Telecommunication Computing Electronics and Control, Vol. 12, pp. 675-682, 2014.

[9] Suryanto Y, Suryadi MT, and Ramli K. 2016, A Secure and Robust Image Encryption Based on Chaotic Permutation Multiple Circular Shrinking and Expanding Journal of Information Hiding and Multimedia Signal Processing 7 697-713

[10] Suryanto Y, Suryadi MT, and Ramli K. 2017 A New Image Encryption using color scrambling based on chaotic permutation multiple circuler shrinking and Expanding Multimedia Tools and Applications 76 16831-16854

[11] Shujun L and Xuan Z, 2002 Cryptanalysis of a chaotic image encryption method International Symposium on Circuits and System 2 87-91.

[12] Sun F, Liu S and Li Z 2008 A novel image encryption scheme based on spatial chaos map Chaos Solitons Fractals 38 631-640

[13] Vinod P, Pareek NK, Purohita G and Suda KK 2011 A robust and secure chaotic standard map based pseudorandom permutation substitution scheme for image encryption Optics Commun 284 4331-4339

[14] Yunpeng Z, Fei Z, Zhengjun Z and Cai X 2008 A new image encryption Algorithm based on Multiple Chaos System International Symposium on Electronic Commerce and Security 142 347-350

[15] Pareek NK 2012 Design and Analysis of a Novel Digital Image Encryption Scheme International Journal of Network Security & Its Applications 4 95-108

[16] Yohan Suryanto , Suryadi MT , and Kalamullah Ramli 2016, A Secure and Robust Image Encryption Based on Chaotic Permutation Multiple Circular Shrinking and Expanding, Journal of Information Hiding and Multimedia Signal Processing.

[17] Tongfeng Zhang, Shouliang Li, Rongjun Ge, Min Yuan, and Yide Ma 2016. A Novel 1D Hybrid Chaotic Map-Based Image Compression and Encryption Using Compressed Sensing and Fibonacci-Lucas Transform. Hindawi Publishing Corporation Mathematical Problems in Engineering.

[18] Prajwalasiminha S N, Usha Surendra 2017 Multimedia Data Encryption based on Discrete Dyadic Transformation. International Conference on Signal Processing and Communication (ICSPC 2017).

[19] Magfirawaty, Andriani AL, Suryadi, Kalamullah Ramli 2018, Modified Logistic Maps for Discrete Time Chaos Based Random Number Generator, IEEE Xplore, pp. 391-396.

[20] Bo Li & Xiaofeng Liao & Yan Jiang 2017 A novel image encryption scheme based on logistic map and dynatonmic modular curve. Multimed Tools Appl (2018).

[21] Suryadi MT, Yudi Satria, Muhammad Fauzi 2018 Implementation of digital image encryption algorithm using logistic function and DNA encoding. Journal of Physics : Conference Series, IOP Publishing, Vol 974 (012028).

[22] Zhenjun Tang, Ye Yang, Shijie Xu, Chunqiang Yu, and Xianquan Zhang 2019 Image Encryption with Double Spiral Scans and Chaotic Maps. Hindawi Security and Communication Networks Volume 2019.

[23] Wu, X., Kana, H. and K Jürgen 2015 A New Color Image Encryption Scheme Based on DNA Sequences and Multiple Improved 1D Chaotic Maps. Applied Soft Computing 37, pp 24-39.

[24] Suryadi MT, Maria YTI, and Satria Y 2015 Encryption Algorithm using New Modified map for digital image Proceedings of IICMA pp 71-78

[25] Suryadi M T, Maria Y T I, and Yudi S 2017 New Modified Map for Digital Image Encryption and Its Performance. Journal of Physics: Conference Series, IOP Publishing, 893, 012050.

[26] Chanil Pak, Kwangil An, Paeksan Jang, Jonggun Kim, Sok Kim 2019 A Novel Bit-Level Color Image Encryption Using Improved 1D Chaotic Map. Multimedia Tools and Applications, 78:12027–12042

[27] Devaney, R.L 1989 An Introduction to Chaotic Dynamical Systems (2nd ed.). (Addison-Wesley Publishing company, Inc.)

[28] Andrew Rukhin, Juan Soto, et.all. 2010 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. (NIST Special Publication) 800-22.